Mathematics Handbook

Zexiang Chen
Guolong Li
Liang Zhang

June 26, 2013

Contents

I Elementary **1**

1 Notations **3**
1.1 Statement . . . 3
1.2 Elementary . . . 3
1.2.1 Number . . . 3
1.2.2 Functions . . . 3
1.3 Algebra . . . 3
1.4 Analysis . . . 3
1.5 Probability . . . 3

2 Sets **5**
2.1 Fundamentals . . . 5
2.2 Set Operations . . . 6
2.3 Images and Inverse Images . . . 7
2.4 Cartesian Product . . . 7
2.5 Cardinality of Sets . . . 8
2.6 Infinite Sets . . . 8
2.7 Other Definitions . . . 8

3 Numbers **9**
3.1 Natual Numbers . . . 9
3.1.1 Peano axioms and natural numbers . . . 9
3.1.2 Addition of natural numbers . . . 9
3.1.3 Multiplication of natural numbers . . . 11
3.2 Integers and Rational Numbers . . . 11
3.2.1 The integers . . . 11
3.2.2 Rational numbers . . . 13
3.2.3 Absolute value and exponentiation . . . 14
3.2.4 Gaps in the rational numbers . . . 16
3.3 Real Numbers . . . 16
3.3.1 Cauchy sequences . . . 16
3.3.2 Equivalent Cauchy sequences . . . 16
3.3.3 The construction of the real numbers . . . 16
3.3.4 Ordering the reals . . . 16
3.4 Complex Numbers . . . 16
3.5 Sequence . . . 16
3.6 Other Theorems . . . 17

4 Functions **19**
4.1 Fundamentals . . . 19
4.1.1 Definition . . . 19
4.1.2 Injective, surjective and bijective functions . . . 19
4.2 Elementary function . . . 20

4.2.1 Kronecker delta . . . 20
4.3 Hyperbolic function . . . 20
4.4 Binomial series . . . 22
4.5 Gamma function . . . 22
4.6 Beta function . . . 22

5 Vectors **25**

II Algebra **27**

6 Groups **29**
6.1 Groups . . . 29
6.1.1 Basic concepts . . . 29
6.1.2 Subgroup . . . 30
6.1.3 Class of groups . . . 31
6.1.4 Cycles . . . 33
6.1.5 Homomorphisms and isomorphisms . . . 34
6.1.6 Signs . . . 36
6.2 Cosets and Lagrange's theorem . . . 37
6.2.1 Cosets . . . 37
6.2.2 Lagrange's theorem . . . 38
6.3 Small groups . . . 40
6.3.1 Cyclic groups . . . 40
6.3.2 Direct (Cartesian) products of groups . . . 40
6.3.3 Dihedral groups . . . 41
6.3.4 The groups of order ≤ 10 . . . 41
6.4 Normal Subgroups, Quotient Groups and Isomorphism Theorem . . . 43
6.4.1 Normal Subgroups, Quotient Groups . . . 43
6.4.2 Isomorphism theorem . . . 44
6.4.3 Simple groups . . . 46
6.5 Group actions . . . 47
6.5.1 Group actions . . . 47
6.5.2 The orbit-stabiliser theorem . . . 48
6.5.3 Groups of symmetries of regular solids . . . 50
6.5.4 Burnside's Theorem . . . 50
6.5.5 Conjugation . . . 50
6.5.6 Cayley's theorem . . . 54
6.6 Finite p-groups and Finite Abelian Groups . . . 54
6.6.1 Finite p-groups . . . 54
6.6.2 Finite Abelian Groups . . . 56
6.7 Sylow's Theorems and Applications to Groups of Small Orders . . . 56
6.7.1 Sylow's theorems . . . 56
6.7.2 Applications to groups of small orders . . . 59
6.8 Summary . . . 60
6.8.1 List of small groups . . . 60
6.9 Problems . . . 60
6.9.1 Groups, subgroups, orders and homomorphism . . . 60
6.9.2 Normal groups and isomorphism theorems . . . 62
6.9.3 Group actions . . . 65
6.9.4 Sylow's theorem . . . 65

7 Rings **73**
7.1 Rings and Polynomials . . . 73
7.1.1 Definitions and Examples . . . 73
7.1.2 Polynomials . . . 74
7.2 Ring Homomorphism, Ideal, Quotient Ring and Isomorphism Theorems . . . 74
7.2.1 Ring Homomorphism . . . 74
7.2.2 Ideal . . . 75
7.2.3 Quotient ring . . . 76
7.2.4 Isomorphism theorems . . . 78
7.3 Integral Domain, Associativity, Irreducibility, Primeness and Field of Fractions . . . 79
7.3.1 Integral domain . . . 79
7.3.2 Associativity, irreducibility, primeness . . . 81
7.3.3 Field of fractions . . . 81
7.4 Principal Ideal Domain, Maximal Ideal and Prime Ideal . . . 82
7.4.1 Principal ideal domain . . . 82
7.4.2 Maximal ideal and prime ideal . . . 83
7.5 Euclidean Domain . . . 84
7.6 Ascending Chain Condition and Hilbert's basis theorem . . . 87
7.6.1 Ascending chain condition . . . 87
7.6.2 Hilbert's basis theorem . . . 87
7.7 Unique Factorisation Domain . . . 88
7.7.1 Unique factorisation domain . . . 88
7.7.2 Highest common factor . . . 89
7.8 Gauss' Lemma and Eisenstein's Criterion . . . 90
7.8.1 Content and primitiveness . . . 90
7.8.2 Gauss' lemma . . . 91
7.8.3 Eisenstein's criterion . . . 94
7.9 $\mathbb{Z}[\cdot]$ . . . 94
7.9.1 Gaussian integers $\mathbb{Z}[i]$ . . . 94
7.9.2 $\mathbb{Z}[\alpha]$ with α an algebraic integer . . . 96
7.10 Problems . . . 97
7.11 Summary . . . 107

8 Linear Algebra **109**
8.1 Vector spaces . . . 109
8.1.1 Definitions . . . 109
8.1.2 Algebra and subalgebra . . . 110
8.1.3 Linear span, linear independence, basis and dimension . . . 110
8.2 Vector Norm . . . 113
8.3 Linear maps . . . 114
8.3.1 Basic definitions and properties . . . 114
8.3.2 The vector space of linear maps . . . 116
8.3.3 Relation between linear maps and matrices . . . 117
8.3.4 Change of bases . . . 117
8.4 Endomorphisms . . . 118

9 Matrix **121**
9.1 Basic Definitions and Properties . . . 121
9.1.1 Definitions . . . 121
9.1.2 Multiplication of matrices . . . 121
9.1.3 Transpose . . . 122
9.1.4 Identity matrix . . . 122
9.1.5 Inverible matrices . . . 123

9.1.6 Equivalent matrices . . . 123
9.1.7 Ranks . . . 124
9.1.8 Elementary operations . . . 125
9.2 Square Matrices . . . 126
9.2.1 Basic square matrices . . . 126
9.2.2 Determinant . . . 128
9.2.3 Special square matrices . . . 131
9.2.4 Adjugate matrices . . . 133
9.2.5 Similar Matrices . . . 139
9.3 Groups of Matrices . . . 139
9.4 Matrix Calculus . . . 139
9.5 Problems . . . 139
9.6 Summary . . . 139

III Analysis 141

10 Real Analysis 143
10.1 Series . . . 143
10.2 Fundamental Axioms and Theorems . . . 143
10.2.1 Limits, convergence and fundamental axim of analysis . . . 143
10.2.2 The axiom of Archimedes . . . 143
10.2.3 Series and sums . . . 145
10.2.4 Absolute convergence . . . 149
10.2.5 Least upper bounds and greatest lower bounds . . . 150
10.2.6 Bolzano-Weierstrass theorem . . . 151
10.2.7 Cauchy sequences . . . 152
10.3 Continuity . . . 153
10.3.1 Definitions . . . 153
10.3.2 Limits of functions . . . 154
10.3.3 Bounded continuous functions . . . 155
10.3.4 Inverse functions . . . 156
10.3.5 Càdlàg function . . . 156
10.3.6 Uniform continuity . . . 159
10.4 Differentiability . . . 159
10.4.1 Definitions . . . 159
10.4.2 Mean value theorem . . . 162
10.4.3 Inverse Rule (Inverse Function Theorem) . . . 163
10.4.4 Taylor's theorems . . . 165
10.5 Power Series . . . 167
10.5.1 Trigonometric functions . . . 171
10.5.2 Hyperbolic functions . . . 172
10.6 Integration . . . 172
10.6.1 Riemann integration . . . 172
10.6.2 Elementary properties of the integral . . . 176
10.6.3 Infinite integrals (Improper integrals) . . . 180
10.6.4 Final remarks on improper integrals . . . 182
10.6.5 Stirling's formula . . . 183
10.7 Euclidean Space . . . 184
10.8 Norms . . . 184
10.9 Inner Product . . . 184
10.10Function Sequences . . . 184
10.11Problems . . . 185

11 Complex Analysis **187**

12 Metric Space **189**

13 Topological Space **193**
13.1 Topology . . . 193
13.1.1 Topology and topological space . . . 193
13.2 Spaces . . . 193
13.3 Function Sequence . . . 193

14 Linear Analysis **195**

15 Measure Theory **197**
15.1 Set Systems and Measures . . . 197
15.1.1 Set systems . . . 197
15.1.2 Measures . . . 200
15.1.3 Existence and Uniqueness . . . 205
15.1.4 Measure notations . . . 208
15.1.5 Lebesgue measure . . . 208
15.2 Measurable Functions . . . 211
15.2.1 Measurable functions . . . 211
15.2.2 Image measures . . . 214
15.2.3 Convergence in measure and convergence almost everywhere . . . 215
15.3 Integration and Basic Theorems . . . 216
15.3.1 Definition of integral and basic properties . . . 216
15.3.2 Integrals and limits . . . 222
15.3.3 Transformations of integrals . . . 226
15.3.4 Relation to Riemann integral . . . 228
15.3.5 Fundamental theorem of calculus . . . 229
15.3.6 Differentiation under integral sign . . . 231
15.3.7 Product measure and Fubini's theorem . . . 231
15.3.8 Applications . . . 236
15.4 $\mathcal{L}^p$ Space, L^p Space and Convergence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$ . . . 237
15.4.1 $\mathcal{L}^p$-norms . . . 237
15.4.2 Chebyshev's inequality . . . 237
15.4.3 Jensen's inequality . . . 238
15.4.4 Hölder's inequality and Minkowski's inequality . . . 239
15.4.5 Completeness of $\mathcal{L}^p$ . . . 241
15.4.6 L^p space . . . 243
15.4.7 Orthogonal Projection . . . 243
15.4.8 Uniform integrable . . . 244
15.4.9 Convergence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$ . . . 246
15.4.10 Dense property . . . 249
15.4.11 Fourier transform . . . 249
15.5 Convergence of Measures . . . 251
15.5.1 Weak convergence and vague convergence . . . 251
15.5.2 Tightness . . . 253
15.6 Ergodic theory . . . 253
15.6.1 Measure-preserving transformations . . . 253
15.6.2 Ergodic measure-preserving transformation . . . 254
15.6.3 Birkhoff's and von Neumann's ergodic theorems . . . 255
15.7 Signed Measure . . . 260
15.8 Problems . . . 260

IV Dynamics **261**

16 Differential Equations **263**
16.1 Some literature reviews . . . 263
16.2 Modified Bessel functions . . . 263
16.2.1 Definition . . . 263
16.2.2 General case ν . . . 263
16.2.3 Special case ν . . . 264

V Geometry **265**

17 Geometry **267**

18 Differential Geometry **269**
18.1 . . . 269

VI Probability **271**

19 Probability **273**
19.1 Basic Concepts . . . 273
19.1.1 Sample spaces, events and probability . . . 273
19.1.2 Combinatorial analysis . . . 275
19.1.3 Independence and Borel-Cantelli lemmas . . . 278
19.2 Random variables . . . 280
19.2.1 Random variables . . . 280
19.2.2 Independence of random variables . . . 282
19.2.3 Rademacher functions . . . 284
19.2.4 Tail events . . . 285
19.2.5 Large values in sequences of IID random variables . . . 286
19.2.6 Convergence almost surely and convergence in probability . . . 287
19.3 Expectation and Convergence in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ . . . 287
19.3.1 Expectation . . . 287
19.3.2 Convergence Theorems for probability . . . 289
19.3.3 Transformations of expectations and density function . . . 291
19.3.4 Inequalities and orthogonal projection . . . 293
19.3.5 Bounded in $\mathcal{L}^p$ and uniform integrability . . . 294
19.3.6 Convergence in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ . . . 296
19.3.7 Variance and covariance . . . 297
19.4 Conditional Expectation . . . 299
19.4.1 Elementary conditional probabilities of events . . . 299
19.4.2 Elementary conditional probabilities of random variables . . . 303
19.4.3 Conditional expectation . . . 305
19.4.4 Non-negative conditional expectation . . . 307
19.4.5 Specific theorems of conditional expectation . . . 308
19.4.6 Uniformly integrable property and multivariable conditional expectation . . . 312
19.4.7 Conditional probability density function . . . 313
19.5 Characteristic Function and Moment Generating Function . . . 314
19.5.1 Characteristic function . . . 314
19.5.2 Characteristic functions and independence . . . 317
19.5.3 Moment generating function . . . 320
19.6 Convergence in Distribution and Weak Convergence . . . 322
19.6.1 Convergence in distribution for random variables . . . 322

19.6.2 Weak convergence . . . 323
19.6.3 Tightness and Lévy's convergence theorem . . . 325
19.7 Discrete Random Variables . . . 328
19.7.1 Discrete random variable and probability generating function . . . 328
19.7.2 Bernoulli random variables . . . 330
19.7.3 Binomial random variables . . . 331
19.7.4 Geometric random variables . . . 332
19.7.5 Negative binomial random variables . . . 333
19.7.6 Poisson random variables . . . 336
19.8 Continuous Random Variables . . . 337
19.8.1 Continuous random variable . . . 337
19.8.2 Uniform random variables . . . 337
19.8.3 Exponential random variables . . . 343
19.8.4 Gaussian random variables . . . 345
19.8.5 Cauchy random variables . . . 350
19.8.6 Gamma random variables . . . 351
19.8.7 Beta random variables . . . 353
19.9 Sums of independent random variables . . . 353
19.9.1 Weak Law of large numbers . . . 353
19.9.2 Strong law of large numbers for finite fourth moment . . . 355
19.9.3 Canonical probability space . . . 356
19.9.4 Stationary sequence of random variables . . . 357
19.9.5 Strong law of large numbers . . . 358
19.9.6 Central limit theorem . . . 359
19.10 Geometric probability . . . 361
19.10.1 Buffon's needle . . . 361
19.10.2 Bertrand's Paradox . . . 362
19.11 Problems . . . 363
19.11.1 Classical probability . . . 363
19.11.2 Theoretical problems . . . 364
19.11.3 Random variables . . . 368
19.11.4 Practical problems . . . 370

20 Stochastic Processes and Martingale Theory 375
20.1 Discrete-time Processes . . . 375
20.1.1 Stochastic processes and filtrations . . . 375
20.1.2 Stopping times . . . 375
20.1.3 Branching process . . . 377
20.1.4 Random walks . . . 377
20.2 Discrete-time Martingales . . . 377
20.2.1 Definitions . . . 377
20.2.2 Previsible process and construction of a martingale . . . 378
20.2.3 Optional stopping theorem for bounded stopping time . . . 379
20.2.4 Martingale Convergence Theorem . . . 381
20.2.5 Doob's inequalities and Kolmogorov's inequality . . . 383
20.2.6 Convergence in $\mathcal{L}^p$ for $p \in (1, \infty)$ . . . 385
20.2.7 UI martingale and convergence in $\mathcal{L}^1$ . . . 387
20.2.8 Backward martingales . . . 389
20.3 Applications of Discrete Time Martingales . . . 390
20.3.1 Strong law of large numbers . . . 390
20.3.2 Kakutani's theorem for product martingales . . . 391
20.3.3 Radon-Nikodym theorem . . . 392
20.4 Continuous-time Processes . . . 393

20.4.1 Definition . . . 393
20.4.2 Stopping time properties . . . 396
20.4.3 Technical issues in dealing with continuous-time . . . 399
20.4.4 Càdlàg processes, finite variation processes . . . 400
20.4.5 Finite dimensional marginal distributions . . . 401
20.4.6 Versions and indistinguishability . . . 402
20.4.7 Canonical Processes . . . 404
20.4.8 Previsible processes and finite variation integrals . . . 404
20.4.9 Convergence of stochastic processes . . . 413
20.5 Continuous-time Martingales . . . 415
20.5.1 Definitions . . . 415
20.5.2 Martingale regularization theorem . . . 417
20.5.3 Martingale convergence theorem and inequalities . . . 420
20.5.4 Convergence in continuous time . . . 422
20.5.5 Optional stopping theorems . . . 423
20.5.6 Convergence of martingale sequence . . . 425
20.6 Local Martingales . . . 426
20.6.1 Definitions . . . 426
20.6.2 The relationship between martingales and local martingales . . . 428
20.6.3 Local martingale properties . . . 430
20.6.4 Semimartingales . . . 431

21 Markov Chains **433**
21.1 Discrete-time Markov Chains . . . 433
21.1.1 Definition and basic facts . . . 433
21.2 Continuous-time Markov Chains . . . 433
21.3 Problems . . . 433
21.3.1 Discrete-time Markov chains . . . 433
21.3.2 Continuous-time Markov chains . . . 436

22 Brownian Motion, Poisson Process and Lévy Process **439**
22.1 Brownian Motion . . . 439
22.1.1 History and definition . . . 439
22.1.2 Basic properties . . . 444
22.1.3 Markov property . . . 445
22.1.4 Reflection principle . . . 449
22.1.5 Martingales for Brownian Motion . . . 450
22.1.6 Recurrence and Transience . . . 455
22.1.7 Conditioned Brownian motion and Brownian bridge . . . 458
22.1.8 Quadratic variation . . . 460
22.2 Problems . . . 462
22.2.1 Brownian motion . . . 462

23 Stochastic Calculus **465**
23.1 Itô Stochastic Integral . . . 465
23.1.1 Simple integrands and $\mathcal{M}^2$ properties . . . 465
23.1.2 Quadratic variation . . . 471
23.1.3 Itô stochastic integrals for $\mathcal{L}^2(M)$ with $M \in \mathcal{M}_c^2$ . . . 476
23.1.4 Stochastic integrals for locally bounded previsible processes with $M \in \mathcal{M}_{c,loc}^2$ . . . 480
23.1.5 Covariation . . . 483
23.1.6 Stochastic integral for semimartingales . . . 487
23.1.7 Itô's formula . . . 491
23.2 Applications to Brownian Motion and Martingales . . . 494

23.2.1 Brownian martingales . . . 494
23.2.2 Dubins-Schwarz theorem . . . 497
23.3 Stochastic Differential Equations . . . 498
23.4 Problem . . . 498

VII Statistics **499**

24 Distributions **501**
24.0.1 Gaussian distribution . . . 501
24.0.2 Chi-squared random variables . . . 501
24.0.3 Student-t random variables . . . 505
24.0.4 Inverse Gaussian random variables . . . 508
24.0.5 Generalized inverse Gaussian random variables . . . 510
24.0.6 Weibull random variables . . . 512
24.0.7 Hyperbolic random variables . . . 512
24.0.8 Generalized hyperbolic random variables . . . 514

25 Statistics **515**
25.0.9 Linear model . . . 515

VIII Optimization **517**

26 Optimization **519**
26.1 Problems . . . 519

Part I

Elementary

Chapter 1

Notations

1.1 Statement

'iff' is shorthand for 'if and only if'.

'x:=y' denotes the statement that x is defined to equal y.

1.2 Elementary

1.2.1 Number

$\mathbb{Z}^+ := \{1, 2, \dots\}$. $\mathbb{N} := \{0, 1, 2, 3, \dots\}$. Clearly, $\mathbb{Z}^+ \subset \mathbb{N}$.

$\mathbb{R}^+ := (0, \infty)$, $\mathbb{Q}^+ := \mathbb{Q} \cap \mathbb{R}^+$. $\mathbb{R}^{++} := [0, \infty)$. $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$.

$f \vee g = \max\{f, g\}$, $f \wedge g = \min\{f, g\}$, $f^+ = f \vee 0$, $f^- = (-f) \vee 0$.

$\overline{z}$ for conjugate of z (number), $\overline{A}$ for conjugate of A (vector, matrix, etc.)

α^* is the dual of α where α is a linear map.

1.2.2 Functions

Y^X is the set of all function maps from X to Y, i.e., $f : X \to Y$.

1.3 Algebra

$\mathbb{F}_p$ is a field with p elements.

If p is a prime number, we have $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} := \{0, 1, \dots, p-1\}$.

$\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ where p is a prime number.

$M_{m,n}(\mathbb{F})$ are $m \times n$ matrices over field $\mathbb{F}$.

1.4 Analysis

1.5 Probability

Chapter 2

Sets

2.1 Fundamentals

Definition 2.1.1 (set, element)**.** A set A is any unordered collection of objects.

If x is an object, we say that x is an element of A or $x \in A$ if x lies in the collection; otherwise we say that $x \notin A$.

Axiom 2.1.1 (sets are objects)**.** If A is a set, then A is also an object. In particular, given two sets A and B, it is meaningful to ask whether A is also an element of B.

Definition 2.1.2 (equality of sets)**.** Two sets A and B are equal, $A = B$ iff every element of A is an element of B and vice versa. To put it another way, $A = B$ if and only if every element x of A belongs also to B, and every element y of B belongs also to A.

Example 2.1.2. For instance, $\{a, b, c, d, e\}$ and $\{c, d, b, a, e\}$ are the same set.

The $\{c, c, a, e, b, d, b\}$ is also equal to $\{a, b, c, d, e\}$; the repetition of b and c is irrelevant as it does not further change the status of b and c being elements of the set.

Axiom 2.1.3 (empty set)**.** There exists a set $\emptyset$, known as the empty set, which contains no elments, i.e., for every object x we have $x \notin \emptyset$.

Remark. Note that there can only be one empty set; if there were two sets $\emptyset$ and $\emptyset'$ which were both empty, then by Definition 2.1.2 they would be equal to each other.

Lemma 2.1.4 (single choice)**.** Let A be a non-empty set. Then there exists an object x such that $x \in A$.

Proof. We prove by contradiction. Suppose there does not exist any object $x \in A$. Then for all objects x, we have $x \notin A$. Also, by Axiom 2.1.3 we have $x \notin \emptyset$. Thus, $x \in A \Leftrightarrow x \in \emptyset$ (both statements are equally false), and so $A = \emptyset$ by Definition 2.1.2. Contradiction. □

Axiom 2.1.5 (singleton sets and pair sets)**.** If a is an object, then there exists a set $\{a\}$ whose only element is a, i.e., for every object y, we have $y \in \{a\}$ if and only if $y = a$; we refer to $\{a\}$ as the singleton set whose element is a.

Furthermore, if a and b are objects, then there exists a set $\{a, b\}$ whose only elements are a and b; i.e., for every object y, we have $y \in \{a, b\}$ if and only if $y = a$ or $y = b$; we refer to this set as the pair set formed by a and b.

Definition 2.1.3 (subset)**.** Let A, B be sets. Then A is a subset of B, denoted $A \subseteq B$, iff every element of A is also an element of B, i.e., for any object x, $x \in A \Rightarrow x \in B$.

We say that A is a proper subset of B, denoted $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Remark. Given any set A, we always have $A \subseteq A$ and $\emptyset \subseteq A$.

Example 2.1.6. $\{a, b, d\} \subset \{a, b, c, d, e\}$.

Proposition 2.1.7 (sets are partially ordered by set inclusion)**.** Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. If $A \subseteq B$ and $B \subseteq A$, then $A = B$. Finally, if $A \subset B$ and $B \subset C$ then $A \subset C$.

Proof. [1] □

[1] need proof

Axiom 2.1.8 (axiom of specification)**.** Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (i.e., $P(x)$ is either a true statement or a false one). Then there exists a set called $\{x \in A : P(x) \text{ is true}\}$, whose elements are precisely the elements x in A for which $P(x)$ is true. In other words, for any object y,

$$y \in \{x \in A : P(x) \text{ is true}\} \Rightarrow y \in A \text{ and } P(y) \text{ is true.} \tag{2.1.1}$$

Axiom 2.1.9 (axiom of replacement)**.** Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y : P(x, y)\}$ is true for some $x \in A$, such that for any object z,

$$z \in \{y : P(x, y) \text{ is true for some } x \in A\} \Leftrightarrow P(x, z) \text{ is true for some } x \in A. \tag{2.1.2}$$

2.2 Set Operations

Axiom 2.2.1 (pairwise union)**.** Given any two sets A, B, there exists a set $A \cup B$, called the union $A \cup B$ of A and B, whose elements consists of all the elements which belong to A or B or both. In other words, for any object x,

$$x \in A \cup B \Rightarrow x \in A \text{ or } x \in B. \tag{2.2.1}$$

Note that $A \cup B = B \cup A$ as the set is unordered.

Example 2.2.2. $\{a, b\} \cup \{b, c\} = \{a, b, c\}$.

Remark. If A, B, A' are sets, and A is equal to A', then $A \cup B$ is equal to $A' \cup B$.[2]

Lemma 2.2.3. If a and b are objects, then $\{a, b\} = \{a\} \cup \{b\}$. If A, B, C are sets, then the union operation is commutative (i.e., $A \cup B = B \cup A$) and associative (i.e., $(A \cup B) \cup C = A \cup (B \cup C)$).

Also, we have $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.

Proof. [3] □

Definition 2.2.1 (intersection)**.** The intersection $A \cap B$ of two sets A, B is defined to be the set

$$A \cap B = \{x \in A : x \in B\}. \tag{2.2.2}$$

In other words, $A \cap B$ consists of all the elements which belong to both A and B. Thus, for all object x,

$$x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B. \tag{2.2.3}$$

Note that $A \cap B = B \cap A$ as the set is unordered.

Example 2.2.4. $\{a, b, d\} \cap \{b, c, d\} = \{b, d\}$, $\{a, b\} \cap \{c, d\} = \emptyset$.

Definition 2.2.2 (difference set)**.** Given two sets A and B, we define the set $A - B$ or $A \backslash B$ to be the set A with any elements of B removed:

$$A \backslash B := \{x \in A : x \notin B\}. \tag{2.2.4}$$

Note that in many cases B will be a subset of A, but not necessarily.

Proposition 2.2.5 (sets form a boolean algebra)**.** Let A, B, C be sets, and let X be a set containing A, B, C as subsets.

(i) (minimal element) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

(ii) (maximal element) $A \cup X = X$ and $A \cap X = A$.

(iii) (identity) $A \cap A = A$ and $A \cup A = A$.

(iv) (commutativity) $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

[2] need proof.
[3] need proof

(v) (associativity) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.

(vi) (distributivity) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(vii) (partition) $A \cup (X \backslash A) = X$ and $A \cap (X \backslash A) = \emptyset$.

(viii) (De Morgan laws) $X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B)$ and $X \backslash (A \cap B) = (X \backslash A) \cup (X \backslash B)$.

Proof. [4] □

Remark. The above laws are collectively known as the laws of Boolean algebra, after the mathematician Geoge Boole (1815-1864), and are also applicable to a number of other objects other than sets; it plays a particularly impartant role in logic.

Definition 2.2.3 (symmetric difference)**.** Given two sets A, B, the symmetric difference is written by $A \triangle B = (A \backslash B) \cup (B \backslash A)$.

2.3 Images and Inverse Images

Definition 2.3.1 (images of set)**.** If $f : X \to Y$ is function from X to Y (see Definition 4.1.1), and S is subset in X, we define $f(S)$ to be the set

$$f(S) := \{f(x) : x \in S\}; \tag{2.3.1}$$

this set is a subset of Y, and is sometimes called the image of S under the map f. We sometimes call $f(S)$ the forward image of S to distinguish it from the concept of the inverse image $f^{-1}(S)$ of S, which is defined below.

Definition 2.3.2 (inverse image)**.** If U is a subset of Y, we define the set $f^{-1}(U)$ to be the set

$$f^{-1}(U) := \{x \in X : f(x) \in U\}. \tag{2.3.2}$$

In other words, $f^{-1}(U)$ consists of all the elements of X which map into U:

$$f(x) \in U \;\Leftrightarrow\; x \in f^{-1}(U). \tag{2.3.3}$$

We call $f^{-1}(U)$ the inverse image of U.

Proposition 2.3.1. Let A, B be two subsets of a set X, and let $f : X \to Y$ be a function. Then

$$f(A \cap B) \subseteq f(A) \cap f(B), \quad f(A) \backslash f(B) \subseteq f(A \backslash B), \quad f(A \cup B) = f(A) \cup f(B). \tag{2.3.4}$$

Proof. [5] □

Proposition 2.3.2. Let $f : X \to Y$ be a function from one set X to another set Y, and let A, B be subsets of Y. Then

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), \quad f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B), \quad f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B). \tag{2.3.5}$$

Proof. [6] □

2.4 Cartesian Product

Definition 2.4.1 (ordered pair)**.** If x and y are any objects (possibly equal), we define the ordered pair (x, y) to be a new object, consisting of x as its first component and y as its second component.

Definition 2.4.2 (equality of ordered pair)**.** Two ordered pairs (x, y) and (x', y') are considered equal if and only if their components match, i.e.,

$$(x, y) = (x', y') \;\Leftrightarrow\; x = x', y = y'. \tag{2.4.1}$$

[4] need proof
[5] need proof
[6] need proof

2.5 Cardinality of Sets

2.6 Infinite Sets

Proposition 2.6.1 (inverse image preserves set operation[7])**.** For any function $f : X \to Y$, the inverse image preserves set operations, for subsets $A_i, A \subseteq B$ of Y

$$f^{-1}\left(\bigcup_i A_i\right) = \bigcup_i f^{-1}(A_i), \qquad f^{-1}(B \backslash A) = f^{-1}(B) \setminus f^{-1}(A)\ . \tag{2.6.1}$$

Proof. First,

$$\begin{aligned} x \in f^{-1}\left(\bigcup_i A_i\right) \ \Leftrightarrow\ f(x) \in \bigcup_i A_i \quad &\Leftrightarrow \quad f(x) \in A_i \text{ for some } i \\ &\Leftrightarrow \quad x \in f^{-1}\left(A_i\right) \text{ for some } i \ \Leftrightarrow\ x \in \bigcup_i f^{-1}\left(A_i\right). \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(B \backslash A) \ \Leftrightarrow\ f(x) \in B \backslash A \quad &\Leftrightarrow \quad f(x) \in B,\ f(x) \in A^c \\ &\Leftrightarrow \quad x \in f^{-1}\left(B\right),\ x \in f^{-1}\left(A^c\right) \\ &\Leftrightarrow \quad x \in f^{-1}\left(B\right),\ x \in \left(f^{-1}\left(A\right)\right)^c \ \Leftrightarrow\ x \in f^{-1}(B) \setminus f^{-1}(A)\ . \end{aligned}$$

□

2.7 Other Definitions

Definition 2.7.1 (supremum, infimum)**.**

Definition 2.7.2. The support of a function is the set of points where the function is not zero, or the closure of that set.[8]

Definition 2.7.3. Functions with compact support in X are those with support that is a compact subset of X.

Remark. If X is the real line, they are functions of bounded support and therefore vanish at infinity (and negative infinity).

[7] need $\alpha \in I$ (infinity) argument
[8] should be put in topology

Chapter 3

Numbers

3.1 Natual Numbers

3.1.1 Peano axioms and natural numbers

First we recall the definition of natural number from [15].P_{17-50}[1].

Axiom 3.1.1 (natural numbers)**.** There exists a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object 0 in $\mathbb{N}$, and object $n++$ assigned to every natural number $n \in \mathbb{N}$, such that the following axioms (Peano axioms) hold:

(i) 0 is a natural number.

(ii) If n is a natural number, then $n++$ is also a natural number.

(iii) 0 is not the successor of any natural number; i.e., we have $n++ \neq 0$ for every natural number n.

(iv) Different natural numbers must have different successors; i.e., if n, m are natural numbers and $n \neq m$, then $n++ \neq m++$. Equivalently, if $n++ = m++$, then we must have $n = m$.

(v) (principle of mathematical induction). Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n++)$ is also true. Then $P(n)$ is true for every natural number n.

Remark. [2]

Remark. One interesting feature about the natural numbers is that while each individual natural number is finite[3], the set of natural numbers is infinite [15].P_{24}.

3.1.2 Addition of natural numbers

Definition 3.1.1 (addition of natural numbers)**.** Let m be a natural number. To add zero to m, we define $0+m := m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n{+}{+}$ to m by defining $(n{+}{+}){+}m := (n{+}m){+}{+}$.

Lemma 3.1.2. For any natural number n, $n + 0 = n$.

Proof. [4] □

Lemma 3.1.3. For any natural numbers n and m, $n + (m++) = (n + m)++$.

Proof. [5] □

Proposition 3.1.4 (addition is commutative)**.** For any natural numbers n and m, $n + m = m + n$.

Proof. [6] □

[1] need to introduce 0 and increment operation ++ first
[2] explain the axioms
[3] need definition
[4] need proof
[5] need proof
[6] need proof

Proposition 3.1.5 (addition is associative)**.** For any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$..

Proof. [7] □

Proposition 3.1.6 (cancellation law)**.** Let a, b, c be natural numbers such that $a + b = a + c$. Then we have $b = c$.

Proof. [8] □

Definition 3.1.2 (positive natural numbers)**.** A natural number n is said to be positive iff it is not equal to 0.

Proposition 3.1.7. If natural number a is positive and b is a natural number, then $a + b$ is positive. Hence $b + a$ is also positive by Proposition 3.1.4.

Proof. [9] □

Corollary 3.1.8. If a and b are natural numbers such that $a + b = 0$, then $a = 0$ and $b = 0$

Proof. [10] □

Lemma 3.1.9. Let a be a positive number. Then there exists exactly one natural number b such that $b++ = a$.

Proof. [11] □

Definition 3.1.3 (ordering of the natural numbers)**.** Let n and m be natural numbers. We say that n is greater than or equal to m, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some natrual number a. We say that n is strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

Proposition 3.1.10 (basic properties of order for natural numbers)**.** Let a, b, c be natural numbers. Then

(i) (order is reflexive). $a \geq a$.

(ii) (order is transitive). If $a \geq b$ and $b \geq c$, then $a \geq c$.

(iii) (order is anti-symmetric). If $a \geq b$ and $b \geq a$, then $a = b$.

(iv) (addition preserves order). $a \geq b$ if and only if $a + c \geq b + c$.

(v) $a < b$ if and only if $a++ \leq b$.

(vi) $a < b$ if and only if $b = a + d$ for some positive natural number d.

Proof. [12] □

Proposition 3.1.11 (trichotomy of order for natural numbers)**.** Let a and b be natural numbers. Then exactly one of the following statement is true: $a < b$, $a = b$, or $a > b$.

Proof. [13] □

Proposition 3.1.12 (strong principle of induction)**.** Let m_0 be natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' \leq m$, then $P(m)$ is also true. In particular, this means that $P(m_0)$ is true, since in this case the hypothesis is vacuous. Then we can conclude that $P(m)$ is true for all natural numbers $m \geq m_0$.

Proof. [14] □

[7] need proof
[8] need proof
[9] need proof
[10] need proof
[11] need proof
[12] need proof
[13] need proof
[14] need proof

3.1.3 Multiplication of natural numbers

Definition 3.1.4 (multiplication of natural numbers)**.** Let m be a natural number. To multiply zero to m, we define $0 \times m := 0$. Now suppose inductively that we have defined how to multiply $n \to m$. Then we can multiply $n++$ to m by defining $(n++) \times m := (n \times m) + m$.

Remark. We can abbreviate $n \times m$ as nm.

Lemma 3.1.13 (multiplication is commutative)**.** Let n, m be natural numbers. Then $n \times m = m \times n$.

Remark. Therefore, we have no confusion on abc ($a \times b \times c$) where a, b, c are natural numbers.

Proof. [15] □

Lemma 3.1.14 (natural numbers have no zero divisors)**.** Let n, m be natural numbers. Then $n \times m = 0$ if and only if at least one of n, m is equal to zero. In particular, if n and m are both positive, then nm is positive.

Proof. [16] □

Proposition 3.1.15 (distributive law)**.** For any natural numbers a, b, c, we have

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca. \tag{3.1.1}$$

Proof. [17] □

Proposition 3.1.16 (multiplication is associative)**.** For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.

Proof. [18] □

Proposition 3.1.17 (multiplication preserves order)**.** If a, b are natural numbers, such that $a < b$, and c is positive, then $ac < bc$.

Proof. [19] □

Corollary 3.1.18 (cancellation law)**.** Let a, b, c be natural numbers, such that $ac = bc$ and c is non-zero. Then $a = b$.

Proof. [20] □

Proposition 3.1.19 (Euclidean algorithm)**.** Let n be a natural number, and let q be a positive natural number. Then there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.

Proof. [21] □

3.2 Integers and Rational Numbers

3.2.1 The integers

Definition 3.2.1 (intergers)**.** An integer is an expression[22] of the form $a—b$[23], where a and b are natural numbers. Two integers are considered to be equal, $a—b = c—d$, if and only if $a + d = c + b$. We let $\mathbb{Z}$ denote the set of all integers.

[15] need proof
[16] need proof
[17] need proof
[18] need proof
[19] need proof
[20] need proof
[21] need proof
[22] In the language of set theory, what we are doing here is starting with the space $\mathbb{N} \times \mathbb{N}$ of ordered pairs (a, b) of natural numbers. Then we place an equivalence relation $\sim$ on these pairs by declaring $(a, b) \sim (c, d)$ iff $a + d = c + b$. The set-theoretic interpretation of the symbol $a—b$ is that it is the space of all pairs equivalent to (a, b): $a—b := \{(c, d) \in \mathbb{N} \times \mathbb{N} : (a, b) \sim (c, d)\}$.
[23] need to check this is an equivalence relation

Definition 3.2.2. The sum of two integers, $(a—b) + (c—d)$, is defined by the formula

$$(a—b) + (c—d) := (a + c)—(b + d). \tag{3.2.1}$$

The product of two integers, $(a—b) \times (c—d)$, is defined by

$$(a—b) \times (c—d) := (ac + bd)—(ad + bc). \tag{3.2.2}$$

Lemma 3.2.1 (addition and multiplication of integers are well-defined)**.** Let a, a', b, b', c, d be natural numbers. If $(a—b) = (a'—b')$, then $(a—b) + (c—d) = (a'—b') + (c—d)$ and $(a—b) \times (c—d) = (a'—b') \times (c—d)$, and also $(c—d) + (a—b) = (c—d) + (a'—b')$ and $(c—d) \times (a—b) = (c—d) \times (a'—b')$.

Thus addition and multiplication are well-defined operations (equal inputs give equal outputs).

Proof. [24] □

Definition 3.2.3 (negation of integers)**.** If $(a—b)$ is an integer, we define the negation $-(a—b)$ to be the integer $(b—a)$. In particular if $n = n—0$ is a positive natural number, we can define its negation $-n = 0—n$.

Lemma 3.2.2. Let x be an integer. Then exactly one of the following three statements is true:

(i) x is zero;

(ii) x is equal to a positive natural number n;

(iii) x is negation $-n$ of a positive natural number n.

Proof. [25] □

Proposition 3.2.3 (laws of algebra for integers)**.** Let x, y, z be integers. Then we have

(i) $x + y = y + x$.

(ii) $(x + y) + z = x + (y + z)$.

(iii) $x + 0 = 0 + x = x$.

(iv) $x + (-x) = (-x) + x = 0$.

(v) $xy = yx$.

(vi) $(xy)z = x(yz)$.

(vii) $x1 = 1x = x$.

(viii) $x(y + z) = xy + xz$.

(ix) $(y + z)x = yx + zx$.

Proof. [26] □

Definition 3.2.4 (subtraction)**.** We define the operation of subtraction $x - y$ of two integers by the formula

$$x - y := x + (-y). \tag{3.2.3}$$

Proposition 3.2.4 (integers have no zero divisors)**.** Let a and b be integers such that $ab = 0$. Then either $a = 0$ or $b = 0$ (or both).

Proof. [27] □

Corollary 3.2.5 (cancellation law for integers)**.** If a, b, c are integers such that $ac = bc$ and c is non-zero, then $a = b$.

[24] need proof
[25] need proof
[26] need proof
[27] need proof

Proof. [28] □

Definition 3.2.5 (ordering for the integers)**.** Let n and m be integers. We say that n is greater than or equal to m, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some natural number a. We say that n is strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

Proposition 3.2.6 (properties of order for integers)**.** Let a, b, c be integers.

(i) $a > b$ if and only if $a - b$ is a positive natural number.

(ii) (addition preserves order). If $a > b$, then $a + c > b + c$.

(iii) (positive multiplication preserves order). If $a > b$ and c is positive, then $ac > bc$.

(iv) (negation reverses order). If $a > b$, then $-a < -b$.

(v) (order is transitive). If $a > b$ and $b > c$, then $a > c$.

(vi) (order trichotomy). Exactly one of the statements is true: $a > b$, $a < b$, or $a = b$.

Proof. [29] □

3.2.2 Rational numbers

Definition 3.2.6 (rational numbers)**.** A rational number is an expression of the form $a//b$, where a and b are integers and b is non-zero; $a//0$ is not considered to be a rational number.

Two rational numbers are considered to be equal, $a//b = c//d$, if and only if $ad = cb$.

The set of all rational numbers is denoted $\mathbb{Q}$.

Definition 3.2.7. If $a//b$ and $c//d$ are rational numbers, we define their sum

$$(a//b) + (c//d) := (ad + bc)//(bd), \tag{3.2.4}$$

their product

$$(a//b) \times (c//d) := (ac)//(bd) \tag{3.2.5}$$

and the negation

$$-(a//b) := (-a)//b. \tag{3.2.6}$$

Lemma 3.2.7. The sum, product, and negation operations on rational numbers are well-defined, in the sense that if one replaces $a//b$ with another rational number $a'//b'$ which is equal to $a//b$, then the output of the above operations remains unchanged, and similarly for $c//d$.

Proof. [30] □

Definition 3.2.8 (reciprocal)**.** If $x = a//b$ is non-zero rational (so that $a, b \neq 0$) then we define the reciprocal x^{-1} of x to be the rational number $x^{-1} := b/a$.

Proposition 3.2.8 (laws of algebra for rationals)**.** Let x, y, z be rationals. Then the following laws of algebra hold:

(i) $x + y = y + x$.

(ii) $(x + y) + z = x + (y + z)$.

(iii) $x + 0 = 0 + x = x$.

(iv) $x + (-x) = (-x) + x = 0$.

(v) $xy = yx$.

[28] need proof
[29] need proof
[30] need proof

(vi) $(xy)z = x(yz)$.

(vii) $x1 = 1x = x$.

(viii) $x(y+z) = xy + xz$.

(ix) $(y+z)x = yx + zx$.

If x is non-zero, we also have

(x) $xx^{-1} = x^{-1}x = 1$.

Proof. [31] □

Definition 3.2.9 (division (quotient))**.** We define the division (quotient) x/y of two rational numbers x and y, provided that y is non-zero, by the formula

$$x/y := x \times y^{-1}. \tag{3.2.7}$$

Definition 3.2.10 (positive rational numbers, negative rational numbers)**.** A rational number x is said to be positive iff we have $x = a/b$ for some positive integers a and b. It is said to be negative iff we have $x = -y$ for some positive rational y (i.e., $x = (-a)/b$ for some positive integers a and b).

Lemma 3.2.9 (trichotomy of rationals)**.** Let x be rational number. Then exactly one of the following three statements is ture:

(i) x is equal to 0.

(ii) x is a positive rational number.

(iii) x is a negative rational number.

Definition 3.2.11 (ordering of the rational numbers)**.** Let x and y be rational numbers. We say that $x > y$ iff $x - y$ is positive rational number, and $x < y$ iff $x - y$ is a negative rational number. We write $x \geq y$ iff either $x > y$ or $x = y$, and similarly define $x \leq y$.

Proposition 3.2.10 (basic properties of order on the rationals)**.** Let x, y, z be rational numbers. Then the following properties hold.

(i) (order trichotomy). Exactly one of the three statements $x = y$, $x < y$, or $x > y$ is true.

(ii) (order is anti-symmetric). One has $x < y$ if and only if $y > x$.

(iii) (order is transitive). If $x < y$ and $y < z$, then $x < z$.

(iv) (addition preserves order). If $x < y$, then $x + z < y + z$.

(v) (positive multiplication preserves order). If $x < y$ and z is positive, then $xz < yz$.

Remark. Note that (v) only works when z is positive[32].

3.2.3 Absolute value and exponentiation

Definition 3.2.12 (absolute value)**.** If x is a rational number, then absolute value $|x|$ of x is defined as follows. If x is positive, then $|x| := x$. If x is negative, then $|x| := -x$. If x is zero, then $|x| = 0$.

Definition 3.2.13 (distance)**.** Let x and y be rational numbers. Then quantity $|x - y|$ is called the distance between x and y and is sometimes denoted $d(x, y)$, thus $d(x, y) := |x - y|$. For instance, $d(3, 5) = d(5, 3) = 2$.

Proposition 3.2.11 (basic properties of absolute value and distance)**.** Let x, y, z be rational numbers.

(i) (non-degeneracy of absolute value). We have $|x| \geq 0$. Also, $|x| = 0$ if and only if x is 0.

[31] need proof
[32] need proof

(ii) (triangle inequality for absolute value). We have $|x+y| \leq |x| + |y|$.

(iii) We have the inequalities $-y \leq x \leq y$ if and only if $y \geq |x|$. In particular, we have $-|x| \leq x \leq |x|$.

(iv) (multiplicativity of absolute value). We have $|xy| = |x|\,|y|$. In particular, $|-x| = |x|$.

(v) (non-degeneracy of distance). We have $d(x,y) \geq 0$. Also, $d(x,y) = 0$ if and only if $x = y$.

(vi) (symmetry of distance). $d(x,y) = d(y,x)$.

(vii) (triangle inequality for distance). $d(x,z) \leq d(x,y) + d(y,z)$.

Definition 3.2.14 (ε-closeness)**.** Let $\varepsilon > 0$[33], and x, y be rational numbers. We say that y is ε-close to x iff we have $d(y,x) \leq \varepsilon$.

Remark. This definition is not standard in mathematics textbook; we will use it as 'scaffolding' to construct the more important notions of limits (and of Cauchy sequences)[34], and once we have those more advanced notions we will discard the notion of ε-close.

Proposition 3.2.12. Let x, y, z, w be rational numbers. Also, let $\varepsilon, \delta > 0$[35]

(i) If $x = y$, then x is ε-close to y for every $\varepsilon > 0$, then we have $x = y$.

(ii) If x is ε-close to y, then y is ε-close to x.

(iii) If x is ε-close to y, and y is δ-close to z, then x and z are $(\varepsilon+\delta)$-close.

(iv) If x and y are ε-close, and z and w are δ-close, then $x+z$ and $y+w$ are $(\varepsilon+\delta)$-close, and $x-z$ and $y-w$ are also $(\varepsilon+\delta)$-close.

(v) If x and y are ε-close, they are also ε'-close for every $\varepsilon' > \varepsilon$.

(vi) If y and z are both ε-close to x, and w is between y and z (i.e., $y \leq w \leq z$ or $z \leq w \leq y$), then w is also ε-close to x.

(vii) If x and y are ε-close, and z is non-zero, then xz and yz are $\varepsilon\,|z|$-close.

(viii) If x and y are ε-close, and z and w are δ-close, then xz and yw are $(\varepsilon\,|z| + \delta\,|x| + \varepsilon\delta)$-close.

Definition 3.2.15 (exponentiation to a natural number)**.** Let x be a rational number. To raise x to the power 0, we define $x^0 := 1$. Now suppose inductively that x^n has been defined for some natural number n, then we define $x^{n+1} := x^n \times x$.

Proposition 3.2.13 (properties of exponentiation, I)**.** Let x, y be rational numbers, and let n, m be natural numbers.

(i) We have $x^n x^m = x^{n+m}$, $(x^n)^m = x^{nm}$ and $(xy)^n = x^n y^n$.

(ii) We have $x^n = 0$ if and only if $x = 0$.

(iii) If $x \geq y \geq 0$, then $x^n \geq y^n \geq 0$. If $x > y \geq 0$ and $n > 0$, then $x^n > y^n \geq 0$.

(iv) We have $|x^n| = |x|^n$.

Definition 3.2.16 (exponentiation to a negative integer)**.** Let x be a non-zero rational number. Then for any negative integer $-n$, we define $x^{-n} := 1/x^n$.

Proposition 3.2.14 (properties of exponentiation, II)**.** Let x, y be non-zero rational numbers, and let n, m be integers.

(i) We have $x^n x^m = x^{n+m}$, $(x^n)^m = x^{nm}$ and $(xy)^n = x^n y^n$.

(ii) If $x \geq y > 0$, then $x^n \geq y^n > 0$ if n is positive, and $0 < x^n \leq y^n$ if n is negative.

(iii) If $x, y > 0$, $n \neq 0$, and $x^n = y^n$, then $x = y$.

(iv) We have $|x^n| = |x|^n$.

[33] rational?
[34] give link later
[35] rational?

3.2.4 Gaps in the rational numbers

Proposition 3.2.15 (interspersing of integers by rationals)**.** Let x be a rational number. Then there exists an integer n such that $n \leq x < n+1$. In fact, this integer is unique (i.e., for each x there is only one n for which $n \leq x < n+1$). In particular, there exists a natural number N such that $N > x$ (i.e., there is no such thing as a rational number which is larger than all the natural numbers).

The integer n for which $n \leq x < n+1$ is sometimes referred to as the integer part of x and is sometimes denoted $n = \lfloor x \rfloor$.

Proposition 3.2.16 (interspering of rationals by rationalys)**.** If x and y are two rationals such that $x < y$, then exists a third rational z such that $x < z < y$.

Proposition 3.2.17. There does not exist any rational number x for which $x^2 = 2$.

On the other hand, we can get rational numbers which are arbitrarily close to a square root of 2.

Proposition 3.2.18. For every rational number $\varepsilon > 0$, there exists a non-negative rational number x such that $x^2 < 2 < (x+\varepsilon)^2$.

3.3 Real Numbers

3.3.1 Cauchy sequences

3.3.2 Equivalent Cauchy sequences

3.3.3 The construction of the real numbers

3.3.4 Ordering the reals

3.4 Complex Numbers

3.5 Sequence

Definition 3.5.1. We say that a sequence a_n is increasing, or non-decreasing (decreasing, or non-increasing) if $a_{n+1} \geq a_n$ ($a_{n+1} \leq a_n$) for all n.

Also, the sequence is strictly increasing (strictly decreasing) if $a_{n+1} > a_n$ ($a_{n+1} < a_n$) for all n.

We say the a sequence is monotonic if it is either increasing or decreasing.

Definition 3.5.2 ($\limsup$, $\liminf$)**.** (i) Let $(x_n)_{n\in\mathbb{N}}$ be a sequence of real numbers. We define

$$\limsup_n x_n := \inf_n \left(\sup_{m\geq n} x_m \right) = \downarrow \lim_n \left(\sup_{m\geq n} x_m \right) \in [-\infty, \infty]. \tag{3.5.1}$$

Obviously, $y_n := \sup_{m\geq n} x_m$ is monotone non-increasing in n, so that the limit of the sequence y_n exists in $[-\infty, \infty]$.

(ii) Analogously,

$$\liminf_n x_n := \sup_n \left(\inf_{m\geq n} x_m \right) = \uparrow \lim_n \left(\inf_{m\geq n} x_m \right) \in [-\infty, \infty]. \tag{3.5.2}$$

(iii) We have

$$x_n \text{ converges in } [-\infty, \infty] \quad \Leftrightarrow \quad \limsup_n x_n = \liminf_n x_n, \tag{3.5.3}$$

and then

$$\lim x_n = \limsup_n x_n = \liminf_n x_n. \tag{3.5.4}$$

(iv) Additionally, we have

(a) if $z > \limsup_n x_n$, then $x_n < z$ eventually (that is, for all sufficiently large n),

(b) if $z < \limsup_n x_n$, then $x_n > z$ infinitely often (that is, for infinitely many n).

Remark. Note that lim sup and lim inf always exist.

Remark. Equivalently, if $x \in \mathbb{R}$ then[36]

$$x = \limsup_n x_n \;\Leftrightarrow\; \text{for all } \varepsilon > 0 \begin{cases} \{n \in N : x_n > x + \varepsilon\} \text{ is finite} \\ \{n \in N : x_n > x - \varepsilon\} \text{ is infinite} \end{cases} \tag{3.5.5}$$

$$x = \liminf_n x_n \;\Leftrightarrow\; \text{for all } \varepsilon > 0 \begin{cases} \{n \in N : x_n < x + \varepsilon\} \text{ is infinite} \\ \{n \in N : x_n < x - \varepsilon\} \text{ is finite} \end{cases} \tag{3.5.6}$$

Remark. The use of $\uparrow \lim$ or $\downarrow \lim$ to signify monotone limits will be handy, as will $y_n \downarrow y_\infty$ to signify $y_\infty = \downarrow \lim y_n$.

Definition 3.5.3. For $x \in [0, \infty]$ and a sequence $(x_n : n \in \mathbb{N})$ in $[0, \infty]$, we write $x_n \uparrow x$ to mean that $x_n \leq x_{n+1}$ for all n and $x_n \to x$ as $n \to \infty$. For a non-negative function f on E and a sequence of such functions $(f_n : n \in \mathbb{N})$, we write $f_n \uparrow f$ to mean that $f_n(x) \uparrow f(x)$ for all $x \in E$.

3.6 Other Theorems

Theorem 3.6.1 (Completeness of $\mathbb{R}$)**.** $\mathbb{R}$ is complete.

Proof. [37] □

Theorem 3.6.2 (Borel's Normal Number Theorem)**.** Almost every point in $(0, 1]$ is normal, that is, has 'equal' proportions of 0's and 1's in its binary expansion.

Proof. [38] □

[36] from notes
[37] unsorted, need proof
[38] unsorted, need proof

Chapter 4

Functions

4.1 Fundamentals

4.1.1 Definition

Definition 4.1.1 (function)**.** Let X, Y be sets, and let $P(x, y)$ be a property pertaining to an object $x \in X$ and an object $y \in Y$, such that for every $x \in X$, there is exactly one $y \in Y$ for which $P(x, y)$ is true (this is sometimes known as the vertical line test).

Then we define the function $f : X \to Y, x \mapsto f(x)$ defined by P on the domain X and range Y to be the object which, given any input $x \in X$, assigns an output $f(x) \in Y$, defined to be the unique object $f(x)$ for which $P(x, f(x))$ is true. Thus, for any $x \in X$ and $y \in Y$,

$$y = f(x) \;\Leftrightarrow\; P(x, y) \text{ is true.} \tag{4.1.1}$$

Definition 4.1.2 (equality of functions)**.** Two functions $f : X \to Y$, $g : X \to Y$ with the same domain and range are said to be equal, $f = g$, if and only if $f(x) = g(x)$ for all $x \in X$.

Remark. If $f(x)$ and $g(x)$ agree for some values of x, but not others, then we do not consider f and g to be equal.

Example 4.1.1. (i) The functions $x \mapsto x^2 + 2x + 1$ and $x \mapsto (x + 1)^2$ are equal on the domain $\mathbb{R}$ and range $[1, \infty)$.

(ii) The functions $x \mapsto x$ and $x \mapsto |x|$ are equal on the positive real axis, but are not equal on $\mathbb{R}$; thus the concept of equality of functions can depend on the choice of domain.

Definition 4.1.3 (composition)**.** Let $f : X \to Y$ and $g : Y \to Z$ be two functions, such that the range of f is the same set as the domain of g. We then define the composition $g \circ f : X \to Z$ of the two functions g and f to be the function define explicitly by the formula

$$(g \circ f)(x) := g(f(x)). \tag{4.1.2}$$

If the range of f does not match the domain of g, we leave the composition $g \circ f$ undefined.

Lemma 4.1.2 (composition is associative)**.** Let $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. [1] □

4.1.2 Injective, surjective and bijective functions

Definition 4.1.4 (injective (one-to-one) function)**.** A function $f : X \to Y$ is injective(or one-to-one) if different elements map to different elements:

$$x \neq x' \;\Rightarrow\; f(x) \neq f(x'). \tag{4.1.3}$$

Equivalently, a function is injective if

$$f(x) = f(x') \;\Rightarrow\; x = x'. \tag{4.1.4}$$

[1] need proof

Definition 4.1.5 (surjective (onto) function)**.** A function $f : X \to Y$ is surjective (or onto Y) if $f(X) = Y$, i.e., every element in Y comes from applying f to some element in X:

$$\text{for every } y \in Y, \text{ there exists } x \in X \text{ such that } f(x) = y. \tag{4.1.5}$$

Definition 4.1.6 (bijective (invertible) function)**.** $f : X \to Y$ is bijective (or invertible) if it is both injective and surjective.

Lemma 4.1.3. If $f : X \to Y$ and $g : Y \to Z$ are both injective, both surjective or both bijective, then so is $g \circ f$.

Proof. If $g \circ f(x) = g \circ f(x')$ then $g(f(x)) = g(f(x'))$ by definition. But g is injective, thus $f(x) = f(x')$. Also f is injective, thus $x = x'$.

Since g is surjective, for any $z \in Z$, we can find $y \in Y$ such that $z = g(y)$. Also, we can find $x \in X$ such that $y = f(x)$ as f is surjective. Thus, for any $z \in Z$, we can find $x \in X$ such that $z = g(f(x)) = g \circ f(x)$. Therefore, $g \circ f$ is surjective.

Then the conclusion of bijectivity is from the definition. □

4.2 Elementary function

4.2.1 Kronecker delta

Definition 4.2.1 (Kronecker delta)**.** Kronecker delta[2], is a function of two variables, usually integers. The function is 1 if the variables are equal, and 0 otherwise:

$$\delta_{ij} = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j \end{cases} \tag{4.2.1}$$

where Kronecker delta δ_{ij} is a piecewise function of variables i and j. For example, $\delta_{12} = 0$, whereas $\delta_{33} = 1$.

4.3 Hyperbolic function

Definition 4.3.1 (hyperbolic functions)**.** The hyperbolic functions are:

Hyperbolic sine:

$$\sinh x = \frac{e^x - e^{-x}}{2} = \frac{e^{2x} - 1}{2e^x} \tag{4.3.1}$$

Hyperbolic cosine:

$$\cosh x = \frac{e^x + e^{-x}}{2} = \frac{e^{2x} + 1}{2e^x} \tag{4.3.2}$$

Hyperbolic tangent:

$$\tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{e^{2x} - 1}{e^{2x} + 1} \tag{4.3.3}$$

Hyperbolic cotangent:

$$\coth x = \frac{\cosh x}{\sinh x} = \frac{e^x + e^{-x}}{e^x - e^{-x}} = \frac{e^{2x} + 1}{e^{2x} - 1} \tag{4.3.4}$$

Hyperbolic secant:

$$\operatorname{sech} x = (\cosh x)^{-1} = \frac{2}{e^x + e^{-x}} = \frac{2e^x}{e^{2x} + 1} \tag{4.3.5}$$

Hyperbolic cosecant:

$$\operatorname{csch} x = (\sinh x)^{-1} = \frac{2}{e^x - e^{-x}} = \frac{2e^x}{e^{2x} - 1} \tag{4.3.6}$$

Hyperbolic functions can be introduced via imaginary circular angles:

Hyperbolic sine:

$$\sinh x = -\mathrm{i} \sin \mathrm{i}x \tag{4.3.7}$$

Hyperbolic cosine:

$$\cosh x = \cos \mathrm{i}x \tag{4.3.8}$$

Hyperbolic tangent:

$$\tanh x = -\mathrm{i} \tan \mathrm{i}x \tag{4.3.9}$$

[2]named after Leopold Kronecker

Hyperbolic cotangent:

$$\coth x = \mathrm{i}\cot \mathrm{i}x \tag{4.3.10}$$

Hyperbolic secant:

$$\operatorname{sech}\ x = \sec \mathrm{i}x \tag{4.3.11}$$

Hyperbolic cosecant:

$$\operatorname{csch}\ x = \mathrm{i}\ \csc\ \mathrm{i}x \tag{4.3.12}$$

where i is the imaginary unit defined by $i^2 = -1$. The complex forms in the definitions above derive from Euler's formula.

Proposition 4.3.1. Odd and even functions:

$$\sinh(-x) = -\sinh(x), \quad \cosh(-x) = \cosh(x) \tag{4.3.13}$$

Hence:

$$\tanh(-x) = -\tanh(x) \tag{4.3.14}$$
$$\coth(-x) = -\coth(x) \tag{4.3.15}$$
$$\operatorname{sech}(-x) = \operatorname{sech}(x) \tag{4.3.16}$$
$$\operatorname{csch}(-x) = -\operatorname{csch}(x) \tag{4.3.17}$$

It can be seen that cosh x and sech x are even functions; the others are odd functions.

$$\operatorname{arsech}(x) = \operatorname{arcosh}\left(\frac{1}{x}\right) \tag{4.3.18}$$
$$\operatorname{arcsch}(x) = \operatorname{arsinh}\left(\frac{1}{x}\right) \tag{4.3.19}$$
$$\operatorname{arcoth}(x) = \operatorname{artanh}\left(\frac{1}{x}\right) \tag{4.3.20}$$

Hyperbolic sine and cosine satisfy the identity

$$\cosh^2(x) - \sinh^2(x) = 1 \tag{4.3.21}$$

which is similar to the Pythagorean trigonometric identity. One also has

$$\operatorname{sech}^2(x) = 1 - \tanh^2(x) \tag{4.3.22}$$
$$\coth^2(x) = 1 + \operatorname{csch}^2(x) \tag{4.3.23}$$

for the other functions.

The hyperbolic tangent is the solution to the nonlinear boundary value problem[3]:

$$\frac{1}{2}f'' = f^3 - f; \quad f(0) = f'(\infty) = 0 \tag{4.3.24}$$

It can be shown that the area under the curve of $\cosh(x)$ is always equal to the arc length:

$$\text{area} = \int_a^b \cosh(x)\ dx = \int_a^b \sqrt{1 + \left(\frac{d}{dx}\cosh(x)\right)^2}\ dx = \text{arc length} \tag{4.3.25}$$

Sums of arguments:

$$\cosh(x+y) = \sinh(x)\cdot\sinh(y) + \cosh(x)\cdot\cosh(y) \tag{4.3.26}$$
$$\sinh(x+y) = \cosh(x)\cdot\sinh(y) + \sinh(x)\cdot\cosh(y) \tag{4.3.27}$$

[3] see wiki

Sum and difference of cosh and sinh:

$$\cosh(x) + \sinh(x) = e^x \tag{4.3.28}$$

$$\cosh(x) - \sinh(x) = e^{-x} \tag{4.3.29}$$

4.4 Binomial series

Definition 4.4.1 (binomial series)**.** The binomial series is the Taylor series at $x = 0$ of the function f given by $f(x) = (1+x)^\alpha$, where $\alpha \in \mathbb{C}$ is an arbitrary complex number. Explicitly,

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!}x^2 + \cdots, \quad (*) \tag{4.4.1}$$

and the binomial series is the power series on the right hand side, expressed in terms of the (generalized) binomial coefficients

$$\binom{\alpha}{k} := \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!}. \tag{4.4.2}$$

4.5 Gamma function

Definition 4.5.1 (gamma function)**.** The gamma function (represented by the capital Greek letter Γ) is an extension of the factorial function, with its argument shifted down by 1, to real and complex numbers. That is, if n is a positive integer, $\Gamma(n) = (n-1)!$.

The gamma function is defined for all complex numbers except the non-positive integers. For complex numbers with a positive real part ($\Re z > 0$), it is defined via an improper integral that converges:

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt. \tag{4.5.1}$$

Remark. This integral function is extended by analytic continuation to all complex numbers except the non-positive integers (where the function has simple poles), yielding the meromorphic function we call the gamma function.

The gamma function is a component in various probability-distribution functions, and as such it is applicable in the fields of probability and statistics, as well as combinatorics.

Proposition 4.5.1. For $z \in \mathbb{C}$,

$$\Gamma(z+1) = z\Gamma(z). \tag{4.5.2}$$

Proposition 4.5.2.

$$\begin{aligned}
\Gamma\left(\frac{1}{2}\right) &= \sqrt{\pi}, \\
\Gamma\left(\frac{1}{2}+n\right) &= \frac{(2n)!}{4^n n!}\sqrt{\pi} = \frac{(2n-1)!!}{2^n}\sqrt{\pi} = \sqrt{\pi}\cdot\left[\binom{n-\frac{1}{2}}{n} n!\right] \\
\Gamma\left(\frac{1}{2}-n\right) &= \frac{(-4)^n n!}{(2n)!}\sqrt{\pi} = \frac{(-2)^n}{(2n-1)!!}\sqrt{\pi} = \sqrt{\pi}/\left[\binom{-\frac{1}{2}}{n} n!\right]
\end{aligned}$$

4.6 Beta function

Definition 4.6.1 (beta function)**.** In mathematics, the beta function, also called the Euler integral of the first kind, is a special function defined by

$$B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1} dx, \qquad \Re a, \Re b > 0. \tag{4.6.1}$$

Proposition 4.6.1.

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \tag{4.6.2}$$

Proof. First, write the product of two factorials as

$$\Gamma(a)\Gamma(b) = \int_0^\infty e^{-u}u^{a-1}du \int_0^\infty e^{-v}v^{b-1}dv = \int_0^\infty \int_0^\infty e^{-u-v}u^{a-1}v^{b-1}dudv. \tag{4.6.3}$$

Changing variables by putting $u = zt$, $v = z(1-t)$ shows that this is

$$\int_0^\infty \int_0^1 e^{-z}(zt)^{a-1}(z(1-t))^{b-1}zdtdz = \int_0^\infty e^{-z}z^{a+b-1}\,dz \int_0^1 t^{a-1}(1-t)^{b-1}dt. \tag{4.6.4}$$

Hence $\Gamma(a)\Gamma(b) = \Gamma(a+b)B(a,b)$. □

Chapter 5

Vectors

Part II

Algebra

Chapter 6

Groups

6.1 Groups

6.1.1 Basic concepts

Definition 6.1.1 (Group)**.** A set G is a group if there is a binary operation $*$ (one that combines two elements) $G \times G \to G$, satisfying

(i) If $g_1, g_2 \in G$ then $g_1 * g_2 \in G$ (closure axiom).

(ii) For all $g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (associativity).

(iii) There exists an element $e \in G$ such that, for all $g \in G$, $e * g = g * e = g$ (existence of identity (or unit) element).

(iv) For all $g \in G$ there exists and element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$ (existence of inverses).

Remark. A group G is a set equipped with an associative binary operation, an identity element for this operation, and which has inverses.

Remark. The set is a semigroup if it satisfies (i) and (ii).

Example 6.1.1. (i) $(\mathbb{Z}, +)$, the integers under addition, where $e = 0$ and $g^{-1} = -g$.

(ii) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ etc. are all groups as well.

(iii) $(\mathbb{Q} \setminus \{0\}, \times)$, the rationals under multiplication, where $e = 1$ and $g^{-1} = 1/g$.

Remark. $(\mathbb{Z}, -)$ is not a group because it is not associative, and $(\mathbb{Z}, \times)$ lacks inverses.

Definition 6.1.2. A group G is said to be abelian if $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$

Remark. (i) Groups may or may not be abelian.

(ii) $(\{\pm 1\}, \times)$ is a group.

(iii) Associativity means no brackets are needed, i.e. $g_1 * g_2 * g_3$ is unambiguous.

(iv) We often omit the and write e.g. $g_1 g_2 = g_1 * g_2$.

Lemma 6.1.2. (i) Let $(G, *)$ be a group. Then the identity element is unique, that is to say, if $g * e = g = e * g$ for all $g \in G$, and $ge' = g = e'g$ for all $g \in G$, then $e = e'$.

(ii) Inverses are also unique.

Proof. (i) $e = e * e' = e'$ using the fact that is a right identity and is a left identity.

(ii) Assume $g_1 * g_2 = e = g_2' * g_1$. By Definition 6.1.1 (ii), $g_2' = g_2' e = g_2'(g_1 g_2) = (g_2' g_1) g_2 = e g_2 = g_2$.

□

Lemma 6.1.3. Let $(G, *)$ be a group and let $g, g_1, g_2 \in G$. Then

$$\text{(i) } (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} (\text{not } g_1^{-1} g_2^{-1}); \qquad \text{(ii) } \left(g^{-1}\right)^{-1} = g. \tag{6.1.1}$$

Proof. (i) $(g_1 g_2)(g_2^{-1} g_1^{-1}) = g_1 e g_1^{-1} = g_1 g_1^{-1} = e$ and similarly, $g_2^{-1} g_1^{-1} g_1 g_2 = e$. Therefore $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$.

(ii) Let $f = g^{-1} \in G$, $fg = g^{-1} g = e = g g^{-1} = gf$, thus $g = f^{-1} = \left(g^{-1}\right)^{-1}$.

□

Lemma 6.1.4. If $(G, *)$ is a group, for $g_1, g_2, h \in G$, $g_1 h = g_2 h \Rightarrow g_1 = g_2$.

Proof. $g_1 h h^{-1} = g_2 h h^{-1} \Rightarrow g_1 e = g_2 e \Rightarrow g_1 = g_2$, and similarly in reverse. □

Definition 6.1.3 (order)**.** The order of the group G is written $|G|$ and defined to be the size of the set G.

6.1.2 Subgroup

Definition 6.1.4. Let $(G, *)$ be a group. The subset $H \subseteq G$ (i.e. $x \in H \Rightarrow x \in G$) is subgroup if it is a group under the restriction of the operation,

(i) $h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H$;

(ii) $e_G \in H$;

(iii) $h \in H \Rightarrow h^{-1} \in H$.

Note that associativity is inherited. We write $H \leq G$ to indicate that H is a subgroup.

Example 6.1.5.

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +), \qquad (\{\pm 1\}, \times) \leq (\mathbb{Q} - \{0\}, \times). \tag{6.1.2}$$

Remark. If G is finite and H is non-empty, then condition (i) is sufficient.

Example 6.1.6. (i) Additive groups, e.g. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

(ii) Multiple groups, e.g. $(\{\pm 1\}, \times) \leq (\mathbb{Q} - \{0\}, \times)$.

(iii) Matrix groups, such as the general linear group $GL(\mathbb{R}^n)$, i.e. the group of invertible $n \times n$ matrices, or the special linear group $SL(\mathbb{R}^n)$, i.e. matrices with determinant 1.

(iv) Permutation groups, i.e. the symmetric group S_n of permutations on $\{1, \ldots, n\}$ and the alternating group A_n containing even permutations.

(v) Cyclic groups of order n, i.e. $\{e, g, \ldots, g^{n-1}\}$, and dihedral groups D_{2n} of order $2n$, i.e. the symmetries of the regular n-gon.

(vi) Abelian groups, e.g. groups of order 4 including the Viergruppe V.

(vii) The quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$, $ij = k$, $ji = -k$ of order 8.

Lemma 6.1.7. The subset H of G is a subgroup if H is non-empty and $h_1, h_2 \in H \Rightarrow h_1^{-1} h_2 \in H$.

Proof. Let $a, b \in H$. Then letting $h_1 = h_2 = a$, we obtain $a^{-1} a = h_1^{-1} h_2 \in H$, and this is the identity, so $e \in H$. Next, letting $h_1 = a$, $h_2 = e$, we obtain $a^{-1} = a^{-1} e = h_1^{-1} h_2 \in H$. Finally, letting $h_1 = a^{-1}$, $h_2 = b$, we obtain $ab = (a^{-1})^{-1} b = h_1^{-1} h_2 \in H$.

Thus all three conditions are satisfied and H is a subgroup. □

Proposition 6.1.8. Let H_1 and H_2 be two subgroups of the group G. Then the intersection $H_1 \cap H_2$ is a subgroup of G.

Proof. Obviously, $H_1 \cap H_2$ is non-empty. If $h_1, h_2 \in H_1 \cap H_2$, then $h_1, h_2 \in H_1$ and $h_1, h_2 \in H_2$. Thus,

$$h_1^{-1} h_2 \in H_1, \ h_1^{-1} h_2 \in H_2 \Rightarrow h_1^{-1} h_2 \in H. \tag{6.1.3}$$

Then $H_1 \cap H_2$ is subgroup of G by Lemma 6.1.7. □

Proposition 6.1.9. Let H_1 and H_2 be two subgroups of the group G. Then if L is a subgroup of G contained in $H_1 \cup H_2$, then L is contained either in H_1 or in H_2 (note: it may be contained in both).

Particularly, the union $H_1 \cup H_2$ is a subgroup of G if and only if one of the H_i contains the other.

Proof. If $L\backslash H_1 \neq \emptyset, L\backslash H_2 \neq \emptyset$, then we can find $g_1 \in L\backslash H_1$ and $g_2 \in L\backslash H_2$ ($g_1 \in H_2$ and $g_2 \in H_1$). Thus, we can have $g_1 g_2 \in L \subseteq H_1 \cup H_2$ and $g_1 g_2 \in H_1$ or $g_1 g_2 \in H_2$. If $g_1 g_2 \in H_1$, then $g_1 \in H_1$. Contradiction with the fact that $g_1 \in L\backslash H_1$. Similarly, $g_1 g_2 \in H_2$ implies that $g_2 \in H_2$. Thus, one of $L\backslash H_1$ and $L\backslash H_2$ has to be empty set. This means that L is contained either in H_1 or in H_2.

In particular, we can let $L = H_1 \cup H_2$ and it has to be contained in H_1 or H_2. This will give the conclusion that one of the H_i contains the other. □

Definition 6.1.5. If $g_1, \ldots, g_k \in G$, the subgroup generated by the elements $g_1, \ldots, g_k$ is the smallest subgroup of G containing all the g_js. It is denoted by $\{g_1, \ldots, g_k\}$ and is the intersection of all the subgroups of G that contain all the g_js.

Remark. If there is no proper subgroup of G containing all the g_js, then the subgroup generated by $g_1, \ldots, g_k \in G$ is G itself.

Theorem 6.1.10. S_n is generated by each of

$$\text{(i) } \{(j\ k) | j < k\}, \quad \text{(ii) } \{(1\ k) | 1 < k \leq n\}, \quad \text{(iii) } \{(j\ j+1) | 1 \leq j < n\}, \quad \text{(iv) } \{(1\ 2), (1\ 2\ \ldots\ n)\}. \tag{6.1.4}$$

Proof. [1] □

Example 6.1.11. S_3 has order 6. Its subgroups are:

(i) $\{\iota\}$, of order 1.

(ii) $\{\iota, (1\ 2)\}$, of order 2, and two others which are similar; $\{\iota, (1\ 3)\}$ and $\{\iota, (2\ 3)\}$.

(iii) $\{\iota, (1\ 2\ 3), (1\ 3\ 2)\}$, of order 3.

(iv) S_3, of order 6.

6.1.3 Class of groups

Definition 6.1.6 (cyclic group)**.** A group is cyclic if there exists $x \in G$ such that $g = x^n, \forall g \in G$. x is called the generator of the group. Thus

$$x^n = \begin{cases} \overbrace{x * x * \cdots * x}^{n \text{ times}} & n > 0 \\ e & n = 0 \\ \underbrace{x^{-1} * x^{-1} * \cdots * x^{-1}}_{n \text{ times}} & n < 0 \end{cases} \tag{6.1.5}$$

The cyclic group of order n is denoted by $C_n = \langle x \rangle$.

Remark. Clearly, cyclic group is abelian.

Example 6.1.12. (i) $(\mathbb{Z}, +)$ is cyclic with generator 1.

(ii) The group of rotations of a regular n-gon is cyclic (see Theorem 6.1.15).

Definition 6.1.7 (permutation)**.** For $f : A \to B$, let $A = B = X$, i.e. we are mapping from a set to itself. Bijective functions $X \to X$ are called permutations of X (think shuffling).

It is customary to use small Greek letters to denote permutations; ι represents the permutation which maps every element to itself (the 'identity').

[1] need proof

Definition 6.1.8 (symmetric group)**.** We define $\mathrm{Sym}(X)$ to be the set of all permutations. If X is finite of size $|X| = n$, often we take X to be the set $\{1, 2, \ldots, n\}$ and S_n write for $\mathrm{Sym}(X)$. For $\sigma \in S_n$, we write it and its inverse

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}, \qquad \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix} \tag{6.1.6}$$

Theorem 6.1.13. $\mathrm{Sym}(X)$ is a group under composition. (It is called the symmetric group on X.)

Proof. We prove each of the axioms in turn;

(i) If $f, g \in \mathrm{Sym}(X)$ then $f \circ g \in \mathrm{Sym}(X)$; this follows from permutation (Definiton 6.1.7).

(ii) If $f, g, h \in \mathrm{Sym}(X)$, we want to show that for any $x \in X$, $(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x)$. However,

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))), \qquad ((f \circ g) \circ h)(x) = ((f \circ g) \circ h(x)) = f(g(h(x))). \tag{6.1.7}$$

so the two are identical.

(iii) $\iota : X \to X$ does nothing, thus $f \circ \iota = f = \iota \circ f$.

(iv) Define $f^{-1} : X \to X$ as follows, for $y \in X$ let $f^{-1}(y)$ be the unique pre-image of in X. Then $f^{-1} \in \mathrm{Sym}(X)$ and $(f^{-1} \circ f)(x) = x = \iota(x)$ for $x \in X$. Also $(f \circ f^{-1}(x)) = x = \iota(x)$, so the result follows since f, $f^{-1}$are bijective.

□

Example 6.1.14. We can now write

$$S_1 = \{\iota\}, \qquad S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} \tag{6.1.8}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}. \tag{6.1.9}$$

In S_3, if we let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tag{6.1.10}$$

then $\sigma^2 = \iota$, $\tau^3 = \iota$, $\tau^2 = \tau^{-1}$, and in particular note that

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{6.1.11}$$

so $\sigma \circ \tau \neq \tau \circ \sigma$, which means S_3 is not abelian (this is true of S_n in general with $n \geq 3$).

We can write $S_3 = \left\{\iota, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\right\}$ so $|S_3| = 6$. In general, $|S_n| = n!$.

Definition 6.1.9. (permutation group) A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ with $|X| = n$.

Remark. $S_n, A_n, D_{2n} \leq \mathrm{Sym}(X)$ where X is the set of vertices of the regular n-gon (see Definition 6.1.8, 6.1.24, 6.1.11).

Definition 6.1.10 (isomorphism group)**.** [2]

Definition 6.1.11 (dihedral group)**.** Consider the group of symmetries of a regular n-gon, with n vertices (for example, the nth roots of unity in $\mathbb{C}$). This is a subgroup of S_n, since

(i) the composition of symmetries is a symmetry

(ii) the identity is a symmetry

(iii) if α is a symmetry then α^{-1} is a symmetry

[2] need more details

This is called dihedral group and denoted as D_{2n} (for $n \geq 3$. In geometry the group is denoted D_n, while in algebra the same group is denoted by D_{2n} to indicate the number of elements.).

With the following theorem, we have $D_{2n} \leq S_n$; for example, $D_6 \leq S_3$ (as a matter of fact, $D_6 \cong S_3$, see Definition 6.1.16).

Theorem 6.1.15. The group D_{2n} of symmetries of a regular n-gon ($n \geq 3$) is a non-abelian subgroup of S_n, of order $2n$. It is generated by the elements τ and σ, of orders n and respectively, representing a rotation τ and a reflection σ, subject to $\tau^n = \iota$, $\sigma^2 = \iota$, $\sigma\tau\sigma = \tau^{-1}$.

Remark. The symmetries of a regular n-gon reserve the relative positions.

Proof. First look at the n rotations; these are the set $\left\{\iota, \tau, \tau^2, \ldots, \tau^{n-1}\right\}$ where

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix} \tag{6.1.12}$$

so that $\tau^n = \iota$. These form a subgroup of order n, which is a cyclic group C_n of order n, since each element is a power of τ and $\tau^i\tau^j = \tau^{i+j(\mathrm{mod}\ n)}$.

Let σ be a reflection through the real axis. There are reflections in the n different axes of symmetry ($n/2$ axes cross edges and $n/2$ cross vertices if n is even. n axes cross vertices if n is odd). Therefore $|D_{2n}| \geq 2n$.

We now need to show that any symmetry $g \in D_{2n}$ is either of the form τ^j for some j or of the form $\sigma\tau^j$.

Let $j = g(1)$. Then as $\tau^{j-1}(1) = j$ (rotating $j-1$ times, from 1 to j), we have $x = \left(\tau^{j-1}\right)^{-1} g$ fixes 1 ($\left(\tau^{j-1}\right)^{-1} g(1) = 1$). Since only two vertices, 2 and n, are next to 1 (because the operation can not change the relative positions), either x fixes 2 and n as well (and therefore it fixes everything, by induction), so that $g = \tau^{j-1}$, or x swaps 2 and n and all the other vertices take a reflection in the axis crossing vertex 1.

Thus the second case gives $\iota = \sigma^{-1}x = x\sigma^{-1}$, that is,

$$\iota = \sigma^{-1}\left(\tau^{j-1}\right)^{-1} g = \left(\tau^{j-1}\right)^{-1} g\sigma^{-1} \ \Rightarrow\ g = \tau^{j-1}\sigma = \sigma\tau^{1-j}. \tag{6.1.13}$$

So any symmetry of our n-gon is either τ^j for some j, or $\sigma\tau^j$ for some j, so $|D_{2n}| \leq 2n \ \Rightarrow\ |D_{2n}| = 2n$. □

Remark. Algebraically, we write $D_{2n} = \left\{t, s | t^n = \iota, s^2 = \iota, sts = t^{-1}\right\} = \left\{t^j, st^j | 0 \leq j < n\right\}$.

6.1.4 Cycles

Definition 6.1.12. $\sigma \in S_n$ is a k-cycle if the following hold:

$$\sigma(a_i) = a_{i+1}, \quad \sigma(a_k) = a_1, \quad \sigma(x) = x \ \text{ for all } x \in S_n \text{ not one of the } a_j\text{s}. \tag{6.1.14}$$

We denote it by $\sigma = (a_1\ a_2\ \ldots\ a_k)$.

Example 6.1.16. For $S_5 = \{1, 2, 3, 4, 5\}$, we can write

$$\sigma = (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \tag{6.1.15}$$

Remark. (i) $(a_1\ a_2\ \ldots\ a_k) = (a_2\ a_3\ \ldots\ a_k\ a_1) = \ldots$ so we can cycle cycles and these cycles are not unique.

(ii) $(a_1\ a_2\ \ldots\ a_k)^{-1} = (a_1\ a_k\ a_{k-1}\ \ldots\ a_2) = (a_k\ a_{k-1}\ \ldots\ a_1)$

(iii) $\sigma^k = \iota$, but $\sigma^l \neq \iota$ if $0 < l < k$, so k is the order of the k-cycle $G = \left\{\iota, \sigma, \sigma^2, \ldots, \sigma^{k-1}\right\}$.

Definition 6.1.13. Two cycles $\sigma, \tau \in S_n$ with $\sigma = (a_1\ a_2\ \ldots\ a_k)$ and $\tau = (b_1\ b_2\ \ldots\ b_l)$ are disjoint if all the a_js are different from all the b_is, i.e. the sets are non-intersecting.

Lemma 6.1.17. If σ, τ are disjoint cycles as above, then $\sigma\tau = \tau\sigma$. E.g. $(1\ 2)(3\ 4\ 5) = (3\ 4\ 5)(1\ 2)$.

Remark. This is only true of disjoint cycles, e.g. $(2\ 3)(1\ 2\ 3) = (1\ 3) \neq (1\ 2) = (1\ 2\ 3)(2\ 3)$.

Proof. If $x \in X$ is one of the a_js, then $\tau\sigma(a_j) = \tau(a_j + 1) = a_j + 1$ and $\sigma\tau(a_j) = \sigma(a_j) = a_j + 1$, and similarly if x is one of the b_is. If x is in neither set then $\tau\sigma(x) = \tau(x) = x = \sigma\tau(x)$ by the definition. So $\tau\sigma(x) = \sigma\tau(x)$ for all $x \in X$. Thus $\tau\sigma = \sigma\tau$. □

Theorem 6.1.18 (disjoint cycle decomposition)**.** Any permutation of a finite set X can be written as a product of disjoint cycles (in an essentially unique way). E.g.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 6 & 8 & 5 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 7)(3\ 6\ 4\ 8)(5) \tag{6.1.16}$$

Proof. Let $\sigma \in S_n$. Start with any point a_1, and 'chase it' to get a sequence $a_1, \sigma(a_1), \sigma^2(a_1), \ldots, X$ is finite, so we have to get $\sigma^l(a_1)$ being equal to one of the previous entries, say $\sigma^j(a_1)$. If l is the smallest such that we get repetition and $\sigma^l(a_1) = \sigma^j(a_1)$, then $j = 0$, so $\sigma^l(a_1) = a_1$.

If not all points of X are covered, choose b_1 to be a point in X not yet reached. Chase it, to obtain $b_2 = \sigma(b_1)$, and in general, $b_k = \sigma^{k-1}(b_1)$ with $\sigma^k(b_1) = b_1$.

Note that all the b_js are different from all the a_js, since σ is injective. Continue until finished. □

Remark. If $(a_1\ a_2\ \ldots\ a_{k_1})(b_1\ b_2\ \ldots\ b_{k_2})\ldots(z_1\ z_2\ \ldots\ z_{k_r}) = \sigma$, then the order of π is the least common multiple of $k_1, \ldots, k_r$.

Definition 6.1.14. A transposition on X is a 2-cycle on X.

Theorem 6.1.19. Any permutation of finite X can be written as a product of transpositions.

Proof. Let $\sigma \in S_n$, and write it as a product of disjoint cycles (by Theorem 6.1.18). Now note that the cycle

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k), \tag{6.1.17}$$

so a k-cycle is a product of $k - 1$ transpositions. □

Example 6.1.20. $(1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)$. Note that $\iota = (1\ 2)(1\ 2) = (1\ 2)(2\ 3)(2\ 3)(1\ 2)$ so there are many representations of each permutation. Note that for ι there must be an even number of factors; this is explained in Section 6.1.6.

6.1.5 Homomorphisms and isomorphisms

Definition 6.1.15 (homomorphism)**.** Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. The function $\theta : G_1 \to G_2$ is a homomorphism if $\theta(a *_1 b) = \theta(a) *_2 \theta(b)$ for any $a, b \in G_1$.

Definition 6.1.16 (isomorphism)**.** An isomorphism is a bijective homomorphism.

We write $G_1 \cong G_2$ if there is an isomorphism $G_1 \to G_2$.

Definition 6.1.17 (endomorphism)**.** An endomorphism is a homomorphism with $G \to G$ ($G_1 = G_2$).

Definition 6.1.18 (automorphism)**.** An automorphism is a bijective homomorphism with $G \to G$ ($G_1 = G_2$).

Definition 6.1.19. The automorphism group $\mathrm{Aut}(G)$ of automorphisms $G \to G$ is a group under the composition of maps.

Remark. An automorphism is an isomorphism. The elements of automorphism group $\mathrm{Aut}(G)$ are the maps $G \to G$.

Example 6.1.21. (i) $C_n \cong \{x | x^n = e\}$, i.e. the group generated by an x with this property (see Definition 6.1.6).

(ii)

$$\text{rotations of an } n\text{-gon} \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}, + \bmod n\right) = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \oplus_n\right) \tag{6.1.18}$$

where $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$, i.e. the group of rotations of a regular n-gon has an isomorphism to addition modulo n. The isomorphism can be taken to be $x^j \mapsto j$, which is a bijection, and then $\theta(x^j, x^k) = \theta(x^{j+k}) = j + k = \theta(x^j) + \theta(x^k)$ which satisfies the definition.

Lemma 6.1.22. (i) The composition of homomorphisms is a homomorphism, and the same with isomorphisms.

(ii) If $\theta : G_1 \to G_2$ is an isomorphism, its inverse $\theta^{-1} : G_2 \to G_1$ is also one.

Hence,

$$G \cong G, \qquad G_1 \cong G_2 \;\Rightarrow\; G_2 \cong G_1, \qquad G_1 \cong G_2 \cong G_3 \;\Rightarrow\; G_1 \cong G_3. \tag{6.1.19}$$

Proof. (i) Let $\theta : G_1 \to G_2$ and $\varphi : G_2 \to G_3$. Then $\varphi \circ \theta$ is a homomorphism, since

$$(\varphi \circ \theta)(a *_1 b) = \varphi(\theta(a *_1 b)) = \varphi(\theta(a) *_2 \theta(b)) = \varphi(\theta(a)) *_3 \varphi(\theta(b)) = (\varphi \circ \theta)(a) *_3 (\varphi \circ \theta)(b). \tag{6.1.20}$$

(ii) $\forall a, b \in G_2$, since θ is isomorphism (bijective), let $a = \theta(a')$, $b = \theta(b')$, $a', b' \in G_1$

$$\theta^{-1}(a *_2 b) = \theta^{-1}\left(\theta(a') *_2 \theta(b')\right) = \underbrace{\theta^{-1}\left(\theta(a' *_1 b')\right)}_{\theta \text{ is an isomorphism}} = (\theta^{-1} \circ \theta)(a' *_1 b') = a' *_1 b' = \theta^{-1}(a) *_1 \theta^{-1}(b). \tag{6.1.21}$$

Thus, θ^{-1} is also an isomorphism.

□

Lemma 6.1.23. If $\theta : G \to H$ is a homomorphism then

(i) $\theta(e_G) = e_H$.

(ii) $\theta(g^{-1}) = (\theta(g))^{-1}$.

Proof. (i) Let $g \in G$. Then $\theta(g) *_H e_H = \theta(g) = \theta(g *_G e_G) = \theta(g) *_H \theta(e_G)$ by the definition of a homomorphism. So, cancelling, $\theta(e_G) = e_H$.

(ii) Let $g \in G$. Then $\theta(g) *_H \theta(g^{-1}) = \theta(g *_G g^{-1}) = \theta(e_G) = e_H$ by (i). Similarly, $\theta(g^{-1}) *_H \theta(g) = \theta(g^{-1} *_G g) = \theta(e_G) = e_H$ by (i). Thus, $(\theta(g))^{-1} = \theta(g^{-1})$.

□

Definition 6.1.20 (image)**.** The image of a homomorphism $\theta : G \to H$ is $\operatorname{Im}\theta = \theta(G) = \{\theta(g) : g \in G\}$.

Lemma 6.1.24. For a homomorphism $\theta : G \to H$. The image $\theta(G) \leq H$.

Proof. (i) $e_H = \theta(e_G) \in \theta(G)$ by Lemma 6.1.23 (i).

(ii) If $h_1, h_2 \in \theta(G)$, then there are $g_1, g_2 \in G$ s.t. $\theta(g_1) = h_1$ and $\theta(g_2) = h_2$, thus with $g_1 g_2 \in G$,

$$h_1 h_2 \in \theta(g_1)\theta(g_2) = \theta(g_1 g_2) \in \theta(G). \tag{6.1.22}$$

(iii) If $h \in \theta(G)$, there is $g \in G$ s.t. $h = \theta(g)$. Then $h^{-1} = (\theta(g))^{-1} = \theta(g^{-1}) \in \theta(G)$ by Lemma 6.1.23 (ii).

□

Remark. In fact, for any $K \leq G$ it follows that $\theta(K) \leq H$.

Definition 6.1.21 (kernel)**.** The kernel of a homomorphism θ is $\ker\theta = \{g \in G : \theta(g) = e_H\}$.

Example 6.1.25. (i) $G = S_n$, $H = \{\pm 1, \times\}$. Then $\operatorname{sgn} : G \to H$ is a surjective homomorphism (see Theorem 6.1.28), with kernel the alternating group A_n (since all even elements are mapped to the identity).

(ii) Let $\mathbb{C}^* = (\mathbb{C}\setminus\{0\}, \times)$ and $H = \{z \in \mathbb{C}^* : |z| = 1\}$. Then $\theta : z \to z/|z|$ is a homomorphism in which case the image is obviously the unit circle H - in fact, θ does nothing to the unit circle. The kernel of θ is those elements which map to the identity 1, i.e. the positive half of the real line, i.e. $(\mathbb{R} > 0, \times)$.

Lemma 6.1.26. A homomorphism $\theta : G \to H$ is injective iff $\ker\theta = \{e_G\}$. ($\ker\theta$ is the 'obstruction to injectivity' of θ.)

Proof. ($\Rightarrow$). If θ is injective, assume $g \in \ker\theta$. Then $\theta(g) = e_H = \theta(e_G)$, so $g = e_G$ due to θ being injective. So the kernel is just the identity.

($\Leftarrow$). If $\ker\theta = \{e_G\}$, let $g_1, g_2 \in G$ with $\theta(g_1) = \theta(g_2)$. Since θ is a homomorphism,

$$\theta(g_1^{-1} g_2) = \underbrace{\theta(g_1^{-1})\theta(g_2) = (\theta(g_1))^{-1}\theta(g_2)}_{\text{Lemma 6.1.23 (ii)}} = (\theta(g_2))^{-1}\theta(g_2) = e_H, \tag{6.1.23}$$

so $g_1^{-1} g_2 \in \ker\theta$. But $\ker\theta = \{e_G\}$, so $g_1 = g_2$. Hence θ is injective. □

6.1.6 Signs

Definition 6.1.22 (sign)**.** The sign of a permutation σ is $(-1)^k$ where k is the number of factors in some expression of σ as a product of transpositions.

Lemma 6.1.27. The function $\operatorname{sgn} : S_n \to \{\pm 1\}$ taking $\sigma \to \operatorname{sgn}\sigma$ is well defined; that is, if $\sigma = \tau_1\tau_2\ldots\tau_a = \tau_1'\tau_2'\ldots\tau_b'$, two lots of transpositions, then $(-1)^a = (-1)^b$.

Proof. Let $c(\sigma)$ be the number of cycles in a disjoint cycle decomposition of σ, including 1-cycles. E.g. $c(\iota) = n$.

We claim that if τ is any transposition then $c(\sigma\tau) = c(\sigma) \pm 1 = c(\sigma) + 1 (\mathrm{mod} 2)$.

Write $\tau = (k\ l)$. Then the $\sigma\tau$ cycles are the same as the σ cycles, except for the one other involving k and l. If k, l are in two different cycles of σ, these two become one cycle of $\sigma\tau$; if they are in the same cycle, then the cycle splits into two cycles of $\sigma\tau$.

Now assume that $\sigma = \iota\tau_1\tau_2\ldots\tau_a = \iota\tau_1'\tau_2'\ldots\tau_b'\iota$. Since $c(\iota) = n$, using the above result gives $c(\sigma) = n + a (\mathrm{mod}\, 2) = n + b$. So $a = b (\mathrm{mod} 2) \ \Rightarrow\ (-1)^a = (-1)^b$. □

Theorem 6.1.28. $\operatorname{sgn} : (S_n, \circ) \to (\{\pm 1\}, \times)$ taking is a well-defined, non-trivial homomorphism.

Proof. Non-trivial due to the sign of any transposition being -1.

If $\operatorname{sgn}\alpha = (-1)^k$ and $\operatorname{sgn}\beta = (-1)^l$, then write $\alpha = \tau_1\tau_2\ldots\tau_k$ and $\beta = \tau_1'\tau_2'\ldots\tau_l'$ where all the τs are transpositions. Then $\alpha\beta = \tau_1\tau_2\ldots\tau_k\tau_1'\tau_2'\ldots\tau_l'$, so $\operatorname{sgn}\alpha\beta = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sgn}\alpha \operatorname{sgn}\beta$, satisfying the definition of a homomorphism. Thus, sgn is well-defined. □

Definition 6.1.23. $\sigma \in S_n$ is an even permutation if its sign is $+1$, and an odd permutation if its sign is -1. Note that even $\circ$ even = even, odd $\circ$ odd = even, and the other compositions as expected.

Definition 6.1.24 (alternating group)**.** The even permutations in S_n form a subgroup of S_n, called the alternating group and written A_n. E.g.

$$A_4 = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

Theorem 6.1.29. Exactly half the permutations in S_n are even and thus are in A_n, i.e. $|A_n| = n!/2$.

In fact, if $H \leq S_n$, and H contains some odd permutation, then $|A_n \cap H| = |H|/2$.

Proof. [3] □

Remark. Cycles of even length are odd permutations whereas cycles of odd length are even permutations (see Theorem 6.1.19).

Corollary 6.1.30. σ is an odd permutation iff the number of cycles of even length in its disjoint-cycle representation is odd.

Definition 6.1.25. Given $\sigma \in S_n$, let $x_1, x_2, \ldots, x_n$ be distinct integers. Then the sign of σ is

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i} \tag{6.1.24}$$

Example 6.1.31. Let $\sigma = (1\ 2\ 3)$ and $x_j = j$, then

$$\varepsilon(\sigma) = \frac{3-2}{2-1} \times \frac{1-2}{3-1} \times \frac{1-3}{3-2} = +1 \tag{6.1.25}$$

Lemma 6.1.32. $\varepsilon(\sigma) = \pm 1$, independent of the actual numbers x_j. In fact, $\varepsilon(\sigma) = (-1)^{N(\sigma)}$, where $N(\sigma) = |\{i < j | \sigma(i) > \sigma(j)\}|$.

Proof. For each $r \neq s$, either $x_r - x_s$ or $x_s - x_r$ appears on the top of the fraction. If $i = \sigma^{-1}(r) < \sigma^{-1}(s) = j$, then $x_s - x_r$ appears; if vice versa, then $x_r - x_s$ appears. □

Lemma 6.1.33. For any permutations $\sigma, \tau \in S_n$, we have $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

[3] need proof

Proof.

$$\varepsilon(\sigma\tau) = \prod_{i<j} \frac{\sigma\tau(j) - \sigma\tau(i)}{j-i} = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} \prod_{i<j} \frac{\sigma\tau(j)-\sigma\tau(i)}{\sigma(j)-\sigma(i)} = \varepsilon(\sigma)\varepsilon(\tau) \tag{6.1.26}$$

since the product on the right, taking $x_i = \sigma(i)$, gives us $x_{\tau(i)} = \sigma(\tau(i))$. □

Lemma 6.1.34. If is a transposition then $\varepsilon(\tau) = -1$.

Proof. Let $\tau = (1\ 2)$, $x_j = j$. Then

$$\varepsilon(\tau) = \frac{1-2}{2-1} \times \underbrace{\frac{3-2}{3-1} \times \ \ldots \ \times \ \ldots}_{\text{not affected by transposition}} = -1 \tag{6.1.27}$$

If $\tau = (1\ l)$ then write it as $(2\ l)(1\ 2)(2\ l)$ and cancel the end terms. If $\tau = (k\ l)$it can be written in the form $(1\ k)(1\ l)(1\ k)$. Thus $\varepsilon(k\ l) = \varepsilon(1\ 2)$ and the lemma is proved. □

Corollary 6.1.35. $\varepsilon(\sigma) = \operatorname{sgn}\sigma$ for all $\sigma \in S_n$.

6.2 Cosets and Lagrange's theorem

6.2.1 Cosets

Definition 6.2.1 (left coset)**.** Let $g \in G$. The left coset of H in G is

$$gH = \{gh : h \in H\}. \tag{6.2.1}$$

Example 6.2.1. $A_n \leq S_n$ has precisely two different cosets, H and τH, with τ any odd permutation, such as $(1\ 2)$.

Example 6.2.2. $G = S_3$ and $H = \{\iota, (1\ 2)\}$. Now $|H| = 2$ and $|G| = 6$, so we are expecting 3 left cosets.

$$H = \{\iota, (1\ 2)\}, \qquad (1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}, \qquad (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\} \tag{6.2.2}$$

Lemma 6.2.3. All the left cosets of H in G have size equal to $|H|$.

Proof. If gH is a coset, then consider the map $H \to gH$ taking $h \to gh$. Now if $gh_1 = gh_2$ then $h_1 = h_2$ so this map is injective. If $x \in gH$ then $x = gh$ for some $h \in H$, so x is the image of h; therefore the map is surjective. Hence the map is a bijection, so $|H| = |gH|$. □

Theorem 6.2.4. Let $H \leq G$. Then $H = eH = hH$ for some $h \in H$, so there are many ways of writing a coset. In fact, $gH = H$ iff $g \in H$.

Also, $aH = bH \Leftrightarrow a^{-1}b \in H$, and this is the defining characteristic of a coset.

Proof. If $aH = bH$, then $be = ah$ for some $h \in H$, so $a^{-1}b \in H$.

Conversely, if $a^{-1}b \in H$, for any $h \in bH$, $h = bg$ for some $g \in H$. Then $a^{-1}h = a^{-1}bg = \left(a^{-1}b\right)g \in H$ and thus $h \in aH$ and $bH \subseteq aH$. Similarly, we have $aH \subseteq bH$. Hence, $aH = bH$. □

Lemma 6.2.5. The left cosets form a partition of G, which means:

(i) each $g \in G$ lies in some left coset.

(ii) if $aH \cap bH$ is non-empty, then $aH = bH$ (i.e. any two cosets overlap totally or not at all).

Proof. (i) $g = ge \in gH$.

(ii) If $b \in aH$, then $b = ah_1$ for some $h_1 \in H$. For any $h_2 \in H$, we have $bh_2 = (ah_1)h_2 \in aH$, since $h_1h_2 \in H$. Therefore $bH \subseteq aH$.

However, also, $a = bh_1^{-1} \in bH$, so by the same reasoning, $aH \subseteq bH$. Therefore $aH = bH$.

□

Definition 6.2.2 (right coset)**.** The right coset Hg of H in G is defined by $Hg = \{hg | h \in H\}$.

Remark. The distinct left (or right) cosets of H all have size $|H|$, and form a partition of G. If $H \leq G$, precisely one of the cosets is a subgroup, because only one can contain the identity.

Corollary 6.2.6. The number of distinct left cosets of H in G is equal to the number of distinct right cosets of H in G.

Remark. A bijection between the left and right cosets of $H \leq G$:

$$gH \to Hg : x \mapsto g^{-1}xg. \tag{6.2.3}$$

Proof. We have $x \in aH \Leftrightarrow x = ah$ for some $h \in H \Leftrightarrow x^{-1} = h^{-1}a^{-1}$ for some $h \in H \Leftrightarrow x^{-1} = h'a^{-1}$ for some $h' \in H \Leftrightarrow x^{-1} \in Ha^{-1}$.

Thus if $aH = bH$, taking inverses gives $Ha^{-1} = Hb^{-1}$; moreover $x \mapsto x^{-1}$ sends left cosets to right cosets, and is a bijection, so it gives a bijection between the set of left cosets and the set of right cosets. □

Definition 6.2.3 (Equivalence relation)**.** Given a subgroup $H \leq G$, we can define an equivalence relation on G by $g_1 \sim g_2$ if $g_1^{-1}g_2 \in H$. Check this: $a, b, c \in G$,

(i) $a \sim a$, since $a^{-1}a = e \in H$.

(ii) $a \sim b \Rightarrow b \sim a$, since $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H$.

(iii) $a \sim b, b \sim c \Rightarrow a \sim c$, since $a^{-1}b \in H$ and $b^{-1}c \in H$ imply $a^{-1}c = a^{-1}bb^{-1}c \in H$.

Remark. Now if $[a] = \{b : a \sim b\}$ is the equivalence class of a, then $[a] = aH$, the left coset, since $[a] = \left\{b : a^{-1}b \in H\right\} = \{b : b \in aH\}$. Therefore the left cosets form a partition of G.

That is, an equivalence relation partitions G into equivalence classes which are known as left (right) cosets.

6.2.2 Lagrange's theorem

Theorem 6.2.7 (Lagrange's theorem)**.** If H is a subgroup of the finite group G, then the order of H divides the order of G. That is,

$$|G| = |H|\,[G : H] \tag{6.2.4}$$

where $[G : H]$ is the number of left cosets of H in G, called the index of H in G.

Proof. From Lemma 6.2.5 (ii), if $c \in (aH \cap bH)$, then $aH = cH = bH$. Hence G is covered by the distinct cosets of H, which are all of size $|H|$. Therefore $|H|\,|\,|G|$. □

Remark. A_4 has order 12 but no subgroup of order 6, so the converse is not true[4]. A later example will be to show that A_5 has no subgroup of index 2, 3 or 4[5].

Definition 6.2.4 (order of element)**.** The order of an element $g \in G$, written $o(g)$, is the least positive integer n (if one exists) such that $g^n = e_G$. If no such integer exists, then we say that g has infinite order.

Proposition 6.2.8. Let G be any group. Given $g \in G$, show by induction that $g^{m+n} = g^m g^n$ for all integers m and n.

Proof. Since $g^0 = e$, the result is clear if m or n is 0, so assume $m, n \neq 0$. If $m, n > 0$, both sides are the product of $m + n$ terms equal to g, so are equal, likewise if $m, n < 0$ both sides are the product of $m + n$ terms equal to g^{-1}. If $m > 0 > n$, write $k = -n$, then

$$g^{m+n} = g^{m-k}, \quad g^m g^n = g^m(g^{-1})^k = g^{m-1}gg^{-1}(g^{-1})^{k-1} = g^{m-1}e(g^{-1})^{k-1} = g^{m-1}(g^{-1})^{k-1} \tag{6.2.5}$$

Thus, if $m \geq k$, by induction on k, we obtain $g^m g^n = g^{m-k} = g^{m+n}$ as required, which if $k > m$, by induction on m we obtain $g^m g^n = (g^{-1})^{k-m} = g^{m+n}$ as required. A similar argument treats the case $m < 0 < n$. □

Proposition 6.2.9. Let G be a finite group. Let $g \in G$. Then there is a positive integer n such that g^n equals e, the identity element. The least such positive n is the order of g.

There also exists a positive integer n such that $g^n = e$ for all $g \in G$. The least such positive n is the exponent of G.

[4] see example sheet 1
[5] see example sheet 1

Proof. Let $|G| = m$. Given $g \in G$, then the $m+1$ elements $g, g^2, \ldots, g^m, g^{m+1}$ cannot all distinct, so $\exists s, t$ with $1 \leq s < t \leq m+1$ such that $g^s = g^t$. Thus, $g^{t-s} = g^{t-s} = g^s g^{-s} = e$ by Proposition 6.2.8. So $\exists$ a positive integer n_g with $g^{n_g} = e$. Set $n = \prod_{g \in G} n_g$, then $\forall g \in G$, we sset that n_g divides n, so $g^n = e$. Thus, such n is exponent of group G. □

Lemma 6.2.10. If $o(g) = n$ then $g^m = e$ iff $n|m$.

Proof. $\Rightarrow$. If $g^m = e$, then write with $m = qn + r$, $q, r \in \mathbb{Z}$, $0 \leq r < n$. Then $g^r = g^m((g^{-1})^n)^q = e$, but $r < n$ and n is the smallest positive integer such that $g^n = e$. Therefore $r = 0$, which means $n|m$.

$\Leftarrow$. If $m = qn$, then $g^m = (g^n)^q = e$. □

Corollary 6.2.11 (Lagrange's corollary)**.** If G is a finite group, and $g \in G$, then $o(g) \,|\, |G|$. Thus $g^{|G|} = e$ for all $g \in G$.

Proof. Consider the subgroup $\langle g \rangle = \left\{e, g, g^2, \ldots, g^{n-1}\right\}$ where $n = o(g)$.

So $o(g) = |\langle g \rangle| \,|\, |G|$ by Lagrange's theorem (Theorem 6.2.7). □

Corollary 6.2.12. If G is a group of prime order p, then G is cyclic. In fact, any element $g \in G \setminus \{e\}$ generates G.

Proof. Take $g \in G \setminus \{e\}$. Then $\langle g \rangle \leq G$ of an order dividing p, so $G = \langle g \rangle$. Thus $G \cong C_p$. □

Definition 6.2.5 ($\bmod n$)**.** Let $n \in \mathbb{N}$. Then $R_n = \{0, 1, \ldots, n-1\}$ = a cyclic group under $+ \bmod n$, denoted as $\oplus_n$.

For $a \in \mathbb{Z}$, define $r_n(a)$ to be the remainder in R_n (also known as the residue $\bmod n$); that is, if $\exists q \in \mathbb{Z}$, $r \in R_n$ with $a = qn + r$, then $r_n(a) = r$.

We see that there is a function $r_n : \mathbb{Z} \to R_n$ which takes $a \to r_n(a)$. This is a surjective function, and in fact, a homomorphism from $(\mathbb{Z}, +) \to (R_n, \oplus_n)$.

Definition 6.2.6 (numbers coprime to n)**.** Let $n \in \mathbb{N}$. Define $R_n^* = \{a \in R_n | \operatorname{hcf}(a, n) = 1\}$[6]. Define the operation $\otimes_n$ to be multiplication mod$n$, that is, $a \otimes_n b = r_n(ab)$.

Lemma 6.2.13. R_n^* is an abelian group with operation $\otimes_n$.

Proof. (i) Closure. If $\operatorname{hcf}(a, n) = 1 = \operatorname{hcf}(b, n)$, then $\operatorname{hcf}(ab, n) = 1$, so $(a \otimes_n b) \in R_n^*$.

(ii) Abelian. Multiplication in $\mathbb{Z}$ is abelian, so $a \otimes_n b = b \otimes_n a$.

(iii) Identity is 1, since $a \otimes_n 1 = a, \forall a \in R_n^*$.

(iv) Associativity. Multiplication in $\mathbb{Z}$ is associative.

(v) Inverses. Given $a \in R_n^*$, $u, v \in \mathbb{Z}$ with $au + nv = 1$[7]. So $a \otimes_n u = 1 \bmod n$. Then $r_n(u)$ is the inverse of a under $\otimes_n$.

□

Definition 6.2.7 (Euler's totient function)**.** The order of R_n^* is $\phi(n)$, Euler's totient function, defined by

$$\phi(n) = \{\#a : \operatorname{hcf}(a, n) = 1, 1 \leq a \leq n\} \tag{6.2.6}$$

Note that $\phi(p) = p - 1$ for prime p.

Theorem 6.2.14 (Fermat-Euler theorem)**.** If $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with a coprime to n, then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof. Since $|R_n^*| = \phi(n)$, $r_n(a^{\phi(n)}) = 1$ in R_n^* by Theorem 6.2.11. Hence $a^{\phi(n)} \equiv 1 \bmod n$. [8] □

Theorem 6.2.15 (Fermat's little theorem)**.** If p is a prime and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.

Proof. This is just the special case of Theorem 6.2.14 when n is prime. □

[6] need definition of hcf

[7] see Numbers and Sets

[8] There is another proof in Numbers and Sets.

6.3 Small groups

6.3.1 Cyclic groups

Recall Definition 6.1.6. The group G is cyclic if there exists $x \in G$ such that every element of G is a power of x.

Lemma 6.3.1. Let G be cyclic and generated by x. Then either

(i) G is infinite, all the x^js are distinct, and $G \cong (\mathbb{Z}, +)$; or

(ii) G is finite with order n for some $n \in \mathbb{N}$, and $G = \left\{e, x, x^2, \ldots, x^{n-1}\right\}$ with $G \cong C_n \cong (R_n, \oplus_n) \cong (\mathbb{Z}/n\mathbb{Z}, \oplus_n)$.

Proof. (i) Assume G is infinite. Note that if $x^k = x^l$ for some $k, l \in \mathbb{Z}$, then $x^{k-l} = e$. If $k > l$, we get $G = \left\{e, x, x^2, \ldots, x^{k-l-1}\right\}$, which is not infinite, and similarly if $k < l$. So if G is infinite and $x^k = x^l$ then $k = l$, so all the x^js are distinct.

Also, the mapping $\theta : G \to (\mathbb{Z}, +)$ taking $x^j \to j$ is bijective, and $\theta(x^j x^k) = \theta(x^{j+k}) = j + k = \theta(x^j)\theta(x^k)$. Thus, it is an isomorphism and $G \cong (\mathbb{Z}, +)$.

(ii) If G is finite and $|G| = n$, then $o(x) = n$, so $G = \left\{e, x, \ldots, x^{n-1}\right\}$. Also, consider the map $\theta : G \to (\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ taking $x^j \to j$. If $x^{j_1} = x^{j_2}$, then $x^{j_1 - j_2} = e$, so $n|(j_1 - j_2)$ by Lemma 6.2.10. Thus $[j_1] = [j_2]$ in $\mathbb{Z}/n\mathbb{Z}$, so the map is well-defined.

If $[j_1] = [j_2]$, we have $n|(j_1 - j_2)$, $x^{j_1 - j_2} = e \Rightarrow x^{j_1} = x^{j_2}$ and thus θ is injective. Also, for any $j \in \mathbb{Z}/n\mathbb{Z}$, we can find $x^j \in G$ since $j \in \{0, 1, \ldots, n-1\}$. Thus, θ is bijective.

Furthermore, $\theta(x^j x^k) = \theta(x^{j+k}) = (j+k) \bmod n = (j \bmod n) \oplus_n (k \bmod n) = \theta(x^j)\theta(x^k)$. So θ is also a homomorphism and thus an isomorphism.

□

Lemma 6.3.2. Any subgroup H of a cyclic group $G = \langle x \rangle$ is cyclic. In fact, if $H \neq \{e\}$, then $H = \left\langle x^k \right\rangle$ with k the smallest positive integer such that $x^k \in H$.

Proof. Let $G = \langle g \rangle$ be a cyclic group, and H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic so we may assume $H \neq \langle e \rangle$; take $h_1 \in H \backslash \{e\}$, then $h_1 = g^n$ for some $n \in \mathbb{Z}$. Since $h_1^{-1} = g^{-n} \in H$, $\exists m \in \mathbb{N}$ with $g^m \in H$.

Let $n \in \mathbb{N}$ be minimal with $g^n \in H$, and set $h = g^n$. Certainly $\langle h \rangle \subseteq H$. Conversely, given $g^r \in H$ write $c = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n - 1$, then $g^r = g^{c - qn} = g^c \left(g^n\right)^{-q} = g^c h^{-q} \in H$, so by the minimality of n we must have $r = 0$, whence $c = qn$ and $g^c = g^{qn} = h^q \in \langle h \rangle$. Thus, $H \subseteq \langle h \rangle$ which gives $\langle h \rangle = H$, and thus H is cyclic.[9] □

Remark. Let $a, b \in \mathbb{Z}$. By The above lemma, the subgroup of $\mathbb{Z}$ generated by a, b is cyclic, say $\langle c \rangle$ for some $c \in \mathbb{Z}$. Note that $c = \text{hcf}(a, b)$. Then $c \in \langle a, b \rangle$, so $c = a^u b^v$ in $\mathbb{Z}$ (since $\mathbb{Z}$ is abelian).

Remark. Multiplication here is actually addition since the operation in $\mathbb{Z}$ is $+$, so we can write $c = ua + vb$.

6.3.2 Direct (Cartesian) products of groups

Definition 6.3.1 (direct product)**.** Given groups H and K, we can construct the direct product $H \times K = \{h, k | h \in H, k \in K\}$ with operation $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$.

Lemma 6.3.3. If H and K are groups then $H \times K$ is a group.

Proof. (i) Closed under the given operation, as $h_1 h_2 \in H$ and $k_1 k_2 \in K$.

(ii) Associative since multiplication in H and K is associative.

(iii) Identity $e = (e_H, e_K)$.

(iv) Inverse of $(h, k) = (h^{-1}, k^{-1})$.

□

[9] See example sheet 2, question 6. still need all the subgroups of the cyclic group C_n

Example 6.3.4 (Klein 4-group)**.** $C_2 \times C_2 = \{e, x\} \times \{e, y\} = \{(e, e), (x, e), (y, e), (x, y)\}$ where all non-identity elements have order 2.

Alternatively, $C_2 \times C_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$ under addition mod2.

Now $C_2 \times C_3 \cong C_6$ since C_2 is generated by x of order 2 and C_3 is generated by of order 3, so $o(x, y) = 6$. In general, $C_m \times C_n \cong C_{mn}$ iff $\text{hcf}(m, n) = 1$ (see Lemma 6.6.8).

It follows that $\mathbb{R}^n$ for $n \in \mathbb{N}$ is a group under component-wise addition, since $\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ times}}$.

Remark. (i) If H, K are finite, then so is $H \times K$, and $|H \times K| = |H|\,|K|$[10].

(ii) H, K are abelian iff $H \times K$ is abelian.

(iii) $H \times K$ contains a subgroup $\{(h, e) : h \in H\}$ isomorphic to H and a subgroup $\{(e, k) : k \in K\}$ isomorphic to K.

Proposition 6.3.5. Let G be a group with subgroups H, K such that

(i) each element in G can be written as hk with $h \in H$, $k \in K$.

(ii) $H \cap K = \{e\}$.

(iii) $hk = kh$, $\forall h \in H, k \in K$.

Then $G \cong H \times K$.

Proof. If $h_1k_1 = h_2k_2$ with $h_i \in H$, $k_i \in K$, then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, so expressions hk for elements of G are unique. Thus we can define $\theta : G \to H \times K$, taking $g = hk \to (h, k)$. This is well defined, by uniqueness of expressions hk.

If $(h_1, k_1) = (h_2, k_2)$, $h_1 = h_2, k_1 = k_2 \;\Rightarrow\; h_1k_1 = h_2k_2$, so θ is injective. Since $\forall h \in H, k \in K$, $h, k \in G$ (H, K are subgroups), $hk \in G$. Thus, θ is surjective and therefore bijective. By condition (iii),

$$\theta((h_1k_1)(h_2k_2)) = \theta(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \theta(h_1k_1)\theta(h_2k_2), \tag{6.3.1}$$

so the map θ is a homomorphism. Thus, θ is an isomorphism and $G \cong H \times K$. □

6.3.3 Dihedral groups

Proposition 6.3.6 (dihedral group)**.** Let G be a group generated by two elements, s of order n and t of order 2, with $tst = s^{-1}$. Algebraically, $G = \langle s, t | s^n = e, t^2 = e, tst = s^{-1} \rangle$. Then G is dihedral of order $2n$, that is, G is isomorphic to the group of symmetries of a regular n-gon.

Proof. $G = \{e, s, s^2, \ldots, s^{n-1}, t, ts, ts^2, \ldots, ts^{n-1}\}$ and these are precisely the elements of G. (Note Saxl's Theorem, the very useful fact that $s^jt = ts^{-j}$.)

Now the group of symmetries of a regular n-gon contains σ, a rotation of order n, and τ, a reflection satisfying $\tau^2 = \iota$ and $\tau\sigma\tau = \sigma^{-1}$ (see Definition 6.1.11). So the mapping $\theta : t^ks^j \to \tau^k\sigma^j$ is a well-defined bijective homomorphism, i.e. an isomorphism, since both groups satisfy the same conditions. □

6.3.4 The groups of order ≤ 10

Here is a table of them. For groups of prime order we use Corollary 6.2.12. For other orders see the Table 6.8.1. There are 10 groups of order 16, and $\approx 50,000,000,000$ groups of order 2^{10}.

Lemma 6.3.7. A group G of order 4 is abelian, and is isomorphic to C_4 or $C_2 \times C_2$.

Proof. Non-identity elements have order 2 or 4. If G contains an element of order 4, then $G \cong C_4$ (of course, it is abelian). So assume all non-identity elements have order 2. Let $a \in G \setminus \{e\}$ and let $b \in G \setminus \langle a \rangle$. Then $G = \{e, a, b, ab\}$. So $G \cong \langle a \rangle \times \langle b \rangle = C_2 \times C_2$ by Proposition 6.3.5. Also, $e = (ab)^2 = abab \;\Rightarrow\; ab = a^2bab^2 = ebae = ba$. Thus, G is abelian. □

Lemma 6.3.8. A group G of order 6 is isomorphic to either C_6 or D_6.

[10] need details

Proof. If all the elements of G have order 2, then take a, b of order 2 and observe that $|\langle a, b\rangle| = 4 \nmid 6$. If all the elements have order 3, then consider $a, b \in G$ with $\langle a\rangle \in G\backslash\{e\}, b \in G\backslash\langle a\rangle$. Thus $G \geq \{e, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}$ which is too big. Therefore G contains an element s of order 3 and an element t of order 2, i.e., $s^3 = e$, $t^2 = e$.

Thus $G = \{e, s, s^2, t, ts, ts^2\}$. Now st must be ts or ts^2 (the other possibilities lead to contradictions).

If $ts = st$, $(st)^2 = stst = sstt = s^2t^2 = s^2$, $(st)^3 = s^2st = t$, $(st)^4 = tst = tts = t^2s = s$, $(st)^5 = sst = s^2t$, $(st)^6 = s^2tst = s^2stt = s^3t^2 = e$, so $o(st) = 6$. Then $G \cong C_6$.

If $st = ts^2$, $tst = t^2s^2 = ees^{-1} = s^{-1}$, then G is generated by t, s of orders 2 and 3 with $tst = s^{-1}$, so $G \cong D_6$. □

Definition 6.3.2 (The quaternion group Q_8)**.** The quaternion group Q_8 is defined as $\{a, b | a^4 = e, b^2 = a^2, bab^{-1} = a^{-1}\}$. It has one element of order 2, a^2, and six elements of order 4, all the others.

The customary notation for Q_8 is $\{\pm 1, \pm i, \pm j, \pm k\}$ with the operation $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $ik = -j$, $kj = -i$ and $i^2 = j^2 = k^2 = -1$.

Remark. We can see $a = i$, $b = j$.

Another realisation is 2×2 matrices over $\mathbb{C}$;

$$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{6.3.2}$$

corresponding to the $1, i, j, k$ from above.

It follows that there is a 4-dimensional, non-commutative, associative algebra over $\mathbb{R}$. $\mathbb{H} = \{\alpha 1 + \beta i + \gamma j + \delta k\}$ where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Lemma 6.3.9. If G is a group of order 8, then G is isomorphic to exactly one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 and Q_8.

Proof. The orders of non-identity elements are 2,4 and 8 by Lagrange's corollary (Theorem 6.2.11).

(i) If G contains an order-8 element, then $G \cong C_8$. So assume none such.

(ii) If all the elements of $G\backslash\{e\}$ have order 2, then G is abelian since $ba = (ba)^{-1} = a^{-1}b^{-1} = ab$. Take $a \in G\backslash\{e\}$, $b \in G\backslash\langle a\rangle$. Then by Lemma 6.3.7, $\langle a, b\rangle$ is isomorphic to $C_2 \times C_2$ and $|\langle a, b\rangle| = 4$. Let $c \in G\backslash\langle a, b\rangle$.

We the elment ca has order 2. Then $(ca)^2 = e \Rightarrow caca = e \Rightarrow c^2aca^2 = ca \Rightarrow ac = ca$. Similarly, we can have $cx = xc$, $\forall x \in \{e, a, b, ab\} = \langle a, b\rangle$ and thus $xy = yx$ $\forall x \in \langle a, b\rangle, y \in \langle c\rangle$.

Thus $G \cong \langle a, b\rangle \times \langle c\rangle \cong (C_2 \times C_2) \times C_2 = C_2 \times C_2 \times C_2$ by Proposition 6.3.5.

(iii) So there is an element a of order 4 in G but none of order 8. Let $b \in G\backslash\langle a\rangle$ with order 2 or 4. Hence $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ with no more elements. What are b^2 and ba?

(a) If $b^2 \in \{b, ab, a^2b, a^3b\}$, then $b \in \{e, a, a^2, a^3\} = \langle a\rangle$ which is a contradiction. Thus $b^2 \in \langle a\rangle$. If b^2 is a or a^3, then $o(b) = 8$ which cannot be. So $b^2 = e$ or $b^2 = a^2$.

(b) We know $ba \notin \langle a\rangle$, thus $ba = a^jb$ for some $j \in \{1, 2, 3\}$. So $bab^{-1} = a^j$. Note that $b^2 = e$ or $b^2 = a^2$, so $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^jb^{-1} = bab^{-1} \ldots b^{-1}bab^{-1} = (bab^{-1})^j = (a^j)^j = a^{j^2}$. Therefore $a^{j^2-1} = e$, so 4 divides $j^2 - 1$ (using Lemma 6.2.10), so j is odd. So $j \in \{1, 3\}$ and $bab^{-1} = a$ or a^3.

Case 1. $bab^{-1} = a$. Then $ba = ab$ so G is abelian.

(a) If $b^2 = e$, by Proposition 6.3.5, $G \cong \langle a\rangle \times \langle b\rangle \cong C_4 \times C_2$.

(b) If $b^2 = a^2$, replace b by $b' = ab^{-1}$. Then $b'^2 = (ab^{-1})^2 = a^2b^{-2} = e$. So $G \cong \langle a\rangle \times \langle b'\rangle \cong C_4 \times C_2$ by Proposition 6.3.5.

Case 2. $bab^{-1} = a^{-1}$

(a) If $b^2 = e$, $bab = a^{-1}$, then $G = D_8$ by Proposition 6.3.6. G then has two elements of order 4, a and a^{-1}, and five elements of order 2, a^2, ab, b, a^2b and a^3b.

(b) If $b^2 = a^2$, then $G \cong Q_8$.

□

Lemma 6.3.10. A group G of order 10 is isomorphic to either C_{10} or D_{10}.

Proof. Let G be a group of order 10. The possible orders of non-identity elements are 2,5,10. If there exists $g \in G$ of order 10 then $G = \langle g \rangle \cong C_{10}$; so assume G has no element of order 10.

By first example sheet, G has an element of order and if all non-identity elements of G had order 2 then G would be abelian - if wo, take $g_1, g_2 \in G$ with $g_1 \neq e$ and $g_2 \notin \langle g_1 \rangle$, then $\langle g_1, g_2 \rangle = \{e, g_1, g_2, g_1 g_2\}$, contrary to Lagrange's theorem. Thus G contains x of order 2 and y of order 5; so we must have

$$G = \left\{e, y, y^2, y^3, y^4, x, xy, xy^2, xy^3, xy^4\right\}. \tag{6.3.3}$$

Consider yx - it cannot be y^i for some i, as this would give $x = y^{i-1}$, (contradiction) and it is not x, so it must be xy^i for some $i = \{1, 2, 3, 4\}$, and hence $x^{-1}yx = y^i$. We have

$$x^{-1}y^i x = \left(x^{-1}yx\right)^i = \left(y^i\right)^i = y^{i^2} \tag{6.3.4}$$

but $x^{-1}y^i x = xy^i x^{-1} = y$, so $y^{i^2} = y$. Then we cannot have $i \in \{2, 3\}$ since $y^4, y^9 \neq y$. If $i = 1$ then $yx = xy$, i.e., x and y commute - but then $(xy)^k = x^k y^k$ for all k, $(xy)^2 = x^2y^2 = y^2 \neq e$ and $(xy)^5 = x^5y^5 = x \neq e$, so xy does not have order 2 or 5, contradiction.

So $i = 4$, so $x^{-1}yx = y^4 = y^{-1}$ and thus $G \cong D_{10}$.

Thus any group of order 10 is isomorphic to either C_{10} or D_{10}. □

6.4 Normal Subgroups, Quotient Groups and Isomorphism Theorem

6.4.1 Normal Subgroups, Quotient Groups

Example 6.4.1. The integers lie inside the real numbers, $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$. We would like to add cosets,

$$(\mathbb{Z} + r_1) + (\mathbb{Z} + r_2) = \mathbb{Z} + (r_1 + r_2). \tag{6.4.1}$$

In general, we want to copy this procedure to define an operation on the cosets of a subgroup. If $K \leq G$ we want to define $g_1 K g_2 K = g_1 g_2 K$. But this requires $K g_2 K = g_2 K$, after multiplying on left by g_1^{-1}. In particular, we need $K g_2 \subseteq g_2 K$ for all $g_2 \in G$, and also $K g_2^{-1} \subseteq g_2^{-1} K$ which implies $g_2 K \subseteq K g_2$. So to make the definition work we need that $gK = Kg$ for all $g \in G$.

Definition 6.4.1 (normal subgroup)**.** A subgroup $K \leq G$ is normal if each left coset of K is equal to the corresponding right coset, i.e. $gK = Kg$, $\forall g \in G$. Therefore for any $g \in G, k \in K, \exists k' \in K$ with $gk = k'g$, i.e. $gkg^{-1} \in K, \forall g \in G, k \in K$ or equivalently, $gKg^{-1} = K$ for all $g \in G$. We write $K \lhd G$.

Example 6.4.2. (i) If G is abelian, then any subgroup K is normal, because $gkg^{-1} = k \in K$ for any $g \in G, k \in K$.

(i) In general, $\{e\}$ and G are always normal.

(iii) In the dihedral group D_{2n}, the subgroup of rotations is normal but $\{e, \tau\}$, for a reflection τ, is not normal if $n \geq 3$.

Proposition 6.4.3. $A_n \lhd S_n$.

Proof. [11] □

Lemma 6.4.4. If $K \leq G$ of index 2, then $K \lhd G$.

Proof. If $g \in G$, then either $g \in K$, in which case $gK = K = Kg$, or $g \in G \backslash K$, in which case $gK = G \backslash K = Kg$. Either way, $K \lhd G$.

It follows from the definition that if any one member of a conjugacy class is an element of a normal subgroup, then the entire conjugacy class must be within that subgroup. Therefore any normal subgroup is a (disjoint) union of conjugacy classes. □

Lemma 6.4.5. If $\theta : G \to H$ is a homomorphism, then $\ker \theta \lhd G$.

[11] need proof

Proof. First note that $e_G \in \ker\theta$ by Theorem 6.1.23 (i). Next, if $g_1, g_2 \in \ker\theta$, then

$$\theta(g_1^{-1}g_2) = \theta(g_1^{-1})\theta(g_2) = (\theta(g_1))^{-1}\,\theta(g_2) = e_H \tag{6.4.2}$$

by Theorem 6.1.23 (ii). then $g_1^{-1}g_2 \in \ker\theta$. Therefore $\ker\theta \leq G$ by Lemma 6.1.7.

Now if $\forall g \in G, k \in \ker\theta$, then

$$\theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g^{-1}) = \theta(g)e_H\theta(g^{-1}) = \theta(g)e_H\,(\theta(g))^{-1} = e_H \tag{6.4.3}$$

Thus, $gkg^{-1} \in \ker\theta$. Therefore the subgroup $\ker\theta$ is normal. □

Lemma 6.4.6. If $G_1, G_2 \lhd G$ such that $G = \langle G_1, G_2\rangle$ and $G_1 \cap G_2 = \{e\}$, then $G \cong G_1 \times G_2$.

Proof. It is enough to show, by Proposition 6.3.5, that $g_1g_2 = g_2g_1$ for any $g_1 \in G_1$, $g_2 \in G_2$.

Since $g_1g_2g_1^{-1} \in G_2$ and $g_2g_1^{-1}g_2^{-1} \in G_1$ (definition of normal), we have $g_1g_2g_1^{-1}g_2^{-1} \in G_1 \cap G_2 = \{e\}$. So $g_1g_2 = g_2g_1$. □

Theorem 6.4.7 (quotient group)**.** Let $K \lhd G$ and $g_1, g_2 \in G$. Then the set of cosets of K in G form a group under the operation of coset multiplication, defined by $g_1Kg_2K = g_1g_2K$. This group $((G:K) = \{gK : g \in G\})$ is called the quotient group G/K.

Remark. Normality of K is necessary.

Proof. Let $g, g_1, g_2, g_3 \in G$. First we must check this operation is well-defined on $(G:K)$; that is, $(g_1g_2)K$ is a valid coset of K in G (obvious), and if $g_1K = g_1'K$ and $g_2K = g_2'K$ then $(g_1g_2)K = (g_1'g_2')K$ (less obvious, the proof is from [3]) .

Directly from the above expressions $g_i^{-1}g_i' \in K$ (for $i = 1, 2$) so call it k_i. Now

$$(g_1g_2)K = (g_1'g_2')K \;\Leftrightarrow\; g_2^{-1}g_1^{-1}g_1'g_2' \in K \tag{6.4.4}$$

but $g_2^{-1}g_1^{-1}g_1'g_2' = g_2^{-1}k_1g_2' = g_2^{-1}g_2'(g_2')^{-1}k_1g_2' = k_2(g_2')^{-1}k_1g_2' \in k_2K$ due to the fact that $(g_2')^{-1}k_1g_2' \in K$. Finally, $k_2K = K$ so we are done.

Next we check the remaining group axioms (as Closure is $g_1Kg_2K = g_1g_2K$).

Associativity:

$$(g_1Kg_2K)g_3K = (g_1g_2)Kg_3K = (g_1g_2)g_3K = g_1(g_2g_3)K = g_1K(g_2Kg_3K) = g_1K(g_2g_3)K. \tag{6.4.5}$$

Identity element: $gKeK = gK$ and $eKgK = gK$ so the identity $= eK = K$.

Inverses: $gKg^{-1}K = eK = K = g^{-1}KgK$, thus $(gK)^{-1} = g^{-1}K$. □

Example 6.4.8. $G = D_8 = \langle a, b : a^4 = e = b^2, bab^{-1} = a^{-1}\rangle$ and $K = \langle a^2\rangle$. Then

$$\frac{G}{K} = G/K = \{K, aK, bK, abK\} \cong C_2 \times C_2 = \langle aK, bK\rangle \tag{6.4.6}$$

Note that $\langle b\rangle$ is not normal (as $aba^{-1} = ba^{-2} \notin \langle b\rangle$), but $\langle a^2\rangle$ and all subgroups of order 4 are normal.

6.4.2 Isomorphism theorem

Theorem 6.4.9 (first isomorphism theorem)**.** Let $\theta : G \to H$ be a homomorphism. Then $\ker\theta$ is a normal subgroup $(\ker\theta \lhd G)$ and $G/\ker\theta \cong \operatorname{Im}\theta$.

Remark. $G/\ker\theta \cong \operatorname{Im}\theta$ means that any homomorphic image of G is isomorphic to a quotient.

Proof. For the first assertion see Lemma 6.4.5.

In general, the way to show that two groups are isomorphic is to construct an isomorphism between them. Therefore we define a map $\Phi : G/K \to \operatorname{Im}\theta$, $gK \mapsto \theta(g)$ where $K = \ker\theta$ and will show that it is an isomorphism.

First check that Φ is well-defined,

$$g_1K = g_2K \;\Rightarrow\; g_2^{-1}g_1 \in K \;\Rightarrow\; \theta(g_2^{-1}g_1) = e \;\Rightarrow\; \theta(g_2)^{-1}\theta(g_1) = e \;\Rightarrow\; \theta(g_1) = \theta(g_2) \;\Rightarrow\; \Phi(g_1K) = \Phi(g_2K). \tag{6.4.7}$$

If $\theta(g_1) = \theta(g_2)$ then $\theta(g_1^{-1}g_2) = e$ and so $g_1^{-1}g_2 \in K$. Hence $g_1K = g_2K$ by Theorem 6.2.4. Thus, Φ is injective.
Any element in $\mathrm{Im}(\theta) = \theta(G)$ is $\theta(g)$ for some $g \in G$, so $\Phi(gK) = \theta(g)$. Hence, Φ is surjective.
$\forall g_1, g_2 \in G$,

$$\Phi(g_1Kg_2K) = \Phi(g_1g_2K) = \theta(g_1g_2) = \theta(g_1)\theta(g_2) = \Phi(g_1K)\Phi(g_2K). \tag{6.4.8}$$

So Φ is a homomorphism. Thus, Φ is an isomorphism. □

Example 6.4.10. Let $G = (\mathbb{Z}, +)$. Then $\langle n \rangle = \{nk : k \in \mathbb{Z}\} \lhd G$. Let $H = C_n = \langle x : x^n = 1 \rangle$. Define $\theta : G \to H$ taking $m \to x^m$. This is a surjective homomorphism with kernel $\langle n \rangle$.

Therefore by Theorem 6.4.9, $\mathbb{Z}/\langle n \rangle \cong C_n$ and $\mathbb{Z}/\langle n \rangle$ is the group of integers mod$n$, sometines written $\mathbb{Z}/n\mathbb{Z}$.

Example 6.4.11. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{C}\setminus\{0\}, \times)$, with $\theta : G \to H$ taking $t \to e^{it}$.

First we check θ is a homomorphism: $\theta(t_1 + t_2) = e^{i(t_1+t_2)} = e^{it_1}e^{it_2} = \theta(t_1)\theta(t_2)$.

Now $\mathrm{Im}\,\theta = \theta(G) = \{z \in \mathbb{C} : |z| = 1\}$. Then $K = \ker\theta = \{2n\pi : n \in \mathbb{Z}\} := \langle 2\pi \rangle \leq \mathbb{R}$, which is normal in $(\mathbb{R}, +)$ since

$$\forall g \in G, k \in K \;\Rightarrow\; g \in \mathbb{R}, k = 2n\pi, n \in \mathbb{Z} \;\Rightarrow\; gkg^{-1} = g + 2n\pi + (-g) = 2n\pi \in K. \tag{6.4.9}$$

Therefore Theorem 6.4.9 implies that $\mathbb{R}/\langle 2\pi \rangle \cong \mathrm{Im}\,\theta = \left\{e^{it} : t \in \mathbb{R}\right\} = \{z \in \mathbb{C} : |z| = 1\}$.

The map Φ is $\Phi(t + \langle 2\pi \rangle) = e^{it}$. Similarly, if $\theta : t \mapsto e^{2\pi it}$, the map Φ is $\Phi(t + \mathbb{Z}) = e^{2\pi it}$.

Theorem 6.4.12 (second isomorphism theorem)**.** Let $H \leq G$ and $K \lhd G$. Then $HK \leq G$ and $H \cap K \lhd G$ where $HK = \{hk : h \in H, k \in K\}$ and $(HK)/K \cong H/(H \cap K)$.

Proof. First show that HK is a subgroup. It suffices to show $(h_1k_1)(h_2k_2)^{-1} \in HK$ with $h_1, h_2 \in H, k_1, k_2 \in K$ by Lemma 6.1.7.

$$(h_1k_1)(h_2k_2)^{-1} = h_1 \underbrace{k_1k_2^{-1}}_{\in K} h_2^{-1} \tag{6.4.10}$$

But $Kh_2^{-1} = h_2^{-1}K$ since $K \lhd G$ and so $(k_1k_2^{-1})h_2^{-1} = h_2^{-1}k_3$ for some $k_3 \in K$. So $(h_1k_2)(h_2k_2)^{-1} = h_1h_2^{-1}k_3 \in HK$.

Define

$$\theta : H \to H/K,\; h \mapsto hK. \tag{6.4.11}$$

This is a group homomorphism (identity is e_HK) since

$$\theta(h_1h_2) = h_1h_2K = h_1Kh_2K = \theta(h_1)\theta(h_2). \tag{6.4.12}$$

So Theorem 6.4.9 implies that $\ker\theta \lhd G$ and $H/\ker\theta \cong \mathrm{Im}\,\theta$. Now

$$\ker\theta = \{h \in H : hK = eK = K\} = H \cap K. \tag{6.4.13}$$

Thus $H \cap K \lhd G$. Also,

$$\mathrm{Im}\,\theta = \{hK : h \in H\} = \{(hk)K : h \in H, k \in K\} = \{gK : g \in HK\} = (HK)/K \;\text{ (by Theorem 6.4.7)} \tag{6.4.14}$$

cosets of K in HK. Thus $H/(H \cap K) \cong (HK)/K$, as required. □

Proposition 6.4.13. Let $K \lhd G$ and $L \leq G$ be a subgroup containing K. Then

$$L/K \lhd G/K \;\Leftrightarrow\; L \lhd G. \tag{6.4.15}$$

Proof. In fact, there is a bijection[12] between subgroups of G/K and the subgroups of G containing K. This is given by the maps

$$\begin{array}{ccc} \{\text{subgroups of } G/K\} & & \{\text{subgroups of } G \text{ containing } K\} \\ X & \longrightarrow & \{g \in G : gK \in X\} \\ L/K & \longleftarrow & L \end{array}$$

[12] need proof

These maps are inverses of each other.

Take a normal subgroup $K \lhd G$ and form the quotient group G/K, with elements the cosets gK and multiplication defined by $g_1Kg_2K = g_1g_2K$. The correspondence

$$\{\text{subgroups of } G/K\} \longleftrightarrow \{\text{subgroups of } G \text{ containing } K\} \tag{6.4.16}$$

restricts to

$$\{\text{normal subgroups of } G/K\} \longleftrightarrow \{\text{normal subgroups of } G \text{ containing } K\} \tag{6.4.17}$$

For a subgroup $L/K \leq G/K$ (L is a normal subgroup of G containing K) we have that

$$(gK)(L/K)(gK)^{-1} = (gLg^{-1})/K \tag{6.4.18}$$

so $K \leq L$, we have $(gLg^{-1})/K = L/K \;\Rightarrow\; gl_1g^{-1}K = l_2K \;\Rightarrow\; gl_1g^{-1} \in L \;\Rightarrow\; gLg^{-1} = L$. It is obvious that $gLg^{-1} = L \;\Rightarrow\; (gLg^{-1})/K = L/K$. Thus,

$$(gK)(L/K)(gK)^{-1} = L/K \;\Leftrightarrow\; gLg^{-1} = L, \tag{6.4.19}$$

that is, $L/K \lhd G/K \;\Leftrightarrow\; L \lhd G$. □

Theorem 6.4.14 (Third Isomorphism Theorem)**.** If K and L are normal subgroups of G with $K \leq L \lhd G$ (i.e. $K \lhd L$) then $(G/K)/(L/K) \cong G/L$.

Proof. Apply Theorem 6.4.9 to the well chosen map

$$\theta : G/K \to G/L,\; gK \mapsto gL. \tag{6.4.20}$$

We need to check this is well-defined,

$$g_1K = g_2K \;\Rightarrow\; g_1^{-1}g_2 \in K \leq L \;\Rightarrow\; g_1L = g_2L. \tag{6.4.21}$$

To check θ is a homomorphism,

$$\theta(g_1Kg_2K) = \theta(g_1g_2K) = g_1g_2L = g_1Lg_2L = \theta(g_1K)\theta(g_2K). \tag{6.4.22}$$

Clearly, $\operatorname{Im}\theta = G/L$. Also $\ker\theta = \{gK : gL = L\} = \{gK : g \in L\} = L/K$ and so Theorem 6.4.9 implies

$$(G/K)/(L/K) \cong G/L. \tag{6.4.23}$$

□

6.4.3 Simple groups

Definition 6.4.2 (Simplicity)**.** G is simple if the only normal subgroups in it are $\{e\}$ and G itself.

Proposition 6.4.15. The only simple abelian groups are C_p for p prime.

Proof. 'Normal' for abelian groups is easy to understand as all subgroups are normal because of commutativity. Take a non-trivial element $g \neq e$ in a simple abelian group G.

Then either g is of infinite order and G contains the normal subgroup $\{\dots, g^{-1}, e, g, g^2, \dots\}$.

Simplicity implies that $G = \{\dots, g^{-1}, e, g, g^2, \dots\}$. But then there is also the normal subgroup $\{\dots, g^{-2}, e, g^2, g^4, \dots\}$, a contradiction.

Or g is of finite order and G has the subgroup $\{e, g, g^2, \dots, g^{o(g)-1}\}$. Simplicity implies that $G = \{e, g, g^2, \dots, g^{o(g)-1}\}$. But if $o(g) = rs$, say, then we also have the subgroup $\{e, g^r, g^{2r}, \dots, g^{r(s-1)}\}$. Now simplicity implies that there are no non-trivial factorisations of $o(g)$ so $G = \{e, g, \dots, g^{p-1}\}$ for some prime p. □

Thus, combining Corollary 6.2.12 and Proposition 6.4.15, we have the following corollary,

Corollary 6.4.16. A group of order p where p is a prime is cyclic one, C_p. Also, it's simple and abelian.

Theorem 6.4.17. A_n is simple for $n \geq 5$.

Remark. We shall see shortly that the alternating group A_5 on $\{1, \ldots, 5\}$ is simple (see Proposition 6.5.33).

Note that $|A_3| = 3$, so A_3 is isomorphic to C_3 and simple. $|A_4| = 12$ and A_4 contains the normal subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\} \lhd A_4$, so A_4 is not simple.

There are finitely many families of finite simple groups, and 26 groups that do not fit into those general families, called the sporadic ones.

Note $|A_5| = 60$ and $|A_6| = 360$. There is another finite simple group of order 168, $GL_3(\mathbb{Z} \bmod 2)$, the group of invertible 3×3 matrices entries $\{0, 1\}$ modulo 2[13].

Proof. [14] □

Theorem 6.4.18. Let G be a finite group. Then there are subgroups $H_1, \ldots, H_s$ such that

$$G = H_1 \geq H_2 \geq \cdots \geq H_s = \{e\} \tag{6.4.24}$$

with $H_{i+1} \lhd H_i$ and H_i/H_{i+1} simple.

Remark. Not all H_i normal in G.

Proof. Let H_2 be normal in G with $|H_2|$ of largest order not equal to $|G|$. Then the correspondence between normal subgroups of G containing H_2 and the normal subgroups of G/H_2 implies that G/H_2 simple. Repeat this to find $H_3 \lhd H_2$ with H_2/H_3 simple.

The process stops when we reach $H_s = \{e\}$. □

Remark. The simple groups H_i/H_{i+1} are essentially unique, although there may be lots of ways of picking the subgroups H_i, called composition factors.

Definition 6.4.3. G is soluble if all composition factors can be chosen to be cyclic of prime order.

Remark. The terminology comes from Galois theory, see the relevant Part II course. You all know a formula for solving quadratic equations. You can do something similar involving roots for cubics and quartics, the process is called 'solution by radicals'. But you cannot necessarily do it for a quintic, e.g. $t^5 - 6t + 3 = 0$. This can be shown by defining a Galois group associated with the polynomial. If you can solve the polynomial by radicals then the Galois group is soluble.

Example 6.4.19 (finte simple groups)**.** (i) C_p, for p prime.

(ii) A_n for $n \geq 5$ (see Theorem 6.4.17).

(iii) [15] $PSL_n(q)$ where q is a prime power and $n \geq 2$; also $PSO_n(q)$, $PSU_n(q)$ and $PS_{p_n}(q)$. These four are known as the 'classical groups'

$$GL_2(5) \lhd \frac{SL_2(5)}{2} \tag{6.4.25}$$

where $GL_2(5)$ is integer arithmeticmod5 and Z = centre = {scalars in $SL_2(5)$} = $\{\pm I\}$

(iv) $PSL_2(5) \cong A_5$[16].

Then there are the exceptional groups; G_2 and 10 more families corresponding to Lie algebras, and the 26 sporadic groups, starting with M_{11} (which was discovered in the 1860s and has elements) and working up to M, the 'Monster' group.

6.5 Group actions

6.5.1 Group actions

Definition 6.5.1. Let G be a group and X a non-empty set. We say that G acts on X if there is a mapping $\rho : G \times X \to X$, taking $(g, x) \to \rho(g, x) = g(x)$, such that

[13] This is left as an exercise.
[14] proof needed, see IB for the proof where $n > 5$.
[15] need check, add in matrix section
[16] see example sheet 4, question 13

(i) if $g \in G$, $x \in X$ then $g(x) \in X$.

(ii) $(g_1 g_2)(x) = g_1(g_2(x)), \forall g_1, g_2 \in G, x \in X$.

(iii) $e(x) = x, \forall x \in X$.

ρ is called group action.

Lemma 6.5.1. Fixing $g \in G$, the map $\varphi_g : X \to X$, $x \mapsto g(x)$ is a permutation of X, so $\varphi_g \in \mathrm{Sym}(X)$. Then the mapping $\varphi : G \to \mathrm{Sym}(X)$, $g \mapsto \varphi_g$, with $\varphi_g(x) = g(x)$, is a homomorphism called a permutation representation of G.

The image $\varphi(G)$ is a subgroup of $\mathrm{Sym}(X)$, denoted G^X. The kernel of φ, $\ker\varphi = \{g \in G : g(x) = x, \forall x \in X\}$, also denoted G_X, is a normal subgroup and $G/G_X \cong G^X$.

Proof. φ_g is certainly a mapping $X \to X$. For $x \in X$, $\varphi_{g^{-1}} \circ \varphi_g = \varphi_{g^{-1}}(g(x)) = g^{-1}(g(x)) = (g^{-1}g)(x)$ by condition (ii) $= e(x) = x$ by condition (iii), and similarly in reverse. Thus we have inverses, which means the map is bijective, so it is a permutation.

Now consider the mapping $\varphi : G \to \mathrm{Sym}(X)$, $g \mapsto \varphi_g$. $\forall g_1, g_2 \in G$, $\forall x \in X$,

$$\varphi(g_1 g_2)(x) = \varphi_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2(x)) = \varphi_{g_1}(\varphi_{g_2}(x)) = (\varphi_{g_1}\varphi_{g_2})(x) = (\varphi(g_1)\varphi(g_2))(x). \tag{6.5.1}$$

Thus $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ and the map φ is a homomorphism.

The rest is from Theorem 6.4.9. □

Remark. G-actions on $X \Leftrightarrow$ homomorphisms from $G \to \mathrm{Sym}(X)$.

Remark. It follows that G has a normal subgroup (G_X) of index dividing $n!$, where $|X| = n$ so that $|\mathrm{Sym}(X)| = n!$.

Example 6.5.2. (i) $G = D_8$ = the group of symmetries of a square. Then if X is the set of vertices and Y the set of edges, G acts on both X and Y. Both give an injective homomorphism into S_4.

(ii) Let G be the symmetry group of the cube, $|G| = 48$, and X the set of diagonals, $|X| = 4$. G acts on X,

$$G^X = S_4, \qquad G_X = \{e, \text{ symmetry sending each vertex to the opposite one}\}^{17}. \tag{6.5.2}$$

6.5.2 The orbit-stabiliser theorem

Definition 6.5.2. G acting on X is transitive if for every pair $x_1, x_2 \in X$ there is an element $g \in G$ with $g(x_1) = x_2$.

Definition 6.5.3 (orbit)**.** Let G act on X and let $x \in X$. The orbit of G on X containing x is $G(x) = \{g(x) | g \in G\}$. This is a subset of X on which g acts transitively.

Lemma 6.5.3. Each G-orbit on X is G-invariant, with G transitive in its action on $G(x)$, for $x \in X$. The distinct G-orbits form a partition of X.

Proof. The orbit $G(x)$ is G-invariant, so that $g(G(x)) = G(x)$ for $g \in G$. So the action of G on X induces an action on $G(x)$, which is transitive. It follows that we can define an equivalence relation on X given by [$x_1 \sim x_2$ if $\exists g \in G : x_2 = g(x_1)$]. □

Example 6.5.4. The left regular action[18] is transitive on $X = G$, because if $x_1, x_2 \in G$ then we can set $g = x_2 x_1^{-1}$ to get $(x_2 x_1^{-1})x_1 = x_2$.

Definition 6.5.4 (stabiliser)**.** If G acts on X, and $x \in X$, the stabiliser of x in G is $G_x = \{g \in G : g(x) = x\}$.

Lemma 6.5.5. G_x is a subgroup of G.

Proof. $e \in G_x$, obviously. If $g_1, g_2 \in G_x$ then so is $g_1^{-1} g_2$, because $(g_1^{-1} g_2)(x) = g_1^{-1}(g_2(x)) = g_1^{-1}(x) = x$. □

Theorem 6.5.6 (Orbit-stabiliser theorem)**.** Let a finite group G act on X and let $x \in X$. Then $G_x \leq G$, and $|G| = |G_x|\,|G(x)|$; that is, $|G : G_x|$, the number of left cosets of G_x in G, is equal to $|G(x)|$.

[17] need details

[18] see section Definition 6.5.10, check needed.

Proof. Define $(G : G_x)$ to be the set of left cosets of G_x in G. Then all that is needed is to prove that the mapping $G(x) \to (G : G_x)$ taking $g(x) \to gG_x$ is a well-defined bijection.

This can be proved as follows. If $g_1(x) = g_2(x)$ then $g_2^{-1}g_1(x) = x$, so $g_2^{-1}g_1 = G_x \Leftrightarrow g_2G_x = g_1G_x$ (Theorem 6.2.4), so the map is well-defined.

To prove injectivity, reverse the steps ($g_2G_x = g_1G_x \Rightarrow g_2^{-1}g_1 = G_x$ by Theorem 6.2.4, then $g_1(x) = g_2(x)$). For surjectivity, note that any coset of G_x is gG_x for some $g \in G$, so gG_x is the image of $g(x)$. □

Example 6.5.7 (Examples including the left coset action)**.** If G is the group of all symmetries of a regular n-gon (see Theorem 6.1.15), then $|G| \geq 2n$ because there are n rotations and reflections. Let $X = \{\text{vertices of the } n\text{-gon}\}$. G acts on X and is transitive (e.g. by rotations). Then considering the point 1, we get $|G| = |X|\,|G_1| = n\,|G_1| = n \times 2$ because the stabiliser of the point 1 contains just a reflection and the identity.

Example 6.5.8. Let G be a group, H a subgroup of G and $X = (G : H)$ the set of left cosets of G_x in G.

Definition 6.5.5 (kernel)**.** Let G act on X. Then the kernel of the action is $\bigcap_{x\in X} G_x$, that is, the set consisting of all the elements of G which act trivially on X.

An action is faithful if its kernel is trivial $\{e_G\}$.

Lemma 6.5.9. The kernel $\bigcap_{x\in X} G_x$ is a subgroup of G.

Proof. Since G_x is subgroup of G by Lemma 6.5.5 (that is $\forall g_1, g_2 \in G_x$, $g_1^{-1}g_2 \in G_x$), we have that the kernel is a subgroup of G as well ($g_1, g_2 \in \bigcap_{x\in X} G_x$, $g_1^{-1}g_2 \in \bigcap_{x\in X} G_x$). □

Example 6.5.10. $G = S_4$ and $X =$ the set of all partitions of $\{1, 2, 3, 4\}$ into two parts of size $2 = \{12|34, 13|24, 14|23\}$. Then G acts on X in the way you would expect. The kernel is

$$\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \tag{6.5.3}$$

Example 6.5.11. For a subgroup H of G, let X be the set of left cosets of H. Consider the action of G on X given by

$$g * g_1H = gg_1H. \tag{6.5.4}$$

for all $g_1 \in G$. Then

$$gg_1H = g_1H \Leftrightarrow g_1^{-1}gg_1H = H \Leftrightarrow g_1^{-1}gg_1 \in H \Leftrightarrow g \in g_1Hg_1^{-1}. \tag{6.5.5}$$

Thus, the kernel is $\bigcap_{g_1\in G} g_1Hg_1^{-1}$. Let $H' = \bigcap_{g_1\in G} g_1Hg_1^{-1}$. We have that the kernel H' is a subgroup of G (Lemma 6.5.9) and $H' \subseteq H$,

$$H' = \bigcap_{g_1\in G} g_1Hg_1^{-1} \supseteq \bigcap_{g_1\in G} g_1H'g_1^{-1}. \tag{6.5.6}$$

That is, $\forall h \in H', g \in G$, $\exists h' \in H'$ such that $ghg^{-1} = h' \Leftrightarrow gh = h'g$. By Definition 6.4.1, we have that H' is normal subgroup.

If $K \lhd G$, $K \leq H$ then $g_1Kg_1^{-1} = K$ since K is normal. But $g_1Kg_1^{-1} \leq g_1Hg_1^{-1}$ so $g_1Kg_1^{-1} = K \leq g_1Hg_1^{-1}$ for all $g_1 \in G$. Thus, The kernel is the largest normal subgroup of G contained in H.

Theorem 6.5.12. Let G be a finite group and H a proper subgroup of G of index n. Then there is a normal subgroup K of G contained in H such that G/K is isomorphic to a subgroup of S_n. In particular $|G : K|$ divides $n!$ and is at least n.

Moreover, if G is non-abelian simple then G is isomorphic to a subgroup of A_n and $n \geq 5$.

Proof. Let K be the kernel of the action of G on X, where X is the set of left cosets of H. Lemma 6.5.1 implies that $G/K \cong G^X$, a subgroup of S_n. Lagrange's theorem 6.2.7 implies subgroups of S_n have order dividing $n!$. Since $K \leq H$ and H is of index n in G we have that $|G/K| \geq n$.

Now assume G is non-abelian simple. Then $K = \{e\}$ (since H is a proper subgroup containing K), and so $G \cong G^X$ subgroup of S_n. Thus, G^X is non-abelian simple. But $A_n \lhd S_n$ (by Proposition 6.4.3) and so by the second isomorphism theorem (Theorem 6.4.12), $G^X \cap A_n \lhd S_n$. Since $G^X \cap A_n \subseteq G^X$, $G^X \cap A_n \lhd G^X$ ($G^X \cap A_n$ is normal subgroup in S_n). Simplicity implies that either

$$G^X \cap A_n = \{e\} \quad \text{or} \quad G^X \cap A_n = G^X. \tag{6.5.7}$$

In the first case, the second isomorphism theorem (Theorem 6.4.12) implies

$$G^X = G^X / \{e\} = G^X / (G^X \cap A_n) \cong (G^X A_n)/A_n \leq S_n/A_n \tag{6.5.8}$$

and hence $\left|G^X\right| \leq 2$, which should be abelian, a contradiction. In the second case, $G^X \subseteq A_n$ and thus $G^X \leq A_n$.

Finally, we have $n > 4$ since A_4 ($A_n, n < 4$ are subgroups of A_4) has no non-abelian simple subgroups[19]. □

Proposition 6.5.13. If G is any group acting on a set X, with $x \in X$ and $g \in G$, then $G_{g(x)} = gG_xg^{-1} = \left\{ghg^{-1} : h \in G_x\right\}$.

Proof. $G_{g(x)} = \{g' \in G : g'(g(x)) = g(x)\}$. Let $g'' = g'g$. Then

$$G_{g(x)} = \left\{g''g^{-1} : g'' \in G, g''(x) = g(x)\right\}. \tag{6.5.9}$$

Let $g''' = g^{-1}g''$. Then $G_{g(x)} = \left\{gg'''g^{-1} : g''' \in G, g'''(x) = x\right\} = gG_xg^{-1}$. □

6.5.3 Groups of symmetries of regular solids

[20]

6.5.4 Burnside's Theorem

[21]

6.5.5 Conjugation

Lemma 6.5.14. Let G be a group, $X = G$ with

$$g * x = g(x) = gxg^{-1} \tag{6.5.10}$$

for $g \in G$, $x \in G$. Then gxg^{-1} is an element of G (which is X). The action $\rho : G \times G \to G$ is called the conjugation action.

Proof. For $g_1, g_2 \in G$,

$$(g_1g_2)x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = g_1(g_2(x)) \tag{6.5.11}$$

so it satisfies the condition (ii) in Definition 6.5.1. □

Remark. In this case the permutation $\varphi_g : x \mapsto gxg^{-1}$ as well as being bijective is a homomorphism $G \to G$. Thus they are automorphisms and we have $\varphi_g \in \operatorname{Aut} G$ (see Definition 6.1.19).

Definition 6.5.6. The orbit of $x \in G$ is called its conjugacy class, written

$$\operatorname{ccl}_G(x) = \left\{gxg^{-1} : g \in G\right\}. \tag{6.5.12}$$

Note that e is the only element in its conjugacy class, and others may be the only element in their classes as well. If two elements are in the same orbit, they are said to be conjugate.

Definition 6.5.7. The stabiliser of x in G is called its centraliser, written

$$C_G(x) = \left\{g \in G : gxg^{-1} = x\right\} = \{g \in G : gx = xg\}. \tag{6.5.13}$$

This is the set of all elements which commute with x.

Remark. If G is a finite group and $x \in G$, $C_G(x)$ is a subgroup of G by Lemma 6.5.5. Also, $|G : C_G(x)| = |\operatorname{ccl}_G(x)|$ by the orbit-stabiliser theorem.

[19] need proof
[20] need to check
[21] need to check

Definition 6.5.8 (centre)**.** The kernel of the conjugation action is called the centre of G, written $Z(G) = \bigcap_{x\in G} C_G(x)$. This is the intersection of all the centralisers, so consists of the elements which commute with everything, i.e.

$$Z(G) = \bigcap_{x\in G} C_G(x) = \left\{g \in G : gxg^{-1} = x, \forall x \in G\right\} = \left\{g \in G : gx = xg, \forall x \in G\right\}. \tag{6.5.14}$$

Proposition 6.5.15. $Z(G)$ is a subgroup of G.

Proof. Direct result from Lemma 6.5.9. □

Proposition 6.5.16. A group G is abelian if and only if $Z(G) = G$.

Remark. This is obvious from Definition 6.5.8

Lemma 6.5.17. For any group G, if $G/Z(G)$ is cyclic then G is abelian.

Proof. Let $G/Z(G)$ be cyclic (Definition 6.1.6). Suppose gZ ($Z = Z(G)$) generates $G/Z(G)$ ($G/Z(G) = \langle gZ\rangle$) and thus each coset in Z is of the form $(gZ)^r = g^r Z$ (by definition of centre, Definition 6.5.8) for some r. Thus any element $x \in G$ is of the form $g^r z$ for some $z \in Z$, $r \in \mathbb{Z}$.

$$x_1x_2 = (g^{r_1}z_1)(g^{r_2}z_2) = g^{r_1}g^{r_2}z_1z_2 = g^{r_1+r_2}z_2z_1 = g^{r_2}g^{r_1}z_2z_1 = (g^{r_2}z_2)(g^{r_1}z_1) = x_2x_1 \tag{6.5.15}$$

using that $z_1, z_2 \in Z$. Thus G is abelian and so $G = Z(G)$. □

Lemma 6.5.18. Let G be a finite group. Then $1 = \sum \frac{1}{|C_G(x)|}$, summing over distinct conjugacy classes.

Proof. We count the elements of G. $|G| = \sum |\mathrm{ccl}_G(x)|$, so

$$|G| = \sum \frac{|G|}{|C_G(x)|} \tag{6.5.16}$$

since $|\mathrm{ccl}_G(x)| = |G|/|C_G(x)|$. Now divide by $|G|$. □

Example 6.5.19. The conjugacy classes of elements of D_8 and find its centre. (The centre of D_8 is $\langle a^2\rangle$.[22])

Example 6.5.20. The conjugacy classes of elements of Q_8 and find its centre. [23]

Proposition 6.5.21. (i) $o(gxg^{-1}) = o(x)$, i.e. conjugate elements have the same order.

(ii) $z \in Z(G)$ iff $\mathrm{ccl}_G(z) = \{z\}$, i.e. z is the only element in its conjugacy class, i.e. $G = C_G(z)$.

Proof. (i) Assume gxg^{-1} has order m and x has order n, $x^n = e \Rightarrow e = gx^ng^{-1} = \left(gxg^{-1}\right)^n$, thus $m|n$ by Lemma 6.2.10. Similarly, $e = \left(gxg^{-1}\right)^m = gx^mg^{-1} \Rightarrow e = x^m \Rightarrow n|m$. Thus $m = n$.

(ii) $z \in Z(G) \Leftrightarrow \forall x \in G, xz = zx \Leftrightarrow \forall x \in G, xzx^{-1} = z \Leftrightarrow \mathrm{ccl}_G(z) = \left\{xzx^{-1} : x \in G\right\} = \{z : x \in G\} = \{z\}$.

□

Proposition 6.5.22. If G is a finite group of order p^a for some prime p, then the centre of G is not just the identity but contains at least $p - 1$ other element.

Proof. Consider the conjugation action of G and its conjugacy class sizes, which must divide the order of G. Thus, we assume there are b_0 conjugacy classes with size 1, b_1 conjugacy classes with size p, b_2 conjugacy classes with size p^2, …, b_{a-1} conjugacy classes with size p^{a-1}. Thus,

$$|G| = b_0 \times 1 + b_1 \times p + b_2 \times p^2 + \cdots + b_{a-1} \times p^{a-1} = \sum_{n=0}^{a-1} b_n p^n \Rightarrow p|b_0. \tag{6.5.17}$$

However, we know $e \in Z(G)$, thus $b_0 \neq 0$, so there are at least $p - 1$ other element in the centre of G. □

[22] details needed
[23] details needed

Definition 6.5.9. Consider the permutation $\pi \in S_n$, written in disjoint-cycle notation (including fixed points or 1-cycles). The cycle type of π is $(n_1, n_2, \ldots, n_k)$ where $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$, and the cycles in have length n_i. It follows that $n = n_1 + \cdots + n_k$.

Example 6.5.23. $(1\ 2\ 3)(4\ 5)(6) \in S_6$. has cycle type $(3, 2, 1)$.

$e \in S_6$ has cycle type $(1, 1, 1, 1, 1, 1) = (1^6)$.

Theorem 6.5.24. The permutations $\pi, \sigma \in S_n$ are conjugate in S_n iff they have the same cycle type.

Proof. If $\sigma = (a_{11}a_{12}\ldots a_{1n_1})\,(a_{21}a_{22}\ldots a_{2n_2})\ldots(a_{k1}a_{k2}\ldots a_{kn_k})$ and $\tau \in S_n$(any element), then

$$\tau\sigma\tau^{-1}(\tau(a_{11})) = \tau\sigma(a_{11}) = \tau(a_{12}) \;\Rightarrow\; \tau\sigma\tau^{-1} = (\tau(a_{11})\tau(a_{12})\ldots\tau(a_{1n_1}))\,(\tau(a_{21})\ldots\tau(a_{2n_2}))\ldots(\tau(a_{k1})\ldots\tau(a_{kn_k}))\,. \tag{6.5.18}$$

The same pattern works for all a_{ij}. Therefore if elements are conjugate in S_n then they have the same cycle type.

Conversely, if σ is as before and π has the same cycle type, say

$$\pi = (b_{11}b_{12}\ldots b_{1n_1})\,(b_{21}\ldots b_{2n_2})\ldots(b_{k1}\ldots b_{kn_k})\,, \tag{6.5.19}$$

then let τ be a permutation with $\tau : a_{ij} \to b_{ij}$. Then by the previous result $\tau\sigma\tau^{-1}(\tau(a_{11})) = \tau(a_{12})$, we have $\pi = \tau\sigma\tau^{-1}$, so π, σ are conjugate. □

Corollary 6.5.25. The number of conjugacy classes in S_n is $p(n)$, the number of partitions of n into $n = n_1 + \cdots + n_k$ for some k with $n_1 \geq \ldots n_k \geq 1$.

Example 6.5.26. $(1\ k) = (2\ k)(1\ 2)(2\ k)^{-1}$ and $(k\ l) = (1\ l)(1\ k)(1\ l)$.

In fact, all transpositions are conjugate as they have the same cycle type.

Example 6.5.27. The conjugacy classes in S_4;

example member	cycle type	size	sign	centraliser	size of centraliser
ι	1,1,1,1	1	+	S_4	24
$(1\ 2)(3)(4)$	2,1,1	6	-	$\langle(1\ 2), (3\ 4)\rangle$	4
$(1\ 2\ 3)(4)$	3,1	8	+	self-centralising	3
$(1\ 2)(3\ 4)$	2,2	3	+	D_8	8
$(1\ 2\ 3\ 4)$	4	6	-	$\langle(1\ 2\ 3\ 4)\rangle$	4

Example 6.5.28. The conjugacy classes in A_4;

example member	cycle type	size	centraliser
ι	1^4	1	A_4
$(1\ 2)(3\ 4)$	2^2	3	$\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$
$(1\ 2\ 3)(4)$	3,1	4	$\langle(1\ 2\ 3)\rangle$
$(1\ 3\ 2)(4)$	3,1	4	$\langle(1\ 2\ 3)\rangle$

Example 6.5.29. The conjugacy classes in S_5;

cycle type	example member	size	centraliser	sign
1^5	ι	1	S_5	+
$2,1^3$	$(1\ 2)$	10	$\langle(1\ 2)\rangle \times S_3$	-
$2^2,1$	$(1\ 2)(3\ 4)$	15	D_8	+
$3,1^2$	$(1\ 2\ 3)$	20	$\langle(1\ 2\ 3)\rangle \times S_2$	+
3,2	$(1\ 2\ 3)(4\ 5)$	20	$\langle(1\ 2\ 3)\rangle \times \langle(4\ 5)\rangle$	-
4,1	$(1\ 2\ 3\ 4)$	30	$\langle(1\ 2\ 3\ 4)\rangle$	-
5	$(1\ 2\ 3\ 4\ 5)$	24	$\langle x\rangle$	+

Example 6.5.30. The conjugacy classes in A_5;

cycle type	size	centraliser
1^5	1	A_5
$2^2, 1$	15	V_4(Klein 4-group)
$3, 1^2$	20	$\langle x \rangle$
5	12	$\langle x \rangle$
5	12	$\langle x' \rangle$

Example 6.5.31. Consider S_5 and A_5, take $x \in A_5$. (1 2)(3 4)(5) commutes with (1 2), (1 2 3)(4)(5) commutes with (4 5). But conjugacy classes of 5 cycles do not split into 2 conjugacy classes of size 12. Consider (1 2 3 4 5) and its conjugates.

$$g(1\ 2\ 3\ 4\ 5)g^{-1} = (g(1) \dots g(5)) \tag{6.5.20}$$

$$C_{S_n}(1\ 2\ 3\ 4\ 5) = \{\iota, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2)\} \tag{6.5.21}$$

$C_{S_n}(1\ 2\ 3\ 4\ 5)$ is of order 5, all elements are even.

Lemma 6.5.32. Let $H \neq \{\iota\}$ be a normal subgroup of A_5. It must contain a 3-cycle.

Proof. Let $\sigma \in A_5$. When we write σ in disjoint cycle notation it is either a 5-cycle, a 3-cycle or a product of two 2-cycles. (since the other possible cycle types are odd permutations.)

Suppose H contains a 5-cycle $\sigma = (abcde)$. Since $(ace) \in A_5$ and $H \lhd A_5$ we have:

$$(ace)\sigma(ace)^{-1} = (ace)(abcde)(eca) = (ace)(abcde)(eca) = (acbed) \in H \tag{6.5.22}$$

But H is a subgroup so $(abcde)(acbed) = (adb) \in H$.

Now suppose H contains a product of two disjoint transpositions: $\sigma = (ab)(cd) \in H$. Then $(ae)(cd) \in A_5$ so

$$(ae)(cd)\sigma(ae)(cd)^{-1} = (ae)(cd)(ab)(cd)(ae)(cd) = (be)(cd) \in H \tag{6.5.23}$$

since $H \lhd A_5$. Thus $(ab)(cd)(be)(cd) = (abe) \in H$.

Thus $H \neq \{\iota\}$ implies H contains a 3-cycle. □

Proposition 6.5.33. A_5 is simple.

Proof. Consider a normal subgroup K of A_5. Thus $gkg^{-1} \in K$ for all $k \in K$, $g \in A_5$. Thus K must be a union of conjugacy classes in A_5 and contains $\{\iota\}$. So the order of K should be one of the following possibilities

$$1, \underbrace{16}_{1+15}, \underbrace{21}_{1+20}, \underbrace{25}_{1+24}, \underbrace{36}_{1+15+20}, \underbrace{40}_{1+15+24}, \underbrace{45}_{1+20+24}, \underbrace{60}_{1+15+20+24}. \tag{6.5.24}$$

But by Lagrange's Theorem 6.2.7, $|K|$ divides $60 = |A_5|$. There is no way of taking a union of the conjugacy classes we've worked out to give $|K|$ dividing 60, unless $K = \{e\}$ or $K = A_5$. □

Alternative Proof. Suppose $\{\iota\} \neq H \lhd A_5$. We will prove that $H = A_5$. From Lemma 6.5.32, We know that H contains a 3-cycle. Now pick a 3-cycle $(abc) \in H$. Consider the following two permutations:

$$\tau = \begin{pmatrix} a & b & c & d & e \\ x & y & z & s & t \end{pmatrix}, \qquad \tau' = \begin{pmatrix} a & b & c & d & e \\ x & y & z & t & s \end{pmatrix} \tag{6.5.25}$$

Notice that $\tau(abc)\tau^{-1} = (xyz)$ and $\tau'(abc)\tau'^{-1} = (xyz)$. Exactly one of τ or τ' is in A_5 since they differ by a transposition (st). Thus $(xyz) \in H$. But (xyz) was arbitrary so H contains all possible 3-cycles.

Finally notice that in 6.5.30:

$$\iota = (abc)(abc)(abc), \quad (ab)(cd) = (dac)(abd), \quad (ab)(bc) = (abc), \quad (abcde) = (abc)(cde). \tag{6.5.26}$$

Thus any even permutation can be written as a product of 3-cycles. But all possible 3-cycles are in H so H must be all

of A_5, and A_5 is simple. [24] □

Theorem 6.5.34. Let $x \in A_n$. Then $\mathrm{ccl}_{A_n}(x) \leq \mathrm{ccl}_{S_n}(x)$, with equality iff the centraliser in S_n of x is half odd. Moreover, if inequality holds, then $\mathrm{ccl}_{S_n}(x)$ splits into two classes in A_n, both of the same size, $|\mathrm{ccl}_{S_n}(x)|/2$.

Proof. For $x \in A_n$ we have that $\mathrm{ccl}_{A_n}(x) \subset \mathrm{ccl}_{S_n}(x)$. We also have

$$|\mathrm{ccl}_{S_n}(x)| = |S_n : C_{S_n}(x)|, \qquad |\mathrm{ccl}_{A_n}(x)| = |A_n : C_{A_n}(x)| \tag{6.5.27}$$

by the orbit-stabiliser theorem (Theorem 6.5.6). But $C_{A_n}(x) = A_n \cap C_{S_n}$, and thus this set has index 1 or 2 in $C_{S_n}(x)$. To see this, use the second isomorphism theorem (Theorem 6.4.12),

$$C_{S_n}(x)/(A_n \cap C_{S_n}(x)) \cong (A_n C_{S_n}(x))/A_n \leq S_n/A_n. \tag{6.5.28}$$

If all permutations that commute with x are even, i.e. $C_{S_n}(x) = C_{A_n}(x)$,

$$|\mathrm{ccl}_{S_n}(x)| = \frac{|S_n|}{|C_{S_n}(x)|} = \frac{2|A_n|}{C_{A_n}(x)} = 2|\mathrm{ccl}_{A_n}(x)|. \tag{6.5.29}$$

If there is an odd permutation commuting with x, i.e. $|C_{S_n}(x) : C_{A_n}(x)| = 2$,

$$|\mathrm{ccl}_{S_n}(x)| = \frac{|S_n|}{|C_{S_n}(x)|} = \frac{|A_n|}{C_{A_n}(x)} = |\mathrm{ccl}_{A_n}(x)|. \tag{6.5.30}$$

□

6.5.6 Cayley's theorem

Definition 6.5.10 (left regular action)**.** Recall Definition 6.5.1 and let $X = G$. Then the map $\rho : G \times X \to X$ (actually $\rho : G \times G \to G$) taking $(g, x) \to g(x) = gx$ is an action (because it satisfies all the axioms). This is called the left regular action of G.

Theorem 6.5.35 (Cayley Theorem)**.** Any group G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

Proof. Recall Lemma 6.5.1 and let $X = G$, we have the map $\varphi : G \to \mathrm{Sym}(G)$ is a permutation representation and the image $\varphi(G)$ is a subgroup of $\mathrm{Sym}(G)$. Also, from Lemma 6.5.1,

$$G/G_G \cong G^G = \varphi(G) \tag{6.5.31}$$

where G_G is the kernel of φ. Since we have left regular action,

$$G_G = \{g \in G : g(x) = x, \forall x \in X\} = \{g \in G : gx = x, \forall x \in X\} = \{g \in G : g = e, \forall x \in X\} = \{e\}. \tag{6.5.32}$$

Thus $G/G_G = G/\{e\} = G$, so we have $G \cong G^G = \varphi(G)$ i.e. the group G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. □

6.6 Finite p-groups and Finite Abelian Groups

6.6.1 Finite p-groups

Definition 6.6.1 (p-group)**.** A finite group G is a p-group if $|G| = p^n$ for prime p.

Now restating Proposition 6.5.22, we can have

Theorem 6.6.1. Let G be a finite p-group. Then $Z(G) \neq \{e\}$.

Proof. We count the elements of G,

$$|G| = \sum |\mathrm{ccl}_G(x)|. \tag{6.6.1}$$

[24] need check: Remark: A_4 is not simple since $\{\iota, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup. Can you see why the proof above will not work for A_4?

But the size of conjugacy classes divides $|G| = p^n$. So $|\mathrm{ccl}_G(x)| = p^a$ for some $0 \leq a \leq n$.

$$|G| = (\text{no. of conjugacy classes of size } 1) \cdot 1 + (\text{no. of conjugacy classes of size } p) \cdot p + \ldots$$

But p divides $|G|$. So p divides the number of conjugacy classes of size 1. But by Proposition 6.5.21 $\{x\}$ is a conjugacy class if and only if

$$\forall g \in G,\ gxg^{-1} = x \ \Leftrightarrow\ x \in Z(G) \tag{6.6.2}$$

So $p||Z|$. Thus $Z(G) \neq \{e\}$. □

Proposition 6.6.2. If $|G| = p^2$ for p prime then G is abelian.

Proof. Let G be a group of order p^2. In the action of G on itself by conjugation, one orbit is $\{e\}$ as the possible stabilizer order are $1, p, p^2$ (by Lagrange's theorem (Theorem 6.2.7)), the possible orbit sizes are $p^2, p, 1$. So all orbits have size 1 or p, and as the sume of the orbit sizes is $|G| = p^2$, there must be at least p orbits of size 1 (by considering the sum module p).

Now $\{z\}$ is an orbit of size 1 $\Leftrightarrow\ \forall g \in G, gzg^{-1} = z\ \Leftrightarrow\ \forall g \in G, gz = zg$. Write

$$Z(G) = \{z \in G : \forall g \in G, gz = zg\}, \tag{6.6.3}$$

so that $Z(G) \geq p$. If $|Z(G)| < p^2$, take $g \in G \backslash Z(G)$, then $\mathrm{Stab}(g)$ contains $Z(G)$ since

$$z \in Z(G)\ \Rightarrow\ zg = gz\ \Rightarrow\ zgz^{-1} = g \tag{6.6.4}$$

and also g itself since $ggg^{-1} = g$, so $\mathrm{Stab}(g) > p$ (as $g \notin Z(G)$ and $Z(G) \geq p$). As $\mathrm{Stab}\, g$ is a subgroup of G (Lemma 6.5.5) we must have $\mathrm{Stab}(g) = G$, whence the orbit containing g is of size 1, contrary to $g \in Z(G)$. Thus $|Z(G)| = p^2$ and so $Z(G) = G$. That is, for all $g, h \in G$, we have $gh = hg$, i.e., G is abelian. □

Remark. The abelian groups of order p^2 are isomorphic to C_{p^2} or $C_p \times C_p$.

Proposition 6.6.3. Suppose that G is a non-abelian group of order p^3 where p is prime.

(i) The order of the centre $Z(G)$ is p.

(ii) If $g \notin Z(G)$ then the order of the centralizer $C(g)$ is p^2.

(iii) There are p conjugacy classes with size 1 and $p^2 - 1$ conjugacy classes with size p.

Proof. (i) By Theorem 3.6.1., $Z(G)$ is non-trivial and $Z(G) \lhd G$. So $|Z(G)| = p$, p^2 or p^3.

If $|Z(G)| = p^3 = G$, by Proposition 3.5.15, G is abelian. Contradiction.

If $|Z(G)| = p^2$, $|G/Z(G)| = p$ and thus $G/Z(G)$ is cyclic, then by Lemma 3.5.16., G is abelian.

Thus $|Z(G)| = p$.

(ii) Suppose $g \notin Z(G)$. $C_G(g) = \left\{x \in G : xgx^{-1} = g\right\}$. Since $C_G(g) \leq G$, so $|C_G(g)| = 1$, p, p^2 or p^3.

$|C_G(g)|$ is not 1 since $Z(G) \subseteq C_G(g)$.

If $|C_G(g)| = p$, $C_G(g) = Z(G)$, but $g \in C_G(g)$ but $g \notin Z(G)$. Contradiction.

If $|C_G(g)| = p^3$, $C_G(g) = G$, $\forall x \in G$, $xg = gx$, so $g \in Z(G)$. Contradiction.

Thus, $|C_G(g)| = p^2$.

(iii) If $g \in Z(G)$, $\forall x \in G$, $xg = gx$, $C_G(g) = G$, so $|\mathrm{ccl}(g)| = 1$ and $\mathrm{ccl}\, g = \{g\}$. Furthermore, there are p conjugacy classes like this. (by (i)).

If $g \notin Z(G)$, $|\mathrm{ccl}(g)| = |G| / |C_G(g)| = p^3/p^2 = p$ by orbit-stablizer theorem. Thus, we there are $(p^3 - p)/p = p^2 - 1$ conjugacy classes with size p.

Thus, totoally we have $p^2 + p - 1$ conjugacy classes.

□

Theorem 6.6.4 (Cauchy's theorem)**.** If G is a finite group of order divisible by the prime p, then G contains an element of order p.

Proof. Let $X = \{(x_1, x_2, \ldots, x_p) | x_1 x_2 \ldots x_p = e\}$ with all $x_i \in G$. Let the cyclic group $C_p = \langle g | g^p = e \rangle$ act on the set X such that $g^j : (x_1, x_2, \ldots, x_p) \to (x_{1+j}, x_{2+j}, \ldots, x_j)$, so that g cycles the coordinates. (Note that we are working mod$p$.)

This is an action of C_p; the image is in X since if $x_1 x_2 \ldots x_p = e$, then $x_{1+j} x_{2+j} \ldots x_j = e$.

Now look at the orbits of this action. For arbitrary x_i, its orbit is

$$\left\{x_i, g(x_i), g^2(x_i), \ldots, g^{p-1}(x_i)\right\}. \tag{6.6.5}$$

If these elements are distinct, then this orbit has size p. Otherwise, if any of these elements are the same, we will have $g = e$, which gives that the orbit size 1. Thus, the orbits have sizes 1 or p.

Any orbit of size 1 is $\{(x, x, \ldots, x) | x^p = e\}$, e.g. $(e, e, \ldots, e)$. Finally, $|X| = |G|^{p-1}$, since the first $p-1$ coordinates can be chosen independently, but the last is forced; $x_p = (x_1 x_2 \ldots x_{p-1})^{-1}$. Therefore $p \,|\, |X|$. Since X is partitioned into C_p-orbits of sizes 1 or p, there are at least p of them of size 1.

Thus, we can pick a orbit of size 1, $\{(x, x, \ldots, x) | x^p = e\}$ where $x \neq e$ and by Lemma 6.2.10 we have $o(x) = p$[25]. □

Theorem 6.6.5. Let G be a p-group of order p^a. Then there is a subgroup of order p^b for any $0 \leq b \leq a$.

Proof. By induction on a. The result is clearly true for $a = 1$. Suppose it is true for $a - 1$.

Since $Z(G)$ is a subgroup of G (Lemma 6.5.9), we have $|Z(G)| \,|p^a$ (Theorem 6.2.7) and thus $p \,|\, |Z(G)|$. By Cauchy's theorem (Theorem 6.6.4), we have $x \in Z(G)$, an element of order p.

Hence let $K = \{e, x, \ldots, x^{p-1}\}$ be a subgroup of G, and it is normal in G since x is central.

Consider the quotient G/K. Its order is p^{a-1} and we can apply the inductive hypothesis to get a subgroup $L/K \leq G/K$ of order p^{b-1}. The correspondence between subgroups of G/K and subgroups of G containing K gives a subgroup L of G containing K of order p^b. □

6.6.2 Finite Abelian Groups

Theorem 6.6.6 (structure theorem for finite abelian groups)**.** Let G be a finite abelian group. Then

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k} \tag{6.6.6}$$

with $1 \neq d_i \mid d_{i+1}$ and $d_1 \ldots d_k = |G|$.

Proof. [26] □

Example 6.6.7. The abelian groups of order 8 are $C_2 \times C_4$, $C_2 \times C_2 \times C_2$ and C_8. The abelian groups of order 16 are $C_2 \times C_8$, $C_2 \times C_2 \times C_4$, $C_2 \times C_2 \times C_2 \times C_2$, $C_4 \times C_4$,and C_{16}.

Lemma 6.6.8. If m and n are coprime then $C_m \times C_n \cong C_{mn}$.

Proof. Take elements g of order m in C_m and h or order n in C_n.

Then (g, h) is of order mn in $C_m \times C_n$ since $(g, h)^r = (g^r, h^r)$ (by Definition 6.3.1) and so the order of (g, h) is the least common multiple of m and n which is mn since m and n are coprime.

But $|C_m \times C_n| = mn$ and so (g, h) is a generator for the group. □

Example 6.6.9. $C_2 \times C_3 \cong C_6$. Abelian groups of order $24 = 2^3 \times 3$ are $C_2 \times C_2 \times C_6$, $C_2 \times C_{12}$ and C_{24}.

6.7 Sylow's Theorems and Applications to Groups of Small Orders

6.7.1 Sylow's theorems

Theorem 6.7.1 (Sylow's theorem)**.** Let G be a finite group of order $p^a m$ where p is prime and $p \nmid m$.

(i) There exists a subgroup P of order p^a, called the Sylow p-subgroup.

(ii) All Sylow p-subgroups are conjugate.

(iii) The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 (\text{mod} p)$ and divides $|G|$, and hence $n_p | m$.

[25] another proof is on wiki

[26] Postponed until Ring & Modules

Proof of (i). Consider the set X of subsets of G of size p^a and let $\{g_1, \ldots, g_{p^a}\} \in X$. G acts on X via left multiplication,

$$g * \{g_1, \ldots, g_{p^a}\} = \{gg_1, \ldots, gg_{p^a}\}. \tag{6.7.1}$$

Consider an orbit $\Sigma \subseteq X$ (Σ is a subset of X). Take $g \in G$. If $\{g_1, \ldots, g_{p^a}\} \in X$ then

$$gg_1^{-1} * \{g_1, \ldots, g_{p^a}\} = \{g, gg_1^{-1}g_2, \ldots, gg_1^{-1}g_{p^a}\} \in \Sigma. \tag{6.7.2}$$

So g appears as an entry in one of the p^a-sets in orbit the Σ. Counting,

$$|\Sigma| \geq \frac{|G|}{p^a} = \frac{p^a m}{p^a} = m. \tag{6.7.3}$$

So we have two types of orbits Σ, (a) $|\Sigma| = m$, (b) $|\Sigma| > m$. By the orbit-stabiliser theorem (Theorem 6.5.6), $|\Sigma|$ divides $|G| = p^a m$. So for orbits Σ of type (b), where $|\Sigma| > m$, we deduce that $p||\Sigma|$.

The next step is to show that $|X|$ is not divisible by p,

$$|X| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a}\frac{p^a m - 1}{p^a - 1}\cdots\frac{p^a m - p^a + 1}{1}. \tag{6.7.4}$$

Consider $(p^a m - k)/(p^a - k)$ for $0 \leq k \leq p^a - 1$. If $k = 0$ then

$$\frac{p^a m - k}{p^a - k} = \frac{p^a m}{p^a} = m. \tag{6.7.5}$$

If $k > 0$ then set $k = p^b q$, where $p \nmid q$, so that

$$\frac{p^a m - k}{p^a - k} = \frac{p^a m - p^b q}{p^a - p^b q} = \frac{p^{a-b} m - q}{p^{a-b} - q}. \tag{6.7.6}$$

Note that $b < a$, so p does not divide the numerator after this cancellation process. Thus $p \nmid |X|$, as required.

Now count the elements of X,

$$|X| = \text{sum of sizes of orbits} = \text{sum of sizes of orbits of type (a)} + \text{sum of sizes of orbits of type (b)}.$$

But $p \nmid |\Omega|$ and p divides the size of orbits of type (b), thus we do have orbits of type (a).

Consider the orbit-stabiliser theorem (Theorem 6.5.6) for an orbit $\sum$ of type (a),

$$m = |\Sigma| = \frac{|G|}{|P|} = \frac{p^a m}{|P|} \tag{6.7.7}$$

where P is the stabiliser of an element x chosen in Σ. So $|P| = p^a$ and thus there is a subgroup of order p^a. □

Proof of (ii). In fact, we will prove the following. If P is a Sylow p-subgroup and $Q \leq G$ with $|Q| = p^b$ for $1 \leq b \leq a$, then there exists $g_1 \in G$ such that $Q \leq g_1 P g_1^{-1}$. In particular, if Q is of order p^a then $Q = g_1 P g_1^{-1}$.

This time consider the action of Q on the set H of left cosets of P via left multiplication,

$$g * g_1 P = gg_1 P \;\Leftrightarrow\; g * h = gh, \quad h \in H = \{gP : g \in G\}, g \in Q, g_1 \in G. \tag{6.7.8}$$

We consider the orbits of Q. By the orbit-stabiliser theorem (Theorem 6.5.6), the size of an orbit divides $|Q|$, thus is either 1 or a power of p ($|Q(gP)| = p^k$, $0 \leq k \leq a$). The number of cosets of P is equal to the index of P in G, (Lagrange theorem, Theorem 6.2.7)

$$|H| = \frac{|G|}{|P|} = \frac{p^a m}{p^a} = m. \tag{6.7.9}$$

In particular, m is equal to the number of orbits of size 1 plus p^k times the number of orbits of size k.

$$\begin{aligned} m &= |H| = (\text{no. of orbits of size 1}) \cdot 1 + (\text{no. of conjugacy classes of size } p) \cdot p + \dots \\ &= \sum_{k=0}^{a} (\text{no. of orbits of size } p^k) \cdot p^k. \end{aligned}$$

Counting cosets, we see that we must have an orbit of size 1 since $p \nmid m$. Suppose $\{g_1 P\}$ is such an orbit. Thus $gg_1P = g_1P$ for all $g \in Q$ and hence $g_1^{-1}gg_1P = P$. So $g_1^{-1}gg_1 \in P$ and $g \in g_1Pg_1^{-1}$. Thus $Q \leq g_1Pg_1^{-1}$, as required. □

Definition 6.7.1 (normaliser)**.** G acts on the set X of Sylow p-subgroups via conjugation, $g * P = gPg^{-1}$, $P \in X$. The stabiliser, called the normaliser of P, is $N_G(P) = \{g \in G : gPg^{-1} = P\}$.

Remark. Note that P might not be Sylow p-subgroups in G. For instance, P is Sylow p-subgroup in H and $H \leq G$.

Lemma 6.7.2. If $n_p = 1$, then the unique Sylow p-subgroup P is normal in G.

Also, P is the unique Sylow p-subgroup of $N_G(P)$.

Proof. Take the unique Sylow p-subgroup P. Then gPg^{-1} is also a Sylow p-subgroup. Thus $gPg^{-1} = P$ for all $g \in G$.

By Definition 6.7.1, $P \subseteq N_G(P)$ and P is a subgroup of G, so $P \lhd N_G(P)$.

$N_G(P) \leq G$ by Lemma 6.5.5, so $N_G(P)$ is of order of $p^a n$, $p \nmid n$ as P is the subgroup of $N_G(P)$. So applying Sylow's second theorem to $N_G(P)$, we see that P is the Sylow p-subgroup and all Sylow p-subgroups of $N_G(P)$ are conjugate to P. But $P \lhd N_G(P)$ and so all its conjugates are P itself. Thus P is the unique Sylow p-subgroup of $N_G(P)$. □

Proof of (iii). By (ii), all Sylow p-subgroups are conjugate and there is exactly one orbit which contains all the Sylow p-subgroups. From (ii), we know all Sylow p-subgroups are in the orbit. Let $P = \{h_1, h_2, \dots, h_{p^a}\}$. If Q in the orbit is not Sylow p-subgroup then its order is less than p^a, that is for some $g \in G$, $1 \leq i, j \leq p^a$, $i \neq j$, we have

$$gh_ig^{-1} = gh_jg^{-1} \;\Rightarrow\; h_i = h_j \;\Rightarrow\; |P| < p^a \tag{6.7.10}$$

So we know all the element in this orbit are Sylow p-subgroup. By the orbit-stabiliser theorem (Theorem 6.5.6), the size of the orbit is n_p (also known as the number of Sylow p-subgroups) and $n_p || G|$.

Consider the action of P on the set X of Sylow p-subgroups of G via conjugation, $g * P_i = gP_ig^{-1}$, $g \in P$ where $X = \{P_1, P_2, \dots\}$. By the orbit-stabiliser theorem (Theorem 6.5.6), orbits of P are of size 1 or of size divisible by p. We need to show that there is exactly one orbit of size 1.

Visibly $\{P\} = \{e * P\}$ ($e \in P$) is an orbit of size 1. Are there any others?

Suppose $\{Q\}$ is an orbit of size 1. Thus $gQg^{-1} = Q$ for all $g \in G$ and of course for all $g \in P$ and so $P \subseteq N_G(Q)$ and thus $P \leq N_G(Q)$. From Lemma 6.7.2, Q is the unique Sylow p-subgroup of $N_G(Q)$, so $P = Q$, since both are Sylow subgroups of $N_G(Q)$. Thus $\{P\}$ is the only orbit of size 1. Counting Sylow p-subgroups in G,

$$n_p = 1 + \text{ sum of sizes of other orbits (divisible by } p). \tag{6.7.11}$$

But p divides the size of every other orbit. Therefore, $n_p \equiv 1 (\mathrm{mod} p)$ and $n_p \mid m$. □

Corollary 6.7.3. Let n_p be number of p-subgroups and $N_G(P)$ be a normaliser of $P \in X$ where X is the set of p-subgroups. Then

$$|G| = n_p \, |N_G(P)| \,. \tag{6.7.12}$$

Proof. This is the direct result from orbit-stabiliser theorem (Theorem 6.5.6) and Sylow theorem (Theorem 6.7.1.(ii)) since all p-subgroups are conjugate. □

Corollary 6.7.4. Let G be a non-abelian simple group. Then $|G|$ divides $n_p!/2$, and $n_p \geq 5$ once we have shown that all non-abelian subgroups of S_4 are not simple.

Proof. [27] □

[27] need to check: G is acting on the set X of Sylow p-subgroups where $|X| = n_p$. If G is non-abelian simple then by Theorem 6.2.7 G is isomorphic to a subgroup of A_{n_p}, and $n_p \geq 5$ subject to proviso.

6.7.2 Applications to groups of small orders

Example 6.7.5. Let $|G| = 1000 = 2^3 5^3$. Then G is not simple.

Proof. $n_5 \equiv 1 (\mathrm{mod}\, 5)$ and $n_5 \mid 8$. So $n_5 = 1$ and so there exists a unique Sylow 5-subgroup which is normal (by Lemma 6.7.2). Thus G is not simple. □

Example 6.7.6. Let $|G| = 300 = 2^2 \cdot 3 \cdot 5^2$. Then G is not simple.

Proof. $n_5 \equiv 1 (\mathrm{mod}\, 5)$ and $n_5 \mid 12$. Assume G is simple and so $n_5 \neq 1$ (by Lemma 6.7.2). Then $n_5 = 6$. But 300 does not divide 6!/2 by Corollary 6.7.4. Contradiction! Thus $|G| = 300$ implies that $n_5 = 1$. (G is not abelian simple since it is not of prime order.) □

Example 6.7.7. Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Then G is not simple.

Proof. $n_{11} \equiv 1 (\mathrm{mod}\ 11)$ and $n_{11} | 12$. Assume G is simple and so $n_{11} \neq 1$ (by Lemma 6.7.2). Then $n_{11} = 12$. $n_3 \equiv 1 \pmod 3$ and $n_3 | 44$. By simplicity, $n_3 \neq 1$ and $n_3 \neq 4$ by Corollary 6.7.4 ($132 \nmid 4!$), so $n_3 = 22$.

But since $n_{11} = 12$ and $n_3 = 22$ there are $12 \cdot (11 - 1)$ elements of order 11 and $22 \cdot (3 - 1)$ elements of order 3. But this gives too many elements, a contradiction! □

Remark. This is a typical argument. We use Sylow's theorem to estimate the number of subgroups and then count elements.

Lemma 6.7.8. Suppose $|G| = 2p$ for an odd prime p. Then $G \cong C_{2p}$ or D_{2p}.

Proof. $n_p \equiv 1 (\mathrm{mod}\, p)$ and $n_p | 2$, so $n_p = 1$. Thus there is a normal subgroup K of order p by Lemma 6.7.2. Since K is of order p, the supgroup size is either 1 or p, so K is simple. Since K is simple and abelian, we have K is C_p by Proposition 6.4.15. Sylow's theorem also implies there is a subgroup H of order 2. Let $H = \{e, g\}$, $K = \{e, x, \ldots, x^{p-1}\}$.

Now consider the action of H on K by conjugation. In particular, consider conjugation by g – it permutes the elements of K. (In fact, conjugation by g gives an automorphism of K.) This is uniquely determined by the image of x, that is, $gxg^{-1} = x^r$ for some r, $1 \leq r \leq p$. Then also

$$x = exe = g^2 x g^{-2} = g x^r g^{-1} = (gxg^{-1})^r = x^{r^2}. \tag{6.7.13}$$

So $r^2 \equiv 1 (\mathrm{mod}\, p)$ by Lemma 6.2.10. This gives two choices. Suppose $r \equiv 1 (\mathrm{mod} p)$, then g and x commute so gx is of order $2p$ (as $g \neq x^a$, $1 \leq a \leq p-1$) and hence $G \cong C_{2p}$. Otherwise suppose $r \equiv -1 (\mathrm{mod}\, p)$, then $gxg^{-1} = x^{-1} = x^{p-1}$ and $G \cong D_{2p}$ by Theorem 6.1.15. In the latter case, x is a rotation and g is a reflection. □

Example 6.7.9. There is a problem on the examples sheet for the case $|G| = 15$.[28]

Recall the definition of a soluble group (Definition 6.4.3), a group for which the composition factors can be chosen to be abelian simple.

Theorem 6.7.10 (1904, Burnside)**.** If $|G| = p^a q^b$, where p and q are primes, then G is soluble.

Proof. [29] □

Theorem 6.7.11 (1937, Hall)**.** G is soluble if and only if whenever $|G|$ factorises as $|G| = mn$ with m and n coprime there is a subgroup of order m.

Proof. [30] □

Theorem 6.7.12 (1963, Feit, Thompson, "Odd Order Theorem")**.** If $|G|$ is odd then G is soluble.

Proof. [31] □

order	groups (up to isomorphism)	number of these
1	$\{e\}$	1
2	C_2	1
3	C_3	1
4	C_4, $C_2 \times C_2$ (see Lemma 6.3.7)	2
5	C_5	1
6	C_6, D_6 (see Lemma 6.3.8)	2
7	C_7	1
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, Q_8 (see Lemma 6.3.9)	5
9	C_9, $C_3 \times C_3$ (method similar to Lemma 6.3.7)	2
10	C_{10}, D_{10} (see Lemma 6.3.10)	2

Table 6.1: small groups

6.8 Summary

6.8.1 List of small groups

6.9 Problems

6.9.1 Groups, subgroups, orders and homomorphism

Problem 6.9.1. Let G be any group. Show that the identity e is the unique solution of the equation $x^2 = x$.

Solution. As $e^2 = e$, certainly e is a solution. For uniqueness,

$$g^2 = g \;\Rightarrow\; g^{-1}g^2 = g^{-1}g \;\Rightarrow\; g = e, \tag{6.9.1}$$

so e is the unique solution.

Problem 6.9.2. Show that S, the set of functions on $\mathbb{R}$ of the form $f(x) = ax + b$, where a and b are real numbers and $a \neq 0$, forms a group under composition of functions. Is this group abelian?

Solution. Obviously, $e(x) = x$ is the identity. If $f_1(x) = a_1x + b_1, f_2(x) = a_2x + b_2, f_3(x) = a_3x + b_3 \in S$ with $a_1, a_2, a_3 \neq 0$, then

$$f_1 \circ f_2(x) = a_1(a_2x + b_2) + b_1 = a_1a_2x + a_1b_2 + b_2 = (a_1a_2)x + (a_1b_2 + b_1) \in S. \tag{6.9.2}$$

Also, associativity is given by

$$\begin{aligned}(f_1 \circ f_2) \circ f_3(x) &= (f_1 \circ f_2)(a_3x + b_3) = (a_1a_2)(a_3x + b_3) + (a_1b_2 + b_1)\\ &= a_1a_2a_3x + a_1a_2b3 + a_1b_2 + b_1 = a_1(a_2a_3x + a_2b3 + b_2) + b_1\\ &= f_1(a_2a_3x + a_2b3 + b_2) = f_1 \circ (a_2(a_3x + b_3) + b_2) = f_1 \circ (f_2(a_3x + b_3)) = f_1 \circ (f_2 \circ f_3(x)).\end{aligned}$$

Let $g_1 = (x - b_1)/a_1$. Then

$$f_1 \circ (g_1(x)) = a_1\left(\frac{x - b_1}{a_1}\right) + b_1 = x - b_1 + b_1 = x = e(x) \quad \text{and} \quad g_1 \circ (f_1(x)) = (a_1x + b_1 - b_1)/a_1 = x = e(x). \tag{6.9.3}$$

Thus, S is a group under composition.
However, S is not abelian since

$$f_1 \circ f_2(x) = a_2(a_1x + b_1) + b_2 = a_1a_2x + a_2b_1 + b_2 \neq a_1a_2x + a_1b_2 + b_1 = a_1(a_2x + b_2) + b_1 = f_1 \circ f_2(x). \tag{6.9.4}$$

Problem 6.9.3. Let $G = \{x \in \mathbb{R} : x \neq -1\}$, and let $x * y = x + y + xy$, where xy denotes the usual product of two real numbers. Show that $(G, *)$ is a group. What is the inverse 2^{-1} of 2 in this group? Solve the equation $2 * x * 5 = 6$.

[28] need to check
[29] proof needed
[30] proof needed
[31] proof needed

Solution. $\forall x, y \in G$, then $x, y \neq 1$ so $x+1, y+1 \neq 0$. Thus, $(x+1)(y+1) \neq 0 \Rightarrow xy+x+y \neq -1$. Then $x * y \in G$, so $*$ is a binary operation on G. Given $x, y, z \in G$, we have

$$(x*y)*z = (xy+x+y)*z = (xy+x+y)z + (xy+x+y) + z = x(yz+y+z) + (yz+y+z) + x = x*(y*z). \quad (6.9.5)$$

So $*$ is associative. For $x \in G$, we have

$$x*0 = x0 + x + 0 = x = 0x + 0 + x = 0*x \Rightarrow 0 \text{ is an identity.} \quad (6.9.6)$$

Given $x \in G$, we have

$$x*y = 0 \Rightarrow xy+x+y = 0 \Rightarrow y = -\frac{x}{x+1}, \quad y*x = \left(-\frac{x}{x+1}\right)*x = -\frac{x^2}{x+1} - \frac{x}{x+1} + x = 0. \quad (6.9.7)$$

It follows that $-\frac{x}{x+1}$ is an inverse for x. Thus $(G, *)$ is a group. Then

$$2^{-1} = -\frac{2}{2+1} = -\frac{2}{3}, \quad 5^{-1} = -\frac{5}{5+1} = -\frac{5}{6}, \quad (6.9.8)$$

Thus, $2*x*5 = 6 \Rightarrow 2^{-1}*2*x*5*5^{-1} = 2^{-1}*6*5^{-1}$

$$x = \left(-\frac{2}{3}\right)*6*\left(-\frac{5}{6}\right) = (-4-\frac{2}{3}+6)*\left(-\frac{5}{6}\right) = \frac{4}{3}*\left(-\frac{5}{6}\right) = -\frac{10}{9}+\frac{4}{3}-\frac{5}{6} = -\frac{11}{18}. \quad (6.9.9)$$

Problem 6.9.4. Let G be a group in which every element other than the identity has order two. Show that G is abelian. Show also that if G is finite, the order of G is a power of 2. (Consider a minimal generating set.)

Solution. Take $x, y \in G$, then xy is either e or an element of order two, so $(xy)^2 = e$, that is

$$xyxy = e \Rightarrow yx = x^{-1}y^{-1}. \quad (6.9.10)$$

But $x^2 = e, y^2 = e \Rightarrow x = x^{-1}, y = y^{-1}$, we have $yx = xy$. As this is true $\forall x, y \in G$, G is abelian.

If G is finite, we can pick $g_1 \in G$ such that $\langle e, g_1\rangle$ is a subgroup of G with order 2. Then for any $g_2 \in G \backslash \langle e, g_1\rangle$, we have $\langle e, g_1, g_2\rangle$ is a subgroup of G with order 4. Repeating the process, we can choose g_i such that $\langle e, g_1, \ldots, g_i\rangle$ is a subgroup of G with order 2^i. Since G is finite, we can have that order of G is a power of 2.

Problem 6.9.5. Show that the set G of complex numbers of the form $\exp(i\pi t)$ with t rational is a group under multiplication (with identity 1). Show that G is infinite, but that every element g of G has finite order.

Solution. For any $t \in \mathbb{Q}$, we can find $a, b \in \mathbb{Z}$ with $a \neq 0$. Thus, for any $t_1, t_2, t_3 \in \mathbb{Q}$, we have

$$\exp(i\pi t_1)\exp(i\pi t_2) = \exp(i\pi(t_1+t_2)) = \exp\left(i\pi\frac{a_1b_2+a_2b_1}{a_1a_2}\right) \in G. \quad (6.9.11)$$

Also, it is obvious that

$$(\exp(i\pi t_1)\exp(i\pi t_2))\exp(i\pi t_3) = \exp(i\pi(t_1+t_2+t_3)) = \exp(i\pi t_1)(\exp(i\pi t_2)\exp(i\pi t_3)). \quad (6.9.12)$$

Obviously, 1 ($t = 0$) is the identity. Finally, let $t_1' = -t_1$, we have

$$\exp(i\pi t_1)\exp(i\pi t_1') = 1 = \exp(i\pi t_1')\exp(i\pi t_1). \quad (6.9.13)$$

Thus, $\exp(i\pi t_1')$ is the inverse of $\exp(i\pi t_1)$. Hence, G is a group under multiplication.

Problem 6.9.6. Let S be a finite non-empty set of non-zero complex numbers which is closed under multiplication. Show that S is a subset of the set $\{z \in \mathbb{C} : |z| = 1\}$. Show that S is a group, and deduce that for some $n \in \mathbb{N}$, S is the set of nth roots of unity; that is, $S = \{\exp(2k\pi i/n) : k = 0, \ldots, n-1\}$.

Solution. Given S, by Proposition 6.2.9, $\exists n \in \mathbb{N}$ such that $\forall g \in S$, we have $g^n = 1$. Take $g \in S$ and write $g = e^{i\theta}$, then $e^{in\theta} = 1$. So $n\theta = 2\pi k$ for some $k \in \mathbb{Z}$. Thus $g = e^{2\pi ki/n}$.

Take $k > 0$ minimal such that $e^{2\pi ki/n} \in S$, by taking powers we have

$$\left\{e^{2\pi mki/n} : m \in \mathbb{Z}\right\} \subseteq S \tag{6.9.14}$$

by definition of group. Now given $e^{2\pi li/n} \in S$, wirte $l = qk + r$ with $q \in \mathbb{Z}$ and $0 \leq r < k$; then S contains

$$\underbrace{e^{2\pi li/n}}_{\in S}\underbrace{e^{2\pi(-q)ki/n}}_{\in S} = e^{2\pi ri/n}. \tag{6.9.15}$$

By minimality of k we must have $r = 0$ and $l = qk$. Thus, we have

$$S \subseteq \left\{e^{2\pi mki/n} : m \in \mathbb{Z}\right\} \;\Rightarrow\; S = \left\{e^{2\pi mki/n} : m \in \mathbb{Z}\right\}. \tag{6.9.16}$$

Since $e^{2\pi ni/n} = 1 \in S$, we see that $n = qk$ for some q, and so

$$S = \left\{e^{2\pi mi/q} : m \in \mathbb{Z}\right\} \quad \text{i.e., } S \text{ is the group of } q\text{th roots of unity.} \tag{6.9.17}$$

Problem 6.9.7. Write the following permutations as products of disjoint cycles and compute their order and sign:

(a) (12)(1234)(12);

(b) (123)(45)(16789)(15).

Solution. (a) (12)(1234)(12) = (1342) - order = 4, sign = $(-1)^3$ = -1.

(b) (123)(45)(16789)(15) = (145678923) - order = 9, sign = $(-1)^8 = 1$.

Problem 6.9.8. Let C_n be the cyclic group with n elements and D_{2n} the group of symmetries of the regular n-gon. If n is odd and $\theta : D_{2n} \to C_n$ is a homomorphism, show that $\theta(g) = e$ for all $g \in D_{2n}$. What can you say if n is even?

Solution. If n is odd, then only element if C_n satisfying $x^2 = e$ is e itself, because if g is a generator of C_n then $x = g^r$ for some r and

$$(g^r)^2 = e \;\Leftrightarrow\; g^{2r} = e \;\Leftrightarrow\; \underbrace{n|2r \;\Leftrightarrow\; n|r}_{\text{since } n \text{ is odd}} \;\Leftrightarrow\; e = g^r = x. \tag{6.9.18}$$

Now if $x \in D_{2n}$ is a reflection, then $x^2 = e$, thus $\theta(x^2) = \theta(e) = e$, so $\theta(x)^2 = e \;\Rightarrow\; \theta(x) = e$ by the previous result.

If $a \in D_{2n}$ is a rotation, then for any reflection $x \in D_{2n}$, ax is a reflection. Thus, $\theta(ax) = e$, i.e., $e = \theta(a)\theta(x) = e\theta(x) = \theta(x)$. So for all $g \in D_{2n}$, we have $\theta(g) = e$.

If instead n is even, let g be a generator of C_n, then $\left(g^{\frac{n}{2}}\right)^2 = g^n = e$. Write $z = g^{\frac{n}{2}}$, then $\{e, z\}$ is a subgroup of C_n. By the argument above, if $x \in D_{2n}$ is a reflection then $\theta(x) \in \{e, z\}$ and thus if $a \in D_{2n}$ is rotation then $\theta(a) \in \{e, z\}$ as well.

Thus if we let a be a rotation clockwise by $\frac{2\pi}{n}$ and b be any given reflection, then a and b generate D_{2n} and so θ is determined by its effect on a and b. Hence there exist 4 possible homomorphisms.

Problem 6.9.9. Show that if a group G contains an element of order six, and an element of order ten, then G has order at least 30.

Solution. If $g, h \in G$ with $o(g) = 6$ and $o(h) = 10$ then $\langle g\rangle$ and $\langle h\rangle$ are subgroups of G of order 6 and 10. So by Lagrange's theorem $6 \mid |G|$ and $10 \mid |G|$, and thus $30 \mid |G|$ so $|G| \geq 30$.

6.9.2 Normal groups and isomorphism theorems

Problem 6.9.10. (i) What are the orders of elements of the group S_4? How many elements are there of each order?

(ii) How many subgroups of order 2 are there in S_4? Of order 3? How many cyclic subgroups are there of order 4?

(iii) Find a non-cyclic subgroup V of S_4 of order 4. How many of these are there?

(iv) Find a subgroup D of S_4 of order 8. How many of these are there?

Solution. (i) For S_4,

cycle type	example member	order	number
1^4	ι	1	1
2^2	(1 2)(3 4)	2	3
3,1	(1 2 3)	3	8
$2,1^2$	(1 2)	2	6
4	(1 2 3 4)	4	6

(ii) Subgroups of order 2: $\{\iota, (1\ 2)(3\ 4)\}$, $\{\iota, (1\ 3)(2\ 4)\}$, $\{\iota, (1\ 4)(2\ 3)\}$,

$$\{\iota, (1\ 2)\}, \quad \{\iota, (1\ 3)\}, \quad \{\iota, (1\ 4)\}, \quad \{\iota, (2\ 3)\}, \quad \{\iota, (2\ 4)\}, \quad \{\iota, (3\ 4)\} \tag{6.9.19}$$

Thus, totally $6 + 3 = 9$.

Subgroups of order 3:

$$\{\iota, (1\ 2\ 3), (1\ 3\ 2)\}, \quad \{\iota, (1\ 3\ 4), (1\ 4\ 3)\}, \quad \{\iota, (1\ 4\ 2), (1\ 2\ 4)\}, \quad \{\iota, (2\ 3\ 4), (2\ 4\ 3)\} \tag{6.9.20}$$

Thus, totally 4.

Subgroups of order 4:

$$\{\iota, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}, \quad \{\iota, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}, \quad \{\iota, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}. \tag{6.9.21}$$

Thus, totally 3.

(iii) $\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

(iv) Since $|D| = 8$, D does not contain elements of order 3 (Lagrange's corollary (Corollary 6.2.11)). Thus, D has to contain elements of order 2 and 4. If all the non-identiy elements are of order 2, we have we must pick at least 4 element from type (1 2), but they are not disjoint. Thus this will generate some element of the form (123), so there must be some element of order 4. The elements $a = (1\ 2\ 3\ 4)$, easliy we can find another two elements $(1\ 3)(2\ 4) = a^2$ and $(1\ 4\ 3\ 2) = a^3$. There cannot be any other element of order 4, otherwise there will be some element of order 3. For instance,

$$(1\ 2\ 3\ 4)(1\ 4\ 2\ 3) = (2\ 4\ 3). \tag{6.9.22}$$

Thus, we have the other four elements are of order 2. They cannot be of the form (1 2) since

$$(1\ 2)\,((13)(24)) = (1324) \tag{6.9.23}$$

which is an element of order 4. Thus, they have to be (1 3), so the subgroup is

$$\{\iota, (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3)(2\ 4), (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}. \tag{6.9.24}$$

There are 3 of this type. So there are 3 subgroups.

(Alternative way to approach might be discussing C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 and Q_8).

Problem 6.9.11. (i) Show that A_4 has no subgroups of index 2. Exhibit a subgroup of index 3.

(ii) Show that A_5 has no subgroups of index 2, 3 or 4. Exhibit a subgroup of index 5.

(iii) Show that A_5 is generated by (12)(34) and (135). (Multiply the two elements to show that the subgroup they generate has order 30 or 60.)

Solution. (i) $|A_4| = 4!/2 = 12$,

$$A_4 = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\} \tag{6.9.25}$$

If H is subgroup of index 2, we have $|H| = 6$ by Lagrange's theorem (Theorem 6.2.7). Thus from Corollary 6.2.11, it has an element of order 2, and an element of order 3. By Lemma 6.3.8 we know that $H \cong C_6$ or D_6. C_6 is impossible since

there must be an element of order 6. Thus, we must have $D_6 = \langle a, b : a^3 = b^2 = e, aba = b^{-1} \rangle$. Suppose $b = (1\ 2)(3\ 4)$, we have $(ab)^2 = e$, but such a does not exist.

A subgroup of index 3 will be of order 4, thus we can have

$$\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \tag{6.9.26}$$

(ii) Let $H \leq A_5$ with order of n. Let A_5 act on the left cosets of H, say $\Omega = \{gH : g \in A_5\}$.

Let $\varphi : A_5 \to \mathrm{Sym}(\Omega) = S_n, f \mapsto \varphi_f$ where $\varphi_f : \Omega \to \Omega$. Thus, $\ker\varphi \lhd A_5$, but A_5 is simple, so $\ker\varphi = \{e\}$. Also, $A_5/\ker\varphi \cong \mathrm{Im}\,\varphi \leq S_n$, so $|A_5/\ker\varphi| \mid |S_n|$ by Lagrange Theorem (Theorem 6.2.7). Since $\ker\varphi = \{e\}$, we have

$$|A_5| \mid |S_n| \ \Rightarrow\ n \neq 2, 3, 4. \tag{6.9.27}$$

Thus, we can find a subgroup $H = A_4$ of index 5.

(iii) For the subgroup $H = \langle (1\ 2)(3\ 4), (1\ 3\ 5) \rangle$, we have $H \leq A_5$, $|H| \mid 60$. Since $(1\ 2)(3\ 4)$ has order 2 and $(1\ 3\ 5)$ has order 3, we have

$$2 \mid |H|,\ 3 \mid |H| \ \Rightarrow\ 6 \mid |H|. \tag{6.9.28}$$

Also, $((1\ 2)(3\ 4))(1\ 3\ 5) = (1\ 4\ 3\ 5\ 2)$ has order 5, so we have $5 \mid |H|$ and $30 \mid |H|$. If $|H| = 30$, it has index 2, thus H is normal (by Lemma 6.4.4). But H is not normal since A_5 is simple. Thus, $|H| = 60$. So (12)(34) and (135) generate A_5.

Problem 6.9.12. Calculate the size of the conjugacy class of $(1\ 2\ 3)$ as an element of S_4, as an element of S_5 and as an element of S_6. Find in each case the centralizer. Hence calculate the size of the conjugacy class of (123) as an element of A_4, as an element of A_5 and as an element of A_6.

Solution. By Theorem 6.5.24, the permutations of S_n are conjugate iff they have the same cycle-type. Thus,

$$\begin{aligned} |\mathrm{ccl}_{S_4}(1\ 2\ 3)| &= C_3^4 P_1^2 = 8, \\ |\mathrm{ccl}_{S_5}(1\ 2\ 3)| &= C_3^5 P_1^2 = 20, \\ |\mathrm{ccl}_{S_6}(1\ 2\ 3)| &= C_3^6 P_1^2 = 40. \end{aligned}$$

The centralizers are

$$C_{S_4}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle \tag{6.9.29}$$

since $(1\ 2\ 3)$ is order $3 = 24/8$,

$$C_{S_4}((1\ 2\ 3)) = \langle (1\ 2\ 3), (4\ 5) \rangle \tag{6.9.30}$$

since $(1\ 2\ 3)$ is of order 3 and $(4\ 5)$ is of order 2, $3{\times}2 = 6 = 120/20$,

$$C_{S_4}((1\ 2\ 3)) = \langle (1\ 2\ 3), (4\ 5\ 6), (4\ 5) \rangle \tag{6.9.31}$$

since $(1\ 2\ 3)$ and $(4\ 5\ 6)$ are of order 3 and $(4\ 5)$ is of order 3, $3{\times}3{\times}2 = 18 = 720/40$.

For alternative group A_n, we have all permutations in S_4 that commute with $(1\ 2\ 3)$ are even (since the centralizer is generated by $(1\ 2\ 3)$), by Theorem 6.5.34,

$$|\mathrm{ccl}_{A_4}(1\ 2\ 3)| = |\mathrm{ccl}_{S_4}(1\ 2\ 3)|/2 = 4. \tag{6.9.32}$$

Also, there are odd permutation $(4\ 5)$ commute with $(1\ 2\ 3)$ for both S_5 and S_6, we have

$$\begin{aligned} |\mathrm{ccl}_{A_5}(1\ 2\ 3)| &= |\mathrm{ccl}_{S_5}(1\ 2\ 3)| = 20, \\ |\mathrm{ccl}_{A_6}(1\ 2\ 3)| &= |\mathrm{ccl}_{S_6}(1\ 2\ 3)| = 40. \end{aligned}$$

Problem 6.9.13. Suppose that $H, K \lhd G$ with $H \cap K = \{e\}$. Consider the commutator $[h, k] = hkh^{-1}k^{-1}$ with $h \in H$ and $k \in K$, and prove that any element of H commutes with any element of K. Hence show that $HK \cong H \times K$.

Solution. Since $K, H \lhd G$, we have $\forall h \in H, k \in K$, $hkh^{-1} \in K$ and $kh^{-1}k^{-1} \in H$. Thus,

$$hkh^{-1}k^{-1} \in K, \quad hkh^{-1}k^{-1} \in H \;\Rightarrow\; hkh^{-1}k^{-1} \in H \cap K = e \;\Rightarrow\; hk = kh. \tag{6.9.33}$$

Now define $\theta : HK \to H \times K, hk \mapsto (h, k)$. First we should prove θ is well-defined.

If $h_1k_1 = h_2k_2$, we have

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K \;\Rightarrow\; h_2^{-1}h_1 = k_2k_1^{-1} = e \;\Rightarrow\; h_1 = h_2,\ k_1 = k_2 \;\Rightarrow\; \theta(h_1k_1) = (h_1, k_1) = (h_2, k_2) = \theta(h_2k_2). \tag{6.9.34}$$

Now θ is a homomorphism:

$$\theta((h_1k_1)(h_2k_2)) = \theta(h_1k_1h_2k_2) = \theta(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \theta(h_1k_1)\theta(h_2k_2). \tag{6.9.35}$$

It is injective since

$$(h_1, k_1) = (h_2, k_2) \;\Rightarrow\; h_1 = h_2, k_1 = k_2 \;\Rightarrow\; h_1k_1 = h_2k_2. \tag{6.9.36}$$

It is surjective since for all $(h, k) \in HK$ there exists $hk \in HK$. Thus θ is isomorphism and $HK \cong H \times K$. (It might be easier if we consider $\theta : H \times K \to HK$).

Problem 6.9.14. Let $\theta : G \to H$ be a homomorphism between finite groups. Given $g \in G$, show that the order of $\theta(g)$ must divide the order of g. Describe all the homomorphisms from C_n to C_m, in particular, what happens if n and m are coprime?

Solution. Let r be the order of g. Then $\theta(g)^r = \theta(g^r) = \theta(e_G) = e_H$ by definition of homomorphism. So the order of $\theta(g)$ must divides r.

Write

$$C_n = \left\{e_G, g, \ldots, g^{n-1}\right\}, \quad C_m = \left\{e_H, h, \ldots, h^{m-1}\right\}. \tag{6.9.37}$$

Given a homomorphism $\theta : C_n \to C_m$ write $\theta(g) = h^k$ with $0 \le k \le m-1$, then we must have

$$h^{kn} = \left(h^k\right)^n = (\theta(g))^n = \theta(g^n) = \theta(e_G) = e_H \;\Rightarrow\; m | nk \tag{6.9.38}$$

by Lemma 6.2.10. Let $c = \mathrm{hcf}(m, n)$, then $\frac{m}{c} \big| \frac{n}{c}k$, so $\frac{m}{c} \big| k$. Thus, $k = a\frac{m}{c}$ for some $0 \le a \le c-1$ (since $k \le m-1$), and then

$$\theta(g^t) = h^{\frac{atm}{c}}. \tag{6.9.39}$$

In particular, if m and n are coprime then $c = 1$, we must have $a = 0$, so the only homorphism $\theta : C_n \to C_m$ is the map θ satisfying $\theta(g^t) = e$ for all t.

6.9.3 Group actions

Problem 6.9.15. Suppose that the group G acts on the set X. Let $x \in X$, let $y = g(x)$ for some $g \in G$. Show that the stabiliser G_y equals the conjugate gG_xg^{-1} of the stabiliser G_x.

Solution. If $\forall h \in G_x$, then

$$ghg^{-1} \cdot y = ghg^{-1} \cdot gx = ghx = gx = y \;\Rightarrow\; ghg^{-1} \in G_y \;\Rightarrow\; gG_xg^{-1} \subseteq G_y. \tag{6.9.40}$$

Simiarly, as $x = g^{-1}y$ we have $g^{-1}G_yg \subseteq G_x$, i.e. $G_y = gG_xg^{-1}$. Thus $gG_xg^{-1} = G_y$.

6.9.4 Sylow's theorem

Problem 6.9.16. (i) In Problem 6.9.10 we found the number of Sylow 2-subgroups and Sylow 3-subgroups of S_4. Check that your answer is consistent with Sylow's theorem (Theorem 6.7.1). (Note that if you did not then quite complete proofs for subgroups of order 8, you can do so now.) Identify the normalizers of the Sylow 2-subgroups and Sylow 3-subgroups.

(ii) For $p = 2, 3, 5$ find a Sylow p-subgroup of A_5 and find the normalizer of the subgroup.

Solution. (i) $|S_4| = 4! = 24 = 2^3 \cdot 3$.

Let $p = 3$. Thus, there exist 4 subgroups of order 3 ($4 \equiv 1 \pmod p$) by Lagrange theorem (Theorem 6.2.7),

$$\langle (1\ 2\ 3) \rangle\,,\ \langle (1\ 2\ 4) \rangle\,,\ \langle (1\ 3\ 4) \rangle\,,\ \langle (2\ 3\ 4) \rangle\,, \tag{6.9.41}$$

We know that

$$(3\ 4)\,\{\iota, (1\ 2\ 3), (1\ 3\ 2)\}\,(3\ 4)^{-1} = \{\iota, (1\ 2\ 4), (1\ 4\ 2)\}\,. \tag{6.9.42}$$

Thus, the subgroups are conjugate. So the case $p = 3$ is consistent with Sylow's theorem (Theorem 6.7.1). The normalizer is of order $|G|/n_p = 24/4 = 6$, thus, for the subgroup $H = \{\iota, (1\ 2\ 3), (1\ 3\ 2)\}$, the normalizer N_H is

$$\{\iota, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (2\ 3), (1\ 3)\} \tag{6.9.43}$$

Let $p = 2$. There exist 3 subgroups of order 8 ($3 \equiv 1 \pmod p$) by Lagrange theorem,

$$\begin{aligned}
&\{\iota, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}\\
&\{\iota, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2), (1\ 4), (2\ 3), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\}\\
&\{\iota, (4\ 2\ 3\ 1), (4\ 3)(2\ 1), (4\ 1\ 3\ 2), (4\ 3), (2\ 1), (1\ 4)(2\ 3), (4\ 2)(3\ 1)\}
\end{aligned}$$

We know that

$$\begin{aligned}
&(1\ 2)\,\{\iota, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}\,(1\ 2)\\
=\ &\{\iota, (1\ 3\ 4\ 2), (1\ 4)(2\ 3), (1\ 2\ 4\ 3), (2\ 3), (1\ 4), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\}
\end{aligned}$$

Thus, the subgroups are conjugate. So the case $p = 2$ is consistent with Sylow's theorems. The normalizer is of order $|G|/n_p = 24/3 = 8$, thus, for the subgroup $H = \{\iota, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}$, the normalizer N_H is H.

(ii) $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$.

Suppose $p = 2$, A_5 has n_p subgroups of order 4, with $n_p \equiv 1 \pmod 2$ and $n_p \mid 15$. So n_p =3, 5 or 15. We know that the element can be the form of $(1\ 2\ 3)$ since its order is 3 and $3 \nmid 4$. Also the element can not be the form of $(1\ 2)$ or $(1\ 2\ 3\ 4)$ since they have odd transpositions. Thus it has to be of the form

$$\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \tag{6.9.44}$$

Totally, we have $n_p = 5$. Thus, the normalizer is of order $60/5 = 12$. Thus, for $H = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, we have

$$N_{A_5}(H) = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\} \tag{6.9.45}$$

Suppose $p = 3$, A_5 has n_p subgroups of order 3, with $n_p \equiv 1 \pmod 3$ and $n_p \mid 20$, So $n_p = 4$ or 10. We know

$$\{\iota, (1\ 2\ 3), (1\ 3\ 2)\} \tag{6.9.46}$$

is one of them. Thus $n_p = C_2^5 = 10$. So the normalizer is of order $60/10 = 6$. Thus, for $H = \{\iota, (1\ 2\ 3), (1\ 3\ 2)\}$, we have

$$N_{A_5}(H) = \{\iota, (1\ 2\ 3), (1\ 3\ 2), (1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\}\,. \tag{6.9.47}$$

Suppose $p = 5$, A_5 has n_p subgroups of order 5, with $n_p \equiv 1 \pmod 5$ and $n_p \mid 12$.

But $H = \{\iota, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2)\}$ is the only subgroup. Thus $|N_{A_5}(H)| = 60/1 = 60$. Hence, $N_{A_5}(H) = A_5$.

Problem 6.9.17. Show that there is no simple group of order 441. Show that there is no simple group of order 351. How about orders 300 and 320?

Solution. $441 = 3^2 \cdot 7^2$. $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 9$. Thus, $n_7 = 1$. Since Sylow 7-subgroup is normal in G. Thus, G is not simple.

$351 = 3^3 \cdot 13$. $n_{13} = \equiv 1 \pmod{13}$ and $n_{13} \mid 27$. Thus, $n_{13} = 1$ or 27. If $n_{13} = 1$, G is not simple as above. So we assume $n_{13} = 27$. $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 13$. If $n_3 = 1$, G is not simple as above. So we assume $n_3 = 13$. Thus there will be $13 * (27 - 1) + 9 * (13 - 1) > 351$ elements. Contradiction. Thus, G is no simple.

$300 = 2^2 \cdot 3 \cdot 5^2$. $n_5 \equiv 1 \pmod 5$ amd $n_5 \mid 12$. Thus $n_5 = 1$ or 6. So we assume $n_5 = 6$. If G is abelian, all the subgroups are normal and thus G is not simple. If G is not abelian simple, it must have $300 \mid n_5!/2$ (by Corollary 6.7.4), but $300 \nmid 360 = n_5!/2$. Thus G is not simple.

$320 = 2^6 \cdot 5$. $n_2 \equiv 1 \pmod 2$, $n_2 \mid 5$. So assume $n_2 = 5$. If G is abelian, all the subgroups are normal and thus G is not simple. If G is not abelian simple, it must have $300 \mid n_2!/2$ (by Corollary 6.7.4), but $300 \nmid 60 = n_2!/2$. Thus G is not simple.

Problem 6.9.18. Let p, q and r be primes (not neccessarily distinct). Show that no group of order pq is simple. Show that no group of order pq^2 is simple. Show that no group of order pqr is simple.

Solution. If $p = q$, G of order p^2 is abelian (Proposition 6.6.2), thus G is not simple. If $p \neq q$, assume $p > q$, $n_p \equiv 1 \pmod p$ with $n_p \mid q$ and $n_q \equiv 1 \pmod q$ with $n_q \mid p$. So $n_p = 1$. Thus, G is not simple.

If $p = q$, G is of order p^3. If G is abelian, it is not simple. So assume G is non-abelian, thus the center $Z(G)$ is of order p by question 6.6.3 (i). Since center is normal and non-trivial, we have the contradiction. Thus, G is not simple.

If $p \neq q$, $n_p \equiv 1 \pmod p$ with $n_p \mid q^2$ and $n_q \equiv 1 \pmod q$ with $n_q \mid p$. If n_p or $n_q = 1$, we are done. So assume $n_q = p$ and $n_p = q$ or q^2.

If $n_p = q$, we have $q \equiv 1 \pmod p$ and $p \equiv 1 \pmod q$. Contradiction.

Suppose $n_p = q^2$. We have $p = 1 + rq$, thus $p > q$. Also, $q^2 = 1 + sp$, thus

$$p \mid (q+1) \text{ or } p \mid (q-1) \;\Rightarrow\; p \mid (q+1) \tag{6.9.48}$$

Thus the only possibility is $p = 3$, $q = 2$. Thus $|G| = 12$, but for non-abelian group G, $12 \nmid 1 = n_3!/2$. Thus, G is not simple.

For pqr, we only need to check the distinct prime numbers. Assume $p > q > r$, we have

$$n_p \equiv 1 \pmod p,\ n_p \mid qr, \quad n_q \equiv 1 \pmod q,\ n_q \mid pr, n_r \equiv 1 \pmod r,\ n_r \mid pq, \tag{6.9.49}$$

Note that p-subgroups are cyclic, thus the same element can not appear in two different subgroups.

If any of n_p, n_q, n_r is 1, we are done. So we assume they are not 1.

We know that $n_p \geq p + 1$, thus, we have $n_p > q, n_p > r$, so $n_p = qr$. Thus, we have $qr(p-1)$ elements of order p.

Also, we have $n_q \geq q + 1$, thus $n_q = p$ or pr.

If $n_q = pr$, we have $pr(q-1)$ elements of order q. Thus, totally, at least

$$qr(p-1) + pr(q-1) = pqr + (pqr - qr - pr) = pqr + ((p-1)(q-1) - 1)r > pqr \tag{6.9.50}$$

elements. Contradiction.

So we have $n_q = p$, will be $p(q-1)$ elements of order q. Furthermore, n_r is at least q. Thus, there are at least $q(r-1)$ elements of order r.

Thus, totally, there are at least

$$qr(p-1) + p(q-1) + q(r-1) = pqr + pq - qr + qr - p - q = pqr + (p-1)(q-1) - 1 > pqr \tag{6.9.51}$$

elements. Contradiction.

Thus pqr is not simple.

Problem 6.9.19. (i) Show that any group of order 15 is cyclic.

(ii) Show that any group of order 30 has a normal cyclic subgroup of order 15.

Solution. (i) $15 = 3 \cdot 5$. Thus, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 5$ gives that $n_3 = 1$. Similarly, $n_5 = 1$. So H and K are normal if $|H| = 3$, $|K| = 5$. Since H and K are cyclic and $H, K \lhd G$, $H \cap K = e$, we have $G \cong H \times K$ by Problem 6.9.13. Then by Lemma 6.6.8, 3 and 5 are coprime. Thus $G \cong C_3 \times C_5 \cong C_{15}$.

(ii) $30 = 2 \cdot 3 \cdot 5$. Thus,

$$n_2 \equiv 1 \pmod 2, n_2 \mid 15, \quad n_3 \equiv 1 \pmod 3, n_3 \mid 10, \quad n_5 \equiv 1 \pmod 5, n_5 \mid 6. \tag{6.9.52}$$

If $n_3, n_5 \neq 1$, we have $n_3 = 10$ and $n_5 = 6$ and therefore there are at least $10 \cdot (3-1) + 6 \cdot (5-1) = 20 + 24 = 48$ elements. Thus, at least one of n_3, n_5 is 1.

(a) If $n_3 = 1$, we have a normal $H \lhd G$ with $|H| = 3$. Thus $|G/H| = 10$. Now consider G/H, $n_5 \equiv 1 \pmod 5$ with $n_5 \mid 2$, so $n_5 = 1$. Then there is a normal $G'/H \lhd G/H$ with $|G'/H| = 5$. Thus, $|G'| = |G'/H|\,|H| = 15$. Thus, G' is cyclic subgroup by (i).
Thus $\forall hk \in G', g \in G$ where $h \in H$, $k \in K$, we know that

$$hg = gh,\ kg = gk \ \Rightarrow\ (hk)g = h(kg) = h(gk) = ghk = g(hk). \tag{6.9.53}$$

Thus G' is normal.

(b) If $n_5 = 1$. we have a normal $H \lhd G$ with $|H| = 5$. Thus, $|G/H| = 6$. Now consider G/H, $n_3 \equiv 1 \pmod 3$ with $n_3 \mid 2$, so $n_3 = 1$. Then there is a normal $G'/H \lhd G/H$ with $|G'/H| = 3$. Thus, $|G'| = |G'/H|\,|H| = 15$. Thus, G' is cyclic subgroup by (i). Similarly, G' is normal.

Problem 6.9.20. Let N and H be groups, and suppose that there is a homomorphism ϕ from H to $\mathrm{Aut}(N)$. Show that we can define a group operation on $N \times H$ by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot n_2^{\phi(h_1)}, h_1 \cdot h_2), \tag{6.9.54}$$

where we write $n^{\phi(h)}$ for the image of n under $\phi(h)$. Show that the resulting group G has (copies of) N and H as subgroups, that N is normal in G, that $G = NH$ and $N \cap H = 1$. (We say that G is a semidirect product of N by H.)

Find an element of $\mathrm{Aut}(C_7)$ of order 3 and construct a non-abelian group of order 21 as a semidirect product of C_7 by C_3.

Solution. Note that the elements of $Aut(N)$ are the maps $N \to N$.

The closure is obvious. Thus, for $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$, since ϕ is a homomorphism and $\phi(h)$ is an automorphism (map) $N \to N$,

$$\begin{aligned}
((n_1,h_1)(n_2,h_2))\,(n_3,h_3) &= \left((n_1 \cdot n_2^{\phi(h_1)}, h_1 \cdot h_2)\right)(n_3,h_3) = \left(n_1 n_2^{\phi(h_1)} n_3^{\phi(h_1 h_2)}, h_1h_2h_3\right) \\
&= \left(n_1 n_2^{\phi(h_1)} n_3^{\phi(h_1)\phi(h_2)}, h_1h_2h_3\right) = \left(n_1 n_2^{\phi(h_1)} \left(n_3^{\phi(h_2)}\right)^{\phi(h_1)}, h_1h_2h_3\right) \\
&= \left(n_1 \left(n_2 n_3^{\phi(h_2)}\right)^{\phi(h_1)}, h_1h_2h_3\right) \quad \phi(h_1) \text{ is homomorphism} \\
&= \left(n_1 \left(n_2 n_3^{\phi(h_2)}\right)^{\phi(h_1)}, h_1h_2h_3\right) = (n_1,h_1)(n_2 n_3^{\phi(h_2)}, h_2h_3) \\
&= (n_1,h_1)\left((n_2,h_2)(n_3,h_3)\right).
\end{aligned}$$

Thus associativity holds. For the identity, we try (e_N, e_H), Thus, $\phi(e_H) = \iota$ where ι is the identity map, since ϕ is a homomorphism. Thus, $\forall n \in N, h \in H$,

$$(e_N, e_H)(n,h) = \left(e_N n^{\phi(e_H)}, e_H h\right) = (e_N \iota(n), e_H h) = (e_N n, e_H h) = (n,h). \tag{6.9.55}$$

$$(n,h)(e_N, e_H) = \left(n e_N^{\phi(n)}, h e_H\right) = (n e_N, h e_H) = (n,h). \tag{6.9.56}$$

For the inverse, try $\left((n^{-1})^{\phi^{-1}(h)}, h^{-1}\right)$,

$$\begin{aligned}
(n,h)\left((n^{-1})^{\phi^{-1}(h)}, h^{-1}\right) &= \left(n\left((n^{-1})^{\phi^{-1}(h)}\right)^{\phi(h)}, hh^{-1}\right) = \left(n(n^{-1})^{\phi^{-1}(h)\phi(h)}, hh^{-1}\right) \\
&= \left(nn^{-1}, hh^{-1}\right) = (e_N, e_H).
\end{aligned}$$

$$\begin{aligned}\left((n^{-1})^{\phi^{-1}(h)},h^{-1}\right)(n,h) &= \left((n^{-1})^{\phi^{-1}(h)}n^{\phi(h^{-1})},h^{-1}h\right)=\left((n^{-1})^{\phi^{-1}(h)}n^{\phi^{-1}(h)},h^{-1}h\right)\\ &= \left((n^{-1}n)^{\phi^{-1}(h)},h^{-1}h\right)=\left(e_N^{\phi(h)^{-1}},e_H\right)=(e_N,e_H)\end{aligned}$$

since $\phi(h)^{-1}$ is homomorphism.

We know that $N\cong N\times\{e_H\}:=N'\leq G$, $H\cong\{e_N\}\times H:=H'\leq G$. Thus, N',H' are subgroups. $\forall x=(m,e_H)\in N', g=(n,h)\in G$, we have

$$\begin{aligned}gxg^{-1} &= (n,h)(m,e_H)\left((n^{-1})^{\phi^{-1}(h)},h^{-1}\right)=\left(nm^{\phi(h)},he_H\right)\left((n^{-1})^{\phi^{-1}(h)},h^{-1}\right)\\ &= \left(nm^{\phi(h)},h\right)\left((n^{-1})^{\phi^{-1}(h)},h^{-1}\right)=\left(nm^{\phi(h)}\left((n^{-1})^{\phi^{-1}(h)}\right)^{\phi(h)},hh^{-1}\right)\\ &= \left(nm^{\phi^{-1}(h)}n^{-1},hh^{-1}\right)=\left(nm^{\phi^{-1}(h)}n^{-1},e_H\right)\in N'.\end{aligned}$$

So N' is normal in G.

$\forall(n,h)\in G$, we have $(n,e_H)\in N'$ and $(e_N,h)\in H'$.

$$(n,e_H)(e_N,h)=\left(ne_N^{\phi(e_H)},e_Hh\right)=(ne_N^{\iota},h)=(n,h)\in G\ \Leftrightarrow\ G=N'H'. \tag{6.9.57}$$

Clearly, $N'\cap H'=\{(e_N,e_H)\}$.

Now we have the map f for $N=C_7$ containing $\{1,2,3,4,5,6,7\}$,

$$f(1)=1,\ f(2)=3,\ f(3)=4,\ f(4)=2,\ f(5)=6,\ f(6)=7,\ f(7)=5\ \Rightarrow\ f:(2\ 3\ 4)(5\ 6\ 7) \tag{6.9.58}$$

Thus, $f^2=f\circ f=(2\ 4\ 3)(5\ 7\ 6)$, $f\circ f\circ f=f^3=\iota$. So $f\in\mathrm{Aut}(C_7)$ is of order 3.

Let $g\in H=C_3$ ($C_3=\left\{e,g,g^2\right\}$) and

$$\phi(e)=\iota,\ \phi(g)=f,\ \phi(g^2)=f^2. \tag{6.9.59}$$

Then $G=NH$ defined as above is semidirect product of C_7 by C_3 whose order is 21.

Let $n\in C_7, h\in C_3$ and $\forall(n^{i_1},h^{j_1}),(n^{i_2},h^{j_2})\in G$ where $i_1,i_2\in\{0,1,2,3,4,5,6\}$, $j_1,j_2\in\{0,1,2\}$

$$\begin{aligned}(n^{i_1},h^{j_1})(n^{i_2},h^{j_2}) &= \left(n^{i_1}\left(n^{i_2}\right)^{\phi(h^{j_1})},h^{j_1}h^{j_2}\right)=\left(n^{i_1}\left(n^{\phi(h^{j_1})}\right)^{i_2},h^{j_1}h^{j_2}\right)\\ (n^{i_2},h^{j_2})(n^{i_1},h^{j_1}) &= \left(n^{i_2}\left(n^{i_1}\right)^{\phi(h^{j_2})},h^{j_2}h^{j_1}\right)=\left(n^{i_2}\left(n^{\phi(h^{j_2})}\right)^{i_1},h^{j_2}h^{j_1}\right)\end{aligned}$$

If we set $i_1=1$, $i_2=2$, $j_1=j_2=1$,

$$n^{i_1}\left(n^{\phi(h^{j_1})}\right)^{i_2}=n\left(n^{\phi(h)}\right)^2,\quad n^{i_2}\left(n^{\phi(h^{j_2})}\right)^{i_1}=n^2\left(n^{\phi(h)}\right) \tag{6.9.60}$$

Let $C_7=\left\{e,t,t^2,t^3,t^4,t^5,t^6\right\}$ with indices from 1 to 7. Then if we have $\phi(h)=f$ and $n=t$,

$$n\left(n^{\phi(h)}\right)^2=t\left(f(t)\right)^2=t\left(t^2\right)^2=t^5,\quad n^2\left(n^{\phi(h)}\right)=t^2\left(f(t)\right)=t^4. \tag{6.9.61}$$

Thus, we have $(n^{i_1},h^{j_1})(n^{i_2},h^{j_2})\neq(n^{i_2},h^{j_2})(n^{i_1},h^{j_1})$. Thus, G is non-abelian.

Problem 6.9.21. Let p be a prime. How many elements of order p are there in S_p, the symmetric group of order p? What are their centralizers? How many Sylow p-subgroups are there? What are the orders of their normalizers? If q is a prime dividing $p-1$, deduce that there exists a non-abelian group of order pq.

Solution. Suppose $\tau\in S_p$ with $o(\tau)=p$. Clearly, $\langle\tau\rangle\cong C_p$ since p is a prime. Now consider the centraliser of τ in S_p, thus,

$$C_{S_p}(\tau)=\left\{\sigma\in S_p:\sigma\tau\sigma^{-1}=\tau\right\} \tag{6.9.62}$$

We know that $\tau=(a_1a_2\dots a_p)$ and $\sigma\tau\sigma^{-1}=(\sigma(a_1)\sigma(a_2)\dots\sigma(a_p))$ by the result in Theorem 6.5.24. Thus, $C_{S_p}(\tau)\cong C_p$ and therefore $C_{S_p}(\tau)=\langle\tau\rangle$. So $\left|C_{S_p}(\tau)\right|=p$. By orbit-stabiliser theorem, we have $p!/p=(p-1)!$ elements in the conjugacy

class of τ.

Then by Theorem 6.5.24, the permutations in S_n are conjugate in S_n iff they have the same cycle type. Thus, all the elements in the conjugacy class are of order p. Hence, there are $(p-1)!$ elements of order p.

We know that in each p-subgroup, there are $p-1$ elements of p. Then we have that there are $(p-1)!/(p-1) = (p-2)! = n_p$ p-subgroups.

(Recall that $n_p \equiv 1 \pmod p$ by Sylow Theorem. It is true that $(p-2)! \equiv 1 \pmod p$ when p is a prime.)

Then we have (by Corollary 6.7.3) for $P \in X$ where X is the set of p-subgroups,

$$\left|N_{S_p}(P)\right| = \frac{|S_p|}{n_p} = \frac{p!}{(p-2)!} = p(p-1). \tag{6.9.63}$$

If $p = 2$, there is no prime q dividing $p-1$.

If $p = 3$, then $q = 2$ and D_6 is a non-abelian group of order $2 \cdot 3$.

If $p > 3$, then by Sylow theorem there exist $(p-2)!$ Sylow p-subgroup of S_p. Let P be a Sylow p-subgroup which is cyclic, generated by h ($P = \langle h \rangle$). Now consider the normaliser $N_{S_p}(P)$ of order $p(p-1) = npq$ since $q \mid (p-1)$. Then by Sylow theorem (Theorem 6.7.1)there exists a q-subgroup generated by $k \in N_{S_p}(P)$ i.e. $kP = Pk$. Since q is prime, we have q-subgroup is cyclic. Let $Q = \{k\}$.

Then consider $G := PQ = \{hk : h \in P, k \in Q\}$. $\forall h_1k_1, h_2k_2 \in PQ$,

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} \underbrace{=}_{kP=Pk,\ h_3 \in P} \underbrace{h_1h_3}_{\in P}\underbrace{k_1k_2^{-1}}_{\in Q} \in G. \tag{6.9.64}$$

So by Lemma 6.1.7, $G \leq S_p$. Thus, $k \in N_{S_p}(P) \ \Rightarrow \ k \in N_G(P)$. Since $P \cap Q = \{e\}$, we have $|G| = |P|\,|Q| = pq$. Then apply Sylow theorem (Theorem 6.7.1) (i),(iii) on G, there are n_p p-subgroups in G and

$$n_p \equiv 1 \pmod p, \quad n_p \mid q \ \Rightarrow \ n_p = 1. \tag{6.9.65}$$

Thus there are only one p-subgroup and thus $p - 1 = q$ elements in conjugacy class. Thus let the centraliser be $C_G(h)$ and we have $|C_G(h)| = pq/q = p$ by orbit-stabiliser theorem. Thus $C_G(h) = \langle h \rangle$.

If $hk = kh$, then $k \in C_G(h)$. Contradiction. Thus, G is non-abelian.

Problem 6.9.22. Show that no non-abelian simple group has order less than 60.

Solution. According to Problem 6.9.18, we can remove all the cases that p, pq, pq^2, pqr where p, q, r are primes.

So we remove the corresponding number and then we have 16, 24, 32, 36, 40, 48, 54 and 56 left.

For $|G| = 16, 32$, G is a finite 2-group. Then by Theorem 3.6.1., $Z(G)$ is non-trivial. $Z(G) \leq G$ by Proposition 3.5.15., so $Z(G) \lhd G$. Thus, G is not simple.

If $|G| = 24 = 2^3 \cdot 3$. Then $n_3 \equiv 1 \pmod 3$, $n_3 \mid 8$, so $n_3 = 1, 4$. Then $n_3 < 5$ and it is a contradiction to Corollary 3.7.4. Thus, G is not non-abelian simple.

If $|G| = 36 = 2^2 \cdot 3^2$. Then $n_3 \equiv 1 \pmod 3$, $n_3 \mid 4$, so $n_3 = 1, 4$. So the same argument gives that G is not non-abelian simple.

If $|G| = 40 = 2^3 \cdot 5$. Then $n_5 \equiv 1 \pmod 5$, $n_5 \mid 8$, $n_5 = 1$. So the unique 5-subgroup is normal in G by Lemma 3.7.2.. Then G is not simple.

If $|G| = 48 = 2^4 \cdot 3$. Then $n_2 \equiv 1 \pmod 5$, $n_2 \mid 3$, $n_2 = 1, 3$. So the same argument with the case $|G| = 24$ gives that G is not non-abelian simple.

If $|G| = 54 = 2 \cdot 3^3$. Then $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 2$, $n_3 = 1$. So the unique 3-subgroup is normal in G by Lemma 3.7.2.. Then G is not simple.

If $|G| = 56 = 2^3 \cdot 7$. Then $n_2 \equiv 1 \pmod 2$, $n_2 \mid 7$, $n_2 = 1, 7$. Similarly, $n_7 = 1, 8$. If any of n_2 or n_5 is 1, G is not simple. If $n_2 = 7$, $n_7 = 8$, we have $(8-1)+8(7-1) = 55$ different elements in one of Sylow 2-subgroups and in all 8 Sylow 7-subgroups. But in the other 6 Sylow 2-subgroups there is at least one different element. Thus, the total number of non-identity elements is at least 56. But that's too many. Hence $n_2 = 1$ or $n_7 = 1$. So G is not simple.

Problem 6.9.23. Let G be a simple group of order 60. Show that G is isomorphic to the alternating group A_5, as follows. Show that G has six Sylow 5-subgroups. Deduce that G is isomorphic to a subgroup (also denoted by G) of index 6 of the alternating group A_6. By considering the coset action of A_6 on the set of cosets of G in A_6, show that there is an automorphism of A_6 which takes G to A_5.

Solution. $|G| = 60 = 2^2 \cdot 3 \cdot 5$. $n_5 \equiv 1 \pmod 5$, $n_5 \mid 12$, thus, $n_5 = 1, 6$. If $n_5 = 1$, 5-subgroup is normal and thus G is not simple. Hence $n_5 = 6$.

Recall Lemma 6.5.1: Fixing $g \in G$, the map $\varphi_g : X \to X$, $x \mapsto g(x)$ is a permutation of $X = \{\text{Sylow 5-subgroup}\}$ with $|X| = 6$, so $\varphi_g \in \mathrm{Sym}(X) = S_6$. Then the mapping $\varphi : G \to \mathrm{Sym}(X)$, $g \mapsto \varphi_g$, with $\varphi_g(x) = g(x)$, is a homomorphism called a permutation representation of G.

The image $\varphi(G)$ is a subgroup of $\mathrm{Sym}(X) = S_6$, denoted G^X. The kernel of φ, $\ker\varphi = \{g \in G : g(x) = x, \forall x \in X\}$, also denoted G_X, is a normal subgroup and $G/G_X \cong G^X$.

We know that G_X is normal, if it is non-trivial, G is not simple. Contradiction. Thus, we have G_X is trivial and therefore we have $G = G/G_X \cong G^X \leq \mathrm{Sym}(X) = S_6$.

But $A_6 \lhd S_6$ and so by the second isomorphism theorem (Theorem 6.4.12), $G^X \cap A_6 \lhd S_6$. Since $G^X \cap A_6 \subseteq G^X$, $G^X \cap A_6 \lhd G^X$ ($G^X \cap A_6$ is normal subgroup in S_6). Simplicity of G^X implies that either

$$G^X \cap A_6 = \{e\} \quad \text{or} \quad G^X \cap A_6 = G^X. \tag{6.9.66}$$

In the first case, the second isomorphism theorem implies

$$G^X = G^X/\{e\} = G^X/(G^X \cap A_6) \cong (G^X A_6)/A_6 \leq S_6/A_6 \tag{6.9.67}$$

and hence $\left|G^X\right| \leq 2$, which should be abelian, a contradiction. Thus, $G^X \subseteq A_6$ and $G \cong G^X \leq A_6$.

We know that G^X is of order 60, and $|A_6| = 6!/2 = 360$. Thus, G^X is a subgroup of A_6 with index 6.

Now we apply Lemma 6.5.1 again. Considering the mapping $\phi_g : Y \to Y$, $y \mapsto g(y)$ where $g \in A_6$ and $y \in Y = \left\{hG^X : h \in A_6\right\} = A_6/G^X$, $|Y| = 6$. Then the mapping $\phi : A_6 \to \mathrm{Sym}(Y) = S_6$, $g \mapsto \phi_g$, with $\phi_g(y) = g(y)$, is a homomorphism called a permutation representation of A_6.

Then by first isomorphism theorem (Theorem 6.4.9), $A_6/\ker\phi = \mathrm{Im}\,\phi$. Since A_6 is simple, $\ker\phi = \{e\}$, thus

$$A_6 = A_6/\{e\} = A_6/\ker\phi \cong \mathrm{Im}\,\phi = \phi(A_6). \tag{6.9.68}$$

So $\phi : A_6 \to A_6$ is an automorphism. We know that $G^X \leq A_6$, so $\phi(G^X) \leq A_6$.

Now we have $y \in \left\{G^X, g_1G^X, g_2G^X, g_3G^X, g_4G^X, g_5G^X\right\}$ where $g_1, g_2, g_3, g_4, g_5 \in A_6, \notin G^X$. Then for the element $g \in G^X$,

$$\phi(g) = g(y) \in \left\{G^X, gg_1G^X, gg_2G^X, gg_3G^X, gg_4G^X, gg_5G^X\right\}. \tag{6.9.69}$$

Thus $\phi(G^X)$ is the even permutation of 5 cosets of G^X, $g_1G^X, g_2G^X, g_3G^X, g_4G^X, g_5G^X$. Thus, $\phi(G^X) \subseteq A_5$ and $\phi(G^X) \leq A_5$. Then since G^X is simple as $G \cong G^X$, we have $\ker\phi = \{e\}$,

$$G^X = G^X/\{e\} = G^X/\ker\phi \cong \mathrm{Im}\,\phi = \phi(G^X) \tag{6.9.70}$$

Thus, $\left|\phi(G^X)\right| = \left|G^X\right| = |G| = 60 = 6!/2 = |A_5|$. Since $\phi(G^X) \leq A_5$, we have $\phi(G^X) = A_5$. Thus,

$$A_5 = \phi(G^X) \cong G^X \cong G. \tag{6.9.71}$$

Problem 6.9.24. Let G be a group of order 60 which has more than one Sylow 5-subgroup. Show that G must be simple.

Solution. $|G| = 60 = 2^2 \cdot 3 \cdot 5$. By Sylow theorem, $n_5 \equiv 1 \pmod 5$, $n_p \mid 12$, thus $n_5 = 1, 6$. Since G has more than one Sylow 5-subgroup, we have $n_5 = 6$. Since 5-subgroup is C_5, there are $6 \cdot (5-1) = 24$ distinct elements of order 5.

If H is normal subgroup of G, $H \lhd G$, it must have the size of 2,3,4,5,6,10,12,15,20,30.

(a) If $|H| = 5, 10, 15, 20$, it must have Sylow 5-subgroup. Also, H is normal and it must have all Sylow 5-subgroup since all Sylow 5-subgroup are conjugate. However, $24 > 5, 10, 15, 20$. Contradiction.

(b) If $|H| = 30$, we use the result in Problem 6.9.19.(ii), $n_5 = 1$. Contradiction.

(c) If $|H| = 2, 3, 4, 6$, $|G/H| = 30, 20, 15, 10$. $n_5 \equiv 1 \pmod 5$, $n_5 \mid 6, 4, 3, 2$. From the above, we have $n_5 = 1$. Let G'/H be a 5-subgroup of G/H. Since $n_5 = 1$, we have $G'/H \lhd G/H$ by Lemma 6.7.2. Then $|G'| = 5\,|H| = 10, 15, 20, 30$, respectively. Then by Proposition 6.4.13, let $K \lhd G$ and $L \leq G$ be a subgroup containing K. Then

$$L/K \lhd G/K \;\Leftrightarrow\; L \lhd G. \tag{6.9.72}$$

Thus we have

$$G'/H \lhd G/H \;\Rightarrow\; G' \lhd G. \tag{6.9.73}$$

However, $|G'| = 10, 15, 20, 30$. Contradiction by result in (a) and (b).

(d) Finally, if $|H| = 12 = 2^2 \cdot 3$, we have

$$n_2 \equiv 1 \pmod 2,\ n_2 \mid 3, \quad n_3 \equiv 1 \pmod 3,\ n_3 \mid 4 \;\Rightarrow\; n_2 = 1, 3,\ n_3 = 1, 4. \tag{6.9.74}$$

If $n_2 = 3$ and $n_3 = 4$, we have at least $(4-1) + 4(3-1) + 1$ (since elements of order 3 are distinct, $4-1$ elements in one group are distinct and there is an extra distinct element in other Sylow 2-subgroup) non-identity elements. Then one of n_2 or n_3 has to be 1.

Let N be unique Sylow 2/3-subgroup of H. Then $N \lhd H$ by Lemma 6.7.2. Clearly, N is also a Sylow 2/3-subgroup of G. Thus H contains all Sylow 2/3-subgroup of G since $H \lhd G$ and all Sylow 2/3-subgroup are conjugate. Thus, N is the unique Sylow 2/3-subgroup of G. Again, by Lemma 6.7.2, $N \lhd G$. But $|N| = 3, 4$ which is contradiction by (c).

Thus, G must be simple.

Chapter 7

Rings

7.1 Rings and Polynomials

7.1.1 Definitions and Examples

Definition 7.1.1 (ring)**.** A set R with two operations, $+$ and $\cdot$, forms a ring if

(i) $(R, +)$ is an abelian group,

(ii) multiplication is closed and associative and there is a multiplicative identity $1_R \in R$ such that

$$\forall r \in R,\ 1_R \cdot r = r \cdot 1_R = r, \tag{7.1.1}$$

(iii) multiplication is distributive over addition, that is

$$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3, \qquad (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3. \tag{7.1.2}$$

Definition 7.1.2 (commutative ring)**.** A rings R is commutative if the multiplication is commutative, i.e.,

$$r_1 \cdot r_2 = r_2 \cdot r_1,\ \forall r_1, r_2 \in R. \tag{7.1.3}$$

Definition 7.1.3 (subring)**.** A subset S of R is a subring if it is a ring under the restriction of the two operations. In particular, $1_R \in S$. The notation is $S \leq R$.

Definition 7.1.4 (field)**.** A field $\mathbb{F}$ is a commutative ring with an identity element 1, $1 \neq 0$, in which every non-zero element is invertible, i.e., $\forall a \in \mathbb{F} \setminus \{0\}$, $\exists b \in \mathbb{F}$ s.t. $ab = 1$.

Note that $\mathbb{F}_i$ denotes the field with i elements.

Example 7.1.1. (i) We have the four nested rings $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(ii) The Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$, $i^2 = -1$ (see Definition 7.9.1).

(iii) $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\} \leq \mathbb{R}$.

Remark. All fields are rings, e.g. $\mathbb{Z}$ modulo n, the set $\{0, \ldots, n-1\}$ with addition and multiplication modulo n.

Definition 7.1.5 (unit)**.** A unit of R is an element with a multiplicative inverse in R, e.g. 2 is a unit in $\mathbb{Q}$, but not a unit in $\mathbb{Z}$.

Remark. Some people confusingly talk about 1_R as the unit of R.

Example 7.1.2. The zero ring $\{0\}$. In this case the multiplicative identity is the same as the additive one. But in all other rings $0 \neq 1$.

$$(0 + 0) \cdot r = 0 \cdot r, \qquad (0 + 0) \cdot r = 0r + 0 \cdot r \tag{7.1.4}$$

so $0r = 0$ for all $r \in R$. Hence 0 is not the multiplicative identity if R has more than one element.

Definition 7.1.6 (idompotent)**.** An element r of a ring R is idempotent if $r^2 = r$.

7.1.2 Polynomials

Definition 7.1.7 (polynomial)**.** Let R be a ring. A polynomial f over R is of the form

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 \tag{7.1.5}$$

with $a_i \in R$. The degree of f is the largest n with $a_n \neq 0$. f is monic if $a_n = 1$, where n is the degree of f.

Definition 7.1.8 (polynomial ring)**.** $R[X]$ is the (commutative) polynomial ring over R with ring operations

$$(f+g)(X) = \sum_i (a_i + b_i) X^i, \qquad (fg)(X) = \sum_i \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i \tag{7.1.6}$$

where $f(X) = \sum a_i X^i$, $g(X) = \sum b_i X^i$.

Remark. R is a subring of $R[X]$ by identifying R with the constant polynomials $f(X) = \sum a_i X^i$ with $a_i = 0$ for all $i \geq 1$.

Definition 7.1.9 (ring of formal power series)**.** $R[[X]]$ is the (commutative) ring of formal power series

$$f(X) = a_0 + a_1 X + a_2 X^2 + \ldots \tag{7.1.7}$$

with the same addition and multiplication as for $R[X]$ but note that there is no restriction demanding that all but finitely many coefficients be zero (could be infinitely many).

Definition 7.1.10 (Laurent polynomials)**.** The (commutative) Laurent polynomials are

$$f(X) = \sum_{i \in \mathbb{Z}} a_i X^i, \qquad (fg)(X) = \sum_i \left(\sum_j a_j b_{i-j} \right) X^i \tag{7.1.8}$$

with the condition that all but finitely many a_i are zero, e.g. $X^{-1} + X$.

Definition 7.1.11 (Laurent series)**.** Laurent series are

$$\sum_{i \in \mathbb{Z}} a_i X^i \tag{7.1.9}$$

with the condition that all but finitely many of the a_i for $i \leq 0$ are zero. Addition and multiplication are defined in the same way as for Laurent polynomials.

Example 7.1.3. The ring of all R-valued functions on a set A, $f : A \to R$. The ring operations can be defined by pointwise addition and multiplication,

$$(f+g)(a) = f(a) + g(a), \qquad (fg)(a) = f(a)g(a). \tag{7.1.10}$$

Example 7.1.4. The set of continuous functions $f : \mathbb{R} \to \mathbb{R}$ forms a subring of the (commutative) ring of all functions $\mathbb{R} \to \mathbb{R}$. The set of continuous functions $\mathbb{R} \to \mathbb{R}$ contains the subring of polynomial functions, $f : \mathbb{R} \to \mathbb{R}$, $a \mapsto f(a)$, where $f(X) \in \mathbb{R}[X]$.

Remark. We can similarly consider Laurent polynomial functions, power series functions $\mathbb{C} \to \mathbb{C}$ and Laurent series functions $\mathbb{C} \to \mathbb{C}$.

7.2 Ring Homomorphism, Ideal, Quotient Ring and Isomorphism Theorems

7.2.1 Ring Homomorphism

Definition 7.2.1 (ring homomorphism)**.** Let R and S be rings (not necessarily commutative). A map $\theta : R \to S$ is a ring homomorphism if

(i) $\theta(r_1 + r_2) = \theta(r_1) + \theta(r_2)$,

(ii) $\theta(r_1 r_2) = \theta(r_1)\theta(r_2)$,

(iii) $\theta(1_R) = 1_S$.

A bijective homomorphism is called an isomorphism.

Definition 7.2.2 (kernel)**.** The kernel of θ is $\ker\theta = \{r \in R : \theta(r) = 0\}$.

Lemma 7.2.1. Let θ be a ring homomorphism. θ is injective if and only if $\ker\theta = \{0\}$.

Proof. θ is a homomorphism of the additive groups (Definition 6.1.15). Then we have the required result by Lemma 6.1.26. □

7.2.2 Ideal

Definition 7.2.3 (ideal, left ideal, right ideal)**.** A subset I of R is an ideal, written $I \lhd R$, if

(i) I is a subgroup of R under addition,

(ii) whenever $a \in I$ and $r \in R$ then $ar \in I$ and $ra \in I$.

The second condition is called the strong closure property.

A subset I of R is called a left ideal of R if it is an additive subgroup of R and absorbs multiplication on the left, i.e.,

(i) $(I, +)$ is a subgroup of $(R, +)$

(ii) $\forall a \in I$, $\forall r \in R$, then $ra \in I$.

A subset I of R is called a right ideal of R if it is an additive subgroup of R and absorbs multiplication on the right, i.e.,

(i) $(I, +)$ is a subgroup of $(R, +)$

(ii) $\forall a \in I$, $\forall r \in R$, then $ar \in I$.

Remark. An ideal in general is not a subring.

Lemma 7.2.2. Let $I \lhd R$. Then $I = R$ if $1 \in I$.

Remark. The only ideal which is a subring of R is R itself.

Proof. If $1 \in I$ then $r = 1r \in I$ for all $r \in R$ and so $I = R$ if $1 \in I$. □

Lemma 7.2.3. A non-zero commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. Suppose that R is a field and take an ideal $I \lhd R$. If $I \neq \{0\}$ then pick $0 \neq a \in I$. Then we can pick $a^{-1} \in R$ such that $1 = aa^{-1} \in I$. Hence $I = R$ by Lemma 7.2.2.

Conversely, assume that $\{0\}$ and R are the only ideals. Take $a \in R$ with $a \neq 0$. Then $\langle a \rangle \neq \{0\}$ and so $\langle a \rangle = R$. Hence $1 \in R = \langle a \rangle$ (by Definition 7.1.1.(iii)) and there exists $r \in R$ (as $\langle a \rangle = aR$) such that $ar = 1$. Thus, R is a field. □

Lemma 7.2.4. The kernel of a ring homomorphism $\theta : R \to S$ is an ideal.

Proof. θ is a homomorphism of the additive groups $(R, +) \to (S, +)$ and so $\ker\theta$ is an additive subgroup of R by first isomorphism theorem of groups (Theorem 6.4.9).

If $a \in \ker\theta$, then $\theta(a) = 0$ (by recalling Definition 7.2.2). Consider $r \in R$,

$$\theta(ar) = \theta(a)\theta(r) = 0 \cdot \theta(r) = 0. \tag{7.2.1}$$

Thus $ar \in \ker\theta$, so we have the strong closure property. □

Example 7.2.5. (i) In a field $\mathbb{F}$, the only ideals are $\{0\}$ and $\mathbb{F}$. (Multiply any non-trivial element in the ideal by its inverse to see that 1 is in the ideal.)

(ii) In $\mathbb{Z}$ the ideals are of the form

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}. \tag{7.2.2}$$

Proof. Certainly each set $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Suppose I is a non-zero ideal. We show that all the non-zero additive subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

Let n be the least positive element of I and use Euclidean algorithm[1]. If $b \in I$ then $b = nq + r$ with $0 \leq r < n$ and some q. Note that $r = b - nq \in I$. Minimality of n implies that $r = 0$ and hence $b = nq$. Thus $I = n\mathbb{Z}$. □

Proposition 7.2.6. Let R be a ring and $I_j \lhd R$ with $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$. Then the union $I = \bigcup_j I_j$ is an ideal.

Proof. $\forall a, b \in I$, if $a \in I_j$ and $b \in I_k$, $j \leq k$ then $a \in I_k$, $b \in I_k$ implies $a + b \in I_k \subseteq I$.
$\forall a \in I, r \in R$, $a \in I_j$, $ar \in I_j \subseteq I$. Thus, $I \lhd R$. □

Definition 7.2.4 (principal ideal)**.** Let R be a ring and $a \in R$. Then the ideal generated by a is $aR = \{ar : r \in R\}$. We often use the notation $\langle a \rangle$ for aR.

Note that this is the smallest ideal of R containing a. Such an ideal is called a principal ideal.

More generally, the ideal generated by $a_1, \dots, a_k$ is

$$\langle a_1, \dots, a_k \rangle = a_1R + \dots a_kR = \left\{ \sum_{i=1}^{k} a_i r_i : r_i \in R \right\}. \tag{7.2.3}$$

Even more generally, the ideal generated by a subset A of R is

$$\langle A \rangle = \left\{ \sum_{a \in A} ar_a : \text{ only finitely many } r_a \in R \text{ are non-zero} \right\}. \tag{7.2.4}$$

Example 7.2.7. Examples of principal ideals include $n\mathbb{Z}$ in $\mathbb{Z}$ and $\langle X \rangle$ in $\mathbb{C}[X]$, where $\langle X \rangle$ is the ideal of polynomials with zero constant term.

7.2.3 Quotient ring

Proposition 7.2.8. Let $I \lhd R$ be an ideal. Then the quotient ring R/I has elements consisting of the cosets $r + I$ with the operations

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I, \qquad (r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I. \tag{7.2.5}$$

This defines a ring R/I.

Proof. From Theorem 6.4.7 we have already checked that R/I forms a group under addition as defined. So we need to check that multiplication is well-defined, closed and associative. If

$$r_1 + I = r_1' + I, \qquad r_2 + I = r_2' + I \tag{7.2.6}$$

then $r_1' = r_1 + a_1$, $r_2' = r_2 + a_2$ for some $a_1, a_2 \in I$, and therefore

$$r_1' r_2' = (r_1 + a_1)(r_2 + a_2) = r_1 r_2 + (a_1 r_2 + r_1 a_2 + a_1 a_2) \tag{7.2.7}$$

where the second term is contained in I by the strong multiplicative closure property of ideal. Thus $r_1' r_2' + I = r_1 r_2 + I$ and therefore multiplication is well-defined.

The multiplicative identity is $1 + I$ since $(1 + I)(r + I) = r + I$.

Closure and associativity: $\forall r_1 + I, r_2 + I \in R/I, r_1, r_2 \in R$, by the closure of ring R,

$$(r_1 + I)(r_2 + I) = r_1 r_2 + r_1 I + r_2 I + I = \underbrace{r_1 r_2}_{\in R} + I \in R/I. \tag{7.2.8}$$

Thus, R/I is closed. Also, by associativity of ring R

$$(r_1 + I)(r_2 + I) = r_1 r_2 + r_1 I + r_2 I + I = r_1 r_2 + I = r_2 r_1 + I = (r_2 + I)(r_1 + I). \tag{7.2.9}$$

[1] need quote

So, $\mathbb{R}/I$ is associative. $\forall r_1+I, r_2+I, r_3+I \in R/I, r_1, r_2, r_3 \in R$, by distributivity of ring R,

$$\begin{aligned}(r_1+I)(r_2+I+r_3+I) &= (r_1+I)(r_2+r_3+I) = r_1(r_2+r_3)+r_1I+r_2I+r_3I+I \\ &= r_1r_2+r_1r_3+r_1I+r_2I+r_3I+I = r_1r_2+r_1I+r_2I+I+r_1r_3+r_1I+r_3I+I \\ &= (r_1+I)(r_2+I)+(r_1+I)(r_3+I).\end{aligned}$$

Hence, R/I has distributivity. Therefore R/I is a ring. □

Example 7.2.9. (i) $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring.

$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Elements $m+n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$ may be expressed as one of

$$0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}. \tag{7.2.10}$$

Addition and multiplication correspond to arithmetic modulo n.

(ii) Consider the (principal) ideal $I=(X) \lhd C[X]$. Elements $f(X)+I$ of the quotient ring $\mathbb{C}[X]/I$ may be expressed in the form $a+I$ where $a \in \mathbb{C}$ is the constant term of $f(X)$. Addition and multiplication correspond to that in $\mathbb{C}$,

$$(a+I)+(b+I)=(a+b)+I, \qquad (a+I)(b+I)=ab+I. \tag{7.2.11}$$

Therefore, $\mathbb{C}[X]/I \cong \mathbb{C}$.

Proposition 7.2.10 (Euclidean algorithm for polynomials)**.** Let $\mathbb{F}$ be a field and consider polynomials $f(X)$, $g(X) \in \mathbb{F}[X]$. Then we can write

$$f(X)=g(X)q(X)+r(X) \tag{7.2.12}$$

with $\deg r < \deg g$.

Proof. Write

$$f(X)=\sum_{i=0}^{n} a_iX^i, \qquad g(X)=\sum_{i=0}^{m} b_iX^i \tag{7.2.13}$$

with $\deg f(X)=n$ and $\deg g(X)=m$.

If $n<m$ then set $q(X)=0$ and $r(X)=f(X)$. Now assume $n \geq m$, and argue by induction on n. Set $f_1(X)=f(X)-a_nb_m^{-1}X^{n-m}g(X)$ so $\deg f_1(X) < \deg f(X)$. If $m=n$ then $\deg f_1(X) < m$ and we can apply our first case to $f_1(X)$,

$$f(X)=a_nb_m^{-1}g(X)+f_1(X). \tag{7.2.14}$$

If $n>m$ then we have by induction

$$f_1(X)=g(X)q_1(X)+r_1(X) \tag{7.2.15}$$

for suitable $q_1(X)$ and $r_1(X)$, so

$$f(X)=g(X)(q_1(X)+a_nb_m^{-1}X^{n-m})+r_1(X). \tag{7.2.16}$$

□

Remark. We require $\mathbb{F}$ to be a field as we need b_m^{-1}.

Example 7.2.11. Consider the ideal

$$I=\left\{X^2+1\right\} \lhd \mathbb{R}[X]. \tag{7.2.17}$$

For any $f(X) \in \mathbb{R}[X]$, we can write $f(X)=(X^2+1)q(X)+r(X)$ with $\deg r(X) \leq 1$. Thus $f(X)+I=r(X)+I$. The elements of $\mathbb{R}[X]/I$ are of the form $a+bX+I$.

Addition takes the form

$$(a_1+b_1X+I)+(a_2+b_2X+I)=(a_1+a_2)+(b_1+b_2)X+I, \tag{7.2.18}$$

and similarly multiplication is given by ($XI = I$ since I is ideal)

$$\begin{aligned}(a_1 + b_1X + I)(a_2 + b_2X + I) &= a_1a_2 + (b_1a_2 + a_1b_2)X + b_1b_2X^2 + I \\ &= (a_1a_2 - b_1b_2) + (b_1a_2 + a_1b_2)X + I.\end{aligned}$$

This corresponds to addition and multiplication in $\mathbb{C}$. In fact,

$$\begin{aligned}\mathbb{R}[X]/\left\{X^2 + 1\right\} &\cong \mathbb{C}, \\ a + bX + I &\mapsto a + bi.\end{aligned}$$

7.2.4 Isomorphism theorems

Theorem 7.2.12 (first isomorphism theorem)**.** Let $\theta : R \to S$ be a ring homomorphism. Then $\ker\theta \lhd R$, $\operatorname{Im}\theta \leq S$ and $R/\ker\theta \cong \operatorname{Im}\theta$.

Proof. Lemma 7.2.4 states that $\ker\theta$ is an ideal.

Now we show that $\operatorname{Im}\theta$ is a subring of S,

(i) θ is a homomorphism of additive groups and so Lemma 6.1.24 implies that $\operatorname{Im}\theta$ is an additive subgroup of S.

(ii) $\theta(r_1)\theta(r_2) = \theta(r_1r_2) \in \operatorname{Im}\theta$, so we have closure under multiplication. Associativity is inherited from S. Moreover, $\theta(1_R) = 1_S$.

(iii) $\forall s_1, s_2, s_3 \in S$ where $s_1 = \theta(r_1), s_2 = \theta(r_2), s_3 = \theta(r_3)$, $r_1, r_2, r_3 \in R$,

$$s_1(s_2 + s_3) = \theta(r_1)\left(\theta(r_2) + \theta(r_3)\right) = \theta(r_1)\theta(r_2 + r_3) = \theta\left(r_1(r_2 + r_3)\right) \tag{7.2.19}$$

Then by distributivity of ring R,

$$\theta\left(r_1(r_2 + r_3)\right) = \theta(r_1r_2 + r_1r_3) = \theta(r_1r_2) + \theta(r_1r_3) = \theta(r_1)\theta(r_2) + \theta(r_1)\theta(r_3) = s_1s_2 + s_1s_3. \tag{7.2.20}$$

Thus, $s_1(s_2 + s_3) = s_1s_2 + s_1s_3$ and therefore $\operatorname{Im}\theta$ is a subring of R.

Let $\Phi : R/I \to \operatorname{Im}\theta$, $r + I \mapsto \theta(r)$ and note $I = \ker\theta$. We know that Φ is well-defined and bijective and an isomorphism of additive groups from first isomorphism theorem of group (Theorem 6.4.9). It is left to check that Φ is a ring homomorphism.

$$\begin{aligned}\Phi(r_1 + I + r_2 + I) &= \Phi(r_1 + r_2 + I) = \theta(r_1 + r_2) = \theta(r_1) + \theta(r_2) = \Phi(r_1 + I) + \Phi(r_2 + I) \\ \Phi((r_1 + I)(r_2 + I)) &= \Phi(r_1r_2 + I) = \theta(r_1r_2) = \theta(r_1)\theta(r_2) = \Phi(r_1 + I)\Phi(r_2 + I), \\ \Phi(1_R + I) &= \theta(1_R) = 1_S.\end{aligned}$$

Thus Φ is a ring homomorphism. □

Example 7.2.13. The map

$$\theta : \mathbb{R}[X] \to \mathbb{C},\ \sum a_jX^j \mapsto \sum a_ji^j, \quad i^2 = -1 \tag{7.2.21}$$

is a ring homomorphism with $\ker\theta = (X^2 + 1)$ (all the polynomials can be divided by $X^2 + 1$) and $\operatorname{Im}\theta = \mathbb{C}$. (Comparing this with Example 7.2.11)

Theorem 7.2.14 (second isomorphism theorem)**.** Let R be a subring of S and $J \lhd S$ an ideal. Then $R \cap J \lhd S$ is an ideal, $(R + J)/J \leq S/J$ and $\{r + J : r \in R\} = (R + J)/J \leq S/J$ and $R/(R \cap J) \cong (R + J)/J$.

Proof. Let θ be the map

$$\theta : R \to S/J,\ r \mapsto r + J. \tag{7.2.22}$$

Now $\forall r_1, r_2 \in R$,

$$\begin{aligned}\theta(r_1 + r_2) &= r_1 + r_2 + J = r_1 + J + r_2 + J = \theta(r_1) + \theta(r_2) \\ \theta(r_1r_2) &= r_1r_2 + J = r_1r_2 + r_1J + r_2J + J = (r_1 + J)(r_2 + J) = \theta(r_1)\theta(r_2) \quad \text{(since } J \text{ is a ideal)} \\ \theta(1_R) &= 1_R + J = 1_S + J.\end{aligned}$$

Thus, θ is a ring homomorphism. By first isomorphism theorem of ring (Theorem 7.2.12), we have that

$$\begin{aligned}\ker\theta &= \{r \in R : r + J = J\} = R \cap J \lhd R,\\ \operatorname{Im}\theta &= \{r + J : r \in R\} = (R + J)/J \leq S/J.\end{aligned}$$

such that $R/\ker\theta \cong \operatorname{Im}\theta$, that is, $R/(R \cap J) \cong (R + J)/J \leq S/J$. □

Remark. There is a correspondence between additive groups,

$$\{\text{additive subgroups of } R \text{ containing ideal } I\} \longleftrightarrow \{\text{additive subgroups of } R/I\} \tag{7.2.23}$$

as in Proposition 6.4.13. This correspondence induces[2]

$$\{\text{subrings of } R \text{ containing } I\} \longleftrightarrow \{\text{subrings of } R/I\}, \tag{7.2.24}$$

$$\{\text{ideals of } R \text{ containing } I\} \longleftrightarrow \{\text{ideals of } R/I\}. \tag{7.2.25}$$

Theorem 7.2.15 (third isomorphism theorem)**.** Let I and J be ideals of R, with $I \subset J$. Then $(R/I)/(J/I) \cong R/J$ where $J/I = \{r + I : r \in J\}$.

Proof. Let θ be the map

$$\theta : R/I \to R/J,\ r + I \mapsto r + J. \tag{7.2.26}$$

This is well-defined as in Theorem 6.4.14. $\forall r_1 + I, r_2 + I \in R/I$ where $r_1, r_2 \in R$, since I, J are ideals,

$$\begin{aligned}\theta(r_1 + I + r_2 + I) &= \theta(r_1 + r_2 + I) = r_1 + r_2 + J = r_1 + J + r_2 + J = \theta(r_1) + \theta(r_2)\\ \theta((r_1 + I)(r_2 + I)) &= \theta(r_1 r_2 + I) = r_1 r_2 + J = r_1 r_2 + r_1 J + r_2 J + J = (r_1 + J)(r_2 + J) = \theta(r_1 + I)\theta(r_2 + I)\\ \theta(1_R + I) &= 1_R + J.\end{aligned}$$

The first isomorphism theorem of ring (Theorem 7.2.12) implies that $R/\ker\theta \cong \operatorname{Im}\theta \leq R/J$. Noting that

$$\ker\theta = \{r + I : r \in J\} = J/I \lhd R/I, \qquad \operatorname{Im}\theta = R/J, \tag{7.2.27}$$

That is, $(R/I)/(J/I) \cong R/J$. □

Definition 7.2.5. Given a ring R, there is a unique ring homomorphism

$$\phi : \mathbb{Z} \to R,\ 1 \mapsto 1_R,\ m \mapsto \underbrace{1 + \cdots + 1}_{m \text{ times}} \tag{7.2.28}$$

The first isomorphism theorem (Theorem 7.2.12) implies $\mathbb{Z}/\ker\phi \cong \operatorname{Im}\phi \leq R$. $\operatorname{Im}\phi$ is the prime subring[3] of R. $\ker\phi \lhd \mathbb{Z}$ is an ideal and so is of the form $n\mathbb{Z}$ for some n and $\operatorname{Im}\phi \cong \mathbb{Z}/n\mathbb{Z}$.

This n is the characteristic of R.

Remark. If R is one of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ then the characteristic is 0. If $R = \mathbb{Z}/(p\mathbb{Z})$ and p is prime, then the chacteristic is p.

7.3 Integral Domain, Associativity, Irreducibility, Primeness and Field of Fractions

7.3.1 Integral domain

Definition 7.3.1 (zero divisor)**.** A zero divisor a is non-zero and there exists $b \neq 0$ such that $ab = 0$.

[2] This needs to be checked.
[3] need explanation

Definition 7.3.2 (integral domain)**.** A commutative ring is an integral domain if $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$.

Remark. In an integral domain there are no zero divisors.

Example 7.3.1. $\mathbb{Z}$ is an integral domain. All fields are integral domains. Subrings of integral domains are integral domains, e.g. $\mathbb{Z}[i] \leq \mathbb{C}$.

Lemma 7.3.2. Let R be an integral domain and ϕ be a map $\phi : \mathbb{R} \to \mathbb{R}$, $r \mapsto ar$ for $a \neq 0$. Then ϕ is injective.

Proof. If $ar_1 = ar_2$ then $a(r_1 - r_2) = 0$ and so $r_1 - r_2 = 0$, i.e. $r_1 = r_2$.

Note that cancellation is valid in integral domains. □

Lemma 7.3.3. Let R be a finite integral domain. Then R is a field.

Proof. Consider the map $\phi : R \to R$, $r \mapsto ar$, that is, multiplication by $a \neq 0$. Then this map is injective by Lemma 7.3.2. Since $r \mapsto ar$ is injective, the image is at least as big as the domain. Since R is finite the map is also surjective. So the map is bijective. Therefore there exists $r \in R$ with $ar = 1$. Thus a has a multiplicative inverse. So R is a field. □

Lemma 7.3.4. If R is an integral domain then $R[X]$ is an integral domain.

Proof. If

$$f(X) = \sum a_i X^i, \qquad g(X) = \sum b_i X^i \tag{7.3.1}$$

with $\deg f = m$ and $\deg g = n$ then $f(X)g(X)$ has degree $m + n$ since $a_m b_n \neq 0$ as R is an integral domain. Therefore,

$$f(X) \neq 0,\ g(X) \neq 0 \ \Rightarrow\ f(X)g(X) \neq 0. \tag{7.3.2}$$

Thus $R[X]$ is an integral domain. □

Remark. By induction, $R[X_1, \ldots, X_n]$ polynomial ring in indeterminates $X_1, \ldots, X_n$ is an integral domain if R is. This is because $R[X_1, X_2]$ may be regarded as $\langle R[X_1] \rangle [X_2]$.

Proposition 7.3.5. Let R be an integral domain. Then a polynomial in $R[X]$ of degree d can have at most d roots.

Proof. Since R is an integral domain, we have that $R[X]$ is an integral domain (see lemma in notes). Let $f(X) \in R[X]$ with $\deg(f(X)) = d$ and

$$f(X) = \sum_{i=0}^{d} a_i X^i, \quad a_d \neq 0. \tag{7.3.3}$$

If $f(X)$ has no roots, we are done. Suppose a is a root of $f(X)$ then

$$f(X) = (X - a)g(X) \tag{7.3.4}$$

for some $g(X)$. Suppose that

$$g(X) = \sum_{i=0}^{m} b_i X^i. \tag{7.3.5}$$

If $m \geq d$, we have the leading term of $f(X) = (X - a)g(X)$ is $b_m X^{m+1} = 0$ since $\deg(f(X)) = d$. Then we have that

$$b_m X^{m+1} = 0 \ \Rightarrow\ b_m = 0. \tag{7.3.6}$$

since $R[X]$ is an integral domain.

Thus, $m < d$ and thus consider the leading term $f(X)$ which is $b_{d-1} X^d = a_d X^d$, so $b_{d-1} = a_d \neq 0$ since $R[X]$ is integral domain. Thus, $g(X)$ has degree $d - 1$. So apply this method inductively, we have that $f(X)$ has at most d roots. □

Example 7.3.6. Consider $f(X) = X^2 - 1$ in $\mathbb{Z}/8\mathbb{Z}[X]$, we have roots $1, 3, 5, 7$ (more than two roots) as we know that $\mathbb{Z}/8\mathbb{Z}$ is not an integral domain.

7.3.2 Associativity, irreducibility, primeness

Definition 7.3.3 (associativity, irreducibility, primeness)**.** Let R be an integral domain.

An element $a \in R$ is a unit if it has a multiplicative inverse. Equivalently, $\langle a \rangle = aR = R$.

We say a divides b, written $a \mid b$, if there is $c \in R$ such that $b = ac$. Equivalently, $\langle b \rangle \subset \langle a \rangle$, i.e., $bR \subset aR$.

Elements a and b are associates in R if $a = bc$ for some unit $c \in R$. Equivalently, $\langle a \rangle = \langle b \rangle$.

$r \in R$ is irreducible in R if it is non-zero, not a unit and whenever $r = ab$ with $a, b \in R$ then a or b is a unit.

$r \in R$ is prime in R if it is non-zero, not a unit and if $r \mid ab$ then $r \mid a$ or $r \mid b$.

Remark. These definitions do depend on the ring R.

2 is prime and irreducible in $\mathbb{Z}$, but not in $\mathbb{Q}$.

$2X$ is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$, as $2X = 2 \cdot X$ and 2, X are not units in $\mathbb{Z}[X]$.

Lemma 7.3.7. Let R be an integral domain. If r is prime in R then r is irreducible in R.

Proof. Suppose that r is prime in R and $r = ab$ with $a, b \in R$. Then $r \neq 0$ and $r|ab$ and so $r|a$ or $r|b$ by Definition of primeness. Without loss of generality suppose $r|a$. So $a = qr$ for some $q \in R$. So $r = ab = qrb$. Cancellation in integral domains gives $1 = qb$, so b is a unit. □

Definition 7.3.4 (norm)**.** A norm of element z of ring over $\mathbb{C}$ is $N(z) = z\bar{z}$. N is multiplicative, that is, $N(z_1 z_2) = N(z_1)N(z_2)$.

Example 7.3.8. Let R be an integral domain. To show that the converse of Lemma 7.3.7 does not hold in general, consider $R = \mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$. R is an integral domain since it is a subring of a field. Define a norm,

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}_{\geq 0}. \tag{7.3.7}$$

Suppose z is a unit and so there exists $z_1 \in R$ with $zz_1 = 1$ so $N(z)N(z_1) = N(zz_1) = N(1) = 1$ hence $N(z)$ is a unit in Z and also $N(z) \geq 0$. So $N(z) = 1$ is the only possibility. Thus, the units of R are precisely the elements of norm 1, namely ± 1. There are no elements in R of norm 2 or 3. (since we cannot solve $a^2 + 5b^2 = 2$ or 3.)

Consider the identity $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in R.

To see that 2 is irreducible, express $2 = z_1 z_2$ and consider norms, $4 = N(z_1)N(z_2)$. Since there are no elements of norm 2 one of the $N(z_j) = 1$ so z_j is a unit.

But 2 is not prime in R since $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 does not divide either $1 \pm \sqrt{-5}$. (Consider norms, $N(2) = 4$, $N(1 \pm \sqrt{-5}) = 6$ and $4 \nmid 6$.)

Similarly, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible.

7.3.3 Field of fractions

Theorem 7.3.9 (field of fractions)**.** Let R be an integral domain. Then there is a field $\mathbb{F}$ with the properties

(i) $R \leq \mathbb{F}$ is a subring,

(ii) every element of $\mathbb{F}$ has the form ab^{-1} where $a \in R$ and b^{-1} is the multiplicative inverse in $\mathbb{F}$ of $b \in R$.

The field $\mathbb{F}$ is called of field of fractions.

Example 7.3.10. With the notation as above, $R = \mathbb{Z}$, $\mathbb{F} = \mathbb{Q}$.

Proof. Consider pairs (a, b) with $a \in R$, $b \in R$ and $b \neq 0$. Define an equivalence relation[4]

$$(a, b) \sim (c, d) \;\Leftrightarrow\; ad = bc. \tag{7.3.8}$$

(For transitivity, note that

$$\begin{array}{l} (a, b) \sim (c, d) \;\Leftrightarrow\; ad = bc \\ (c, d) \sim (e, f) \;\Leftrightarrow\; cf = de \end{array} \quad \Rightarrow\; adf = bcf = bde \tag{7.3.9}$$

as cancellation is valid in R (integral domain). So $af = be$ (since multiplication is commutative) and $(a, b) \sim (e, f)$.)

[4] need quote

Write a/b for the equivalence class of (a, b). We define addition by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{7.3.10}$$

and multiplication by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{7.3.11}$$

One can easily check that these operations are well-defined[5].

If we let $\mathbb{F} = \{a/b : a \in R, b \in R, b \neq 0\}$ then $\mathbb{F}$ is a ring under these operations.

R may be identified with the subring of elements of the form $r/1$. The multiplicative identity is $1/1$. a/b has multiplicative inverse b/a if $a \neq 0$,

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}. \tag{7.3.12}$$

Thus, $\mathbb{F}$ is a field. Every element a/b is of the form $(a/1)(b/1)^{-1}$ since $(b/1)^{-1} = 1/b$. □

7.4 Principal Ideal Domain, Maximal Ideal and Prime Ideal

7.4.1 Principal ideal domain

Definition 7.4.1 (principal ideal domain)**.** A principal ideal domain (PID) is an integral domain in which all ideals are principal ideals, i.e. of the form $\langle a \rangle = aR$ for some $a \in R$.

Proposition 7.4.1. Let R be any commutative ring. Show that the ring $R[X]$ is a PID if and only if R is a field.

Proof. ($\Leftarrow$). Suppose R is a field and for any $I \lhd R[X]$, we take $f \in I$ with the least degree, then for any $g \in I$, by Euclidean algorithm for polynomials (Proposition 7.2.10), we can find $q(X)$ and $r(X) \in I$,

$$g(X) = q(X)f(X) + r(X) \tag{7.4.1}$$

with $\deg r < \deg f$. Since f has the least degree, we have $r = 0$ and for any $g(X) \in I$, $f(X) | g(X)$. Thus, $I = \langle f(X) \rangle$. Thus, $R[X]$ is PID.

($\Rightarrow$). Suppose $R[X]$ is a PID, for any $a \in R$, we construct $I = \langle a, X \rangle$ for $a \neq 0 \in R$. Also, we can find $b \in R$ such that $I = \langle b \rangle$ since $R[X]$ is PID. Thus, we can find $f(X) = a_0 + a_1X + \cdots \in R[X], a_0, a_1, \cdots \in R$ such that

$$bf = a + X \;\Rightarrow\; b(a_0 + a_1X + \dots) = a + X \;\Rightarrow\; ba_1 = 1. \tag{7.4.2}$$

So b is a unit. So $1 \in bR[X] = \langle b \rangle = \langle a, X \rangle$. Thus, there exist $g(X), h(X) \in R[X]$, $g(X) = c_0 + c_1X + \dots, c_0, c_1, \cdots \in R$

$$ag(X) + Xh(X) = 1 \;\Rightarrow\; ac_0 = 1. \tag{7.4.3}$$

Thus, a is unit. Therefore, this can be done for any a, so R is a field. □

Proposition 7.4.2. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are all PIDs.

Proof. [6] □

Example 7.4.3. $\mathbb{Z}[X]$ is not a PID. It is obvious that $\mathbb{Z}$ is not a field, then $\mathbb{Z}[X]$ is not a PID by Proposition 7.4.1.

Now we want to prove it by checking the definition of PID.

Consider the ideal $I = \langle 2, X \rangle = \left\{a_iX^i : a_0 \text{ is even}\right\} \lhd \mathbb{Z}[X]$. Suppose that $I = \langle f(X) \rangle$ for some $f(X) \in \mathbb{Z}[X]$.

We have $f(X) \mid 2$ and $f(X) \mid X$ since $2, X \in I$. In particular $2 = f(X)g(X)$ for some $g(X) \in \mathbb{Z}[X]$. We deduce that $f(X)$ has to be a constant polynomial, that is, of degree 0, and must be ± 1 or ± 2. Also $X = f(X)h(X)$ for some $h(X) \in \mathbb{Z}[X]$. So $f(X)$ cannot be ± 2. So $f(X) = \pm 1$. Hence $I = \langle f(X) \rangle = \mathbb{Z}[X]$.

This is a contradiction, since $I \neq \mathbb{Z}[X]$ (I has even coefficients).

[5] need to check

[6] need details

Example 7.4.4 (minimal polynomials of matrices with entries in a field $\mathbb{F}$)**.** Let $\triangle \in M_{n\times n}(\mathbb{F})$. Consider $I = \{f(X) \in \mathbb{F}[X] : f(\triangle) = 0\}$.

We can check that $I \lhd \mathbb{F}[X]$ is an ideal[7]. But $\mathbb{F}[X]$ is a PID, so $I = \langle m(X)\rangle$, and by multiplying $m(X)$ by a unit in $\mathbb{F}$ we may assume $m(X)$ is monic. This is the minimal polynomial of $\triangle$. (See the course Linear Algebra (Chapter 8[8]) where Euclidean algorithm (Proposition 7.2.10) is explicitly used.)

Lemma 7.4.5. Let R be a PID. If p is an irreducible then it is prime. (This is the converse of Lemma 7.3.7 for PIDs.)

Proof. Let p be an irreducible and suppose $p|ab$. Without loss of generality, suppose that $p \nmid a$. The ideal (p, a) must be principle in a PID, $\langle p, a\rangle = \langle d\rangle$, say.

Thus $p = q_1 d$ and $a = q_2 d$ for some $q_1, q_2 \in R$. p is irreducible so either q_1 or d is a unit. But if q_1 is a unit, then $d = q_1^{-1}p$ and $a = q_2 d = q_2 q_1^{-1} p$, so $p|a$, a contradiction. Hence d is a unit. Thus $\langle d\rangle = dR = R$ since d is unit and there exist $r, s \in R$ such that (since $\langle p, a\rangle = \langle d\rangle$),

$$1 = rp + sa \;\Rightarrow\; b = rpb + sab. \tag{7.4.4}$$

Since $p \mid rpb$ and $p \mid ab$, $p|b$. □

Remark. In fact, d is a highest common factor of p and a (see Definition 7.7.2). Highest common factors are unique up to units (see Proposition 7.7.5).

7.4.2 Maximal ideal and prime ideal

Definition 7.4.2 (proper ideal)**.** A proper ideal is an ideal I of a ring R which is strictly smaller than the whole ring, i.e., $I \subset R (I \neq R)$.

Definition 7.4.3 (maximal ideal)**.** An proper ideal I in R is maximal in R whenever $I \subseteq J \lhd R$ then $I = J$ or $J = R$.

Example 7.4.6. In $\mathbb{Z}$, the maximal ideals are $p\mathbb{Z}$ where p is a prime number.

Definition 7.4.4 (prime ideal)**.** A proper ideal is a prime ideal in R if whenever $ab \in I$ then $a \in I$ or $b \in I$.

Remark. This generalizes the following property of prime numbers: if p is a prime number and if p divides a product ab of two integers, then p divides a or p divides b. We can therefore say, a positive integer n is a prime number if and only if the ideal $n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Example 7.4.7. In $\mathbb{Z}$, the prime ideals are $p\mathbb{Z}$ for prime number p and $\{0\}$.

Lemma 7.4.8. Let R be a commutative ring. For an ideal $I \lhd R$, the quotient ring R/I is a field if and only if I is maximal in R.

Example 7.4.9. $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements where p is a prime number. $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. R/I is a field if and only if $\{0\} = I/I$ and R/I are the only ideals in R/I (by Lemma 7.2.3). By the usual correspondence, this is equivalent to that the only ideals in R containing I are I and R, which is the statement that I is maximal in R. □

Lemma 7.4.10. Let R be a commutative ring. For an ideal $I \lhd R$, the quotient ring R/I is an integral domain if and only if I is a prime ideal in R.

Proof. Note that zero in R/I is $0 + I = I$.

Suppose R/I is an integral domain and $ab \in I$. Then $0 + I = I = ab + I = (a + I)(b + I)$ and so either $a + I = 0 + I = I$ or $b + I = 0 + I = I$. So $a \in I$ or $b \in I$.

Conversely, suppose I is a prime deal and $(a + I)(b + I) = I$. Then $ab + I = I$ and so $ab \in I$. Primeness implies $a \in I$ or $b \in I$ and so $a + I = I = 0 + I$ or $b + I = 0 + I$. □

Theorem 7.4.11. Let R be a commutative ring. For an ideal $I \lhd R$, if I is a maximal ideal, then it is also a prime ideal.

Remark. This can be seen directly by Lemma 7.4.10 and Lemma 7.4.8 as we can see that a field is an integral domain.

[7] need details
[8] check section number

Proof. Assume there exist a, b such that $ab \in I$ but $a, b \in R \backslash I$. Now let J be the ideal generated by $I \cup \{a\}$, i.e.,

$$J = \{x + ar : x \in I, r \in R\}. \tag{7.4.5}$$

Clearly, $I \subset J$ ($I \subsetneq J$) as we can take $r = 1$. Thus, since I is maximal, we have $J = R$. Therefore, $1 \in J$ and hence there exist $x \in I$ and $r \in R$ such that

$$1 = x + ar. \tag{7.4.6}$$

Then we have

$$b = b \cdot 1 = b(x + ar) = \underbrace{bx}_{\in I} + \underbrace{(ab)r}_{\in I} \in I. \tag{7.4.7}$$

Contradiction with the assumption that $b \in R \backslash I$. □

Theorem 7.4.12. Let R be a PID. For an ideal $I \lhd R$, if I is a non-zero prime ideal, then it is a maximal ideal.

Proof. If I is non-zero prime, then we assume that $I \subseteq J \lhd R$. Since R is a PID, we assume that $I = \langle a \rangle$ and $J = \langle b \rangle$. Thus, $a \in J$.

Then we have $c \in R$ such that $a = bc$. Since I is prime, we have that $a \in I \Rightarrow b \in I$ or $c \in I$.

If $b \in I$, we have $I = \langle b \rangle = J$. If $c \in I$, we have $d \in R$, such that $c = ad = bcd \Rightarrow 1 = bc$. Thus, b is a unit and by Definition 7.3.3, $R = \langle b \rangle = J$.

Thus, either $I = J$ or $J = R$. Therefore, I is a maximal ideal. □

Theorem 7.4.13. In PID, maximal ideal and non-zero prime ideal are equivalent.

Proof. Direct result by Theorem 7.4.11 and Theorem 7.4.12. □

Lemma 7.4.14. Let R be an integral domain. $\langle r \rangle$ is a prime ideal of R if and only if r is prime or $r = 0$.

Proof. If $r \neq 0$ and $r \mid ab$ then $ab \in \langle r \rangle$ and so if $\langle r \rangle$ is a prime ideal then $a \in \langle r \rangle$ or $b \in \langle r \rangle$. Thus $r \mid a$ or $r \mid b$. Thus, r is prime.

If r is unit, by Definition 7.3.3, $\langle r \rangle = R$. Contradiction to Definition 7.4.4.

$\langle 0 \rangle$ is a prime ideal in an integral domain.

Conversely, if r is prime and $ab \in \langle r \rangle$ then $r \mid ab$ and hence $r \mid a$ or $r \mid b$. Thus $a \in \langle r \rangle$ or $b \in \langle r \rangle$. Thus, $\langle r \rangle$ is a prime ideal of R. □

Lemma 7.4.15. The characteristic of an integral domain R is 0 or a prime number p.

Proof. Recall that we have a unique ring homomorphism $\phi : \mathbb{Z} \to R$ (Definition 7.2.5). The prime subring $\operatorname{Im} \phi \cong \mathbb{Z}/n\mathbb{Z}$, where n is the characteristic of R.

If n properly factorises as $n = st$ then working modulo n we have $st = 0 \pmod n$ and so we have zero divisors. Contradiction to the fact that R is an integral domain (by Definition 7.3.1 and Definition 7.3.2).

So if R is an integral domain, its prime subring is an integral domain and so n is prime or 0. □

7.5 Euclidean Domain

Definition 7.5.1 (Euclidean domain)**.** An integral domain R is a Euclidean domain (ED) if there is a function $\phi : R \backslash \{0\} \to \mathbb{Z}^+$ called Euclidean function such that

(i) $\phi(ab) \geq \phi(a)$ for all $a, b \in R \backslash \{0\}$,

(ii) if $a, b \in R$ with $b \neq 0$ then there exist $q, r \in R$ with $a = qb + r$ with either $r = 0$ or $\phi(r) < \phi(b)$.

Proposition 7.5.1. Let $\mathbb{F}$ be a field. Then $\mathbb{F}[X]$ is a Euclidean domain[9].

Proof. Let Euclidean function be $\phi(f(X)) = \deg f$. To check Definition 7.5.1,

(i) It is obvious.

[9] This is given in proof of Proposition 7.4.1

(ii) It is given by Euclidean algorithm (Proposition 7.2.10).

Thus, $\mathbb{F}[X]$ is a ED. □

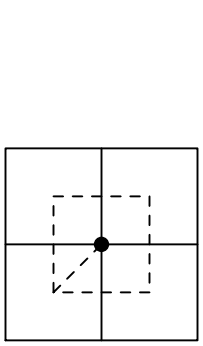
Example 7.5.2. (i) $\mathbb{Z}$ is a Euclidean domain with $\phi(n) = |n|$.

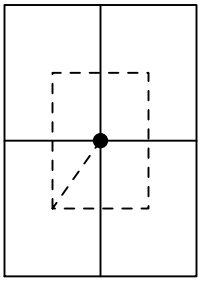
(ii) $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ is a Euclidean domain. As with $\mathbb{Z}[\sqrt{-5}]$ we can define a norm via $N(z) = z\bar{z}$ for $z \in R$. Thus $N(a + bi) = a^2 + b^2$. In this case the norm is a Euclidean function. N is multiplicative and so property (i) holds, $N(z_1z_2) = N(z_1)N(z_2) \geq N(z_1)$, since $N(z_2) \geq 1$.

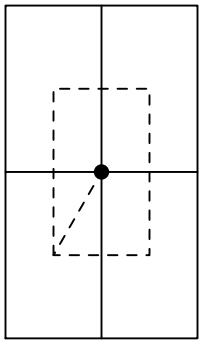
To verify property (ii) take $z_1, z_2 \in R$ with $z_2 \neq 0$. Consider $z_1/z_2 \in \mathbb{C}$. Then in the complex plane it is distance less than $\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{2}/2$ from the nearest element of R.

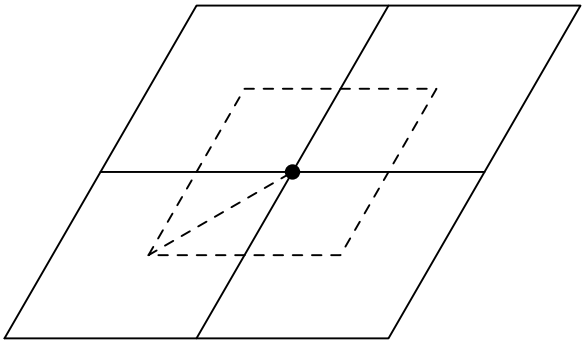
$z_1/z_2 = q + z_3$ with $q \in R$, $z_3 \in \mathbb{C}$ and $|z_3| < 1$. So $z_1 = qz_2 + z_2z_3$. Set $r = z_2z_3$. Thus $z_1 = qz_2 + r$,

$$N(r) = |z_2z_3|^2 = |z_2|^2|z_3|^2 < |z_2|^2 = N(z_2). \tag{7.5.1}$$


$\mathbb{Z}[i]$


$\mathbb{Z}[\sqrt{-2}]$


$\mathbb{Z}[\sqrt{-3}]$


$\mathbb{Z}[\omega]$, $\omega = (1 + \sqrt{-3})/2$

(iv) For $R = \mathbb{Z}[\sqrt{-2}]$, with similar arguments, property (i) holds, for any $z_1/z_2 \in \mathbb{C}$, the longest distance to its nearest point of lattice is $\sqrt{\left(\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{3}/2 < 1$. Thus $|z_3| < 1$ also holds. Hence, $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

(v) For $R = \mathbb{Z}[\sqrt{-3}]$, with similar arguments, property (i) holds, for any $z_1/z_2 \in \mathbb{C}$, the longest distance to its nearest point of lattice is $\sqrt{\left(\frac{\sqrt{3}}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = 1$. So $|z_3| < 1$ doesnt't hold. Hence, we cannot say that $\mathbb{Z}[\sqrt{-3}]$ is a Euclidean domain. Actually, we will see later that $\mathbb{Z}[\sqrt{-3}]$ is not a Euclidean domain since it is not UFD (see Example 7.7.1).

(vi) Similarly, we will see later that $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain since it is not UFD (see Example 7.7.1).

(vii) For $R = \mathbb{Z}[\omega]$, $\omega = (1+\sqrt{-3})/2$. With similar arguments, property (i) holds, for any $z_1/z_2 \in \mathbb{C}$, the longest distance to its nearest point of lattice is $\sqrt{\left(\frac{\sqrt{3}}{4}\right)^2 + \left(\frac{1}{2} + \frac{1}{4}\right)^2} = \sqrt{3}/2 < 1$. Thus $|z_3| < 1$ also holds. Hence, $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

Proposition 7.5.3. The subring $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{R}$ is a Euclidean domain. Its units are $\pm(1 \pm \sqrt{2})^n$ for $n \geq 0$.

Proof. For $a, b \in \mathbb{Z}$, we define a function

$$\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}^+,\ a + b\sqrt{2} \mapsto \left|\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)\right| = \left|a^2 - 2b^2\right|. \tag{7.5.2}$$

Then for $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,

$$\begin{aligned}
\phi\left(\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right)\right) &= \phi\left(ac + 2bd + (ad + bc)\sqrt{2}\right) = \left|(ac + 2bd)^2 - 2(ad + bc)^2\right| \\
&= \left|a^2c^2 + 4b^2d^2 + 4abcd - 2a^2d^2 - 2b^2c^2 - 4abcd\right| = \left|(a^2 - 2b^2)(c^2 - 2d^2)\right| \\
&= \left|a^2 - 2b^2\right|\left|c^2 - 2d^2\right| = \phi(a + b\sqrt{2})\phi(c + d\sqrt{2}).
\end{aligned}$$

Also, since $a, b \in \mathbb{Z}$

$$\phi(a + b\sqrt{2}) = \left|a^2 - 2b^2\right| \geq 1 \text{ if } a + b\sqrt{2} \neq 0. \tag{7.5.3}$$

So we have for $x, y \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$,

$$\phi(xy) \geq \phi(x). \tag{7.5.4}$$

Now we need to prove that if $a, b \in \mathbb{Z}[\sqrt{2}]\setminus\{0\}$ with $b \neq 0$, $\exists q, r \in \mathbb{Z}[\sqrt{2}]$ s.t.

$$a = bq + r, \quad \text{with either } r = 0 \text{ or } \phi(r) < \phi(b). \tag{7.5.5}$$

Given a, b, if $b \mid a$, i.e. $a = bx$ for some $x \in \mathbb{Z}[\sqrt{2}]$, we have that $r = 0$. Otherwise, we can find some $s, t \in \mathbb{R}$ such that

$$a/b = s + t\sqrt{2}. \tag{7.5.6}$$

Then we can find $x, y \in \mathbb{Z}$ such that $|x - s| \leq \frac{1}{2}$ and $|y - t| \leq \frac{1}{2}$. Let

$$q = x + y\sqrt{2} \;\Rightarrow\; a = b(x + y\sqrt{2}) + \underbrace{b(s - x)}_{\in\mathbb{Z}} + \underbrace{b(t - y)}_{\in\mathbb{Z}}\sqrt{2} \tag{7.5.7}$$

with $r = b(s - x) + b(t - y)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and

$$\phi(r) = \phi(b)\left|(s - x)^2 - 2(t - y)^2\right| \leq \phi(b)\left|(s - x)^2 + 2(t - y)^2\right| \leq \phi(b)\left|\frac{1}{4} + 2\frac{1}{4}\right| = \frac{3}{4}\phi(b) < \phi(b) \tag{7.5.8}$$

since $b \neq 0$. Thus, ϕ is an Euclidean function and $\mathbb{Z}[\sqrt{2}]$ is an Euclidean domain.

If x is a unit in $\mathbb{Z}[\sqrt{2}]$, then we have that $\exists y \in \mathbb{Z}[\sqrt{2}]$ such that $xy = 1$ and thus $\phi(x)\phi(y) = 1$. Since $\phi(x), \phi(y) \geq 1$, we have that $\phi(x) = 1$.

Since $\sqrt{2} - 1 = 1/(1 + \sqrt{2})$, we can consider $1 + \sqrt{2}$ only. Now we want to find all the units bigger than 1.

First we prove that $1 + \sqrt{2}$ is actually the smallest unit bigger than 1.

Let $a, b \in \mathbb{N}$. If the smallest unit bigger than 1 is of the form $a - b\sqrt{2} > 1$, then $a + b\sqrt{2} > 1$. However,

$$1 = \phi(a - b\sqrt{2}) = \left|\left(a - b\sqrt{2}\right)\left(a + b\sqrt{2}\right)\right| > |1| = 1. \text{ (Contradiction.)} \tag{7.5.9}$$

Similarly, If the smallest unit bigger than 1 is of the form $-a + b\sqrt{2} > 1$, then $a + b\sqrt{2} > 1$. This will lead to the contradiction again.

Thus, it has to be of the form $a + b\sqrt{2}$. Thus, the smallest unit bigger than 1 is $1 + \sqrt{2}$.

Clearly, the power of $1 + \sqrt{2}$ are units. If there exists any unit between $\left(1 + \sqrt{2}\right)^n$ and $\left(1 + \sqrt{2}\right)^{n+1}$ with integer n (positive or negative), say u,

$$\left(1 + \sqrt{2}\right)^n < u < \left(1 + \sqrt{2}\right)^{n+1} \;\Rightarrow\; 1 < u\left(1 + \sqrt{2}\right)^{-n} < 1 + \sqrt{2}. \tag{7.5.10}$$

Obviously, $u\left(1 + \sqrt{2}\right)^{-n}$ is a unit since u^{-1} and $\left(1 + \sqrt{2}\right)^n$ are units. However, $1 + \sqrt{2}$ is the smallest unit bigger than 1. This leads to contradiction. Thus, there is no other unit bigger than 1 besides $(1 + \sqrt{2})^n$ with $n \in \mathbb{N}$. □

Proposition 7.5.4. A field $\mathbb{F}$ is also an ED (Euclidean domain).

Proof. Let $\phi(x) = 1$ for any non-zero element x. Clearly, this function satisfies (i) of Definition 7.5.1.

Also for $a, b \in \mathbb{F}$, $1/b \in \mathbb{F}$ and there exists $q = a/b \in \mathbb{F}$ such that $a = qb$ which satisfies (ii) of Definition 7.5.1. □

Proposition 7.5.5. If an integral domain R is an ED (Euclidean domain) then R is a PID (principal ideal domain).

Proof. Let R be an ED (therefore an integral domain) with Euclidean function $\phi : R\setminus\{0\} \to \mathbb{Z}^+$.

Let I/R be an ideal and suppose that I is non-zero. Pick $b \in I\{0\}$ with $\phi(b)$ minimal. Then $\forall a \in I$ and use Euclidean algorithm (Proposition 7.2.10): $a = bq + r$ with $r = 0$ or $\phi(r) < \phi(b)$.

Note that $r = a - bq \in R$, and hence minimality of $\phi(b)$ implies $r = 0$. Thus $a = bq$, so $I = \langle b\rangle$. Thus all ideals are prime ideals and therefore R is a PID (by Definition 7.4.1). □

7.6 Ascending Chain Condition and Hilbert's basis theorem

7.6.1 Ascending chain condition

Definition 7.6.1 (ascending chain condition)**.** Let R be a (not necessarily commutative) ring. We say that R satisfies the ascending chain condition[10] (ACC) if for $I_j \lhd R$ with $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$, there exists some $n \in \mathbb{N}$ such that $I_n = I_{n+i}$ for all $i \geq 0$.

Definition 7.6.2 (Noetherian ring)**.** Rings satisfying the ACC are called Noetherian rings (Named after Emmy Noether).

Lemma 7.6.1. Let R be a PID and $I_j \lhd R$ with $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$. Then, R satisfies ACC.

Proof. By Proposition 7.2.6, $I = \bigcup_j I_j \lhd R$. Since R is a PID, $I = \langle a \rangle$ for some $a \in I$. We must have $a \in I_n$ for some $n \in \mathbb{N}$. For all $i \geq 0$,

$$\langle a \rangle \subseteq I_n \subseteq I_{n+i} \subseteq \cdots \subseteq I \subseteq \langle a \rangle , \tag{7.6.1}$$

so we have equality throughout and in particular $I_{n+i} = I_n$. □

Lemma 7.6.2. A ring R is Noetherian if and only if all ideals in R are finitely generated.

Proof. Suppose that all ideals are finitely generated and consider a chain

$$I_1 \subseteq I_2 \subseteq \dots \tag{7.6.2}$$

with $I_j \lhd R$. Then the union $\bigcup_j I_j \lhd R$ is an ideal too (by Proposition 7.2.6). So by supposition $\bigcup_j I_j$ is finitely generated. There exists N such that all these finitely many generators lie in I_N.

If $m \geq N$ then $I_m \subseteq \bigcup_j I_j \subseteq I_N$. Also $I_N \subset I_m$ and so $I_m = I_N$.

Conversely, assume the ACC and let $J \lhd R$. Take $a_1 \in J$ with $a_1 \neq 0$. If $J \neq \langle a_1 \rangle$ (i.e. $\langle a_1 \rangle \subsetneq J$ since $a_1 r \in J$ for any $r \in R$ with the definition of ideal) pick $a_2 \in J \backslash \langle a_1 \rangle$. If $J \neq \langle a_1, a_2 \rangle$ (i.e., $\langle a_1, a_2 \rangle \subsetneq J$ since $a_1 r_1 + a_2 r_2 \in J$ for any $r_1, r_2 \in R$ with the definition of ideal) pick $a_3 \in J \backslash \langle a_1, a_2 \rangle$ etc. We are producing a chain

$$\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots . \tag{7.6.3}$$

By the ACC this process stops, so $J = \langle a_1, \dots, a_N \rangle$ for some N. □

Remark. For a commutative ring to be Noetherian it suffices that every prime ideal of the ring is finitely generated. (The result is due to I. S. Cohen.)[11]

7.6.2 Hilbert's basis theorem

Theorem 7.6.3 (Hilbert's basis theorem)**.** If the commutative ring R is Noetherian then $R[X]$ is Noetherian.

Proof. Let $J \lhd R[X]$ be an ideal. We aim to show that it is finitely generated. Consider

$$I_j = \left\{ a_j \in R : \exists f(X) \in J,\ f(X) = \sum_{i=0}^{j} a_i X^i \in J \right\} \cup \{0\}, \tag{7.6.4}$$

the set of leading coefficients of polynomials of degree j in J.

$I_j \lhd R$ is an ideal since if $\sum_{i=0}^{j} a_i X^i \in J$, $\sum_{i=0}^{j} b_i X^i \in J$ then

$$\sum_{i=0}^{j} (a_i + b_i) X^i \in J \tag{7.6.5}$$

and if $a \in R$ then $\sum_{i=0}^{j} a a_i X^i \in J$. $I_j \subseteq I_{j+1}$ since if $\sum_{i=0}^{j} a_i X^i \in J$ then $X \left(\sum_{i=0}^{j} a_i X^i \right) \in J$.

The ACC for R implies that there exists N with $I_m = I_N$ for all $m \geq N$ and I_N is finitely generated by the leading coefficients of $f_1(X), \dots, f_k(X)$, say (by Definition 7.6.1 and 7.6.2).

[10] need general definition, also need DCC

[11] need details

Now take any $f(X) \in J$ of degree $m \geq N$. The leading coefficient of $f(X)$ lies in $I_m = I_N$ and so there exists $r_1, \ldots, r_k \in R$ so that $r_1 f_1(X) + \cdots + r_k f_k(X)$ has the same leading coefficient. So

$$f(X) - (r_1 f_1(X) + \cdots + r_k f_k(X))X^{m-N} \in J \tag{7.6.6}$$

and is of degree less than m. Repeating this process yields $q_1(X), \ldots, q_k(X) \in R[X]$ such that

$$f(X) - (q_1(X) f_1(X) + \cdots + q_k(X) f_k(X)) \in J \tag{7.6.7}$$

of degree less than N.

Now consider polynomials in J of degree less than N. For $j < N$ there is a finite set S_j of polynomials in J of degree j whose leading coefficients generate I_j (I_j is finitely generated since R is Noetherian by Lemma 7.6.2). Let $S = \bigcup_{j<N} S_j$, a finite set (union of finitely many finite sets).

A similar argument to the one before shows that any polynomial in J of degree less than N is of the form $\sum g_i(X)h_i(X)$ for $g_i(X) \in S$, $h_i(X) \in R[X]$.

Thus J is generated by $S \cup \{f_1(X), \ldots, f_k(X)\}$. □

Corollary 7.6.4. If $\mathbb{F}$ is a field then $\mathbb{F}[X_1, \ldots, X_n]$ is Noetherian.

Proof. $\mathbb{F}$ is field and thus it is PID. So $\mathbb{F}$ is Noetherian by Lemma 7.6.1. Hence $\mathbb{F}[X]$ is Noetherian by Hilbert's basis theorem (Theorem 7.6.3). Then apply Hilbert's basis theorem (Theorem 7.6.3) repeatedly, we have that $\mathbb{F}[X_1, \ldots, X_n]$ is Noetherian. □

Corollary 7.6.5. $\mathbb{Z}[X_1, \ldots, X_n]$ is also Noetherian.

Proof. $\mathbb{Z}$ is ED. Then $\mathbb{Z}$ is PID and thus $\mathbb{Z}$ is Noetherian by Lemma 7.6.1. Hence $\mathbb{Z}[X]$ is Noetherian by Hilbert's basis theorem (Theorem 7.6.3). Then apply Hilbert's basis theorem (Theorem 7.6.3) repeatedly, we have that $\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian. □

Corollary 7.6.6. Any ring image of $\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian.

Proof. Let $\theta : \mathbb{Z}[X_1, \ldots, X_n] \to S$ be a homomorphism. Then θ is surjective (since it is image of ring). If $I \lhd S$ is an ideal then

$$J = \{f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n] : \theta(f(X_1, \ldots, X_n)) \in I\} \tag{7.6.8}$$

is finitely generated. Then I is generated by the images under θ of a finite generating set of J. □

7.7 Unique Factorisation Domain

7.7.1 Unique factorisation domain

Definition 7.7.1 (Unique factorisation domain)**.** An integral domain is a unique factorisation domain (UFD) if

(i) every non-zero element that is not a unit may be expressed as a product of finitely many irreducibles,

(ii) whenever $p_1 \ldots p_m = q_1 \ldots q_n$ for products of irreducibles then $m = n$ and we can reorder so that p_i is an associate of q_i. (So factorisation is unique up to ordering and associates).

Example 7.7.1. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Note that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{7.7.1}$$

where 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducibles (see Example 7.3.8). Units are ± 1 in $\mathbb{Z}[\sqrt{-5}]$, so these irreducibles are not associates of each other.

Proposition 7.7.2. If an integral domain R is a PID then R is a UFD.

Proof. (i) Let $a \in R$, non-zero and not a unit. Assume it cannot be factorised as a product of finitely many irreducibles. So in particular a itself is not irreducible (otherwise it is a product of finitely many irreducibles), hence $a = a_1 b_1$ with a_1, b_1 non-zero and not units (by definition of irreducible element). We may assume that a_1 cannot be factorised as a product of finitely many irreducibles, so write $a_1 = a_2 b_2$ and continue. (If both a_1, b_1 can be factorised into finitely many irreducibles, then so can a.)

So we have that $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \dots$ in PID. Thus, by Lemma 7.6.1, there exists $n \in \mathbb{N}$ such that for all $i \geq 0$, $\langle a_n \rangle = \langle a_{n+i} \rangle$. In particular, $\langle a_n \rangle = \langle a_{n+1} \rangle$, then a_n and a_{n+1} would be associates and b_{n+1} a unit. Contradiction.

(ii) Suppose we have $p_1 \dots p_m = q_1 \dots q_n$ with products of irreducibles. Then p_1 is prime by Lemma 7.4.5 and $p_1 | q_1 \dots q_n$, so p_1 divides one of the q_i (by Definition 7.3.3), $p_1 | q_1$, say, and so $q_1 = p_1 u$. But q_1 is irreducible and p_1 is not a unit, hence u is a unit (by Definition 7.3.3). This is to say p_1 and q_1 are associates. We have (cancellation in R)

$$p_1 \dots p_m = u p_1 q_2 \dots q_n \;\Rightarrow\; p_1 (p_2 \dots p_m - u q_2 \dots q_n) = 0 \;\Rightarrow\; p_2 \dots p_m = u q_2 \dots q_n \tag{7.7.2}$$

Note that (uq_2) is irreducible. Continuing in this way gives the result.

□

Corollary 7.7.3. $\mathbb{Z}$, $\mathbb{F}[X]$ for a field $\mathbb{F}$ and $\mathbb{Z}[i]$ are all UFDs.

Proof. Direct result from Proposition 7.4.2 and Proposition 7.7.2. □

Remark. The proof of (ii) depends just on Lemma 7.4.5, that irreducibles are prime, and (i) depends on the ACC.

There are several properties which follow quickly from the definition of a UFD.

Proposition 7.7.4. Let R be a UFD. An element $p \in R$ is irreducible if and only if it is prime.

Proof. We have already shown the 'only if' direction for integral domains in Lemma 7.3.7.

Suppose p is an irreducible and $p \mid ab$. We have a, b are non-zero (otherwise p is zero). If a or b is a unit, wlog, a is, say. Then $cp = ab$ for some $c \in R$. Then $b = a^{-1} cp$ since a is unit, so $p \mid b$. Thus, $p \mid a$ or $p \mid b$ and therefore p is prime.

If a and b are not units, we can express a and b as

$$a = p_1 \dots p_m, \quad b = q_1 \dots q_n \tag{7.7.3}$$

with p_i, q_i irreducible. Now write $ab = pc$ with $c = r_1 \dots r_s$ where r_i is irreducible. Then

$$(p_1 \dots p_m)(q_1 \dots q_n) = p r_1 \dots r_s \tag{7.7.4}$$

and uniqueness of factorisation (Definition 7.7.1.(ii)) implies that p is an associate of either some p_i or some q_i. Thus, $u_p p = p_i$ or $u_q p = q_i$ where u_p, u_q are units. So

$$a = p_1 \dots p_m = u_p p \cdot (\cdot) \quad \text{or} \quad b = q_1 \dots q_n = u_q p \cdot (\cdot). \tag{7.7.5}$$

Hence $p \mid a$ or $p \mid b$ and therefore p is prime. □

7.7.2 Highest common factor

Definition 7.7.2 (Highest common factor)**.** d is a highest common factor of $a_1, \dots, a_n$, written $\mathrm{hcf}(a_1, \dots, a_n)$, if $d | a_i$ for each i and whenever d' also divides each a_i then $d' | d$.

Remark. Note that one often refers to the highest common factor, although certainly multiplying by a unit will give another highest common factor.

Proposition 7.7.5. Highest common factors exist in UFD and are unique up to multiplication by a unit.

Proof. If a_i is zero, $\mathrm{hcf}(a_1, \dots, a_n) = \mathrm{hcf}(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$. Thus, we only consider the case that a_i is unit or a product of irreducibles, each a_i is of the form

$$u_i \prod_j p_j^{n_{ij}} \tag{7.7.6}$$

where p_j is irreducible and p_j is not associate to p_k whenever $j \neq k$. u_i is a unit in R and $n_{ij} \geq 0$.

The claim is that $\prod_j p_j^{m_j}$ is a highest common factor of $a_1, \ldots, a_n$ where $m_j = \min_i\{n_{ij}\}$. It is clear that this is a factor of each a_i i.e., $d \mid a_i$, and if $d' \mid a_i$ for each i.

If a_i is a unit, we have $a_i = cd'$ for some $c \in R$, then $\left(a_i^{-1}c\right) d' = 1$ and therefore d' is a unit. If a_i is not a unit, then each irreducible dividing d' is also an irreducible dividing a_i and so must be one of the p_j (by Proposition 7.7.4). Thus

$$d' = u \prod_j p_j^{t_j} \tag{7.7.7}$$

where u is a unit. But the t_j can be at most $\min_i\{n_{ij}\}$ if $d'|a_i$ for each i. Thus

$$d = \prod_j p_j^{m_j} = p \cdot \prod_j p_j^{t_j} = pu^{-1}d' \;\Rightarrow\; d' \mid d \tag{7.7.8}$$

where $p \in R$.

Suppose d and d' are highest common factors of a and b, then $d \mid d'$ and $d' \mid d$. Thus, for $r_1, r_2 \in R$, we have

$$d' = dr_1,\; d = d'r_2 \;\Rightarrow\; d' = d'r_1r_2 \;\Rightarrow\; r_1r_2 = 1 \tag{7.7.9}$$

since R is an integral domain. Thus, r_1, r_2 are units. So highest common factors are unique up to multiplication by a unit. □

Definition 7.7.3 (Lowest common multiple)**.** [12]

Proposition 7.7.6. Lowest common multiples exist in UFD.

Proof. [13] □

7.8 Gauss' Lemma and Eisenstein's Criterion

7.8.1 Content and primitiveness

Definition 7.8.1 (coprime)**.** Let R be an integral domain and $a_1, \ldots, a_n \in R$. Then we say $a_1, \ldots, a_n$ are coprime if the highest common factor of $a_1, \ldots, a_n$ is a unit.

Definition 7.8.2 (content, primitiveness)**.** Assume that the ring R is a UFD. Let $f(X) \in R[X]$ with $f(X) = a_0 + \cdots + a_nX_n$ with $a_n \neq 0$, $\deg f = n$. The content $c(f(X))$ is the highest common factor of $a_0, \ldots, a_n$. $f(X)$ is primitive if $c(f(X))$ is a unit, i.e. if the a_i are coprime.

Lemma 7.8.1. Let the ring R be a UFD. If $f(X)$ and $g(X)$ are primitive in $R[X]$ then so is $f(X)g(X)$.

Proof. Let

$$f(X) = a_0 + a_1X + \cdots + a_mX^m, \quad g(X) = b_0 + b_1X + \cdots + b_nX^n \tag{7.8.1}$$

be primitive. Suppose the product $f(X)g(X)$ is not primitive. So $c(f(X)g(X))$ is not a unit and there is a prime $p \in R$ dividing $c(f(X)g(X))$ (by Definition 7.7.1) but $p \nmid c(f(X))$ and $p \nmid c(g(X))$. (If $p \mid c(f(x)) = u$ where u is a unit since $f(x)$ is primitive, then $pa = u$ for some $a \in R$. Then $u^{-1}ap = 1$, so p is a unit. Contradiction.)

Let k and l be the first indice such that $p \nmid a_i$, $p \nmid b_j$ (otherwise, if $p \mid a_i$, $p \mid b_j$ for all i, j, we have $p \mid c(f(x)))$ and $p \mid c(g(x)))$,

$$p \mid a_0,\; p \mid a_1,\; \ldots,\; p \mid a_{k-1},\; p \nmid a_k, \quad p \mid b_0,\; p \mid b_1,\; \ldots,\; p \mid b_{l-1},\; p \nmid b_l. \tag{7.8.2}$$

Thus, $p \nmid a_kb_l$ by the definition of primeness. The coefficient c_{k+l} of X^{k+l} in $f(X)g(X)$ is

$$\cdots + a_{k+1}b_{l-1} + a_kb_l + a_{k-1}b_{l+1} + \ldots. \tag{7.8.3}$$

p divides all of these terms apart from a_kb_l which it does not divide. So $p \nmid c_{k+l}$, contradicting that $p|c(f(X)g(X))$. Thus $f(X)g(X)$ is primitive. □

[12] need LCM
[13] need to prove

Consider the polynomial ring $R[X]$ and let $\mathbb{F}$ be the field of fractions of R.

Corollary 7.8.2. Let the ring R be a UFD. For $f(X), g(X) \in R[X]$, the content $c(f(X)g(X))$ is an associate of $c(f(X))c(g(X))$. (Recall that highest common factors and hence contents are only defined up to associates.)

Proof. As R is a UFD we may write

$$f(X) = c(f(X))f_1(X), \qquad g(X) = c(g(X))g_1(X) \tag{7.8.4}$$

where $f_1(X), g_1(X)$ are primitive. Then $f_1(X)g_1(X)$ is primitive by Lemma 7.8.1. Thus,

$$f(X)g(X) = c(f(X))c(g(X))f_1(X)g_1(X) \tag{7.8.5}$$

So a highest common factor of the coefficients of $f(X)g(X)$ is $c(f(X))c(g(X))$, i.e.,

$$c(f(X)g(X)) = c(f(X))c(g(X))c(f_1(X)g_1(X)) = c(f(X))c(g(X))u. \tag{7.8.6}$$

where u is a unit. That is, $c(f(X)g(X))$ is an associate of $c(f(X))c(g(X))$ □

Proposition 7.8.3. Let the ring R be a UFD. An irreducible $f(X)$ in $R[X]$ is either in R (and irreducible in R) or it is primitive in $R[X]$.

Proof. Assume that $f(X)$ is irreducible and write $f(X) = c(f(X))f_1(X)$ with $f_1(X)$ primitive.

If $f_1(X) \in R$, $c(f(X)) \in R$ implies $f(X) \in R$.

If $f_1(X) \notin R$ then, since a polynomial of degree at least 1 cannot be a unit, $c(f(X))$ must be a unit by Definition 7.3.3. Then $f(X)$ is primitive in $R[X]$. □

7.8.2 Gauss' lemma

Gauss' lemma helps to determine when polynomials are irreducible in $\mathbb{F}[X]$.

Lemma 7.8.4 (Gauss' lemma)**.** Let R be a UFD with $\mathbb{F}$ its field of fractions. Suppose $f(X) \in R[X]$ is primitive. Then $f(X)$ is irreducible in $R[X]$ if and only if $f(X)$ is irreducible in $\mathbb{F}[X]$.

Remark. In particular, when $R = \mathbb{Z}$ then $f(X)$ is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$.

Proof. ($\Leftarrow$) Take $f(X)$ primitive in $R[X]$. Suppose $f(X)$ is not irreducible in $R[X]$, so it factorises in $R[X]$ as a product of non-units in $R[X]$.

Suppose $f(X) = ab$, $a, b \in R[X]$ and a, b are non-units. If $a \in R$, then $a \mid f(X)$ and $a \mid a_i$ for all coefficients a_i of $f(X)$. Thus, $a \mid a_i$ for all a_i. By the definition of highest common factor (Definition 7.7.2), $a \mid c(f(X))$. Since $f(X)$ is primitive, $c(f(X))$ is a unit. Thus, there exists $b \in R$ such that $ab = u$ where u is a unit. Therefore $1 = abu^{-1}$ and a is also a unit. Contradiction. Hence, neither of these non-units is in R, the factors have degrees greater than 0.

So these factors are non-units in $\mathbb{F}[X]$. So $f(X)$ factorises as a product of non-units in $\mathbb{F}[X]$ and therefore $f(X)$ is not irreducible in $\mathbb{F}[X]$. This means that if f is irreducible in $\mathbb{F}[X]$, it must be irreducible in $R[X]$.

($\Rightarrow$) Suppose that $f(X)$ is not irreducible with $f(X) = g(X)h(X)$ with $g(X), h(X) \in \mathbb{F}[X]$ non-units and hence not constant. Multiply by $a \in R$ and $b \in R$ repectively such that $ag(X), bh(X) \in R[X]$ (existence is guaranteed by Definition 7.3.9). Thus

$$abf(X) = (ag(X))(bh(X)). \tag{7.8.7}$$

Write

$$ag(X) = c(ag(X))g_1(X), \qquad bh(X) = c(bh(X))h_1(X) \tag{7.8.8}$$

where $g_1(X)$, $h_1(X)$ are primitive in $R[X]$. Note that $g_1(X)$, $h_1(X)$ are not constant and hence not units. Now Corollary 7.8.2 implies that ab is an associate of $c(ag(X))c(bh(X))$ by considering contents. So

$$abf(X) = uc(ag(X))c(bh(X))u^{-1}g_1(X)h_1(X) \tag{7.8.9}$$

where $ab = uc(ag(X))c(bh(X))$ and u a unit in R. Cancellation (We know that $ab \neq 0$. Otherwise $f(X) = 0$ and $f(X)$ does not have inverse so it is not primitive.) gives

$$f(X) = (u^{-1}g_1(X))h_1(X) \tag{7.8.10}$$

If $u^{-1}g_1(X)$ is a unit then $g_1(X)$ is a unit. Contradiction. Thus $f(X)$ factorises as a product of non-units in $R[X]$. □

Example 7.8.5. $X^3 + X + 1$ is irreducible in $\mathbb{Z}[X]$, and is primitive in $\mathbb{Z}[X]$ and so Gauss' lemma (Lemma 7.8.4) implies $X^3 + X + 1$ is irreducible in $\mathbb{Q}[X]$.

Suppose $X^3 + X + 1$ is reducible in $\mathbb{Z}[X]$, so $X^3 + X + 1 = g(X)h(X)$ for $g(X), h(X) \in \mathbb{Z}[X]$ not units. Primitivity implies that $g(X)$ and $h(X)$ are not constant polynomials, so $\deg g, \deg h \geq 1$ (see the similar argument in proof of Gauss' lemma (Lemma 7.8.4)). So one of $g(X)$ and $h(X)$ is of degree 1, write

$$g(X) = b_0 + b_1X, \qquad h(X) = c_0 + c_1X + c_2X^2. \tag{7.8.11}$$

Considering coefficients of X^0 and X^3,

$$b_0c_0 = 1, \quad b_1c_2 = 1. \tag{7.8.12}$$

So $b_0 = \pm 1$, $b_1 = \pm 1$. This is a contradiction since ± 1 is not a root of $X^3 + X + 1$.

Proposition 7.8.6. Let R be a UFD with $\mathbb{F}$ its field of fractions. If $f(X) \in R[X]$, not necessarily primitive, and $f(X) = g(X)h(X)$ with $g(X)$ primitive in $R[X], h(X) \in \mathbb{F}[X]$ then

$$f(X) = g(X)h_0(X) \tag{7.8.13}$$

with $h_0(X) \in R[X]$.

Proof. There exists $b \in R$ with $bh(X) \in R[X]$ (by Definition 7.3.9). Consider $bf(X) = g(X)(bh(X))$. Write $bh(X) = c(bh(X))h_1(X)$ with $h_1(X)$ primitive. Consider contents,

$$bc(h(X)) = c(g(X)(bh(X))) \;\Rightarrow\; b \mid c(g(X)bh(X)) \;\Rightarrow\; b \mid uc(g(X))c(bh(X)) \tag{7.8.14}$$

by Corollary 7.8.2, where u is a unit. Since $g(X)$ is primitive, we have $b \mid u'c(bh(X))$ where u' is another unit. Thus, we have $b \mid c(bh(X))$ since u' is a unit. Then, let $ab = u'c(bh(X))$ for some $a \in R$,

$$abf(X) = g(X)c(bh(X))ah_1(X) = u'c(bh(X))u'^{-1}ag(X)h_1(X) = abu'^{-1}ag(X)h_1(X) = abg(X)\left(u'^{-1}ah_1(X)\right). \tag{7.8.15}$$

If $ab = 0$, we have $a = 0$ or $b = 0$. If $a = 0$, $c(bh(X)) = 0$, $bf(X) = 0$, $b = 0$ or $f(X) = 0$. If $f(X) = 0$, we have $h(X) = 0$ since $g(X) \neq 0$ ($g(X)$ is primitive). If $b = 0$, $bh(X) = 0$ and this is contradiction to Definition 7.3.9.(ii).

If $ab \neq 0$, we can do the cancellation and have $f(X) = g(X)\left(u'^{-1}ah_1(X)\right) = g(X)h_0(X)$ for some $h_0(X) \in R[X]$. □

Thus, we can have the following proposition.

Proposition 7.8.7. Let R be a UFD with $\mathbb{F}$ its field of fractions and $g(X)$ be primitive in $R[X]$,

$$I = g(X)\mathbb{F}[X] \lhd \mathbb{F}[X], \qquad J = g(X)R[X] \lhd R[X] \quad \Rightarrow \quad I \cap R[X] = J. \tag{7.8.16}$$

Theorem 7.8.8. If R is a UFD then $R[X]$ is a UFD.

Proof. The first step is to show that we need only look at primitives.

Let $f(X) \in R[X]$ be non-zero and a non-unit. Write $f(X) = c(f(X))f_1(X)$ with $f_1(X)$ primitive.

Observe that since R is a UFD, $c(f(X))$ is expressible as a product of irreducibles in R in an essentially unique way. These irreducibles are irreducible in $R[X]$. $p_i \in R$

$$c(f(X)) = p_1 \dots p_m. \quad (*) \tag{7.8.17}$$

If $f(X)$ factorises as a product of irreducibles in $R[X]$, then we can collect together the irreducibles in R and the primitive

irreducibles. $q_j(X) \in R[X]$ are primitive irreducibles,

$$f(X) = c(f(X))f_1(X) = p_1 \dots p_m \cdot q_1(X) \dots q_n(X). \tag{7.8.18}$$

The product of these primitive irreducibles $q_1(X) \dots q_n(X)$ is primitive by Lemma 7.8.1 and so the content of $f(X)$ is an associate of the product of the irreducibles in R. That is, by Corollary 7.8.2 and primitiveness,

$$c(f(X)) = c\left(p_1 \dots p_m \cdot q_1(X) \dots q_n(X)\right) = up_1 \dots p_m \cdot c(q_1(X)) \dots c(q_n(X)) = u'p_1 \dots p_m \quad (\dagger) \tag{7.8.19}$$

where u, u' are units in R. The essentially unique factorisation of $c(f(X))$ means that $(*)$ and $(\dagger)$ are essentially the same. Then

$$f(X) = c(f(X))f_1(X) = u'p_1 \dots p_m u'^{-1} \cdot q_1(X) \dots q_n(X). \tag{7.8.20}$$

Cancellation implies that the product of the primitives is an associate of $f_1(X)$,

$$f_1(X) = u'^{-1} \cdot q_1(X) \dots q_n(X). \tag{7.8.21}$$

Thus we may assume that $f(X)$ is primitive. That is, $c(f(X))$ can be waived since they are in R.

We know that $\mathbb{F}[X]$ is a UFD. So we can factorise $f(X)$ in $\mathbb{F}[X]$,

$$f(X) = p_1(X) \dots p_k(X), \tag{7.8.22}$$

where $p_i(X)$ is irreducible in $\mathbb{F}[X]$.

There exists $a_i \in R$ with $a_i p_i(X) \in R[X]$ (by Definition 7.3.9). We have

$$a_i p_i(X) = c_i q_i(X) \tag{7.8.23}$$

with $c_i = c(a_i p_i(X))$, $q_i(X)$ primitive in $R[X]$. $q_i(X)$ is also irreducible in $\mathbb{F}[X]$ since $\mathbb{F}[X]$ is a UFD. Thus, by Gauss' lemma (Lemma 7.8.4), $q_i(X)$ is also irreducible in $R[X]$. So

$$a_1 \dots a_k f(X) = c_1 \dots c_k q_1(X) \dots q_k(X). \tag{7.8.24}$$

Considering contents and using the assumption that $f(X)$ is primitive, we have

$$a_1 \dots a_k = uc_1 \dots c_k \tag{7.8.25}$$

for some unit $u \in R$ since $q_i(X)$ is primitive by Lemma 7.8.1, i.e. $q_1(X) \dots q_k(X)$ is primitive.

$$a_1 \dots a_k f(X) = (uc_1 \dots c_k)(u^{-1}q_1(X))q_2(X) \dots q_k(X). \tag{7.8.26}$$

Cancellation gives

$$f(X) = (u^{-1}q_1(X))q_2(X) \dots q_k(X), \tag{7.8.27}$$

a product of irreducibles in $R[X]$. This shows the existence part. For the uniqueness of the factorisation assume that

$$f(X) = q_1(X) \dots q_k(X) = r_1(X) \dots r_l(X) \tag{7.8.28}$$

with $q_i(X)$, $r_i(X)$ irreducible in $R[X]$. We are assuming that $f(X)$ is primitive and so each $r_i(X)$ must be primitive (by Corollary 7.8.2).

By Gauss' lemma (Lemma 7.8.4), $r_i(X)$ is irreducible in $\mathbb{F}[X]$. Uniqueness of factorisation in $\mathbb{F}[X]$ implies that $k = l$, and after reordering we have $q_i(X) = u_i r_i(X)$ with u_i a unit in $\mathbb{F}[X]$ (since $\mathbb{F}[X]$ is a UFD), hence in $\mathbb{F}$.

We can write $u_i = a_i/b_i$ for some $a_i, b_i \in R$ with $b_i \neq 0$. Then $b_i q_i(X) = a_i r_i(X)$. But $q_i(X)$ and $r_i(X)$ are primitive and hence b_i and a_i must be associates being the content of $b_i q_i(X) = a_i r_i(X)$. Cancelling gives that $q_i(X)$ and $r_i(X)$ are associates in $R[X]$. Thus factorisation is essentially unique in $R[X]$. □

Corollary 7.8.9. Let R be a UFD. Then $R[X_1, \dots, X_n]$ is a UFD.

Proof. We assume that R is a UFD and repeated application of Theorem 7.8.8 gives that

$$R[X_1], \quad R[X_1, X_2] = (R[X_1])[X_2], \quad R[X_1, X_2, X_3] = ((R[X_1])[X_2])\,[X_3] \ldots. \tag{7.8.29}$$

Thus, $R[X_1, \ldots, X_n]$ is a UFD. □

7.8.3 Eisenstein's criterion

Proposition 7.8.10 (Eisenstein's criterion)**.** Let R be a UFD and let

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X],\ a_n \neq 0, \tag{7.8.30}$$

be primitive. Assume that for some irreducible p we have $p \nmid a_n$, $p \mid a_i$ for $0 \leq i < n$ and $p^2 \nmid a_0$. Then $f(X)$ is irreducible in $R[X]$, and hence in $\mathbb{F}[X]$ by Gauss' lemma (Lemma 7.8.4).

Proof. Suppose that $f(X) = g(X)h(X)$ with

$$g(X) = r_k X^k + \cdots + r_0, \qquad h(X) = s_l X^l + \cdots + s_0 \tag{7.8.31}$$

where $r_k, s_l \neq 0$. Note that $k + l = n$. Since $p \mid a_0 = r_0 s_0$ and $p^2 \nmid a_0$ we know $p \mid r_0$ or $p \mid s_0$ since p is prime. However, $p \mid r_0$ and $p \mid s_0$ gives that $p^2 \mid r_0 s_0 = a_0$. Contradiction to the assumption. Thus we may assume that $p | r_0$ and $p \nmid s_0$. $p \nmid a_n = r_k s_l$ implies $p \nmid r_k$, $p \nmid s_l$.

Set j to be such that $p | r_0, \ldots, p | r_{j-1}, p \nmid r_j$ (This index j exists since $p \nmid r_k$). Consider the term

$$a_j = r_0 s_j + \cdots + r_j s_0. \tag{7.8.32}$$

We have $p \mid r_0 s_j, \ldots, p \mid r_{j-1} s_1$. If $p \mid r_j s_0$, we have $p \mid r_j$ or $p \mid s_0$ since p is a prime. Contradiction. Thus, $p \nmid a_j$. Thus $j = n$, and hence $k = n$, $l = 0$. As $f(X)$ is primitive,

$$u = c(f(X)) = u' c(g(X)) c(h(X)) = u' s_0 c(g(X)) \tag{7.8.33}$$

where u, u' are units. Thus, $h(X) = s_0$ must be a unit. Thus $f(X)$ cannot be factorised as a product of non-units. □

Example 7.8.11. Consider $R = \mathbb{Z}$ and let $f(X) = X^n - p \in \mathbb{Z}[X]$, where p is prime.

By Eisenstein's criterion, $f(X)$ is irreducible in $\mathbb{Z}[X]$ and hence in $\mathbb{Q}[X]$ (by Gauss' lemma (Lemma 7.8.4) since $\mathbb{Q}$ is field of fractions of $\mathbb{Z}$). So $f(X)$ does not have any roots in $\mathbb{Q}$, as a root would yield a linear factor of $f(X)$ in $\mathbb{Q}[X]$. Thus p has no nth roots in $\mathbb{Q}$.

Example 7.8.12. Consider the cyclotomic polynomial

$$f(X) = X^{p-1} + X^{p-2} + \cdots + 1 \tag{7.8.34}$$

where p is prime. The claim is that this is irreducible in $\mathbb{Z}[X]$, and hence in $\mathbb{Q}[X]$. Note that $(X-1)f(X) = X^p - 1$. We make the substitution $X = 1 + Y$ and get

$$Y f(1+Y) = (1+Y)^p - 1, \qquad f(1+Y) = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{p-1} \tag{7.8.35}$$

where $\binom{p}{i}$ are binomial coefficients. Eisenstein's criterion does now apply, we have $p | \binom{p}{i}$, $p^2 \nmid \binom{p}{p-1} = p$. We deduce that $f(1+Y)$ is irreducible and hence $f(X)$ is irreducible in $\mathbb{Z}[X]$, and hence in $\mathbb{Q}[X]$.

7.9 $\mathbb{Z}[\cdot]$

7.9.1 Gaussian integers $\mathbb{Z}[i]$

Definition 7.9.1 (Gaussian integer)**.** Gaussian integers are the set $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$. The norm (see Definition 7.3.4)

$$N(a + ib) = a^2 + b^2 = (a + ib)(a - ib) = z\bar{z}, \tag{7.9.1}$$

where $z = a + ib$, is multiplicative, that is,

$$N(z_1 z_2) = N(z_1)N(z_2). \tag{7.9.2}$$

The units have to be of norm 1, hence the only units are ± 1, $\pm i$.

Example 7.9.1. Recall from an earlier example that $\mathbb{Z}[i]$ is a Euclidean domain and hence a PID and a UFD. Thus the irreducibles and primes are the same, by Lemma 7.3.7 and Lemma 7.4.5.

- $2 = (1+i)(1-i)$ is not irreducible.
- 3 is irreducible since $N(3) = 9$. If it were to factorise as a product of two non-units then they would have norm 3. But there are no elements of norm 3.
- $5 = (1+2i)(1-2i)$ is not irreducible.

Lemma 7.9.2. A prime number p in $\mathbb{Z}$ is irreducible (and prime) in $\mathbb{Z}[i]$ if and only if p is not of the form $x^2 + y^2$ with $x, y \in \mathbb{Z} \setminus \{0\}$.

Proof. ($\Rightarrow$). If $p = x^2 + y^2$ then $p = (x+iy)(x-iy)$ (where $x+iy, x-iy$ are not units) and so p is not irreducible in $\mathbb{Z}[i]$.

($\Leftarrow$). Consider $N(p) = p^2$, since p is not irreducible, it factorises into two non-units, necessarily of norm p ($p = z_1 z_2$, $p^2 = N(p) = N(z_1)N(z_2)$, then $N(z_1) = N(z_2) = p$, since $N(z_1), N(z_2) \neq 1$), only if there is $x + iy$ with $N(x+iy) = p$. So $x^2 + y^2 = p$. □

Proposition 7.9.3. The irreducibles (and primes) in $\mathbb{Z}[i]$ are up to associates

(i) $p \in \mathbb{Z}$ prime with $p \equiv 3 \pmod 4$,

(ii) z with $z\bar{z} = p$, for p prime in $\mathbb{Z}$ with $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. Let us first show that these are actually irreducibles (and primes).

(i) If $p \equiv 3 \pmod 4$ then it is not of the form $x^2 + y^2$ since squares modulo 4 are 0 or 1 and so $x^2 + y^2 \equiv 0,\ 1$ or $2 \pmod 4$. By Lemma 7.9.2, p is irreducible (and prime) in $\mathbb{Z}[i]$.

(ii) (a) If $p = 2 = (1+i)(1-i)$, $1 \pm i$ are irreducibles of norm 2.

(b) If $p \equiv 1 \pmod 4$, we consider the finite field of p elements $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$[14]. Then by structure theorem for finite abelian groups (Theorem 6.6.6), we have the multiplicative group

$$\mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\} \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n} \quad \text{with } d_i \mid d_{i+1} \tag{7.9.3}$$

If $\mathbb{F}_p^*$ is isomorphic to $C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n}$ where $n \geq 2$, then there exists $n_a, n_b \in \{d_1, d_2, \ldots, d_n\}$ s.t. $n_a \mid n_b$. Then there is a cyclic subgroup $\langle a \rangle \cong C_{n_a}$ and $\langle b \rangle \cong C_{n_b}$ generated by a and b with order n_a and n_b. Since $n_a \mid n_b$ we have $\left\langle b^{\frac{n_b}{n_a}} \right\rangle \cong \langle a \rangle \cong C_m$ for some $m > 1$. Thus, there exists a subgroup $\left\langle b^{\frac{n_b}{n_a}} \right\rangle \times \langle a \rangle \cong C_m \times C_m$ by Lemma 6.3.3.

Thus there are at least m^2 elements satisfying $a^m = 1$. These are all roots of $X^m - 1$ in $\mathbb{F}_p[X]$ which is a UFD. $X^m - 1$ has a unique expression up to ordering and associates as a product of at most m irreducibles in $\mathbb{F}_p[X]$.

In particular, there are at most m linear factors $X - a$ and so at most m roots, contradicting that there are at least m^2 roots.

Thus, the multiplicative group $\mathbb{F}_p^*$ is cyclic.

In this case, $\mathbb{F}_p$ has a cyclic multiplicative group. A cyclic group $\langle g \rangle$ of order $4n$ has a subgroup of order 4, namely $\langle g^n \rangle$, and a unique element of order 2, namely g^{2n}. $p-1$ is the element of order 2 in $\mathbb{F}_p \setminus \{0\}$, the multiplicative group since

$$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p \tag{7.9.4}$$

An element of order 4 corresponds to $a \in \mathbb{Z}$ with a^2 is order 2. Thus, $a^2 \equiv -1 \pmod p$. Thus $p | a^2 + 1 = (a+i)(a-i)$. But $p \nmid a \pm i$ (since p is a prime number) and so p is not an irreducible (and prime) in $\mathbb{Z}[i]$ (If p is irreducible, it must divides either $a+i$ or $a-i$ since it is an associate of the irreducible divides $a \pm i$).

[14] see Example 7.4.9

Thus p must factorise, $p = z_1 z_2$ with z_i non-units in $\mathbb{Z}[i]$. We have $N(z_i) = p$. Writing $z_i = x \pm iy$, we have $p = x^2 + y^2$ (Lemma 7.9.2). We also have that z_i are irreducible since if $z_i = y_1 y_2$, $p = N(z_i) = N(y_1)N(y_2)$ which will give that one of y_i is a unit ($N(y_i) = 1$).

Now for any irreducible $\alpha \in \mathbb{Z}[i]$, $\bar{\alpha}$ is irreducible (since the complex conjugate of a unit is still a unit). Since α is a irreducible (not unit), we can take prime number p such that $p \mid N(\alpha)$. We use that $N(\alpha) = \alpha\bar{\alpha}$, a product of irreducibles.

If $p \equiv 3 \pmod 4$ then p is irreducible (and prime) in $\mathbb{Z}[i]$. So the fact that $\mathbb{Z}[i]$ is a UFD and $p \mid \alpha\bar{\alpha}$ implies that p is an associate of either α or $\bar{\alpha}$. So p is an associate of α (since the complex conjugate of a unit is still a unit).

If $p = 2$, or $p \equiv 1 \pmod 4$ then $p = z\bar{z} | \alpha\bar{\alpha}$. If there exists non-unit $b \in Z[i]$ such that $z\bar{z}b\bar{b} = \alpha\bar{\alpha}$ (since $z\bar{z}, \alpha\bar{\alpha} \in \mathbb{Z}^+$), then we α can be expressed by the product of two non-units. Contradiction.

Thus, we have $z\bar{z} = \alpha\bar{\alpha}$. Since z and $\bar{z}$ are irreducibles and $\mathbb{Z}[i]$ is a UFD, we have that z is an associate of α or $\bar{\alpha}$ and so α is an associate of z or $\bar{z}$. □

Corollary 7.9.4. Let $n = p_1^{n_1} \dots p_k^{n_k} \in \mathbb{Z}$ be the prime factorisation of n, with $p_1, \dots, p_k$ distinct primes in $\mathbb{Z}$. Then n is of the form $x^2 + y^2$ if and only if whenever $p_i \equiv 3 \pmod 4$ then n_i is even.

Proof. ($\Rightarrow$). Suppose $n = x^2 + y^2 = (x + iy)(x - iy) = z\bar{z}$ with $z = x + iy$. Thus $N(z) = n$.

Express z as a product of irreducibles in $\mathbb{Z}[i]$, $z = \alpha_1 \dots \alpha_s$, say. But we know what the irreducibles are from Proposition 7.9.3. Either $N(\alpha_j) = p_j^2$ with $p_j \equiv 3 \pmod 4$ or $N(\alpha_j) = p_j$ with $p_j = 2$ or $p_j \equiv 1 \pmod 4$. Thus $n = N(z) = \prod N(\alpha_j)$ is of the required form.

($\Leftarrow$). Conversely, if $n = p_1^{n_1} \dots p_k^{n_k}$ with n_j even for $p_j \equiv 3 \pmod 4$ then we can replace any $p_j = 2$ or $p_j \equiv 1 \pmod 4$ by $p_j = \alpha_j\bar{\alpha}_j$ and any other primes $p_j = \alpha_j = \bar{\alpha}_j$ and so $p_j^2 = \alpha_j\bar{\alpha}_j$ for some irreducible α_j (Proposition 7.9.3). Thus n is of the form $z\bar{z}$ for some $z = x + iy$ and so $n = x^2 + y^2$. □

Example 7.9.5. Let $n = 65 = 5 \times 13$ and note that $5 = (2+i)(2-i)$, $13 = (2+3i)(2-3i)$. The unique factorisation up to reordering and associates is $n = (2 + i)(2 - i)(2 + 3i)(2 - 3i)$.

We use this to express n as $x^2 + y^2 = z\bar{z}$ with $z = x + iy$

$$n = [(2 + i)(2 + 3i)][(2 - i)(2 - 3i)] = (1 + 8i)(1 - 8i) = 1^2 + 8^2 \tag{7.9.5}$$

or

$$n = [(2 + i)(2 - 3i)][(2 - i)(2 + 3i)] = (7 - 4i)(7 + 4i) = 4^2 + 7^2. \tag{7.9.6}$$

7.9.2 $\mathbb{Z}[\alpha]$ with α an algebraic integer

Definition 7.9.2 (algebraic integer)**.** A complex number $\alpha \in \mathbb{C}$ is an algebraic integer if there is a monic polynomial $f(X) \in \mathbb{Z}[X]$ with $f(\alpha) = 0$.

Example 7.9.6. The following are algebraic integers,

$\alpha \in \mathbb{C}$	Minimal polynomial of α
i	$f(X) = X^2 + 1$
$\sqrt{2}$	$f(X) = X^2 - 2$
$\frac{1}{2}(1 + \sqrt{-3})$	$f(X) = X^2 - X + 1$

Definition 7.9.3. $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and α. Then,

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/I \tag{7.9.7}$$

where I is the kernel of the map $\theta : \mathbb{Z}[X] \to \mathbb{Z}[\alpha]$, $f(X) \mapsto f(\alpha)$ (by the first isomorphism theorem (Theorem 7.2.12) since θ is surjective by Definition 7.9.2).

Proposition 7.9.7. For an algebraic integer α, with the notation in Definition 7.9.3, the kernel I is a principal ideal generated by a monic irreducible polynomial $f_\alpha(X) \in \mathbb{Z}[X]$, called the minimal polynomial of α.

Proof. By Definition 7.9.2, $f(\alpha) = 0$ for some monic $f(X) \in \mathbb{Z}[X]$. So we can pick $f_\alpha(X) \in I$ of minimal degree ≥ 0, and we may assume $f_\alpha(X)$ is primitive in $\mathbb{Z}[X]$. The claim is that this is the required polynomial.

We wish to show that $I = \langle f_\alpha(X) \rangle$.

Let $h(X) \in I$. Then, as $\mathbb{Q}$ is a field, we can apply Euclidean algorithm for polynomials (Proposition 7.2.10) and find $q(X), r(X) \in \mathbb{Q}[X]$ such that

$$h(X) = q(X)f_\alpha(X) + r(X) \tag{7.9.8}$$

with $r(X) = 0$ or $\deg r(X) < \deg f_\alpha(X)$. Clearing denominators, there exists $a \in \mathbb{Z}\backslash\{0\}$ such that

$$ah(X) = aq(X)f_\alpha(X) + ar(X) \tag{7.9.9}$$

with $aq(X) \in \mathbb{Z}[X]$ and $ar(X) \in \mathbb{Z}[X]$. But $ar(\alpha) = 0$ so $ar(X) \in I$. Minimality of degree of $f_\alpha(X)$ implies that $ar(X) = 0$ so $r(X) = 0$. So $ah(X) = aq(X)f_\alpha(X)$. Consider the contents of both sides, since $h(X) \in \mathbb{Z}[X]$

$$a \mid c(ah(X)) = c(aq(X)f_\alpha(X)) = c(aq(X))u \quad (u \text{ is a unit}) \tag{7.9.10}$$

by the fact that $f_\alpha(X)$ is primitive (Corollary 7.8.2). So a divides all the coefficients of $aq(X)$. So $q(X) \in \mathbb{Z}[X]$. Thus $h(X) \in \langle f_\alpha(X)\rangle \lhd \mathbb{Z}[X]$.

We also claim that $f_\alpha(X)$ is prime (and irreducible since $\mathbb{Z}[X]$ is a UFD).

If $f_\alpha(X) = f_1(X)f_2(X)$ then $0 = f_1(\alpha)f_2(\alpha)$ and so $f_i(X) \in I = \langle f_\alpha(X)\rangle$ for some i. $f_\alpha(X)|f_i(X)$ for some i. i.e. $f_\alpha(X)g(X) = f_i(X)$, $g(X) \in \mathbb{Z}[X]$. Thus, $f_\alpha(X)$ is prime.

Finally, we show that $f_\alpha(X)$ is monic.

As in the first line of proof, there are some monic $f(X) \in I = \langle f_\alpha(X)\rangle$. Thus, $f_\alpha(X)g(X) = f(X)$ where $g(X) \in \mathbb{Z}[X]$. Checking the leading coefficient of polynomial, we have $a_\alpha a_g = 1$ ($f_\alpha(X) = a_\alpha X^n + \dots$, $g(X) = a_g X^m + \dots$) and then $a_\alpha = \pm 1, \pm i$. But these are all multiplication of 1 and a unit. Thus, $f_\alpha(X)$ is monic. □

Remark. minimal polynomial of algebraic integer $f_\alpha(X)$ is unique[15].

Definition 7.9.4 (rational integers)**.** The elements of $\mathbb{Z}$ are called rational integers.

Lemma 7.9.8. If α is an algebraic integer and $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$.

Proof. $f_\alpha(X)$ is irreducible in $\mathbb{Z}[X]$ and monic (thus primitive) (by Proposition 7.9.7). By Gauss' lemma, Lemma 7.8.4 ($\mathbb{Z}$ is a UFD and $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$), $f_\alpha(X)$ is irreducible in $\mathbb{Q}[X]$.

Since α is a root of $f_\alpha(X)$ in $\mathbb{Q}$, we have $f_\alpha(X) = X - \alpha$ by definition of minimal polynomial of algebraic integer. Also since $f_\alpha \in \mathbb{Z}[X]$, we have $\alpha \in \mathbb{Z}$. □

Example 7.9.9. Let $p \in \mathbb{Z}$ be prime and consider $\mathbb{Z}[X]/\langle p, f_\alpha(X)\rangle$ with $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

$$\begin{aligned}
\mathbb{Z}[X]/\langle p, f_\alpha(X)\rangle &\cong \mathbb{F}_p[X]/\left\langle \bar{f}_\alpha(X)\right\rangle \quad \text{(the third isomorphism theorem, Theorem 7.2.15)} \\
&\cong \mathbb{F}_p[\alpha] \quad \text{(the first isomorphism theorem, Theorem 7.2.12)} \\
&\cong \mathbb{Z}[\alpha]/\langle p\rangle \quad \text{(the third isomorphism theorem, Theorem 7.2.15)}
\end{aligned}$$

where $\bar{f}_\alpha(X)$ is the polynomial in $\mathbb{F}_p[X]$ obtained from $f_\alpha(X)$ by taking coefficients modulo p.

For example, $\alpha = i$, $f_\alpha(X) = X^2 + 1$. Then

$$\mathbb{Z}[X]/\left\langle p, X^2+1\right\rangle \cong \mathbb{F}_p[X]/\left\langle X^2+1\right\rangle \cong \mathbb{F}_p[i] \cong \mathbb{Z}[i]/\langle p\rangle\,. \tag{7.9.11}$$

For $p = 2$ or $p \equiv 1 \pmod 4$ this is not an integral domain, for $p \equiv 3 \pmod 4$ it is an integral domain[16],.

7.10 Problems

Problem 7.10.1. Let $\omega = \frac{1}{2}(1 + \sqrt{-3})$, let $R = \{a + b\omega : a, b \in \mathbb{Z}\}$, and let $F = \{a + b\omega : a, b \in \mathbb{Q}\}$. Show that R is a subring of $\mathbb{C}$, and that F is a subfield of $\mathbb{C}$. What are the units of R?

Solution. Let $a_1 + b_1\omega, a_2 + b_2\omega \in R$. Thus, $a_1 + b_1\omega + a_2 + b_2\omega \in R$ since $a_1 + a_2 \in \mathbb{Z}$ and $b_1 + b_2 \in \mathbb{Z}$.

The identity of addition is $0 = 0 + 0\omega \in R$, thus the inverse of $a + b\omega$ is $-a - b\omega \in R$.

[15] need proof
[16] need details

Also, $(a_1+b_1\omega)(a_2+b_2\omega)=a_1a_2+(a_1b_2+a_2b_1)\omega+b_1b_2\omega^2\in R$. We know that

$$\omega^2=\left(\frac{1+\sqrt{-3}}{2}\right)^2=\frac{1+(-3)+2\sqrt{-3}}{4}=\frac{-1+\sqrt{-3}}{2}=\omega-1. \tag{7.10.1}$$

Thus, $(a_1+b_1\omega)(a_2+b_2\omega)=a_1a_2-b_1b_2+(a_1b_2+a_2b_1+b_1b_2)\omega\in R$.

The multiplicative identity is $1=1+0\omega\in R$. Also, it can be check that the multiplication is distributive over addition. Thus, R is subring of $\mathbb{C}$.

For $F=\{a+b\omega : a,b\in\mathbb{Q}\}$, we only check the multiplication inverse, let $a+b\omega\in F$

$$(a+b\omega)(c+d\omega)=1\ \Rightarrow\ ac-bd+(ad+bc+bd)\omega=1\ \Rightarrow\ \begin{cases} ac-bd=1\\ ad+bc+bd=0\end{cases} \tag{7.10.2}$$

Thus if $a=0$, $b\neq 0$, $d=-\frac{1}{b}$, $c=\frac{1}{b}$, the inverse $a+b\omega=b\omega$ is $\frac{1}{b}-\frac{1}{b}\omega\in F$.

IF $a\neq 0$, $c=\frac{1+bd}{a}$,

$$ad+b\frac{1+bd}{a}+bd=0\ \Rightarrow\ \left(a+b+\frac{b^2}{a}\right)d=-\frac{b}{a} \tag{7.10.3}$$

If $b=0$, $d=0$, $c=\frac{1}{a}$, the inverse $a+b\omega=a$ is $\frac{1}{c}=\frac{1}{c}+0\omega\in F$.

If $b\neq 0$, $d=\frac{b}{a^2+ab+b^2}$, $c=\frac{a^2+ab+2b^2}{a(a^2+ab+b^2)}$, so the inverse $a+b\omega$ is

$$\frac{a^2+ab+2b^2}{a(a^2+ab+b^2)}+\frac{b}{a^2+ab+b^2}\omega\in F. \tag{7.10.4}$$

Thus, F is subfield of $\mathbb{C}$.

We can define

$$N(a+b\omega)=N\left(a+\frac{b}{2}+\frac{\sqrt{-3}}{2}b\right)=(a+\frac{b}{2})^2+\frac{3}{4}b^2=a^2+b^2+ab\geq 0. \tag{7.10.5}$$

Given $r_1=a_1+b_1\omega\in R$, if it is a unit, there must exist $r_2\in R$ (its multiplication inverse) such that $r_1r_2=1$. We have $N(r_1r_2)=N(r_1)N(r_2)=1$. Since $N(r)$ is of form $a^2+b^2+ab\in\mathbb{Z}$, $N(r_1)=N(r_2)=1$. Thus,

$$1=N(r_1)=a_1^2+b_1^2+a_1b_1\ \Rightarrow\ a_1^2+a_1b_1+b_1^2-1=0\ \Rightarrow\ b_1^2-4(b_1^2-1)\geq 0\ \Rightarrow\ b_1^2\leq\frac{4}{3}. \tag{7.10.6}$$

If $b=0$, $a=\pm 1$. If $b=-1$, $a=0,1$. If $b=1$, $a=0,-1$. Thus the units are ± 1, $\pm\omega$, $\pm\omega^2$ $(1-\omega,\ -1+\omega)$.

Problem 7.10.2. Show that the ideal $\langle 2,1+\sqrt{-7}\rangle$ in $\mathbb{Z}[\sqrt{-7}]$ is not principal.

Solution. If $\langle 2,1+\sqrt{-7}\rangle$ is principal, there must exists $a\in\mathbb{Z}[\sqrt{-7}]$ such that $\langle 2,1+\sqrt{-7}\rangle=\langle a\rangle$ and $a\mid 2$ and $a\mid 1+\sqrt{-7}$. That is, $2=ab_1$ and $1+\sqrt{-7}=ab_2$, $b_1,b_2\in\mathbb{Z}[\sqrt{-7}]$.

Thus, the norm is of the form c^2+7d^2,

$$\begin{aligned} 4 &= N(2)=N(a)N(b_1)\ \Rightarrow\ N(a)=1,4\\ 8 &= N(1+\sqrt{-7})=N(a)N(b_2)\ \Rightarrow\ N(a)=1,8\end{aligned}$$

Thus, $N(a)=1$ and a is unit. Hence $\langle a\rangle=\mathbb{Z}[\sqrt{-7}]$. However, $1\in\mathbb{Z}[\sqrt{-7}]$ and $1\notin\langle 2,1+\sqrt{-7}\rangle$. Thus, $\langle 2,1+\sqrt{-7}\rangle$ is not principal.

Problem 7.10.3. Give an element of $\mathbb{Z}[\sqrt{-17}]$ that is a product of two irreducibles and also a product of three irreducibles.

Solution. $18=(1+\sqrt{-17})(1-\sqrt{-17})=2\cdot 3\cdot 3$.

Now we show that they are all irreducible.

Express 2 with $2=z_1z_2$, $z_1,z_2\in\mathbb{Z}[\sqrt{-17}]$. Thus $4=N(z_1)N(z_2)$. Since the norm is the form of a^2+17b^2 and there is no element of norm 2. Thus, one of the $N(z_j)=1$, so z_j is a unit. Thus, 2 is irreducible.

Express 3 with $3=z_1z_2$, $z_1,z_2\in\mathbb{Z}[\sqrt{-17}]$. Thus $9=N(z_1)N(z_2)$. Since the norm is the form of a^2+17b^2 and there is no element of norm 3. Thus, one of the $N(z_j)=1$, so z_j is a unit. Thus, 3 is irreducible.

Express $1\pm\sqrt{-17}$ with $1\pm\sqrt{-17}=z_1z_2$, $z_1,z_2\in\mathbb{Z}[\sqrt{-17}]$. Thus $18=N(z_1)N(z_2)$. Since the norm is the form of a^2+17b^2 and there is no element of norm 2,3,6. Thus, one of the $N(z_j)=1$, so z_j is a unit. Thus, $1\pm\sqrt{-17}$ is irreducible.

Problem 7.10.4. Recall Definition 7.1.6,

(i) What are the idempotent elements of $\mathbb{Z}/6\mathbb{Z}$? Of $\mathbb{Z}/8\mathbb{Z}$? Of $\mathbb{Z}/24\mathbb{Z}$? Of $\mathbb{Z}/1000\mathbb{Z}$?

(ii) Show that if r is idempotent then so is $r' = 1 - r$, and $rr' = 0$.

(iii) Show also that the ideal $\langle r \rangle$ is naturally a ring, and that R is isomorphic to $\langle r \rangle \times \langle r' \rangle$.

Solution. (i) 0,1,3; 0,1; 0,1,9,16; For $\mathbb{Z}/1000\mathbb{Z}$, we see that

$$r = \begin{cases} 10x \\ 10x+1 \\ 10x+5 \\ 10x+6 \end{cases} \tag{7.10.7}$$

If $r = 10x$, for some a,

$$100x^2 = 10x + 1000a \;\Rightarrow\; 10x(10x-1) = 1000a \;\Rightarrow\; x = 100y \;\Rightarrow\; x = 0 \;\Rightarrow\; r = 0. \tag{7.10.8}$$

If $r = 10x + 1$, for some a,

$$100x^2 + 20x + 1 = 10x + 1 + 1000a \;\Rightarrow\; 10x(10x+1) = 1000a \;\Rightarrow\; x = 100y \;\Rightarrow\; x = 0 \;\Rightarrow\; r = 1. \tag{7.10.9}$$

If $r = 10x + 5$, for some a,

$$100x^2 + 100x + 25 = 10x + 5 + 1000a \;\Rightarrow\; x(10x+9) + 2 = 100a \;\Rightarrow\; x = 10y + 2. \tag{7.10.10}$$

Thus, $r = 100y + 25$, for some a,

$$10000y^2 + 5000y + 625 = 100y + 25 + 1000a \;\Rightarrow\; y(100y+49) + 6 = 10a \;\Rightarrow\; y = 10z + 6 \;\Rightarrow\; r = 625. \tag{7.10.11}$$

If $r = 10x + 6$, for some a,

$$100x^2 + 120x + 36 = 10x + 6 + 1000a \;\Rightarrow\; x(10x+11) + 3 = 100a \;\Rightarrow\; x = 10y + 7. \tag{7.10.12}$$

Thus, $r = 100y + 76$, for some a,

$$10000y^2 + 15200y + 5776 = 100y + 76 + 1000a \;\Rightarrow\; y(100y+151) + 57 = 10a \;\Rightarrow\; y = 10z + 3 \;\Rightarrow\; r = 376. \tag{7.10.13}$$

Thus, the idempotents are 0,1,376,625.

(ii) $r^2 = r$, $r'^2 = (1-r)^2 = r^2 - 2r + 1 = r - 2r + 1 = 1 - r = r'$ and $rr' = r(1-r) = r - r^2 = 0$.

(iii) Clearly, $\langle r \rangle$ is group under addition. For the multiplication, $\forall rg_1, rg_2 \in \langle r \rangle$ for some $g_1, g_2 \in R$,

$$rg_1 rg_2 = r^2 g_1 g_2 = rg_1 g_2 \in \langle r \rangle . \tag{7.10.14}$$

Now we need to show that $1 \in \langle r \rangle$. Claim r is the identity in $\langle r \rangle$. It is easy to check that $\forall rg \in \langle r \rangle$ for some $g \in R$

$$r(rg) = r^2 g = rg. \tag{7.10.15}$$

Thus, $\langle r \rangle$ is a ring.

Now let $\phi : R \to \langle r \rangle \times \langle r' \rangle$ by $\phi(g) = (rg, r'g) = (rg, (1-r)g)$. Then for any $g_1, g_2 \in R$,

$$\phi(g_1 + g_2) = (r(g_1+g_2), (1-r)(g_1+g_2)) = (rg_1, (1-r)g_1) + (rg_2, (1-r)g_2) = \phi(g_1) + \phi(g_2), \tag{7.10.16}$$

$$\phi(g_1g_2) = (rg_1g_2, (1-r)g_1g_2) = \left(r^2g_1g_2, (1-r)^2g_1g_2\right) = (rg_1, (1-r)g_1)(rg_2, (1-r)g_2) = \phi(g_1)\phi(g_2). \tag{7.10.17}$$

So ϕ is a homomorphism. Then

$$\ker\phi = \{g \in R : rg = 0, (1-r)g = 0\} \subseteq \{g \in R : rg + (1-r)g = 0\} = \{0\} \;\Rightarrow\; \ker\phi = \{0\}. \tag{7.10.18}$$

If $\phi(g_1) = \phi(g_2)$,

$$rg_1 = rg_2,\ (1-r)g_1 = (1-r)g_2 \;\Rightarrow\; g_1 = g_2 \;\Rightarrow\; \phi \text{ is injective.} \tag{7.10.19}$$

To show ϕ is surjective, $\forall a = rg_1 \in \langle r\rangle, b = (1-r)g_2 \in \langle r'\rangle$, we need to find $g \in R$ s.t. $\phi(g) = (a, b)$. So

$$rg = rg_1,\ (1-r)g = (1-r)g_2 \;\Rightarrow\; g = rg_1 + (1-r)g_2. \tag{7.10.20}$$

by the fact $r \cdot r' = 0$. So ϕ is surjective (i.e., $\operatorname{Im}\phi = \langle r\rangle \times \langle r'\rangle$) and then ϕ is bijective. (We can also use first isomorphism theorem to show that

$$R/\ker\phi \cong \operatorname{Im}\phi \;\Rightarrow\; R = R/\ker\phi \cong \langle r\rangle \times \langle r'\rangle. \tag{7.10.21}$$

Thus, ϕ is bijective.)

Problem 7.10.5. (i) Show that the set $P(S)$ of all subsets of a given set S is a ring with respect to the operations of symmetric difference and intersection (the power-set ring). Note that in this ring $A^2 = A$ for all elements A. Describe the principal ideals in this ring. Show that the ideal (A, B) generated by elements A,B is in fact principal. Are there any non-principal ideals?

(ii) The ring R is Boolean if every element of R is idempotent. Prove that every finite Boolean ring is isomorphic to a power-set ring $P(S)$ for some set S. Give an example to show that this need not remain true for infinite Boolean rings.

Solution. (i) Let $A + B = A\triangle B$ and $AB = A \cap B$. We use indicator function, for symmetric difference (addition),

$$\mathbb{1}_{A\triangle B} = \mathbb{1}_A + \mathbb{1}_B \pmod 2. \tag{7.10.22}$$

Clearly, for $A, B \in P(S)$, $A\triangle B \in P(S)$, $A\triangle B = B\triangle A$, the identity is $\emptyset$ and the inverse of A is $A^c = S\backslash A$.

For intersection (multiplication), $A\cap B = B\cap A$ and $A\cap B \in P(S)$. The identity of multiplication is S, since $S\cap A = A$.

For distributivity, $\forall A, B, C \in S$,

$$\begin{aligned}\mathbb{1}_{A\cap(B\triangle C)} &= \mathbb{1}_A\mathbb{1}_{B\triangle C} = \mathbb{1}_A(\mathbb{1}_B + \mathbb{1}_C \pmod 2)\\ &= \mathbb{1}_A\mathbb{1}_B \pmod 2 + \mathbb{1}_A\mathbb{1}_C \pmod 2 = \mathbb{1}_{A\cap B} + \mathbb{1}_{A\cap C} \pmod 2 = \mathbb{1}_{(A\cap B)\triangle(A\cap C)}.\end{aligned}$$

Thus, $P(S)$ is a ring. So $A^2 = A \cap A = A$ for all elements A. Thus, $\forall A \in P(S)$, the principal ideal is

$$I = \langle A\rangle = \{A \cap B : B \in P(S)\} = \text{set of all subsets of } A. \tag{7.10.23}$$

Also, the ideal $\langle A, B\rangle$ is

$$\begin{aligned}\{(A\cap C)\triangle(B\cap D) : C, D \in P(S)\} &= \{(A\cap C)\triangle(B\cap D) : C \subseteq A, D \subseteq B\}\\ &= \{C\triangle D : C \subseteq A, D \subseteq B\}\\ &= \text{set of all subsets of } A\cup B = \langle A\cup B\rangle.\end{aligned}$$

Thus, the ideal $\langle A, B\rangle$ is also principal. So all the ideals are principal.

(ii) Let $(R, \oplus, \otimes)$ be Boolean ring with $r \otimes r = r$ for any $r \in R$. Then $r \oplus r \in R$ by definition of ring. Thus

$$(r\oplus r)\otimes(r\oplus r) = r\oplus r \;\Rightarrow\; r^2\oplus r^2\oplus r^2\oplus r^2 = r\oplus r \;\Rightarrow\; r\oplus r\oplus r\oplus r = r\oplus r \;\Rightarrow\; r\oplus r = 0 \tag{7.10.24}$$

since $(R, \oplus)$ is a group. A similar proof shows that every Boolean ring is commutative: for any $x, y \in R$

$$x \oplus y = (x \oplus y)^2 = x^2 \oplus xy \oplus yx \oplus y^2 = x \oplus xy \oplus yx \oplus y \tag{7.10.25}$$

and this yields $xy \oplus yx = 0$, which means $x \otimes y = y \otimes x$ (using the property above).

The property $x \oplus x = 0$ shows that R has characteristic 2. Thus, $|R|$ (cardinality of R) must be 2^n for some n.

Claim $R \cong \underbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{n}$.

If $n = 1$. Clearly, $R = \{0, 1\} \cong \mathbb{F}_2$. Suppose it is true for $n - 1$. By Problem 7.10.4, we have $R \cong \langle r \rangle \times \langle r' \rangle$. $\langle r \rangle, \langle r' \rangle$ are both Boolean ring with order $< 2^n$ since for any $rg \in \langle r \rangle$ with $g \in R$,

$$(rg)^2 = r^2 g^2 = rg, \tag{7.10.26}$$

and similar for r'. Then by induction, we have $R \cong \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$.

Let $P(S)$ be a power set of n elements, so $|P(S)| = 2^n$. Let $S = \{a_1, a_2, \ldots, a_n\}$ and

$$\phi : \mathbb{F}_2 \times \cdots \times \mathbb{F}_2 \to P(S), \quad \phi(0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0) = A_i = \{a_i\}. \tag{7.10.27}$$

ϕ can be extended to a homomorphism (inverse of indicator function) with $\varepsilon \in \{0, 1\}^n$

$$\phi(\varepsilon_A + \varepsilon_B) = A \triangle B = \phi(\varepsilon_A) \triangle \phi(\varepsilon_B), \quad \phi(\varepsilon_A \varepsilon_B) = A \cap B = \phi(\varepsilon_A) \cap \phi(\varepsilon_B). \tag{7.10.28}$$

Thus, $\ker \phi = \{0\}^n$ by first isomorphism theorem, we have

$$\mathbb{F}_2 \times \cdots \times \mathbb{F}_2 = \mathbb{F}_2 \times \cdots \times \mathbb{F}_2 / \{0\}^n \cong \operatorname{Im} \phi \leq P(S). \tag{7.10.29}$$

But $|\mathbb{F}_2^n| \, |\mathbb{F}_2 \times \cdots \times \mathbb{F}_2| = |P(S)| = 2^n$, ϕ is surjective and thus $\operatorname{Im} \phi = P(S)$, so

$$\mathbb{F}_2^n \cong P(S) \;\Rightarrow\; R \cong P(S). \tag{7.10.30}$$

If S is infinite, $P(S)$ is not countable, so there is no bijective $\phi : R \to P(S)$.

Problem 7.10.6. Find all ways of writing the following integers as sums of two squares: 221, 209×221, 121×221, 5×221.

Solution. (i) $221 = 13 \times 17 = (3 + 2i)(3 - 2i)(4 + i)(4 - i)$ which is a product of irreducibles. We use this to express n as $x^2 + y^2 = z\bar{z}$ with $z = x + iy$.

$$\begin{aligned} 221 &= (10 + 11i)(10 - 11i) = 10^2 + 11^2, \\ &= (14 + 5i)(14 - 5i) = 14^2 + 5^2. \end{aligned}$$

These are the only ways since we approach it with product of irreducibles.

(ii) $209 \times 221 = 11 \times 13 \times 17 \times 19$ with $11 \equiv 3 \pmod 4$ and $19 \equiv 3 \pmod 4$. Since the power of 11 and 19 are odd, 209×221 is not of the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$ by the corollary in notes.

(iii) $121 \times 221 = 11^2 \times 13 \times 17 = 11^2(3 + 2i)(3 - 2i)(4 + i)(4 - i)$ with $11 \equiv 3 \pmod 4$. Since the power of 11 is even (2), it is of the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$ by the corollary in notes. That is,

$$\begin{aligned} 121 \times 221 &= (110 + 121i)(110 - 121i) = 110^2 + 121^2, \\ &= (154 + 55i)(154 - 55i) = 154^2 + 55^2. \end{aligned}$$

(iv) $5 \times 221 = 5 \times 13 \times 17 = (2+i)(2-i)(3+2i)(3-2i)(4+i)(4-i)$.

$$\begin{aligned} 5 \times 221 &= (9+32i)(9-32i) = 9^2 + 32^2, \\ &= (31+12i)(31-12i) = 31^2 + 12^2, \\ &= (23+24i)(23-24i) = 23^2 + 24^2, \\ &= (33+4i)(33-4i) = 33^2 + 4^2. \end{aligned}$$

These are the only ways since we approach it with product of irreducibles.

Problem 7.10.7. By working in $\mathbb{Z}[\sqrt{-2}]$, show that the only integer solutions to $x^2 + 2 = y^3$ are $x = \pm 5$, $y = 3$.

Solution. First, the only two units in $\mathbb{Z}[\sqrt{-2}]$ is ± 1. We have

$$y^3 \equiv 0, 1, 3 \pmod 4, \quad x^2 + 2 \equiv 2, 3 \pmod 4 \;\Rightarrow\; x^2 + 2 \equiv 3 \pmod 4 \;\Rightarrow\; x^2 \equiv 1 \pmod 4 \;\Rightarrow\; x = 2z + 1. \tag{7.10.31}$$

We know that $x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$. Now we want to show that the hcf of $x + \sqrt{-2}$ and $x - \sqrt{-2})$ is 1.

Then for $x = 0, \pm 1, \pm 2$, there is no solution for y, thus we can see that $x \geq 3$ and $N(x + \sqrt{-2}) = x^2 + 2 \geq 11$. Since $\mathbb{Z}[\sqrt{-2}]$ is a ED, we can use Euclidean algorithm to find the hcf,

$$x + \sqrt{-2} = x - \sqrt{-2} + 2\sqrt{-2} \qquad N(x + \sqrt{-2}) = x^2 + 2 > 8 = N(2\sqrt{-2}) \tag{7.10.32}$$

Rewrite $x = 4z \pm 1$, we have

$$\begin{aligned} 4z \pm 1 - \sqrt{-2} &= 2\sqrt{-2} \cdot (-1 - z\sqrt{-2}) + (\pm 1 + \sqrt{-2}) \qquad N(2\sqrt{-2}) = 8 > 5 = N(\pm 1 + \sqrt{-2}) \\ 2\sqrt{-2} &= (1 \pm \sqrt{-2})(\pm 1 + \sqrt{-2}) \pm 1 \qquad N(\pm 1 + \sqrt{-2}) = 5 > 1 = N(\pm 1) \end{aligned}$$

Thus, we can say the hcf of $x + \sqrt{-2}$ and $x - \sqrt{-2})$ is ± 1. Write $y^3 = \prod_{i=1}^n p_i^3$ where p_i are distinct prime (irreducible). Then

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3 \;\Rightarrow\; x + \sqrt{-2} = u \prod_{i \in A} p_i^3 \quad \text{for some } A \subseteq \{1, \ldots, n\}, \; u \in \{1, -1\} \;\text{(unit)} \tag{7.10.33}$$

Thus, $x + \sqrt{-2} = p^3$, for some $p \in \mathbb{Z}[\sqrt{-2}]$. Thus, let $p = a + b\sqrt{-2}$, we have

$$x + \sqrt{-2} = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2} \;\Rightarrow\; b(3a^2 - 2b^2) = 1 \;\Rightarrow\; b = \pm. \tag{7.10.34}$$

Thus, if $b = 1$, $a = \pm 1$. If $b = -1$, there is no solutio for a. Thus,

$$x = a(a^2 - 6b^2) = (\pm 1)(1 - 6) = \pm 5, y^3 = x^2 + 2 = 27 \;\Rightarrow\; y = 3. \tag{7.10.35}$$

Thus, $x = \pm 5$, $y = 3$ is the only solution.

Problem 7.10.8. Let $\mathbb{F}$ be a field, and let $R = \mathbb{F}[X, Y]$ be the polynomial ring in two variables.

(i) Let I be the principal ideal generated by the element $X - Y$ in R. Show that $R/I \cong \mathbb{F}[X]$.

(ii) What can you say about R/I when I is the principal ideal generated by $X^2 + Y$?

(iii) What can you say about R/I when I is the principal ideal generated by $X^2 - Y^2$?

Solution. (i) Let $\phi : R \to \mathbb{F}[X]$ by $\phi(X) = X$, $\phi(Y) = X$ (which maps Y to X) and extend it homomorphically. So

$$\ker \phi = \{f(X, Y) : f(X, X) = 0\}. \tag{7.10.36}$$

Clearly, $I = \langle X - Y \rangle \in \ker \phi$ when we set $Y = X$. Since $\mathbb{F}[X, Y] = (\mathbb{F}[Y])[X]$ ($\mathbb{F}$ is a field and thus a UFD), then $\forall f(X, Y) \in \ker \phi$, by Euclidean algorithm (Proposition 7.2.10), we can find $q(X, Y), r(X, Y) \in R = \mathbb{F}[X, Y]$,

$$f(X, Y) = (X - Y)q(X, Y) + r(X, Y) \tag{7.10.37}$$

with $\deg(r(X,Y)) < \deg(X-Y)$ for X. So $r(X,Y)$ is constant in X and $r(X,Y) = r(Y)$. Thus,

$$f(X,Y) = (X-Y)q(X,Y) + r(Y) \;\Rightarrow\; 0 = f(X,X) = r(Y). \tag{7.10.38}$$

So

$$f(X,Y) = (X-Y)q(X,Y) \;\Rightarrow\; f(X,Y) \in \langle X-Y\rangle = I \;\Rightarrow\; \ker\phi \subseteq I. \tag{7.10.39}$$

Hence, $I = \ker\phi$. For any $g(X) \in \mathbb{F}[X]$, we can find $h(X,Y) \in \mathbb{F}[X,Y]$ such that $g(X) = h(X,X)$. Thus, ϕ is surjective, $\operatorname{Im}\phi = \mathbb{F}[X]$. Then by the first isomorphism theorem,

$$R/\ker\phi \cong \operatorname{Im}\phi \;\Rightarrow\; R/I \cong \mathbb{F}[X]. \tag{7.10.40}$$

(ii) Let $\phi : R \to \mathbb{F}[X]$ by $\phi(X) = X$, $\phi(Y) = -X^2$ and extend it homomorphically. So

$$\ker\phi = \left\{f(X,Y) : f(X,-X^2) = 0\right\}. \tag{7.10.41}$$

Clearly, $I = \left\langle X^2+Y\right\rangle \in \ker\phi$ when we set $Y = -X^2$. Since $\mathbb{F}[X,Y] = (\mathbb{F}[X])[Y]$ ($\mathbb{F}$ is a field and thus a UFD), then $\forall f(X,Y) \in \ker\phi$, by Euclidean algorithm, we can find $q(X,Y), r(X,Y) \in R = \mathbb{F}[X,Y]$,

$$f(X,Y) = (Y+X^2)q(X,Y) + r(X,Y) \tag{7.10.42}$$

with $\deg(r(X,Y)) < \deg(Y+X^2)$ for Y. So $r(X,Y)$ is constant in Y and $r(X,Y) = r(X)$. Thus,

$$f(X,Y) = (Y+X^2)q(X,Y) + r(X) \;\Rightarrow\; 0 = f(X,X) = r(X). \tag{7.10.43}$$

So

$$f(X,Y) = (Y+X^2)q(X,Y) \;\Rightarrow\; f(X,Y) \in \left\langle X^2+Y\right\rangle = I \;\Rightarrow\; \ker\phi \subseteq I. \tag{7.10.44}$$

Hence, $I = \ker\phi$. For any $g(X) \in \mathbb{F}[X]$, we can find $h(X,Y) \in \mathbb{F}[X,Y]$ such that $g(X) = h(X,-X^2)$. Thus, ϕ is surjective, $\operatorname{Im}\phi = \mathbb{F}[X]$. Then by the first isomorphism theorem,

$$R/\ker\phi \cong \operatorname{Im}\phi \;\Rightarrow\; R/I \cong \mathbb{F}[X]. \tag{7.10.45}$$

(iii) Let $\phi : R \to \mathbb{F}[X] \times \mathbb{F}[Y]$ by $\phi(X) = (X,Y)$ and $\phi(Y) = (-X,Y)$ and extend it homomorphically. So

$$\ker\phi = \{f(X,Y) : \phi(f(X,Y) = (0,0)\}. \tag{7.10.46}$$

In the first coordinate, we replace Y with $-X$, so we need $X+Y$ as a factor. Similarly, for the second coordinate, we need $X-Y$. Thus, we can have

$$\ker\phi = \left\langle X^2-Y^2\right\rangle = I. \tag{7.10.47}$$

However, the map is not surjective since $f(X) \in \mathbb{F}[X]$ and $g(Y) \in \mathbb{F}[Y]$ must have the same order (by having the same coefficients). Thus,

$$\operatorname{Im}\phi = \{(f(X),g(Y)) : \deg(f(X)) = \deg(g(Y)), f(X) \in \mathbb{F}[X], g(Y) \in \mathbb{F}[Y]\}. \tag{7.10.48}$$

By the first isomorphism theorem, $R/I \cong \operatorname{Im}\phi \leq \mathbb{F}[X] \times \mathbb{F}[Y]$.

Problem 7.10.9. Determine whether or not the following rings are fields, EDs, PIDs, UFDs, integral domains:

$$\text{(i) } \mathbb{Z}[X], \quad \text{(ii) } \mathbb{Z}[X]/\left\langle X^2+1\right\rangle, \quad \text{(iii) } (\mathbb{Z}/2\mathbb{Z})[X]/\left\langle X^2+1\right\rangle,$$

$$\text{(iv) } \mathbb{Z}[X]/\left\langle 2, X^2+X+1\right\rangle, \quad \text{(v) } \mathbb{Z}[X]/\left\langle 3, X^2+1\right\rangle, \quad \text{(vi) } \mathbb{Z}[X]/\left\langle 3, X^3-X+1\right\rangle. \tag{7.10.49}$$

Solution. Here we use the following properties:

1. $R[X]$ is a PID iff R is a field.

2. If R is a UFD, then $R[X]$ is also a UFD.

3. Field $\Rightarrow$ ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ ID.

(i) $\mathbb{Z}[X]$. The fact that $\mathbb{Z}$ is not a field implies that $\mathbb{Z}[X]$ is not PID. Since $\mathbb{Z}$ is ED, it is UFD. Then $\mathbb{Z}[X]$ is UFD.

(ii) $\mathbb{Z}[X]/\left\langle X^2+1\right\rangle$. Let $f(X)\in\mathbb{Z}[X]$ and $I=\left\langle X^2+1\right\rangle$. By Euclidean algorithm for polynomials, we have

$$f(X)=g(X)(X^2+1)+r(X),\quad g(X),r(X)\in\mathbb{Z}[X],\ \deg(r(X))<2. \tag{7.10.50}$$

Then

$$f(X)+I=aX+b+g(X)(X^2+1)+I=aX+b+I. \tag{7.10.51}$$

Thus,

$$\begin{aligned} a_1X+b_1+I+a_2X+b_2+I &= (a_1+a_2)X+(b_1+b_2)+I,\\ (a_1X+b_1+I)(a_2X+b_2+I) &= a_1a_2X^2+(a_2b_1+a_1b_2)X+b_1b_2+I\\ &= (a_2b_1+a_1b_2)X+(b_1b_2-a_1a_2)+I. \end{aligned}$$

Thus, we have (or by the third isomorphism theorem)

$$\mathbb{Z}[X]/\left\langle X^2+1\right\rangle\cong\mathbb{Z}[i] \tag{7.10.52}$$

by $b+aX\ \Leftrightarrow\ b+ai$. We already know that $\mathbb{Z}[i]$ is a ED and thus a PID. So $\mathbb{Z}[X]/\left\langle X^2+1\right\rangle$ is a ED and PID, etc. However, we have that $2\in\mathbb{Z}[X]/\left\langle X^2+1\right\rangle$ which doesn't have inverse. Thus, we can say that $\mathbb{Z}[X]/\left\langle X^2+1\right\rangle$ is not a field.

(iii) $(\mathbb{Z}/2\mathbb{Z})[X]/\left\langle X^2+1\right\rangle$. With the similar argument as above (or by the third isomorphism theorem), we have

$$(\mathbb{Z}/2\mathbb{Z})[X]/\left\langle X^2+1\right\rangle=\mathbb{F}_2[X]/\left\langle X^2+1\right\rangle\cong\mathbb{F}_2[i]=\{0,1,i,1+i\}. \tag{7.10.53}$$

We see that $\mathbb{F}_2[i]$ is not an integral domain since $(1+i)^2\mod 2=0$.

It is obvious that 1 is a unit. Also,

$$1\cdot(1+i)=1+i\neq i,\quad 1\cdot i=i,\quad (1+i)i=1+i\neq i. \tag{7.10.54}$$

Thus, if $i=ab$, $a,b\in\mathbb{F}_2[i]$, we have $a=1$ or $b=1$ and thus i is irreducible. Since $1+i=i(1+i)$, $1+i$ is not irreducible. However, $1+i\neq i^n$ for any $n\in\mathbb{Z}$. So $\mathbb{F}_2[i]$ is not a UFD.

Thus, $(\mathbb{Z}/2\mathbb{Z})[X]/\left\langle X^2+1\right\rangle$ is not field, ED, PID, UFD, integral domain. (In this case, b_0 is not related to b_1).

(iv) Let $f(X)\in\mathbb{Z}[X]$ and $I=\left\langle 2,X^2+X+1\right\rangle$. By Euclidean algorithm for polynomials, we have

$$f(X)=g(X)(X^2+X+1)+r(X),\quad g(X),r(X)\in\mathbb{Z}[X],\ \deg(r(X))<2. \tag{7.10.55}$$

Then

$$f(X)+I=aX+b+I,\quad a,b\in\{0,1\}. \tag{7.10.56}$$

Thus,

$$\mathbb{Z}[X]/\left\langle 2,X^2+X+1\right\rangle=\{I,1+I,X+I,X+1+I\}. \tag{7.10.57}$$

Then, $I(1+I)=I$, $(1+I)(1+I)=1+I$, $(X+I)(1+I)=X+I$, $(X+1+I)(1+I)=X+1+I$. $1+I$ is the

multiplicative identity. I is the additional identity.

$$\begin{aligned}(X+I)(X+I) &= X^2+2XI+I = (X^2+X+1)+X+1+I = X+1+I,\\ (X+1+I)(X+1+I) &= X^2+2X+1+I = (X^2+X+1)+X+I = X+I,\\ (X+I)(X+1+I) &= X^2+X+I = X^2+X+1+1+I = 1+I.\end{aligned}$$

Thus, $X+I$ and $X+1+I$ are multiplicative inverse to each other. Hence, $\mathbb{Z}[X]/\left\langle 2, X^2+X+1\right\rangle$ is a field, ED, etc. Another way to see it is using $\mathbb{Z}[X]/\left\langle p, f_\alpha(X)\right\rangle \cong \mathbb{F}_p[\alpha]$ which is

$$\mathbb{Z}[X]/\left\langle 2, X^2+X+1\right\rangle \cong \mathbb{F}_2[\omega], \quad \omega = \frac{-1\pm\sqrt{-3}}{2}. \tag{7.10.58}$$

In particular, take $\omega = \frac{-1+\sqrt{-3}}{2}$

$$\mathbb{F}_2[\omega] = \left\{0, 1, \frac{-1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\right\} \tag{7.10.59}$$

We have

$$\begin{aligned}\left(\frac{-1+\sqrt{-3}}{2}\right)^2 &= \frac{-2-2\sqrt{-3}}{4} = \frac{-1-\sqrt{3}}{2} = (-1)\frac{1+\sqrt{3}}{2} = 1\cdot\frac{1+\sqrt{3}}{2} \pmod{2\omega}\\ \left(\frac{1+\sqrt{-3}}{2}\right)^2 &= \frac{-2+2\sqrt{-3}}{4} = \frac{-1+\sqrt{3}}{2}\\ \left(\frac{-1+\sqrt{-3}}{2}\right)\left(\frac{1+\sqrt{-3}}{2}\right) &= \frac{-3-1}{4} = -1 = 1 \pmod 2\end{aligned}$$

Thus, $\frac{-1+\sqrt{-3}}{2}$ and $\frac{1+\sqrt{-3}}{2}$ are multiplicative inverse to each other.

(v) $\mathbb{Z}[X]/\left\langle 3, X^2+1\right\rangle$. With similarly argument, we have

$$\mathbb{Z}[X]/\left\langle 3, X^2+1\right\rangle \cong \mathbb{F}_3[i] = \{0,1,2,i,1+i,2+i,2i,1+2i,2+2i\}. \tag{7.10.60}$$

Then we have

$$\begin{aligned}2\cdot 2 &= 4\equiv 1 \pmod 3 \quad\Rightarrow\quad 2 \text{ is the inverse of itself}\\ i\cdot 2i &= -2\equiv 1 \pmod 3 \quad\Rightarrow\quad i \text{ is the inverse of } 2i\\ (1+i)(2+i) &= 2-1+3i\equiv 1 \pmod 3 \quad\Rightarrow\quad 1+i \text{ is the inverse of } 2+i\\ (1+2i)(2+2i) &= 2-4+6i\equiv 1 \pmod 3 \quad\Rightarrow\quad 1+2i \text{ is the inverse of } 2+2i\end{aligned}$$

Thus, $\mathbb{Z}[X]/\left\langle 3, X^2+1\right\rangle$ is field, ED, etc.

(vi) $\mathbb{Z}[X]/\left\langle 3, X^3-X+1\right\rangle$. Let $f(X)\in\mathbb{Z}[X]$ and $I = \left\langle 3, X^3-X+1\right\rangle$. By Euclidean algorithm for polynomials, we have

$$f(X) = g(X)(X^3-X+1)+r(X), \quad g(X), r(X)\in\mathbb{Z}[X],\ \deg(r(X))<3. \tag{7.10.61}$$

Then

$$f(X)+I = aX^2+bX+c+I, \quad a,b,c\in\{0,1,-1\}. \tag{7.10.62}$$

Thus,

$$\begin{aligned}\mathbb{Z}[X]/\left\langle 3, X^3-X+1\right\rangle = \{&I, 1+I, -1+I, X+I, X+1+I, X-1+I, -X+I, -X+1+I, -X-1+I,\\ &X^2+I, X^2+1+I, X^2-1+I, X^2+X+I, X^2+X+1+I,\\ &X^2+X-1+I, X^2-X+I, X^2-X+1+I, X^2-X-1+I,\\ &-X^2+I, -X^2+1+I, -X^2-1+I, -X^2+X+I, -X^2+X+1+I,\\ &-X^2+X-1+I, -X^2-X+I, -X^2-X+1+I, -X^2-X-1+I\}\end{aligned}$$

Then, $1+I$ is the multiplicative identity. I is the additional identity.

$$\begin{aligned}
(-1+I)(-1+I) &= 1+I,\\
(-X+I)(X^2-1+I) &= -X^3+X+I=-(X^3-X+1)+1+I=1+I,\\
(-X-1+I)(X^2-X+I) &= -X^3+X+I=-(X^3-X+1)+1+I=1+I,\\
(-X+1+I)(X^2+X+I) &= -X^3-X+I=-(X^3-X+1)+1+I=1+I,\\
-(X^2+1+I)(X^2-X+1+I) &= -X^4+X^3-2X^2+X-1+I=X^3-X-1+I=1+I,\\
-(X^2+I)(X^2+X-1+I) &= -X^4-X^3+X^2+I=-X^3+X-1+1+I=1+I,\\
-(X^2-X-1+I)(X^2+X+1+I) &= -X^4+X^2+2X+1+I=1+I.
\end{aligned}$$

Thus, $\pm(X+I)$ is the inverse of $\mp(X^2-1+I)$,

$\pm(X+1+I)$ is the inverse of $\mp(X^2-X+I)$

$\pm(X-1+I)$ is the inverse of $\mp(X^2+X+I)$

$\pm(X^2+1+I)$ is the inverse of $\mp(X^2-X+1+I)$

$\pm(X^2+I)$ is the inverse of $\mp(X^2+X-1+I)$

$\pm(X^2-X-1+I)$ is the inverse of $\mp(X^2+X+1+I)$

Hence $\mathbb{Z}[X]/\langle 3, X^3-X+1\rangle$ is a field, ED, etc.

Problem 7.10.10. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:

$$X^4+2X+2, \quad X^4+18X^2+24, \quad X^3-9, \quad X^3+X^2+X+1, \quad X^4+1, \quad X^4+4. \tag{7.10.63}$$

Solution. We apply Eisenstein's criterion (Proposition 7.8.10):

(i) X^4+2X+2. Take $p=2$, then $p=2\nmid 1=a_4$, $p=2\mid 2=a_1$ and $p=2\mid 2=a_0$. Also $p^2=4\mid 2=a_0$. Thus, $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(ii) X^4+18X^2+24. Take $p=3$, then $p=3\nmid 1=a_4$, $p=3\mid 18=a_1$ and $p=3\mid 24=a_0$. Also $p^2=9\mid 24=a_0$. Thus, $f(X)$ is irreducible in $\mathbb{Q}[X]$. Thus, $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(iii) X^3-9. Suppose that $X^3-9=(X^2+aX+b)(X+c)$ and thus $bc=-9$. Therefore, $c=\pm1,\pm3,\pm9$. However, $\pm1,\pm3,\pm9$ are not roots of X^3-9. So $f(X)$ is irreducible in $\mathbb{Z}[X]$ and thus irreducible in $\mathbb{Q}[X]$.

(iv) $X^3+X^2+X+1=(X^2+1)(X+1)$. So X^3+X^2+X+1 is not irreducible in $\mathbb{Z}[X]$ and thus not irreducible in $\mathbb{Q}[X]$.

(v) X^4+1.

Suppose that $X^4+1=(X^3+aX^2+bX+c)(X+d)$ and thus $cd=1$. Therefore, $d=\pm1$. However, ±1 are not roots of X^4+1.

Suppose that $X^4+1=(X^2+aX+b)(X^2+cX+d)=X^4+(a+c)X^3+(b+d+ac)X^2+(bc+ad)X+bd$ and thus $bd=1$. Therefore, $b,d=\pm1$ and

$$a+c=0,\ \pm2+ac=0\ \Rightarrow\ \pm2=a^2 \tag{7.10.64}$$

which is contradiction. Thus, X^4+1 is irreducible in $\mathbb{Z}[X]$ and thus irreducible in $\mathbb{Q}[X]$.

(vi) $X^4+4=(X^2-2X+2)(X^2+2X+2)$. Thus, it is not irreducible in $\mathbb{Z}[X]$ and thus not irreducible in $\mathbb{Q}[X]$.

Problem 7.10.11. (i) Consider the polynomial $f(X,Y)=X^3Y+X^2Y^2+Y^3-Y^2-X-Y+1$ in $\mathbb{C}[X,Y]$. Write it as an element of $\mathbb{C}[X][Y]$, that is collect together terms in powers of Y, and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X,Y]$.

(ii) Let F be any field. Show that the polynomial $f(X,Y)=X^2+Y^2-1$ is irreducible in $F[X,Y]$, unless F has characteristic 2. What happens in that case?

Solution. (i) We have that $\mathbb{C}[X][Y]$ is UFD since $\mathbb{C}$ is UFD.

$$f(X,Y) = Y^3 + (X^2-1)Y + (X^3-X)Y - (X-1). \tag{7.10.65}$$

Thus, by Eisenstein's criterion

$$(X-1) \mid (X^2-1), \quad (X-1) \mid (X^3-X), \quad (X-1) \mid -(X-1), \quad (X-1)^2 \nmid -(X-1), \tag{7.10.66}$$

then $f(X,Y)$ is irreducible (and hence prime since $\mathbb{C}[X,Y]$ is a UFD).

(ii) We have $f(X,Y) = X^2 + Y^2 - 1 = Y^2 + (X-1)(X+1)$. Both of $X-1$ and $X+1$ are irreducible.

If $X+1$ and $X-1$ are not associate, we have $f(X,Y)$ is irreducible. In this case, $1 \neq -1$ which implies that $2 \neq 0$ i.e. $\operatorname{char} \mathbb{F} \neq 2$.

If $\operatorname{char} \mathbb{F} = 2$, we have

$$X^2 + Y^2 - 1 = X^2 + Y^2 + 2XY + 2X + 2Y + 2 - 1 = (X+Y+1)(X+Y+1) \tag{7.10.67}$$

which is not irreducible.

7.11 Summary

Recalling the previous results, we have that

Commutative rings $\supset$ integral domains $\supset$ integrally closed domains[17] $\supset$ unique factorization domains $\supset$ principal ideal domains $\supset$ Euclidean domains $\supset$ fields.

	F	ED	PID	UFD	ID	CR
$\mathbb{Z}$	×	√	√	√	√	√
$\mathbb{Z}[i]$	×	√	√	√	√	√
$\mathbb{Z}[\sqrt{-2}]$	×	√	√	√	√	√
$\mathbb{Z}[\omega]$	×	√	√	√	√	√
$\mathbb{Z}[\sqrt{-3}]$	×	×	×	×	√	√
$\mathbb{Z}[\sqrt{-5}]$	×	×	×	×	√	√
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$	√	√	√	√	√	√
$\mathbb{Z}/6\mathbb{Z}$	×	×	×	×	×	√
$\mathbb{Q}$	√	√	√	√	√	√
$\mathbb{R}$	√	√	√	√	√	√
$\mathbb{C}$	√	√	√	√	√	√
$\mathbb{Z}[X]$	×	×	×	√	√	√
$\mathbb{Q}[X]$	×	√	√	√	√	√
$\mathbb{F}[X]$	×	√	√	√	√	√

where $\omega = (1+\sqrt{-3})/2$, $\mathbb{F}$ is a field and p is a prime number.

R is a field if and only if $R[X]$ is a PID.

For commutative ring R, R/I is a field if and only if I is a maximal ideal, R/I is an integral domain if and only if I is a prime ideal.

A maximal ideal is a prime ideal. In PID, maximal ideal and prime ideal are equivalent.

[17] need details

Chapter 8

Linear Algebra

8.1 Vector spaces

8.1.1 Definitions

The crucial properties of field $\mathbb{F}$ are as follows (see definition of field (Definition 7.1.4))

(i) $\mathbb{F}$ is an abelian group under $+$, with additive identity 0.

(ii) $\mathbb{F}\setminus\{0\}$ is an abelian group under $\cdot$, with multiplicative identity 1.

(iii) Multiplication is distributive over addition, $a(b+c) = ab + ac$ for all $a, b, c \in \mathbb{F}$.

Definition 8.1.1. For a field $\mathbb{F}$ (could be a general field, not only $\mathbb{R}$ or $\mathbb{C}$), the set V is a vector space over $\mathbb{F}$ if the following holds.

(A) V is an abelian group under an operation $+$, i.e., (see Definition 6.1.1)

(A0) $+ : V \to V$, $(v_1, v_2) \mapsto v_1 + v_2 \in V$;

(A1) For all $v_1, v_2, v_3 \in V$, $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$;

(A2) For all $v_1, v_2 \in V$, $v_1 + v_2 = v_2 + v_1$;

(A3) There exists $0 \in V$ such that $v + 0 = v$ for all $v \in V$;

(A4) For each $v \in V$ there exists $-v \in V$ such that $-v + v = 0$.

(B) There exists a multiplication $\cdot$ by scalars on V, i.e.,

(B0) $\cdot : \mathbb{F} \times V \to V$, $(\lambda, v) \mapsto \lambda v$;

(B1) For all $\lambda \in \mathbb{F}$, $v_1, v_2 \in V$, $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$;

(B2) For all $\lambda_1, \lambda_2 \in \mathbb{F}$, $v \in V$, $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$;

(B3) For all $\lambda_1, \lambda_2 \in \mathbb{F}$, $v \in V$, $(\lambda_1\lambda_2)v = \lambda_1(\lambda_2 v)$;

(B4) For all $v \in V$, $1 \cdot v = v$.

Lemma 8.1.1. Let V be a vector space over $\mathbb{F}$ and let $v \in V$, $\lambda \in \mathbb{F}$. Then

(i) $0 \cdot v = 0$, $\lambda \cdot 0 = 0$;

(ii) $-v = (-1) \cdot v$;

(iii) if $\lambda v = 0$ then either $\lambda = 0$ or $v = 0$.

Proof. (i) $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$, so $0 = 0 \cdot v$;

(ii) $-v + v = 0 = 0v = (-1 + 1)v = (-1)v + 1v = (-1)v + v$, so $-v = (-1)v$.

(iii) Let $\lambda v = 0$ and suppose $\lambda \neq 0$. Then λ^{-1} exists and $\lambda^{-1}(\lambda v) = \lambda^{-1}0 = 0$ but $\lambda^{-1}(\lambda v) = (\lambda^{-1}\lambda)v = 1v = v$ so $v = 0$. □

Example 8.1.2. (i) The space $\mathbb{F}^n$ of n-tuples with entries in $\mathbb{F}$.

(ii) Let X be any set. The set $\mathbb{F}^X$ of all functions $X \to \mathbb{F}$ is a vector space over $\mathbb{F}$ addition and multiplication defined pointwise.

Definition 8.1.2. Let V be a vector space over $\mathbb{F}$. A subset $U \subseteq V$ is a subspace of V, written $U \leq V$ if

(i) $0 \in U$;

(ii) $\forall u_1, u_2 \in U \ \Rightarrow \ u_1 + u_2 \in U$;

(iii) $\forall \lambda \in \mathbb{F}, \ u \in U \ \Rightarrow \ \lambda u \in U$.

Equivalently, $U \neq \emptyset$ and U is closed under linear combinations[1].

Lemma 8.1.3. If V is a vector space over $\mathbb{F}$ and $U \leq V$ then U is a vector space over $\mathbb{F}$ under the restriction of the operations $+$ and $\cdot$ on V to U.

Proof. This is direct result from Definition 8.1.2. □

Example 8.1.4. (i) $\mathbb{R}^{\mathbb{R}}$ is a vector space over $\mathbb{R}$.

(ii) The set $C(\mathbb{R})$ of continuous real functions is a subspace, and hence a real vector space.

(iii) Similarly, one can also consider the subspaces $D(\mathbb{R})$ and $P(\mathbb{R})$ of differentiable and polynomial functions, respectively.

Remark. If $n \in \mathbb{Z}^+$ (as n could be 0), $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$, $v_1, \ldots, v_n \in V$ write $\sum_{i=1}^n \lambda_i v_i$ for the linear combination $\lambda_1 v_1 + \cdots + \lambda_n v_n$. By convention, $\sum_{i=1}^0 \lambda_i v_i = 0$.

Also note that all linear combinations are finite. If $S \subseteq V$, the linear combination $\sum_{v \in S} \lambda_v v$ has only finitely many v such that $\lambda_v \neq 0$.

8.1.2 Algebra and subalgebra

Definition 8.1.3 (algebra)**.** An algebra over a field is a vector space equipped with a bilinear product[2].

Definition 8.1.4 (subalgebra)**.** A subalgebra of an algebra over a commutative ring or field is a vector subspace which is closed under the multiplication of vectors[3].

Remark. The restriction of the algebra multiplication makes it an algebra over the same ring or field[4].

8.1.3 Linear span, linear independence, basis and dimension

Definition 8.1.5. The vectors $v_1, \ldots, v_n$ in V span (or generate) V over $\mathbb{F}$ if any $v \in V$ is a linear combination of $v_1, \ldots, v_n$. Write $V = \langle v_1, \ldots, v_n \rangle$.

More generally, if $S \subseteq V$ then S spans V if $\forall v \in V$,

$$\exists n \in \mathbb{Z}^+, \ v_1, \ldots, v_n \in S, \ \lambda_1, \ldots, \lambda_n \in \mathbb{F} \quad \text{s.t.} \quad v = \sum_{i=1}^n \lambda_i v_i. \tag{8.1.1}$$

Remark. The span of a set $S \subseteq V$ (not necessarily finite) is defined to be the intersection W of all subspaces of V which contain S. W is referred to as the subspace spanned by S, or by the vectors in S. Conversely, S is called a spanning set of W.

Example 8.1.5. (i) $P_2(\mathbb{R})$ is spanned by $1, X, X^2$ (with coefficients 0 or 1).

(ii) $P(\mathbb{R})$ is not finite-dimensional.

[1] need definition of linear combinations
[2] need checking, see wiki, algebra over a field
[3] need checking
[4] need checking

Definition 8.1.6 (linear independence)**.** The vectors $v_1, \ldots, v_n$ are linearly independent in V over $\mathbb{F}$ if

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \;\Rightarrow\; \lambda_1 = \cdots = \lambda_n = 0. \tag{8.1.2}$$

Otherwise, the vectors are linearly dependent.

More generally, if $S \subseteq V$ then S is linearly independent precisely if every finite subset of S is linearly independent.

Remark. 0 is never contained in a linearly independent set as $1 \cdot 0 = 0$.

Remark. (i) $V = \mathbb{C}$ is a vector space over $\mathbb{R}$ and 1, i are linearly independent.

(ii) $V = \mathbb{C}$ is also a vector space over $\mathbb{C}$. In this case, 1, i are linearly dependent.

Definition 8.1.7 (basis)**.** The vectors $v_1, \ldots, v_n$ form a basis of V if they span V over $\mathbb{F}$ and are linearly independent.

Example 8.1.6. (i) $P_2(\mathbb{R})$ has standard basis $\{1, X, X^2\}$.

(ii) $\mathbb{F}^n$ has standard basis $\{e_1, \ldots, e_n\}$ where $\mathbf{e}_i = (0, \ldots, 1, \ldots, 0)^T$ (ith element is 1, otherwise 0).

(iii) $\{0\}$ has basis $\emptyset$.

Lemma 8.1.7. $v_1, \ldots, v_n \in V$ form a basis of V over $\mathbb{F}$ if and only if each element $v \in V$ can be written uniquely as $v = \sum_{i=1}^n \lambda_i v_i$ with $\lambda_i \in \mathbb{F}$.

Proof. $\forall v \in V$. $v_1, \ldots, v_n$ span V so $v = \sum_{i=1}^n \lambda_i v_i$ for some $\lambda_i \in \mathbb{F}$. If also $v = \sum_{i=1}^n \mu_i v_i$ then $0 = \sum_{i=1}^n (\lambda_i - \mu_i) v_i$, so as $v_1, \ldots, v_n$ are linearly independent, we have $\lambda_i = \mu_i$ for $i = 1, \ldots, n$.

Conversely, since each $v \in V$ is a linear combination of $v_1, \ldots, v_n$, we have $v_1, \ldots, v_n$ span V over $\mathbb{F}$. They are linearly dependent since if $\sum_{i=1}^n \lambda_i v_i = 0 = \sum_{i=1}^n 0 v_i$ then $\lambda_i = 0$ for $i = 1, \ldots, n$ by uniqueness. □

Lemma 8.1.8. If $v_1, \ldots, v_n$ span V over $\mathbb{F}$, some subset of $\{v_1, \ldots, v_n\}$ is a basis of V.

Proof. If $v_1, \ldots, v_n$ are linearly independent, we are done. Otherwise, for some k, there exist $\alpha_1, \ldots, \alpha_{k-1} \in \mathbb{F}$ with $v_k = \alpha_1 v_1 + \cdots + \alpha_{k-1} v_{k-1}$. (If $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ with not all $\lambda_i = 0$, take k maximal with $\lambda_k \neq 0$ and let $\alpha_i = -\frac{\lambda_i}{\lambda_k}$.)

Then $v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n$ still span V since whenever $v = \sum_{i=1}^n \lambda_i v_i$ then $v = \sum_{i=1}^{k-1} (\alpha_i + \lambda_i) v_i + \sum_{i=k+1}^n \lambda_i v_i$. Continue deleting until we have a basis. □

Theorem 8.1.9 (Steinitz exchange lemma)**.** Let V be a finite dimensional vector space over $\mathbb{F}$. Let $v_1, \ldots, v_m$ be linearly independent and let $w_1, \ldots, w_n$ span V over $\mathbb{F}$. Then $m \leq n$, and reordering the w_i if necessary, the vectors $v_1, \ldots, v_m, w_{m+1}, \ldots, w_n$ span V.

Proof. Suppose we have replaced $r \geq 0$ of the w_i by v_i already, renumbering the w_i if necessary, we have $v_1, \ldots, v_r, w_{r+1}, \ldots, w_n$ span V. If $r = m$, we are done. So assume $r < m$. Then

$$v_{r+1} = \sum_{i=1}^r \alpha_i v_i + \sum_{i=r+1}^n \beta_i w_i \tag{8.1.3}$$

for some $\alpha_i, \beta_i \in \mathbb{F}$. Note that $\beta_i \neq 0$ for some i since $v_1, \ldots, v_r, v_{r+1}$ are linearly independent. After reordering $w_{r+1}, \ldots, w_n$ we have $\beta_{r+1} \neq 0$. Then

$$w_{r+1} = \sum_{i=1}^r \frac{-\alpha_i}{\beta_{r+1}} v_i + \frac{1}{\beta_{r+1}} v_{r+1} + \sum_{i=r+2} \frac{-\beta_i}{\beta_{r+1}} w_i. \tag{8.1.4}$$

It follows that V is spanned by $v_1, \ldots, v_r, v_{r+1}, w_{r+2}, \ldots, w_n$. After m steps, we shall have replaced m of the w_i by the v_i, retaining the spanning property.

If $m > n$, we have $v_1, \ldots, v_n$ span V over $\mathbb{F}$. But v_m can be expressed by a linear combination of $v_1, \ldots, v_n$ since $v_1, \ldots, v_m$ are linearly independent. Therefore, it follows that $m \leq n$. □

Theorem 8.1.10 (dimension)**.** If V is a finite dimensional vector space over $\mathbb{F}$, any two bases have the same size, the dimension of V over $\mathbb{F}$, $\dim_{\mathbb{F}} V$.

Proof. Let $\{v_1, \ldots, v_m\}$ and $\{w_1, \ldots, w_n\}$ be two bases. Thus, $v_1, \ldots, v_m$ are linearly independent and span V and so are $w_1, \ldots, w_n$. Then by Steinitz exchange lemma (Theorem 8.1.9), $m \leq n$ since the v_i are linearly independent and the w_i span V. Also $n \leq m$ since the w_i are linearly independent and the v_i span V. □

Example 8.1.11. (i) $\dim_{\mathbb{F}} \mathbb{F}^n = n$, (ii) $\dim_{\mathbb{R}} P_2(\mathbb{R}) = 3$, (iii) $\dim_{\mathbb{R}} \mathbb{C} = 2$, (iv) $\dim_{\mathbb{F}} \mathbb{F} = 1$.

Lemma 8.1.12. If V is a finite dimensional vector space over $\mathbb{F}$, and if the vectors $v_1, \ldots, v_k$ are linearly independent for some $k \geq 0$, there exists a basis $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ of V.

Remark. If V is finite dimensional then whenever $U \leq V$ then $\dim U \leq \dim V$ with equality if and only if $U = V$.

Proof. If $v_1, \ldots, v_k$ span V, we are done. Otherwise, take $v_{k+1} \in V \setminus \langle v_1, \ldots, v_k \rangle$. Then $v_1, \ldots, v_{k+1}$ are linearly independent. We shall obtain a basis after $\dim V - k$ steps. □

Lemma 8.1.13. Let V be a vector space over $\mathbb{F}$ with $\dim V = n$.

(i) An independent set has at most n vectors, with equality if and only if it as basis.

(ii) A spanning set has at least n vectors, with equality if and only if it a basis.

Proof. (i) This follows from Lemma 8.1.12 and Theorem 8.1.10.

(ii) This follows from Lemma 8.1.8 and Theorem 8.1.10.

□

Then Lemma 8.1.13 gives

Lemma 8.1.14. Let $\dim_{\mathbb{F}} V = n$. The following are equivalent.

(i) $v_1, \ldots, v_n$ form a basis.

(ii) $v_1, \ldots, v_n$ are linearly independent.

(iii) $v_1, \ldots, v_n$ span V.

Lemma 8.1.15. Let $S \subseteq V$. There is a unique smallest subspace U of V containing S, denoted by $U = \langle S \rangle$, the subspace generated by S. In fact, U consists of linear combinations of elements of S.

Proof. If we write U for the set of linear combinations of elements of S then U is a subspace of V. On the other hand, U as defined above has to be in any subspace containing S. □

Example 8.1.16. Let $V = \mathbb{R}^{\mathbb{R}}$ (see Example 8.1.4) and $S = \{1, X, X^2, \ldots\}$. Then $\langle S \rangle = P(\mathbb{R})$, the subspace of polynomial functions.

Remark. (i) The intersection of any collection of subspaces is a subspace.

(ii) Note that $U \cup W$ is a subspace if and only if $U \subseteq W$ or $W \subseteq U$.

Definition 8.1.8 (sum of vector space)**.** If $U, W \leq V$ define $U + W = \{u + w : u \in U, w \in W\}$. Then $U + W \leq V$.

Theorem 8.1.17. If U, W are finite dimensional subspaces of V then $U + W$ is also finite dimensional and $\dim U + W = \dim U + \dim W - \dim U \cap W$.

Proof. Let $v_1, \ldots, v_k$ be a basis for $U \cap W$. Extend this to $v_1, \ldots, v_k, u_1, \ldots, u_l$ a basis for U and to $v_1, \ldots, v_k, w_1, \ldots, w_m$ a basis for W. We claim $v_1, \ldots, v_k, u_1, \ldots, u_l, w_1, \ldots, w_m$ is a basis for $U + W$.

If $v \in U + W$, then $v = u + w$ for some $u \in U$, $w \in W$. Now $u = \sum \alpha_i' v_i + \sum \beta_i u_i$ for some $\alpha_i', \beta_i \in \mathbb{F}$ and $w = \sum \alpha_i'' v_i + \sum \gamma_i w_i$ for some $\alpha_i'', \gamma_i \in \mathbb{F}$, and therefore

$$v = \sum (\alpha_i' + \alpha_i'') v_i + \sum \beta_i u_i + \sum \gamma_i w_i := \sum \alpha_i v_i + \sum \beta_i u_i + \sum \gamma_i w_i. \tag{8.1.5}$$

Suppose $\sum \alpha_i v_i + \sum \beta_i u_i + \sum \gamma_i w_i = 0$. Then

$$\sum \alpha_i v_i + \sum \beta_i u_i = -\sum \gamma_i w_i = \sum \delta_i v_i \tag{8.1.6}$$

for some $\delta_i \in \mathbb{F}$, using that the LHS is in U and the RHS is in W, so both vectors are in $U \cap W$. Then

$$\sum (\alpha_i - \delta_i)\, v_i + \sum \beta_i u_i = 0, \tag{8.1.7}$$

and as $v_1, \ldots, v_k, u_1, \ldots, u_l$ form a basis of U, we have that all β_i are 0. But then

$$\sum \alpha_i v_i + \sum \gamma_i w_i = 0, \tag{8.1.8}$$

and as $v_1, \ldots, v_k, w_1, \ldots, w_m$ form a basis of W, we have that all α_i, γ_i are 0. □

Definition 8.1.9 (direct sum)**.** Let V be a vector space over $\mathbb{F}$ and suppose $U, W \leq V$. Then

$$V = U \oplus W \tag{8.1.9}$$

if every element v of V can be written uniquely as $v = u + w$ with $u \in U$ and $w \in W$. If so, we say W is the complement (or complementary subspace) of U in V.

Lemma 8.1.18. Suppose $U, W \leq V$. Then $V = U \oplus W$ if and only if $U + W = V$ and $U \cap W = \{0\}$.

Proof. ($\Rightarrow$). If $V = U \oplus W$, then $V = U + W$. Thus, $\forall v \in V$, we have $v = u + w$ for $u \in U$ and $w \in W$. If $U \cap W \neq \{0\}$, then there exists $x \neq 0$ such that

$$v = u + w = (u + x) + (w - x), \quad u + x \in U, w - x \in W \;\Rightarrow\; \text{Contradiction.} \tag{8.1.10}$$

($\Leftarrow$). If $U \cap W = \{0\}$ and $U + W = V$, there exists $u_1, u_2 \in U$ and $w_1, w_2 \in W$ such that

$$v = u_1 + w_1 = u_2 + w_2 \;\Rightarrow\; u_1 - u_2 = w_2 - w_1 \tag{8.1.11}$$

where the LHS in U and the RHS in W. Thus, $u_1 = u_2, w_1 = w_2$. Therefore, $V = U \oplus W$. □

Lemma 8.1.19. If V is a finite dimensional vector space over $\mathbb{F}$ and $U \leq V$, then U has a complement in V. (Note this is not at all unique unless $U = \{0\}$ or $U = V$.)

Proof. Take $v_1, \ldots, v_k$ a basis for U and extend to a basis $u_1, \ldots, u_k, w_{k+1}, \ldots, w_n$ for V. Then $W = \langle w_{k+1}, \ldots, w_n \rangle$ is a complement of U in V. □

Definition 8.1.10. Suppose $V_1, \ldots, V_k \leq V$ and let $\sum V_i = \{\sum v_i : v_i \in V_i\} \leq V$. The sum is direct, written as $\bigotimes V_i$, if each $v \in V$ is uniquely expressible as $\sum v_i$ with $v_i \in V_i$.

Lemma 8.1.20. Let $V_1, \ldots, V_k \leq V$. The following are equivalent.

(i) $\sum_i V_i$ is direct.

(ii) If B_i is a basis for V_i then $B = \bigcup_{i=1}^k B_i$ is a basis for $\sum_i V_i$.

(iii) For each i, $V_i \cap \sum_{j \neq i} V_j = \{0\}$ and $V = \sum_i V_i$

Note that in (iii), if $k > 2$ it is not enough to assume $V_i \cap V_j = \{0\}$ for all $i \neq j$.

Proof. (i) $\Rightarrow$ (ii). Let B_i be a basis for V_i, let $B = \bigcup_{i=1}^k B_i$. If $v \in \sum V_i$ then $v = \sum_{i=1}^k v_i$, and v_i can be written as a linear combination of vectors in B_i, so substitute for each v_i and obtain v as a linear combination of B. If we have a linear combination of vectors in B equal to 0, collect together terms in each V_i, let v_i denote the part in V_i. Then $v_1 + \cdots + v_k = 0$. By uniqueness of expression for 0, we have $v_i = 0$. Now B_i is linear independent, so all coefficients are 0.

For the rest, we use similar argument in proof of Lemma 8.1.18. □

8.2 Vector Norm

[5]

[5] need definition

8.3 Linear maps

8.3.1 Basic definitions and properties

Definition 8.3.1 (linear map)**.** Let V, W be vector spaces over $\mathbb{F}$. The map $\alpha : V \to W$ is a linear map (or homomorphism) if

$$\begin{aligned} \alpha(v_1 + v_2) &= \alpha(v_1) + \alpha(v_2) \\ \alpha(\lambda v) &= \lambda\alpha(v) \end{aligned}$$

for $v, v_1, v_2 \in V$, $\lambda \in \mathbb{F}$.

Remark. In linear algebra, linear maps are sort of 'homomorphism'.

Example 8.3.1. (i) The map $D : D(\mathbb{R}) \to F(\mathbb{R}) = \mathbb{R}^{\mathbb{R}}$[6], $f \to \frac{df}{dt}$ is linear.

(ii) The map $\int_0^x : C[0,1] \to F[0,1]$, $f \mapsto \int_0^x f(t)dt$ is linear.

(iii) If A is an $m \times n$ matrix, the map $\alpha : \mathbb{F}^n \to \mathbb{F}^m$, $x \mapsto Ax$ is linear.

Lemma 8.3.2. Let U, V, W be vector spaces.

(i) $\iota_v : V \to V$, $v \mapsto v$ is linear.

(ii) If $U \xrightarrow{\beta} V \xrightarrow{\alpha} W$ with α, β linear, then so is $\alpha \circ \beta : U \to W$.

Proof. [7] □

Lemma 8.3.3. Let V, W be vector spaces over $\mathbb{F}$, let B be a basis for V. If $\alpha_0 : B \to W$ is any map, there is a unique linear map $\alpha : V \to W$ which extends α_0, so $\alpha(v) = \alpha_0(v)$ for all $v \in B$.

Proof. For $v \in V$ with $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ where $v_i \in B$, $\lambda_i \in \mathbb{F}$, we can define

$$\alpha(v) := \sum \lambda_i \alpha_0(v_i) = \sum \lambda_i \alpha(v_i) \tag{8.3.1}$$

with $\alpha(v) = \alpha_0(v)$ for all $v \in B$. Thus α is linear.

If $\forall v \in V$, we have two linear maps α_1, α_2 such that $\alpha_1(v) = \alpha_2(v) = \alpha(v)$. We have that

$$\alpha_1(v) = \alpha_1\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \alpha_1(v_i) = \sum_{i=1}^n \lambda_i \alpha_0(v_i) = \sum_{i=1}^n \lambda_i \alpha_2(v_i) = \alpha_2\left(\sum_{i=1}^n \lambda_i v_i\right) = \alpha_2(v). \tag{8.3.2}$$

Thus, the linear map is unique. □

Definition 8.3.2 (isomorphism)**.** If V, W are vector spaces over $\mathbb{F}$, the map $\alpha : V \to W$ is an isomorphism if it is linear and bijective. Write $V \cong W$ if an isomorphism $V \to W$ exists. We say that V and W are isomorphic.

Definition 8.3.3 (endomorphism)**.** An endomorphism is a linear map with $V \to V$ ($V = W$).

Definition 8.3.4 (automorphism)**.** An automorphism is a bijective linear map with $V \to V$ ($V = W$).

Proposition 8.3.4. $\cong$ is an equivalence relation on the set of vector spaces over $\mathbb{F}$.

(i) $\iota_V : V \to V$ is an isomorphism (of course, automorphism).

(ii) If $\alpha : V \to W$ is an isomorphism, then $\alpha^{-1} : W \to V$ is an isomorphism.

(iii) If $U \xrightarrow{\alpha} V \xrightarrow{\beta} W$ are isomorphisms then so is $\beta \circ \alpha : U \to W$.

[6] need definition
[7] need proof

Proof. (i) and (iii) are obvious.

For (ii), suppose α is an isomorphism so $\alpha^{-1} : W \to V$ exists and is a bijection.

$$\begin{aligned} \alpha^{-1}(w_1 + w_2) &= \alpha^{-1}(\alpha(v_1) + \alpha(v_2)) = \alpha^{-1}(\alpha(v_1 + v_2)) = v_1 + v_2 = \alpha^{-1}(w_1) + \alpha^{-1}(w_2) \\ \alpha^{-1}(\lambda w) &= \alpha^{-1}(\lambda\alpha(v)) = \alpha^{-1}(\alpha(\lambda v)) = \lambda v = \lambda\alpha^{-1}(w) \end{aligned}$$

So α^{-1} is linear. □

Theorem 8.3.5. If V is a vector space over $\mathbb{F}$ of finite dimension n, then $V \cong \mathbb{F}^n$.

Proof. Choose a basis $v_1, \ldots, v_n$ by Lemma 8.1.14. The map $\alpha : V \to \mathbb{F}^n$, $\sum_{i=1}^n \lambda_i v_i \mapsto (\lambda_1, \ldots, \lambda_n)^T$ is an isomorphism. □

Theorem 8.3.6. The vector spaces V, W over $\mathbb{F}$ are isomorphic if and only if they have the same dimension.

Proof. ($\Leftarrow$). If $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ are bases for V and W, respectively, then the map $\alpha : V \to W$, $\sum_{i=1}^n \lambda_i v_i \mapsto \sum_{i=1}^n \lambda_i w_i$ is an isomorphism ($V \cong \mathbb{F}^n \cong W$ by Theorem 8.3.5).

($\Rightarrow$). The image of a basis of V under an isomorphism is a basis of W, i.e., let B be a basis of V, $\alpha : V \to W$ an isomorphism. Then $\alpha(B)$ is a basis of W.

If $w \in W$, then $w = \alpha(v)$ for some $v \in V$; write $v = \sum_{i=1}^n \lambda_i v_i$ with $v_1, \ldots, v_n \in B$, $\lambda_i \in \mathbb{F}$. Then $w = \alpha\left(\sum \lambda_i v_i\right) = \sum \lambda_i \alpha(v_i)$. Then if $\lambda_1\alpha(v_1) + \cdots + \lambda_n\alpha(v_n) = 0$ then $\alpha(\lambda_1 v_1 + \cdots + \lambda_n v_n) = 0$ so $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ by definition of linear map (Definition 8.3.1). Hence $\lambda_i = 0$ for all i as B is a basis of V. □

Remark. These isomorphisms are not natural, they depend on the choice of bases.

Definition 8.3.5 (nullspace, nullity, rank)**.** Let $\alpha : V \to W$ be a linear map. We define the nullspace and image of α,

$$\ker(\alpha) = \{v \in V : \alpha(v) = 0\} = N(\alpha), \qquad \mathrm{Im}(\alpha) = \{w \in W : w = \alpha(v) \text{ for some } v \in V\}. \tag{8.3.3}$$

Then $N(\alpha) \leq V$, $\mathrm{Im}(\alpha) \leq W$.

Note that α is injective if and only if $N(\alpha) = \{0\}$ and surjective if and only if $\mathrm{Im}(\alpha) = W$.

Define $\mathrm{n}(\alpha) = \dim(N(\alpha))$, the nullity of α, and $\mathrm{r}(\alpha) = \dim(\mathrm{Im}(\alpha))$, the rank of α.

Theorem 8.3.7 (rank-nullity theorem)**.** Let V, W be vector spaces over $\mathbb{F}$ with $\dim_{\mathbb{F}} V$ finite. Let $\alpha : V \to W$ be a linear map. Then $\dim V = \mathrm{r}(\alpha) + \mathrm{n}(\alpha)$.

Proof. Let $v_1, \ldots, v_k$ be a basis for $N(\alpha)$, extend to $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ a basis for V by Lemma 8.1.12. We claim that $\alpha(v_{k+1}), \ldots, \alpha(v_n)$ is a basis for $\mathrm{Im}(\alpha)$.

$\forall w \in \mathrm{Im}(\alpha)$, say $w = \alpha(v)$ for some $v \in V$, then $v = \sum_{i=1}^n \lambda_i v_i$ for some $\lambda_i \in \mathbb{F}$ as $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ a basis for V. So

$$w = \alpha(v) = \sum_{i=1}^n \lambda_i \alpha(v_i) = \sum_{k+1}^n \lambda_i \alpha(v_i), \qquad (\alpha(v_{k+1}), \ldots, \alpha(v_n) \text{ span } \mathrm{Im}(\alpha)) \tag{8.3.4}$$

since $\alpha(v_i) = 0$ for $i = 1, \ldots, k$. Then

$$\sum_{i=k+1}^n \lambda_i \alpha(v_i) = 0 \;\Rightarrow\; \alpha\left(\sum_{i=k+1}^n \lambda_i v_i\right) = 0 \;\Rightarrow\; \sum_{i=k+1}^n \lambda_i v_i \in N(\alpha), \tag{8.3.5}$$

so it can be written as $\sum_{i=1}^k \lambda_i v_i$. But $v_1, \ldots, v_n$ are linearly independent, so $\lambda_i = 0$ for $i = 1, \ldots, n$. Thus, $\alpha(v_{k+1}), \ldots, \alpha(v_n)$ are linearly independent. Thus $\alpha(v_{k+1}), \ldots, \alpha(v_n)$ is a basis for $\mathrm{Im}(\alpha)$ by Definition 8.1.7. □

Remark. The rank-nullity theorem is a linear version of the first isomorphism theorem (Theorem 6.4.9).

Let V be a vector space over $\mathbb{F}$ and $N \leq V$. Then $V/N = \{v + N : v \in V\}$ is a vector space over $\mathbb{F}$ with the operations defined as follows.

$$\begin{aligned} (v_1 + N) + (v_2 + N) &= (v_1 + v_2) + N \\ \lambda(v + N) &= (\lambda v) + N \end{aligned}$$

Write $U = V/N$, $u = v + N$. Choose a basis $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ for V containing the basis $v_1, \ldots, v_k$ for $N(\alpha)$. Then $u_{k+1}, \ldots, u_n$ is a basis for U. Hence $\dim V/N = \dim V - \dim N$. Now let $\alpha : V \to W$ be linear for some vector space W over $\mathbb{F}$. Then $V/N(\alpha) \cong \mathrm{Im}(\alpha)$. The map $v + N(\alpha) \mapsto \alpha(v)$ is linear. Hence $\dim \mathrm{Im}(\alpha) = \dim (V/N(\alpha)) = \dim V - \dim N(\alpha)$.

Corollary 8.3.8. Let V be a vector space of finite dimension over $\mathbb{F}$, let $\alpha : V \to V$ be a linear map. (More generally, consider $\alpha : V \to W$ with $\dim V = \dim W$.) The following are equivalent.

(i) α is an isomorphism.

(ii) α is surjective.

(iii) α is injective.

Proof. (i) $\Rightarrow$ (ii),(iii) are obivoius.

(ii) $\Rightarrow$ (i). If α is surjective, we have $\mathrm{Im}(\alpha) = W$. Then by rank-nullity theorem 8.3.7, we have

$$\dim V = \mathrm{n}(\alpha) + \mathrm{r}(\alpha) = \dim (\mathrm{Im}(\alpha)) + \dim (N(\alpha)) = \dim W + \dim (N(\alpha)) \ \Rightarrow \ \dim (N(\alpha)) = 0 \ \Rightarrow \ N(\alpha) = \{0\} \quad (*)$$

Thus, $\forall \alpha(v_1) = \alpha(v_2) \in W$ for some $v_1, v_2 \in V$, we have

$$\alpha(v_1 - v_2) = 0 \ \Rightarrow \ v_1 - v_2 = 0 \ \Rightarrow \ v_1 = v_2 \tag{8.3.6}$$

by $(*)$. Thus, α is injective. So α is bijective and therefore isomorphism.

(iii) $\Rightarrow$ (i). We use the same argument of rank-nullity theorem to prove that α is injective imples that α is also surjective. □

8.3.2 The vector space of linear maps

Definition 8.3.6 (vector space of linear maps)**.** Let U, V be vector spaces over $\mathbb{F}$. $\mathcal{L}(U, V) = \{\alpha : U \to V | \alpha \text{ linear}\}$ is a vector space over $\mathbb{F}$ with

$$\begin{aligned} (\alpha_1 + \alpha_2)(u) &= \alpha_1(u) + \alpha_2(u) \\ (\lambda\alpha)(u) &= \lambda\alpha(u) \end{aligned}$$

for $u \in U$, for $\alpha, \alpha_1, \alpha_2 \in \mathcal{L}(U, V)$, $\lambda \in \mathbb{F}$.

Remark. To show this is a vector space over $\mathbb{F}$, consider the vector space of all functions $U \to V$ and show $\mathcal{L}(U, V)$ is a subspace.

Proposition 8.3.9. If U, V are vector spaces over $\mathbb{F}$, then $\mathcal{L}(U, V)$ is a vector space over $\mathbb{F}$. If both U, V are finite dimensional, then so is $\mathcal{L}(U, V)$ and $\dim (\mathcal{L}(U, V)) = \dim U \dim V$.

Proof. We know that $\mathcal{L}(U, V)$ is a vector space over $\mathbb{F}$ by Definition 8.3.6. It remains to check the dimension claim.

Let $u_1, \ldots, u_n$ be a basis for U, let $v_1, \ldots, v_m$ be a basis for V. For $1 \le i \le m$, $1 \le j \le n$, define $\varepsilon_{ij} : u_k \mapsto \delta_{jk} v_i$ for $1 \le k \le n$, and extend linearly (δ_{ij} is Kronecker delta, see Definition 4.2.1). Then $\varepsilon_{ij} \in \mathcal{L}(U, V)$, and there are mn functions of this form. Now we want to show that they form a basis.

If $\sum_{i,j} \lambda_{ij} \varepsilon_{ij} = 0$, then in particular for all $1 \le k \le n$,

$$0 = \sum_{i,j} \lambda_{ij} \varepsilon_{ij}(u_k) = \sum_{i,j} \lambda_{ij} \delta_{jk} v_i = \sum_i \lambda_{ik} v_i. \tag{8.3.7}$$

Now the v_i are linearly independent, so $\lambda_{ik} = 0$ for all $1 \le i \le m$. This is true for all $1 \le k \le n$, so the ε_{ij} are linearly independent.

Now $\forall \alpha \in \mathcal{L}(U, V)$, say $\alpha(u_k) = \sum_i a_{ik} v_i$. Then

$$\sum_{i,j} a_{ij} \left(\varepsilon_{ij}(u_k)\right) = \sum_{i,j} a_{ij} \delta_{jk} v_i = \sum_i a_{ik} v_i = \alpha(u_k) \tag{8.3.8}$$

for any $1 \le k \le n$, so the maps are equal on a basis of U, hence they are equal by Lemma 8.3.3. Thus, ε_{ij} span $\mathcal{L}(U, V)$. Therefore, ε_{ij} is a basis by Definition 8.1.7. □

8.3.3 Relation between linear maps and matrices

Now we can see the relation between linear maps and matrices.

Proposition 8.3.10. If $\alpha : U \to V$ is linear and $\dim U = n$, $\dim V = m$, then $\mathcal{L}(U, V) \cong M_{m,n}(\mathbb{F})$.

Proof. Let $B = \{u_1, \ldots, u_n\}$ and $C = \{v_1, \ldots, v_m\}$ be bases for U and V, respectively.

We have that $\dim(\mathcal{L}(U, V)) = mn$ by Proposition 8.3.9 and $\dim_{\mathbb{F}} M_{m,n}(\mathbb{F}) = mn$ by Proposition 9.1.2.

Then by Theorem 8.3.6, $\theta : \mathcal{L}(U, V) \to M_{m,n}(\mathbb{F})$, $\alpha \mapsto [\alpha]_{B,C}$ is an isomorphism. □

Definition 8.3.7. Let U, V be finite dimensional vector spaces over $\mathbb{F}$, let $\alpha : U \to V$ be linear. Fix bases $B = \{u_1, \ldots, u_n\}$ and $C = \{v_1, \ldots, v_m\}$ for U and V, respectively.

Define $A = (a_{ij})$ by $\alpha(u_j) = \sum_i a_{ij} v_i$. For $u \in U$ with $u = \sum_i \lambda_i u_i$ write $[u]_B = (\lambda_1, \ldots, \lambda_n)^T$. Then

$$A = \left([\alpha(u_1)]_C \ldots [\alpha(u_n)]_C\right), \tag{8.3.9}$$

denoted $A = [\alpha]_{B,C}$.

Remark. We can see that A is a matrix.

Lemma 8.3.11. For all $u \in U$, $[\alpha(u)]_C = [\alpha]_{B,C}[u]_B$.

Proof. If $u \in U$, $u = \sum_j \lambda_j u_j$ so $[u]_B = (\lambda_1, \ldots, \lambda_n)^T$, then

$$\alpha(u) = \sum_j \lambda_j \alpha(u_j) = \sum_j \lambda_j \sum_i a_{ij} v_i = \sum_i \sum_j a_{ij} \lambda_j v_i = \sum_i (A \cdot [u]_B)_i v_i. \tag{8.3.10}$$

so $[\alpha(u)]_C = A \cdot [u]_B$. □

Remark. Let $B = \{u_1, \ldots, u_n\}$, $C = \{v_1, \ldots, v_m\}$ be bases for U, V, respectively. Set $\varepsilon = \varepsilon_B : U \to \mathbb{F}^n$, $u \mapsto [u]_B$, $\phi = \phi_C : V \to \mathbb{F}^m$, $v \mapsto [v]_C$. We have the following commuting diagram.

$$\begin{array}{ccc} U & \xrightarrow{\alpha} & V \\ {\scriptstyle \varepsilon_B}\downarrow & & \downarrow{\scriptstyle \phi_C} \\ \mathbb{F}^n & \xrightarrow{A\cdot} & \mathbb{F}^m \end{array} \tag{8.3.11}$$

Remark. In fact, A as defined above is the only matrix for which $[\alpha(u)]_C = A \cdot [u]_B$ for all $u \in U$. If also $A' \cdot [u]_B = [\alpha(u)]_C$ for all $u \in U$, then this is in particular true for $u_1, \ldots, u_n$. But $[u_k]_B = e_k$ and $A' \cdot e_k$ is the kth column of A'. This is true for each $1 \leq k \leq n$, so it determines the matrix.

Lemma 8.3.12 (chain rule)**.** Let $U \xrightarrow{\alpha} V \xrightarrow{\beta} W$ be linear and choose bases B, C, D for U, V, W, respectively. Then

$$[\beta \circ \alpha]_{B,D} = [\beta]_{C,D} \cdot [\alpha]_{B,C}. \tag{8.3.12}$$

Proof. Write $A = [\alpha]_{B,C}$, $B = [\beta]_{C,D}$. Then

$$\beta \circ \alpha(u_k) = \beta \sum_j a_{jk} v_j = \sum_j a_{jk} \sum_i b_{ij} w_i = \sum_i \sum_j b_{ij} a_{jk} w_i = \sum_i (BA)_{ik} w_i \tag{8.3.13}$$

so $[\beta \circ \alpha]_{B,D} = BA$ by Definition 8.3.7. (That is $B \cdot A = BA$) □

8.3.4 Change of bases

Definition 8.3.8. Let U and V be vector spaces over $\mathbb{F}$. Suppose U has bases $B = \{u_1, \ldots, u_n\}$ and $B' = \{u'_1, \ldots, u'_n\}$, V has bases $C = \{v_1, \ldots, v_m\}$ and $C' = \{v'_1, \ldots, v'_m\}$. The matrix $P = (p_{ij})$ is the change of bases matrix from B to B' if $u'_j = \sum_i p_{ij} u_i$, so

$$P := ([u'_1]_B, \ldots, [u'_n]_B) = ([\iota(u'_1)_B, \ldots, [\iota(u'_n)_B]) = ([\iota(u'_1)_B, \ldots, [\iota(u'_n)_B]) = [\iota_U]_{B'B}[u']_{B'} = [\iota_U]_{B'B} \tag{8.3.14}$$

by Lemma 8.3.11.

Then $[u]_B = P[u]_{B'}$ for all $u \in U$ (This is clear for each u'_j since $[u'_j]_{B'} = e_j$.), i.e.,

$$P[u]_{B'} = [\iota_U]_{B'B}[u]_{B'} = [\iota(u)]_B = [u]_B. \tag{8.3.15}$$

Note that P is invertible, in fact, P^{-1} is the change of basis matrix from B' to B. Similarly, we obtain the change of basis matrix Q from C to C'.

Lemma 8.3.13. Let $\alpha : U \to V$ be a linear map, let B, B', C, C' be as above and let $A = [\alpha]_{B,C}$, $A' = [\alpha]_{B',C'}$. Then $A' = Q^{-1}AP$.

Proof. For all $u \in U$ we have

$$AP[u]_{B'} = A[u]_B = [\alpha(u)]_C = Q[\alpha(u)]_{C'} = QA'[u]_{B'}, \tag{8.3.16}$$

so $A' = Q^{-1}AP$. □

Lemma 8.3.14. Let U, V be vector spaces over $\mathbb{F}$ with $\dim U = n$, $\dim V = m$. Let $\alpha : U \to V$ be linear. There exist bases B of U and C of V such that $[\alpha]_{B,C} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ for some r.

Proof. Let $u_{r+1}, \ldots, u_n$ be a basis for $N(\alpha)$, extend this to a basis $B = \{u_1, \ldots, u_r, u_{r+1}, \ldots, u_n\}$ of U.

Then by rank-nullity theorem (Theorem 8.3.7), we have $\dim(\mathrm{Im}(\alpha)) = n - (n - r) = r$. Also, $\alpha(u_1), \alpha(u_2), \ldots, \alpha(u_r) \in \mathrm{Im}(\alpha)$ are linearly independent since

$$0 = \lambda_1\alpha(u_1) + \cdots + \lambda_r\alpha(u_r) = \alpha(\lambda_1 u_1 + \cdots + \lambda_r u_r) \;\Rightarrow\; \lambda_1 u_1 + \cdots + \lambda_r u_r = 0 \tag{8.3.17}$$

since $u_1, \ldots, u_r \notin N(\alpha)$. Therefore, $\lambda_1 = \cdots = \lambda_r = 0$ since $u_1, \ldots, u_n$ is basis of U.

Then by Lemma 8.1.14, we have that $\alpha(u_1), \alpha(u_2), \ldots, \alpha(u_r) \in \mathrm{Im}(\alpha)$ is a basis for $\mathrm{Im}(\alpha)$.

Then we can extend this to a basis $C = \{\alpha(u_1), \ldots, \alpha(u_r), v_{r+1}, \ldots, v_m\}$ of V. Then for all $u \in U$, $u = \sum_i \lambda_i u_i$, since $u_{r+1}, \ldots, u_n \in N(\alpha)$,

$$[\alpha]_{B,C} = ([\alpha(u_1)]_C, \ldots, [\alpha(u_r)]_C, 0, \ldots, 0) = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{8.3.18}$$

□

Lemma 8.3.15. Suppose U and V are two finite vector spaces. Let $\alpha : U \to V$ be linear, let B be a basis for U, and C be a basis for V. Let $A = [\alpha]_{B,C}$. Then $\mathrm{r}(\alpha) = \mathrm{r}(A)$.

Proof. Consider the map $\theta : \mathrm{Im}(\alpha) \to \mathrm{colsp}(A)$, $\alpha(u) \mapsto [\alpha(u)]_C$.

Let $C = \{v_1, \ldots, v_m\}$. Then $\forall v \in V$ we can find $\lambda_i \in \mathbb{F}$ such that $v = \sum_i \lambda_i v_i$. Clearly, for any $u \in U$, $\alpha_1, \alpha_2, \alpha \in \mathcal{L}(U, V)$,

$$\begin{aligned} \theta(\alpha_1(u) + \alpha_2(u)) &= \theta\left((\alpha_1 + \alpha_2)(u)\right) = [(\alpha_1 + \alpha_2)(u)]_C = [(\alpha_1(u) + \alpha_2(u)]_C \\ &= [\alpha_1(u)]_C + [\alpha_2(u)]_C = \theta(\alpha_1(u)) + \theta(\alpha_2(u)). \end{aligned}$$

since V is vector space. Also, $\theta(\lambda\alpha(u)) = \theta(\alpha(\lambda u)) = [\alpha(\lambda u)]_C = \lambda[\alpha(u)]_C = \lambda\theta(\alpha(u))$. Thus, θ is linear.

If $[\alpha_1(u)]_C = [\alpha_2(u)]_C$, we have $\lambda_i = \mu_i$

$$\alpha_1(u) = \sum_i \lambda_i v_i = \sum_i \mu_i v_i = \alpha_2(u) \;\Rightarrow\; \theta \text{ is injective.} \tag{8.3.19}$$

$\forall \in w = \{w_1, \ldots, w_m\} \in \mathrm{colsp}(A)$, we can find $\alpha(u) = \sum_i w_i v_i$ which is in $\mathrm{Im}(\alpha)$. Thus, θ is surjective. So we have that θ is bijective. Then by Definition 8.3.2, θ is an isomorphism.

Then by Theorem 8.3.6, $\mathrm{Im}(\alpha)$ and $\mathrm{colsp}(A)$ have the same dimension. That is, $\mathrm{r}(\alpha) = \mathrm{r}(A)$. □

8.4 Endomorphisms

Definition 8.4.1 (determinant of linear endomorphism)**.** If $\alpha : V \to V$ is a linear endomorphism, define $\det\alpha = \det[\alpha]_B (= \det[\alpha]_{B,B})$ for any basis B of V.

Theorem 8.4.1. $\det : \mathrm{End}(V) \to \mathbb{F}$ has the following properties.

(i) $\det \iota = 1$.

(ii) $\det \alpha \circ \beta = \det \alpha \det \beta$.

(iii) $\det \alpha \neq 0$ if and only if α is invertible[8], and if α is invertible then $\det \alpha^{-1} = (\det \alpha)^{-1}$.

Remark. Consider the group $GL(V)$ of automorphisms of V and the group $GL_n(\mathbb{F})$ of invertible $n \times n$ matrices over $\mathbb{F}$. Then $GL(V) \cong GL_n(\mathbb{F})$ and $\det : GL_n(\mathbb{F}) \to \mathbb{F}$ is a homomorphism.

Definition 8.4.2 (trace of linear endomorphism)**.** For $\alpha \in \mathrm{End}(V)$ (see endomorphism (Definition 8.3.3)) we can define trace of α, $\mathrm{tr}(\alpha) = \mathrm{tr}[\alpha]_{B,B}$, where B is any basis for V.

[8] need definition

Chapter 9

Matrix

9.1 Basic Definitions and Properties

9.1.1 Definitions

Definition 9.1.1 (matrix)**.** An $m \times n$ matrix over $\mathbb{F}$ is an array $A = (a_{ij})$ with m rows and n columns and $a_{ij} \in \mathbb{F}$ for $1 \leq i \leq m$, $1 \leq j \leq n$. Write $M_{m,n}(\mathbb{F})$ for the set of all $m \times n$ matrices over $\mathbb{F}$. If $m = n$, we can simply write $M_n(\mathbb{F})$.

Example 9.1.1.

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}. \tag{9.1.1}$$

Proposition 9.1.2. $M_{m,n}(\mathbb{F})$ is a vector space under operations

$$\begin{aligned} (a_{ij}) + (b_{ij}) &= (a_{ij} + b_{ij}) \\ \lambda(a_{ij}) &= (\lambda a_{ij}) \end{aligned}$$

with $\dim_{\mathbb{F}} M_{m,n}(\mathbb{F}) = mn$.

Proof. Obviously, $M_{m,n}(\mathbb{F})$ is a vector space by Definition 8.1.1.

We now prove the dimension claim. For $1 \leq i \leq m$, $1 \leq j \leq n$ define

$$E_{ij} = \begin{cases} e_{i'j'} = 1 & (i', j') = (i, j) \\ e_{i'j'} = 0 & (i', j') \neq (i, j). \end{cases} \tag{9.1.2}$$

This is a natural basis. □

Definition 9.1.2. We say two matrics $A = (a_{ij})$,$B = (b_{ij})$ are same, $A = B$ if

$$a_{ij} = b_{ij}, \ \forall i, j. \tag{9.1.3}$$

9.1.2 Multiplication of matrices

Proposition 9.1.3 (associativity of multiplication of matrices)**.** Let $A \in M_{m,n}(\mathbb{F})$, $B \in M_{n,p}(\mathbb{F})$ and $C \in M_{p,q}(\mathbb{F})$. Then

$$A(BC) = (AB)C. \tag{9.1.4}$$

Proof. We have

$$\begin{aligned} (A(BC))_{ij} &= \sum_k a_{ik}(BC)_{kj} = \sum_k \sum_l a_{ik} b_{kl} c_{lj} \\ ((AB)C)_{ij} &= \sum_k (AB)_{ik} C_{kj} = \sum_k \sum_l a_{il} b_{lk} c_{kj} \end{aligned}$$

Then we have the required result by switching k and l. □

Remark. Note that multiplication of matrices are not commutative, i.e. $AB \neq BA$.

Example 9.1.4.

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 6 & 8 \end{pmatrix} \neq \begin{pmatrix} 1 & 4 \\ 3 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}. \tag{9.1.5}$$

9.1.3 Transpose

Definition 9.1.3 (transpose)**.** If $A \in M_{m,n}(\mathbb{F})$ with $A = (a_{ij})$, then its transpose A^T is definite to be a $n \times m$ matrix with

$$A^T = (a_{ji}). \tag{9.1.6}$$

Example 9.1.5. (i)

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}. \tag{9.1.7}$$

(ii) If $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ is column vector, $x^T = \begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix}$ is a row vector.

Proposition 9.1.6. Let $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,l}(\mathbb{F})$. Then

$$\left(A^T\right)^T = A, \qquad (AB)^T = B^T A^T. \tag{9.1.8}$$

Proof. $\left(A^T\right)^T = A$ is obvious. Let $A = (a_{ij})$ and $B = (b_{ij})$. Then $A^T = (a'_{ij}) = (a_{ji})$ and $B^T = (b'_{ij}) = (b_{ji})$. Then

$$\left((AB)^T\right)_{ij} = (AB)_{ji} = \sum_k a_{jk} b_{ki} = \sum_k b_{ki} a_{jk} = \sum_k b'_{ik} a'_{kj} = (B^T A^T)_{ij}. \tag{9.1.9}$$

Thus, we have the required result. □

Proposition 9.1.7. Let $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,l}(\mathbb{F})$ (A and B are completx matrices).

$$\left(A^\dagger\right)^\dagger = A, \qquad (AB)^\dagger = B^\dagger A^\dagger. \tag{9.1.10}$$

Proof. Similar arguement with Proposition 9.1.6. □

9.1.4 Identity matrix

Definition 9.1.4 (identity matrix)**.** The identity $n \times n$ matrix is defined to be

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}, \tag{9.1.11}$$

i.e., all the elements are 0 except for the diagonal elements that are 1.

Example 9.1.8. The 3×3 identity matrix is given by

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (\delta_{ij}) \tag{9.1.12}$$

where δ_{ij} is the Kronecker delta.

Proposition 9.1.9. Let $A, I \in M_n(\mathbb{F})$ and I is an identity matrix. Then $AI = IA = A$.

Proof. We have

$$(IA)_{ij} = \sum_k \delta_{ik} a_{kj} = a_{ij} = \sum_k a_{ik}\delta_{kj} = (AI)_{ij}, \tag{9.1.13}$$

i.e., $IA = AI = A$. □

9.1.5 Inverible matrices

Definition 9.1.5 (left inverse, right inverse)**.** Let $A \in M_n(\mathbb{F})$. Then B is a left inverse of A if $BA = I$ and C is a right inverse of A if $AC = I$.

Proposition 9.1.10 (inverse, invertible matrix)**.** Let $A \in M_n(\mathbb{F})$. If B is a left inverse of A and C is a right inverse of A then $B = C$ and we write $B = C = A^{-1}$. Then we say that A is invertible (or non-singular). Note that A^{-1} is unique.

Proof. By definition of left and right inverse, we have $BA = I$ and $AC = I$. Then

$$B = BI = B(AC) = (BA)C = IC = C. \tag{9.1.14}$$

by Proposition 9.1.9, 9.1.3.

If B and C are both inverses of A, then $B = BI = BAC = IC = C$. Hence, A^{-1} is unique. □

Remark. This property is based on the premise that both a left inverse and right inverse exist. In general the existence of a left inverse does not necessarily guarantee the existence of a right inverse or vice versa. However, in the case of a square matrix, the existence of a left inverse does imply the existence of a right inverse, and vice versa.

The above property then implies that they are the same matrix.

Proposition 9.1.11. If $A, B \in M_n(\mathbb{F})$ are invertible, then

$$\text{(i) } \left(A^{-1}\right)^{-1} = A, \qquad \text{(ii) } (AB)^{-1} = B^{-1}A^{-1}. \tag{9.1.15}$$

Proof. Let $C = A^{-1}$. Then

$$\begin{array}{l} CA = I = CC^{-1} \\ AC = I = C^{-1}C \end{array} \quad \Rightarrow \quad A = \left(A^{-1}\right)^{-1}. \tag{9.1.16}$$

Also, we have

$$\begin{aligned} B^{-1}A^{-1}(AB) &= B^{-1}\left(A^{-1}A\right)B = B^{-1}IB = B^{-1}B = I, \\ (AB)B^{-1}A^{-1} &= A\left(BB^{-1}\right)A^{-1} = AIA^{-1} = AA^{-1} = I \end{aligned}$$

by Proposition 9.1.9, 9.1.10, 9.1.3. □

9.1.6 Equivalent matrices

Definition 9.1.6 (equivalent matrices)**.** The $m \times n$ matrices $A, A' \in M_{m,n}(\mathbb{F})$ are equivalent if there exist invertible matrices $Q \in M_{m,m}(\mathbb{F})$, $P \in M_{n,n}(\mathbb{F})$ such that $A' = QAP$. This defines an equivalence relation on $M_{m,n}(\mathbb{F})$.

Remark. Equivalent matrices arise as representing the same linear map from a space U to a space V of dimension m and n with respect to different bases.

Lemma 9.1.12. Any $m \times n$ matrix is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ for some r.

Proof. Let $A \in M_{m,n}(\mathbb{F})$. Define $\alpha : \mathbb{F}^n \to \mathbb{F}^m$, $x \mapsto Ax$. With respect to the standard bases of $\mathbb{F}^n$, $\mathbb{F}^m$, α has matrix A. By Lemma 8.3.14 and Lemma 8.3.13, A is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ for some r. □

9.1.7 Ranks

Definition 9.1.7 (column space)**.** The column space (sometimes called the range) of a matrix is the set of all possible linear combinations of its column vectors. Let $A \in M_{m,n}(\mathbb{F})$. The column space of A is the subspace of $\mathbb{F}^m$ generated by the column vectors of A, denoted by $\text{colsp}(A)$.

Definition 9.1.8 (column rank)**.** The (column) rank of A, denoted $\text{r}(A)$ is the dimension of the column space of A.

Proposition 9.1.13. The matrices $A, A' \in M_{m,n}(\mathbb{F})$ are equivalent if and only if $\text{r}(A) = \text{r}(A')$.

Proof. ($\Rightarrow$). Assume A, A' are equivalent such that $A' = Q^{-1}AP$ with Q, P invertible. Let $\alpha : \mathbb{F}^n \to \mathbb{F}^m$, $x \mapsto Ax$. Then α with respect to standard bases B, C has matrix A. Let B' be the set of columns of P, let C' be the set of columns of Q'. Then $[\alpha]_{B',C'} = Q^{-1}AP$ by Lemma 8.3.13 since P and C are the change of basis matrices from B to B' and C to C', respectively.

So $[\alpha]_{B',C'} = Q^{-1}AP = A'$ and $[\alpha]_{B,C} = A$. Then by Lemma 8.3.15, $\text{r}(A') = \text{r}(\alpha) = \text{r}(A)$.

($\Leftarrow$). We have that A and A' are equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} I_{r'} & 0 \\ 0 & 0 \end{pmatrix} \tag{9.1.17}$$

for some r and r', respectively by Lemma 9.1.12. By the first part, $\text{r}(A) = r$, $\text{r}(A') = r'$. Since $\text{r}(A) = \text{r}(A')$ we have $r = r'$ so A and A' are equivalent by transitivity of the equivalence relation. □

Definition 9.1.9 (row space)**.** The row space of a matrix is the set of all possible linear combinations of its row vectors. Let $A \in M_{m,n}(\mathbb{F})$. The row space of A is the subspace of $\mathbb{F}^n$ generated by the row vectors of A, denoted by $\text{rowsp}(A)$.

Definition 9.1.10 (row rank)**.** The row rank of A, denoted $\text{rowrank}(A)$ is the dimension of the column space of A. That is, $\text{rowrank}(A) = \dim \text{rowsp}(A) = \text{r}(A^T)$.

Theorem 9.1.14. For $A \in M_{m,n}(\mathbb{F})$, $\text{rowrank}(A) = \text{r}(A)$. That is, $\text{r}(A^T) = \text{r}(A)$.

Proof. Let $A \in M_{m,n}(\mathbb{F})$, let $r = \text{r}(A)$. Then A is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{m\times n}$ by Lemma 9.1.12, so $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{m\times n} = QAP$ for some invertible matrices Q, P by Definition 9.1.6. Consider the transpose, by Proposition 9.1.6,

$$P^T A^T Q^T = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{n\times m}. \tag{9.1.18}$$

So $\text{sp}(A^T)$ is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{n\times m}$. Visibly, $\text{r}\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{n\times m} = r$, so

$$\text{rowrank}(A) = \text{r}(A^T) = \text{r}\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{n\times m} = r = \text{r}(A). \tag{9.1.19}$$

□

Theorem 9.1.15. If $A \in M_n(\mathbb{F})$, then A is invertible iff $\text{r}(A) = n$.

Proof. ($\Rightarrow$). If A is invertible, then we have invertible matrix P such that $AP = I_n$. This means A is equivalent to I_n. Then by Proposition 9.1.13, we have $\text{r}(A) = \text{r}(I_n) = n$.

($\Leftarrow$). Approach 1. If $\text{r}(A)$, we have A is equivalent to I_n by Lemma 9.1.12. Thus, there exist invertible matrices P, Q such that $Q^{-1}AP = I_n$ by Definition 9.1.6. Therefore, we have $A = QP^{-1}$ and $A^{-1} = PQ^{-1}$ by Proposition 9.1.11. Thus, A is invertible as

$$AA^{-1} = QP^{-1}PQ^{-1} = QQ^{-1} = I = PP^{-1} = PQ^{-1}QP^{-1} = A^{-1}A. \tag{9.1.20}$$

Approach 2. Since $\text{r}(A) = n$, we have that the corresponding linear map α is surjective. Then by Corollary 8.3.8, we have that the linear map is bijective (since $\dim V = n = m = \dim W$). Thus, the corresponding inverse matrix A^{-1} exists and therefore A is invertible. □

Lemma 9.1.16. Let $A \in M_n(\mathbb{F})$. Then $\mathrm{r}(A) = n$ iff the columns of A are linearly independent.

Proof. ($\Rightarrow$). If $\mathrm{r}(A) = n$, we have that the columns of A are linearly independent by Lemma 8.1.14 as the columns span the column space.

($\Leftarrow$). If the columns of A are linearly independent, then by Lemma 8.1.13, the columns of A is a basis. Furthermore, by definition of dimension (Theorem 8.1.10), $\mathrm{r}(A) = n$. □

Corollary 9.1.17. If $A \in M_n(\mathbb{F})$, then A is invertible iff the columns of A are linearly independent.

Proof. Direct result from Lemma 9.1.15 and 9.1.16. □

Proposition 9.1.18. Let $A \in M_{m,n}(\mathbb{F})$. Then

(i) If $B \in M_{n,k}(\mathbb{F})$, $\mathrm{r}(AB) \leq \min\{\mathrm{r}(A), \mathrm{r}(B)\}$.

(ii)

Proof. (i) We know that $\mathrm{colsp}(AB)$ is generated by the column vectors of AB. Also, it is generated by the column vectors of B. Thus, $\mathrm{colsp}(AB) \subseteq \mathrm{colsp}(B)$. Then by the definition of rank (Definition 9.1.8), we have $\mathrm{r}(AB) \leq \mathrm{r}(B)$.

Also, we have $\mathrm{r}(B^T A^T) \leq \mathrm{r}(A^T)$. Then by Theorem 9.1.14 and Proposition 9.1.6,

$$\mathrm{r}(AB) = \mathrm{r}\left((AB)^T\right) = \mathrm{r}(B^T A^T) \leq \mathrm{r}(A^T) = \mathrm{r}(A) \;\Rightarrow\; \mathrm{r}(AB) \leq \min\{\mathrm{r}(A), \mathrm{r}(B)\}. \tag{9.1.21}$$

(ii) [1]

□

9.1.8 Elementary operations

Definition 9.1.11 (elementary matrix)**.** The following are the elementary column operations on an $m \times n$ matrix over $\mathbb{F}$.

(i) Swap columns i and j (switching).

(ii) Replace column i by λ column i, where $\lambda \in \mathbb{F}\setminus\{0\}$ (multiplication).

(iii) Add λ column i to column j, where $i \neq j$ and $\lambda \in \mathbb{F}$ (addition).

The corresponding elementary column operation matrices are obtained by applying these operations to I_n. Call these $T_{i,j}$, $M_{i,\lambda}$ and $C_{i,j,\lambda}$. An elementary column operation on A can be performed by postmultiplying A with the corresponding elementary matrix. All these operations are reversible.

Similarly for elementary row operations. We write E_i for elementary (column and row) matrices.

For square matrices, the elementary (column or row) matrices of switching and multiplication are same, given by

$$T_{i,j} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & 1 & & \\ & & & \ddots & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}, \quad M_{i,\lambda} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}. \tag{9.1.22}$$

[1] need proof

The matrices of addition is

$$C_{i,j,\lambda} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & \lambda & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}. \tag{9.1.23}$$

$AC_{i,j,\lambda}$ is adding λ times column i to column j of A and $C_{i,j,\lambda}A$ is adding λ times row j to row i of A.

Definition 9.1.12 (column echolon form)**.** A is an $m \times n$ matrix with the following properties is said to be in column echelon form.

(i) The highest placed non-zero entry in column j is 1 in row i_j , with $i_1 \leq i_2 \leq \dots$.

(ii) The entry in row i_j and column k with $k < j$ is 0.

Example 9.1.19.

$$\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 2 & 3 & 1 \\ 4 & 5 & 2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 6 & 1 & 0 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 6 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{pmatrix} \tag{9.1.24}$$

Lemma 9.1.20. Any matrix A can be reduced to a matrix in column echelon form by a sequence of elementary column matrices.

Remark. If A is a square $n \times n$ matrix and is invertible, the equivalent column echelon form is I_n. This can be used to find A^{-1}.

$$A \mapsto AE_1E_2 \dots E_k = I_n, \quad I_n \mapsto I_nE_1E_2 \dots E_k = A^{-1}. \tag{9.1.25}$$

Proof. [2] □

Proposition 9.1.21. Let $E \in M_n(\mathbb{F})$ be elementary matrix. Then it is invertible.

Remark. The square elementary matrices generate the general linear group of invertible matrices[3].

Proof. It is easy to check that the inverse matrices are

$$(T_{i,j})^{-1} = T_{i,j}, \quad (M_{i,\lambda})^{-1} = M_{i,1/\lambda}, \quad (C_{i,j,\lambda})^{-1} = C_{i,j,-\lambda}. \tag{9.1.26}$$

□

Lemma 9.1.22. If A is an invertible $n \times n$ matrix then A is a product of elementary matrices.

Proof. By the remark of Lemma 9.1.20, $A^{-1} = E_1 \dots E_k$ is a product of elementary matrices, hence so is $A = E_k^{-1} \dots E_1^{-1}$ by Proposition 9.1.11. □

9.2 Square Matrices

9.2.1 Basic square matrices

Definition 9.2.1 (symmetric matrix)**.** A square $n \times n$ matrix $A = (a_{ij})$ is symmetric if

$$A = A^T, \quad \text{i.e., } a_{ij} = a_{ji}. \tag{9.2.1}$$

[2] need proof.
[3] need details

Definition 9.2.2 (anti-symmetric matrix)**.** A square $n \times n$ matrix $A = (a_{ij})$ is anti-symmetric if

$$A = -A^T, \quad \text{i.e., } a_{ij} = -a_{ji}. \tag{9.2.2}$$

Remark. For an anti-symmetric matrix, $a_{11} = -a_{11}$, i.e., $a_{11} = 0$. Similarly we deduce that all the diagonal elements of anti-symmetric matrices are zero, i.e., $a_{11} = a_{22} = \cdots = a_{nn} = 0$.

Definition 9.2.3 (adjoint matrix)**.** For $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$, the adjoint matrix of A is

$$A^\dagger = \left(a'_{ij}\right) := \left(\overline{A}\right)^T, \qquad \text{i.e., } a'_{ij} = \overline{a_{ji}}. \tag{9.2.3}$$

Definition 9.2.4 (Hermitian matrix)**.** A square $n \times n$ complex matrix $A = (a_{ij})$ is Hermitian if

$$A = A^\dagger, \quad \text{i.e., } a_{ij} = \overline{a_{ji}}. \tag{9.2.4}$$

Remark. Hermitian matrix is also called self-adjoint matrix.

Definition 9.2.5 (skew-Hermitian matrix)**.** A square $n \times n$ complex matrix $A = (a_{ij})$ is skew-Hermitian if

$$A = -A^\dagger, \quad \text{i.e., } a_{ij} = -\overline{a_{ji}}. \tag{9.2.5}$$

Remark. All the diagonal elements of Hermitian and skew-Hermitian matrices are real and pure imaginary respectively.

Example 9.2.1. (i) A symmetric 3×3 matrix S has the form

$$S = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}, \tag{9.2.6}$$

i.e., it has six independent elements.

(ii) An anti-symmetric 3×3 matrix A has the form

$$A = \begin{pmatrix} 0 & a & -b \\ -a & 0 & c \\ b & -c & 0 \end{pmatrix}, \tag{9.2.7}$$

i.e., it has three independent elements.

Definition 9.2.6 (orthogonal matrix)**.** $A \in M_n(\mathbb{F})$ is orthogonal matrix if

$$AA^T = I = A^T A, \tag{9.2.8}$$

i.e., if A is invertible and $A^{-1} = A^T$.

Remark. Note that $\det A = \pm 1$ for orthogonal matrix A.

Definition 9.2.7 (unitary matrix)**.** $A \in M_n(\mathbb{C})$ is said to be unitary if its Hermitian conjugate is equal to its inverse, i.e., if

$$U^\dagger = U^{-1}. \tag{9.2.9}$$

Remark. Unitary matrices are to complex matrices what orthogonal matrices are to real matrices. Similar properties to those above for orthogonal matrices also hold for unitary matrices when references to real scalar products are replaced by references to complex scalar products[4].

Definition 9.2.8 (trace)**.** The trace of a square $n \times n$ matrix $A = (a_{ij})$ ($A \in M_n(\mathbb{F})$) is equal to the sum of the diagonal elements, i.e.,

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii}. \tag{9.2.10}$$

[4]need definition

Remark. Note that $\mathrm{tr} : M_n(\mathbb{F}) \to \mathbb{F}$ is linear.

Proposition 9.2.2. Suppose that $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,m}(\mathbb{F})$. Then $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Proof. We have

$$\mathrm{tr}(AB) = \sum_i \left(\sum_j a_{ij} b_{ji} \right) = \sum_j \left(\sum_i b_{ji} a_{ij} \right) = \mathrm{tr}(BA). \tag{9.2.11}$$

□

Definition 9.2.9 (commute matrices)**.** For matrices $A, B \in M_n(\mathbb{F})$, we say that A, B are commute if $AB = BA$. We can write this by

$$[A, B] = 0, \quad \text{where} \quad [A, B] := AB - BA. \tag{9.2.12}$$

9.2.2 Determinant

Definition 9.2.10 (determinant)**.** For $A \in M_n(\mathbb{F})$ define

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}. \tag{9.2.13}$$

where $\varepsilon(\sigma)$ is sign of permutation (see Definition 6.1.22) and it is homomorphism by Theorem 6.1.28.

Writing A_i for the ith column of a matrix A we have $A = (A_1, \dots, A_n)$, so we can think of A is an n-tuple of columns in $\mathbb{F}^n$. Write $\{e_1, \dots, e_n\}$ for the standard basis of $\mathbb{F}^n$.

Example 9.2.3. For 2×2 matrix A, we have $\det A = a_{11}a_{22} - a_{12}a_{21}$.

Definition 9.2.11 (volume form)**.** The function $d : \mathbb{F}^n \times \dots \times \mathbb{F}^n \to \mathbb{F}$ is a volumne form on $\mathbb{F}^n$ if

(i) it is multilinear, i.e.

$$\begin{aligned} d(v_1, \dots, \lambda_i v_i, \dots, v_n) &= \lambda d(v_1, \dots, v_i, \dots, v_n) \\ d(v_1, \dots, v_i + v_i', \dots, v_n) &= d(v_1, \dots, v_i, \dots, v_n) + d(v_1, \dots, v_i', \dots, v_n) \end{aligned}$$

(ii) it is alternating, i.e. whenever $i \neq j$ and $v_i = v_j$ then $d(v_1, \dots, v_n) = 0$.

Definition 9.2.12 (determinant function)**.** d is a determinant function if it is normalised volume form, i.e. $d(e_1, \dots, e_n) = 1$.

Lemma 9.2.4. Swapping columns in a volume form changes the sign. For $i \neq j$,

$$d(v_1, \dots, v_j, \dots, v_i, \dots, v_n) = -d(v_1, \dots, v_i, \dots, v_j, \dots, v_n). \tag{9.2.14}$$

Proof. By Definition 9.2.11.(ii),

$$0 = d(v_1, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_n) = 0 + d(v_1, \dots, v_i, \dots, v_j, \dots, v_n) + d(v_1, \dots, v_j, \dots, v_i, \dots, v_n) + 0 \tag{9.2.15}$$

by Definition 9.2.11.(i). □

Corollary 9.2.5. If $\sigma \in S_n$ and d is a volume form on $\mathbb{F}^n$ then

$$d(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \varepsilon(\sigma) d(v_1, \dots, v_n) \tag{9.2.16}$$

for $v_1, \dots, v_n \in \mathbb{F}^n$. In particular,

$$d(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \varepsilon(\sigma) d(e_1, \dots, e_n) = \varepsilon(\sigma) \tag{9.2.17}$$

if d is a determinant function.

Proof. Think about number of transpositions. □

Theorem 9.2.6. If d is a volume form on $\mathbb{F}^n$ and $A = (a_{ij}) = (A_1, \dots, A_n) \in M_n(\mathbb{F})$ then $d(A_1, \dots, A_n) = (\det A) d(e_1, \dots, e_n)$.

Proof.

$$\begin{aligned} d(A_1,\ldots,A_n) &= d\left(\sum_{j_1} a_{j_1,1}e_{j_1}, A_2,\ldots,A_n\right) = \sum_{j_1} a_{j_1,1} d\left(e_{j_1},A_2,\ldots,A_n\right) \\ &= \sum_{j_1,j_2} a_{j_1,1}a_{j_2,2} d(e_{j_1},e_{j_2},A_3,\ldots,A_n) = \sum_{j_1\neq j_2} a_{j_1,1}a_{j_2,2} d(e_{j_1},e_{j_2},A_3,\ldots,A_n) \end{aligned}$$

as d is zero when $j_1 = j_2$ by Definition 9.2.11.(ii). Then for $j_1,\ldots,j_n$ forming a permutation

$$d(A^{(1)},\ldots,A^{(n)}) = \sum_{j_1,\ldots,j_n} a_{j_1,1}\ldots a_{j_n,n} d(e_{j_1},\ldots,e_{j_n}) = \sum_{\sigma\in S_n} a_{\sigma(1)1}\ldots a_{\sigma(n)n}\varepsilon(\sigma) d(e_1,\ldots,e_n) = (\det A) d(e_1,\ldots,e_n).$$

by Definition 9.2.10. □

Theorem 9.2.7. If we define $d : \mathbb{F}^n \times \cdots \times \mathbb{F}^n \to \mathbb{F},\ d(A_1,\ldots,A_n) = \det A$ for $A = (A_1,\ldots,A_n)$ then d is a determinant function.

Proof. (i) $\prod_{j=1}^n a_{\sigma(j)j}$ is multilinear, hence so is the linear combination $\det A$.

(ii) We want to show that if $A_k = A_l$ with $k \neq l$ then $\det A = 0$. Write $\tau = (k\ l)$, a transposition in S_n.

$$\det A = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_j a_{\sigma(j)j} \tag{9.2.18}$$

Reorder the sum, take each even permutation σ followed by the odd permutation $\sigma\tau$ and note $\varepsilon(\sigma) = 1$, $\varepsilon(\sigma\tau) = -1$. Thus

$$\det A = \sum_{\sigma \text{ even}} \left(\prod_j a_{\sigma(j)j} - \prod_j a_{\sigma\tau(j)j}\right) = 0 \tag{9.2.19}$$

as each of the summands is zero since $a_{\sigma(k)k} = a_{\sigma(k)l}$, $a_{\sigma(l)k} = a_{\sigma(l)l}$ and

$$a_{\sigma(1)1}\ldots a_{\sigma(k)k}\ldots a_{\sigma(l)l}\ldots a_{\sigma(n)n} - a_{\sigma(1)1}\ldots a_{\sigma(l)k}\ldots a_{\sigma(k)l}\ldots a_{\sigma(n)n} = 0. \tag{9.2.20}$$

(iii) For normal basis $\{e_1,\ldots,e_n\}$, $d(e_1,\ldots,e_n) = \sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n \delta_{\sigma(j)j} = \varepsilon(\iota)\cdot 1 = 1$.
Thus, d is a determinant function. □

Proposition 9.2.8. Let $A \in M_n(\mathbb{F})$ and $\lambda \in \mathbb{F}$. Then

(i) $\det(A_1,\ldots,\lambda A_i,\ldots,A_n) = \lambda\det(A_1,\ldots,A_i,\ldots,A_n) = \det A$,

(ii) $\det(A_1,\ldots,A_i + A_i',\ldots,A_n) = \det(A_1,\ldots,A_i,\ldots,A_n) + \det(A_1,\ldots,A_i',\ldots,A_n)$,

(iii) $\det(A_1,\ldots,A_i,\ldots,A_j,\ldots,A_n) = -\det(A_1,\ldots,A_j,\ldots,A_i,\ldots,A_n)$,

(iv) If $A_i = A_j$, $\det(A_1,\ldots,A_i,\ldots,A_j,\ldots,A_n) = 0$.

Proof. This is direct result from Theorem 9.2.7, Lemma 9.2.4. □

Proposition 9.2.9. $\det A^T = \det A$.

Proof. If $\sigma \in S_n$ then $\prod_{j=1}^n a_{\sigma(j)j} = \prod_{j=1}^n a_{j\sigma(j)}$ as they contain the same factors but in a different order. Also, as σ runs through S_n, so does σ^{-1} and $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ (as $\sigma\sigma^{-1} = \iota$). Hence

$$\det A = \sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n a_{\sigma(j)j} = \sum_{\sigma\in S_n}\varepsilon(\sigma^{-1})\prod_{j=1}^n a_{j\sigma^{-1}(j)} = \sum_{\sigma'\in S_n}\varepsilon(\sigma')\prod_{j=1}^n a_{j\sigma'(j)} = \det A^T. \tag{9.2.21}$$

□

Proposition 9.2.10. For elementary matrices, the determinants are

$$\det T_{ij} = -1, \quad \det M_{i,\lambda} = \lambda, \quad \det C_{i,j,\lambda} = 1. \tag{9.2.22}$$

Proof. Obvious from Definition 9.1.11. □

Lemma 9.2.11. If E is an elementary matrix, then for any $n \times n$ matrix A,

$$\det(AE) = \det A \det E = \det(EA). \tag{9.2.23}$$

Performing an elementary column or row operation on A multiplies $\det A$ by the determinant of the corresponding elementary matrix.

Proof. By Proposition 9.2.10, the determinants of the elementary matrices are

$$\det T_{ij} = -1, \quad \det M_{i,\lambda} = \lambda, \quad \det C_{i,j,\lambda} = 1 \tag{9.2.24}$$

as we can see that the column and row operation have the same determinant by Proposition 9.2.9.

Performing the corresponding elementary column or row operation multiplies $\det A$ by $-1, \lambda, 1$, respectively. Then

$$\det(AE) = \det A \det E = \det\left(A^T\right) \det\left(E^T\right) = \det\left(A^T E^T\right) = \det\left((EA)^T\right) = \det(EA) \tag{9.2.25}$$

by Proposition 9.2.9. □

Theorem 9.2.12. Let $A \in M_n(\mathbb{F})$. Then A is invertible if and only if $\det A \neq 0$.

Proof. If A is invertible then A can be written as a product of elementary matrices by Lemma 9.1.22, so $\det A$ is the product of the corresponding determinants, so $\det A \neq 0$.

If A is singular (not invertible), we have that the columns of A are linearly dependent (Corollary 9.1.17). Then we can obtain a 0 column as a non-trivial combination of columns of A, so using elementary column operations on A we can obtain a matrix with a 0 column. Hence $\det A = 0$ by Lemma 9.2.11 as determinants of elementary matrices are no-zero. □

Theorem 9.2.13. If $A, B \in M_n(\mathbb{F})$, then $\det(AB) = \det A \det B = \det(BA)$.

Approach 1. First fix A. Consider $d_A : (B_1, \ldots, B_n) \mapsto \det(AB)$ for $B = (B_1, \ldots, B_n)$. Note that $\det(AB) = d_A(B_1, \ldots, B_n) = d((AB)_1, \ldots, (AB)_n)$ where d is volume form by Theorem 9.2.7. So d_A is multilinear and alternating and d_A is a volume form on $\mathbb{F}^n$. Hence

$$\det(AB) = d_A(B_1, \ldots, B_n) = (\det B) d_A(e_1, \ldots, e_n) = \det B \det A, \tag{9.2.26}$$

using Theorem 9.2.6. □

Approach 2. Expand by columns and by Corollary 9.2.5,

$$\begin{aligned}
\det(AB) &= \det\left(\sum_{j_1=1}^{n} b_{j_1,1} A_{j_1}, \ldots, \sum_{j_n=1}^{n} b_{j_n,n} A_{j_n}\right) = \sum_{\sigma \in S_n} \left(\prod_{j=1}^{n} b_{\sigma(j)j}\right) \det(A_{\sigma(1)}, \ldots, A_{\sigma(n)}) \\
&= \sum_{\sigma \in S_n} \left(\prod_{j=1}^{n} b_{\sigma(j)j}\right) \varepsilon(\sigma) \det(A_1, \ldots, A_n) = \sum_{\sigma \in S_n} \left(\prod_{j=1}^{n} b_{\sigma(j)j}\right) \varepsilon(\sigma) \det A = \det A \det B.
\end{aligned}$$

□

Approach 3. If B is singular, so $\mathrm{r}(B) < n$ by Theorem 9.1.15 and let $\mathrm{r}(B) = r$. Then by Lemma 9.1.12, we have for some invertible matrices P, Q,

$$B \sim \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \; B = Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} P^{-1} = \begin{pmatrix} C_r & 0 \\ 0 & 0 \end{pmatrix} \; \Rightarrow \; AB = A \begin{pmatrix} C_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} D_r & 0 \\ 0 & 0 \end{pmatrix} \tag{9.2.27}$$

where C_r and D_r are $r \times r$ submatrices. Therefore, we see that $\mathrm{r}(AB) \leq r \neq n$. So we have that AB is singular as well by Theorem 9.1.15. Hence $\det B = 0 = \det(AB)$.

So assume B is non-singular (invertible) and write it as a product of elementary matrices, $B = E_1 \ldots E_k$ by Lemma 9.1.22. Using Lemma 9.2.11,

$$\det(AB) = \det(AE_1 \ldots E_k) = \det A \det E_1 \ldots \det E_k = \det A \det B \tag{9.2.28}$$

as required. □

Corollary 9.2.14. If A is invertible then $\det A^{-1} = (\det A)^{-1}$.

Proof. As A is invertible, $AA^{-1} = I$ so $(\det A)(\det A^{-1}) = \det I = 1$ and hence $\det A^{-1} = (\det A)^{-1}$. □

Consider the system of linear equations $Ax = b$ with m equations and n unknowns. Here A is an $m \times n$ matrix, b is a column vector in $\mathbb{F}^m$. This has a solution if $\mathrm{r}(A) = \mathrm{r}(A|b)$. The solution is unique if and only if $n = \mathrm{r}\, A = \mathrm{r}(A|b)$, then the solution is $x = A^{-1}b$. To solve this equation, use Gaussian elimination[5]. In the case $m = n$, there is another method.

Lemma 9.2.15 (Cramer's rule)**.** If $A \in M_n(\mathbb{F})$ is non-singular then $Ax = b$ has $x = (x_1, \ldots, x_n)^T$ with $x_i = \frac{1}{\det A} \det A_{ib}$ for $i = 1, \ldots, n$ as its unique solution, where A_{ib} is the matrix obtained from A by deleting column i and inserting b.

Proof. Assume x is the solution of $Ax = b$. Then

$$\begin{aligned} \det A_{ib} &= \det(A_1, \ldots, A_{i-1}, b, A_{i+1}, \ldots, A_n) = \det(A_1, \ldots, A_{i-1}, Ax, A_{i+1}, \ldots, A_n) \\ &= \sum_{j=1} x_j \det(A_1, \ldots, A_{i-1}, A_j, A_{i+1}, \ldots, A_n) = x_i \det(A_1, \ldots, A_{i-1}, A_i, A_{i+1}, \ldots, A_n) = x_i \det A, \end{aligned}$$

so $x_i = \frac{1}{\det A} \det A_{ib}$ for $i = 1, \ldots, n$. □

Corollary 9.2.16. If $A \in M_n(\mathbb{Z})$ with $\det A = \pm 1$ and if $b \in \mathbb{Z}^n$ then we can solve $Ax = b$ over $\mathbb{Z}$.

Remark. The solution over $\mathbb{Z}$ is guaranteed since $\det A = \pm 1$.

9.2.3 Special square matrices

Definition 9.2.13 (diagonal matrix)**.** The matrix $D = (d_{ij}) \in M_n(\mathbb{F})$ is called diagonal matrix if $d_{ij} = 0$ whenever $i \neq j$, i.e.,

$$D = \begin{pmatrix} d_{11} & & & \\ & d_{22} & & \\ & & \ddots & \\ & & & d_{nn} \end{pmatrix}. \tag{9.2.29}$$

We denote such a matrix as

$$D = \mathrm{diag}(d_{11}, \ldots, d_{nn}) \quad \text{or} \quad D = \mathrm{diag}\, d, \tag{9.2.30}$$

where d is the vector of diagonal entries of D.

If all the diagonal entries of a diagonal matrix are positive (non-negative) real numbers, we refer to it as a positive (non-negative) diagonal matrix.

Remark. The identity matrix $I \in M_n(\mathbb{F})$ is an example of a positive diagonal matrix.

Definition 9.2.14 (scalar matrix)**.** A diagonal matrix $D \in M_n(\mathbb{F})$ is called scalar matrix if the diagonal entries of D are equal; that is, $D = \alpha I$ for some $\alpha \in \mathbb{C}$.

Proposition 9.2.17 (diagonal matrices properties)**.** (i) The determinant of a diagonal matrix is just the product of its diagonal entries: $\det D = \prod_{i=1}^n d_{ii}$.

(ii) A diagonal matrix is invertible if and only if all its diagonal entries are non-zero (by Theorem 9.2.12).

(iii) All diagonal matrices commute with each other under multiplication, i.e., $D_1 D_2 = D_2 D_1$, for diagonal matrices D_1, D_2.

(iv) A diagonal matrix D commutes with a given matrix $A = (a_{ij}) \in M_n(\mathbb{F})$ if and only if $a_{ij} = 0$ whenever the ith and jth diagonal entries of D differ.

(v) The product of two diagonal matrices is just the diagonal matrix of pairwise products of their respective diagonal entries and similarly for postive integer powers of a single diagonal matrix.

[5] need details

Definition 9.2.15 (block diagonal matrix)**.** A matrix $A = M_n(\mathbb{F})$ of the form

$$A = \begin{pmatrix} A_{11} & & & 0 \\ & A_{22} & & \\ & & \ddots & \\ 0 & & & A_{kk} \end{pmatrix} \tag{9.2.31}$$

in which $A_{ii} \in M_{n_i}(\mathbb{F})$, $i = 1, \ldots, k$ and $n = \sum_{j=1}^{k} n_j$, is called block diagonal matrix. Notationally, such a matrix is often indicated as

$$A = A_{11} \oplus A_{22} \oplus \cdots \oplus A_{kk}, \quad \text{or} \quad \bigoplus_{i=1}^{k} A_{ii}, \tag{9.2.32}$$

which is called the direct sum of the matrices $A_{11}, \ldots, A_{kk}$.

Proposition 9.2.18 (block diagonal matrices properties)**.** For matrix $A = \bigoplus_{i=1}^{k} A_{ii}$ and $B = \bigoplus_{i=1}^{k} B_{ii}$, in which each pair A_{ii}, B_{ii} has the same size.

(i) $\det A = \prod_{i=1}^{k} \det(A_{ii})$.

(ii) A is invertible if and only if each A_{ii}, $i = 1, \ldots, k$ is invertible.

(iii) $\mathrm{r}(A) = \sum_{i=1}^{k} \mathrm{r}(A_{ii})$.

(iv) A, B commute if and only if A_{ii} and B_{ii} commute, $i = 1, \ldots, k$.

Definition 9.2.16 (triangular matrix)**.** $A \in M_n(\mathbb{F})$ is an upper triangular matrix if $a_{ij} = 0$ whenever $i > j$. If $a_{ij} = 0$ whenever $i \geq j$, then A is said to be strictly upper triangular.

A is said to be lower triangular (or strictly upper triangular) if its transpose is upper triangular (or strictly upper triangular).

Example 9.2.19.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}, \tag{9.2.33}$$

A is upper triangular.

Lemma 9.2.20. If A is an upper triangular matrix, then $\det A = a_{11} \ldots a_{nn}$.

Proof. From the definition the determinant (Definition 9.2.10),

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(n)n}. \tag{9.2.34}$$

For a product to contribute, we must have $\sigma(i) \leq i$ for all $i = 1, \ldots, n$. Hence $\sigma(1) = 1$, $\sigma(2) = 2$, $\ldots$, $\sigma(n) = n$, so $\sigma = \iota$ and hence $\det A = a_{11} \ldots a_{nn}$. □

Proposition 9.2.21. If $A \in M_m(\mathbb{F})$, $B \in M_n(\mathbb{F})$ and $C \in M_{m,n}(\mathbb{F})$. Then $\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \det B$.

Approach 1. Fix B, C. Then $d_{B,C} : A \mapsto \det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ is a volume form on the column space $\mathbb{F}^m$ by Proposition 9.2.8. Hence by Theorem 9.2.6, $d_{B,C}(A) = \det A \det \begin{pmatrix} I & C \\ 0 & B \end{pmatrix}$.

Now keep C fixed. The map $B \mapsto \det \begin{pmatrix} I & C \\ 0 & B \end{pmatrix}$ is a volume form on the row space $\mathbb{F}^n$ by Proposition 9.2.8. Hence $\det \begin{pmatrix} I & C \\ 0 & B \end{pmatrix} = \det B \begin{pmatrix} I & C \\ 0 & I \end{pmatrix}$ by Theorem 9.2.6.

Now $\det \begin{pmatrix} I & C \\ 0 & I \end{pmatrix} = 1$ as $\begin{pmatrix} I & C \\ 0 & I \end{pmatrix}$ is upper triangular matrix. So $\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \det B \cdot 1 = \det A \det B$ by Lemma 9.2.20. □

Approach 2. Write $X = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ and expand the expression for the determinant.

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \sum_{\sigma \in S_{m+n}} \varepsilon(\sigma) \prod_{j=1}^{m+n} x_{\sigma(j)j} \tag{9.2.35}$$

Note $x_{\sigma(j)j} = 0$ if $j \leq m$, $\sigma(j) > m$, so we only sum over σ with the following properties.

(i) For $j \in [1, m]$, $\sigma(j) \in [1, m]$. Here $x_{\sigma(j)j} = a_{\sigma_1(j)j}$ where $\sigma_1 \in S_m$ is the restriction of σ to $[1, m]$.

(ii) For $j \in [m+1, m+n]$, $\sigma(j) \in [m+1, m+n]$. Here, writing $k = j-m$, we have $x_{\sigma(j)j} = b_{\sigma_2(k)k}$ where $\sigma_2(k) = \sigma(m+k)-m$.

Noting also that $\varepsilon(\sigma) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$ for such σ, we obtain

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \left(\sum_{\sigma_1 \in S_m} \varepsilon(\sigma_1) \prod_{j=1}^{m} a_{\sigma_1(j)j} \right) \left(\sum_{\sigma_2 \in S_k} \varepsilon(\sigma_2) \prod_{l=1}^{k} a_{\sigma_2(j)j} \right) = \det A \det B. \tag{9.2.36}$$

□

9.2.4 Adjugate matrices

Definition 9.2.17 (minor)**.** Let $A = (a_{ij})$ be an $n \times n$ matrix. Write $\widehat{A}_{ij}$ for the $(n-1) \times (n-1)$ matrix obtained from A by deleting row i and column j. Let $M_{ij} = \det \widehat{A}_{ij}$. We call M_{ij} the (i, j) minor of A.

Example 9.2.22. As a specific example, we have

$$A = \begin{pmatrix} -3 & 2 & -5 \\ -1 & 0 & -2 \\ 3 & -4 & 1 \end{pmatrix} \Rightarrow \operatorname{adj} A = \begin{pmatrix} -8 & 18 & -4 \\ -5 & 12 & -1 \\ 4 & -6 & 2 \end{pmatrix}. \tag{9.2.37}$$

The -6 in the third row, second column of the adjugate was computed as follows:

$$(-1)^{2+3} \det \begin{pmatrix} -3 & 2 \\ 3 & -4 \end{pmatrix} = -((-3)(-4) - (3)(2)) = -6. \tag{9.2.38}$$

Again, the (3,2) entry of the adjugate is the (2,3) cofactor of A. Thus, the submatrix $\begin{pmatrix} -3 & 2 \\ 3 & -4 \end{pmatrix}$ was obtained by deleting the second row and third column of the original matrix A.

Lemma 9.2.23. Let $A \in M_n(\mathbb{F})$ and M is the minor matrix of A.

(i) For fixed j, $\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} M_{ij}$.

(ii) For fixed i, $\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} M_{ij}$.

Remark. This can be used as a definition of determinant.

Proof. By Proposition 9.2.8,

$$\begin{aligned} \det A &= \det(A_1, \ldots, A_n) = \sum_{i=1}^{n} \det \left(A_1, \ldots, A_{j-1}, A'_j, A_{j+1}, \ldots, A_n\right) \\ &= \sum_{i=1}^{n} a_{ij} \det \left(A_1, \ldots, A_{j-1}, e_i, A_{j+1}, \ldots, A_n\right) \end{aligned}$$

where $A'_j = \Big(0, \ldots, 0, a_{ij}, 0, \ldots, 0\Big)^T$ (the only non-zero element is in row i).

Now we can swap row i and row $i-1$, and then swap row $i-1$ and $i-2$,... Finally, we have shift original row i to row 1 and this need $i-1$ transpositions (similarly for column operations which need $j-1$ transpositions, so totally $i+j-2$

transpositions). Thus, by Proposition 9.2.8.(iii),

$$\det A = \sum_{i=1}^{n} a_{ij}(-1)^{i+j-2} \det \begin{pmatrix} 1 & * \\ 0 & \widehat{A}_{ij} \end{pmatrix} = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} M_{ij}, \tag{9.2.39}$$

using Proposition 9.2.21. (ii) is similar by using determinant of transpose matrix (Proposition 9.2.9). □

Definition 9.2.18 (cofactor matrix)**.** Let $A \in M_n(\mathbb{F})$ and M_{ij} is the (i,j) minor of A. Then cofactor matrix of A is $C = (c_{ij})$ where $c_{ij} = (-1)^{i+j} M_{ij}$.

Definition 9.2.19 (adjugate matrix)**.** Let $A \in M_n(\mathbb{F})$ and C is cofactor matrix of A. The adjugate matrix is $\operatorname{adj} A = C^T$, i.e. the $n \times n$ matrix with (i,j) entry equal to $(-1)^{i+j} M_{ji} = (-1)^{i+j} \det\left(\widehat{A}_{ji}\right)$.

Theorem 9.2.24. (i) $(\operatorname{adj} A)A = (\operatorname{adj} A)A = (\det A)I$.

(ii) If A is invertible then $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$.

Proof. (i) By Lemma 9.2.23.(i), fix j,

$$\det A = \sum_{i=1}^{n} (\operatorname{adj} A)_{ji} a_{ij} = ((\operatorname{adj} A)A)_{jj}. \tag{9.2.40}$$

Also, for fix $j < k$, by Proposition 9.2.8 and Lemma 9.2.23,

$$0 = \det(A_1, \ldots, A_k, \ldots, A_k, \ldots, A_n) = \sum_{i=1}^{n} (\operatorname{adj} A)_{ji} a_{ik} = ((\operatorname{adj} A)A)_{jk}. \tag{9.2.41}$$

Similarly, from Lemma 9.2.23.(ii), we have $(\operatorname{adj} A)A = (\det A)I$.

(ii) If A is invertible, then $\det A \neq 0$ (by Theorem 9.2.12), so $\frac{1}{\det A}(\operatorname{adj} A)A = I$ and hence we deduce $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$.

□

Proposition 9.2.25. (i) $\operatorname{adj} I = I$ where $I \in M_n(\mathbb{F})$ is identity matrix.

(ii) For $A \in M_n(\mathbb{F})$, $\operatorname{adj}(\lambda A) = \lambda^{n-1} \operatorname{adj} A$.

(iii) $\operatorname{adj}\left(A^T\right) = (\operatorname{adj} A)^T$.

(iv) $\operatorname{adj}\left(\overline{A}\right) = \overline{\operatorname{adj} A}$.

(v) Adjugate matrices of diagonal matrices are still diagonal matrices, i.e., if $A = \operatorname{diag}(a_1, a_2, \ldots, a_n)$, then

$$\operatorname{adj} A = \operatorname{diag}\left(\prod_{i=2}^{n} a_i, \prod_{i=1, i\neq 2}^{n} a_i, \prod_{i=1, i\neq 3}^{n} a_i, \ldots, \prod_{i=1}^{n-1} a_i\right). \tag{9.2.42}$$

(vi) Adjugate matrices of symmetric matrices are still symmetric matrices, i.e., if $A^T = A$, then $(\operatorname{adj} A)^T = \operatorname{adj} A$.

(vii) If $A \in M_n(\mathbb{F})$ is antisymmetric, i.e., $A^T = -A$, then

$$(\operatorname{adj} A)^T = \begin{cases} -\operatorname{adj} A & n \text{ is even} \\ \operatorname{adj} A & n \text{ is odd} \end{cases} \tag{9.2.43}$$

(viii) For elementary operations,

$$\operatorname{adj} T_{i,j} = -T_{i,j}, \quad i \neq j, \qquad \operatorname{adj} M_{i,\lambda} = \lambda M_{i,1/\lambda}, \quad c \neq 0, \qquad \operatorname{adj} C_{i,j,\lambda} = C_{i,j,-\lambda}. \tag{9.2.44}$$

(ix) Let Q be an othogonal matrix. Then

$$\operatorname{adj} Q = \begin{cases} Q^T & \det Q = 1 \\ -Q^T & \det Q = -1 \end{cases} \tag{9.2.45}$$

Proof. (i)-(iv) are obvious from definition of adjugate matrix (Definition 9.2.19).

(v) [6]

□

Lemma 9.2.26. For any $A \in M_n(\mathbb{F})$ and invertible matices $P, Q \in M_n(\mathbb{F})$, $\operatorname{adj}(PAQ) = \operatorname{adj} Q \operatorname{adj} A \operatorname{adj} P$.

Proof. Let E be an elementary matrix.

If E is switching matrix $T_{i,j}$ $(i < j)$, then by Proposition 9.2.8.(iii),

$$\begin{aligned}
\operatorname{adj}(AT_{i,j}) &= \operatorname{adj}\left(A_1, \ldots, A_j, \ldots, A_i, \ldots, A_n\right) \\
&= \begin{pmatrix}
-(-1)^{1+1}\det\left(\widehat{A}_{11}\right) & & -(-1)^{2+1}\det\left(\widehat{A}_{21}\right) & \cdots & -(-1)^{n+1}\det\left(\widehat{A}_{n1}\right) \\
& \vdots & & & \\
(-1)^{1+i}(-1)^{j-i-1}\det\left(\widehat{A}_{1j}\right) & & (-1)^{2+i}(-1)^{j-i-1}\det\left(\widehat{A}_{2j}\right) & \cdots & (-1)^{n+i}(-1)^{j-i-1}\det\left(\widehat{A}_{nj}\right) \\
& \vdots & & & \\
(-1)^{1+j}(-1)^{j-i-1}\det\left(\widehat{A}_{1i}\right) & & (-1)^{2+j}(-1)^{j-i-1}\det\left(\widehat{A}_{2i}\right) & \cdots & (-1)^{n+j}(-1)^{j-i-1}\det\left(\widehat{A}_{ni}\right) \\
& \vdots & & & \\
-(-1)^{1+n}\det\left(\widehat{A}_{1n}\right) & & -(-1)^{2+n}\det\left(\widehat{A}_{2n}\right) & \cdots & -(-1)^{n+n}\det\left(\widehat{A}_{nn}\right)
\end{pmatrix}
\end{aligned}$$

where $(-1)^{j-i}\det\left(\widehat{A}_{kj}\right)$ (as we shift A_i to its original position with $j-i-1$ times) is (k,j) minor of $AT_{i,j}$. Thus,

$$\operatorname{adj}(AT_{i,j}) = \begin{pmatrix}
-(-1)^{1+1}\det\left(\widehat{A}_{11}\right) & -(-1)^{2+1}\det\left(\widehat{A}_{21}\right) & \cdots & -(-1)^{n+1}\det\left(\widehat{A}_{n1}\right) \\
\vdots & & & \\
-(-1)^{1+j}\det\left(\widehat{A}_{1j}\right) & -(-1)^{2+j}\det\left(\widehat{A}_{2j}\right) & \cdots & -(-1)^{n+j}\det\left(\widehat{A}_{nj}\right) \\
\vdots & & & \\
-(-1)^{1+i}\det\left(\widehat{A}_{1i}\right) & -(-1)^{2+i}\det\left(\widehat{A}_{2i}\right) & \cdots & -(-1)^{n+i}\det\left(\widehat{A}_{ni}\right) \\
\vdots & & & \\
-(-1)^{1+n}\det\left(\widehat{A}_{1n}\right) & -(-1)^{2+n}\det\left(\widehat{A}_{2n}\right) & \cdots & -(-1)^{n+n}\det\left(\widehat{A}_{nn}\right)
\end{pmatrix} = \operatorname{adj} T_{i,j} \operatorname{adj} A.$$

Also, since $T_{i,j}^T = T_{i,j}$, by Proposition 9.2.25.(iii) and Proposition 9.1.6

$$\operatorname{adj}(T_{i,j}A) = \operatorname{adj}\left(T_{i,j}^T A\right) = \operatorname{adj}\left(\left(A^T T_{i,j}\right)^T\right) = \left(\operatorname{adj}\left(A^T T_{i,j}\right)\right)^T = \left(\operatorname{adj} T_{i,j} \operatorname{adj}\left(A^T\right)\right)^T = \operatorname{adj} A \operatorname{adj} T_{i,j}. \tag{9.2.46}$$

If E is multiplication matrix $M_{i,\lambda}$ $(\lambda \neq 0)$, we have by Theorem 9.2.24.(ii) and Proposition 9.1.21,

$$\begin{aligned}
\operatorname{adj}(AM_{i,\lambda}) &= \operatorname{adj}\left(A_1, \ldots, \lambda A_i, \ldots, A_n\right) \\
&= \begin{pmatrix}
\lambda(-1)^{1+1}\det\left(\widehat{A}_{11}\right) & \lambda(-1)^{2+1}\det\left(\widehat{A}_{21}\right) & \cdots & \lambda(-1)^{n+1}\det\left(\widehat{A}_{n1}\right) \\
\vdots & & & \\
(-1)^{1+i}\det\left(\widehat{A}_{1i}\right) & (-1)^{2+i}\det\left(\widehat{A}_{2i}\right) & \cdots & (-1)^{n+i}\det\left(\widehat{A}_{ni}\right) \\
\vdots & & & \\
\lambda(-1)^{1+n}\det\left(\widehat{A}_{1n}\right) & \lambda(-1)^{2+n}\det\left(\widehat{A}_{2n}\right) & \cdots & \lambda(-1)^{n+n}\det\left(\widehat{A}_{nn}\right)
\end{pmatrix} \\
&= \lambda M_{i,1/\lambda} \operatorname{adj} A = \det\left(M_{i,\lambda}\right)\left(M_{i,\lambda}\right)^{-1} \operatorname{adj} A = \operatorname{adj} M_{i,\lambda} \operatorname{adj} A.
\end{aligned}$$

Similarly, since $M_{i,\lambda}^T = M_{i,\lambda}$, by Proposition 9.2.25.(iii) and Proposition 9.1.6

$$\operatorname{adj}(M_{i,\lambda}A) = \operatorname{adj}\left(M_{i,\lambda}^T A\right) = \operatorname{adj}\left(\left(A^T M_{i,\lambda}\right)^T\right) = \left(\operatorname{adj}\left(A^T M_{i,\lambda}\right)\right)^T = \left(\operatorname{adj} M_{i,\lambda} \operatorname{adj}\left(A^T\right)\right)^T = \operatorname{adj} A \operatorname{adj} M_{i,\lambda}. \tag{9.2.47}$$

[6] need proof

If E is addition matrix $C_{i,j,\lambda}$ $(i<j)$, we have by Proposition 9.2.8.(ii,iv),

$$\begin{aligned}\operatorname{adj}(AC_{i,j,\lambda}) &= \operatorname{adj}\left(A_1,\dots,A_i,\dots,A_j+\lambda A_i,\dots,A_n\right)\\ &= \begin{pmatrix} (-1)^{1+1}\det\left(\widehat{A}_{11}\right) & \dots & \lambda(-1)^{n+1}\det\left(\widehat{A}_{n1}\right)\\ \vdots & & \\ (-1)^{1+i}\left(\lambda(-1)^{j-i-1}\det\left(\widehat{A}_{1j}\right)+\det\left(\widehat{A}_{1i}\right)\right) & \dots & (-1)^{n+i}\left(\lambda(-1)^{j-i-1}\det\left(\widehat{A}_{nj}\right)+\det\left(\widehat{A}_{ni}\right)\right)\\ \vdots & & \\ (-1)^{1+j}\det\left(\widehat{A}_{1j}\right) & \dots & (-1)^{n+j}\det\left(\widehat{A}_{nj}\right)\\ \vdots & & \\ (-1)^{1+n}\det\left(\widehat{A}_{1n}\right) & \dots & (-1)^{n+n}\det\left(\widehat{A}_{nn}\right)\end{pmatrix}\end{aligned}$$

Thus, by Theorem 9.2.24.(ii), Proposition 9.1.21 and Proposition 9.2.10 $(\det(C_{i,j,\lambda})=1)$,

$$\begin{aligned}\operatorname{adj}(AC_{i,j,\lambda}) &= \begin{pmatrix} (-1)^{1+1}\det\left(\widehat{A}_{11}\right) & \dots & \lambda(-1)^{n+1}\det\left(\widehat{A}_{n1}\right)\\ \vdots & & \\ -\lambda(-1)^{1+j}\det\left(\widehat{A}_{1j}\right)+(-1)^{1+i}\det\left(\widehat{A}_{1i}\right) & \dots & -\lambda(-1)^{n+j}\det\left(\widehat{A}_{nj}\right)+(-1)^{n+i}\det\left(\widehat{A}_{ni}\right)\\ \vdots & & \\ (-1)^{1+j}\det\left(\widehat{A}_{1j}\right) & \dots & (-1)^{n+j}\det\left(\widehat{A}_{nj}\right)\\ \vdots & & \\ (-1)^{1+n}\det\left(\widehat{A}_{1n}\right) & \dots & (-1)^{n+n}\det\left(\widehat{A}_{nn}\right)\end{pmatrix}\\ &= C_{i,j,-\lambda}\operatorname{adj}A=\det(C_{i,j,\lambda})(C_{i,j,-\lambda})^{-1}\operatorname{adj}A=\operatorname{adj}C_{i,j,\lambda}\operatorname{adj}A.\end{aligned}$$

With the same argument as above, we have $\operatorname{adj}(C_{i,j,\lambda}A)=\operatorname{adj}A\operatorname{adj}C_{i,j,\lambda}$. Therefore, for any elementary matrix E, we have

$$\operatorname{adj}(AE)=\operatorname{adj}E\operatorname{adj}A,\quad \operatorname{adj}(EA)=\operatorname{adj}A\operatorname{adj}E. \tag{9.2.48}$$

Recall Lemma 9.1.22, any invertible matrices P,Q can be written as the products of elementary matrices $P=E_1\dots E_m$, $Q=F_1\dots F_k$. Then

$$\begin{aligned}\operatorname{adj}(PAQ) &= \operatorname{adj}(E_1\dots E_mAF_1\dots F_k)=(\operatorname{adj}F_k\dots\operatorname{adj}F_1)\operatorname{adj}A(\operatorname{adj}E_m\dots\operatorname{adj}E_1)\\ &= \operatorname{adj}(F_1\dots F_k)\operatorname{adj}A\operatorname{adj}(E_1\dots E_m)=\operatorname{adj}Q\operatorname{adj}A\operatorname{adj}P.\end{aligned}$$

□

Theorem 9.2.27. Let $A\in M_n(\mathbb{F})$ $(n>1)$. Then

$$\mathrm{r}(\operatorname{adj}A)=\begin{cases} n & \mathrm{r}(A)=n\\ 1 & \mathrm{r}(A)=n-1\\ 0 & \text{otherwise}\end{cases} \tag{9.2.49}$$

Proof. If $\mathrm{r}(A)=n$, $\det A\neq 0$. Then by Theorem 9.2.24, $\operatorname{adj}A$ is invertible and hence $\mathrm{r}(\operatorname{adj}A)=n$ by Theorem 9.1.15.

If $\mathrm{r}(A)=n-1$, it is equivalent to matrix $I'=\begin{pmatrix} I_{n-1} & 0\\ 0 & 0\end{pmatrix}$. That is, there exists invertible matrices P,Q such that $A=PI'Q$. By Lemma 9.2.26, we have $\operatorname{adj}A=\operatorname{adj}Q\operatorname{adj}I'\operatorname{adj}P$. Since P,Q are full-rank, by Proposition 9.1.18.(i), we have

$$\mathrm{r}(\operatorname{adj}A)\leq\mathrm{r}(\operatorname{adj}I')=\mathrm{r}\begin{pmatrix}0&0\\0&1\end{pmatrix}=1. \tag{9.2.50}$$

Also, $I'=P^{-1}AQ^{-1}$, Proposition 9.1.18.(i) gives that $1=\mathrm{r}(\operatorname{adj}I')\leq\mathrm{r}(\operatorname{adj}A)\ \Rightarrow\ \mathrm{r}(\operatorname{adj}A)=1$.

With similar argument, we have that $\mathrm{r}(\operatorname{adj}A)=0$ if $\mathrm{r}(A)<n-1$. □

Proposition 9.2.28. Let $A \in M_n(\mathbb{F})$. Then the k-fold adjugate matrix of A, $\mathrm{adj}^{[k]}(A) := \mathrm{adj}\,(\mathrm{adj}\,(\ldots \mathrm{adj}\,A \ldots))$ (k times) is

$$\mathrm{adj}^{[k]}(A) = \begin{cases} (\det A)^{\frac{(n-1)^k-(n-1)}{n}} \mathrm{adj}\,A & \mathrm{r}(A) = n,\ k \text{ is odd} \\ (\det A)^{\frac{(n-1)^k-1}{n}} A & \mathrm{r}(A) = n,\ k \text{ is even} \\ 0 & \mathrm{r}(A) = n-1,\ k \geq 2 \\ 0 & \mathrm{r}(A) < n-1,\ k \geq 1 \end{cases} \tag{9.2.51}$$

In particular, $\mathrm{adj}\,(\mathrm{adj}\,A) = (\det A)^{n-2} A$.

Proof. For $k = 1$, by Theorem 9.2.27, the conclusion holds.

For $k \geq 2$, $\mathrm{adj}^{[k]}(A) = 0$ if $\mathrm{r}(A) \leq n-1$ by Theorem 9.2.27. Thus, we only need to check the full-rank situation.

Now assume $\mathrm{r}(A) = n$. If $k = 2$, we have

$$\mathrm{adj}\,(\mathrm{adj}\,A) = \det(\mathrm{adj}\,A)\,(\mathrm{adj}\,A)^{-1} = \det\left(\det AA^{-1}\right)\left(\det AA^{-1}\right)^{-1} = (\det A)^{n-1} \det\left(A^{-1}\right) A = (\det A)^{n-2} A. \tag{9.2.52}$$

Now assume the conclusion holds for k. If k is odd, $\mathrm{adj}^{[k]}(A) = (\det A)^{\frac{(n-1)^k-(n-1)}{n}} \mathrm{adj}\,A$. Then by Proposition 9.2.25.(ii) and the case $k = 2$,

$$\begin{aligned} \mathrm{adj}^{[k+1]}(A) &= \mathrm{adj}\left((\det A)^{\frac{(n-1)^k-(n-1)}{n}} \mathrm{adj}\,A\right) = \left((\det A)^{\frac{(n-1)^k-(n-1)}{n}}\right)^{n-1} \mathrm{adj}^{[2]}(A) \\ &= (\det A)^{\frac{(n-1)^{k+1}-(n-1)^2}{n}} (\det A)^{n-2} A = (\det A)^{\frac{(n-1)^{k+1}-1}{n}} A. \end{aligned}$$

If k is even, $\mathrm{adj}^{[k]}(A) = (\det A)^{\frac{(n-1)^k-1}{n}} A$. Then by Proposition 9.2.25.(ii),

$$\mathrm{adj}^{[k+1]}(A) = \mathrm{adj}\left((\det A)^{\frac{(n-1)^k-1}{n}} A\right) = \left((\det A)^{\frac{(n-1)^k-1}{n}}\right)^{n-1} \mathrm{adj}\,A = (\det A)^{\frac{(n-1)^{k+1}-(n-1)}{n}} \mathrm{adj}\,A.$$

□

Theorem 9.2.29. For any $A, B \in M_n(\mathbb{F})$, $\mathrm{adj}\,(AB) = \mathrm{adj}\,B\,\mathrm{adj}\,A$.

Proof. If A, B are invertible, we have AB is also invertible. Then by Theorem 9.2.13, Proposition 9.1.11 and Theorem 9.2.24,

$$\mathrm{adj}\,(AB) = \det(AB)\,(AB)^{-1} = \det A \det BB^{-1}A^{-1} = \mathrm{adj}\,B\,\mathrm{adj}\,A. \tag{9.2.53}$$

If $\min\{\mathrm{r}(A), \mathrm{r}(B)\} < n-1$ with $\mathrm{adj}\,A = 0$ or $\mathrm{adj}\,B = 0$, then by Proposition 9.1.18.(i),

$$\mathrm{r}(AB) \leq \min\{\mathrm{r}(A), \mathrm{r}(B)\} < n-1 \ \Rightarrow\ \mathrm{adj}\,(AB) = 0 = \mathrm{adj}\,B\,\mathrm{adj}\,A \tag{9.2.54}$$

by Theorem 9.2.27.

If $\min\{\mathrm{r}(A), \mathrm{r}(B)\} = n-1$ and $\max\{\mathrm{r}(A), \mathrm{r}(B)\} = n$, we can assume $\mathrm{r}(A) = n$ and $\mathrm{r}(B) = n-1$ wlog as we can take transpose of AB. Then by Lemma 9.2.26, we have $\mathrm{adj}\,(AB) = \mathrm{adj}\,B\,\mathrm{adj}\,A$.

Therefore, there leaves the last case, $\mathrm{r}(A) = \mathrm{r}(B) = n-1$. Assume that (by Lemma 9.1.12)

$$A = P \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} Q, \quad B = U \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} V \tag{9.2.55}$$

where P, Q, U, V are invertible matrices and

$$QU = \begin{pmatrix} C_{(n-1)\times(n-1)} & D_{(n-1)\times 1} \\ E_{1\times(n-1)} & F_{1\times 1} \end{pmatrix}. \tag{9.2.56}$$

Therefore, by Lemma 9.2.26,

$$\begin{aligned}\operatorname{adj}(AB) &= \operatorname{adj}\left(P\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} C_{(n-1)\times(n-1)} & D_{(n-1)\times 1} \\ E_{1\times(n-1)} & F_{1\times 1}\end{pmatrix}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} V\right) = \operatorname{adj}\left(P\begin{pmatrix} C_{(n-1)\times(n-1)} & 0 \\ 0 & 0 \end{pmatrix} V\right) \\ &= \operatorname{adj} V \operatorname{adj}\begin{pmatrix} C_{(n-1)\times(n-1)} & 0 \\ 0 & 0 \end{pmatrix} \operatorname{adj} P = \operatorname{adj} V \begin{pmatrix} 0 & 0 \\ 0 & \det C_{(n-1)\times(n-1)}\end{pmatrix} \operatorname{adj} P.\end{aligned}$$

But $\operatorname{adj}\begin{pmatrix} C_{(n-1)\times(n-1)} & 0 \\ E_{1\times(n-1)} & 0 \end{pmatrix} \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \alpha & \det C_{(n-1)\times(n-1)}\end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \det C_{(n-1)\times(n-1)}\end{pmatrix}$. Then we have (by Lemma 9.2.26)

$$\begin{aligned}\operatorname{adj}(AB) &= \operatorname{adj} V \left(\operatorname{adj}\begin{pmatrix} C_{(n-1)\times(n-1)} & 0 \\ E_{1\times(n-1)} & 0 \end{pmatrix} \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj} P \\ &= \operatorname{adj} V \left(\operatorname{adj}\left(\begin{pmatrix} C_{(n-1)\times(n-1)} & D_{(n-1)\times 1} \\ E_{1\times(n-1)} & F_{1\times 1}\end{pmatrix}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj} P \\ &= \operatorname{adj} V \left(\operatorname{adj}\left(QU\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj} P \\ &= \operatorname{adj} V \operatorname{adj}\left(\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}\right) \operatorname{adj}(QU) \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} \operatorname{adj} P \\ &= \operatorname{adj} V \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} \operatorname{adj} U \operatorname{adj} Q \operatorname{adj}\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} \operatorname{adj} P \\ &= \operatorname{adj}\left(U\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} V\right) \operatorname{adj}\left(P\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} Q\right) = \operatorname{adj} B \operatorname{adj} A.\end{aligned}$$

Therefore, the equation holds for any $A, B \in M_n(\mathbb{F})$. □

Corollary 9.2.30. For given k and any $A \in M_n(\mathbb{F})$,

(i) $\operatorname{adj}(A_1 A_2 \dots A_k) = \operatorname{adj} A_k \operatorname{adj} A_{k-1} \dots \operatorname{adj} A_1$.

(ii) $\operatorname{adj}\left(A^k\right) = (\operatorname{adj} A)^k$.

Proposition 9.2.31. For given $k \geq 1$,

(i) $\operatorname{adj}\left(A^{-1}\right) = (\operatorname{adj} A)^{-1}$.

(ii) $\det(\operatorname{adj} A) = (\det A)^{n-1}$ for $n \geq 2$.

(iii) $\det\left(\operatorname{adj}^{[k]}(A)\right) = (\det A)^{(n-1)^k}$.

(iv) $\det(\operatorname{adj}(A_1 A_2 \dots A_k)) = \prod_{i=1}^k \det(\operatorname{adj} A_i) = \left(\prod_{i=1}^k \det A_i\right)^{n-1}$.

(v) $\det\left(\operatorname{adj}(A^k)\right) = (\det(\operatorname{adj} A))^k = (\det A)^{k(n-1)}$.

Proof. (i) $\operatorname{adj}\left(A^{-1}\right) \operatorname{adj} A = \operatorname{adj}\left(AA^{-1}\right) = \operatorname{adj} I = I$. $\operatorname{adj} A \operatorname{adj}\left(A^{-1}\right) = \operatorname{adj}\left(A^{-1}A\right) = \operatorname{adj} I = I$. Thus, $\operatorname{adj}\left(A^{-1}\right)$ is the inverse of $\operatorname{adj} A$ by Proposition 9.1.10.

(ii) If $\mathrm{r}(A) < n$, we have $\det A = 0$ and thus $\mathrm{r}(\operatorname{adj} A) < n$ by Theorem 9.2.27. Thus, $\det(\operatorname{adj} A) = 0$, which satisfies the statement.

If A is full-rank, then we have $\det\left(\det AA^{-1}\right) = (\det A)^n \det\left(A^{-1}\right) = (\det A)^{n-1}$.

(iii) If $k = 1$, it is (ii). If $\mathrm{r}(A) < n$, we have $\det A = 0 = \det\left(\operatorname{adj}^{[k]}(A)\right)$. Now we assume the conclusion holds for k and A

is full-rank (thus $\text{adj}^{[k]}(A)$ is full-rank). Then

$$\begin{aligned}\det\left(\text{adj}^{[k+1]}(A)\right) &= \det\left(\text{adj}\left(\text{adj}^{[k]}(A)\right)\right) = \det\left(\det\left(\text{adj}^{[k]}(A)\right)\left(\text{adj}^{[k]}(A)\right)^{-1}\right)\\ &= \left(\det\left(\text{adj}^{[k]}(A)\right)\right)^{n}\det\left(\left(\text{adj}^{[k]}(A)\right)^{-1}\right) = \left(\det\left(\text{adj}^{[k]}(A)\right)\right)^{n-1}\\ &= \left((\det A)^{(n-1)^k}\right)^{n-1} = (\det A)^{(n-1)^{k+1}}.\end{aligned}$$

(iv,v) are direct results from (iii) and Corollary 9.2.30. □

9.2.5 Similar Matrices

Definition 9.2.20 (similar matrices)**.** Two $n \times n$ matrices A, A' are similar if $A' = P^{-1}AP$ for some invertible matrix P.

Proposition 9.2.32. Similar matrices have the same determinant.

Proof. If A and A' are similar, then there exists invertible matrix P such that $A' = P^{-1}AP$. Then by Theorem 9.2.13 and Corollary 9.2.14,

$$\det A' = \det\left(P^{-1}AP\right) = \det\left(P^{-1}\right)\det A\det P = (\det A)(\det P)(\det P)^{-1} = \det A. \tag{9.2.57}$$

□

Proposition 9.2.33. Similar matrices have the same trace, i.e., for $A' = P^{-1}AP$ for some invertible matrix P, $\text{tr}\, A' = \text{tr}\, A$.

Proof. By Proposition 9.2.2,

$$\text{tr}\, A' = \text{tr}\left(P^{-1}AP\right) = \text{tr}\left(APP^{-1}\right) = \text{tr}\left(AI\right) = \text{tr}\, A. \tag{9.2.58}$$

□

9.3 Groups of Matrices

9.4 Matrix Calculus

9.5 Problems

9.6 Summary

	matrix	rank	determinant	trace
equivalence	$m \times n$	$\surd$	-	-
similarity	$n \times n$	$\surd$	$\surd$	$\surd$

Part III

Analysis

Chapter 10

Real Analysis

10.1 Series

10.2 Fundamental Axioms and Theorems

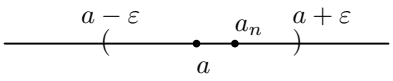
10.2.1 Limits, convergence and fundamental axim of analysis

What is the difference between $\mathbb{R}$ and $\mathbb{Q}$ which makes calculus work on one even though it fails on the other? Both are 'ordered fields', that is, both support operations of 'addition' and 'multiplication' together with a relation 'greater than' ('order') with the properties that we expect.

To state the difference we need the following definition (by recalling definition of sequence[1]):

Definition 10.2.1 (convergence, limit)**.** Let $a_n \in \mathbb{R}$ be a sequence of real numbers and a a real number. We say a_n converges to a limit a, if given $\varepsilon > 0$, there exists $N \in \mathbb{N}$ (or $N(\varepsilon)$) such that $|a_n - a| < \varepsilon$, for all $n \geq N$, denoted by $a_n \to a \in \mathbb{R}$ as $n \to \infty$, i.e.,

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N}\ \text{ s.t. } |a_n - a| < \varepsilon,\ \forall n \geq N. \tag{10.2.1}$$



Otherwise, we say a_n is divergent.

The key property of the reals, the following axiom makes everything work.

Axiom 10.2.1 (Fundamental Axiom of Analysis)**.** Suppose $a_n \in \mathbb{R}$ for all n and there is $A \in \mathbb{R}$ such that $a_n \leq A$ for all n and a_n is increasing. Then there exists $a \in \mathbb{R}$ such that $a_n \to a$ as $n \to \infty$. Less ponderously, and just as rigorously, every increasing sequence bounded above tends to a limit.

Remark. (i) We could have phrased the Axiom with decreasing sequences bounded below.

(ii) The Axiom is equivalent to the fact that every non-empty set of real numbers bounded above has a supremum (or least upper bound).

(iii) Everything which depends on the fundamental axiom is analysis, everything else is mere algebra.

Proposition 10.2.2. A decreasing sequence of real numbers bounded below tends to a limit.

Proof. If $b_1 \geq b_2 \geq b_3 \ldots$ and $b_n \geq B$ then $-b_1 \leq -b_2 \leq -b_3 \ldots$ and $-b_n \leq -B$ so by the fundamental axiom (Axiom 10.2.1) there exists b such that $-b_n \to b$, say, so $b_n = (-1) \cdot (-b_n) \to (-1) \cdot b = -b$. □

10.2.2 The axiom of Archimedes

We start by proving the following results on limits.

Lemma 10.2.3. (i) The limit is unique. That is, if $a_n \to a$ and $a_n \to b$ as $n \to \infty$ then $a = b$.

[1] need link

(ii) If $a_n \to a$ as $n \to \infty$ and $n_1 < n_2 < n_3 \ldots$ then $a_{n_j} \to a$ as $j \to \infty$. (Any subsequence converges to the same limit).

(iii) If $a_n = c$ for all n then $a_n \to c$ as $n \to \infty$.

(iv) If $a_n \to a$ and $b_n \to b$ as $n \to \infty$ then $a_n + b_n \to a + b$.

(v) If $a_n \to a$ and $b_n \to b$ as $n \to \infty$ then $a_n b_n \to ab$.

(vi) If $a_n \to a$ as $n \to \infty$, $a_n \neq 0$ for each n and $a \neq 0$, then $a_n^{-1} \to a^{-1}$.

(vii) If $a_n \leq A$ for each n and $a_n \to a$ as $n \to \infty$ then $a \leq A$.

Proof. (i) $a_n \to a$ means given $\varepsilon > 0$, $\exists N_1$ for all $n \geq N_1$ we have $|a_n - a| < \varepsilon$. Similarly, $a_n \to b$ means given $\varepsilon > 0$, $\exists N_2$ for all $n \geq N_2$ we have $|a_n - b| < \varepsilon$. Thus, we have

$$\underbrace{|a-b| \leq |a-a_n| + |b-a_n|}_{\text{triangle inequality}} < 2\varepsilon \text{ for } n \geq \max\{N_1, N_2\} \tag{10.2.2}$$

Hence we have $|a-b| < 2\varepsilon$. If $a \neq b$, just take $\varepsilon = \frac{|a-b|}{3}$, then $|a-b| < \frac{2|a-b|}{3}$ which is assurd. Thus, $a = b$.

(ii) $a_n \to a$ means given $\varepsilon > 0$, $\exists N$ s.t. $|a_n - a| < \varepsilon, \forall n \geq N$. a_{n_j}, $n_j \geq j$, thus we have

$$|a_{n_j} - a| < \varepsilon, \ \forall j \geq N \ \Rightarrow \ a_{n_j} \to a \ \text{ as } j \to \infty. \tag{10.2.3}$$

(iii) If $a_n = c$ then given $\varepsilon > 0$ set $N(\varepsilon) = 1$. Then

$$|a_n - c| = |c - c| = 0 < \varepsilon, \ \forall n \geq N(\varepsilon). \tag{10.2.4}$$

(iv) We know that given $\varepsilon > 0$, $\exists N_1(\varepsilon), N_2(\varepsilon)$ such that $|a_n - a| < \varepsilon \ \forall n \geq N_1(\varepsilon)$, $|b_n - b| < \varepsilon \ \forall n \geq N_2(\varepsilon)$. Thus if $n \geq N(\varepsilon) = \max\left\{N_1\left(\frac{\varepsilon}{2}\right), N_2\left(\frac{\varepsilon}{2}\right)\right\}$, we have

$$|(a_n + b_n) - (a - b)| = |(a_n - a) + (b_n - b)| \leq |a_n - a| + |b_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \tag{10.2.5}$$

for any $n \geq N(\varepsilon)$.

(v) $a_n \to a$, given $\varepsilon > 0$, $\exists N_1$ s.t. $|a_n - a| < \varepsilon$, $\forall n \geq N_1$. $b_n \to b$, given $\varepsilon > 0$, $\exists N_2$ s.t. $|b_n - b| < \varepsilon, \forall n \geq N_2$.

$$\underbrace{|a_n b_n - ab| \leq |a_n b_n - a_n b| + |a_n b - ab|}_{\text{triangle inequality}} = |a_n||b_n - b| + |b||a_n - a| \tag{10.2.6}$$

We have $|a_n| \leq |a_n - a| + |a| \leq 1 + |a|, \forall n \geq N_1(1)$ $(\varepsilon = 1)$. Thus, we have

$$|a_n b_n - ab| \leq (1 + |a|)\varepsilon + |b|\varepsilon = \varepsilon(|a| + |b| + 1), \ \forall n \geq \max\{N_1(1), N_1(\varepsilon), N_2(\varepsilon)\}. \tag{10.2.7}$$

(vi) Again, given $\varepsilon > 0$, $\exists N_1(\varepsilon)$ such that $|a_n - a| < \varepsilon$. Thus if $n \geq N(\varepsilon) = \max\left\{N_1\left(\frac{|a|}{2}\right), N_1\left(\frac{\varepsilon|a|^2}{2}\right)\right\}$, then

$$\left|\frac{1}{a_n} - \frac{1}{a}\right| = \left|\frac{a - a_n}{a a_n}\right| = \frac{|a - a_n|}{|a||a_n|} < \frac{2|a_n - a|}{|a|^2} < \frac{\varepsilon|a|^2}{2} \cdot \frac{2}{|a|^2} = \varepsilon. \tag{10.2.8}$$

Note: If $n \geq N(\varepsilon)$ then $|a_n - a| < \frac{|a|}{2}$ so $|a_n| > \frac{|a|}{2}$.

(vii) If $a > A$ then set $\varepsilon = \frac{a-A}{2}$. Then

$$a - a_n \geq a - A > \varepsilon, \ \forall n \ \Rightarrow \ a_n \not\to a, \#. \tag{10.2.9}$$

Note that $a_n < A$, $a_n \to a \ \not\Rightarrow \ a < A$, observe $-\frac{1}{n} < 0$ but $-\frac{1}{a_n} \to 0$.

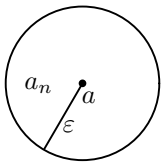
□

If we were considering instead subsequences of complex numbers, $a_n \in \mathbb{C}$, we can give essentially the same definition of limit.

Definition 10.2.2. We say $a_n \to a \in \mathbb{C}$ as $n \to \infty$, if $a_n, a \in \mathbb{C}$ for any n and given $\varepsilon > 0, \exists N$ s.t.

$$|a_n - a| < \varepsilon, \ \forall n \geq N. \tag{10.2.10}$$

where $|\cdot|$ stands for the modulus of a complex number.



Lemma 10.2.4. All properties of Lemma 10.2.3 carry to $\mathbb{C}$ except the last one (we have no order in $\mathbb{C}$).

Proof. [2] □

Theorem 10.2.5 (Axiom of Archimedes)**.** $\frac{1}{n} \to 0$ as $n \to \infty$.

Proof. The sequence $a_n = \frac{1}{n}$ is decreasing and bounded below, so the $a_n \to a \in \mathbb{R}$ by the fundamental axiom.

We claim $a = 0$, thus $\frac{1}{2n} = \frac{1}{2}\frac{1}{n} \to \frac{1}{2}a$ by Lemma 10.2.3.(v). But $\frac{1}{2n}$ is also a subsequence of $\frac{1}{n}$, so by Lemma 10.2.3.(ii), $\frac{1}{2n} \to a$, by uniqueness of the limit (Lemma 10.2.3.(i)), $a = \frac{1}{2}a \ \Rightarrow \ a = 0$. □

Corollary 10.2.6. Given any real number K we can find an integer n with $n > K$.

Proof. Assume we can find a real K that is greater than all numbers. Clearly it is greater than 1.

Thus $0 < \frac{1}{K} \leq \frac{1}{n}$, and thus $\frac{1}{n} \not\to 0$. Contradiction by Axiom of Archimedes (Theorem 10.2.5).

Thus, $\nexists K$ such that $K \geq n, \ \forall n \in \mathbb{Z}$. □

10.2.3 Series and sums

Definition 10.2.3. $a_n \in \mathbb{R}, \mathbb{C}$. We say that $\sum_{j=1}^{\infty} a_j$ converges to S if the sequence of partial sum

$$S_N = \sum_{j=1}^{N} a_j \to S \ \text{ as } N \to \infty. \tag{10.2.11}$$

In that case we write

$$\sum_{j=1}^{\infty} a_j = S. \tag{10.2.12}$$

If S_N does not converge, we say that $\sum_{j=1}^{\infty} a_j$ diverges.

Remark. Any question about series is nearly a question about the sequence of partial sums.

Example 10.2.7. Let $u_n = (-1)^{n+1}$, $S = \sum_{n=1}^{\infty} u_n$. We have two methods

(i) $S = u_1 + \sum_{n=2}^{\infty} u_n = u_1 + \sum_{n=1}^{\infty}(-1)u_n = u_1 - \sum_{n=1}^{\infty} u_n = 1 - S$. So $S = \frac{1}{2}$.

(ii) $S = \sum_{r=1}^{\infty}(u_{2r-1} + u_{2r}) = \sum_{r=1}^{\infty}(1-1) = \sum_{r=1}^{\infty} 0 = 0$.

The above logic is faulty because S does not exist since

$$\sum_{n=1}^{N} u_n = 1 - 1 + \cdots = \begin{cases} 0 & N \text{ is even} \\ 1 & N \text{ is odd} \end{cases} \quad \text{does not converge.} \tag{10.2.13}$$

Lemma 10.2.8. Let $a_n, b_n \in \mathbb{F}$ where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

(i) If $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ converge, then so does $\sum_{j=1}^{\infty}(\lambda a_j + \mu b_j)$ where $\lambda, \mu \in \mathbb{F}$.

(ii) Suppose $\exists N$ s.t. $a_j = b_j, \ \forall j \geq N$, then either $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ both converge or they both diverge. (In other words, initial terms does not matter).

[2] need proof.

Proof. (i) $S_N = \sum_{j=1}^N (\lambda a_j + \mu b_j) = \lambda \sum_{j=1}^N a_j + \mu \sum_{j=1}^N b_j = \lambda c_N + \mu d_N$.

If $c_N \to c$ and $d_N \to d$, then clearly, $S_N \to \lambda c + \mu d$ (by Lemma 10.2.3, 10.2.4).

(ii) Suppose $a_j = b_j$ for $j \geq M$, then $a_j = b_j + c_j$ where $c_j = 0$ for $j \geq M$, so $\sum_{j=1}^N c_j = \sum_{j=1}^M c_j$ for $N \geq M$. Thus, $\sum_{j=1}^N c_j \to \sum_{j=1}^M c_j$ by Lemma 10.2.3, 10.2.4.

So $\sum_{j=1}^\infty c_j$ exists, so if $\sum_{j=1}^\infty b_j$ exists, then $\sum_{j=1}^\infty (b_j + c_j)$ exists, therefore $\sum_{j=1}^\infty a_j$ exists. Otherwise, $\sum_{j=1}^\infty a_j$ does not exist.

□

Lemma 10.2.9. Let $a_n \in \mathbb{R}$ or $\mathbb{C}$. If the series $\sum_{j=1}^n a_j$ converge, then $\lim_{n\to\infty} a_n = 0$.

Proof. $S_n = S_{n-1} + a_n$. If $S_n = \sum_{j=1}^n a_j$ converges, $S_n \to S$. Therefore,

$$a_n = S_n - S_{n-1} \to S - S = 0 \tag{10.2.14}$$

by Lemma 10.2.3, 10.2.4. □

Remark. Converse is not true.

Example 10.2.10. $\sum_{n=1}^\infty \frac{1}{n}$, $a_n = \frac{1}{n} \to 0$, but series diverge. We have

$$S_{2n} = \underbrace{1 + \frac{1}{2} + \cdots + \frac{1}{n}}_{S_n} + \underbrace{\frac{1}{n+1}}_{>\frac{1}{2n}} + \underbrace{\frac{1}{n+2}}_{>\frac{1}{2n}} \cdots + \frac{1}{2n} \;\Rightarrow\; S_{2n} > S_n + \frac{1}{2} \tag{10.2.15}$$

If $\sum_{n=1}^\infty \frac{1}{n}$ converge, then $S_n \to S$, but $S_{2n} > S_n + \frac{1}{2} \;\Rightarrow\; S > S + \frac{1}{2}$, which is absurd.

Example 10.2.11 (Geometric Series)**.** $\sum_{n=0}^\infty x^n$, $S_n = 1 + x + x^2 + \cdots + x^n$, $x \in \mathbb{R}$,

$$xS_n = \underbrace{x + x^2 + \cdots + x^n}_{S_n - 1} + x^{n+1} = S_n - 1 + x^{n+1} \;\Rightarrow\; 1 - x^{n+1} = S_n(1-x). \tag{10.2.16}$$

If $x \neq 1, S_n = \frac{1-x^{n+1}}{1-x} = \frac{1}{1-x} - \frac{x^{n+1}}{1-x}$. (If $x = 1$, the series clearly diverge.)
Applying Lemma 10.2.9, we have

$$\sum_{i=0}^n x^i \text{ converges} \;\Rightarrow\; x^n \to 0 \;\Leftrightarrow\; |x|^n \to 0 \;\Leftrightarrow\; |x| < 1. \tag{10.2.17}$$

Also, we can see that if $|x| < 1$, $S_n \to \frac{1}{1-x} = \sum_{n=0}^\infty x^n$.
Thus, $\sum_{i=0}^n x^i$ converges iff $|x| < 1$.

Theorem 10.2.12 (comparison test)**.** Let $a_n, b_n \in \mathbb{F}$ where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Suppose $0 \leq b_n \leq a_n$, $\forall n$, then if $\sum a_n$ converges, so does $\sum b_n$. ($\sum b_n$ divergent $\Rightarrow \sum a_n$ divergent).

Proof. Let $S_N = \sum_{n=1}^N a_n$, $T_N = \sum_{n=1}^N b_n$. Thus, $S_N = S_{N-1} + a_N \geq S_{N-1}$ ($a_n \geq 0$). So S_N (T_N) is an increasing sequence.

$$\begin{cases} b_n \leq a_n \;\Rightarrow\; T_N \leq S_N \\ \sum_n a_n \text{ converges} \;\Rightarrow\; S_N \to S \end{cases} \Rightarrow T_N \text{ is bounded above} \quad\Rightarrow\quad T_N \text{ has a limit.} \tag{10.2.18}$$

by fundamental axiom of analysis (Axiom 10.2.1). □

Remark. Since initial terms do not matter for convergence in the theorem, it is enough to assume that $0 \leq a_n \leq b_n$, $\forall n \geq N$.

Example 10.2.13. Now look at $\sum_{n=1}^N \frac{x^n}{n^2+3+\sin x}$ for $0 \leq x < 1$.
Since $0 \leq \frac{x^n}{n^2+3+\sin x} \leq x^n, \sum_{n=1}^\infty x^n$ exists, $\Rightarrow \sum_{n=1}^\infty \frac{x^n}{n^2+3+\sin x}$ exists.

We will now derive two applications of the comparison test (root test, ratio test).

Theorem 10.2.14 (root (Cauchy) test)**.** Let $a_n \in \mathbb{R}$. If $a_n \geq 0$, suppose $(a_n)^{\frac{1}{n}} \to a$ as $n \to \infty$, then

$$\begin{cases} \sum a_n \text{ converges} & a < 1 \\ \sum a_n \text{ diverges} & a > 1 \end{cases}$$

Remark. If $a = 1$, the test does not give any information. In fact later on, we will see examples with $a = 1$ which convergent and divergent.

Proof. Suppose $(a_n)^{\frac{1}{n}} \to a$ with $a < 1$. Take r s.t. $a < r < 1$. By the definition of convergence, given $\varepsilon > 0$, $\exists N$ s.t. $\forall n \geq N$,

$$\left|(a_n)^{\frac{1}{n}} - a\right| < \varepsilon \;\Rightarrow\; a - \varepsilon < (a_n)^{\frac{1}{n}} < a + \varepsilon \tag{10.2.19}$$

Take $\varepsilon = r - a$,

$$(a_n)^{\frac{1}{n}} < r,\ \forall n \geq N \;\Rightarrow\; a_n < r^n,\ \forall n \geq N \;\Rightarrow\; \sum a_n < \sum r^n. \tag{10.2.20}$$

Since the geometric series r converges ($r < 1$). The comparison test gives us right away that $\sum a_n$ converges.

Suppose now $(a_n)^{\frac{1}{n}} \to a$ with $a > 1$. By the definition of limit, $\exists N$ s.t. $(a_n)^{\frac{1}{n}} > 1$, $\forall n \geq N$. Thus, $a_n > 1$, $\forall n \geq N$, in particular a_n does not tend to zero. By Lemma 10.2.9, $\sum a_n$ diverges. □

Example 10.2.15. $\sum_{n=2}^{\infty} \left(\frac{1}{\log n}\right)^n$.

$$a_n = \left(\frac{1}{\log n}\right)^n \;\Rightarrow\; (a_n)^{\frac{1}{n}} = \frac{1}{\log n} \to 0 \text{ as } n \to \infty. \tag{10.2.21}$$

Thus, $a = 0 < 1$, $\sum_{n=2}^{\infty} \left(\frac{1}{\log n}\right)^n$ converges by the root test.

Theorem 10.2.16 (ratio test)**.** Suppose $a_n > 0$, and $\frac{a_{n+1}}{a_n} \to l$ as $n \to \infty$.

$$\begin{cases} \sum a_n \text{ converges} & l < 1 \\ \sum a_n \text{ diverges} & l > 1 \end{cases} \tag{10.2.22}$$

Remark. the test is inclusive if $l = 1$.

Proof. Suppose $\frac{a_{n+1}}{a_n} \to l$ with $l < 1$. Take r s.t. $l < r < 1$. By the definition of convergence, given $\varepsilon > 0$, $\exists N$ s.t. $\forall n \geq N$,

$$\left|\frac{a_{n+1}}{a_n} - l\right| < \varepsilon \;\Rightarrow\; l - \varepsilon < \frac{a_{n+1}}{a_n} < l + \varepsilon. \tag{10.2.23}$$

Take $\varepsilon = r - l$, thus $\forall n \geq N$

$$\begin{cases} \frac{a_{n+1}}{a_n} < r \\ a_n = \frac{a_n}{a_{n-1}} \cdot \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_{N+1}}{a_N} \cdot a_N \end{cases} \quad \Rightarrow\; a_n < a_N r^{n-N}$$

In other words, there is a constant K (independent of n) s.t. $a_n < Kr^{n-N}$, $\forall n \geq N$. Since $r < 1$, the series $\sum Kr^n$ converges and $\sum a_n$ also converges by the comparison test.

Suppose now $\frac{a_{n+1}}{a_n} \to l$ with $l > 1$. By the definition of limit, $\exists N$ s.t. $\frac{a_{n+1}}{a_n} > 1$, $\forall n \geq N$. This is saying that sequence a_n increases after N. In particular, $a_n > a_N$, $\forall n \geq N$, which is saying a_n does not tend to zero. By Lemma 10.2.9, $\sum a_n$ diverges. □

Example 10.2.17. $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

(i) root test: $\left(\frac{1}{n}\right)^{1/n} \to 1$ because $n^{1/n} \to 1$. We have

$$n^{1/n} = 1 + \delta_n,\ \delta_n > 0 \;\Rightarrow\; n = (1+\delta_n)^n > \binom{n}{2}\delta_n^2 = \frac{n(n-1)\delta_n^2}{2} \;\Rightarrow\; \delta_n < \sqrt{\frac{2}{n-1}} \to 0 \text{ as } n \to \infty \tag{10.2.24}$$

(ii) ratio test: $\frac{n}{n+1} \to 1$.

Thus, $a = l = 1$.

Example 10.2.18. $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges.

(i) root test: $\left(\frac{1}{n^2}\right)^{1/n} = \left(\frac{1}{n^{1/n}}\right)^2 \to 1$.

(ii) ratio test: $\frac{n^2}{(n+1)^2} \to 1$.

For this series it also holds that $a = l = 1$. However, we have

$$\sum_{n=1}^{N} \frac{1}{n^2} < 1 + \sum_{n=2}^{N} \frac{1}{n(n-1)} = 1 + 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{N-1} - \frac{1}{N} = 2 - \frac{1}{N} \to 2 \text{ as } N \to \infty. \tag{10.2.25}$$

Thus, the series $\sum_{n=2}^{\infty} \frac{1}{n(n-1)}$ converges, and by comparison $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges. This shows that for $a = 1$ in root test or $l = 1$ in ratio test, we can not conclude anything.

Example 10.2.19. $\sum_{n=1}^{\infty} \frac{n^x}{2^n}, x \in \mathbb{R}$ converges. Ratio test:

$$\frac{a_{n+1}}{a_n} = \frac{(n+1)^x}{2^{n+1}} \cdot \frac{2^n}{n^x} = \frac{1}{2}\left(\frac{n+1}{n}\right)^x \to \frac{1}{2} < 1. \tag{10.2.26}$$

We conclude from the ratio test that the series converges.

Theorem 10.2.20 (Cauchy's condensation test)**.** a_n is a decreasing sequence of positive terms, then $\sum_{n=1}^{\infty} a_n$ converges iff $\sum_{n=1}^{\infty} 2^n a_{2^n}$ converges.

Proof. We have $a_{2^k} \le a_{2^{k-1}+i} \le a_{2^{k-1}},\ 1 \le i \le 2^{k-1} (k \ge 1)$ since a_n is decreasing.

Suppose first that $\sum a_n$ converges. We have

$$2^{n-1} a_{2^n} = \underbrace{a_{2^n} + a_{2^n} + \cdots + a_{2^n}}_{2^{n-1} \text{ terms}} \le a_{2^{n-1}+1} + a_{2^{n-1}+2} + \cdots + a_{2^n} \Rightarrow\ 2^{n-1} a_{2^n} \le \sum_{m=2^{n-1}+1}^{2^n} a_m \tag{10.2.27}$$

$$\Rightarrow\ \sum_{n=1}^{N} 2^{n-1} a_{2^n} \le \sum_{n=1}^{N} \sum_{m=2^{n-1}+1}^{2^n} a_m = \sum_{m=2}^{2^N} a_m\ \Rightarrow\ \sum_{n=1}^{N} 2^n a_{2^n} \le 2 \sum_{m=2}^{2^N} a_m \le 2A \tag{10.2.28}$$

since $\sum a_n$ converges. So this (increasing) sequence of partial sum is bounded above, which implies $\sum_{n=1}^{\infty} 2^n a_{2^n}$ converges.

Suppose now conversely that $\sum_{n=1}^{\infty} 2^n a_{2^n}$ converges. Then

$$\sum_{m=2^{n-1}+1}^{2^n} a_m = a_{2^{n-1}+1} + a_{2^{n-1}+2} + \cdots + a_{2^n} \le a_{2^{n-1}} + a_{2^{n-1}} + \cdots + a_{2^{n-1}} = 2^{n-1} a_{2^{n-1}} \tag{10.2.29}$$

$$\Rightarrow\ \sum_{m=2^{n-1}+1}^{2^n} a_m \le 2^{n-1} a_{2^{n-1}}\ \Rightarrow\ \sum_{n=1}^{N} \sum_{m=2^{n-1}+1}^{2^n} a_m \le \sum_{n=1}^{N} 2^{n-1} a_{2^{n-1}}\ \Rightarrow\ \sum_{m=2}^{2^N} a_m \le \sum_{n=1}^{N} 2^{n-1} a_{2^{n-1}} \le B. \tag{10.2.30}$$

since $\sum 2^n a_{2^n}$ converges. So this (increasing) sequence $\sum_{m=2}^{2^N} a_m$ is bounded above in N, which implies $\sum_{n=1}^{\infty} a_n$ converges. □

Example 10.2.21. $\sum_{n=1}^{\infty} \frac{1}{n^k},\ k > 0$. (if $k \le 0$, $\frac{1}{n^k}$ does not tend to zero.)

$a_n = \frac{1}{n^k}$ is decreasing. Let's look at $\sum 2^n a_{2^n}$. We have

$$2^n a_{2^n} = 2^n \frac{1}{2^{nk}} = 2^{n(1-k)} = \left(2^{1-k}\right)^n = r^n \quad \text{(geometric series)} \tag{10.2.31}$$

Thus, $\sum 2^n a_{2^n}$ converges iff $2^{1-k} < 1 \ \Leftrightarrow\ k > 1$. By the condensation test (Theorem 10.2.20), $\sum_{n=1}^{\infty} \frac{1}{n^k}$ converges iff $k > 1$.

Theorem 10.2.22 (alternating series test)**.** $a_1 \ge a_2 \ge \cdots \ge 0$ and $a_n \to 0$, then $\sum_{n=1}^{\infty} (-1)^{n+1} a_n$ converges.

Proof. We have $S_n = a_1 - a_2 + \cdots + (-1)^{n+1} a_n$. Also,

$$\begin{cases} S_{2n} = (a_1 - a_2) + (a_3 - a_4) + \cdots + \underbrace{(a_{2n-1} - a_{2n})}_{\ge 0 (a_n \text{ decreasing})} \ge S_{2n-2} \\ S_{2n} = a_1 - (a_2 - a_3) - (a_4 - a_5) - \cdots - (a_{2n-2} - a_{2n-1}) - a_{2n} \le a_1. \end{cases} \tag{10.2.32}$$

S_{2n} is an increasing series bounded above. Now by the fundamental axiom, we have $S_{2n} \to S$. We know

$$S_{2n+1} = S_{2n} + a_{2n+1} \;\Rightarrow\; S_{2n+1} \to S + 0 = S, \quad (a_n \to 0). \tag{10.2.33}$$

By the definition of convergence. $S_{2n} \to S$ means given $\varepsilon > 0$, $\exists N_1, N_2$ $\forall n_1 \geq N_1, n_2 \geq N_2$

$$|S_{2n_1} - S| < \varepsilon, \qquad |S_{2n_2+1} - S| < \varepsilon. \tag{10.2.34}$$

Thus, we take $N_3 = \max\{2N_1, 2N_2 + 1\}$, then $\forall n \geq N_3$, we have $|S_n - S| < \varepsilon$. □

Example 10.2.23. $\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$ converges.

We have $a_n = \frac{1}{n} \to 0$ and a_n is decreasing. Therefore, the series converges.

10.2.4 Absolute convergence

Definition 10.2.4. Take $a_n \in \mathbb{R}, \mathbb{C}$. If $\sum |a_n|$ is convergent, then the series is called absolutely convergent.

Theorem 10.2.24. If $\sum a_n$ is absolutely convergent, then it is convergent.

Proof. Suppose first $a_n \in \mathbb{R}$. Introduce

$$u_n = \frac{|a_n| + a_n}{2}, \quad v_n = \frac{|a_n| - a_n}{2} \tag{10.2.35}$$

where $u_n, v_n \geq 0$ and $a_n = u_n - v_n, |a_n| = u_n + v_n \geq u_n, v_n$. By the comparison test and Lemma 10.2.3 (iv), we have

$$\sum |a_n| \text{ converges } \;\Rightarrow\; \sum u_n,\ \sum v_n \text{ converges } \;\Rightarrow\; \sum a_n \text{ converges }. \tag{10.2.36}$$

If $a_n \in \mathbb{C}$, we set $a_n = x_n + iy_n$ where $x_n, y_n \in \mathbb{R}$. By comparision test, we have

$$\begin{cases} |x_n|, |y_n| \leq |a_n| = \sqrt{x_n^2 + y_n^2} \\ \sum |a_n| \text{ converges} \end{cases} \Rightarrow \sum |x_n|,\ \sum |y_n| \text{ converges } \xrightarrow{x_n, y_n \in \mathbb{R}} \sum x_n,\ \sum y_n \text{ converges.} \tag{10.2.37}$$

Since $a_n = x_n + iy_n$, we have $\sum a_n$ converges by Lemma 10.2.3.(iv). □

Example 10.2.25. The series $\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$ is convergent, but not absolutely convergent.

Definition 10.2.5. If $\sum a_n$ converges, but $\sum |a_n|$ does not converge. We say that the series is conditionally convergent.

Theorem 10.2.26. If $\sum a_n$ is absolutely convergent, then any series consisting of the same terms in any order (a rearrangement) has the same sum.

Proof. We will prove it for $a_n \in \mathbb{R}$ and leave the extension to $\mathbb{C}$ as an exercise.

Let $\sum a'_n$ be a rearrangement of $\sum a_n$ and $S_n = \sum_{i=1}^{n} a_i$, $S = \sum_{i=1}^{\infty} a_i$, $T_n = \sum_{i=1}^{n} a'_i$. Suppose fixed $a_n \geq 0$, then given n, $\exists m$ s.t. S_m contains every term in T_n, thus $T_n \leq S_m \leq S$, $(a_n \geq 0)$. By the fundamental axiom, $T_n \to T \leq S$. By symmetry, we have $S \leq T \;\Rightarrow\; S = T$.

If a_n has any sign, consider u_n and v_n from the proof of Theorem 10.2.24 and $\sum a'_n$, $\sum u'_n$, $\sum v'_n$. Since $\sum |a_n|$ converges, both $\sum u_n$ and $\sum v_n$ converge. With the fact that $u_n, v_n \geq 0$, we have $\sum u_n$ $(\sum v_n)$ and $\sum u'_n$ $(\sum v'_n)$ converge to the same limit.

Hence $a_n = u_n - v_n$ and $a'_n = u'_n - v'_n$ converge to the same limit. □

Example 10.2.27. Rearrangement cases with the different limits.

$S_n = \sum \frac{(-1)^{n+1}}{n} \to 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log(1+1) = \log 2$ (not absolutely convergent).

$T_n = \sum \left(\frac{1}{4n-3} + \frac{1}{4n-1} - \frac{1}{2n} \right) \to \left(1 + \frac{1}{3} - \frac{1}{2}\right) + \left(\frac{1}{5} + \frac{1}{7} - \frac{1}{4}\right) + \ldots$ (absolutely convergent), which is a rearrangement of $\frac{(-1)^{n+1}}{n}$. However, we have

$$\begin{aligned} T_n &= \sum \left(\frac{1}{4n-3} + \frac{1}{4n-1} - \frac{1}{4n-2} - \frac{1}{4n} \right) + \sum \left(\frac{1}{4n-2} + \frac{1}{4n} - \frac{1}{2n} \right) \\ &= \sum \frac{(-1)^{n+1}}{n} + \sum \left(\frac{1}{4n-2} - \frac{1}{4n} \right) = \sum \frac{(-1)^{n+1}}{n} + \frac{1}{2} \sum \left(\frac{1}{2n-1} - \frac{1}{2n} \right) \\ &= \sum \frac{(-1)^{n+1}}{n} + \frac{1}{2} \sum \frac{(-1)^{n+1}}{n} = \frac{3}{2} \sum \frac{(-1)^{n+1}}{n} = \frac{3}{2} \log 2. \end{aligned}$$

10.2.5 Least upper bounds and greatest lower bounds

Theorem 10.2.28. A non-empty bounded set in $\mathbb{R}$ need not have a maximum.

Example 10.2.29. The set $E = \{-1/n : n \geq 1\}$ is non-empty and any $e \in E$ satisfies the inequalities $-1 \leq e \leq 0$ but E has no largest member.

If $x \leq 0$ then $\exists n$ such that $-x > \frac{1}{n} > 0$ so $-\frac{1}{n} > x$ and x is not a maximum.

If $x \geq 0$ then $x \notin E$.

Thus E contains no largest member.

However, as we shall see every non-empty bounded set in $\mathbb{R}$ has a least upper bound (or supremum).

Definition 10.2.6. Let E be a non-empty set in $\mathbb{R}$. We say that α is a least upper bound for E if

(i) $\alpha \geq e$ for all $e \in E$ (that is, α is an upper bound for E).

(ii) If $\beta \geq e$ for all $e \in E$ then $\beta \geq \alpha$ (that is, α is the least such upper bound).

If E has a supremum α we write $\sup_{e \in E} e = \sup E = \alpha$.

Lemma 10.2.30. If the least upper bound exists it is unique.

Proof. Suppose E is a non-empty subset of $\mathbb{R}$ and α, α' are least upper bounds for E. Then since α' is an upper bound, and α is a least upper bound $\alpha \leq \alpha'$. Similarly $\alpha' \leq \alpha$ and so $\alpha' = \alpha$ □

The following remark is trivial but sometimes helpful.

Lemma 10.2.31. Let E be a non-empty set in $\mathbb{R}$. Then α is a least upper bound for E if and only if we can find $e_n \in E$ with $e_n \to \alpha$ and b_n such that $b_n \geq e$ for all $e \in E$ and $b_n \to \alpha$ as $n \to \infty$.

Proof. First show that α is an upper bound.

If $e \in E$ then $b_n \geq e$. But $b_n \to \alpha$ so $\alpha \geq e$.

Then show α is the least upper bound i.e. if β is an upper bound $\beta \geq \alpha$

If β is an upper bound then, in particular, $\beta \geq e_n$, but $e_n \to \alpha$ so $\beta \geq \alpha$. □

Here is the promised result.

Theorem 10.2.32. Any non-empty set in $\mathbb{R}$ with an upper bound has a least upper bound.

Proof. Let E be such a set. Since E is non-empty, we can find $a_0 \in E$. Observe that $\exists e \in E$ such that $e \geq a_0$ (e.g. a_0 itself). Since E is bounded, we can find b_0 such that $b_0 \geq e \ \forall e \in E$. Set $c_0 = \frac{a_0 + b_0}{2}$. There are two cases

(i) $\exists e \in E$ such that $e \geq c_0$ and we put $a_1 = c_0, b_1 = b_0$.

(ii) $\forall e \in E \ c_0 > e$ and we put $a_1 = a_0, b_1 = c_0$.

Observe that $a_0 \leq a_1 \leq b_1 \leq b_0$, $b_1 - a_1 = \frac{b_0 - a_0}{2^1}$ and

(i) $\exists e_1 \in E$ such that $e_1 \geq a_1$.

(ii) $b_1 \geq e \ \forall e \in E$

Repeating we obtain $a_0 \leq a_1 \leq \ldots \leq a_n \leq b_n \leq \ldots \leq b_1 \leq b_0$, $b_n - a_n = \frac{b_0 - a_0}{2^n}$ and

(i) $\exists e_n \in E$ such that $e_n \geq a_1$.

(ii) $b_n \geq e \ \forall e \in E$.

The a_ns form an increasing sequence bounded above, so $a_n \to \alpha$ by the fundamental axiom of analysis (Axiom 10.2.1), $b_n = a_n + (b_n + a_n) = a_n + 2^{-n}(b_0 - a_0) \to \alpha + 0 = \alpha$ so $a_n \leq e_n \leq b_n$ with all the $e_n \in E$, so $e_n \to \alpha$ and $b_n \geq e \ \forall e \in E$ so α is the least upper bound of E. □

We observe that this result is actually equivalent to the fundamental axiom.

Theorem 10.2.33. Theorem 10.2.32 implies the fundamental axiom of analysis (Axiom 10.2.1).

Proof. On the assumption that every bounded non-empty set has a least upper bound, suppose $a_1 \leq a_2 \leq \ldots \leq a_n \leq A_0 \forall n$

Set $A = \{a_1, a_2, \ldots\}$ is non-empty and bounded, so it has a supremum which we call α. Given $\epsilon > 0$ we know $\alpha - \epsilon$ is not an upper bound, so $\exists N$ such that $a_N > \alpha - \epsilon$. Now if $n \geq N, \alpha \geq a_n \geq a_N \geq \alpha - \epsilon$, so $|a_n - \alpha| < \epsilon$ and $a_n \to \alpha$. □

Of course we have the notion of a greatest lower bound or infimum.

Definition 10.2.7. [3].

If E has an infimum β we write $\inf_{e \in E} e = \inf E = \beta$. One way of dealing with the infimum is to use the following observation.

Lemma 10.2.34. Let E be a non-empty set in $\mathbb{R}$ and write $-E = \{-e : e \in E\}$. Then E has an infimum if and only if $-E$ has a supremum. If E has an infimum $\inf E = -\sup(-E)$.

Proof. If $-E$ has a supremum α,

(i) $\alpha \geq -e \ \forall e \in E$.

(ii) If $\beta \geq -e \ \forall e \in E$ then $\beta \geq \alpha$

Thus,

(i)' $-a \leq e \ \forall e \in E$.

(ii)' If $-\beta \leq e \ \forall e \in E$ then $-\beta \leq -\alpha$.

So $-\alpha$ is the infimum of E. □

Theorem 10.2.35. Any non-empty set in $\mathbb{R}$ with a lower bound has a greatest lower bound.

Proof. [4] □

10.2.6 Bolzano-Weierstrass theorem

Theorem 10.2.36 (Bolzano-Weierstrass theorem)**.** If $x_n \in \mathbb{R}$ and there exists K s.t. $|x_n| < K, \forall n$, then we can find $n_1 < n_2 < \ldots$ and $x \in \mathbb{R}$ s.t. $x_{n_j} \to x$ as $j \to \infty$. (every bounded sequence has a convergent subsequence.)

Remark. We say nothing about uniqueness of x. i.e. $x_n = (-1)^n \ \Rightarrow \ x_{2n-1} = -1, x_{2n} = 1$.

Proof. We see $[a_n, b_n] = [-K, K]$, let $c = \frac{a_0 + b_0}{2}$ (mid-point), thus, either

(i) $x_n \in [a_0, c]$ for infinitely many values of n;

(ii) $x_n \in [c, b_0]$ for infinitely many values of n.

In case (i), set $a_1 = a_0, b_1 = c$; In case (ii), set $a_1 = c, b_1 = b_0$.

Proceed inductively to obtain sequences a_n and b_n s.t. the following holds ($m \leq n$)

(i) $a_m \leq a_n \leq b_n \leq b_m$; ($a_n$ is a bounded increasing sequence, b_n is a bounded decreasing sequence.)

(ii) $x_m \in [a_n, b_n]$ for infinitely many values of m;

(iii) $b_n - a_n = \frac{b_{n-1} - a_{n-1}}{2}$.

By the Fundamental Axiom, $a_n \to a$ and $b_n \to b$. By property (iii) passing to the limit,

$$b - a = \frac{b - a}{2} \ \Rightarrow \ a = b$$

Having selecting n_j s.t. $x_{n_j} \in [a_j, b_j]$, select $n_{j+1} > n_j$ s.t. $x_{n_{j+1}} \in [a_{j+1}, b_{j+1}]$, we can always do this because $x_m \in [a_{j+1}, b_{j+1}]$ for infinitely many values of m. In other words,

$$\begin{cases} a_j \leq x_{n_j} \leq b_j, \forall j \\ a_j \to a, \ b_j \to b = a \end{cases} \Rightarrow \ x_{n_j} \to a.$$

□

[3] Define the greatest lower bound in the manner of Definition, prove its uniqueness in the manner of Lemma 10.2.30 and state and prove a result corresponding to Lemma 10.2.31

[4] need details. Use Lemma 10.2.34 and Theorem 10.2.32.

Remark. This argument (or method) is called bijection method or 'lion hunting'.

Theorem 10.2.37. Bolzano-Weierstrass theorem implies the fundamental axiom of analysis.

Proof. Suppose $a_1 \leq a_2 \leq \ldots$ and $a_n \leq A$. Then $\{a_j\}$ is a bounded sequence so by Bolzano-Weierstrass it has a convergent subset i.e. $\exists n(1) < n(2) < \ldots$ such that $a_{n(k)} \to \alpha$.

Since $a_{n(k)} \leq a_j \ \forall j \geq n(k)$ we have $\alpha \geq a_n(k) \ \forall k$ so $\alpha \geq a_j \ \forall j$.

Now given $\epsilon > 0$ $\exists n(k)$ such that $|\alpha - a_{n(k)}| < \epsilon$ so $\alpha \geq a_j \geq a_{n(k)} \ \forall j \geq n(k)$, so $|\alpha - a_j| < \epsilon \ \forall j \geq n(k)$ and thus $a_j \to \alpha$. □

Then combining Theorem 10.2.33, 10.2.37, we have

Theorem 10.2.38. Bolzano- Weierstrass ⇔ Fundamental Axiom of analysis ⇔ A bounded non-empty set has a supremum.

10.2.7 Cauchy sequences

Definition 10.2.8 (Cauchy sequence)**.** We say that a sequence $a_n \in \mathbb{R}$ is a Cauchy sequence if given $\varepsilon > 0$, $\exists N(= N(\varepsilon))$ s.t. for any $n, m \geq N$,

$$|a_m - a_n| < \varepsilon.$$

Lemma 10.2.39. A convergent sequence is a Cauchy sequence.

Proof. $a_n \in \mathbb{R},\ a_n \to a$ means that given $\frac{\varepsilon}{2} > 0$, $\exists N$ s.t. $\forall n \geq N$, $|a_n - a| < \frac{\varepsilon}{2}$. Thus,

$$|a_m - a_n| \leq |a_m - a| + |a_n - a|$$

so if $m, n \geq N$, we have $|a_m - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. □

As an application of the Bolzano-Weiastrass theorem, we now show that the converse is true.

Theorem 10.2.40. A Cauchy sequence in $\mathbb{R}$ is convergent.

Proof. First, we prove that if a_n is a cauchy sequence, then it is bounded.

a_n is cauchy means that given $\varepsilon > 0$, $\exists N$ s.t. $\forall m, n \geq N$, $|a_n - a_m| < \varepsilon$. Chose $\varepsilon = 1$, we have

$$|a_n - a_m| < 1,\ \forall m, n \geq N(1) \tag{10.2.38}$$

in particular, $m = N(1)$,

$$|a_n - a_N| < 1,\ \forall n \geq N(1) \ \Rightarrow\ |a_n| \leq |a_n - a_N| + |a_N| \leq 1 + |a_N|,\ \forall n \geq N(1) \tag{10.2.39}$$

Take $K = \max\{1 + |a_N|, |a_i|, i = 1, 2, \ldots, N-1\}$. For this choice of K, $|a_n| \leq K,\ \forall n$. Now, by the Bolzano-Weiastrass theorem, a_n has a convergent subsequence $a_{n_j} \to a$.

Second, we show that in fact $a_n \to a$. We have

$$|a_n - a| \leq |a_n - a_{n_j}| + |a_{n_j} - a| \tag{10.2.40}$$

Choose n_j large enough such that

$$\begin{cases} \text{Cauchy}: & |a_n - a_{n_j}| < \frac{\varepsilon}{2}, \forall n \geq N\left(\frac{\varepsilon}{2}\right) \left(\Rightarrow\ n_j \geq N\left(\frac{\varepsilon}{2}\right)\right) \\ a_{n_j} \to a: & |a_{n_j} - a| < \frac{\varepsilon}{2} \end{cases} \Rightarrow\ |a_n - a| < \varepsilon, \forall n \geq N\left(\frac{\varepsilon}{2}\right) \tag{10.2.41}$$

□

Definition 10.2.9 (general principle of convergence)**.** For sequence of real numbers, convergence and Cauchy property are equivalent. This is called the general principle of convergence.

Alternative proof of Theorem 10.2.24. There is an alternative 'quick' proof of this using Cauchy sequences. With $S_n = \sum_{i=1}^{n} a_i,\ T_n = \sum_{i=1}^{n} |a_i|$ and $m \geq 0$, we have $\exists N$ such that

$$|S_{n+m} - S_n| = |\sum_{i=n+1}^{n+m} a_i| \leq \sum_{i=n+1}^{n+m} |a_n| = T_{n+m} - T_n < \varepsilon,\ \forall n \geq N \tag{10.2.42}$$

since T_n is Cauchy sequence $\Leftrightarrow$ T_n converges. Hence, S_n is Cauchy, which implies that S_n converges. □

10.3 Continuity

10.3.1 Definitions

Define a function $f : E \mapsto \mathbb{C}$, $E \subset \mathbb{C}$ is non-empty subset. (also applies of course $f : E \subset \mathbb{R} \to \mathbb{R}$). Usually E will be some intervals.

Definition 10.3.1. $a \in E$. We say f is continuous at a if given any sequence $z_n \in E$ s.t. $z_n \to a$, then $f(z_n) \to f(a)$.

Definition 10.3.2. $a \in E$. We say f is continuous at a if given $\varepsilon > 0$, then $\exists \delta > 0$, s.t. if $z \in E$ and $|z - a| < \delta$, then $|f(z) - f(a)| < \varepsilon$.

We now prove that Definition 10.3.1 $\Leftrightarrow$ Definition 10.3.2.

Proof. Definition 10.3.2 $\Rightarrow$ Definition 10.3.1:

We know tha given $\varepsilon > 0$, $\exists \delta > 0$ s.t. for $z_n \in E$ and $|z_n - a| < \delta$, then $|f(z_n) - f(a)| < \varepsilon$. Since $z_n \to a$, $\exists N$ s.t. $\forall n \geq N$, $|z_n - a| < \delta$. Thus, $|f(z_n) - f(a)| < \varepsilon, \forall \varepsilon > 0$ implies $f(z_n) \to f(a)$.

Definition 10.3.1 $\Rightarrow$ Definition 10.3.2:

Suppose Definition 10.3.2 is not true, $\exists \varepsilon > 0$ s.t. $\forall \delta > 0$ we can find $z \in E$ with $|z - a| < \delta$ and $|f(z) - f(a)| \geq \varepsilon$. Choose $\delta_n = \frac{1}{n}$, thus we can find $z_n \in E$ with $|z_n - a| < \frac{1}{n}$ (which implies $z_n \to a$) and $|f(z_n) - f(a)| \geq \varepsilon$. So $f(z_n)$ does not tend to $f(a)$, which contradicts Defintion 10.3.1. □

Example 10.3.1. We check function $f : \mathbb{R} \mapsto \mathbb{R}$,

$$f(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{10.3.1}$$

Thus, $f(0) = 1$ is not continuous at 0 since $-\frac{1}{n} \to 0,\ f\left(-\frac{1}{n}\right) = 0 \nrightarrow 1$.

Definition 10.3.3. We say that f is continuous on E if it is continuous at any point in E.

Proposition 10.3.2. $f, g : E \mapsto \mathbb{C}$ and $a \in E$ f and g are continuous at a, then for any constant λ

$$\text{(i) } f(z) + g(z), \qquad \text{(ii) } f(z)g(z), \qquad \text{(iii) } \lambda f(z) \tag{10.3.2}$$

are also continuous at a. In addition, (iv) if $f(z) \neq 0, \forall z \in E$, then $\frac{1}{f}$ is also continuous at a.

Remark. It is also trivial that $f(x) = c$ for all $x \in E$, then f is continuous on E.

Proof. This is a direct consequence of Definition 10.3.1 and Lemma 10.2.3 (about sequences). For example, to show that $f(z)+g(z)$ is continuous at a, we take $z_n \in E$ s.t. $z_n \to a$. Since f and g are continuous at a, $f(z_n) \to f(a)$ and $g(z_n) \to g(a)$. Then use Lemma 10.2.3, $f(z_n) + g(z_n) \to f(a) + g(a)$. That is, $f + g$ continuous at a.

Similarly with the other claims.[5] □

Example 10.3.3. (i) Quotent ploynomials (rational functions) are continuous at every point where the denominator does not vanish (by Proposition 10.3.2).

(ii) $f(z) = z$ is clearly continuous. By Proposition 10.3.2, any ploynomial is continuous at every point of $\mathbb{C}$.

[5] need details.

Theorem 10.3.4. Let $f : A \mapsto \mathbb{C}$ and $g : B \mapsto \mathbb{C}$ be two functions s.t. $f(A) \subset B$ (A and B are subsets of $\mathbb{C}$). Suppose f is continuous at $a \in A$ and g is continuous at $f(a)$, thus $g \circ f : A \mapsto \mathbb{C}$ is continuous at a.

Proof. Take $z_n \in A$ with $z_n \to a$, we need to show $g(f(z_n)) \to g(f(a))$.

Since f is continuous at a, $f(z_n) \to f(a)$. Call $y_n = f(z_n)$ and since g is continuous at $f(a)$, $g(y_n) \to g(f(a))$. □

Remark. Of course, one can prove this with Definition 10.3.2.

Example 10.3.5. (i) Assume $\sin x$ is continuous

$$f(x) = \begin{cases} \sin\left(\frac{1}{x}\right) & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{10.3.3}$$

At $x \neq 0$, $f(x)$ is continuous by Proposition 10.3.2 and Theorem 10.3.4.

However, f is not continuous at 0. Take $x_n = \frac{1}{\left(2n+\frac{1}{2}\right)\pi} \to 0$ and $f(x_n) = 1 \neq 0 = f(0)$.

(ii) We know $\sin\left(\frac{1}{x}\right) \leq 1$.

$$f(x) = \begin{cases} x\sin\left(\frac{1}{x}\right) & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{10.3.4}$$

For $x \neq 0$, $f(x)$ is continuous. Let $x_n \to 0$, so

$$|f(x_n) - f(0)| \leq |f(x_n)| \leq |x_n| \to 0 \ \Rightarrow f(x_n) \to 0 = f(0) \tag{10.3.5}$$

So the function is continuous at 0.

10.3.2 Limits of functions

Assume $f : E \subset \mathbb{C} \mapsto \mathbb{C}$, we would like to make sense $\lim_{z\to a} f(z)$ in case in which a may not be in E. For example, $\lim_{z\to 0} \frac{\sin z}{z}$.

Definition 10.3.4. $E \subset \mathbb{C}, f : E \mapsto \mathbb{C}$. Take $a \in \mathbb{C}$ and assume that there exist a sequence $z_n \in E$, $z_n \neq a$, $z_n \to a$. (Note: the point a may be in E, but need not be in E)

We say that $\lim_{z\to a} f(z) = l$ (or $f(z) \to l$ as $z \to a$) if given $\varepsilon > 0$, $\exists \delta > 0$ s.t. whenever $z \in E$ and $0 < |z - a| < \delta$, then $|f(z) - l| < \varepsilon$.

Remark. (i) $\lim_{z\to a} f(z) = l$ iff for every sequence, $z_n \in E$, $z_n \neq a$, $z_n \to a$, then $f(z) \to l$. (Proof of this is exactly as the proof of Definition 10.3.1 $\Leftrightarrow$ Definition 10.3.2).

(ii) If $a \in E$ then $\lim_{z\to a} f(z) = f(a)$ iff f is continuous at a. (Nothing to prove really: straight from the definitions).

The limit enjoys the properties which one would expect

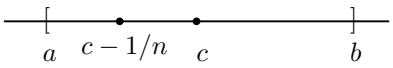
(i) The limit is unique.

(ii) If $f(z) \to A$ as $z \to a$ and $g(z) \to B$ as $z \to a$, then

$$\begin{aligned} f(z) + g(z) &\to A + B \\ f(z)g(z) &\to AB \\ f(z)/g(z) &\to A/B \text{ if } B \neq 0 \end{aligned}$$

Theorem 10.3.6 (intermediate value theorem)**.** $f : [a, b] \mapsto \mathbb{R}$ continuous, and $f(a) \neq f(b)$, then f takes every value which lies between $f(a)$ and $f(b)$.

Proof. Without loss of generality, we assume $f(a) < f(b)$. Take $f(a) < \eta < f(b)$, $\forall \eta$ and $S = \{x \in [a, b] : f(x) < \eta\}$. $S \neq \emptyset$ because $a \in S$ and S is bounded above (by b in fact). Thus S has a supremum c, we need to prove $f(c) = \eta$.



Given n a positive integer, $c-1/n$ is not an upper bound for S (otherwise it would contradict the definition of supremum (least upper bound)). Then $\exists x_n \in S$ s.t. $x_n > c-1/n$.

Thus, $c-1/n < x_n \le c \;\Rightarrow\; x_n \to c$ as $n \to \infty$. By continuity of f, $f(x_n) \to f(c)$. Since $x_n \in S \;\Rightarrow\; f(x_n) < \eta$, we have $f(c) \le \eta$.

Note $c \neq b$, otherwise $f(c) = f(b) < \eta$ but $\eta < f(b)$. Thus, $\forall n$ sufficiently large, $c+1/n \in [a,b]$ and $c+1/n \to c$. Again by continuity of f, $f(c+1/n) \to f(c)$. Since $c+1/n > c \;\Rightarrow\; c+1/n \notin S$, $f(c+1/n) \ge \eta$. Thus, $f(c) \ge \eta$. So we $f(c) = \eta$. □

Example 10.3.7. Existence of N-root of a positive number η (N is positive integer).

Look at $f(x) = x^N,\ x \ge 0$. f is continuous, look at f in $[0, 1+\eta]$. We have

$$0 = f(0) < \eta < f(1+\eta) = (1+\eta)^N \tag{10.3.6}$$

By the intermediate value theorem, $\exists c \in (0, 1+\eta)$ s.t. $f(c) = \eta \;\Leftrightarrow\; c^N = \eta$. This is exactly that η has a positive N-root. In fact this N-root is unique. If d is another positive N-root with $d \neq c$. Without loss of generalities $d < c$, we have

$$d^N < c^N \;\Leftrightarrow\; \eta < \eta \text{ (absurd).} \tag{10.3.7}$$

10.3.3 Bounded continuous functions

Now we want to prove the statement:

A continuous function on a closed bounded interval is bounded and attains its bounds.

Theorem 10.3.8. $f : [a,b] \mapsto \mathbb{R}$ is continuous, $\exists K > 0$ s.t. $|f(x)| \le K$, $\forall x \in [a,b]$.

Note $f(x) = 1/x$ on $(0,1]$ is not bounded (needs a closed bounded interval)

Proof. Suppose the statement is not true (there is no such K). Then $\forall n$ (positive integer), there is $x_n \in [a,b]$ s.t. $|f(x_n)| > n$.

By Bolzano-Weierstrass theorem, x_n has a convergent subsequence $x_{n_j} \to x$, then

$$\begin{cases} a \le x_{n_j} \le b \\ |f(x_n)| > n \end{cases} \Rightarrow \begin{cases} a \le x \le b \\ |f(x_{n_j})| > n_j \to \infty \end{cases} \tag{10.3.8}$$

Since f is continuous, $x_{n_j} \to x \;\Rightarrow\; f(x_{n_j}) \to f(x)$, but $|f(x_{n_j})| > n_j \to \infty$. This is contradiction. □

Theorem 10.3.9. $f : [a,b] \mapsto \mathbb{R}$ is continuous, $\exists x_1, x_2 \in [a,b]$ s.t. $f(x_1) \le f(x) \le f(x_2)$, $\forall x \in [a,b]$.

Proof #1. Let $M = \sup\{f(x), x \in [a,b]\}$ and $M < \infty$ by Theorem 10.3.8.

Then $M - 1/n < M$ and by definition of supremum, $\exists x_n \in [a,b]$ s.t. $M - 1/n \le f(x_n) \le M$.

By Bolzano-Weierstrass theorem, we have a subsequence $x_{n_j} \to x_2$ and $a \le x_{n_j} \le b \;\Rightarrow\; a \le x_2 \le b$. Also, we have $M - 1/n \le f(x_{n_j}) \le M$. Then let $j \to \infty$, we have

$$M \le \lim_{j\to\infty} f(x_{n_j}) \le M \quad \xrightarrow{\text{continuity of } f} \quad M \le f(x_2) \le M \;\Rightarrow\; f(x_2) = M. \tag{10.3.9}$$

Similarly for x_1. □

Proof #2. We know that $M = \sup\{f(x), x \in [a,b]\} < \infty$. By contradiction, suppose $f(x) < M,\ \forall x \in [a,b]$. Consider

$$g(x) = \frac{1}{M - f(x)}, \quad \forall x \in [a,b] \tag{10.3.10}$$

g is continuous since $f(x)$ is. By Theorem 10.3.8 applying to g, $\exists K > 0$ s.t. $|g(x)| \le K$, $\forall x \in [a,b]$. Since g is positive,

$$g(x) \le K \;\Rightarrow\; 1/K \le M - f(x) \;\Rightarrow\; f(x) \le M - 1/K, \quad \forall x \in [a,b] \tag{10.3.11}$$

which implies that $M - 1/K$ is an upper bound of the set $\{f(x),\ x \in [a,b]\}$. This contradicts the definition of M since $M - 1/K < M$. □

10.3.4 Inverse functions

Definition 10.3.5. $f : [a,b] \mapsto \mathbb{R}$ is said to be increasing (decreasing) if $x_1 < x_2 \Rightarrow f(x_1) \leq (\geq) f(x_2)$ $(x_1, x_2 \in [a,b])$. f is strictly increasing (strictly decreasing) if $x_1 < x_2 \Rightarrow f(x_1) < (>) f(x_2)$ $(x_1, x_2 \in [a,b])$.

Theorem 10.3.10. $f : [a,b] \mapsto \mathbb{R}$ is continuous and strictly increasing. Let $c = f(a)$ and $d = f(b)$. Then $f : [a,b] \mapsto [c,d]$ is bijective and the inverse $g := f^{-1} : [c,d] \mapsto [a,b]$ is also continuous and strictly increasing.

Proof. (i) f is injective. If $f(x_1) = f(x_2)$, then $x_1 = x_2$. Otherwise, if $x_1 < x_2$, $f(x_1) < f(x_2)$ and if $x_1 > x_2$, $f(x_1) > f(x_2)$ (since f is strictly increasing).

(ii) f is surjective. Take $k \in (c,d)$. By intermediate value theorem (IVT), $\exists h \in (a,b)$ s.t. $f(h) = k$.

So f is bijective and has an inverse function $g : [c,d] \mapsto [a,b]$.

(iii) g is strictly increasing. We have $y_1 < y_2$ and $y_1 = f(x_1)$, $y_2 = f(x_2)$. If $x_1 \geq x_2$, it implies that $f(x_1) \geq f(x_2) \Rightarrow y_1 \geq y_2$ since f is increasing. Contradiction. Thus, $x_1 < x_2$.

(iv) g is continuous. Given $\varepsilon > 0$, let $k_1 = f(h-\varepsilon)$, $k_2 = f(h+\varepsilon)$, $k_1 < k < k_2$ and $h - \varepsilon < g(y) < h + \varepsilon$ for any $k_1 < y < k_2$. Take $\delta = \min\{k - k_1, k_2 - k\}$. For this δ, $|y-k| < \delta \Rightarrow y \in (k_1, k_2) \Rightarrow |g(y) - h| < \varepsilon$.

This was for $k \in (c,d)$. A similar argument gives continuity at the end points also.

□

10.3.5 Càdlàg function

For continuous funtion $f : E \to \mathbb{R}$, we can have the same value by approaching in either way. However, there are more general functions which only have limit in one direction.

Definition 10.3.6. Let $f : E \to \mathbb{R}$ with $E \subseteq \mathbb{R}$. We say f is right-continuous (left-continuous) at $t \in E$ if

$$\lim_{x \downarrow t} f(x) = f(t). \qquad (\lim_{x \uparrow t} f(x) = f(t).) \tag{10.3.12}$$

If f is right-continuous (left-continuous) at any $t \in E$, we say f is a right-continuous (left-continuous) function on E.

Definition 10.3.7 (càdlàg funciton)**.** Let $f : E \to \mathbb{R}$ with $E \subseteq \mathbb{R}$. f is called a càdlàg function[6] if, for every $t \in E$,

$$f(t^-) := \lim_{s \downarrow t} f(s) \text{ exists and } f(t^+) := \lim_{s \downarrow t} f(s) = f(t). \tag{10.3.13}$$

That is, f is right-continuous with left limits.

In this subsection, for a càdlàg function and an interval I, we define (with a slight abuse of notation)

$$df(I) := f(\sup I) - f(\inf I), \qquad \Delta f(t) := f(t) - f(t^-). \tag{10.3.14}$$

Lemma 10.3.11. Let $f : [0,\infty) \to \mathbb{R}$ be càdlàg and define $v^n(0) = 0$, and for all $t > 0$

$$v^n(t) = \sum_{k=0}^{\lceil 2^n t \rceil - 1} \left| f((k+1)2^{-n}) - f(k2^{-n}) \right|. \tag{10.3.15}$$

Then $v(t) := \lim_{n\to\infty} v^n(t)$ is well-defined for all $t \geq 0$ and is non-decreasing in t and $|f(t) - f(0)| \leq v(t)$.

Proof. Let $t_n^+ = 2^{-n}\lceil 2^n t \rceil$, $t_n^- = 2^{-n}(\lceil 2^n t \rceil - 1)$ and $\Delta_n = \{(k2^{-n}, (k+1)2^{-n}] : k \in \mathbb{N}\}$. Write

$$\begin{aligned} v^n(t) = \sum_{k=0}^{\lceil 2^n t \rceil - 1} \left| f((k+1)2^{-n}) - f(k2^{-n}) \right| &= \sum_{\substack{I \in \Delta_n \\ \inf I \leq 2^{-n}(\lceil 2^n t \rceil - 1)}} |f(\sup I) - f(\inf I)| = \sum_{\substack{I \in \Delta_n \\ \inf I \leq 2^{-n}(\lceil 2^n t \rceil - 1)}} |df(I)| \\ &= \sum_{\substack{I \in \Delta_n \\ \inf I < 2^{-n}\lceil 2^n t \rceil}} |df(I)| = \sum_{\substack{I \in \Delta_n \\ \sup I < 2^{-n}\lceil 2^n t \rceil}} |df(I)| + \left| f(t_n^+) - f(t_n^-) \right|. \end{aligned}$$

[6] this can be extended to metric space case

If $t = k2^{-n}$ for some $k \in \mathbb{N}$, we have $\sup I < k2^{-n} = t$. If $t \in ((k-1)2^{-n}, k2^{-n})$ for some $k \in \mathbb{N}$,

$$\lceil 2^n t \rceil = k \;\Rightarrow\; 2^{-n}\lceil 2^n t \rceil = k2^{-n} \;\Rightarrow\; \sup I < k2^{-n} \;\Rightarrow\; \max\{\sup I\} = (k-1)2^{-n} \;\Rightarrow\; \sup I < t. \tag{10.3.16}$$

Thus, we have

$$v^n(t) = \sum_{I \in \Delta_n, \inf I < t} |df(I)| = \sum_{I \in \Delta_n, \sup I < t} |df(I)| + \left|f(t_n^+) - f(t_n^-)\right|. \qquad (*) \tag{10.3.17}$$

The first term is non-decreasing in n by the triangle inequality, we express I by $I_1 \cup I_2$ where $I_1, I_2 \in \Delta_{n+1}$ with $\sup I_2 = \sup I$, $\inf I_1 = \inf I$ and $\inf I_2 = \sup I_1$. Then

$$\begin{aligned}
\sum_{I \in \Delta_n, \sup I < t} |df(I)| &= \sum_{I_1, I_2 \in \Delta_{n+1}, \sup I < t} |f(\sup I) - f(\inf I)| = \sum_{I_1, I_2 \in \Delta_{n+1}, \sup I < t} |f(\sup I_2) - f(\inf I_1)| \\
&= \sum_{I_1, I_2 \in \Delta_{n+1}, \sup I_2 < t} |f(\sup I_2) - f(\inf I_2) + f(\sup I_1) - f(\inf I_1)| \\
&\le \sum_{I_1, I_2 \in \Delta_{n+1}, \sup I_2 < t} |f(\sup I_2) - f(\inf I_2)| + |f(\sup I_1) - f(\inf I_1)| \\
&= \sum_{\substack{I_1 \in \left\{(k2^{-n-1}, (k+1)2^{-n-1}]\right\} \\ k \text{ is even}, \sup I_1 < t - 2^{-n-1}}} |f(\sup I_1) - f(\inf I_1)| + \sum_{\substack{I_1 \in \left\{(k2^{-n-1}, (k+1)2^{-n-1}]\right\} \\ k \text{ is odd}, \sup I_2 < t}} |f(\sup I_2) - f(\inf I_2)| \\
&\le \sum_{I \in \Delta_{n+1}, \sup I < t} |f(\sup I) - f(\inf I)|.
\end{aligned}$$

So $\sum_{I \in \Delta_n, \sup I < t} |df(I)|$ has a limit as $n \to \infty$ (Note that this limit could be infinity).

The second converges to $|\Delta f(t)| = |f(t) - f(t^-)|$ as f is càdlàg, and so $v(t)$ is well defined for all $t \ge 0$.

Since $v^n(t)$ is non-decreasing in t for all n, the same holds for $v(t)$.

Since f is càdlàg, we have

$$\begin{aligned}
|f(t) - f(0)| &= \left| \lim_{n \to \infty} \sum_{k=0}^{\lceil 2^n t \rceil - 1} f((k+1)2^{-n}) - f(k2^{-n}) \right| = \lim_{n \to \infty} \left| \sum_{k=0}^{\lceil 2^n t \rceil - 1} f((k+1)2^{-n}) - f(k2^{-n}) \right| \\
&\le \lim_{n \to \infty} \sum_{k=0}^{\lceil 2^n t \rceil - 1} \left| f((k+1)2^{-n}) - f(k2^{-n}) \right| = v(t).
\end{aligned}$$

□

With the same setup with Lemma 10.3.11, we have

Definition 10.3.8 (total variation, finite variation)**.** $v(t)$ is called the total variation of f over $(0, t]$ and f is said to be of finite variation if $v(t) < \infty$ for all $t \ge 0$.

Proposition 10.3.12. A càdlàg function $f : [0, \infty) \to \mathbb{R}$ can be expressed as $f = f' - f''$, with f', f'' increasing and càdlàg, iff f is of finite variation.

In this case, $t \mapsto v(t)$ is càdlàg with $\Delta v(t) = |\Delta f(t)|$ and $f^{\pm} := \frac{1}{2}(v \pm f)$ are the smallest functions f' and f'' with that property.

Remark. If f is continous, we have v is also continous (see $(*)$ in the following proof).

Proof. ($\Rightarrow$). Assume that $f = f' - f''$ for two càdlàg non-decreasing functions f', f'', and let us show that $v(t) < \infty$.

If $I \in \Delta_n$, then we have by the triangle inequality (since f' and f'' are non-decreasing)

$$|df(I)| = |(f' - f'')(\sup I) - (f' - f'')(\inf I)| \le |f'(\sup I) - f'(\inf I)| + |f''(\sup I) - f''(\inf I)| = df'(I) + df''(I), \tag{10.3.18}$$

as f' and f'' are non-decreasing. So we sum over all intervals $I \in \Delta_n$ with $\inf I < t$, by noting that the sums on the right-hand side telescope: wlog we take $f'(0) = f''(0) = 0$,

$$v^n(t) = \sum_{I \in \Delta_n, \inf I < t} |df(I)| \le \sum_{I \in \Delta_n, \inf I < t} (df'(I) + df''(I)) \le f'(t_n^+) + f''(t_n^+). \tag{10.3.19}$$

Since f' and f'' are càdlàg, the right-hand side converges to $f'(t) + f''(t)$ as $n \to \infty$ and is in particular bounded. Thus $v(t) < \infty$ for all $t \geq 0$.

($\Leftarrow$). Assume that $v(t) < \infty$ for all $t \geq 0$. Let us first show that v is càdlàg. Fix $T > 0$ and consider

$$u^n(t) = \sum_{\substack{I \in \Delta_n \\ t < \inf I < \sup I < T}} |df(I)| \quad \text{for } t < T. \tag{10.3.20}$$

$u^n(t)$ is clearly non-increasing in t, and it is easy to see that it is also right-continuous. To see this, let $t_m = 2^{-m} \lceil 2^m t \rceil$ such that $t_n \downarrow t$. Thus,

$$|u^n(t_m) - u^n(t)| = \sum_{\substack{I \in \Delta_n \\ t < \inf I < t_m}} |df(I)| \tag{10.3.21}$$

Since there exists an interval I such $t < \inf I$, we can find a $t_m < \infty$ with sufficiently large m which will give that no I satisfies the inequality. Thus, $|u^n(t_m) - u^n(t)| = 0$. These two properties imply that $\{t \in [0,T] : u^n(t) \leq x\}$ is closed for all $x \geq 0$.

Now, just as for $v^n(t)$, the sum defining $u^n(t)$ is non-decreasing in n by the triangular inequality. Thus for all $t \geq 0$, $u^n(t)$ has a limit ($u(t) \leq v(t) < \infty$) as $n \to \infty$ which we may call $u(t)$. We have that

$$\{t \in [0,T] : u(t) \leq x\} = \bigcap_{n \in \mathbb{N}} \{t \in [0,T] : u^n(t) \leq x\} \tag{10.3.22}$$

is closed as a countable intersection of closed sets[7]. This, together with the fact that $u(t)$ is non-increasing in t, implies that u is right-continuous. Furthermore, observe that for all $t < T$:

$$\begin{aligned} v^n(T) &= \sum_{\substack{I \in \Delta_n \\ \sup I < T}} |df(I)| + \left| f(T_n^+) - f(T_n^-) \right| \\ &= \sum_{\substack{I \in \Delta_n \\ \sup I < t}} |df(I)| + \sum_{\substack{I \in \Delta_n \\ t = \inf I}} |df(I)| + \sum_{\substack{I \in \Delta_n \\ t < \inf I < \sup I < T}} |df(I)| + \left| f(T_n^+) - f(T_n^-) \right| \\ &= v^n(t) + u^n(t) + \left| f(t + 2^{-n}) - f(t) \right| + \left| f(T_n^+) - f(T_n^-) \right|, \end{aligned}$$

The final two terms on the right converges to $|\Delta f(T)|$ as $n \to \infty$ because f is right-continuous (with $|f(t + 2^{-n}) - f(t)| \to 0$). Hence for all $t < T$ we have (since $u(t), v(t) < \infty$),

$$v(t) = v(T) - u(t) - |\Delta a(T)|. \tag{10.3.23}$$

Since T was arbitrary and u is right-continuous, we have v is right-continuous.

v has left limits since it is non-decreasing, and taking the limit $n \to \infty$ in (*) of Lemma 10.3.11 we get

$$\begin{aligned} v(t) &= \lim_{n \to \infty} v^n(t) = \lim_{n \to \infty} \left(\sum_{I \in \Delta_n, \sup I < t} |df(I)| + \left| f(t_n^+) - f(t_n^-) \right| \right) = \lim_{n \to \infty} \sum_{I \in \Delta_n, \sup I < t} |df(I)| + \lim_{n \to \infty} \left| f(t_n^+) - f(t_n^-) \right| \\ &= \lim_{n \to \infty} \sum_{\substack{I \in \Delta_n \\ \inf I < t - \sup I + \inf I}} |df(I)| + \lim_{n \to \infty} \left| f(t_n^+) - f(t_n^-) \right| = \sum_{\substack{I \in \Delta_n \\ \inf I < \lim_{s \uparrow t} s}} |df(I)| + \lim_{n \to \infty} \left| f(t_n^+) - f(t_n^-) \right| \\ &= \sum_{I \in \Delta_n, \inf I < t^-} |df(I)| + \lim_{n \to \infty} \left| f(t_n^+) - f(t_n^-) \right| = v(t^-) + |\Delta a(t)|. \qquad (*) \end{aligned}$$

Hence, v is càdlàg.

Now we prove that $f = f^+ - f^-$ where f^+ and f^- are non-decreasing and càdlàg. We define two functions f^+ and f^-

$$f^+ = \frac{1}{2}(v + f), \qquad f^- = \frac{1}{2}(v - f). \qquad (\dagger) \tag{10.3.24}$$

Since v and f are càdlàg, then f^+ and f^- are also càdlàg[8]. It thus suffices to prove that they are non-decreasing.

[7] need theorem

[8] need basic property of càdlàg functions

However, note that for each $m \in \mathbb{Z}^+$,

$$\begin{aligned} dv^m(I) &= |df(I)| \qquad \text{for all } I \in \Delta_m \\ dv^n(I) &\geq |df(I)| \qquad \text{for all } I \in \Delta_m \text{ if } n \geq m. \end{aligned}$$

Thus $df^{\pm}(I) = \frac{1}{2}dv(I) \pm \frac{1}{2}df(I) \geq 0$ for all $I \in \bigcup_{m\geq 1} \Delta_m$. So for any $s \leq t$, by right-continuity of $f^{\pm}$ we have

$$\begin{aligned} f^{\pm}(t) - f^{\pm}(s) &= \lim_{n\to\infty} f^{\pm}\left(2^{-n}\lceil 2^n t\rceil\right) - \lim_{n\to\infty} f^{\pm}\left(2^{-n}\lceil 2^n s\rceil\right) \\ &= \lim_{n\to\infty} \left(f^{\pm}\left(2^{-n}\lceil 2^n t\rceil\right) - f^{\pm}\left(2^{-n}\lceil 2^n s\rceil\right)\right) \\ &= \lim_{n\to\infty} \sum_{\substack{I\in\Delta_m \\ 2^{-n}\lceil 2^n s\rceil \leq \inf I \\ \sup I \leq 2^{-n}\lceil 2^n t\rceil}} df^{\pm}(I) \quad \geq 0. \end{aligned}$$

So we have that f^+ and f^- are non-decreasing.

Now Suppose $f = f' - f''$ where f', f'' are non-decreasing càdlàg with $f(0) = f'(0) = f''(0) = 0$ without loss of generality. Then for any $I \in \Delta_n$, $n \geq 0$,

$$|df(I)| \leq df'(I) + df''(I). \tag{10.3.25}$$

Summing over $I \in \Delta_n$ with $\inf I < t$ in (*) of Lemma 10.3.11, the terms in the sum telescope and we obtain

$$v^n(t) = \sum_{I\in\Delta_n, \inf I<t} |df(I)| \leq \sum_{I\in\Delta_n, \inf I<t} df'(I) + df''(I) = f'(t_n^+) + f''(t_n^+). \tag{10.3.26}$$

Letting $n \to \infty$, the left-hand side converges to $v(t)$ by definition, and the right-hand side converges to $f'(t) + f''(t)$ since f' and f'' are right-continuous. Note that we can also write $v(t) = f^+(t) + f^-(t)$ (from (†)) and hence the last inequality shows

$$f^+(t) + f^-(t) = v(t) \leq f'(t) + f''(t) \tag{10.3.27}$$

for all $t \geq 0$, Adding and substracting $f = f^+ - f^- = f' - f''$ on both sides we get

$$f^+(t) \leq f'(t), \quad f^-(t) \leq f''(t) \tag{10.3.28}$$

for all $t \geq 0$, as required. □

10.3.6 Uniform continuity

[9]

10.4 Differentiability

10.4.1 Definitions

$f : E \subseteq \mathbb{C} \mapsto \mathbb{C}$ is a function. We will look at the case: E is the interval in $\mathbb{R}$ and f is real-valued. $x \in E$ s.t. $\exists x_n \in E$, $x_n \neq x$ and $x_n \to x$.

Definition 10.4.1 (differentiable)**.** f is differentiable at x with derivative $f'(x)$ if (the limit exists and)

$$\lim_{y\to x} \frac{f(y) - f(x)}{y - x} = f'(x). \tag{10.4.1}$$

f is differentiable on E if it is differentiable at every point in E.

Remark. (i) We also write $h = y - x$,

$$\lim_{h\to 0} \frac{f(x+h) - f(x)}{h} = f'(x) \tag{10.4.2}$$

[9] need definitions

(ii) Consider

$$\varepsilon(h) = \frac{f(x+h) - f(x) - hf'(x)}{h}, \quad f(x+h) = f(x) + hf'(x) + \varepsilon(h)h, \quad \lim_{h\to 0} \varepsilon(h) = 0 \tag{10.4.3}$$

Thus, an equivalent way of saying that f is differentiable at x with derivative $f'(x)$ is that there is a function $\varepsilon(h)$ s.t. $f(x+h) = f(x) + hf'(x) + h\varepsilon(h)$ with $\lim_{h\to 0} \varepsilon(h) = 0$.

The other ways of writing the same thing:

$f(x+h) = f(x) + hf'(x) + \tilde{\varepsilon}(h)$ with $\frac{\tilde{\varepsilon}(h)}{h} \to 0$ as $h \to 0$.

$f(x) = f(a) + (x-a)f'(a) + (x-a)\varepsilon(x)$ with $\lim_{x\to a} \varepsilon(x) = 0$.

(iii) We can also use this in 3-D with grad

$$\begin{aligned} \delta f &= \nabla f.\delta x \\ \delta f &= \frac{\delta f}{\delta x_1}\delta x_1 + \frac{\delta f}{\delta x_2}\delta x_2 + \frac{\delta f}{\delta x_3}\delta x_3 \\ \Rightarrow f(\underline{y}) &= f(\underline{x}) + \nabla f_0.(\underline{y} - \underline{x}) + \text{error term} \end{aligned}$$

and as before error $\to 0$ faster than the linear term.

Here are some easy consequences of the definition.

Proposition 10.4.1. Let E be a subset of $\mathbb{R}$, f some function from E to $\mathbb{R}$, and x some point of E. Show that if f is differentiable at x then f is continuous at x.

Proof. Given $\epsilon > 0$ $\exists$ $\delta(\epsilon) > 0$ such that $|\frac{f(x)-f(y)}{y-x} - f'(x)| < \epsilon$ for $|y-x| < \delta(\epsilon)$, so $|f(y) - f(x) - f'(x)(y-x)| < \epsilon|y-x|$. Thus,

$$|f(y) - f(x)| < \epsilon|y-x| + |f'(x)(y-x)| = \epsilon|y-x| + |f'(x)||y-x| \tag{10.4.4}$$

All of the terms in the last expression are small except $|f'(x)|$ which is fixed. So if we set $\delta_1(\epsilon) = \min\{\delta(1), \frac{\epsilon}{2}, \frac{\epsilon}{2(|f'(x)+1|)}\}$ for $\epsilon < 1$. Then if $0 < |x-y| < \delta_1(\epsilon)$

$$|f(x) - f(y)| < 1.|y-x| + |f'(x)||y-x| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \tag{10.4.5}$$

□

However, the inverse doesn't hold.

Example 10.4.2. $f : \mathbb{R} \mapsto \mathbb{R}$, $f(x) = |x|$. If $x > 0$,

$$\lim_{h\to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h\to 0} \frac{x+h-x}{h} = 1 = f'(x) \tag{10.4.6}$$

If $x < 0$, then f is differentiable but $f'(x) = -1$. But at $x = 0$, f is not differentiable since

$$\begin{aligned} \lim_{h\to 0^+} \frac{f(h)}{h} &= \lim_{h\to 0^+} \frac{h}{h} = 1 \\ \lim_{h\to 0^-} \frac{f(h)}{h} &= \lim_{h\to 0^-} \frac{-h}{h} = -1 \end{aligned}$$

However, f is continuous at 0, $\lim_{x\to 0} |x| = 0$.

Proposition 10.4.3. (i) If $f(x) = c$, $x \in E$, then f is differentiable at x with $f'(x) = 0$,

(ii) f, g is differentiable at x, then so is $f+g$ and $(f+g)'(x) = f'(x) + g'(x)$,

(iii) f, g is differentiable at x, then so is fg and $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$,

(iv) f is differentiable at x and $f(t) \neq 0$, $\forall t \in E$, then $\frac{1}{f}$ is differentiable at x and

$$\left(\frac{1}{f}\right)'(x) = -\frac{f'(x)}{f^2(x)}. \tag{10.4.7}$$

(v) If $f(t) = \sum_{r=0}^{n} a_r t^r$ on E then f is differentiable at x and

$$f'(x) = \sum_{r=1}^{n} r a_r x^{r-1} \tag{10.4.8}$$

Remark. From (iii) and (iv), we get

$$\left(\frac{f}{g}\right)'(x) = \frac{f'(x)g(x) - f(x)g'(x)}{g^2(x)}. \tag{10.4.9}$$

Proof. (i)

$$\lim_{h\to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h\to 0} \frac{c-c}{h} = 0. \tag{10.4.10}$$

(ii)

$$\lim_{h\to 0} \frac{f(x+h) + g(x+h) - f(x) - g(x)}{h} = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} + \lim_{h\to 0} \frac{g(x+h) - g(x)}{h} = f'(x) + g'(x) \tag{10.4.11}$$

(iii) $\phi(x) = f(x)g(x)$,

$$\begin{aligned} \lim_{h\to 0} \frac{\phi(x+h) - \phi(x)}{h} &= \lim_{h\to 0} \frac{f(x+h)g(x+h) - f(x)g(x)}{h} \\ &= \lim_{h\to 0} \frac{(f(x+h) - f(x))g(x+h)}{h} + \lim_{h\to 0} \frac{f(x)(g(x+h) - g(x))}{h} \\ &= f'(x)g(x) + f(x)g'(x) \end{aligned} \tag{10.4.12}$$

(iv) $\phi(x) = 1/f(x)$,

$$\lim_{h\to 0} \frac{\phi(x+h) - \phi(x)}{h} = \lim_{h\to 0} \frac{1/f(x+h) - 1/f(x)}{h} = \lim_{h\to 0} \frac{f(x) - f(x+h)}{hf(x+h)f(x)} = -\frac{f'(x)}{f^2(x)} \tag{10.4.13}$$

(v) [10]

□

Example 10.4.4. $f(x) = x^n$, $x \neq 0$ and n is a integer, $f'(x) = nx^{n-1}$.

Thus, all polynomials of rational functions are differentiable.

Theorem 10.4.5 (chain rule)**.** $f : U \mapsto \mathbb{R}$ is differentiable at $a \in U$ and $f(x) \in V, \forall x \in U$. $g : V \mapsto \mathbb{R}$ is differentiable at $f(a)$. Then $g \circ f : U \mapsto \mathbb{R}$ is differentiable at a and

$$(g \circ f)'(a) = g'(f(a))f'(a). \tag{10.4.14}$$

Proof. f is differentiable at a means: $f(x) = f(a) + (x-a)f'(a) + (x-a)\varepsilon_f(x)$ with $\lim_{x\to a} \varepsilon_f(x) = 0$.

Similarly, g is differentiable at $f(a)$ means:

$g(y) = g(f(a)) + (y - f(a))g'(f(a)) + (y - f(a))\varepsilon_g(y)$ with $\lim_{y\to f(a)} \varepsilon_g(y) = 0$.

We substitute to obtain

$$\begin{aligned} g(f(x)) &= g(f(a)) + (f(x) - f(a))\left[g'(f(a)) + \varepsilon_g(f(x))\right] \\ &= g(f(a)) + ((x-a)f'(a) + (x-a)\varepsilon_f(x))\left[g'(f(a)) + \varepsilon_g(f(x))\right] \\ &= g(f(a)) + (x-a)\left[f'(a) + \varepsilon_f(x)\right]\left[g'(f(a)) + \varepsilon_g(f(x))\right] \\ &= g(f(a)) + (x-a)f'(a)g'(f(a)) + (x-a)\left[\varepsilon_f(x)g'(f(a)) + (f'(a) + \varepsilon_f(x))\varepsilon_g(f(x))\right] \end{aligned}$$

Let $\sigma(x) = \varepsilon_f(x)g'(f(a)) + (f'(a) + \varepsilon_f(x))\varepsilon_g(f(x))$, we have

$$g(f(x)) = g(f(a)) + (x-a)f'(a)g'(f(a)) + (x-a)\sigma(x) \tag{10.4.15}$$

[10] need proof

Need to prove that $\lim_{x\to a}\sigma(x)=0$. Define $\varepsilon_f(a)=0, \varepsilon_g(f(a))=0$, then ε_f is continuous at a and ε_g is continuous at $f(a)$. Thus, now $\sigma(x)$ is continuous at a (because it is products, sums and compositions of continuous functions). So

$$\lim_{x\to a}\sigma(x)=\sigma(a)=0 \tag{10.4.16}$$

□

Remark. If we want to prove in the way by checking $\frac{g(f(x+h)-g(f(x))}{h}$, we need to discuss whether $f(x)=0$ or not.

Alternative proof. If $f'(x)\neq 0$ then $f(x+h)-f(x)\neq 0$ for h small and thus

$$\frac{g(f(x+h))-g(f(x))}{h}=\frac{g(f(x+h))-g(f(x))}{f(x+h)-f(x)}\cdot\frac{f(x+h)-f(x)}{h}=g'(f(x)).f'(x). \tag{10.4.17}$$

since f is continuous at $x\leq 0$, $f(x+h)\to f(x)$.

We have lots of different ways of dealing with $f'(x)=0$. Since g is differentiable at $f(x)$,

$$\frac{g(f(x)+h)-g(f(x))}{k}\to g'(f(x)) \tag{10.4.18}$$

so if k is sufficiently small, say for $0<|k|<\mu$,

$$\Big|\frac{g(f(x)+k)-g(f(x))}{k}-g'(f(x))\Big|<1\ \Rightarrow\ |g(f(x)+k)-g(f(x))|\leq|k|(1+|g'(f(x))|). \tag{10.4.19}$$

Now f is continuous at x so $\exists\delta(\mu)>0$ such that $|f(x+h)-f(x)|<\mu$ for $|h|<\delta(\mu)$. Take $k=f(x+h)-f(x)$. We have

$$|g(f(x+h))-g(f(x))|\leq|f(x+h)-f(x)|(1+|g'(f(x))|) \tag{10.4.20}$$

so

$$\Big|\frac{g(f(x+h))-g(f(x))}{h}\Big|\leq\underbrace{\Big|\frac{f(x+h)-f(x)}{h}\Big|}_{\to 0}(1+|g'(f(x))|) \tag{10.4.21}$$

Thus $g\circ f$ is differentiable with derivative 0. □

Example 10.4.6. $\phi(x)=\sin x^2:\ f(x)=x^2,\ g(x)=\sin x,\ \phi(x)=(g\circ f)(x)$. Thus, $\phi'(x)=2x\cos x^2$.

10.4.2 Mean value theorem

We first prove the following basic existence result.

Theorem 10.4.7 (Rolle's Theorem)**.** $f:[a,b]\mapsto\mathbb{R}$ is continuous and differentiable on (a,b). If $f(a)=f(b)$, then $\exists c\in(a,b)$ s.t. $f'(c)=0$.

Proof. Define

$$M=\max_{x\in[a,b]}f(x),\quad m=\min_{x\in[a,b]}f(x) \tag{10.4.22}$$

(By Theorem 10.3.9, the values M and m are achieved.) Let $k=f(a)=f(b)$. If $M=m=k$, then f is constant, and $f'(c)=0,\ \forall c\in(a,b)$.

Otherwise, $M>k$ or $m<k$. Suppose $M>k$ (the proof of $m<k$ is similar). We know from Theorem 10.3.9, $\exists c\in(a,b)$ s.t. $f(c)=M$. We want to prove that $f'(c)=0$. Since f is differentiable at c, we can write

$$f(c+h)=\underbrace{f(c)}_{M}+h(f'(c)+\varepsilon(h)).\quad\left(\lim_{h\to 0}\varepsilon(h)=0\right) \tag{10.4.23}$$

If $f'(c)>0$, we have $f'(c)+\varepsilon(h)>0$ for all h sufficiently small ($\lim_{h\to0}\varepsilon(h)=0$). In addition we take $h>0$, then $f(c+h)=M+h(f'(c)+\varepsilon(h))>M$ which is absurd because M is the maximum of f. If $f'(c)<0$, the same argument shows that there are points at left of c, for which f is strictly bigger than M. Again absurd, thus $f'(c)=0$. □

Theorem 10.4.8 (mean value theorem)**.** $f:[a,b]\mapsto\mathbb{R}$ is continuous and differentiable on (a,b). Then $\exists c\in(a,b)$ s.t. $f(b)-f(a)=f'(c)(b-a)$.

Remark. We can rewrite this as follows: $b = a + h$, $f(a + h) = f(a) + hf'(a + \theta h)$ where $\theta \in (0, 1)$.

Proof. We consider the auxilary function $\phi(x) = f(x) - kx$. Let's choose k s.t. $\phi(a) = \phi(b)$. Thus,

$$f(a) - ka = f(b) - kb \;\Rightarrow\; k = \frac{f(b) - f(a)}{b - a} \tag{10.4.24}$$

So for this choice of k, ϕ satisfies the hypothesis of Roller's theorem. Hence, $\exists c \in (a, b)$ s.t. $\phi'(c) = 0$. Then

$$\phi'(c) = f'(c) - k = 0 \;\Rightarrow\; f'(c) = k = \frac{f(b) - f(a)}{b - a}. \tag{10.4.25}$$

□

We have the following important corollary.

Corollary 10.4.9. $f : [a, b] \mapsto \mathbb{R}$ is continuous and differentiable,

(i) If $f'(x) > 0$ $\forall x \in (a, b)$, then f is strictly increasing.

(ii) If $f'(x) \geq 0$ $\forall x \in (a, b)$, then f is increasing.

(iii) If $f'(x) = 0$ $\forall x \in (a, b)$, then f is constant.

Proof. (i) Let $x, y \in [a, b]$ with $x < y$. The mean value theorem says

$$f(y) - f(x) = f'(c)(y - x), \quad \exists c \in (x, y). \tag{10.4.26}$$

Then $f'(c) > 0 \;\Rightarrow\; f(y) - f(x) = f'(c)(y - x) > 0 \;\Rightarrow\; f(y) > f(x)$.

(ii) Same argument with (i).

(iii) Consider f on the interval $[a, x]$, $\forall x \in (a, b)$ and apply mean value theorem to get

$$f(x) - f(a) = f'(c)(x - a) = 0,\ \exists c \in (a, x) \;\Rightarrow\; f(x) = f(a). \tag{10.4.27}$$

□

10.4.3 Inverse Rule (Inverse Function Theorem)

Lemma 10.4.10. (i) Suppose $f : [a, b] \to \mathbb{R}$ is continuous. Then f is injective if and only if it is strictly increasing (that is $f(t) > f(s)$ whenever $a \leq s < t \leq b$) or strictly decreasing.

(ii) Suppose $f : [a, b] \to \mathbb{R}$ is continuous and strictly increasing. Let $f(a) = c$ and $f(b) = d$. Then the map $f : [a, b] \to [c, d]$ is bijective and f^{-1} is continuous on $[c, d]$.

Proof. (i) If f is strictly increasing, $y \neq x$ then either $y > x$ or $x > y$. If $y > x, f(y) > f(x)$ so $f(y) \neq f(x)$, same for $x > y$

Conversely, suppose f is not strictly increasing. Then either

(a) We can find $x_1 < x_2 < x_3$ such that $f(x_1) \leq f(x_2)$ and $f(x_3) \leq f(x_2)$.

(b) we can find $x_1 < x_2 < x_3$ such that $f(x_1) \geq f(x_2)$ and $f(x_3) \geq f(x_2)$.

WLOG assume case A (otherwise look at $-f$)

If $f(x_1) = f(x_2)$ or $f(x_2) = f(x_3)$ then we have a contradiction (f would not be injective). So suppose all are strict inequalities

Choose c with $f(x_2) > c > \max\{f(x_1), f(x_2)\}$. By the Intermediate Value Theorem we can find α_1, α_2 such that $x_1 < \alpha_1 < x_3, x_2 < \alpha_2 < x_3$ and $f(\alpha_1) = x = f(\alpha_2)$. Thus f is not injective

(ii) The injectivity follows from (i).

Surjectivity follows from the Intermediate Value Theorem: If $x \le \gamma \le d$ then since $f(a) = c, f(b) = d$ $\exists t$ with $a \le t \le b$ such that $f(t) = \gamma$

Thus f is bijective and f^{-1} is defined as a function, $f^{-1} : [c, d] \mapsto [a, b]$

Claim that f^{-1} is continuous

Let $y \in [c, d]$. To simplify matters, suppose $y \neq c, y \neq d$

If $\delta > 0$ consider the interval $[\theta_1, \theta_2] = [a, b] \cap [f^{-1}(y - \frac{\delta}{2}), f^{-1}(y + \frac{\delta}{2})]$

$\theta_1 < f^{-1}(y) < \theta_2$

$f(\theta_1) < y < f(\theta_2)$ so choose $\epsilon > 0$ such that $f(\theta_1) < y - \epsilon < y < y + \epsilon < f(\theta_2)$

If $|y - z| < \epsilon$, $f(\theta_1) < z < f(\theta_2)$ so $\theta_1 < f^{-1}(z) < \theta_2$ and so $|f^{-1}(z) - f^{-1}(y)| < \frac{\delta}{2} < \delta$

The proof if $y = c$ or $y = d$ is similar, but one-sided.

□

Theorem 10.4.11 (inverse function theorem)**.** $f : [a, b] \mapsto \mathbb{R}$ is continuous in $[a, b]$ and differentiable in (a, b) with $f'(x) > 0$, $\forall x \in (a, b)$. Let $c = f(a)$ and $d = f(b)$. The function $f : [a, b] \mapsto [c, d]$ is a bijection and $f^{-1} : [c, d] \mapsto [a, b]$ is continuous on $[c, d]$ and differentiable on (c, d) with

$$\left(f^{-1}\right)'(x) = \frac{1}{f'\left(f^{-1}(x)\right)}, \quad \forall x \in (c, d). \tag{10.4.28}$$

Proof. Since $f'(x) > 0$, $\forall x \in (a, b)$, by Corollary 10.4.9, f is strictly increasing. By Theorem 10.3.10, $f^{-1} : [c, d] \mapsto [a, b]$ exists and is bijective and continuous.

Let $g(y) = f^{-1}(y)$, we need to prove that g is differentiable with

$$g'(y) = \frac{1}{f'(x)}, \quad x = f^{-1}(y) \tag{10.4.29}$$

If $h \neq 0$ and small enough, then there exists a unique k s.t. $y + k = f(x + h)$, $g(y + k) = x + h$ and $f(x + h) - f(x) = k$ $(k \neq 0)$. Thus

$$\frac{g(y + k) - g(y)}{k} = \frac{x + h - x}{f(x + h) - f(x)} = \frac{h}{f(x + h) - f(x)} = \frac{1}{\frac{f(x+h)-f(x)}{h}} \tag{10.4.30}$$

If $k \to 0$, then $h \to 0$ (g continuous at y). Thus,

$$g'(y) = \lim_{k \to 0} \frac{g(y + k) - g(y)}{k} = \lim_{h \to 0} \frac{1}{\frac{f(x+h)-f(x)}{h}} = \frac{1}{\lim_{h \to 0} \frac{f(x+h)-f(x)}{h}} = \frac{1}{f'(x)}. \tag{10.4.31}$$

□

Example 10.4.12. 1. $f(x) = x^q$, q is a positive integer and $g(x) = x^{1/q}$ $(x \ge 0)$. $g(f(x)) = x$, $f'(x) = qx^{q-1} > 0$ if $x > 0$.

Inverse rule gives g is differentiable in $(0, \infty)$ and

$$g'(x) = \frac{1}{q(x^{1/q})^{q-1}} = \frac{1}{q} x^{1/q - 1} \tag{10.4.32}$$

2. $g(x) = x^{p/q}$, p is any integer and q is positive integer. We find $g'(x)$ using the chain rule,

$$g(x) = (x^{1/q})^p \;\Rightarrow\; g'(x) = p(x^{1/q})^{p-1} \frac{1}{q} x^{1/q - 1} = \frac{p}{q} x^{\frac{p}{q} - 1} \tag{10.4.33}$$

In other words, if $g(x) = x^r$, where r is any rational number, then $g'(x) = rx^{r-1}$. Later on we will define x^r for r is <u>real</u> and discover that $(x^r)' = rx^{r-1}$.

Theorem 10.4.13 (Cauchy's mean value theorem)**.** $f, g : [a, b] \mapsto \mathbb{R}$ is continuous in $[a, b]$ and differentiable in (a, b). Then $\exists t \in (a, b)$ s.t. $(f(b) - f(a))g'(t) = f'(t)(g(b) - g(a))$.

Proof. Consider the function $h : [a, b] \mapsto \mathbb{R}$.

$$\begin{vmatrix} 1 & 1 & 1 \\ f(a) & f(x) & f(b) \\ g(a) & g(x) & g(b) \end{vmatrix} \tag{10.4.34}$$

Thus h is continuous in $[a, b]$ and differentiable in (a, b) (It is just a product and sum of functions with the same property). $h(a) = h(b) = 0$ because in either 2 columns are equal. By Rolle's Theorem, $\exists t \in (a, b)$ s.t. $h'(t) = 0$. Now expand the determinant and differentiate to see that $h'(t) = 0$ gives exactly what we want. □

Example 10.4.14. $\lim_{x\to 0} \frac{e^x-1}{\sin x}$.

$f(x) = e^x$ and $g(x) = \sin x$. With Cauchy mean value theorem, $\exists t \in (0, x)$,

$$\frac{e^x - 1}{\sin x} = \frac{f(x) - f(0)}{g(x) - g(0)} = \frac{f'(t)}{g'(t)} = \frac{e^t}{\cos t} \tag{10.4.35}$$

Let $x \to 0 \Rightarrow t \to 0$. $\frac{e^t}{\cos t} \to 1$. Thus,

$$\lim_{x\to 0} \frac{e^x - 1}{\sin x} = 1. \quad \text{(L'Hôpital Rule)}^{11} \tag{10.4.36}$$

10.4.4 Taylor's theorems

Theorem 10.4.15 (Taylor's theorem with Lagrange's remainder)**.** Suppose f and its derivative up to order $n - 1$ are continuous on $[a, a + h]$ and $f^{(n)}$ exists for $x \in (a, a + h)$, then

$$f(a + h) = f(a) + hf'(a) + \cdots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(a) + \frac{h^n}{n!} f^{(n)}(a + \theta h), \quad \theta \in (0, 1). \tag{10.4.37}$$

Note 1. $R_n = \frac{h^n}{n!} f^{(n)}(a + \theta h)$ is Lagrange's form for the remainder.

2. For $n = 1$ this is the mean value theorem.

Proof. Consider $t \in [0, h]$

$$\phi(t) = f(a + t) - f(a) - f'(a)t - \cdots - \frac{t^{n-1} f^{(n-1)}(a)}{(n-1)!} - \frac{t^n B}{n!} \tag{10.4.38}$$

B is chosen s.t. $\phi(h) = 0$. $\phi(0) = f(a + 0) = f(a) = 0$.

We will apply Rolle's Theorem n times. We apply it to ϕ first to get $h_1 \in (0, 1)$ s.t. $\phi'(h_1) = 0$ and $\phi'(0) = f'(a) - f'(a) + 0 = 0$.

Apply Rolle's Theorem to ϕ' in $[0, h_1]$ to get $h_2 \in (0, h_1)$ s.t. $\phi''(h_2) = 0$.

Note that in fact from definition of ϕ, we see that $\phi(0) = \phi'(0) = \phi''(0) = \cdots = \phi^{(n-1)}(0) = 0$. We keep apply Rolle's Theorem to get $0 < h_n < h_{n-1} < \cdots < h$ at which $\phi^{(i)}(h_i) = 0,\ 1 \le i \le n$.

Now note $\phi^{(n)}(t) = f^{(n)}(a + t) - B \Rightarrow \phi^{(n)}(h_n) = 0 = f^{(n-1)}(a + h_n) - B = 0$.

Write $h_n = \theta_n$ for $\theta \in (0, 1)$ to get $B = f^{(n)}(a + \theta h)$.

Now put this value of B in the definition of ϕ and the statement $\phi(h) = 0$ is exactly the statement of the theorem. □

Theorem 10.4.16 (Taylor's theorem with Cauchy's form of the remainder)**.** Let f satisfy the same hypothesis as Theorem 10.4.15 and in addition suppose $a = 0$. (This is just to simplify maths)

$$f(h) = f(0) + hf'(0) + \cdots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(0) + R_n \tag{10.4.39}$$

where

$$R_n = \frac{(1 - \theta)^{n-1} h^n}{(n-1)!} f^{(n)}(\theta h), \quad \theta \in (0, 1). \tag{10.4.40}$$

Proof. Consider $t \in [0, h]$

$$F(t) = f(h) - f(t) - f'(t)(h - t) - \cdots - \frac{(h - t)^{n-1}}{(n-1)!} f^{(n-1)}(t) \tag{10.4.41}$$

$$F'(t) = -f'(t) + f'(t) - f''(t)(h - t) + f''(t)(h - t) - \frac{(h - t)^2}{2} f'''(t) - \cdots - \frac{(h - t)^{n-1}}{(n-1)!} f^{(n)}(t) \tag{10.4.42}$$

In summary:

$$F'(t) = -\frac{(h-t)^{n-1}}{(n-1)!} f^{(n)}(t) \tag{10.4.43}$$

Set $\phi(0) = F(t) - \left(\frac{h-t}{h}\right)^p F(0),\ 1 \le p \le n,\ \phi(0) = 0,\ \phi(h) = F(h) = 0$, (from definition of F).
Rolle's Theorem applied to ϕ gives $\theta \in (0,1)$ s.t. $\phi'(\theta h) = 0$.
Now we compute

$$0 = \phi'(\theta h) = F'(\theta h) + p\left(\frac{h-\theta h}{h}\right)^{p-1}\left(\frac{1}{h}\right)F(0) = F'(\theta h) + p\frac{(1-\theta)^{p-1}}{h}F(0) \tag{10.4.44}$$

$$\Rightarrow\ 0 = -\frac{h^{n-1}(1-\theta)^{n-1}}{(n-1)!}f^{(n)}(\theta h) + p\frac{(1-\theta)^{p-1}}{h}\left[f(h) - f(0) - hf'(0) - \cdots - \frac{h^{n-1}}{(n-1)!}f^{(n-1)(0)}\right] \tag{10.4.45}$$

Rearranging

$$f(h) = f(0) + hf'(0) + \cdots + \frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0) + \frac{(1-\theta)^{n-1}h^n}{(n-1)!p(1-\theta)^{p-1}}f^{(n)}(\theta h) \tag{10.4.46}$$

$$R_n = \frac{(1-\theta)^{n-1}h^n}{(n-1)!p(1-\theta)^{p-1}}f^{(n)}(\theta h), \quad 1 \le p \le n,\ p \in \mathbb{Z},\ \theta \in (0,1) \tag{10.4.47}$$

Set $p = 1$,

$$R_n = \frac{(1-\theta)^{n-1}h^n}{(n-1)!}f^{(n)}(\theta h), \quad \text{(Cauchy)}. \tag{10.4.48}$$

Set $p = n$,

$$R_n = \frac{h^n}{n!}f^{(n)}(\theta h), \quad \text{(Lagrange)}. \tag{10.4.49}$$

Taylor's series needs $R_n \to 0$ as $n \to \infty$.

$$f(h) = \sum_{n=0}^{\infty}\frac{f^{(n)}(0)}{n!}h^n \tag{10.4.50}$$

□

Remark. (i) $[0,h)$ is just to simplify matters.

(ii) The same result holds in an interval $[h,0]$ $(h < 0)$.

(iii) $a = 0$. Mclaurin expansion.

Example 10.4.17. binomial series

$$f(x) = (1+x)^r,\ (r \in \mathbb{Q}), \quad f'(x) = r(1+x)^{r-1} \tag{10.4.51}$$

we have

$$(1+x)^r = \sum_{n=0}^{\infty}\underbrace{\binom{r}{n}x^n}_{a_n}, \quad |x| < 1. \tag{10.4.52}$$

If r is a positive integer, then

$$\binom{r}{n} = 0, \quad n > r. \tag{10.4.53}$$

Let's prove that for $|x| < 1$, the series is absolutely convergent. Ratio test

$$\left|\frac{a_{n+1}}{a_n}\right| = \left|\frac{r(r-1)\dots(r-n+1)(r-n)x^{n+1}n!}{r(r-1)\dots(r-n+1)x^n(n+1)!}\right| = \left|\frac{r-n}{n+1}x\right| \to |x| \quad \text{as } n \to \infty. \tag{10.4.54}$$

So, the series converges absolutely for $|x| < 1$. In particular, $a_n \to 0$ i.e. $\binom{r}{n}x^n \to 0$ as $n \to \infty$ $(|x| < 1)$.
Now we study the remainders in the Taylor Theorem.

$$f'(x) = r(1+x)^{r-1}, \quad f^{(n)}(x) = r(r-1)\dots(r-n+1)(1+x)^{r-n} \ \Rightarrow\ f^{(n)}(0)/n! = \binom{r}{n}. \tag{10.4.55}$$

We look at the Lagrange's form:

$$R_n = (1+\theta x)^{r-n}\binom{r}{n}x^n, \quad \theta \in (0,1). \tag{10.4.56}$$

For $0 < x < 1$

$$1+\theta x > 1 \;\Rightarrow\; (1+\theta x)^{n-r} > 1,\ (n > r) \;\Rightarrow\; |R_n| \le \left|\binom{r}{n}x^n\right|,\ (n > r) \;\Rightarrow\; R_n \to 0 \text{ as } n \to \infty. \tag{10.4.57}$$

For $-1 < x < 0$, the Cauchy form:

$$\begin{aligned} R_n &= \frac{(1-\theta)^{n-1}r(r-1)\dots(r-n+1)(1+\theta x)^{r-n}x^n}{(n-1)!} = r\binom{r-1}{n-1}\frac{(1-\theta)^{n-1}}{(1+\theta x)^{n-r}}x^n \\ &= r\binom{r-1}{n-1}\frac{(1-\theta)^{n-r}}{(1+\theta x)^{n-r}}(1-\theta)^{r-1}x^n \end{aligned}$$

$$-1 < x < 0 \;\Rightarrow\; \frac{1-\theta}{1+\theta x} < 1 \;\Rightarrow\; |R_n| \le \underbrace{r(1-\theta)^{r-1}}_{\text{bounded in } n}\left|\binom{r-1}{n-1}x^n\right| \to 0 \text{ as } n \to \infty \;\Rightarrow\; R_n \to 0. \tag{10.4.58}$$

Some comments on differentiability of functions $f : \mathbb{C} \to \mathbb{C}$.

$$f'(z) = \lim_{w \to z}\frac{f(w)-f(z)}{w-z} \tag{10.4.59}$$

"Standard properties" work for both $\mathbb{R}$ and $\mathbb{C}$.

Example 10.4.18. $f : \mathbb{C} \to \mathbb{C},\ f(z) = \bar{z}$

$$z_n = z + \frac{1}{n} \;\Rightarrow\; \frac{f(z_n)-f(z)}{z_n - z} = \frac{\bar{z}+\frac{1}{n}-\bar{z}}{z+\frac{1}{n}-z} = 1, \qquad z_n = z + \frac{i}{n} \;\Rightarrow\; \frac{f(z_n)-f(z)}{z_n-z} = \frac{\bar{z}-\frac{i}{n}-\bar{z}}{z+\frac{i}{n}-z} = -1 \tag{10.4.60}$$

So $\lim_{w-z}\frac{f(w)-f(z)}{w-z}$ does not exist!

10.5 Power Series

Look at $\sum_{n=0}^{\infty} a_n z^n,\ a_n \in \mathbb{C},\ z \in \mathbb{C}$.

Lemma 10.5.1. If $\sum_{n=0}^{\infty} a_n z_0^n$ converges, and $|z| < |z_0|$, then $\sum_{n=0}^{\infty} a_n z^n$ converges absolutely.

Proof. Since $\sum_{n=0}^{\infty} a_n z_0^n$ converges, $a_n z_0^n \to 0$ as $n \to \infty$. In particular, there is a constant K s.t. $|a_n z_0^n| \le K,\ \forall n$.

$$|a_n z^n| = \left|a_n z^n \frac{z_0^n}{z_0^n}\right| \le K\left|\frac{z}{z_0}\right|^n \tag{10.5.1}$$

Since $|z| < |z_0|$, the geometric series $\sum\left|\frac{z}{z_0}\right|^n$ converges. By comparison, $\sum_{n=0}^{\infty}|a_n z^n|$ converges, i.e. $\sum_{n=0}^{\infty} a_n z^n$ converges absolutely. □

Theorem 10.5.2. A power series either

(i) converges absolutely for all z, or

(ii) converges absolutely for all z inside a circle $|z| = R$, and diverges for all z outside it, or

(iii) converges for $z = 0$, only.

Definition 10.5.1. The circle $|z| = R$ is called the circle of convergence and R the radius of convergence. In case (i), we agree that $R = \infty$ and in case (iii), we agree that $R = 0$.

Proof. Let $S = \{x \in \mathbb{R} : x \ge 0 \text{ and } \sum a_n x^n \text{ converges}\}$, $0 \in S \ne \emptyset$.

If $x_1 \in S$, then by Lemma 10.5.1, $[0, x_1] \subset S$.

If S is unbounded, then $S = \mathbb{R}^+\{x \in \mathbb{R} : x \ge 0\}$ and we have case (i).

If S is bounded, there exists a finite supremum for S, we call it R.

If $R > 0$, we will prove that if $|z_1| < R$, then $\sum a_n z_1^n$ converges absolutely: Choose R_0 s.t. $|z_1| < R_0 < R$, then $R_0 \in S$ implies that $\sum a_n R_0^n$ converges and by Lemma 10.5.1, $\sum a_n z_1^n$ converges absolutely.

Finally, we show that if $|z_2| > R > 0$, then $\sum a_n z_2^n$ diverges. Take R_0 s.t. $R < R_0 < |z_0|$. If $\sum a_n z_2^n$ converges, again by Lemma 10.5.1, $\sum a_n R_0^n$ converges. But this contradicts the definition of R as supremum of S. Thus, $\sum a_n z_2^n$ diverges. □

The next lemma is useful for computing R.

Lemma 10.5.3. If $\left|\frac{a_{n+1}}{a_n}\right| \to l$ as $n \to \infty$, then $R = 1/l$.

Proof. By the ratio test we have absolute convergence if

$$\lim \left|\frac{a_{n+1} z^{n+1}}{a_n z^n}\right| < 1, \text{ i.e. } |z| < 1/l \tag{10.5.2}$$

and if $|z| > 1/l$, then $\lim \left|\frac{a_{n+1} z^{n+1}}{a_n z^n}\right| > 1$ implies that

$$\left|a_{n+1} z^{n+1}\right| > |a_n z^n|, \ \forall n \geq n_0 \tag{10.5.3}$$

and $a_n z^n$ does not tend to zero which implies that $R = 1/l$. □

Remark. By the Root test, if $|a_n|^{1/n} \to l$, then $R = 1/l$.

Example 10.5.4. (i) $\sum_{n=0}^{\infty} \frac{z^n}{n!}$, $\left|\frac{n!}{(n+1)!}\right| = \frac{1}{n+1} \to 0 \ \Rightarrow \ R = \infty$.

(ii) $\sum_{n=0}^{\infty} z^n$, $R = 1$. Note that if $|z| = 1$, then the series diverges, $|z|^n = 1 \nrightarrow 0$.

(iii) $\sum_{n=0}^{\infty} n! z^n$, $\left|\frac{(n+1)!}{n!}\right| = n + 1 \to \infty \ \Rightarrow \ R = 0$.

(iv) $\sum_{n=1}^{\infty} \frac{z^n}{n}$, $\left|\frac{n}{n+1}\right| \to 1 \ \Rightarrow \ R = 1$. If $z = 1$, $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges. By Abel's Test (If b_n is a decreasing sequence of positive terms tending to zero and $S_n = \sum_{i=1}^{n} a_i$ is bounded, $\sum_{i=1}^{\infty} a_i b_i$ converges), we have $a_n = z^n$, $b_n = 1/n \to 0$. Thus, for $z \neq 1$,

$$S_n = \sum_{i=1}^{n} z^i = \frac{1 - z^{n+1}}{1 - z} - 1 \ \Rightarrow \ |S_n| \leq 1 + \frac{2}{|1 - z|} \tag{10.5.4}$$

which is bounded in n. Hence, $\sum_{n=1}^{\infty} \frac{z^n}{n}$ converges for $|z| = 1, \ z \neq 1$.

(v) $\sum_{n=1}^{\infty} \frac{z^n}{n^2}$, $\left|\frac{n^2}{(n+1)^2}\right| \to 1 \ \Rightarrow \ R = 1$ but converge for every $|z| \leq 1$.

(vi) $\sum_{n=1}^{\infty} n z^n$, $\left|\frac{n+1}{n}\right| \to 1 \ \Rightarrow \ R = 1$ but on $|z| = 1$, $|nz^n| = n \to \infty$, we have divergence.

Conclusion: in general nothing can be said at $|z| = R$.

Lemma 10.5.5. If $\sum a_n z^n$ has radius of convergence R, then so do $\sum n a_n z^{n-1}$ and $\sum n(n-1) a_n z^{n-2}$. Furthermore, for any $k \in \mathbb{N}$, we have that

$$\sum_n \frac{n!}{(n-k)!} a_n z^{n-k} \text{ has radius of convergence } R. \tag{10.5.5}$$

Proof. $\sum a_n z^n$ has radius of convergence R, and $\sum n a_n z^{n-1}$ has radius of convergence R'. RTP: $R = R'$.

Take z with $|z| < R$, choose R_0 s.t. $|z_0| < R_0 < R$. Since $R_0 < R$, $a_n R_0^n \to 0$ as $n \to \infty$. In particular, there exists K s.t. $|a_n R_0^n| \leq K, \ \forall n$.

$$|n a_n z^{n-1}| = \frac{n}{|z|} |a_n z^n| \frac{R_0^n}{R_0^n} \leq \frac{K}{|z|} n \left|\frac{z}{R_0}\right|^n \tag{10.5.6}$$

We see that $\sum n \left|\frac{z}{R_0}\right|^n$ converges. By comparison, $\sum n a_n z^{n-1}$ converges absolutely which implies that $R \leq R'$.

But in fact we have equality because

$$|a_n z^n| \leq n |a_n z^n| = \frac{1}{|z|} n |a_n z^{n-1}| \tag{10.5.7}$$

by comparison, if $\sum n a_n z^{n+1}$ converges absolutely, so does $\sum a_n z^n$. Thus, $R = R'$. What we proved also implies that $\sum n(n-1) a_n z^{n-2}$ has radius of convergence R. The similar arguement for $k \in \mathbb{N}$. □

Lemma 10.5.6. (i) $\binom{n}{r} \leq n(n-1)\binom{n-2}{r-2}, \quad 2 \leq r \leq n$

(ii) $|(z+h)^n - z^n - nhz^{n-1}| \leq n(n-1)(|z| + |h|)^{n-2} |h|^2, \quad \forall h, z \in \mathbb{Z}$

Proof. (i)

$$\frac{\binom{n}{r}}{\binom{n-2}{r-2}} = \frac{n!}{r!(n-r)!} \cdot \frac{(r-2)!(n-r)!}{(n-2)!} = \frac{n(n-1)}{r(r-1)} \leq n(n-1). \tag{10.5.8}$$

(ii)

$$\begin{aligned} (z+h)^n - z^n - nhz^{n-1} &= \sum_{r=2}^{n} \binom{n}{r} z^{n-r} h^r \\ \Rightarrow\ |(z+h)^n - z^n - nhz^{n-1}| &\leq \sum_{r=2}^{n} \binom{n}{r} |z|^{n-r}|h|^r \leq \sum_{r=2}^{n} n(n-1)\binom{n-2}{r-2}|z|^{n-r}|h|^r \quad \text{(by (i))} \\ &= n(n-1)|h|^2 \underbrace{\sum_{r=2}^{n} \binom{n-2}{r-2}|z|^{n-r}|h|^{r-2}}_{(|z|+|h|)^{n-2}} \end{aligned}$$

□

Theorem 10.5.7. Suppose $\sum a_n z^n$ has radius of convergence R, so let

$$f(z) = \sum_{n=0}^{\infty} a_n z^n,\ |z| < R \tag{10.5.9}$$

Then f is differentiable and $f'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$.

Remark. Iterate this theorem, to get that f can be differentiated infinitely many as if it was a polynomial.

Proof. By Lemma 10.5.5, since $\sum n a_n z^n$ has radius of convergence R, it defines a function $g(z) = \sum n a_n z^{n-1}$ for z with $|z| < R$. We would like to prove that

$$\frac{f(z+h) - f(z) - hg(z)}{h} \to 0 \text{ as } h \to 0. \tag{10.5.10}$$

This implies that f is differentiable with $f'(z) = g(z)$.

$$\frac{f(z+h) - f(z) - hg(z)}{h} = \frac{1}{h}\left(\sum_{n=0}^{\infty} a_n (z+h)^n - \sum_{n=0}^{\infty} a_n z^n - h\sum_{n=0}^{\infty} n a_n z^{n-1}\right) = \frac{1}{h}\sum_{n=0}^{\infty} a_n \left((z+h)^n - z^n - nhz^{n-1}\right) \tag{10.5.11}$$

By Lemma 10.5.6,

$$\left|a_n \left((z+h)^n - z^n - nhz^{n-1}\right)\right| \leq |a_n| n(n-1)(|z|+|h|)^{n-2}|h|^2 \tag{10.5.12}$$

Take r s.t. $|z| + r < R$. If $|h| < r$, we get

$$\left|a_n \left((z+h)^n - z^n - nhz^{n-1}\right)\right| \leq |a_n| n(n-1)(|z|+r)^{n-2}|h|^2 \tag{10.5.13}$$

By Lemma 10.5.5, we know that $\sum |a_n| n(n-1)(|z|+r)^{n-2}$ converges to some number A. Thus,

$$\frac{|f(z+h) - f(z) - hg(z)|}{|h|} \leq \frac{1}{|h|} A|h|^2 = A|h| \to 0 \text{ as } h \to 0. \tag{10.5.14}$$

□

Example 10.5.8. $\sum_{n=0}^{\infty} \frac{z^n}{n!}$ has radius of convergence $R = \infty$. Thus, $e : \mathbb{C} \mapsto \mathbb{C}$, $e(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$. The theorem tells us right away that e is differentiable and

$$e'(z) = \sum_{n=1}^{\infty} \frac{n}{n!} z^{n-1} = e(z). \tag{10.5.15}$$

Remark. $F : \mathbb{C} \mapsto \mathbb{C}$ is differentiable. If $F'(z) = 0,\ \forall z \in \mathbb{C}$, then F is constant. Let $g(t) = F(tz)$, $g : [0,1] \mapsto \mathbb{C}$. Write

$$g(t) = u(t) + iv(t), \quad \text{where } u, v : [0,1] \mapsto \mathbb{R}. \tag{10.5.16}$$

With chain rule, we have $g'(t) = F'(tz)z = 0 \ \Rightarrow\ u'(t) = v'(t) = 0$. By Corollary 10.4.9, we have u and v are constants.

Thus, we claim $e(a+b)=e(a)e(b),\ a,b\in\mathbb{C}$ and define $F:\mathbb{C}\mapsto\mathbb{C}$

$$F(z)=e(a+b-z)e(z)\ \Rightarrow\ F'(z)=-e(a+b-z)e(z)+e(a+b-z)e(z)=0\ \Rightarrow\ F \text{ is constant} \tag{10.5.17}$$

Thus, $F(z)=F(0)=e(a+b)e(0)$. From the definition of e, $e(0)=1$, so $F(z)=e(a+b),\ \forall z\in\mathbb{C}$. Let $z=b$, we have $e(a+b)=e(a)e(b)$.

Now we restrict $e:\mathbb{R}\mapsto\mathbb{R}$ and prove

Theorem 10.5.9. (i) $e:\mathbb{R}\mapsto\mathbb{R}$ is differentiable everywhere;
(ii) $e(x+y)=e(x)e(y),\quad \forall x,y\in\mathbb{R}$;
(iii) $e(x)>0,\quad \forall x\in\mathbb{R}$;
(iv) e is strictly increasing;
(v) $e(x)\to\infty$ as $x\to\infty$, $e(x)\to 0$ as $x\to-\infty$;
(vi) $e:\mathbb{R}\mapsto(0,\infty)$ is a bijection.

Proof. (i) and (ii) done.
(iii) clearly from the definition of $e(x)$, $e(x)>0$ if $x\geq 0$ and $e(0)=1$. We have

$$1=e(0)=e(x-x)=e(x)e(-x)\ \Rightarrow\ e(x)>0,\ \forall x\in\mathbb{R}. \tag{10.5.18}$$

(iv) $e'(x)=e(x)>0$, then e is strictly increasing by Corollary 10.4.9.
(v) From definition of $e(x)$, by $e(-x)=\frac{1}{e(x)}$

$$e(x)>1+x,\quad x>0\ \Rightarrow\ e(x)\to\infty \text{ as } x\to\infty\ \Rightarrow\ e(x)\to 0 \text{ as } x\to-\infty. \tag{10.5.19}$$

(vi) e is strictly increasing implies that e is injective.
For any $y\in(0,\infty)$, $\exists a,b\in\mathbb{R}$ s.t. $e(a)<y<e(b)$ since $e(x)\to\infty$ as $x\to\infty$, $e(x)\to 0$ as $x\to-\infty$. Thus, with Intermediate value theorem, $\exists x\in\mathbb{R}$ s.t. $e(x)=y$ which proves surjectivity. □

Remark. (vi) and (ii) are saying that the map $e:(\mathbb{R},+)\mapsto((0,\infty),\times)$ is group isomorphism. Since $e:\mathbb{R}\mapsto(0,\infty)$ is a bijection, $\exists l:(0,\infty)\mapsto\mathbb{R}$ s.t. $e(l(t))=t,\ \forall t\in(0,\infty)$ and $l(e(x))=x,\ \forall x\in\mathbb{R}$.

Theorem 10.5.10. (i) $l:(0,\infty)\mapsto\mathbb{R}$ is a bijection and $l(e(x))=x,\ \forall x\in\mathbb{R}$, $e(l(t))=t,\ \forall t\in(0,\infty)$;
(ii) l is differentiable and $l'(t)=1/t$;
(iii) $l(xy)=l(x)+l(y),\ \forall x,y\in(0,\infty)$.

Proof. (i) Obvious.
(ii) l is differentiable by the Inverse rule (Theorem 10.4.11)

$$l'(t)=\frac{1}{e'(l(t))}=\frac{1}{e(l(t))}=\frac{1}{t}. \tag{10.5.20}$$

(iii) By Groups, $l((0,\infty),x)\mapsto(\mathbb{R},t)$ is a homomorphism. □

$\alpha\in\mathbb{R}$, x is any positive number. We define

$$\gamma_\alpha(x)=e(\alpha l(x)),\quad \gamma_1(x)=x. \tag{10.5.21}$$

Theorem 10.5.11. Suppose $x,y>0,\ \alpha,\beta\in\mathbb{R}$, then
(i) $\gamma_\alpha(xy)=\gamma_\alpha(x)\gamma_\alpha(y)$;
(ii) $\gamma_{\alpha+\beta}(x)=\gamma_\alpha(x)\gamma_\beta(x)$;
(iii) $\gamma_\alpha(\gamma_\beta(x))=\gamma_{\alpha\beta}(x)$;

Proof. (i) $\gamma_\alpha(xy)=e(\alpha l(xy))=e(\alpha(l(x)+l(y)))=e(\alpha l(x))e(\alpha l(y))=\gamma_\alpha(x)\gamma_\alpha(y)$.
(ii) $\gamma_{\alpha+\beta}(x)=e((\alpha+\beta)l(x))=e(\alpha l(x))e(\beta l(x))=\gamma_\alpha(x)\gamma_\beta(x)$.
(iii) $\gamma_\alpha(\gamma_\beta(x))=e(\alpha l(\gamma_\beta(x)))=e(\alpha l(e(\beta l(x))))=e(\alpha\beta l(x))=\gamma_{\alpha\beta}(x)$. □

If n is positive integer,

$$\gamma_n(x) = \gamma_{1+1+\cdots+1}(x) = x \cdots x = x^n, \quad \gamma_0(x) = 1, \quad \gamma_{-1}(x) = 1/x, \quad \gamma_{-n}(x) = x^{-n} \tag{10.5.22}$$

If q is a positive integer,

$$(\gamma_{1/q}(x))^q = \gamma_{q/q}(x) = x \;\Rightarrow\; \gamma_{1/q} = x^{1/q} \;\Rightarrow\; \gamma_{p/q} = x^{p/q} \tag{10.5.23}$$

Thus, we have

$$\gamma_\alpha(x) = x^\alpha, \quad \alpha \in \mathbb{R}. \tag{10.5.24}$$

This definition agrees with the one given before for $\alpha \in \mathbb{R}$, $\exp(x) = e^x = e(x)$ and $\log(x) = l(x)$. Define the real number, e as

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} \qquad (\gamma_\alpha(x) = e(\alpha l(x)) \;\Rightarrow\; x^\alpha = e^{\alpha \log x}) \tag{10.5.25}$$

$$(x^\alpha)' = e^{\alpha \log x} \frac{\alpha}{x} = \alpha x^{\alpha-1}, \quad \alpha \in \mathbb{R}. \tag{10.5.26}$$

Define $f(x) = a^x = e^{x \log a}$, $a > 0, a \in \mathbb{R}$

$$f'(x) = e^{x \log a} \log a = a^x \log a. \tag{10.5.27}$$

10.5.1 Trigonometric functions

$$\left.\begin{array}{rcl} \sin z & = & \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{(2n+1)!} \\ \cos z & = & \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n}}{(2n)!} \end{array}\right\} \text{both have infinite radius of convergence.} \tag{10.5.28}$$

$\sin z, \cos z : \mathbb{C} \mapsto \mathbb{C}$. By Theorem 10.5.7, they are differentiable and

$$(\sin z)' = \cos z, \quad (\cos z)' = -\sin z \tag{10.5.29}$$

$$e^{iz} = \sum_{n=0}^{\infty} \frac{(iz)^n}{n!} = \sum_{n=0}^{\infty} \frac{(iz)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{(iz)^{2n+1}}{(2n+1)!} = \cos z + i \sin z. \tag{10.5.30}$$

From defintion,

$$\cos(-z) = \cos z, \quad \sin(-z) = -\sin z. \tag{10.5.31}$$

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \sin z = \frac{e^{iz} - e^{-iz}}{2} \tag{10.5.32}$$

Now we get using $e^{a+b} = e^a e^b$,

$$\sin(z+w) = \sin z \cos w + \cos z \sin w, \quad \cos(z+w) = \cos z \cos w - \sin z \sin w, \quad z, w \in \mathbb{C} \tag{10.5.33}$$

Also, $\cos^2 z + \sin^2 z = 1$, $z \in \mathbb{C}$. If $x \in \mathbb{R}$, $|\sin x| \le 1$ and $|\cos x| \le 1$.
Warning $|\cos z|$ ($|\sin z|$) are not bounded for $z \in \mathbb{C}$. If $z = iy$, $\cos(iy) = \frac{e^y + e^{-y}}{2} \to \infty$ as $y \to \pm\infty$.
Periodicity of the trigonometric functions:

Proposition 10.5.12. There is a smallest positive number w (when $\sqrt{2} < w/2 < \sqrt{3}$) s.t.

$$\cos(w/2) = 0. \tag{10.5.34}$$

Proof. If $0 < x < 2$,

$$\sin x = \underbrace{\left(x - \frac{x^3}{3!}\right)}_{>0} + \underbrace{\left(\frac{x^5}{5!} - \frac{x^7}{7!}\right)}_{>0} + \ldots \quad \left(\frac{x^{2n-1}}{(2n-1)!} > \frac{x^{2n+1}}{(2n+1)!}\right) \;\Rightarrow\; \sin x > 0. \tag{10.5.35}$$

But $(\cos x)' = -\sin x < 0$, $x \in (0,2)$ implies that $\cos x$ is a strictly decreasing function in $(0,2)$. We will prove that $\cos\sqrt{2} > 0, \cos\sqrt{3} < 0$. By the Intermediate value theorem, there exists w s.t. $w/2 \in (\sqrt{2}, \sqrt{3})$.

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots \Rightarrow \begin{cases} \cos\sqrt{2} &= \underbrace{\left(1 - \frac{\sqrt{2}^2}{2!}\right)}_{>0} + \underbrace{\left(\frac{\sqrt{2}^4}{4!} - \frac{\sqrt{2}^6}{6!}\right)}_{>0} + \cdots > 0 \\ \cos\sqrt{3} &= \underbrace{\left(1 - \frac{\sqrt{3}^2}{2!} + \frac{\sqrt{3}^4}{4!}\right)}_{<0} - \underbrace{\left(\frac{\sqrt{3}^6}{6!} - \frac{\sqrt{3}^8}{8!}\right)}_{>0} + \cdots < 0 \end{cases}$$

□

Corollary 10.5.13. $\sin\frac{w}{2} = 1$

Proof. $\underbrace{\cos^2\frac{w}{2}}_{=0} + \sin^2\frac{w}{2} = 1 \Rightarrow \sin^2\frac{w}{2} = 1 \Rightarrow \sin\frac{w}{2} = 1$ since $\sin x > 0$. □

Definition 10.5.2. $\pi := w$.

Theorem 10.5.14. (i) $\sin(z + \frac{\pi}{2}) = \cos z, \quad \cos(z + \frac{\pi}{2}) = -\sin z;$
(ii) $\sin(z + \pi) = -\sin z, \quad \cos(z + \pi) = -\cos z;$
(iii) $\sin(z + 2\pi) = \sin z, \quad \cos(z + 2\pi) = \cos z.$

Note that we $e^{z+2\pi i} = e^z$.

10.5.2 Hyperbolic functions

$$\cosh z = \frac{1}{2}(e^z + e^{-z}), \quad \sinh z = \frac{1}{2}(e^z - e^{-z}), \quad z \in \mathbb{C} \tag{10.5.36}$$

From this,

$$\begin{cases} \cosh z = \cos iz \\ i\sinh z = \sin iz \end{cases}, \quad \begin{cases} (\cosh z)' = \sinh z \\ (\sinh z)' = \cosh z \end{cases}, \quad \cosh^2 z - \sinh^2 z = 1 \tag{10.5.37}$$

Remark. 1. The other trigonometric functions (tan, sec, etc.) are defined in the usual way.

2. Exponential bear powers $\frac{e^x}{x^k} \to \infty$ as $x \to \infty$, $k > 0$. To prove this, take a positive integer n s.t. $n > k$, and observe (from the definition of e^k as a power series) that $e^x > \frac{x^n}{n!}$, $x > 0$

$$\frac{e^x}{x^n} > \frac{x^{n-k}}{n!} \to \infty \text{ as } x \to \infty \ (n > k). \tag{10.5.38}$$

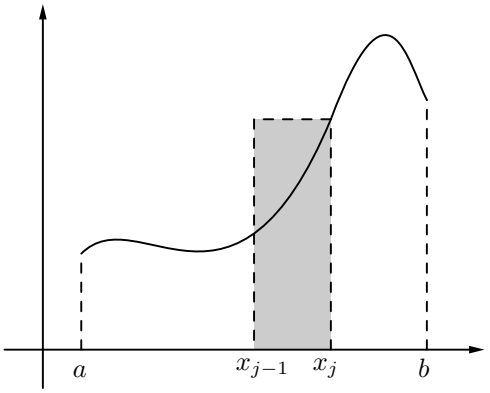
10.6 Integration

10.6.1 Riemann integration

$f : [a,b] \mapsto \mathbb{R}$, bounded. There exists $K > 0$ s.t. $|f(x)| \le K$, $\forall x \in [a,b]$.

Definition 10.6.1. A dissection (or partition) of the interval $[a,b]$ is a finite subset D of $[a,b]$ which contains a and b. We write it as

$$D = \{a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b\} \tag{10.6.1}$$



We define the upper and lower sum of f w.r.t. D as

$$S(f,D)=\sum_{j=1}^{n}(x_j-x_{j-1})\sup_{x\in[x_{j-1},x_j]}f(x),\quad s(f,D)=\sum_{j=1}^{n}(x_j-x_{j-1})\inf_{x\in[x_{j-1},x_j]}f(x) \tag{10.6.2}$$

Clearly, $S(f,D)>s(f,D)$.

Lemma 10.6.1. If D and D' are dissections with $D'>D$, then

$$S(f,D)\geq S(f,D')\geq s(f,D')\geq s(f,D). \tag{10.6.3}$$

Proof. Suppose D' has one extra point, let's say $y\in(x_{r-1},x_r)$ for some r. We know

$$\sup_{x\in[x_{r-1},y]}f(x),\ \sup_{x\in[y,x_r]}f(x)\leq\sup_{x\in[x_{r-1},x_r]}f(x). \tag{10.6.4}$$

Thus,

$$(x_r-x_{r-1})\sup_{x\in[x_{r-1},x_r]}f(x)\geq(y-x_{r-1})\sup_{x\in[x_{r-1},y]}f(x)+(x_r-y)\sup_{x\in[y,x_r]}f(x) \tag{10.6.5}$$

which implies that $S(f,D)\geq S(f,D')$. If now D' has more than one D extra point, just do the argument for each extra point. The proof for $s(f,D')\geq s(f,D)$ is similar to the one for the upper sums. □

Lemma 10.6.2. If D_1 and D_2 are any two dissections, then

$$S(f,D_1)\geq S(f,D_1\cup D_2)\geq s(f,D_1\cup D_2)\geq s(f,D_2). \tag{10.6.6}$$

Proof. $D1\cup D_2\geq D_1,D_2$, so by Lemma 10.6.1, we get the conclusion as required. □

Definition 10.6.2. The upper and lower integrals are defined as

$$I^*(f)=\inf_D S(f,D),\qquad I_*(f)=\sup_D s(f,D). \tag{10.6.7}$$

Remark. These numbers are well-defined because f is bounded so

$$S(f,D)\geq -K(b-a),\quad s(f,D)\leq K(b-a),\quad \forall D \tag{10.6.8}$$

Definition 10.6.3. We say that a bounded function f is Riemann integrable if $I^*(f)=I_*(f)$. In this case, we write

$$\int_a^b f(x)dx=I^*(f)=I_*(f)\qquad\left(\text{or just }\int_a^b f.\right) \tag{10.6.9}$$

Remark. $I^*(f)\geq I_*(f)$ thanks to Lemma 10.6.2,

$$S(f,D_1)\geq s(f,D_2)\ \Rightarrow\ \inf_{D_1}S(f,D_1)\geq s(f,D_2),\quad S(f,D_1)\geq\sup_{D_2}s(f,D_2). \tag{10.6.10}$$

Which functions are Riemann integrable?

Example 10.6.3. (**Dirichlet**)

$$f(x) = \begin{cases} 1 & x \text{ is rational in } [0,1] \\ 0 & x \text{ is irrational in } [0,1] \end{cases} \quad \text{bounded.} \tag{10.6.11}$$

D is any partition, $S(f,D) = 1$ because every $[x_{r-1}, x_r]$ contains a rational. But $s(f,D) = 0$ and

$$I^*(f) = 1, \quad I_*(f) = 0. \tag{10.6.12}$$

Thus, f is not Riemann integrable.

We now prove the following useful criterion for integrabilities.

Theorem 10.6.4 (Riemann)**.** A bounded function $f : [a,b] \mapsto \mathbb{R}$ is integrable iff given $\varepsilon > 0$, $\exists D$ s.t. $S(f,D) - s(f,D) < \varepsilon$.

Proof. Let's assume first that f is Riemann integrable. Given $\varepsilon > 0$, by definition of $I^*(f)$, $\exists D_1$ s.t.

$$S(f, D_1) < I^*(f) + \varepsilon \tag{10.6.13}$$

By definition of $I_*(f)$, $\exists D_2$ s.t.

$$s(f, D_2) > I_*(f) - \varepsilon \tag{10.6.14}$$

Consider $D = D_1 \cup D_2$, by Lemma 10.6.2, we have

$$S(f, D_1 \cup D_2) - s(f, D_1 \cup D_2) \leq S(f, D_1) - s(f, D_2) < I^*(f) + \varepsilon - I_*(f) + \varepsilon = 2\varepsilon. \tag{10.6.15}$$

To prove a converse, assume that given $\varepsilon > 0$, $\exists D$ s.t. $S(f,D) - s(f,D) < \varepsilon$. Applying the definition of I^* and I_*,

$$0 \leq I^*(f) - I_*(f) \leq S(f,D) - s(f,D) < \varepsilon. \tag{10.6.16}$$

Given this is true, for all $\varepsilon > 0$, $I^* = I_*$. Thus, f is integrable. □

We now prove monotonic functions and continuous function are integrable.

Remark. Monotonic and continuous function on $[a,b]$ are bounded.

Theorem 10.6.5. $f : [a,b] \mapsto \mathbb{R}$ is monotonic, then f is integrable.

Proof. Assume f is increasing. Take D any partition of $[a,b]$

$$S(f,D) = \sum_{j=1}^{n} \sup_{x \in [x_{j-1}, x_j]} f(x)(x_j - x_{j-1}) = \sum_{j=1}^{n} f(x_j)(x_j - x_{j-1}) \quad \text{(since } f \text{ increasing)} \tag{10.6.17}$$

Similarly,

$$s(f,D) = \sum_{j=1}^{n} f(x_{j-1})(x_j - x_{j-1}) \tag{10.6.18}$$

Thus,

$$S(f,D) - s(f,D) = \sum_{j=1}^{n} (f(x_j) - f(x_{j-1}))(x_j - x_{j-1}) \tag{10.6.19}$$

Now consider a positive integer n

$$D = \left\{ a, a + \frac{b-a}{n}, \ldots, a + \frac{(b-a)(n-1)}{n}, b \right\}, \qquad x_j = a + \frac{(b-a)j}{n}, \quad 0 \leq j \leq n. \tag{10.6.20}$$

For this D,

$$S(f,D) - s(f,D) = \frac{b-a}{n} \sum_{j=1}^{n} (f(x_j) - f(x_{j-1})) = \frac{(b-a)(f(b) - f(a))}{n}. \tag{10.6.21}$$

Given $\varepsilon > 0$, take n large enough s.t.

$$\frac{(b-a)(f(b) - f(a))}{n} < \varepsilon \tag{10.6.22}$$

By Theorem 10.6.4, f is integrable. □

Lemma 10.6.6. $f:[a,b]\mapsto\mathbb{R}$ is continuous. Given $\varepsilon>0$, $\exists\delta>0$ s.t. if $|x-y|<\delta$, $(x,y\in[a,b])$ then $|f(x)-f(y)|<\varepsilon$ (uniform continuity).

Remark. Continuity at a point, let's say $x\in[a,b]$ means that given $\varepsilon>0$, $\exists\delta(x)$ s.t. $|y-x|<\delta\ \Rightarrow\ |f(y)-f(x)|<\varepsilon$.

Proof. Suppose claim is not true. There exists $\varepsilon>0$ s.t. for every $\delta>0$, we can find x,y with $|x-y|<\delta$ but $|f(x)-f(y)|\geq\varepsilon$.

Take $\delta=\frac{1}{n}$ to get x_n,y_n with $|x_n-y_n|<\frac{1}{n}$, but $|f(x_n)-f(y_n)|\geq\varepsilon$.

By Bolzano-Weierstrass theorem, $x_{n_k}\to c$ and $x_n\in[a,b]\ \Rightarrow\ c\in[a,b]$.

$$|y_{n_k}-c|\leq|x_{n_k}-y_{n_k}|+|x_{n_k}-c|<\frac{1}{n_k}+|x_{n_k}-c| \tag{10.6.23}$$

let $n_k\to\infty$, $\frac{1}{n_k}+|x_{n_k}-c|\to0$, so $y_{n_k}\to c$.

On the other hand, $|f(x_{n_k})-f(y_{n_k})|\geq\varepsilon$. Since f is continuous,

$$f(x_{n_k})\to f(c),\quad f(y_{n_k})\to f(c)\ \Rightarrow\ 0=|f(c)-f(c)|\geq\varepsilon\quad\text{(absurd.)} \tag{10.6.24}$$

□

Theorem 10.6.7. $f:[a,b]\mapsto\mathbb{R}$ is continuous. Then f is integrable.

Proof. Consider the partition D with points (n is a positive integer)

$$x_j=a+\frac{(b-a)j}{n},\quad 0\leq j\leq n. \tag{10.6.25}$$

$$S(f,D)-s(f,D)=\sum_{j=1}^{n}\left(\sup_{x\in[x_{j-1},x_j]}f(x)-\inf_{x\in[x_{j-1},x_j]}f(x)\right)\frac{b-a}{n} \tag{10.6.26}$$

Let $\varepsilon>0$ be given and consider δ given in Lemma 10.6.6. Choose n large enough s.t. $\frac{b-a}{n}<\delta$. Then for any $x,y\in[x_{j-1},x_j]$, $|f(x)-f(y)|<\varepsilon$ which implies that

$$\sup_{x\in[x_{j-1},x_j]}f(x)-\inf_{x\in[x_{j-1},x_j]}f(x)<\varepsilon\ \Rightarrow\ S(f,D)-s(f,D)<\varepsilon(b-a) \tag{10.6.27}$$

By Riemann's criterion, f is integrable. □

Example 10.6.8.

$$f(x)=\begin{cases}1/q & \text{if } x \text{ is } p/q \text{ in } [0,1]\\ 0 & \text{if } x \text{ is irrational in } [0,1]\end{cases} \tag{10.6.28}$$

Claim f is integrable and $\int_0^1 f=0$.

Take D as any partition, then $s(f,D)=0$ (every $[x_{j-1},x_j]$ contains irrational numbers, where f is zero). Clearly, $I_*(f)=0$.

To prove the claim, it suffices to show that given $\varepsilon>0$, $\exists D$ s.t. $S(f,D)<\varepsilon$ (by Riemann's and $I_*(f)=0$).

Let $\varepsilon>0$ be given, take an integer N with $1/N<\varepsilon$. $S=\{x\in[0,1],f(x)\geq1/N\}$ is a finite set with a cardinality of R. Thus,

$$x\in S=\{0=t_1<t_2<\cdots<t_R=1\}\ \Leftrightarrow\ \begin{cases}x=p/q\\ 1/q\geq1/N\ (q\leq N)\end{cases} \tag{10.6.29}$$

Choose a partition D s.t. the point t_i belong to the interval $[x_{i_1},x_{i_2}]$ with length less than ε/R. $(0=t_1=x_0)$. Thus, we have

$$\begin{aligned}S(f,D) &= \sum_{\text{intervals containing } t_i}\underbrace{\sup_D f(x)}_{\leq1}(x_j-x_{j-1})+\sum_{\text{all the other intervals}}\underbrace{\sup_D f(x)}_{<1/N}(x_j-x_{j-1})\\ &< \sum_{\text{intervals containing } t_i}(x_j-x_{j-1})+\quad 1/N\cdot\sum_{\text{all the other intervals}}(x_j-x_{j-1})\\ &< \varepsilon/R\cdot R+1/N<2\varepsilon.\end{aligned}$$

10.6.2 Elementary properties of the integral

Proposition 10.6.9. f, g are bounded, and integrable on $[a, b]$, then

(i) If $f \leq g$ on $[a, b]$, then $\int_a^b f \leq \int_a^b g$,

(ii) $f + g$ is integrable over $[a, b]$,

(iii) For any constant k, kf is integrable and $\int_a^b kf = k\int_a^b f$,

(iv) $|f|$ is integrable and $\left|\int_a^b f\right| \leq \int_a^b |f|$,

(v) The product fg is integrable,

(vi) If $f(x) = F(x)$ except at finitely many points in $[a, b]$, then F is integrable and $\int_a^b F = \int_a^b f$,

(vii) If $a < c < b$, f is integrable over $[a, c]$ and $[c, b]$ and $\int_a^b f = \int_a^c f + \int_c^b f$.

Proof. (i) If $f \leq g$, then

$$\int_a^b f = I^*(f) \leq S(f, D) \leq S(g, D) \forall D. \tag{10.6.30}$$

Take infimum over all D

$$\int_a^b f \leq I^*(g) = \inf_a^b g. \tag{10.6.31}$$

(ii) Observe first

$$\sup_{x\in[x_{j-1},x_j]} (f + g)(x) \leq \sup_{x\in[x_{j-1},x_j]} f(x) + \sup_{x\in[x_{j-1},x_j]} g(x) \;\Rightarrow\; S(f + g, D) \leq S(f, D) + S(g, D) \tag{10.6.32}$$

Now take any two partitions D_1 and D_2

$$I^*(f + g) \leq S(f + g, D_1 \cup D_2) \leq S(f, D_1 \cup D_2) + S(g, D_1 \cup D_2) \leq S(f, D_1) + S(g, D_2) \quad \text{(Lemma 10.6.2)} \tag{10.6.33}$$

Keep D_1 fixed and take infimum over all D_2,

$$I^*(f + g) \leq S(f, D_1) + I^*(g) \;\Rightarrow\; I^*(f + g) \leq I^*(f) + I^*(g) = \int_a^b f + \int_a^b g. \tag{10.6.34}$$

A similar argument for the lower sums gives

$$I_*(f + g) \geq \int_a^b f + \int_a^b g \tag{10.6.35}$$

With $I^*(f + g) \geq I_*(f + g)$, we have

$$I^*(f + g) = I_*(f + g) = \int_a^b f + \int_a^b g \tag{10.6.36}$$

(iii) Observe first if $k \geq 0$

$$\sup_{x\in[x_{j-1},x_j]} (kf)(x) = k \sup_{x\in[x_{j-1},x_j]} f(x) \tag{10.6.37}$$

with $k \geq 0$, we have

$$I^*(kf) \leq S(kf, D) = kS(f, D), \quad \forall D \tag{10.6.38}$$

take infimum over all D, we have $I^*(kf) \leq kI^*(f)$, Similarly, we have $I_*(kf) \geq kI_*(f)$ which implies that $I^*(kf) = I_*(kf)$. For $k \leq 0$, we use the similar argument.

(iv) Let $f^+(x) = \max\{f(x), 0\}$ and $|f(x)| = 2f^+(x) - f(x)$. Claim that $f^+(x)$ is integrable.

$$\sup_{x\in[x_{j-1},x_j]} f^+(x) - \inf_{x\in[x_{j-1},x_j]} f^+(x) \leq \sup_{x\in[x_{j-1},x_j]} f(x) - \inf_{x\in[x_{j-1},x_j]} f(x) \tag{10.6.39}$$

So for any partition D

$$S(f^+, D) - s(f^+, D) \leq S(f, D) - s(f, D) \tag{10.6.40}$$

By Riemann's, f is integrable, given $\varepsilon > 0$, $\exists D$ s.t. $S(f, D) - s(f, D) < \varepsilon$ and then $S(f^+, D) - s(f^+, D) < \varepsilon$. Thus, by Riemann's again, f^+ is integrable and $|f|$ is integrable. Also, follows from (i), we have $-|f| \leq f \leq |f| \Rightarrow \left|\int_a^b f\right| \leq \int_a^b |f|$.

(v) First we prove that if f is integrable, then f^2 is integrable. Suppose first $f \geq 0$. Since f is integrable, given $\varepsilon > 0$, $\exists D$ partition of $[a, b]$ s.t. $S(f, D) - s(f, D) < \varepsilon$. Define

$$M_j = \sup_{x \in [x_{j-1}, x_j]} f(x), \quad m_j = \inf_{x \in [x_{j-1}, x_j]} f(x) \Rightarrow \sup_{x \in [x_{j-1}, x_j]} f^2(x) - \inf_{x \in [x_{j-1}, x_j]} f^2(x) = M_j^2 - m_j^2 \quad (\text{since } f \geq 0) \tag{10.6.41}$$

Thus,

$$S(f^2, D) - s(f^2, D) = \sum_{j=1}^{n} (M_j^2 - m_j^2)(x_j - x_{j-1}) = \sum_{j=1}^{n} (M_j + m_j)(M_j - m_j)(x_j - x_{j-1}) \tag{10.6.42}$$

f is bounded, $M_j + m_j \leq 2K$, where $f(x) \leq K$, $\forall x \in [a, b]$

$$S(f^2, D) - s(f^2, D) < 2K \sum_{j=1}^{n} (M_j - m_j)(x_j - x_{j-1}) = 2K(S(f, D) - s(f, D)) < 2K\varepsilon \Rightarrow f^2 \text{ is integrable.} \tag{10.6.43}$$

If f is now arbitrary (i.e. just integrable). Then $|f|$ is integrable by (iv), but $|f|^2 = f^2$. Since $|f| \geq 0$, f^2 is integrable.

To prove that fg is integrable, just write

$$4f(x)g(x) = (f(x) + g(x))^2 - (f(x) - g(x))^2 \tag{10.6.44}$$

Now f, g are integrable $\Rightarrow f + g$ and $f - g$ are integrable $\Rightarrow (f + g)^2$ and $(f - g)^2$ are integrable. as required.

(vi) Let $h = f - F$, then $h(x) = 0$, for every $x \in [a, b]$ except perhaps a finite set. (just from the definition of the integral) It must be integrable with $\int_a^b h = 0$. But $F = f - h$, so F is integrable with $\int_a^b F = \int_a^b f$.

□

$\int_a^b f$, $a < b$. If $a > b$, define $\int_a^b f = -\int_b^a f$ and $\int_a^a f = 0$.
How do we compute $\int_a^b f$? $f : [a, b] \mapsto \mathbb{R}$ is bounded Riemann integrable. $x \in [a, b]$

$$F(x) = \int_a^x f(t)dt. \tag{10.6.45}$$

Theorem 10.6.10. F is continuous.

Proof. $x \in [a, b]$,

$$F(x + h) - F(x) = \int_a^{x+h} f(t)dt - \int_a^x f(t)dt = \int_x^{x+h} f(t)dt \tag{10.6.46}$$

$$|F(x + h) - F(x)| = \left|\int_x^{x+h} f(t)dt\right| \leq \int_x^{x+h} |f(t)|dt \leq \int_x^{x+h} Kdt = Kh, \quad (h > 0) \tag{10.6.47}$$

In fact for any h,

$$|F(x + h) - F(x)| \leq K|h| \Rightarrow \lim_{h \to 0} F(x + h) = F(x). \tag{10.6.48}$$

□

Theorem 10.6.11 (The Fundamental Theorem of Calculus)**.** If in addition f is continuous, then F is differentiable and

$$F'(x) = f(x) \quad \forall x \in [a, b] \tag{10.6.49}$$

Proof. For $x \in [a,b],\ h \neq 0$,

$$\left|\frac{F(x+h)-F(x)}{h} - f(x)\right| = \frac{1}{|h|}|F(x+h)-F(x)-hf(x)| = \frac{1}{|h|}\left|\int_x^{x+h} f(t)dt - hf(x)\right| = \frac{1}{|h|}\left|\int_x^{x+h}[f(t)-f(x)]dt\right| \tag{10.6.50}$$

Since $|f(t)-f(x)| \leq \max|f(x+\theta h)-f(x)|,\ \theta \in [0,1],\ \forall t \in [x,x+h]$. We have

$$\left|\frac{F(x+h)-F(x)}{h} - f(x)\right| \leq \frac{1}{|h|}|h| \max_{\theta\in[0,1]}|f(x+\theta h)-f(x)| = \max_{\theta\in[0,1]}|f(x+\theta h)-f(x)| \tag{10.6.51}$$

Now if $h \to 0$, then by continuity of f

$$\lim_{h\to 0}\max_{\theta\in[0,1]}|f(x+\theta h)-f(x)| = 0. \tag{10.6.52}$$

□

Corollary 10.6.12 (Integration is the 'inverse' of differentiation)**.** If $f = g'$ is continuous on $[a,b]$, then

$$\int_a^x f(t)dt = g(x) - g(a), \quad \forall x \in [a,b]. \tag{10.6.53}$$

Proof. From Theorem 10.6.11, we know $F'(x) = f(x)$. Therefore,

$$(F-g)'(x) = F'(x) - g'(x) = 0 \ \Rightarrow\ F - g \text{ is constant.} \tag{10.6.54}$$

Thus,

$$F(x) - g(x) = F(a) - g(a) = 0 - g(a) \ \Rightarrow\ \int_a^x f = g(x) - g(a). \tag{10.6.55}$$

□

This gives a way of computing $\int_a^b f$ if we know a 'primitive' for f, i.e. a function g s.t. $g' = f$.
Primitives of continuous functions always exist (Theorem 10.6.11) and they all differ by a constant.

Corollary 10.6.13 (Integration by parts)**.** Suppose f' and g' exist and are continuous on $[a,b]$, then

$$\int_a^b f'g = f(b)g(b) - f(a)g(a) - \int_a^b fg'. \tag{10.6.56}$$

Proof. Product rule gives

$$(fg)' = f'g + fg' \ \Rightarrow\ \int_a^b (f'g + fg') = fg|_a^b = f(b)g(b) - f(a)g(a). \tag{10.6.57}$$

□

Corollary 10.6.14 (Integration by substitution)**.** $g : [\alpha,\beta] \mapsto [a,b]$ with $g(\alpha) = a,\ g(\beta) = b$, and g' exists and is continuous on $[\alpha,\beta]$. Let $f : [a,b] \mapsto \mathbb{R}$ be continuous, then

$$\int_a^b f(x)dx = \int_\alpha^\beta f(g(t))g'(t)dt. \tag{10.6.58}$$

Proof. Set $F(x) = \int_a^x f(t)dt$ for $x \in [a,b]$. Let $h(t) = F(g(t))$ (g takes value in $[a,b]$). Apply chain rule,

$$h'(t) = F'(g(t))g'(t) = f(g(t))g'(t). \tag{10.6.59}$$

Hence,

$$\int_\alpha^\beta f(g(t))g'(t)dt = h|_\alpha^\beta = h(\beta) - h(\alpha) = F(g(\beta)) - F(g(\alpha)) = F(b) - F(a) = \int_a^b f(x)dx.$$

□

We now revisit Taylor's theorem and find an integral form for the remainder.

Theorem 10.6.15 (Taylor's theorem with remainders an integral)**.** Let $f^{(n)}$ be continuous for $x \in [0,h]$, then

$$f(h) = f(0) + f'(0)h + \cdots + \frac{f^{(n-1)}(0)h^{n-1}}{(n-1)!} + R_n \tag{10.6.60}$$

where

$$R_n = \frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(ht)dt. \tag{10.6.61}$$

Remark. Note that here we assume continuity of $f^{(n)}$ and not just existence (as in our previous version), so that theorem is a little weaker, but just practical purposes.

Proof. Let's make the substitution, $u = ht$.

$$\begin{aligned} R_n &= \frac{h^n}{(n-1)!}\int_0^h \left(1-\frac{u}{h}\right)^{n-1} f^{(n)}(u)\frac{du}{h} = \frac{1}{(n-1)!}\int_0^h (h-u)^{n-1} f^{(n)}(u)du \\ &= \frac{1}{(n-1)!}(h-u)^{n-1} f^{(n-1)}\Big|_0^h - \frac{1}{(n-1)!}\int_0^h -(n-1)(h-u)^{n-2} f^{(n-1)}(u)du \\ &= -\frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0) + \frac{1}{(n-2)!}\int_0^h (h-u)^{n-2} f^{(n-1)}(u)du \\ &= -\frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0) + R_{n-1} \end{aligned}$$

Integrate by parts $n-1$ times to get

$$R_n = -\frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0) - \cdots - hf'(0) + \underbrace{\int_0^h f'(u)du}_{f(h)-f(0)}. \tag{10.6.62}$$

Thus, integral form gives back Cauchy's and Lagrange's form. □

Remark. $F(x) = \int_a^x f(t)dt,\ x \in [a,b]$ (f is continuous). The mean value theorem applied to F, $\exists c \in (a,b)$ s.t.

$$f(h) = f(0) + hf'(0) + \cdots + \frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0) + R_n \tag{10.6.63}$$

where

$$R_n = \frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(ht)dt. \tag{10.6.64}$$

Let's apply this to $\int_0^1 (1-t)^{n-1} f^{(n)}(ht)dt$, $\exists \theta \in (0,1)$ s.t.

$$\int_0^1 (1-t)^{n-1} f^{(n)}(ht)dt = (1-\theta)^{n-1} f^{(n)}(\theta h) \Rightarrow\ R_n = \frac{h^n}{(n-1)!}(1-\theta)^{n-1} f^{(n)}(\theta h) \qquad \text{(Cauchy's form)} \tag{10.6.65}$$

To get Lagrange's form we use the following. Suppose $g \geq 0$,

$$\int_a^b f(x)g(x)dx = f(c)\int_a^b g(x)dx, \qquad \text{for some } c \in [a,b]. \tag{10.6.66}$$

Thus,

$$\int_0^1 \underbrace{(1-t)^{n-1}}_{'g'}\underbrace{f^{(n)}(ht)}_{'f'}dt = f^{(n)}(\theta h)\int_0^1 (1-t)^{n-1}dt = f^{(n)}(\theta h)\frac{1}{n} \ \Rightarrow\ R_n = \frac{h^n}{(n)!}f^{(n)}(\theta h) \qquad \text{(Lagrange's form)} \tag{10.6.67}$$

Now we prove the above statement: $f, g : [a,b] \mapsto \mathbb{R}$ are continuous, $g(x) > 0,\ \forall x \in (a,b)$, then $\exists c \in (a,b)$ s.t.

$$\int_a^b f(x)g(x)dx = f(c)\int_a^b g(x)dx. \tag{10.6.68}$$

Proof. Let

$$H(x) = \int_a^x f(t)g(t)dt, \quad G(x) = \int_a^x g(t)dt \tag{10.6.69}$$

By Fundamental theorem of calculus

$$H'(x) = f(x)g(x), \quad G'(x) = g(x) \tag{10.6.70}$$

Cauchy's mean value theorem (Theorem 10.4.13) applied to H and G: $\exists c \in (a,b)$ s.t.

$$G'(c)(H(b) - H(a)) = H'(c)(G(b) - G(a)) \ \Rightarrow \ g(c)\int_a^b f(t)g(t)dt = f(c)g(c)\int_a^b g(t)dt \tag{10.6.71}$$

Since $g(c) \neq 0$, we get the required result. □

10.6.3 Infinite integrals (Improper integrals)

We'd like to sense of $\int_a^\infty f(x)dx$. Suppose we have $f : [a,\infty) \mapsto \mathbb{R}$ s.t. for every $R \geq a$. f is bounded and integrable on $[0,R]$.

Definition 10.6.4. If $\lim_{R\to\infty} \int_a^x f(x)dx = l$ we say that $\int_a^\infty f(x)dx$ exists and that its vlaue is l.

In this case, we also say that $\int_a^\infty f(x)dx$ converges. If $\int_a^\infty f(x)dx$ does not tend to a limit, we say $\int_a^\infty f(x)dx$ diverges.

Example 10.6.16. $\int_1^\infty \frac{dx}{x^k}, \quad f(x) = \frac{1}{x^k}$

$$\int_1^R \frac{dx}{x^k} = \frac{x^{1-k}}{1-k}\bigg|_1^R = \frac{R^{1-k}}{1-k} \tag{10.6.72}$$

If $k \neq 1$, let $R \to \infty$, we say that the limit is finite only if $k > 1$. If $k = 1$, $\int_1^R \frac{dx}{x} = \log R \to \infty$ as $R \to \infty$. So $\int_1^\infty \frac{dx}{x^k}$ iff $k > 1$.

Notice the similarities with $\sum_{n=1}^\infty \frac{1}{n^k} = \sum_{n=1}^\infty f(n)$.

Remark. 1. If $f \geq 0$, $g \geq 0$, for $x \geq a$, and $f(x) \leq Kg(x)$, K is constant, then if $\int_a^\infty g$ converges, then $\int_a^\infty f$ converges and $\int_a^\infty f \leq K\int_a^\infty g$. (analogue of comparison test)

Proof.

$$f(x) \leq Kg(x) \ \Rightarrow \ \int_a^R f(x)dx \leq K\int_a^R g(x)dx \tag{10.6.73}$$

The function $R \mapsto \int_a^R f(x)dx$ is an increasing function.

$$R_1 \geq R_2, \quad \int_a^{R_1} f(x)dx = \int_a^{R_2} f(x)dx + \int_{R_2}^{R_1} f(x)dx \ \Rightarrow \ \int_{R_2}^{R_1} f(x)dx \geq 0. \tag{10.6.74}$$

If $\int_a^\infty g$ converges, then $R \mapsto \int_a^R f$ is bounded above, and so we can consider $\sup_{R\geq a}\int_a^R f(x)dx = l$ and claim $\lim_{R\to\infty}\int_a^R f = l$.

By defintion of supremum, given $\varepsilon > 0$, $\exists R_0$ s.t.

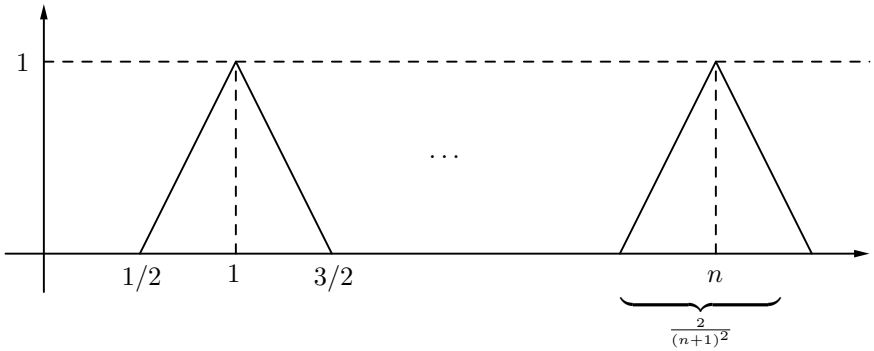
$$\int_a^{R_0} f > l - \varepsilon. \tag{10.6.75}$$

If $R \geq R_0$,

$$\int_a^R f \geq \int_a^{R_0} f \geq l - \varepsilon \ \Rightarrow \ 0 \leq l - \int_a^R f < \varepsilon \ \Rightarrow \ \lim_{R\to\infty}\int_a^R f = l. \tag{10.6.76}$$

□

2. For series, we know if $\sum a_n$ converges then $a_n \to 0$. However, it is not ture that if $\int_a^\infty f$ converges, then $f(x) \to 0$ as $x \to \infty$.



Example 10.6.17. $\sum \frac{1}{(n+1)^2}$ converges $\Rightarrow \int_a^\infty f$ converges, but $f(n) = 1$ for $n \in \mathbb{N}$.

Theorem 10.6.18 (The integral test)**.** $f : [1, \infty) \mapsto \mathbb{R}$ be a positive decreasing function, then
(i) $\int_1^\infty f(x)dx$ and $\sum_{n=1}^\infty f(n)$ both converge or diverge;
(ii) $\sum_{r=1}^n f(r) - \int_1^n f(x)dx$ tends to a limit l as $n \to \infty$, and $0 \le l \le f(1)$.

Proof. Note that since f is decreasing, it is Riemann integrable in every interval $[1, R]$ and

$$f(n-1) \ge \int_{n-1}^n f(x)dx \ge f(n) \;\Rightarrow\; \sum_{r=1}^{n-1} f(r) \ge \int_1^n f(x)dx \ge \sum_{r=2}^n f(r). \tag{10.6.77}$$

Suppose $\int_1^\infty f(x)dx$ converges, then $\int_1^\infty f(x)dx$ is bounded. By the above inequality, $\sum_{r=2}^n f(r)$ is bounded and therefore it must converge by the fundamental axiom (increasing n).

Suppose $\sum_{r=1}^n f(r)$ converges, then $\sum_{r=1}^n f(r)$ is bounded and $\int_1^n f(x)dx$ is bounded, thus since $R \mapsto \int_1^R f(x)dx$ is increasing, $\int_1^\infty f(x)dx$. Thus, proves (i).

For the proof of (ii), let

$$\phi(n) = \sum_{r=1}^n f(r) - \int_1^n f(x)dx \tag{10.6.78}$$

we have

$$\phi(n) - \phi(n-1) = \sum_{r=1}^n f(r) - \int_1^n f(x)dx - \left(\sum_{r=1}^{n-1} f(r) - \int_1^{n-1} f(x)dx\right) = f(n) - \int_{n-1}^n f(x)dx \le 0 \tag{10.6.79}$$

so $\phi(n)$ is decreasing. Also, from the above inequality

$$0 \le \phi(n) \le f(1). \tag{10.6.80}$$

Thus, $\phi(n)$ is a bounded decreasing sequence and therefore it must converge to a limit l with $0 \le l \le f(1)$. □

Example 10.6.19.
1. $\sum_{n=1}^\infty \frac{1}{n^k}$. We just saw that $\int_1^\infty \frac{dx}{x^k}$ converges iff $k > 1$. We can apply the integral test to deduce that

$$\sum_{n=1}^\infty \frac{1}{n^k} \text{ converge iff } k > 1. \tag{10.6.81}$$

2. $\sum_{n=1}^\infty \frac{1}{n \log n}$. Let $f(x) = \frac{1}{x \log x}$, we have

$$\int_2^R \frac{dx}{x \log x} = \log(\log x)|_1^R = \log(\log R) - \log(\log 2) \to \infty \text{ as } R \to \infty. \tag{10.6.82}$$

Thus, it diverges.

Corollary 10.6.20 (Eula's constant)**.**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \to \gamma \text{ as } n \to \infty, \quad 0 \le \gamma \le 1. \tag{10.6.83}$$

Proof. $f(x) = 1/x$ and apply Theorem 10.6.18. □

Remark. 1. Still unknown if γ is rational/irrational;

2. $\gamma \sim 0.577$;

3. $\frac{1}{2} < \gamma < 1$.

Here we prove that $\frac{1}{2} < \gamma < 1$.

Proof.

$$a_n := \int_0^1 \frac{t}{n(n-t)dt}, \quad n \geq 2. \tag{10.6.84}$$

We will derive an estimate for a_n. Let $g(t) = t$, $f(t) = 1/(n-t)$, $\exists c \in (0,1)$,

$$a_n = \frac{1}{n}\frac{1}{n-c}\int_0^1 tdt = \frac{1}{2n(n-c)} < \frac{1}{2n(n-1)} \;\Rightarrow\; 0 < a_n < \frac{1}{2n(n-1)} \tag{10.6.85}$$

Thus,

$$0 < \sum_{n=2}^{N} a_n < \sum_{n=2}^{N} \frac{1}{2n(n-1)} = \frac{1}{2}\sum_{n=2}^{N}\left(\frac{1}{n-1} - \frac{1}{n}\right) = \frac{1}{2}\left(1 - \frac{1}{N}\right) \to \frac{1}{2}. \tag{10.6.86}$$

But a_n can be easily computed integrating by parts. If you do the calculation, you can get

$$a_n = \log\left(\frac{n}{n-1}\right) - \frac{1}{n} \tag{10.6.87}$$

$$\sum_{n=2}^{N} a_n = -\sum_{n=2}^{N}\frac{1}{n} + (\log 2 - \log 1) + (\log 3 - \log 2) + \cdots + (\log N - \log(N-1)) = -\sum_{n=2}^{N}\frac{1}{n} + \log N \to 1 - \gamma. \tag{10.6.88}$$

□

10.6.4 Final remarks on improper integrals

So far we looked at $\int_a^\infty f(x)dx$. We can also make perfect series of $\int_{-\infty}^a f(x)dx$

$$\lim_{R\to\infty}\int_{-R}^{a} f. \tag{10.6.89}$$

We can also make sense of $\int_{-\infty}^{\infty} f(x)dx$.

Definition 10.6.5. $\int_{-\infty}^{\infty} f(x)dx$ converges if $\int_a^\infty f(x)dx$ converges and $\int_{-\infty}^a f(x)dx$ converges. Also, if $\int_a^\infty f(x)dx = l_1$, $\int_{-\infty}^a f(x)dx = l_2$. We let $\int_{-\infty}^{\infty} f(x)dx = l_1 + l_2$.

This definition is independent of a

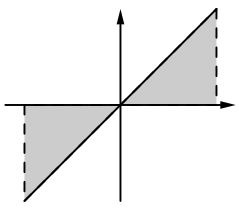
$$\left.\begin{array}{rcl} \int_{a'}^{\infty} f(x)dx & = & \int_{a'}^{a} f(x)dx + \int_{a'}^{\infty} f(x)dx \\ \int_{-\infty}^{a'} f(x)dx & = & \int_{-\infty}^{a} f(x)dx + \int_{a}^{a'} f(x)dx \end{array}\right\} \text{the sume will not change } l_1 + l_2. \tag{10.6.90}$$

Not quite the same as saying that $\lim_{R\to\infty}\int_{-R}^{R} f(x)dx$ exists.

$\lim_{R\to\infty}\int_{-R}^{R} xdx = 0$

but $\int_{-\infty}^{\infty} xdx$ does not exist,

because neither $\int_0^\infty xdx$ or $\int_{-\infty}^0 xdx$



Example 10.6.21.

Example 10.6.22. $f(x) = \frac{1}{\sqrt{x}}$, $x \in (0,1]$. $\delta > 0$,

$$\int_\delta^1 \frac{1}{\sqrt{x}}dx = 2\sqrt{x}|_\delta^1 = 2(1-\delta) \to 2 \text{ as } \delta \to 0. \;\Rightarrow\; \int_0^1 \frac{dx}{\sqrt{x}} = \lim_{\delta\to 0}\int_\delta^1 \frac{1}{\sqrt{x}}dx. \tag{10.6.91}$$

10.6.5 Stirling's formula

Theorem 10.6.23 (Stirling's formula)**.** As $n \to \infty$,

$$\log\left(\frac{n!e^n}{n^{n+\frac{1}{2}}}\right) = \log\left(\sqrt{2\pi}\right) + O(1/n). \tag{10.6.92}$$

Proof. Let $c_n = \log(n!) + n - (n+\frac{1}{2})\log n$, then

$$c_n - c_{n+1} = (n+\tfrac{1}{2})\log(1+1/n) - 1. \qquad (*) \tag{10.6.93}$$

For $0 < x < 1$, if we subtract the two expressions

$$\begin{aligned} \log(1+x) - x &= -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots \qquad (\dagger) \\ \log(1-x) + x &= -\frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \dots \qquad (\dagger\dagger) \end{aligned}$$

and divide by $2x$, we obtain

$$\frac{1}{2x}\log\left(\frac{1+x}{1-x}\right) - 1 = \frac{x^2}{3} + \frac{x^4}{5} + \frac{x^6}{7} + \dots \le \frac{x^2}{3} + \frac{x^4}{3} + \frac{x^6}{3} + \dots = \frac{1}{3}\frac{x^2}{1-x^2}.$$

Now put $x = 1/(2n+1)$ and we see from $(*)$ that the left-hand side of $(\dagger)$ is then $c_n - c_{n+1}$, and furthermore from $(\dagger)$ that $c_n - c_{n+1} \ge 0$ and from $(\dagger\dagger)$ that

$$c_n - c_{n+1} \le \frac{1}{12}\left(\frac{1}{n} - \frac{1}{n+1}\right). \tag{10.6.94}$$

This shows that c_n is monotone non-increasing in n and $c_n - 1/(12n)$ is monotone non-decreasing so that c_n is bounded below and hence converges $c_n \to c$, for some c.

To determine the value of c, define $I_r = \int_0^{\pi/2} \sin^r\theta d\theta$, for $r \ge 0$, so that $I_0 = \pi/2$ and $I_1 = 1$. Integrating by parts for $r > 1$, we have

$$I_r = -[-\sin^{r-1}\theta\cos\theta]_0^{\pi/2} + (r-1)\int_0^{\pi/2} \sin^{r-2}\theta\cos^2\theta d\theta = (r-1)(I_{r-2} - I_r), \tag{10.6.95}$$

so that $rI_r = (r-1)I_{r-2}$. It is immediate that $I_{2n+1} \le I_{2n} \le I_{2n-1}$, hence

$$1 \le \frac{I_{2n}}{I_{2n+1}} \le \frac{I_{2n-1}}{I_{2n+1}} = \frac{2n+1}{2n} \to 1, \quad \text{as } n \to \infty. \tag{10.6.96}$$

Calculate

$$I_{2n} = \frac{2n-1}{2n}I_{2n-2} = \frac{(2n-1)(2n-3)\dots 1}{(2n)(2n-2)\dots 2}I_0 = \frac{(2n)!}{(2^n n!)^2}\frac{\pi}{2}. \tag{10.6.97}$$

$$I_{2n+1} = \frac{2n}{2n+1}I_{2n-1} = \frac{(2n)(2n-2)\dots 2}{(2n+1)(2n-1)\dots 1}I_1 = \frac{(2^n n!)^2}{(2n+1)!}. \tag{10.6.98}$$

Dividing these we see that, as $n \to \infty$,

$$\frac{I_{2n}}{I_{2n+1}} = \frac{(2n+1)((2n)!)^2}{(2^n n!)^4}\frac{\pi}{2} \to 1, \quad \text{or} \quad \frac{(2^n n!)^2}{(2n)!}\frac{1}{\sqrt{n}} \to \sqrt{\pi}. \tag{10.6.99}$$

Now note that

$$2c_n - c_{2n} = \log\sqrt{2} + \log\left(\frac{(2^n n!)^2}{(2n)!}\frac{1}{\sqrt{n}}\right) \to \log\sqrt{2} + \log\sqrt{\pi} = \log 2\pi, \tag{10.6.100}$$

so that $c = \lim_{n\to\infty}(2c_n - c_{2n}) = \log\sqrt{2\pi}$, as required. □

The most common statement of Stirling's formula is given as a corollary.

Corollary 10.6.24. As $n \to \infty$,

$$n! \sim \sqrt{2\pi}e^{-n}n^{n+\frac{1}{2}}, \tag{10.6.101}$$

where, in this context, $\sim$ indicates that the ratio of the two sides tends to 1.

Example 10.6.25. Suppose that $4n$ balls, of which $2n$ are red and $2n$ are black, are put at random into two urns, so that each urn contains $2n$ balls. What is the probability that each urn contains n red balls and n black balls? The probability is

$$p_n = \binom{2n}{n}\binom{2n}{n} \Big/ \binom{4n}{2n} = \left(\frac{(2n)!}{n!}\right)^4 \frac{1}{(4n)!} \sim \left(\frac{\sqrt{2\pi}e^{-2n}(2n)^{2n+\frac{1}{2}}}{\sqrt{2\pi}e^{-n}n^{n+\frac{1}{2}}}\right)^4 \frac{1}{\sqrt{2\pi}e^{-4n}(4n)^{4n+\frac{1}{2}}} = \sqrt{\frac{2}{\pi n}} = a_n.$$

We may calculate the exact probability p_n, its approximant a_n from Stirling's formula and their ratio for different values of n.

n	1	10	13	20	40	60	100
p_n	0.667	0.248	0.218	0.177	0.126	0.103	0.080
a_n	0.798	0.252	0.221	0.178	0.126	0.103	0.080
p_n/a_n	0.836	0.981	0.986	0.991	0.995	0.997	0.998

The case $n = 13$ corresponds to dividing a standard pack of cards in two and obtaining equal numbers of red and black cards in each half.

10.7 Euclidean Space

Definition 10.7.1. [12]

10.8 Norms

Definition 10.8.1 (norm)**.** Let V be a vector space. A map $v \mapsto \|v\| : V \to [0, \infty)$ is a norm[13] if

(i) $\|u\| \geq 0$ for all $u \in V$,

(ii) $\|v\| = 0$ implies $v = 0$,

(iii) $\|\alpha v\| = |\alpha| \, \|v\|$ for all $v \in V$ and $\alpha \in \mathbb{R}$,

(iv) $\|u + v\| \leq \|u\| + \|v\|$ for all $u, v \in V$.

Remark. We note that, for any norm, if $\|v_n - v\| \to 0$ then $\|v_n\| \to \|v\|$.

10.9 Inner Product

Definition 10.9.1 (inner product)**.** A symmetric bilinear map $(u, v) \to \langle u, v\rangle : V \times V \to \mathbb{R}$ is an inner product[14] if $\langle v, v\rangle \geq 0$, with equality only if $v = 0$. For any inner product, $\langle \cdot, \cdot \rangle$, the map $v \mapsto \sqrt{\langle v, v\rangle}$ is a norm, by the Cauchy-Schwarz inequality.

10.10 Function Sequences

Definition 10.10.1 (uniform convergence)**.** Suppose X is a set and $f_n : X \to \mathbb{R}$ is a real-valued function for every natural number n. We say that the sequence $(f_n)_{n\in\mathbb{N}}$ is uniformly convergent with limit $f : X \to \mathbb{R}$ if for every $\varepsilon > 0$, there exists a natural number N such that for all $x \in X$ and all $n \geq N$ we have $|f_n(x)f(x)| < \varepsilon$[15].

Remark. Consider the sequence $a_n = \sup x \in X \, |f_n(x)f(x)|$. Clearly f_n converges to f uniformly if and only if a_n tends to 0.

Definition 10.10.2 (locally uniform convergence)**.**] Suppose X is a set and $f_n : X \to \mathbb{R}$ is a real-valued function for every natural number n. We say that the sequence $(f_n)_{n\in\mathbb{N}}$ is uniformly convergent with limit $f : X \to \mathbb{R}$ if for every $x \in X$, there exists $r > 0$ such that f_n converges uniformly on $(x - r, x + r) \cap X$[16].

[12] need definition
[13] need checking
[14] need checking
[15] can be extended to metric space
[16] can be extended to metric space

Example 10.10.1. [17] Let $a_n(x) = \frac{\sin(n\pi x)}{n^2}$ and thus $a_n'(x) = \frac{\pi\cos(n\pi x)}{n}$. Then

$$\left|\sum_n a_n(x)\right| \le \sum_n \frac{1}{n^2} \;\Rightarrow\; \sum_n a_n(x) \text{ converges.} \tag{10.10.1}$$

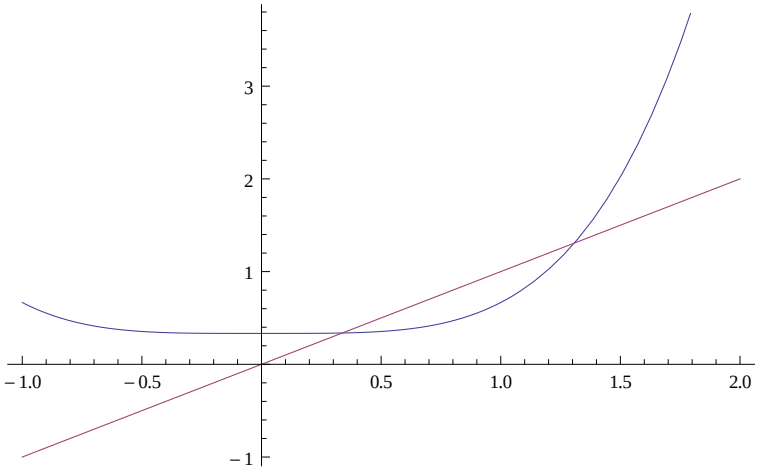
However, at $x = 0$,

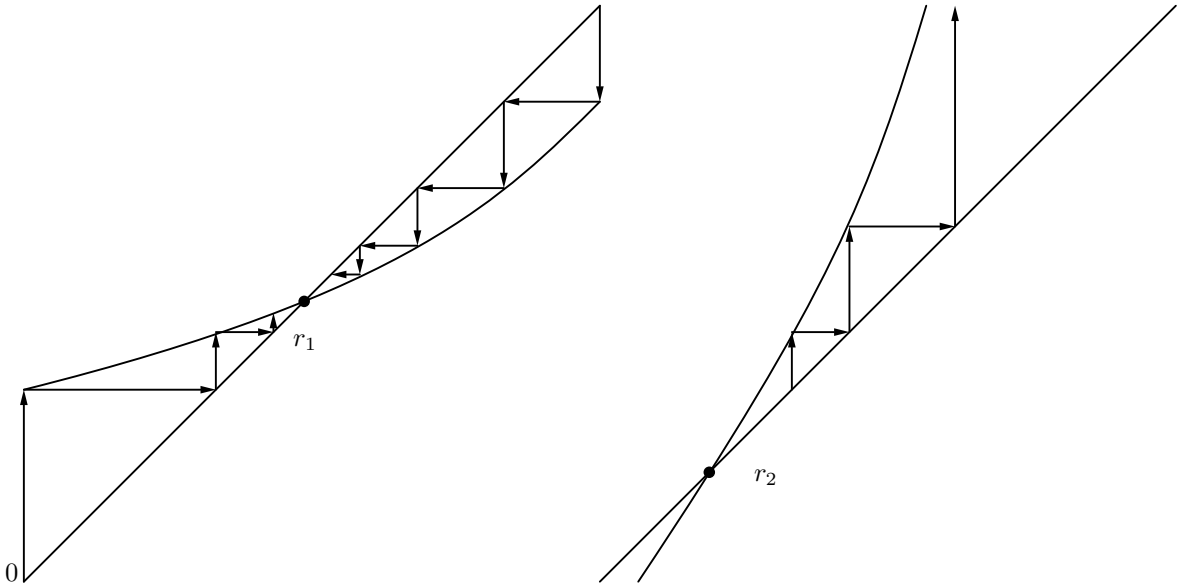
$$\left|\sum_n a_n'(x)\right| = \sum_n \frac{1}{n} \;\Rightarrow\; \sum_n a_n'(x) \text{ diverges.} \tag{10.10.2}$$

10.11 Problems

Problem 10.11.1. Sketch the graph of $y = x$ and $y = (x^4 + 1)/3$, and thereby illustrate the behaviour of the real sequence a_n where $a_{n+1} = (a_n^4 + 1)/3$. For which of the three starting cases $a_1 = 0$, $a_1 = 1$ and $a_1 = 2$ does the sequence converge? Now prove your assertion.

Solution. First, we plot the diagram





Let the two roots of $f(x) = (x^4 + 1)/3 - x$ be r_1 and r_2 ($r_1 < r_2$). Because $f(0) > 0$, $f(1) < 0$ and $f(2) > 0$, we have $r_1 \in (0, 1)$ and $r_2 \in (1, 2)$.

Graphical analysis tells us that sequences starting with $a_1 = 0, 1$ converge to r_1 and $a_1 = 2$ diverges to infinity.

$a_1 = 0$. If $a_n \in (0, r_1)$, $f(a_n) = (a_n^4 + 1)/3 - a_n = a_{n+1} - a_n > 0 \;\Rightarrow\; a_{n+1} > a_n$. But

$$a_{n+1} = (a_n^4 + 1)/3 < (r_1^4 + 1)/3 = r_1 \tag{10.11.1}$$

[17] could be placed at absolute uniform-convergence series

Thus, a_n is increasing and bounded above so it is converging.

$a_1 = 1$. If $a_n \in (r_1, r_2)$, $f(a_n) = (a_n^4 + 1)/3 - a_n = a_{n+1} - a_n < 0 \ \Rightarrow \ a_{n+1} < a_n$. But

$$a_{n+1} = (a_n^4 + 1)/3 > (r_1^4 + 1)/3 = r_1 \tag{10.11.2}$$

Thus, a_n is decreasing and bounded above so it is converging.

$a_1 = 2$. If $a_n \in (r_2, \infty)$, $f(a_n) = (a_n^4 + 1)/3 - a_n = a_{n+1} - a_n > 0 \ \Rightarrow \ a_{n+1} > a_n$. Thus, a_n is increasing and unbounded above so it is diverging.

Problem 10.11.2. Let $a_1 > b_1 > 0$ and let $a_{n+1} = (a_n + b_n)/2$, $b_{n+1} = 2a_n b_n/(a_n + b_n)$ for $n \geq 1$. Show that $a_n > a_{n+1} > b_{n+1} > b_n$ and deduce the two sequences converge to a common limit. What limit?

Solution. Since $a_1 > b_1 > 0$,

$$\begin{cases} 2a_1 > a_1 + b_1 \ \Rightarrow \ a_1 > \frac{a_1+b_1}{2} = a_2 \\ \frac{1}{a_1} < \frac{1}{b_1} \ \Rightarrow \ \frac{1}{a_1} + \frac{1}{b_1} < \frac{2}{b_1} \ \Rightarrow \ b_1 < \frac{2}{\frac{1}{a_1}+\frac{1}{b_1}} = b_2 \quad \Rightarrow \ a_1 > a_2 > b_2 > b_1. \\ a_2 - b_2 = \frac{a_1+b_1}{2} - \frac{2a_1b_1}{a_1+b_1} = \frac{(a_1-b_1)^2}{2(a_1+b_1)} > 0 \end{cases} \tag{10.11.3}$$

By induction, we have $a_n > a_{n+1} > b_{n+1} > b_n$. Since a_n is a decreasing sequence, and bounded below (by 0), thus a_n converges to a. Similarly, b_n is an increasing sequence and bounded above (by a_1). Thus,

$$\begin{cases} a = \frac{a+b}{2} \\ b = \frac{2ab}{a+b} \end{cases} \quad \Rightarrow \ a = b. \tag{10.11.4}$$

which means that a_n and b_n converge to a common limit c. We know that

$$a_{n+1}b_{n+1} = (a_n + b_n)/2 \times 2a_n b_n/(a_n + b_n) = a_n b_n \ \Rightarrow \ c^2 = a_1 b_1 \ \Rightarrow \ c = \sqrt{a_1 b_1}. \tag{10.11.5}$$

Chapter 11

Complex Analysis

Theorem 11.0.3 (Cauchy's residue theorem)**.** [1]

Example 11.0.4.

$$\lim_{N\to\infty}\int_{-N}^{N}\frac{\sin x}{x}dx=\pi. \tag{11.0.1}$$

Example 11.0.5.

$$\int_{-\infty}^{\infty}\frac{\sin^2 x}{x^2}dx=\pi. \tag{11.0.2}$$

[1] need statement.

Chapter 12

Metric Space

Definition 12.0.1 (metric, metric space)**.** A metric on a set X is a function (called the distance function or simply distance) $d : X \times X \to \mathbb{R}$ (where $\mathbb{R}$ is the set of real numbers). For all $x, y, z \in X$, this function is required to satisfy the following conditions:

(i) $d(x, y) \geq 0$. (non-negativity, or separation axiom)

(ii) $d(x, y) = 0$ if and only if $x = y$. (identity of indiscernibles, or coincidence axiom)

(iii) $d(x, y) = d(y, x)$. (symmetry)

(iv) $d(x, z) \leq d(x, y) + d(y, z)$. (subadditivity / triangle inequality)

Then (X, d) is called metric space.

Remark. Note that (i) and (ii) together produce positive definiteness and (i) is implied by the others.

Definition 12.0.2 (ultrametric)**.** A metric is called an ultrametric if it satisfies the following stronger version of the triangle inequality where points can never fall 'between' other points:

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}, \quad \forall x, y, z \in X. \tag{12.0.1}$$

Definition 12.0.3 (intrinsic metric)**.** A metric d on X is called intrinsic if any two points $x, y \in X$ can be joined by a curve with length arbitrarily close to $d(x, y)$.

Definition 12.0.4 (translation invariant metric)**.** For sets on which an addition $+ : X \times X \to X$ is defined, d is called a translation invariant metric if

$$d(x, y) = d(x + a, y + a), \quad x, y \in X. \tag{12.0.2}$$

Definition 12.0.5 (pseudometric)**.** A pseudometric on X is a function $d : X \times X \to \mathbb{R}$ which satisfies the axioms for a metric, except that instead of the second (identity of indiscernibles) only $d(x, x) = 0$ for all x is required. In other words, the axioms for a pseudometric are: for any $x, y, z \in X$,

(i) $d(x, y) \geq 0$.

(ii) $d(x, x) = 0$ (but possibly $d(x, y) = 0$ for some distinct values $x \neq y$).

(iii) $d(x, y) = d(y, x)$.

(iv) $d(x, z) \leq d(x, y) + d(y, z)$.

Remark. This is the most common generalization of metrics. In some contexts, pseudometrics are referred to as semimetrics because of their relation to seminorms[1].

Definition 12.0.6 (quasimetric)**.** A quasimetric is defined as a function that satisfies all axioms for a metric with the possible exception of symmetry:

[1] need details

(i) $d(x, y) \geq 0$. (positivity)

(ii) $d(x, y) = 0$ if and only if $x = y$. (positive definiteness)

(iii) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality)

Remark. Quasimetrics are common in real life. For example, given a set X of mountain villages, the typical walking times between elements of X form a quasimetric because travel up hill takes longer than travel down hill. Another example is a taxicab geometry topology having one-way streets, where a path from point A to point B comprises a different set of streets than a path from B to A. Nevertheless, this notion is rarely used in mathematics, and its name is not entirely standardized (see Rolewicz [13]).

Example 12.0.6. A quasimetric on the reals can be defined by setting

$$d(x, y) = \begin{cases} x - y & x \geq y, \\ 1 & \text{otherwise} \end{cases} \tag{12.0.3}$$

The 1 may be replaced by infinity or by $1 + 10(y - x)$.

The topological space underlying this quasimetric space is the Sorgenfrey line. This space describes the process of filing down a metal stick: it is easy to reduce its size, but it is difficult or impossible to grow it.

Example 12.0.7. If d is a quasimetric on X, a metric d' on X can be formed by taking

$$d'(x, y) = (d(x, y) + d(y, x))/2. \tag{12.0.4}$$

Definition 12.0.7 (semimetric)**.** A semimetric on X is a function $d : X \times X \to \mathbb{R}$ that satisfies the first three axioms, but not necessarily the triangle inequality:

(i) $d(x, y) \geq 0$.

(ii) $d(x, y) = 0$ if and only if $x = y$.

(iii) $d(x, y) = d(y, x)$.

Remark. Some mathematicians work with a weaker form of the triangle inequality, such as:

$$d(x, z) \leq \rho(d(x, y) + d(y, z)) \qquad (\rho\text{-relaxed triangle inequality})$$
$$d(x, z) \leq \rho \max\{d(x, y), d(y, z)\} \qquad (\rho\text{-inframetric inequality}).$$

Definition 12.0.8 (topologically equivalent metrics)**.** [2]

Definition 12.0.9 (Lipschitz equivalent metrics)**.** Two metrics d_1, d_2 on a set X are called Lipschitz equivalent if there are positive constants k, K such that for any $x, y \in X$,

$$k d_2(x, y) \leq d_1(x, y) \leq K d_2(x, y). \tag{12.0.5}$$

Proposition 12.0.8. [3] Lipschitz equivalent metrics are topologically equivalent.

Theorem 12.0.9. [4] If (X, d) is a metric space, then the following statements are true.

(i) The empty set $\emptyset$ and the space X are open.

(ii) If U_α is open for all $\alpha \in A$, then $\bigcup_{\alpha \in A} U_\alpha$ is open. (In other words, the union of open sets is open.)

(iii) If U_j is open for all $1 \leq j \leq n$, then $\bigcap_{j=1}^{n} U_j$ is open.

Proof. [5]

[2] see Metric and Topological Space
[3] need checking
[4] need checking
[5] need checking

(i) Since there are no points e in $\emptyset$, the statement $x \in \emptyset$ whenever $d(x,e) < 1$ holds for all $e \in \emptyset$. Since every point x belongs to X, the statement $x \in X$ whenever $d(x,e) < 1$ holds for all $e \in X$.

(ii) If $e \in \bigcup_{\alpha\in A} U_\alpha$, then we can find a particular $\alpha_1 \in A$ with $e \in U_{\alpha_1}$. Since U_{α_1} is open, we can find a $\delta > 0$ such that $x \in U_{\alpha_1}$ whenever $d(x,e) < \delta$.

Since $U_{\alpha_1} \subseteq \bigcup_{\alpha\in A} U_\alpha$, $x \in \bigcup_{\alpha\in A} U_\alpha$whenever $d(x,e) < \delta$. Thus $\bigcup_{\alpha\in A} U_\alpha$ is open.

(iii) If $e \in \bigcap_{j=1}^n U_j$ then $e \in U_j$ for each $1 \le j \le n$. Since U_j is open, we can find a $\delta_j > 0$ such that $x \in U_j$ whenever $d(x,e) < \delta_j$. Setting $\delta = \min_{1\le j\le n} \delta_j$, we have $\delta > 0$ and $x \in U_j$ whenever $d(x,e) < \delta$ for all $1 \le j \le n$. Thus

$$x \in \bigcap_{j=1}^{n} U_j \text{ whenever } d(x,e) < \delta \tag{12.0.6}$$

and we have shown that $\bigcap_{j=1}^n U_j$ is open.

□

Definition 12.0.10. [6] Given two metric spaces (X, d_X) and (Y, d_Y), where d_X denotes the metric on the set X and d_Y is the metric on set Y. A function $f : X \to Y$ is called Lipschitz continuous if there exists a real constant $K \ge 0$ such that, for all x_1 and x_2 in X,

$$d_Y(f(x_1), f(x_2)) \le K d_X(x_1, x_2). \tag{12.0.7}$$

Any such K is referred to as a Lipschitz constant for the function f. The smallest constant is sometimes called the (best) Lipschitz constant. The space of Lipschitz continuous functions with constant K is $\mathrm{Lip}_K(X,Y)$ and the space of Lipschitz continous functions on X is $\mathrm{Lip}(X,Y) = \bigcup_{K>0} \mathrm{Lip}_K(X,Y)$.

Remark. [7] Lipschitz continuity is a strong form of uniform continuity.

Lemma 12.0.10. [8] Let (X,d) be a metric space. For any closed set $A \subseteq X$ and any $\varepsilon > 0$, there is a Lipschitz continuous map $\rho_{A,\varepsilon} : X \to [0,1]$ with

$$\rho_{A,\varepsilon}(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } d(x,A) \ge \varepsilon. \end{cases} \tag{12.0.8}$$

Proof. [9] Let $\varphi : \mathbb{R} \to [0,1]$, $t \mapsto (t \vee 0) \wedge 1$. For $x \in X$, define $\rho_{A,\varepsilon} = 1 - \varphi(\varepsilon^{-1} d(x,A))$. □

[6] need checking
[7] need checking
[8] need checking
[9] need checking

Chapter 13

Topological Space

13.1 Topology

13.1.1 Topology and topological space

Definition 13.1.1 (topology, topological space)**.** A topological space $T = (X, \mathcal{T})$ consists of a non-empty set X together with a fixed family $\mathcal{T}$ of subsets of X satisfying

(i) $X, \emptyset \in \mathcal{T}$,

(ii) the intersection of finitely many sets in $\mathcal{T}$ is in $\mathcal{T}$,

(iii) the union of any collection of sets in $\mathcal{T}$ is in $\mathcal{T}$.

The family $\mathcal{T}$ is called a topology for X.

Remark. Note that the collection can be uncountable in (iii).

Definition 13.1.2 (open set in topological space)**.** Let $T = (X, \mathcal{T})$ be a topological space. Then the members of sT are called the open sets of T.

Definition 13.1.3 (continuous topological space)**.** We say that $f : E \to \mathbb{R}$ is continuous, if $f^{-1}(U)$ is open in E whenever U is open in $\mathbb{R}$.

13.2 Spaces

Definition 13.2.1 (second-countable space)**.** A second-countable space, also called a completely separable space, is a topological space satisfying the second axiom of countability[1].

A space is said to be second-countable if its topology has a countable base. More explicitly, this means that a topological space X is second countable if there exists some countable collection $\mathcal{U} = \{U_i\}_{i=1}^{\infty}$ of open subsets of X such that any open subset of X can be written as a union of elements of some subfamily of $\mathcal{U}$.

Remark. Like other countability axioms, the property of being second-countable restricts the number of open sets that a space can have.

13.3 Function Sequence

Definition 13.3.1 (convergence on compact)**.** Let $(X, \mathcal{T})$ be a topological space and (Y, d_Y) be a metric space. A sequence of functions

$$f_n : X \to Y, \quad n \in \mathbb{N}, \tag{13.3.1}$$

is said to converge on compact (or converge compactly) as $n \to \infty$ to some function $f : X \to Y$ if, for every compact set $K \subseteq X$, $\forall x \in K$,

$$\lim_{n\to\infty} d_Y\left(f_n(x), f(x)\right) = 0. \tag{13.3.2}$$

[1] need details

Definition 13.3.2 (uniform convergence on compacts)**.** Let $(X, \mathcal{T})$ be a topological space and (Y, d_Y) be a metric space. A sequence of functions

$$f_n : X \to Y, n \in \mathbb{N}, \tag{13.3.3}$$

is said to converge uniformly on compacts (or converge uniformly compactly) as $n \to \infty$ to some function $f : X \to Y$ if, for every compact set $K \subseteq X$,

$$\lim_{n\to\infty} \sup_{x\in K} d_Y\left(f_n(x), f(x)\right) = 0. \tag{13.3.4}$$

Chapter 14

Linear Analysis

Theorem 14.0.1 (arithmetic-geometric mean inequality)**.** For positive real numbers $x_1, \ldots, x_n$,

$$\left(\prod_{i=1}^{n} x_i\right)^{1/n} \leq \frac{1}{n}\sum_{i=1}^{n} x_i. \tag{14.0.1}$$

Proof. See Example 19.3.23. □

Definition 14.0.3 (Banach space)**.**

Theorem 14.0.2 (Stone-Weierstrass theorem)**.** Suppose X is a compact Hausdorff space and $\mathcal{A}$ is a subalgebra of $C(X)$ which contains a non-zero constant function. Then A is dense in $C(X)$ if and only if it separates points, i.e., $\forall x \in X$, there exist elements $f, g \in \mathcal{A}$ such that $f(x) \neq g(x)$.

Proof. see [11].II80 □

Corollary 14.0.3 (Weierstrass' approximation theorem)**.** Since the polynomials on $[a, b]$ form a subalgebra of $C[a, b]$, $\mathcal{A}$, which contains the constants and separates points, $\mathcal{A}$ is dense.

Chapter 15

Measure Theory

15.1 Set Systems and Measures

15.1.1 Set systems

In this chapter, we denote E as a set. Then we have the following definitions.

Definition 15.1.1. Let $\mathcal{A}$ be a set of subsets of E. Say that $\mathcal{A}$ is an algebra on E if for all $A, B \in \mathcal{A}$

$$\text{(i) } \emptyset \in \mathcal{A} \qquad \text{(ii) } A^c = E \backslash A \in \mathcal{A} \qquad \text{(iii) } A \cup B \in \mathcal{A}. \tag{15.1.1}$$

Definition 15.1.2 (σ-algebra)**.** Let $\mathcal{E}$ be a set of subsets of E. Say that $\mathcal{E}$ is a σ-algebra on E if for all countable sequences $(A_n : n \in \mathbb{N}) \in \mathcal{E}$ and $A \in \mathcal{E}$,

$$\text{(i) } \emptyset \in \mathcal{E} \qquad \text{(ii) } A^c = E \backslash A \in \mathcal{E} \qquad \text{(iii) } \bigcup_n A_n \in \mathcal{E}. \tag{15.1.2}$$

Remark. $\bigcap_{i \in I} \mathcal{F}_i$ is still a σ-albebra, but $\bigcup_{i \in I} \mathcal{F}_i$ is not in general. Note I can be uncountable.

Definition 15.1.3 (measurable space)**.** The pair $(E, \mathcal{E})$ is called a measurable space. Given $(E, \mathcal{E})$, each $A \in \mathcal{E}$ is called a measurable set.

Definition 15.1.4. A separable (or countably generated) σ-algebra (or separable σ-field) is a σ-algebra that can be generated by a countable collection of sets, i.e. for the separable σ-algebra $\mathcal{F}$, there are countable sets $A_1, A_2, \ldots$ such that $\mathcal{F} = \sigma(A_1, A_2, \ldots)$.

Definition 15.1.5 (π-system)**.** Let $\mathcal{A}$ be a set of subsets of E. Say that $\mathcal{A}$ is a π-system on E if for all $A, B \in \mathcal{A}$

$$\text{(i) } \emptyset \in \mathcal{A} \qquad \text{(ii) } A \cap B \in \mathcal{A}. \tag{15.1.3}$$

Remark. $\bigcup_{i \in I} \mathcal{F}_i$ is a π-system. Note I can be uncountable.

Definition 15.1.6 (d-system)**.** Let $\mathcal{A}$ be a set of subsets of E. Say that $\mathcal{A}$ is a d-system on E if for all $A, B \in \mathcal{A}$ with $A \subseteq B$ and all increasing sequences $(A_n)_{n \in \mathbb{N}}$ in $\mathcal{A}$, i.e., $\forall A_1, A_2, \ldots, \in \mathcal{A} : A_1 \subseteq A_2 \subseteq \ldots$

$$\text{(i) } E \in \mathcal{A} \qquad \text{(ii) } B \backslash A \in \mathcal{A} \qquad \text{(iii) } \bigcup_n A_n \in \mathcal{A}. \tag{15.1.4}$$

Lemma 15.1.1. If $\mathcal{E}$ is both a π-system and a d-system, then $\mathcal{E}$ is a σ-algebra.

Proof. ($\Leftarrow$) If $\mathcal{E}$ is a σ-algebra, $\forall A, B \in \mathcal{A}$, $\forall A_1, A_2, \ldots, \in \mathcal{A} : A_1 \subseteq A_2 \subseteq \ldots$ (increasing sequence). Thus, by definition of σ-algebra (Definition 15.1.2).

$$E \in \mathcal{E},\ A^c \in \mathcal{E},\ B^c \in \mathcal{E},\ A^c \cup B^c \in \mathcal{E},\ \bigcup_n A_n \in \mathcal{E}. \tag{15.1.5}$$

Thus,

$$\text{(i) } \emptyset \in \mathcal{E}, \quad \text{(ii) } A \cap B = (A^c \cup B^c)^c \in \mathcal{E}, \qquad \Rightarrow \quad \mathcal{E} \text{ is } \pi\text{-system.} \tag{15.1.6}$$

Also, if $A \subseteq B$,

$$\text{(i) } E \in \mathcal{E}, \quad \text{(ii) } B\backslash A = B \cap A^c = (A \cup B^c)^c \in \mathcal{E}, \quad \text{(iii) } \bigcup_n A_n \in \mathcal{E} \qquad \Rightarrow \quad \mathcal{E} \text{ is } d\text{-system.} \tag{15.1.7}$$

($\Rightarrow$) Suppose that $\mathcal{E}$ is both a π-system and a d-system on a set E. Then, we know that

(i) $\emptyset = E\backslash E \in \mathcal{E}$ (since $\mathcal{E}$ is a d-system $\Rightarrow$ for $A = B = E \in \mathcal{E}$, $A \subseteq B$, $B\backslash A \in \mathcal{E}$)

(ii) $A \in \mathcal{E} \Rightarrow A^c \in \mathcal{E}$ (since $\mathcal{E}$ is a d-system $\Rightarrow$ for $B = E \in \mathcal{E}$, $\forall A \subseteq B$, $B\backslash A = A^c \in \mathcal{E}$)

(iii) $\forall (A_n : n \in \mathbb{N}) \in \mathcal{E}$, we set

$$B_n = \bigcup_{m \le n} A_m = \left(\bigcap_{m \le n} A_m^c \right)^c \tag{15.1.8}$$

Since $\mathcal{E}$ is a d-system, we have that $A_m^c \in \mathcal{E}$. Also, $\bigcap_{m\le n} A_m^c \in \mathcal{E}$ since $\mathcal{E}$ is π-system. Consequently, $B_n = \left(\bigcap_{m\le n} A_m^c\right)^c \in \mathcal{E}$. We know that $\bigcup_n A_n = \bigcup_n B_n$ and B_n is an increasing sequence. Since $\mathcal{E}$ is a d-system, for the increasing sequence $B_n \in \mathcal{E}$, we have

$$\bigcup_n B_n \in \mathcal{E} \;\Rightarrow\; \bigcup_n A_n \in \mathcal{E} \tag{15.1.9}$$

Thus, (i), (ii) and (iii) imply that $\mathcal{E}$ is a σ-algebra. □

Definition 15.1.7. Let $\mathcal{A}$ be a set of subsets of E. Define

$$\sigma(\mathcal{A}) = \{A \subseteq E : A \in \mathcal{E} \text{ for all } \sigma\text{-algebra } \mathcal{E} \text{ containing } \mathcal{A}\}. \tag{15.1.10}$$

Then $\sigma(\mathcal{A})$ is a σ-algebra, which is called the σ-algebra generated by $\mathcal{A}$. It is the smallest σ-algebra containing $\mathcal{A}$.

Proposition 15.1.2. The intersection of d-systems containing a set of subsets $\mathcal{A}$, is also a d-system.

Proof. For the set E, we have $\mathcal{D}$, the intersection of all d-system.

(i) $E \in \mathcal{D}'$ for any d-system $\mathcal{D}'$, then $E \in \mathcal{D}$.

(ii) For all $A, B \in \mathcal{D}$ with $A \subseteq B$, we have for any d-system $\mathcal{D}'$, $\mathcal{D} \subseteq \mathcal{D}'$. Then

$$A, B \in \mathcal{D}' \;\Rightarrow\; B\backslash A \in \mathcal{D}' \;\Rightarrow\; B\backslash A \in \mathcal{D}. \tag{15.1.11}$$

(iii) For all increasing sequences $(A_n : n \in \mathbb{N}) \in \mathcal{D}$, we have for any d-system $\mathcal{D}'$, $\mathcal{D} \subseteq \mathcal{D}'$. Then

$$(A_n : n \in \mathbb{N}) \in \mathcal{D}' \;\Rightarrow\; \bigcup_n A_n \in \mathcal{D}' \;\Rightarrow\; \bigcup_n A_n \in \mathcal{D}. \tag{15.1.12}$$

Thus, we have $\mathcal{D}$ is also a d-system. □

Lemma 15.1.3 (Dynkin's Lemma)**.** Let $\mathcal{A}$ be a π-system. Then any d-system containing $\mathcal{A}$ also contains the σ-algebra generated by $\mathcal{A}$.

Proof. Denote by $\mathcal{D}$ the intersection of all d-systems containing $\mathcal{A}$, then $\mathcal{D}$ itself is a d-system (by proposition 15.1.2).

We shall show that $\mathcal{D}$ is also a π-system and hence a σ-algebra, thus proving the lemma. Consider

$$\mathcal{D}' = \{B \in \mathcal{D} : A \cap B \in \mathcal{D} \text{ for all } A \in \mathcal{A}\}. \qquad (\mathcal{D}' \subseteq \mathcal{D}) \tag{15.1.13}$$

Then $\mathcal{A} \subseteq \mathcal{D}'$ because $\mathcal{A}$ is a π-system ($\forall B \in \mathcal{A} \subseteq \mathcal{D}$, for all $A \in \mathcal{A}$, $A \cap B \in \mathcal{A} \subseteq \mathcal{D}$). Let us check that $\mathcal{D}'$ is a d-system,

(i) $E \in \mathcal{D}$ since $\mathcal{D}$ is a d-system and $E \cap A = A \in \mathcal{A} \subseteq \mathcal{D}$ for all $A \in \mathcal{A}$. Thus, $E \in \mathcal{D}'$.

(ii) Suppose $B_1, B_2 \in \mathcal{D}'$ with $B_1 \subseteq B_2$, then $B_1, B_2 \in \mathcal{D} \;\Rightarrow\; B_2\backslash B_1 \in \mathcal{D}$ since $\mathcal{D}' \subseteq \mathcal{D}$ and $\mathcal{D}$ is a d-system. Also for all $A \in \mathcal{A}$,

$$A \cap (B_2\backslash B_1) = (\underbrace{A \cap B_2}_{\in \mathcal{D}})\backslash(\underbrace{A \cap B_1}_{\in \mathcal{D}}) \in \mathcal{D} \tag{15.1.14}$$

since $\mathcal{D}$ is a d-system, so $B_2 \backslash B_1 \in \mathcal{D}'$.

(iii) If $B_n \in \mathcal{D}'$, $n \in \mathbb{N}$ and $B_n \uparrow B$, then for all $A \in \mathcal{A}$ we have $A \cap B_n \uparrow A \cap B$. Thus, $B \in \mathcal{D}$ and $A \cap B \in \mathcal{D}$ and hence $B \in \mathcal{D}'$.

Combine the fact that $\mathcal{D}'$ is a d-system, $\mathcal{D}$ is a intersection of all d-system and $\mathcal{D}' \subseteq \mathcal{D}$, we have $\mathcal{D} = \mathcal{D}'$.

Now we consider

$$\mathcal{D}'' = \{B \in \mathcal{D} : A \cap B \in \mathcal{D} \text{ for all } A \in \mathcal{D}\}. \qquad (\mathcal{D}'' \subseteq \mathcal{D}) \tag{15.1.15}$$

Then $\mathcal{A} \subseteq \mathcal{D}''$ by definition of $\mathcal{D}'$ and $\mathcal{D}''$ ($\forall B \in \mathcal{A} \subseteq \mathcal{D}$, for all $A \in \mathcal{D}'(= \mathcal{D})$, $A \cap B \in \mathcal{D}$). Let us check that $\mathcal{D}''$ is also a d-system,

(i) $E \in \mathcal{D}$ since $\mathcal{D}$ is a d-system and $E \cap A = A \in \mathcal{D}$ for all $A \in \mathcal{D}$. Thus, $E \in \mathcal{D}''$.

(ii) Suppose $B_1, B_2 \in \mathcal{D}''$ with $B_1 \subseteq B_2$, then $B_1, B_2 \in \mathcal{D} \Rightarrow B_2 \backslash B_1 \in \mathcal{D}$ since $\mathcal{D}'' \subseteq \mathcal{D}$ and $\mathcal{D}$ is a d-system. Also for all $A \in \mathcal{D}$,

$$A \cap (B_2 \backslash B_1) = (\underbrace{A \cap B_2}_{\in \mathcal{D}}) \backslash (\underbrace{A \cap B_1}_{\in \mathcal{D}}) \in \mathcal{D} \tag{15.1.16}$$

since $\mathcal{D}$ is a d-system, so $B_2 \backslash B_1 \in \mathcal{D}''$.

(iii) If $B_n \in \mathcal{D}''$, $n \in \mathbb{N}$ and $B_n \uparrow B$, then for all $A \in \mathcal{D}$ we have $A \cap B_n \uparrow A \cap B$. Thus, $B \in \mathcal{D}$ and $A \cap B \in \mathcal{D}$ and hence $B \in \mathcal{D}''$.

Combine the fact that $\mathcal{D}''$ is a d-system, $\mathcal{D}$ is a intersection of all d-system and $\mathcal{D}'' \subseteq \mathcal{D}$, we have $\mathcal{D} = \mathcal{D}''$. That is,

$$\mathcal{D} = \{B \in \mathcal{D} : A \cap B \in \mathcal{D} \text{ for all } A \in \mathcal{D}\}. \tag{15.1.17}$$

This result shows that $\emptyset \in \mathcal{D}$ and for all $A, B \in \mathcal{D}$, $A \cap B \in \mathcal{D}$. Thus $\mathcal{D}$ is a π-system as promised. □

Definition 15.1.8 (ring)**.** Let $\mathcal{A}$ be a set of subsets of E. Say that $\mathcal{A}$ is a ring on E if for all $A, B \in \mathcal{A}$

$$\text{(i) } \emptyset \in \mathcal{A} \qquad \text{(ii) } B \backslash A \in \mathcal{A} \qquad \text{(iii) } A \cup B \in \mathcal{A}. \tag{15.1.18}$$

Remark. If $\mathcal{A}$ is a ring on E, for all $A, B \in \mathcal{A}$, recalling Definition 2.2.3, we have $A \triangle B \in \mathcal{A}$. Thus

$$A \cap B = (A \cup B) \backslash (A \triangle B) \in \mathcal{A}, \tag{15.1.19}$$

so any ring is also stable by intersection. Thus, any ring is also a π-system.

Definition 15.1.9. Let $(E, \mathcal{T})$ be a topological space. The σ-algebra generated by the set of open sets in E is called the Borel σ-algebra of E and is denoted $\mathcal{B}(E)$, which is the smallest σ-algebra contains all the open sets.

$(E, \mathcal{B}(E))$ is called Borel measurable space.

Remark. Obviously, $\mathcal{T} \subseteq \mathcal{B}(E)$. The Borel σ-algebra of $\mathbb{R}$ is denoted by $\mathcal{B}(\mathbb{R})$.

Lemma 15.1.4. The following sets of subsets of $\mathbb{R}$ all generate the same σ-algebra:

$$\text{(i) } \{(a, b) : a < b\}, \qquad \text{(ii) } \{(a, b] : a < b\}, \qquad \text{(iii)} \{(-\infty, b] : b \in \mathbb{R}\}. \tag{15.1.20}$$

Proof. Let $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ be the set systems in (i), (ii) and (iii) respectively. So it is sufficient to show that

$$\begin{cases} \mathcal{A}_2 \subseteq \sigma(\mathcal{A}_1) \\ \mathcal{A}_3 \subseteq \sigma(\mathcal{A}_2) \\ \mathcal{A}_1 \subseteq \sigma(\mathcal{A}_3) \end{cases} \Rightarrow \begin{cases} \sigma(\mathcal{A}_2) \subseteq \sigma(\mathcal{A}_1) \\ \sigma(\mathcal{A}_3) \subseteq \sigma(\mathcal{A}_2) \\ \sigma(\mathcal{A}_1) \subseteq \sigma(\mathcal{A}_3) \end{cases} \Rightarrow \sigma(\mathcal{A}_1) = \sigma(\mathcal{A}_2) = \sigma(\mathcal{A}_3) \tag{15.1.21}$$

since $\sigma(\mathcal{A}_i)$ is the smallest σ-algebra contains $\mathcal{A}_i$. Then we can check that

$$\underbrace{(a, b]}_{\in \mathcal{A}_2} = \underbrace{\bigcap_{n \in \mathbb{N}} \left(a, b + \frac{1}{n}\right)}_{\in \sigma(\mathcal{A}_1)}, \qquad \underbrace{(-\infty, b]}_{\in \mathcal{A}_3} = \underbrace{\bigcup_{n \in \mathbb{N}} (a - n, b]}_{\in \sigma(\mathcal{A}_2)}, \qquad \underbrace{(a, b)}_{\in \mathcal{A}_1} = \underbrace{\left(\bigcup_{n \in \mathbb{N}} \left(-\infty, b - \frac{1}{n}\right]\right) \Bigg\backslash (-\infty, a]}_{\in \sigma(\mathcal{A}_3)}.$$ □

Proposition 15.1.5. Let (E_1, d_1) and (E_2, d_2) be metric spaces and let $f : E_1 \to E_2$ be an arbitrary map. Denote the set of points of discontinuity of f, $U_f = \{x \in E_1 : f \text{ is discontinuous at } x\}$. Then $U_f \in \mathcal{B}(E_1)$.

Proof. For any $\varepsilon, \delta > 0$, the set

$$U_f^{\delta,\varepsilon} := \{x \in E_1 : \text{there are } y, z \in B_\varepsilon(x),\ d_2(f(y), f(z)) \geq \delta\} \tag{15.1.22}$$

where $B_\varepsilon(x) = \{y \in \mathbb{E}_1 : d_1(x, y) < \varepsilon\}$. Then

$$U_f^{\delta,\varepsilon} = \bigcup_{\substack{y,z \in E_1 \\ d_2(f(y),f(z)) \geq \delta}} \bigcup_{x \in E_1} \{x : d_1(x, y) < \varepsilon\} \cap \{x : d_1(x, z) < \varepsilon\} \tag{15.1.23}$$

We see that $\{x : d_1(x, y) < \varepsilon\}$ and $\{x : d_1(x, z) < \varepsilon\}$ are open. then by Theorem 12.0.9, we have $U_f^{\delta,\varepsilon}$ is open. Thus, by Theorem 12.0.9 again, $U_f = \bigcup_{\varepsilon>0} \bigcup_{\delta>0} U_f^{\delta,\varepsilon}$ is open. Hence $U_f \in \mathcal{B}(E_1)$. □

15.1.2 Measures

Definition 15.1.10. Let $\mathcal{A}$ be any set of subsets of E containing the empty set $\emptyset$. A set function is a function $\mu : \mathcal{A} \to [0, \infty]$ with $\mu(\emptyset) = 0$.

Definition 15.1.11. Let μ be a set function. Say that μ is increasing (decreasing) if, for all $A, B \in \mathcal{A}$ with $A \subseteq B$,

$$\mu(A) \leq \mu(B) \quad (\mu(A) \geq \mu(B)) . \tag{15.1.24}$$

Definition 15.1.12. Let μ be a set function. Say that μ is additive if, for all disjoint sets $A, B \in \mathcal{A}$ with $A \cap B = \emptyset$, $A \cup B \in \mathcal{A}$,

$$\mu(A \cup B) = \mu(A) + \mu(B). \tag{15.1.25}$$

Definition 15.1.13 (countable additivity)**.** Let μ be a set function. Say that μ is countably additive if, for all sequences of disjoint sets $(A_n : n \in \mathbb{N}) \in \mathcal{A}$ with $\bigcup_n A_n \in \mathcal{A}$,

$$\mu\left(\bigcup_n A_n\right) = \sum_n \mu(A_n). \tag{15.1.26}$$

Definition 15.1.14 (countable subadditivity)**.** Let μ be a set function. Say that μ is countably subadditive if, for all sequences $(A_n : n \in \mathbb{N}) \in \mathcal{A}$ with $\bigcup_n A_n \in \mathcal{A}$,

$$\mu\left(\bigcup_n A_n\right) \leq \sum_n \mu(A_n). \tag{15.1.27}$$

Lemma 15.1.6. Let μ be a countably additive set function on a ring $\mathcal{A}$. Then μ is increasing and countably subadditive.

Proof. μ is increasing since μ is countably additive and $\mathcal{A}$ is a ring. Suppose that $A, B \in \mathcal{A}$ with $A \subseteq B$,

$$\mu(A) \leq \mu(A) + \mu(\underbrace{B \backslash A}_{\in \mathcal{A}}) = \mu\left(A \cup (B \backslash A)\right) = \mu(B) \ \Rightarrow\ \mu \text{ is increasing.} \tag{15.1.28}$$

Now assume that $A_n \in \mathcal{A}$ and $\bigcup_n A_n \in \mathcal{A}$. Let $B_1 = A_1,\ B_2 = A_2 \backslash B_1,\ \ldots,\ B_n = A_n \Big\backslash \bigcup_{i=1}^{n-1} B_i$. By induction, $B_n \in \mathcal{A}$ since $\mathcal{A}$ is a ring. Moreover, B_n are disjoint, and $\bigcup_{i=1}^n B_i = \bigcup_{i=1}^n A_i$. Thus by countable additivity, we get

$$\mu\left(\bigcup_n A_n\right) = \mu\left(\bigcup_n B_n\right) = \mu\left(\bigcup_{i=1}^\infty B_i\right) = \sum_{i=1}^\infty \mu(B_i) \leq \sum_{i=1}^\infty \mu(A_i), \tag{15.1.29}$$

since μ is increasing ($\mu(B_i) \leq \mu(A_i)$). □

Lemma 15.1.7. Let μ be a finite-valued additive set function on a ring $\mathcal{A}$. Show that μ is countably additive iff

$$A_n \supseteq A_{n+1} \in \mathcal{A},\ n \in \mathbb{N},\quad \bigcap_n A_n = \emptyset \ \Rightarrow\ \mu(A_n) \to 0. \tag{15.1.30}$$

Proof. ($\Rightarrow$) Assume μ is countably additive and let $B_n = A_n \backslash A_{n+1}$. We have B_n are disjoint and $B_n \in \mathcal{A}$ since $\mathcal{A}$ is a ring. Then we have

$$\bigcup_{m\le n} B_m = \bigcup_{m\le n} (A_m \backslash A_{m+1}) = A_1 \backslash A_{n+1} \in \mathcal{A}. \tag{15.1.31}$$

$$\bigcup_n B_n = \bigcup_n \bigcup_{m\le n} B_m = \bigcup_n (A_1 \backslash A_{n+1}) = A_1 \left\backslash \left(\bigcap_n A_{n+1}\right) = A_1 \right\backslash \underbrace{\left(\bigcap_n A_n\right)}_{=\emptyset} = A_1 \in \mathcal{A}. \tag{15.1.32}$$

Since μ is countably additive we have

$$\sum_{m\le n} \mu(B_m) = \mu\left(\bigcup_{m\le n} B_m\right) = \mu\left(A_1 \backslash A_{n+1}\right) = \mu(A_1) - \mu(A_{n+1}), \qquad \sum_n \mu(B_n) = \mu(A_1) < \infty. \tag{15.1.33}$$

Thus we have $\lim_{n\to\infty} \sum_{m\ge n} \mu(B_m) = 0$ and then from the above two equations

$$\mu(A_{n+1}) = \sum_{m>n} \mu(B_m) \ \Rightarrow\ \lim_{n\to\infty} \mu(A_n) = \lim_{n\to\infty} \sum_{m\ge n} \mu(B_m) = 0. \tag{15.1.34}$$

($\Leftarrow$) Suppose that B_n is a sequence of disjoint sets with $\bigcup_n B_n \in \mathcal{A}$, we define

$$A_1 = \bigcup_n B_n, \quad A_n = \bigcup_{m\ge n} B_m = \bigcup_m B_m \left\backslash \left(\bigcup_{m<n} B_m\right) \in \mathcal{A} \ \Rightarrow\ A_n \supseteq A_{n+1}, \tag{15.1.35}$$

$$\bigcap_n A_n = \bigcap_n \left(\bigcup_{m\ge n} B_m\right) = \bigcap_n \left(\bigcup_m B_m \left\backslash \left(\bigcup_{m<n} B_m\right)\right.\right) = \bigcup_m B_m \left\backslash \left(\bigcup_n \bigcup_{m<n} B_m\right) = \bigcup_m B_m \right\backslash \bigcup_n B_n = \emptyset \tag{15.1.36}$$

Since μ is finite and additive. we have

$$\begin{aligned} \mu(A_n) &= \mu\left(\bigcup_m B_m \left\backslash \left(\bigcup_{m<n} B_m\right)\right.\right) = \mu\left(A_1 \left\backslash \left(\bigcup_{m<n} B_m\right)\right.\right) = \mu(A_1) - \mu\left(\bigcup_{m<n} B_m\right) \\ &= \mu(A_1) - \sum_{m<n} \mu(B_m) = \mu\left(\bigcup_n B_n\right) - \sum_{m<n} \mu(B_m) \end{aligned}$$

Thus, we have

$$\mu(A_n) \to 0 \ \Rightarrow\ \mu\left(\bigcup_n B_n\right) - \sum_n \mu(B_n) = 0 \ \Rightarrow\ \mu\left(\bigcup_n B_n\right) = \sum_n \mu(B_n) \tag{15.1.37}$$

which implies that μ is countably additive. □

Definition 15.1.15 (measure)**.** A measure μ on measurable space $(E, \mathcal{E})$ is a set function $\mu : \mathcal{E} \to [0, \infty]$, such that, for any sequence $(A_n : n \in \mathbb{N})$ of disjoint elements of $\mathcal{E}$,

$$\mu\left(\bigcup_n A_n\right) = \sum_n \mu(A_n) \qquad \text{(countably additive)} \tag{15.1.38}$$

The triple $(E, \mathcal{E}, \mu)$ is called a measure space.

Remark. Note that the set function is defined on $\mathcal{A}$, a set of subsets of E and the measure is defined on a σ-algebra $\mathcal{E}$ on E.

Definition 15.1.16 (finite measure)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. If $\mu(E) < \infty$, then μ is a finite measure.

Definition 15.1.17 (σ-finite Measure)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. The measure μ is called σ-finite if E is the countable union of measurable sets of finite measure, i.e., there exists A_n with $\bigcup_n A_n = E$, $\mu(A_n) < \infty \ \forall n$.

Now we give some basic properties of measure:

Proposition 15.1.8. Let $(E, \mathcal{E}, \mu)$ be a measure space, then for $A, B, A_n \in \mathcal{E}$, $n \in \mathbb{N}$,

(i) $\mu(A \cup B) \leq \mu(A) + \mu(B)$, (ii) $\mu\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i}^{n} \mu(A_i)$, (iii) $\mu\left(\bigcup_n A_n\right) \leq \sum_n \mu(A_n)$,

If $\mu(E) < \infty$,

(iv) $\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B)$,

(v) $$\mu\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mu(A_i) - \sum_{1 \leq i_1 < i_2 \leq n} \mu(A_{i_1} \cap A_{i_2}) + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \mu(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \cdots + (-1)^{n-1} \mu\left(\bigcap_{i=1}^{n} A_i\right).$$

Remark. (v) is called inclusion-exclusion formula.

Proof. (i), (ii) and (iii) are implied by Lemma 15.1.6.

For (iv), we have disjoint sets $A \cap B$, $B \backslash A$, $A \backslash B$, by definition of measure (Definition 15.1.15),

$$\mu(A \cup B) = \mu((A \cap B) \cup (A \backslash B) \cup (B \backslash A)) = \mu(A \cap B) + \mu(A \backslash B) + \mu(B \backslash A). \tag{15.1.39}$$

Also, $\mu(A) = \mu(A \backslash B) + \mu(A \cap B)$, $\mu(B) = \mu(B \backslash A) + \mu(A \cap B)$. Since $\mu(A \cap B)$ is finite,

$$\mu(A \cup B) = \mu(A \cap B) + \mu(A) - \mu(A \cap B) + \mu(B) - \mu(A \cap B) = \mu(A) + \mu(B) - \mu(A \cap B). \tag{15.1.40}$$

The proof of (v) is by the induction on (iv). The case $n = 2$ is just (iv). Now assume the result holds for any n events and consider $A_1, \ldots, A_{n+1}$. Now see from (iv) again that

$$\mu\left(\bigcup_{i=1}^{n+1} A_i\right) = \mu\left(\bigcup_{i=1}^{n} A_i\right) + \mu(A_{n+1}) - \mu\left(\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1}\right) = \mu\left(\bigcup_{i=1}^{n} A_i\right) + \mu(A_{n+1}) - \mu\left(\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right).$$

and then apply the inductive hypothesis to the first and the third terms to complete the induction and obtain the conclusion. □

Definition 15.1.18 (null set)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. Call a subset $N \subseteq E$ μ-null set if

$$N \subseteq B \text{ for some } B \in \mathcal{E} \text{ with } \mu(B) = 0. \tag{15.1.41}$$

Definition 15.1.19 (complete measure space)**.** A measure space $(E, \mathcal{E}, \mu)$ is said to be complete if every subset of a set of measure 0 is measurable (and consequently, has measure 0), i.e. if for all $A \in \mathcal{E}$ such that $\mu(A) = 0$ and then for all $B \subseteq A$ we have $\mu(B) = 0$.

Proposition 15.1.9. The set of subsets $\mathcal{E}^\mu = \{A \cup N : A \in \mathcal{E}, N \text{ is } \mu\text{-null set}\}$ is a σ-algebra and μ has a well-defined and countably additive extension to $\mathcal{E}^\mu$ given by

$$\mu(A \cup N) = \mu(A). \tag{15.1.42}$$

We call $\mathcal{E}^\mu$ the completion of $\mathcal{E}$ with respect to μ.

Proof. First, we prove that $\mathcal{E}^\mu$ is a σ-algebra. Suppose $A_n \cup N_n \in \mathcal{E}^\mu$ with $A_n \in \mathcal{E}$ and $N_n \subseteq B_n$, $B_n \in \mathcal{E}$ and $\mu(B_n) = 0$. Then

(i) It is obvious that $\emptyset \in \mathcal{E}^\mu$.

(ii) For $A \cup N \in \mathcal{E}^\mu$, we have $N \subseteq B \in \mathcal{E}$ and $\mu(B) = 0$.

$$(A \cup N)^c = A^c \cap N^c = A^c \backslash N = \underbrace{(A^c \backslash B)}_{\in \mathcal{E}} \cup \underbrace{((A^c \cap B) \backslash N)}_{\subseteq B \in \mathcal{E}} \in \mathcal{E}^\mu. \tag{15.1.43}$$

(iii) Suppose $(A_n \cup N_n : n \in \mathbb{N}) \in \mathcal{E}^\mu$. Then

$$\bigcup_n (A_n \cup N_n) = \underbrace{\left(\bigcup_n A_n\right)}_{\in \mathcal{E}} \cup \underbrace{\left(\bigcup_n N_n\right)}_{\subseteq \bigcup_n B_n \in \mathcal{E}} \in \mathcal{E}^\mu \quad \left(\text{since } \mu\left(\bigcup_n B_n\right) \leq \sum_n \mu(B_n) = 0\right) \tag{15.1.44}$$

Thus, $\mathcal{E}^\mu$ is a σ-algebra. Now suppose $A_1 \cup N_1 = A_2 \cup N_2$, then

$$\mu(A_1) = \mu(A_1) + \mu(B_1) \geq \mu(A_1 \cup B_1) \geq \mu(A_1 \cup N_1) = \mu(A_2 \cup N_2) \geq \mu(A_2) \tag{15.1.45}$$

Similarly,

$$\mu(A_2) \geq \mu(A_1) \;\Rightarrow\; \mu(A_1) = \mu(A_2) = \mu(A_1 \cup N_1) \;\Rightarrow\; \mu \text{ is well defined on } \mathcal{E}^\mu. \tag{15.1.46}$$

Now we check countable additivity. Suppose that $(A_n \cup N_n)$ are sequences of disjoint sets

$$\mu\left(\bigcup_n (A_n \cup N_n)\right) = \mu\left(\left(\bigcup_n A_n\right) \cup \left(\bigcup_n N_n\right)\right) = \mu\left(\bigcup_n A_n\right) = \sum_n \mu(A_n) = \sum_n \mu(A_n \cup N_n). \qquad \square$$

Remark. If a measure space is not complete, there exists a completion of it, which is a complete measure space $(E, \mathcal{E}^\mu, \overline{\mu})$ such that $\mathcal{E} \subset \mathcal{E}^\mu$ and $\overline{\mu}|_{\mathcal{E}} = \mu$ (i.e., $\forall A \in \mathcal{E}$, $\overline{\mu}(A) = \mu(A)$), where $\mathcal{E}^\mu$ is the smallest σ-algebra containing both $\mathcal{E}$ and all subsets of elements of zero measure of $\mathcal{E}$.

Now we give the monotone convergece properties of measure.

Lemma 15.1.10 (fundamental property of measure)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. A_n is an increasing sequence of $\mathcal{E}$, and let $A = \bigcup_n A_n$. Then $\mu(A) = \lim_n \mu(A_n)$.

Proof. Let $B_1 = A_1, B_2 = A_2 \backslash A_1, \ldots, B_n = A_n \backslash A_{n-1} \in \mathcal{E}$. Moreover, the B_n are disjoint, and $\bigcup_{i=1}^n B_i = \bigcup_{i=1}^n A_i$ for all $n \geq 1$. Thus by countable additivity, we get

$$\mu(A) = \mu\left(\bigcup_n A_n\right) = \mu\left(\bigcup_n B_n\right) = \sum_n \mu(B_n) = \lim_n \sum_{i=1}^n \mu(B_i) = \lim_n \mu(A_n). \qquad \square$$

Corollary 15.1.11. Let $(E, \mathcal{E}, \mu)$ be a measure space. A_n is a decreasing sequence of $\mathcal{E}$ and $A = \bigcap_n A_n$. Also, $\mu(A_n) < \infty$ for some n. Then $\mu(A) = \lim_n \mu(A_n)$.

Proof. For $m \in \mathbb{N}$, $\mu(A_m) < \infty$ and let $B_n := A_m \backslash A_{m+n}$ and B_n is an increasing sequence. Applying fundamental property of measure (Lemma 15.1.10), we have

$$\begin{aligned} \mu(B) = \lim_n \mu(B_n) \quad &\Rightarrow \quad \mu(A_m \backslash A) = \lim_n \mu(A_m \backslash A_{m+n}) \;\Rightarrow\; \mu(A_m) - \mu(A) = \lim_n \mu(A_m) - \lim_n \mu(A_{m+n}) \\ &\Rightarrow \quad \mu(A) = \lim_n \mu(A_{m+n}) \quad \Rightarrow \quad \mu(A) = \lim_n \mu(A_n) \end{aligned}$$

$\square$

Corollary 15.1.12. Let $(E, \mathcal{E}, \mu)$ be a measure space. The union of a countable number of μ-null sets is μ-null.

Proof. For the μ-null sets $N_n \subseteq B_n$, $n \in \mathbb{N}$, with $\mu(B_n) = 0$, $\bigcup_n N_n \subseteq \bigcup_n B_n$, we know that $\bigcup_{m=1}^n N_m \uparrow \bigcup_n N_n$ and apply fundamental property of measure (Lemma 15.1.10),

$$\mu\left(\bigcup_n B_n\right) = \underbrace{\lim_n \mu\left(\bigcup_{m=1}^n B_m\right) \leq \lim_n \sum_{m=1}^n \mu(B_m)}_{\text{by countable subadditivity}} = \sum_n 0 = 0 \quad \Rightarrow \quad \bigcup_n N_n \text{ is } \mu\text{-null set.} \qquad \square$$

Definition 15.1.20. Given a sequence of events $(A_n : n \in \mathbb{N})$, we may ask for the probability that infinitely many occur. Set

$$\limsup A_n = \bigcap_n \bigcup_{m \geq n} A_m, \qquad \liminf A_n = \bigcup_n \bigcap_{m \geq n} A_m. \tag{15.1.47}$$

We write $\{A_n \text{ infinitely often}\}$ as an alternative for $\limsup A_n$, because $\omega \in \limsup A_n$ if and only if $\omega \in A_n$ for infinitely many n. Similarly, we write $\{A_n \text{ eventually}\}$ for $\liminf A_n$. The abbreviations i.o. and ev. are often used.

Note that $\{A_n \text{ i.o.}\}^c = \{A_n^c \text{ ev.}\}$.

Lemma 15.1.13 (First Borel-Cantelli Lemma)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. For sequence $A_n \subseteq E$, if $\sum_n \mu(A_n) < \infty$, then $\mu(A_n \text{ i.o.}) = 0$. (That is almost surely, A_n^c occurs eventually.)

Proof. As $n \to \infty$, we have $\mu(A_n \text{ i.o.}) \leq \mu\left(\bigcup_{m \geq n} A_m\right) \leq \sum_{m \geq n} \mu(A_m) \to 0$. □

Lemma 15.1.14 (Fatou's Lemma)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. For any sequence of sets $(A_n : n \in \mathbb{N}) \in \mathcal{E}$,

$$\mu(\liminf A_n) \leq \liminf \mu(A_n). \tag{15.1.48}$$

(Inverse Fatou's Lemma). If μ is finite, then also

$$\mu(\limsup A_n) \geq \limsup \mu(A_n) \tag{15.1.49}$$

Proof. Set $B_n = \bigcap_{m \geq n} A_m$, then $B_n \subseteq B_{n+1}$

$$\mu(B_n) \leq \inf_{m \geq n} \mu(A_m) \;\Rightarrow\; \lim_{n \to \infty} \mu(B_n) \leq \lim_{n \to \infty} \inf_{m \geq n} \mu(A_m) \tag{15.1.50}$$

We know that $B_n \uparrow \bigcup_n B_n = \bigcup_n \bigcap_{m \geq n} A_m = \liminf A_n \;\Rightarrow\; \lim_{n \to \infty} \mu(B_n) = \mu(\liminf A_n) \;\Rightarrow\; \mu(\liminf A_n) \leq \liminf \mu(A_n)$.

Now we have $E \backslash \limsup A_n = \liminf(E \backslash A_n)$, then

$$\mu(E \backslash \limsup A_n) = \mu(\liminf(E \backslash A_n)) \leq \liminf \mu(E \backslash A_n) \tag{15.1.51}$$

If $\mu(E) < \infty$, $\mu(E) - \mu(\limsup A_n) \leq \mu(E) + \liminf(-\mu(A_n)) = \mu(E) - \limsup \mu(A_n)$.

Then, we have $\mu(\limsup A_n) \geq \limsup \mu(A_n)$. □

Example 15.1.15. The second inequality of Fatou's Lemma may fail if μ is not finite. If μ is counting measure on $E = \mathbb{N}$, $A_n = \{n, n+1, \dots\}$, then $\mu(A_n) = \infty$,

$$\begin{aligned} \mu\left(\limsup_n A_n\right) &= \mu\left(\bigcap_n \bigcup_{m \geq n} A_m\right) = \mu\left(\left(\bigcup_n \bigcap_{m \geq n} A_m^c\right)^c\right) = \mu\left(\left(\bigcup_n \bigcap_{m \geq n} \{1, \dots, m-1\}\right)^c\right) \\ &= \mu\left(\left(\bigcup_n \{1, \dots, n-1\}\right)^c\right) = \mu\left(\{1, 2, \dots\}^c\right) = \mu(E^c) = \mu(\emptyset) = 0. \end{aligned}$$

Also, $\limsup \mu(A_n) = \limsup \infty = \infty \;\Rightarrow\; \mu(\limsup A_n) < \limsup \mu(A_n)$.

Definition 15.1.21. Let E be a countable set and let $\mathcal{E} = \mathcal{P}(E)$. A mass function is any function $m : E \to [0, \infty]$.

If μ is a measure on $(E, \mathcal{E})$, then, by countable additivity

$$\mu(A) = \sum_{x \in A} \mu(\{x\}), \quad A \subseteq E. \tag{15.1.52}$$

So there is a one-to-one correspondence between measures and mass functions, given by

$$m(x) = \mu(\{x\}), \qquad \mu(A) = \sum_{x \in A} m(x). \tag{15.1.53}$$

This sort of measure space provides a 'toy' version of the general theory, where each of the results we prove for general measure spaces reduces to some straightforward fact about the convergence of series. This is all one needs to do elementary discrete probability and discrete-time Markov chains, so these topics are usually introduced without discussing measure theory.

Discrete measure theory is essentially the only context where one can define a measure explicitly, because, in general, σ-algebras are not amenable to an explicit presentation which allow us to make such a definition. Instead one specifies the values to be taken on some smaller set of subsets, which generates the σ-algebra.

This gives rise to two problems: first to know that there is a measure extending the given set function, second to know that there is not more than one. The first problem, which is one of construction, is often dealt with by Carathéodory's extension theorem. The second problem, that of uniqueness, is often dealt with by Dynkin's π-system lemma.

15.1.3 Existence and Uniqueness

Definition 15.1.22. Let $\mathcal{A}$ be a ring of subsets of E and let $\mu : \mathcal{A} \to [0, \infty]$ be a countably additive set function. For any $B \subseteq E$, define outer measure μ^*,

$$\mu^*(B) = \inf_{A_n} \sum_n \mu(A_n) \tag{15.1.54}$$

where the infimum is taken over all sequences $(A_n : n \in \mathbb{N})$ in $\mathcal{A}$ such that $B \subseteq \bigcup_n A_n$ and is taken to be ∞ if there is no such sequence.

Proposition 15.1.16. Let $\mathcal{A}$ be a ring of subsets of E and $\mu : \mathcal{A} \to [0, \infty]$ be a countably additive set function. If μ^* is an outer measure, then μ^* is increasing and $\mu^*(\emptyset) = 0$.

Proof. For $\mu^*(\emptyset) = 0$, we simply let $A_n = \emptyset$ for all n. Now we prove μ^* is increasing. For $B, B' \in \mathcal{A}$ with $B \subseteq B'$,

(i) If we can not find a sequence A_n such that $B \subseteq \bigcup_n A_n$, then we can not find a sequence A'_n such that $B' \subseteq \bigcup_n A'_n$ either, otherwise $B \subseteq \bigcup_n A'_n$. Thus, $\mu^*(B) = \mu^*(B') = \infty$.

(ii) If we can find a sequence A_n such that $B \subseteq \bigcup_n A_n$ but we can not find a sequence A'_n such that $B' \subseteq \bigcup_n A'_n$, $\mu^*(B') = \infty$, which gives $\mu^*(B) \leq \mu^*(B')$.

(iii) If we can find a sequence A'_n such that $B' \subseteq \bigcup_n A'_n$, then we can find a sequence A_n such that $B \subseteq \bigcup_n A_n$. For any sequence A'_n, we have $B \subseteq \bigcup_n A'_n$, thus $\{A'_n, n \in \mathbb{N}\} \subseteq \{A_n, n \in \mathbb{N}\}$. Then we have

$$\mu^*(B) = \inf_{A_n} \sum_n \mu(A_n) \leq \inf_{A'_n} \sum_n \mu(A'_n) = \mu^*(B'). \tag{15.1.55}$$

Thus μ^* is increasing for any case.

□

Theorem 15.1.17 (Carathéodory's Extension Theorem)**.** Let $\mathcal{A}$ be a ring of subsets of E and let $\mu : \mathcal{A} \to [0, \infty]$ be a countably additive set function. Then μ extends to a measure on the σ-algebra generated by $\mathcal{A}$.

Proof. Let μ^* be a outer measure defined in Definition 15.1.22 and we say that $A \subseteq E$ is μ^*-measurable if, for all $B \subseteq E$,

$$\mu^*(B) = \mu^*(B \cap A) + \mu^*(B \cap A^c). \tag{15.1.56}$$

Write $\mathcal{M}$ for the set of all μ^*-measurable sets. We shall show that $\mathcal{M}$ is a σ-algebra containing $\mathcal{A}$ and that μ^* is a measure on $\mathcal{M}$, extending μ. This will prove the theorem.

Step I. We show that μ^* is countably subadditive. Suppose that $B \in E$, $B_n \in E$ and $B \subseteq \bigcup_n B_n$. If $\mu^*(B_n) = \infty$ for some n,

$$\mu^*\left(\bigcup_n B_n\right) \leq \infty = \sum_n \mu^*(B_n). \tag{15.1.57}$$

If $\mu^*(B_n) < \infty$ for all n, then given $\varepsilon > 0$, there exist sequences $(A_{nm} : m \in \mathbb{N})$ in $\mathcal{A}$, with

$$\underbrace{B_n \subseteq \bigcup_m A_{nm},}_{\text{definition of } \mu^*} \qquad \underbrace{\mu^*(B_n) + \varepsilon/2^n \geq \sum_m \mu(A_{nm})\,.}_{\text{definition of infimum}} \tag{15.1.58}$$

Then $B \subseteq \bigcup_n B_n \subseteq \bigcup_n \bigcup_m A_{nm}$ implies that

$$\mu^*(B) = \underbrace{\inf \sum_n \mu(A_n) = \inf \sum_n \sum_m \mu(A_{nm})}_{\mathbb{N}\times\mathbb{N} \text{ is countable}} \leq \sum_n \sum_m \mu(A_{nm}) \leq \sum_n (\mu^*(B_n) + \varepsilon/2^n) = \sum_n \mu^*(B_n) + \varepsilon. \tag{15.1.59}$$

Hence, in any case,

$$\mu^*(B) \leq \sum_n \mu^*(B_n) \;\Rightarrow\; \mu^*\left(\bigcup_n B_n\right) \leq \sum_n \mu^*(B_n). \tag{15.1.60}$$

Step II. We show that μ^* extends μ. Since $\mathcal{A}$ is a ring and μ is countably additive, we have μ is countably subadditive and increasing by using Lemma 15.1.6. Hence, for $A \in \mathcal{A}$ and any sequence $(A_n : n \in \mathbb{N}) \in \mathcal{A}$ with $A \subseteq \bigcup_n A_n$,

$$\mu(A) \underbrace{\leq}_{\mu \text{ is increasing}} \mu\left(\bigcup_n A_n\right) \underbrace{\leq}_{\mu \text{ is countably subadditive}} \sum_n \mu(A_n) \tag{15.1.61}$$

On taking the infimum over all such sequences, we see that $\mu(A) \leq \mu^*(A)$. On the other hand, Set the sequence to be $B_1 = A, B_2 = \emptyset, B_3 = \emptyset, \ldots$, we have $A \subseteq \bigcup_n B_n$

$$\mu^*(A) = \inf_{A_n} \sum_n \mu(A_n) \leq \sum_n \mu(B_n) = \mu(A). \tag{15.1.62}$$

Thus, $\mu(A) = \mu^*(A)$ for all $A \in \mathcal{A}$.

Step III. We show that $\mathcal{M}$ contains $\mathcal{A}$. To show $\mathcal{A} \subseteq \mathcal{M}$, we have to show that $\forall A \in \mathcal{A}$, $B \subseteq E$, $\mu^*(B) = \mu^*(B \cap A) + \mu^*(B \cap A^c)$. By countable subadditivity of μ^*,

$$\mu^*(B) = \mu^*\left((B \cap A) \cup (B \cap A^c)\right) \leq \mu^*(B \cap A) + \mu^*(B \cap A^c). \tag{15.1.63}$$

so it is enough to show that

$$\mu^*(B) \geq \mu^*(B \cap A) + \mu^*(B \cap A^c). \tag{15.1.64}$$

If $\mu^*(B) = \infty$, this is clearly true, so let us assume that $\mu^*(B) < \infty$. Then given $\varepsilon > 0$, we can find a sequence $(A_n : n \in \mathbb{N}) \in \mathcal{A}$ such that

$$\underbrace{B \subseteq \bigcup_n A_n}_{\text{definition of } \mu^*}, \qquad \underbrace{\mu^*(B) + \varepsilon \geq \sum_n \mu(A_n) s}_{\text{definition of infimum}} \quad \Rightarrow \quad B \cap A \subseteq \bigcup_n (A_n \cap A), \qquad B \cap A^c \subseteq \bigcup_n (A_n \cap A^c). \tag{15.1.65}$$

Since $A_n \cap A \in \mathcal{A}$ and $A_n \cap A^c = A_n \backslash A \in \mathcal{A}$,

$$\begin{aligned} \mu^*(B \cap A) + \mu^*(B \cap A^c) &= \inf_{A_n \cap A} \sum_n \mu\left(A_n \cap A\right) + \inf_{A_n \cap A^c} \sum_n \mu\left(A_n \cap A^c\right) \\ &\leq \sum_n \left(\underbrace{\mu\left(A_n \cap A\right) + \mu\left(A_n \cap A^c\right)}_{\text{two disjoint sets}} \right) = \underbrace{\sum_n \mu\left(A_n\right)}_{\text{countably additive}} \leq \mu^*(B) + \varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ was arbitrary, we are done.

Step VI. We show that $\mathcal{M}$ is an algebra. Clearly $E \in \mathcal{M}$ and $A^c \in \mathcal{M}$ whenever $A \in \mathcal{M}$. Suppose that $A_1, A_2 \in \mathcal{M}$ and $B \subseteq E$. Then

$$\begin{aligned} \mu^*(B) &\overset{A_1 \in \mathcal{M}}{=} \mu^*(B \cap A_1) + \mu^*(B \cap A_1^c) \overset{A_2 \in \mathcal{M}}{=} \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap A_1 \cap A_2^c) + \mu^*(B \cap A_1^c) \\ &= \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap (\emptyset \cup (A_2^c \cap A_1))) + \mu^*(B \cap (A_1^c \cup (A_1^c \cap A_2^c))) \\ &= \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap ((A_1^c \cap A_1) \cup (A_2^c \cap A_1))) + \mu^*(B \cap ((A_1^c \cup A_1^c) \cap (A_1^c \cup A_2^c))) \\ &= \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap (A_1^c \cup A_2^c) \cap A_1) + \mu^*(B \cap A_1^c \cap (A_1^c \cup A_2^c)) \\ &= \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap (A_1 \cap A_2)^c \cap A_1) + \mu^*(B \cap (A_1 \cap A_2)^c \cap A_1^c) \\ &\overset{A_1 \in \mathcal{M}}{=} \mu^*(B \cap A_1 \cap A_2) + \mu^*(B \cap (A_1 \cap A_2)^c) \end{aligned}$$

Hence, $A_1 \cap A_2 \in \mathcal{M}$. Then we can have $A_1 \cup A_2 \in \mathcal{M}$, thus $\mathcal{M}$ is an algebra.

Step V. We show that $\mathcal{M}$ is a σ-algebra and that μ^* is a measure on $\mathcal{M}$. We already know that $\mathcal{M}$ is an algebra,

so it suffices to show that, for any sequence of disjoint sets $(A_n : n \in \mathbb{N})$ in $\mathcal{M}$, for $A = \bigcup_n A_n$ we have

$$A \in \mathcal{M}, \qquad \mu^*\left(\bigcup_n A_n\right) = \mu^*(A) = \sum_n \mu^*(A_n). \tag{15.1.66}$$

So take any $B \subseteq E$, then

$$\begin{aligned}
\mu^*(B) &\overset{A_1\in\mathcal{M}}{=} \mu^*(B\cap A_1) + \mu^*(B\cap A_1^c) \overset{A_2\in\mathcal{M}}{=} \mu^*(B\cap A_1) + \mu^*(B\cap A_1^c\cap A_2) + \mu^*(B\cap A_1^c\cap A_2^c) \\
&= \mu^*(B\cap A_1) + \mu^*(B\cap A_2) + \mu^*(B\cap A_1^c\cap A_2^c) \qquad (A_1, A_2 \text{ are disjoint}) \\
&= \cdots = \sum_{i=1}^n \mu^*(B\cap A_i) + \mu^*(B\cap A_1^c\cap A_2^c\cap\cdots\cap A_n^c) = \sum_{i=1}^n \mu^*(B\cap A_i) + \mu^*\left(B\cap\left(\bigcap_{i=1}^n A_i^c\right)\right).
\end{aligned}$$

Since $A = \bigcup_n A_n$,

$$A^c = \bigcap_n A_n^c \;\Rightarrow\; B\cap A^c = B\cap\left(\bigcap_n A_n^c\right) \subseteq B\cap\left(\bigcap_{i=1}^n A_i^c\right) \;\Rightarrow\; \mu^*(B\cap A^c) \le \mu^*\left(B\cap\left(\bigcap_{i=1}^n A_i^c\right)\right), \tag{15.1.67}$$

for all n since μ^* is increasing. Hence, we get

$$\begin{aligned}
\mu^*(B) &= \sum_{i=1}^n \mu^*(B\cap A_i) + \mu^*\left(B\cap\left(\bigcap_{i=1}^n A_i^c\right)\right) \\
&\ge \sum_{i=1}^n \mu^*(B\cap A_i) + \mu^*(B\cap A^c) = \sum_n \mu^*(B\cap A_n) + \mu^*(B\cap A^c) \qquad \text{as } n\to\infty \\
&\ge \mu^*\left(\bigcup_n (B\cap A_n)\right) + \mu^*(B\cap A^c) \qquad (\mu^* \text{ is countably additive}) \\
&= \mu^*\left(B\cap\left(\bigcup_n A_n\right)\right) + \mu^*(B\cap A^c) = \mu^*(B\cap A) + \mu^*(B\cap A^c).
\end{aligned}$$

Also, using countable subadditivity, we have

$$\mu^*(B) \le \mu^*(B\cap A) + \mu^*(B\cap A^c) \;\Rightarrow\; \mu^*(B) = \mu^*(B\cap A) + \mu^*(B\cap A^c) \tag{15.1.68}$$

Thus, $A \in \mathcal{M}$. Then setting $B = A$, we get

$$\begin{aligned}
\mu^*(B) &= \sum_{i=1}^n \mu^*(B\cap A_i) + \mu^*\left(B\cap\left(\bigcap_{i=1}^n A_i^c\right)\right) \\
\mu^*(A) &= \sum_{i=1}^n \mu^*(A\cap A_i) + \mu^*\left(A\cap\left(\bigcap_{i=1}^n A_i^c\right)\right) = \sum_n \mu^*(A\cap A_n) + \mu^*\left(A\cap\left(\bigcup_n A_n\right)^c\right) \qquad \text{as } n\to\infty \\
&= \sum_n \mu^*(A_n) + \mu^*(A\cap A^c) = \sum_n \mu^*(A_n) + \mu^*(\emptyset) = \sum_n \mu^*(A_n),
\end{aligned}$$

as $\mu^*(\emptyset) = 0$. □

Theorem 15.1.18 (uniqueness of extension)**.** Let μ_1, μ_2 be measures on $(E, \mathcal{E})$ with $\mu_1(E) = \mu_2(E) < \infty$. Suppose $\mu_1 = \mu_2$ on $\mathcal{A}$, for some π-system $\mathcal{A}$ generating $\mathcal{E}$. Then $\mu_1 = \mu_2$ on $\mathcal{E}$.

Proof. Consider $\mathcal{D} = \{A \in \mathcal{E} : \mu_1(A) = \mu_2(A)\}$, which gives $\mathcal{A} \subseteq \mathcal{D}$ and $\mathcal{D} \subseteq \mathcal{E}$. By hypothesis, $E \in \mathcal{D}$. For $A, B \in \mathcal{D}$ with $A \subseteq B$, we have $A, B \in \mathcal{E}$ and $B\backslash A \in \mathcal{E}$. Then we have

$$\mu_1(A) + \mu_1(B\backslash A) = \mu_1(B) < \infty, \quad \mu_2(A) + \mu_2(B\backslash A) = \mu_2(B) < \infty \;\Rightarrow\; \mu_1(B\backslash A) = \mu_2(B\backslash A) \;\Rightarrow\; B\backslash A \in \mathcal{D}. \tag{15.1.69}$$

Now suppose that $A_n \in \mathcal{D}, n \in \mathbb{N}$ with $A_n \uparrow A$, thus $A_n \in \mathcal{E} \;\Rightarrow\; \bigcup_n A_n \in \mathcal{E}$. Then by Lemma 15.1.10,

$$\mu_1(A) = \lim_n \mu_1(A_n) \underbrace{=}_{A_n\in\mathcal{D}} \lim_n \mu_2(A_n) = \mu_2(A) \;\Rightarrow\; A \in \mathcal{D}. \tag{15.1.70}$$

Thus $\mathcal{D}$ is a d-system containing the π-system $\mathcal{A}$. We apply Dynkin's Lemma (Lemma 15.1.3) and get that $\mathcal{D}$ is a σ-algebra containing $\mathcal{A}$. Since $\mathcal{D} \subseteq \mathcal{E}$ and $\mathcal{E}$ is the smallest σ-algebra (by definition of $\mathcal{E}$) containing $\mathcal{A}$, we have $\mathcal{D} = \mathcal{E}$. □

15.1.4 Measure notations

Definition 15.1.23. A measure μ on $(E, \mathcal{B}(E))$ is called Borel measure on $(E, \mathcal{B}(E))$.

Recall σ-finite measure and Borel measurable space (Definition 15.1.17, 15.1.9), we have following definitions with respect to topology:

Definition 15.1.24. Let μ be σ-finite measure on $(E, \mathcal{E})$. It is called locally finite if for any $x \in E$, there exists an open neighourhood U, such that $x \in U$ and $\mu(U) < \infty$.

Definition 15.1.25. Let μ be σ-finite measure on $(E, \mathcal{E})$. It is called inner regular if

$$\mu(A) = \sup\{\mu(K) : K \subseteq A \text{ is compact}\}, \quad \forall A \in \mathcal{E}. \tag{15.1.71}$$

Definition 15.1.26. Let μ be σ-finite measure on $(E, \mathcal{E})$. It is called outer regular if

$$\mu(A) = \inf\{\mu(U) : U \text{ is open}, A \subseteq U\}, \quad \forall A \in \mathcal{E}. \tag{15.1.72}$$

Definition 15.1.27. Let μ be σ-finite measure on $(E, \mathcal{E})$. It is called regular measure if it is inner regular and outer regular.

Definition 15.1.28. Let μ be σ-finite measure on $(E, \mathcal{E})$. It is called a Radon measure if it is inner regular, locally finite Borel measure.

Definition 15.1.29. We introduce the following spaces of measures on E (in [10]):

$$\mathcal{M}_R(E) := \{\text{Radon measures on } (E, \mathcal{B}(E))\}, \qquad \mathcal{M}_f(E) := \{\text{finite Borel measures on } (E, \mathcal{B}(E))\}.$$

Definition 15.1.30. Furthermore, we agree on the following notations for spaces of continuous functions:

$$C(E) := \{f : E \to \mathbb{R} \text{ is continuous}\}, \qquad C_b(E) := \{f \in C(E) \text{ is bounded}\},$$
$$C_c(E) := \{f \in C(E) \text{ has compact support}\} \subseteq C_b(E).$$

Remark. Recall that the support of a real function f is $\overline{f^{-1}(\mathbb{R} \setminus \{0\})}$.

15.1.5 Lebesgue measure

Recall Definition 15.1.23, we have

Theorem 15.1.19. There exists a unique Borel measure μ on $\mathbb{R}$ such that, for all $a, b \in \mathbb{R}$ with $a < b$,

$$\mu((a, b]) = b - a. \tag{15.1.73}$$

The measure μ is called Lebesgue measure on $\mathbb{R}$.[1]

Proof. (Existence.) Consider the ring $\mathcal{A}$ of finite unions of disjoint intervals of the form $A = (a_1, b_1] \cup \cdots \cup (a_n, b_n]$.

We note that $\mathcal{A}$ generates $\mathcal{B}$. Define for such $A \in \mathcal{A}$, the set function

$$\mu(A) = \sum_{i=1}^{n} (b_i - a_i). \tag{15.1.74}$$

Note that the presentation of A is not unique, as $(a, b] \cup (b, c] = (a, c]$ whenever $a < b < c$. Nevertheless, it is easy to check that μ is well-defined and additive. We aim to show that μ is countably additive on $\mathcal{A}$, which then proves existence by Carathéodory's extension theorem.

By additivity, it suffices to show that, if $A \in \mathcal{A}$ and if $(A_n : n \in \mathbb{N})$ is an increasing sequence in $\mathcal{A}$ with $A_n \uparrow A$, then $\mu(A_n) \to \mu(A)$ (by fundamental property of measure, Lemma 15.1.10). Set $B_n = A \backslash A_n$ then $B_n \in \mathcal{A}$ and $B_n \downarrow \emptyset$. By

[1] For $\mathbb{R}^n$ case, $\mu(A)$

additivity again, it suffices to show that $\mu(B_n) \to 0$. Suppose, in fact, that for some $\varepsilon > 0$, we have $\mu(B_n) \geq 2\varepsilon$ for all n. For each n we can find $C_n \in \mathcal{A}$ with $\overline{C}_n \subseteq B_n$ and $\mu(B_n \backslash C_n) \leq \varepsilon 2^{-n}$ (since $B_n \backslash C_n \in \mathcal{A}$), where $\overline{C}_i$ is the closure of C_i. That is, for

$$B_n = (a_1, b_1] \cup \cdots \cup (a_m, b_m] \tag{15.1.75}$$

where m is finite by definition, we can find $m' \leq m$ (for case that $a_i + \frac{\varepsilon 2^{-n}}{m} \geq b_i$) and choose

$$C_n = \left(a_1 + \frac{\varepsilon 2^{-n}}{m}, b_1\right] \bigcup \cdots \bigcup \left(a_{m'} + \frac{\varepsilon 2^{-n}}{m}, b_{m'}\right]. \tag{15.1.76}$$

Thus, $\mu(B_n \backslash C_n) = \underbrace{\mu(B_n) - \mu(C_n)}_{\text{by additivity of } \mu} = \underbrace{\sum_{i=1}^{m}(b_i - a_i) - \sum_{i=1}^{m'}\left(b_i - a_i - \frac{\varepsilon 2^{-n}}{m}\right)}_{\text{definition of } \mu} \leq \sum_{i=1}^{m} \frac{\varepsilon 2^{-n}}{m} = \varepsilon 2^{-n}$. Then

$$\mu(B_n \backslash (C_1 \cap \cdots \cap C_n)) \leq \mu((B_1 \backslash C_1) \cup \cdots \cup (B_n \backslash C_n)) \leq \sum_{n \in \mathbb{N}} \varepsilon 2^{-n} = \varepsilon. \tag{15.1.77}$$

Since $\mu(B_n) \geq 2\varepsilon$, we must have $\mu(C_1 \cap \cdots \cap C_n) \geq \varepsilon$, so $C_1 \cap \cdots \cap C_n \neq \emptyset$ (definition of the set function), and so $K_n = \overline{C}_1 \cap \cdots \cap \overline{C}_n \neq \emptyset$. Now $(K_n : n \in \mathbb{N})$ is a decreasing sequence of bounded non-empty closed sets in $\mathbb{R}$ (since the intersect of closed sets is closed), so $\emptyset \neq \bigcap_n K_n \subseteq \bigcap_n B_n$, which is a contradiction.

(Uniqueness.) Let μ, λ be two measures on $\mathcal{B}(\mathbb{R})$ with

$$\mu((a, b]) = b - a, \qquad \lambda((a, b]) = b - a, \tag{15.1.78}$$

for all $a < b$. Fix n and consider $A \in \mathcal{A}$

$$\mu_n(A) = \mu((n, n+1] \cap A), \qquad \lambda_n(A) = \lambda((n, n+1] \cap A). \tag{15.1.79}$$

Then we have μ_n and λ_n are measures on $\mathcal{B}$ with $\mu_n(\mathbb{R}) = \lambda_n(\mathbb{R}) = 1 < \infty$ since with disjoint sets A_n,

$$\begin{aligned} \mu_n\left(\bigcup_m A_m\right) &= \mu\left((n, n+1] \cap \bigcup_m A_m\right) = \mu\left(\bigcup_m (n, n+1] \cap A_m\right) = \mu\left(\bigcup_m B_m\right) \\ &= \sum_m \mu(B_m) = \sum_m \mu\left((n, n+1] \cap A_m\right) = \sum_m \mu_n\left(A_m\right) \end{aligned}$$

where $B_m := (n, n+1] \cap A_m$ are disjoint. So $\mu_n = \lambda_n$ on the π-system of intervals of the form $(a, b]$, which generates $\mathcal{B}$. So, by Theorem 15.1.18 (Uniqueness of extension), $\mu_n = \lambda_n$ on $\mathcal{B}$. Hence, for all $A \in \mathcal{B}$, we have

$$\mu(A) = \underbrace{\mu(\mathbb{R} \cap A) = \sum_n \mu\left((n, n+1] \cap A\right)}_{\text{countable additivity of } \mu} = \sum_n \mu_n(A) = \sum_n \lambda_n(A) = \underbrace{\sum_n \lambda\left((n, n+1] \cap A\right) = \lambda(\mathbb{R} \cap A)}_{\text{countable additivity of } \lambda} = \lambda(A). \tag{15.1.80}$$

Note that you cannot apply uniqueness of extension (Theorem 15.1.18) directly to μ since $\mu(\mathbb{R})$ is not finite. □

Proposition 15.1.20. For Lebesgue measure space $(E, \mathcal{E}, \mu)$ and singleton point x, $\mu(\{x\}) = 0$.

Proof. For Lebesgue measure μ, we have for any $a < b$, $\mu((a, b]) = b - a$. Now fix b and let $a < b - 1$ and define

$$A_n := \left(a, b - \frac{1}{n}\right] \quad \Rightarrow \quad A_n \uparrow (a, b) := A. \tag{15.1.81}$$

By fundamental property of measure (Lemma 15.1.10),

$$\begin{aligned} \lim_n \mu\left(A_n\right) = \mu\left(A\right) \quad \Rightarrow \quad \lim_n \mu\left(\left(a, b - \frac{1}{n}\right]\right) &= \mu\left((a, b)\right) = \mu\left((a, b]\right) - \mu(\{b\}) \\ \lim_n \left(b - \frac{1}{n} - a\right) &= b - a - \mu(\{b\}) \quad \Rightarrow \quad \mu(\{b\}) = \lim_n \frac{1}{n} = 0. \end{aligned}$$

□

Existence of a non-Lebesgue-measurable subset of $\mathbb{R}$ For $x, y \in [0,1)$, let us write $x \sim y$ if $x - y \in \mathbb{Q}$. Then $\sim$ is an equivalence relation. Using the Axiom of Choice, we can find a subset S of $[0,1)$ containing exactly one representative of each equivalence class. Set $Q = \mathbb{Q} \cap [0,1)$ and, for each $q \in Q$, define $S_q = S + q = \{s + q (\text{mod} 1) : s \in S\}$. It is an easy exercise to check that the sets S_q are all disjoint and their union is $[0,1)$.

Now, Lebesgue measure μ on $\mathcal{B} = \mathcal{B}([0,1))$ is translation invariant. That is to say, $\mu(B) = \mu(B + x)$ for all $B \in \mathcal{B}$ and all $x \in [0,1)$. If S were a Borel set, then we would have

$$1 = \mu([0,1)) = \sum_{q \in Q} \mu(S + q) = \sum_{q \in Q} \mu(S) \tag{15.1.82}$$

which is impossible. Hence $S \notin \mathcal{B}$.

A Lebesgue measurable set in $\mathbb{R}$ is any set of the form $A \cup N$, with A Borel and $N \subseteq B$ for some Borel set B with $\mu(B) = 0$. Thus the set of Lebesgue measurable sets is the completion of the Borel σ-algebra with respect to μ.

Proposition 15.1.21. For every Borel set $B \subseteq \mathbb{R}$ of finite Lebesgue measure and every $\varepsilon > 0$, there exists a finite union of disjoint intervals $A = (a_1, b_1] \cup \cdots \cup (a_n, b_n]$ such that the Lebesgue measure of symmetric difference $A \triangle B (= (A^c \cap B) \cup (A \cap B^c))$ is less than ε.

Proof. First let μ be Lebesgue measure on $(\mathbb{R}, \mathcal{B})$ and let

$$\mathcal{A}_n = \{((a_1, b_1] \cup \cdots \cup (a_m, b_m]) \cap [-n, n] : \ a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{R}, m \text{ is finite}\} \tag{15.1.83}$$

Then it is obvious that $\mathcal{A}_n$ is a π-system (also a ring) with $\sigma(\mathcal{A}_n) = \mathcal{B}([-n, n])$ (the Borel σ-algebra on $[-n, n]$). Let

$$\mathcal{D}_n = \{B \in \mathcal{B}([-n, n]) : \forall \varepsilon > 0, \ \exists A \in \mathcal{A}_n, \ \mu(A \triangle B) < \varepsilon\}. \tag{15.1.84}$$

It is clear that $\mathcal{A}_n \subseteq \mathcal{D}_n \subseteq \mathcal{B}([-n, n])$. We shall show that $\mathcal{D}_n$ is a d-system on $[-n, n]$. Then by Dynkin's lemma we will have that $\mathcal{B}([-n, n]) \subseteq \mathcal{D}_n$. Thus, $\mathcal{D}_n = \mathcal{B}([-n, n])$. Thus,

(i) For $A = B = [-n, n]$, $\mu(A \triangle B) = \mu((A^c \cap B) \cup (A \cap B^c)) = \mu(\emptyset \cup \emptyset) = 0 < \varepsilon$.

(ii) Suppose $A_1, A_2 \in \mathcal{D}_n$ with $A_1 \subseteq A_2$. We know that $\forall \varepsilon$, $\exists A_1', A_2' \in \mathcal{A}_n$

$$\mu(A_1' \triangle A_1)) < \frac{\varepsilon}{2}, \quad \mu(A_2' \triangle A_2)) < \frac{\varepsilon}{2} \tag{15.1.85}$$

then $A_2' \backslash A_1' \in \mathcal{A}_n$ since $\mathcal{A}_n$ is a ring. Thus, $\exists A = A_2' \backslash A_1' \in \mathcal{A}_n$

$$\begin{aligned} A \triangle (A_2 \backslash A_1) &= (A_2' \backslash A_1') \triangle (A_2 \backslash A_1) \subseteq (A_2' \triangle A_1') \triangle (A_2 \triangle A_1) \\ &= (A_1' \triangle A_1) \triangle (A_2' \triangle A_2) \qquad (\triangle \text{ is commutative and associative}) \\ &\subseteq (A_1' \triangle A_1) \cup (A_2' \triangle A_2) \end{aligned}$$

Thus, we have $\mu(A \triangle (A_2 \backslash A_1)) \leq \mu((A_1' \triangle A_1) \cup (A_2' \triangle A_2)) \leq \mu(A_1' \triangle A_1)) + \mu(A_2' \triangle A_2)) < \varepsilon \ \Rightarrow \ A_2 \backslash A_1 \in \mathcal{D}_n$.

(iii) Suppose $\{A_m : m \in \mathbb{N}\}$ is an increasing sequence in $\mathcal{D}_n$ with $A_m \uparrow \bigcup_n A_n = A$. Then $A \backslash A_m \downarrow \emptyset$. Since μ is finite on $[-n, n]$ and countably additive. From the previous question (4), we have

$$\bigcap_n (A \backslash A_n) = A \left\backslash \left(\bigcup_n A_n \right) \right. = A \backslash A = \emptyset \ \Rightarrow \ \mu(A \backslash A_n) \to 0. \tag{15.1.86}$$

Thus, $\forall \varepsilon$, $\exists N$ s.t. $A_N \in \mathcal{D}_n$, $\mu(A \backslash A_N) < \frac{\varepsilon}{2}$. Since $A_N \in \mathcal{D}_n$, $\exists A_N' \in \mathcal{A}_n$ s.t. $\mu(A_N' \triangle A_N) < \frac{\varepsilon}{2}$.

Thus, we have $A \triangle A_N' = A \triangle A_N \triangle A_N \triangle A_N' = (A \triangle A_N) \triangle (A_N \triangle A_N') = \underbrace{(A \backslash A_N) \triangle (A_N \triangle A_N')}_{\text{since } A_N \subseteq A} \subseteq (A \backslash A_N) \cup (A_N \triangle A_N')$.

Then, we have $\mu(A \triangle A_N') \leq \mu(A \backslash A_N) \cup (A_N \triangle A_N') \leq \mu(A \backslash A_N) + \mu(A_N \triangle A_N') < \varepsilon \ \Rightarrow \ A = \bigcup_n A_n \in \mathcal{D}_n$.

Thus, we say that $\mathcal{D}_n$ is a d-system and $\mathcal{D}_n = \mathcal{B}([-n, n])$. Now, for any $B \in \mathcal{B}$ with $\mu(B) < \infty$, set $B_n = B \cap [-n, n]$. Then $B_n \uparrow B$ and $B \backslash B_n \downarrow \emptyset$. So $\mu(B \backslash B_n) \to 0$. Then $\forall \varepsilon$, $\exists N$ s.t. $\mu(B \backslash B_N) < \frac{\varepsilon}{2}$. Also, we have $B_N \in \mathcal{D}_N$, so $\exists A_N \in \mathcal{A}_N$

s.t.

$$\mu(A_N \triangle B_N) < \frac{\varepsilon}{2}. \tag{15.1.87}$$

Hence, $A_N \triangle B = (A_N \triangle B_N) \triangle (B_N \triangle B) = (A_N \triangle B_N) \triangle (B \backslash B_N) \subseteq (A_N \triangle B_N) \cup (B \backslash B_N)$, and

$$\mu(A_N \triangle B) \leq \mu((A_N \triangle B_N) \cup (B \backslash B_N)) \leq \mu(A_N \triangle B_N) + \mu(B \backslash B_N) < \varepsilon. \qquad \square$$

15.2 Measurable Functions

15.2.1 Measurable functions

Definition 15.2.1 (measurable function, Borel function)**.** Let $(E, \mathcal{E})$ and $(G, \mathcal{G})$ be measurable spaces. A function $f : E \to G$ is $\mathcal{E}$-measurable (or $\mathcal{E}$-$\mathcal{G}$-measurable) if $f^{-1}(A) \in \mathcal{E}$ whenever $A \in \mathcal{G}$. Here $f^{-1}(A)$ denotes the inverse image of A by f

$$f^{-1}(A) = \{x \in E : f(x) \in A\}. \tag{15.2.1}$$

Usually $G = \mathbb{R}$ or $G = \overline{\mathbb{R}} = [-\infty, \infty]$, in which case $\mathcal{G}$ is always taken to be the Borel σ-algebra. If $(E, \mathcal{T})$ is a topological space and $\mathcal{E} = \mathcal{B}(E)$, then a measurable function on E is called a Borel function.

Proposition 15.2.1. In particular, if $\mathcal{G} = \sigma(\mathcal{A})$ and $f^{-1}(A) \in \mathcal{E}$ whenever $A \in \mathcal{A}$ (A is in a π-system $\mathcal{A}$), then $\{A : f^{-1}(A) \in \mathcal{E}\}$ is a σ-algebra containing $\mathcal{A}$ and hence $\mathcal{G}$, so f is measurable.

Proposition 15.2.2 (inverse image preserves set operation)**.** The set $\{f^{-1}(A) : A \in \mathcal{G}\}$ is a σ-algebra on E and $\{A \subseteq G : f^{-1}(A) \in \mathcal{E}\}$ is a σ-algebra on G.[2]

Proof. For any function $f : E \to G$ and $A_i, A \subseteq B \in \mathcal{G}$, we have $f^{-1}(A^c) = E \setminus f^{-1}(A) = \left(f^{-1}(A)\right)^c$, $f^{-1}(A) \subseteq f^{-1}(B)$. Also, by Proposition 2.6.1 we have,

$$f^{-1}\left(\bigcup_i A_i\right) = \bigcup_i f^{-1}(A_i), \qquad f^{-1}(B \backslash A) = f^{-1}(B) \setminus f^{-1}(A). \tag{15.2.2}$$

Therefore, for $\mathcal{E} = \{f^{-1}(A) : A \in \mathcal{G}\}$ and $A \subseteq B, A_i \in \mathcal{G}$, we have $f^{-1}(A) \subseteq f^{-1}(B) \in \mathcal{E}$, $f^{-1}(A_i) \in \mathcal{E}$ and

$$\begin{aligned} B \backslash A \in \mathcal{G}, \quad \bigcup_i A_i \in \mathcal{G} \quad &\Rightarrow \quad f^{-1}(B \backslash A) \in \mathcal{E}, \quad f^{-1}\left(\bigcup_i A_i\right) \in \mathcal{E} \\ &\Rightarrow \quad f^{-1}(B) \setminus f^{-1}(A) \in \mathcal{E}, \quad \bigcup_i f^{-1}(A_i) \in \mathcal{E} \end{aligned}$$

Thus, $\{f^{-1}(A) : A \in \mathcal{G}\}$ is a σ-algebra on E and similar for $\{A \subseteq G : f^{-1}(A) \in \mathcal{E}\}$. $\square$

Proof. This is the direct result from Proposition 15.2.2 as $\mathcal{A}$ is also a d-system. $\square$

In the case $G = \mathbb{R}$, the Borel σ-algebra is generated by intervals of the form $(-\infty, y], y \in \mathbb{R}$, so, to show that $f : E \to \mathbb{R}$ is Borel measurable, it suffices to show that $\{x \in E : f(x) \leq y\} \in \mathcal{E}$ for all y.[3]

Proposition 15.2.3. For topological space $(E, \mathcal{T})$, any continuous function $f : E \to \mathbb{R}$ is $\mathcal{B}(E)$-measurable.

Proof. If $(E, \mathcal{B}(E))$ is Borel measurable space and $f : E \to \mathbb{R}$ is continuous, then $f^{-1}(U)$ is open in E, whenever U is open in $\mathbb{R}$ (Definition 13.1.3). Thus, $f^{-1}(U) \in \mathcal{B}(E)$ since $\mathcal{B}(E)$ is generated by all the open sets in E and hence any continuous function is measurable[4]. $\square$

Definition 15.2.2. Given any family of functions $f_i : E \to G, i \in I$, we can make them all measurable by taking

$$\mathcal{E} = \sigma\left(f_i^{-1}(A) : A \in \mathcal{G}, i \in I\right). \tag{15.2.3}$$

Then $\mathcal{E}$ is the σ-algebra generated by $(f_i : i \in I)$, and is often denoted by $\sigma(f_i, i \in I)$.

[2] should be in topology
[3] this should be a proposition. see Rogers-Williams [11] I P89.
[4] see Rogers & Williams I P90.

Definition 15.2.3 (indicator function)**.** For $A \subseteq E$, the indicator function $\mathbb{1}_A$ of A is the function $\mathbb{1}_A : E \to \{0,1\}$ which takes the value 1 on A and 0 otherwise, i.e.,

$$\mathbb{1}_A(x) = \begin{cases} 1 & x \in A, \\ 0 & x \notin A, \end{cases} \tag{15.2.4}$$

Proposition 15.2.4. Let A and B be two sets in E. Then

(i) $\mathbb{1}_{A^c} = 1 - \mathbb{1}_A$.

(ii) $\mathbb{1}_{A\cap B} = \mathbb{1}_A \mathbb{1}_B$.

(iii) $\mathbb{1}_{A\cup B} = 1 - (1 - \mathbb{1}_A)(1 - \mathbb{1}_B)$.

(iv) For sets $A_1, A_2, \ldots, A_n$, (ii) and (iii) generalize to $\mathbb{1}_{A_1\cap A_2\cap\cdots\cap A_n} = \prod_{i=1}^n \mathbb{1}_{A_i}$, and

$$\begin{aligned} \mathbb{1}_{A_1\cup A_2\cup\cdots\cup A_n} = 1 - \prod_{i=1}^n (1 - \mathbb{1}_{A_i}) &= \sum_i \mathbb{1}_{A_i} - \sum_{i_1<i_2} \mathbb{1}_{A_{i_1}} \mathbb{1}_{A_{i_2}} + \sum_{i_1<i_2<i_3} \mathbb{1}_{A_{i_1}} \mathbb{1}_{A_{i_2}} \mathbb{1}_{A_{i_3}} - \cdots + (-1)^{n-1} \mathbb{1}_{A_1} \ldots \mathbb{1}_{A_n} \\ &= \sum_i \mathbb{1}_{A_i} - \sum_{i_1<i_2} \mathbb{1}_{A_{i_1}\cap A_{i_2}} + \sum_{i_1<i_2<i_3} \mathbb{1}_{A_{i_1}\cap A_{i_2}\cap A_{i_3}} - \cdots + (-1)^{n-1} \mathbb{1}_{A_1\cap\cdots\cap A_n}. \end{aligned}$$

Proof. Direct results from Definition 15.2.3. □

Remark. (iv) provides an alternate proof of the inclusion-exclusion formula (see Proposition 19.1.6).

Proposition 15.2.5. The indicator function of any measurable set is a measurable function.

Proof. For any measurable set $A \in \mathcal{E}$, we have $A^c \in \mathcal{E}$,
Case 1. If $y \geq 1$, we have $\{x \in E : \mathbb{1}_A(x) \leq y\} = E \in \mathcal{E}$,
Case 2. If $y < 0$, we have $\{x \in E : \mathbb{1}_A(x) \leq y\} = \{x \in E : \mathbb{1}_A(x) > y\}^c = E \in \mathcal{E} \Rightarrow \{x \in E : \mathbb{1}_A(x) \leq y\} = \emptyset \in \mathcal{E}$,
Case 3. If $y \in [0,1)$, we have $\{x \in E : \mathbb{1}_A(x) \leq y\} = A^c \in \mathcal{E}$. □

Proposition 15.2.6. The composition of measurable functions is measurable.

Proof. For the measurable spaces $(E,\mathcal{E})$, $(G,\mathcal{G})$, $(H,\mathcal{H})$ and the functions $f : E \to G$ and $g : G \to H$ are measurable if $f^{-1}(A) \in \mathcal{E}$ whenever $A \in \mathcal{G}$, $f^{-1}(B) \in \mathcal{G}$ whenever $B \in \mathcal{H}$ respectively. Thus, given $A = f^{-1}(B)$, $f^{-1}(A) \in \mathcal{E}$ whenever $B \in \mathcal{H}$, for the composition function $f \circ g : E \to H$ and hence it is measurable. □

In the following theorem, we agree that $\frac{x}{0} := 0$ for all $x \in \mathbb{R}$.

Theorem 15.2.7. Let $f, g : E \to \mathbb{R}$, $n \in \mathbb{N}$ be $\mathcal{B}(\mathbb{R})$-measurable functions and $\lambda \in \mathbb{R}$. Then so are f^+, f^-, $f + g$[5], fg, λf and f/g.

Proof. (i) $f^+ = \max\{f, 0\} \geq 0$. We have for any $y \in \mathbb{R}$, if $y < 0$, $\{x \in E : f^+(x) \leq y\} = \emptyset \in \mathcal{E}$. For the case $y \geq 0$,

$$\{x \in E : f^+(x) \leq y\} = \{x \in E : f^+(x) > y\}^c = \{x \in E : f(x) > y\}^c = \{x \in E : f(x) \leq y\} \in \mathcal{E} \tag{15.2.5}$$

as f is measurable. Thus, f^+ is measurable. Similarly, f^- is measurable.

(ii) Note that

$$\{f + g > y\} = \bigcup_{q\in\mathbb{Q}} \{f > q\} \cap \{g > y - q\} \Rightarrow f + g \text{ is measurable.} \tag{15.2.6}$$

(iii) Using the identity $ab = \frac{1}{4}\left((a+b)^2 - (a-b)^2\right)$, it suffices to prove that f^2 is measurable whenever f is. So

$$\begin{aligned} & \{f^2 > y\} = E\mathbb{1}_{\{y<0\}} \cup \{-\sqrt{y} < f < \sqrt{y}\}\mathbb{1}_{\{y\geq 0\}} \\ = \;& E\mathbb{1}_{\{y<0\}} \cup \left(\{f < \sqrt{y}\} \cap \{f > -\sqrt{y}\}\right) \mathbb{1}_{\{y\geq 0\}} \\ = \;& E\mathbb{1}_{\{y<0\}} \cup \left(\left(\bigcup_n \{f \leq \sqrt{y} - 1/n\}\right) \cap \{f > -\sqrt{y}\}\right) \mathbb{1}_{\{y\geq 0\}} \quad \Rightarrow \quad fg \text{ is measurable.} \end{aligned}$$

[5] what about countably many f?

(iv) For $\lambda \in \mathbb{R}$,

$$\begin{aligned}\{\lambda f > y\} &= \{f > y/\lambda\}\mathbb{1}_{\{\lambda>0\}} \cup \{f < y/\lambda\}\mathbb{1}_{\{\lambda<0\}} \cup \{0 > y\}\mathbb{1}_{\{\lambda=0\}} \\ &= \{f > y/\lambda\}\mathbb{1}_{\{\lambda>0\}} \cup \left(\bigcup_n \{f \le y/\lambda - 1/n\}\mathbb{1}_{\{\lambda<0\}}\right) \cup \{0 > y\}\mathbb{1}_{\{\lambda=0\}} \quad \Rightarrow \quad \lambda f_1 \text{ is measurable.}\end{aligned}$$

(v) [6]

□

Theorem 15.2.8. Let $f, g : E \to \overline{\mathbb{R}}$, $n \in \mathbb{N}$ be $\mathcal{B}(\overline{\mathbb{R}})$-measurable functions (see Klenke [10].P_{39}). Then the following function are measurable:

$$\inf_n f_n, \quad \sup_n f_n, \quad \liminf_n f_n, \quad \limsup_n f_n. \tag{15.2.7}$$

Also, for any sequence $(f_n : n \in \mathbb{N})$ of measurable functions on $(E, \mathcal{E})$,

$$\{x \in E : f_n(x) \text{ converges as } n \to \infty\} \in \mathcal{E}. \tag{15.2.8}$$

Proof. (i) $\forall a \in \mathbb{R}$, $\{x \in E : \inf_n f_n(x) > a\} = \bigcap_n f_n^{-1}((a, \infty))$, so $\inf_n f_n$ is measurable.

(ii) If f is measurable, $-f$ is also measurable. Thus $\sup_n f_n = -\inf_n(-f_n)$ is measurable.

(iii) Since $\inf_n f_n$ and $\sup_n f_n$ are measurable,

$$\liminf_n f_n = \sup_n \left(\inf_{m \ge n} f_m\right) \quad \text{and} \quad \limsup_n f_n = \inf_n \left(\sup_{m \ge n} f_m\right) \text{ are measurable.} \tag{15.2.9}$$

(iv) Let $g = \liminf_n f_n$ and $h = \limsup_n f_n$, we have

$$\{x \in E : f_n(x) \text{ converges as } n \to \infty\} = g^{-1}((-\infty, \infty)) \cap h^{-1}((-\infty, \infty)) \cap (h - g)^{-1}(\{0\}) \in \mathcal{E}. \tag{15.2.10}$$

Thus, $\{x \in E : f_n(x) \text{ converges as } n \to \infty\} \in \mathcal{E}$.

□

Theorem 15.2.9 (monotone class Theorem)**.** Let $(E, \mathcal{E})$ be a measurable space and let $\mathcal{A}$ be a π-system generating $\mathcal{E}$. Let $\mathcal{V}$ be a vector space of bounded functions (satisfying some conditions) $f : E \to \mathbb{R}$ such that:

(i) $\mathbb{1}_E \in \mathcal{V}$ and $\mathbb{1}_A \in \mathcal{V}$ for all $A \in \mathcal{A}$;

(ii) if $f_n \in \mathcal{V}$ for all n and f is bounded with $0 \le f_n \uparrow f$, then $f \in \mathcal{V}$.

Then $\mathcal{V}$ contains every bounded measurable function.

Remark. The monotone class theorem says that the smallest monotone class containing an algebra $\mathcal{A}$ is precisely the smallest σ-algebra containing $\mathcal{A}$.

Proof. Consider $\mathcal{D} = \{A \in \mathcal{E} : \mathbb{1}_A \in \mathcal{V}\}$. Clearly, $\mathcal{A} \subseteq \mathcal{D} \subseteq \mathcal{E}$. Now we show that $\mathcal{D}$ is a d-system containing $\mathcal{A}$,

(i) $E \in \mathcal{D}$ since $E \in \mathcal{E}$ and $\mathbb{1}_E \in \mathcal{V}$ by definition (i) of $\mathcal{V}$, then $E \in \mathcal{D}$.

(ii) For all $A, B \in \mathcal{D}$ with $A \subseteq B$, we have $\mathbb{1}_A = \{0, 1\} \ \Rightarrow \ \mathbb{1}_{\{A \cap B\}} = \mathbb{1}_A \mathbb{1}_B = \mathbb{1}_B \cdot (0 \text{ or } 1) \in \mathcal{V}$ by definition of vector space.

$$\left\{ \begin{array}{l} A, B \in \mathcal{E} \ \Rightarrow \ B \backslash A \in \mathcal{E}, \quad \text{(definition of } \mathcal{E}) \\ \mathbb{1}_A \in \mathcal{V}, \ \mathbb{1}_B \in \mathcal{V} \ \Rightarrow \ \mathbb{1}_{\{B \backslash A\}} = \underbrace{\mathbb{1}_B - \mathbb{1}_{\{A \cap B\}} \in \mathcal{V}}_{\text{definition of vector space}} \end{array} \right\} \ \Rightarrow \ B \backslash A \in \mathcal{D}. \tag{15.2.11}$$

(iii) For all increasing sequences $(A_n : n \in \mathbb{N}) \in \mathcal{D}$, then let $A = \bigcup_n A_n$,

$$\left\{ \begin{array}{l} A_n \in \mathcal{E} \ \Rightarrow \ \bigcup_n A_n \in \mathcal{E}, \quad \text{(definition of } \mathcal{E}) \\ \mathbb{1}_{A_n} \in \mathcal{V} \ \Rightarrow \ \mathbb{1}_A \in \mathcal{V} \quad \text{(definition (ii) of } \mathcal{V}) \ \Rightarrow \ \mathbb{1}_{\{\bigcup_n A_n\}} \in \mathcal{V} \end{array} \right\} \ \Rightarrow \ \bigcup_n A_n \in \mathcal{D}. \tag{15.2.12}$$

[6] still need f/g

Hence, we have $\mathcal{D}$ is also a d-system containing $\mathcal{A}$, thus $\mathcal{D}$ also contains σ-algebra generated by $\mathcal{A}$, $\mathcal{E}$ (by Dynkin's Lemma (Lemma 15.1.3)). Thus, $\mathcal{E} \subseteq \mathcal{D} \Rightarrow \mathcal{D} = \mathcal{E}$.

Since $\mathcal{V}$ is a vector space, it thus contains all finite linear combinations of indicator functions of measurable sets.

For any bounded and non-negative measurable function f, the functions

$$f_n = 2^{-n} \lfloor 2^n f \rfloor \wedge n, \quad n \in \mathbb{N} \quad \text{are measurable as} \quad \lfloor 2^n f \rfloor = \sum_{k=1}^{\infty} \mathbb{1}_{\{2^n f \geq k\}} = \sum_{k=1}^{\infty} \mathbb{1}_{\{f \geq k2^{-n}\}} \tag{15.2.13}$$

is measurable (since f is measurable). Hence f_n belong to $\mathcal{V}$ and $0 \leq f_n \uparrow f$, so $f \in \mathcal{V}$ (by definition (ii) of $\mathcal{V}$).

Finally, any bounded measurable function f is the difference of two non-negative such functions, f^+ and f^-,

$$f = f^+ - f^-, \qquad \text{where} \quad f^+ = \max\{f, 0\}, \quad f^- = \max\{-f, 0\}. \tag{15.2.14}$$

From proposition 15.2.7, we know that both of f^+ and f^- are measurable. Also,

$$\left|f^+\right| = |\max\{f, 0\}| \leq |f| < \infty, \qquad \left|f^-\right| = |\max\{-f, 0\}| \leq |f| < \infty. \tag{15.2.15}$$

Thus f^+ and f^- are bounded and therefore $f^+, f^- \in \mathcal{V}$. So $f \in \mathcal{V}$ by the definition of vector space. □

15.2.2 Image measures

Definition 15.2.4. Let $(E, \mathcal{E})$ and $(G, \mathcal{G})$ be measurable spaces and let μ be a measure on $\mathcal{E}$. Then any measurable function $f : E \to G$ induces an image measure $\nu = \mu \circ f^{-1}$ on $\mathcal{G}$[7], given by

$$\nu(A) = \mu(f^{-1}(A)). \tag{15.2.16}$$

We shall construct some new measures from Lebesgue measure in this way.

Lemma 15.2.10. Let $g : \mathbb{R} \to \mathbb{R}$ be non-constant, right-continuous and non-decreasing. Let $I = (g(-\infty), g(\infty))$ and define $f : I \to \mathbb{R}$ by $f(x) = \inf\{y \in \mathbb{R} : x \leq g(y)\}$. Then f is left-continuous and non-decreasing. Moreover, for $x \in I$ and $y \in \mathbb{R}$,

$$f(x) \leq y \quad \text{if and only if} \quad x \leq g(y). \tag{15.2.17}$$

Proof. Fix $x \in I$ and consider the set $J_x = \{y \in \mathbb{R} : x \leq g(y)\}$. Note that J_x is non-empty and is not the whole of $\mathbb{R}$.

Since g is non-decreasing, if $y \in J_x$ and $y' \geq y$, then $y' \in J_x$. Since g is right-continuous, if $y_n \in J_x$ and $y_n \downarrow y$, then $y \in J_x$. Thus, J_x is closed. Hence $J_x = [f(x), \infty)$ and $x \leq g(y)$ if and only if $f(x) \leq y$.

For $x \leq x'$, we have $J_x \supseteq J_{x'}$ and so $f(x) \leq f(x')$, thus f is non-dereasing. For $x_n \uparrow x$, we have $J_x = \cap_n J_{x_n}$. Since f is bounded and non-decreasing, $\ell = \lim f(x_n)$ exists by monotonicity, then

$$[f(x), \infty) = J_x = \bigcap_n J_{x_n} = \bigcap_n [f(x_n), \infty) = [\ell, \infty) \Rightarrow f(x) = \ell = \lim f(x_n). \tag{15.2.18}$$

Thus, $f(x_n) \to f(x)$. So f is left-continuous and non-decreasing. □

Theorem 15.2.11. Let $g : \mathbb{R} \to \mathbb{R}$ be non-constant, right-continuous and non-decreasing. Then there exists a unique Borel measure dg on $\mathbb{R}$ such that, for all $a, b \in \mathbb{R}$ with $a < b$,

$$dg((a, b]) = g(b) - g(a). \tag{15.2.19}$$

Moreover, we obtain in this way all non-zero Radon measures on $\mathbb{R}$.

The measure dg is called the Lebesgue-Stieltjes measure associated with g.

Proof. Define I and f as in Lemma 15.2.10 and let μ denote Lebesgue measure on I. Then f is Borel measurable, since for all $y \in \mathbb{R}$,

$$\{x \in I : f(x) \leq y\} = \{x \in I : x \leq g(y)\} = I \cap (-\infty, g(y)]. \tag{15.2.20}$$

[7] should prove that ν is a measure

The induced Borel measure $dg = \mu \circ f^{-1}$ on $\mathbb{R}$ satisfies

$$dg((a,b]) = \mu(f^{-1}((a,b])) = \underbrace{\mu\left(\{x : f(x) > a \text{ and } f(x) \leq b\}\right) = \mu\left((g(a), g(b)]\right)}_{f(x) \leq y \text{ if and only if } x \leq g(y)} = g(b) - g(a). \tag{15.2.21}$$

The argument used for uniqueness of Lebesgue measure (Theorem 15.1.19) shows that there is a unique (Lebesgue measure) μ with this property and therefore there is a unique Borel measure dg with this property.

Finally, if ν is any non-zero Radon measure on $\mathbb{R}$, we can define $g : \mathbb{R} \to \mathbb{R}$, by

$$g(y) = \begin{cases} \nu((0,y]) & y \geq 0, \\ -\nu((y,0]) & y < 0. \end{cases} \tag{15.2.22}$$

Then g is nondecreasing and nonconstant, since ν is not the zero measure. Moreover, ν is finite-valued for compact set $[0,y]$ or $[y,0]$, thus $\nu((0,y])$ or $\nu((y,0])$ are finite (due to the additivity of measure).

If $y \geq 0$, let $y_n \downarrow y \geq 0$. Then $\bigcap_n (y, y_n] = \emptyset$, $\nu((y,y_n])$ are finite and $\nu((y,y_n]) \to 0$ by 15.1.7. Thus

$$g(y) = \nu((0,y]) = \nu((0,y_n]) - \nu((y,y_n]) \to \lim_{n\to\infty} \nu((0,y_n]) \tag{15.2.23}$$

since the limit exists as $\nu((0,y_n])$ is monotone and bounded (Fundamental Axiom of Real Numbers, Axiom 10.2.1).

If $y < 0$, let $0 > y_n \downarrow y$. Then similarly, $\bigcap_n (y, y_n] = \emptyset$, $\nu((y,y_n])$ are finite and $\nu((y,y_n]) \to 0$ by 15.1.7.

$$g(y) = -\nu((y,0]) = -\left(\nu((y,y_n]) + \nu((y_n,0])\right) \to -\lim \nu((y_n,0]). \tag{15.2.24}$$

Again, the limit exists as $\nu((0,y_n])$ is monotone and bounded (fundamental axiom of real numbers, Axiom 10.2.1). So g is right-continuous. Then $\nu((a,b]) = g(b) - g(a)$ whenever $a < b$, so $\nu = dg$ by uniqueness. □

Example 15.2.12. Let $\alpha > 0$, and let $g(x) = \alpha x$. Then g satisfies the conditions of Theorem 15.2.11, and the Lebesgue-Stieltjes measure associated with it is $dg = \alpha\mu$, where μ is Lebesgue measure.

Example 15.2.13. Dirac mass. Let $x \in \mathbb{R}$, and $k > 0$. The Dirac mass at the point x, with mass k is the Borel measure on $\mathbb{R}$ defined by

$$\mu(A) = k \quad \text{if } x \in A \tag{15.2.25}$$

and $\mu(A) = 0$ else, for all Borel set A. Then μ is a Radon measure. Moreover, it is the Radon measure dg associated with the function:

$$g(t) = k\mathbb{1}_{[x,\infty)}(t). \tag{15.2.26}$$

If $k = 1$, then μ is simply denoted by $\delta_{\{x\}}$, and hence in general μ is written $k\delta_{\{x\}}$. We thus have

$$\delta_{\{x\}} = dg, \tag{15.2.27}$$

where g is the Heavyside function at x.

15.2.3 Convergence in measure and convergence almost everywhere

Definition 15.2.5. Let $(E, \mathcal{E}, \mu)$ be a measure space. A set $A \in \mathcal{E}$ is sometimes defined by a property shared by its elements. If $\mu(A^c) = 0$, then we say that property holds almost everywhere (or a.e.). Thus, for a sequence of measurable functions $(f_n : n \in \mathbb{N})$, we say f_n converges to f a.e. to mean that

$$\mu(\{x \in E : f_n(x) \nrightarrow f(x)\}) = 0, \qquad \text{denoted as } f_n \to f \text{ a.e..} \tag{15.2.28}$$

Definition 15.2.6. Let $(E, \mathcal{E}, \mu)$ be a measure space. For a sequence of measurable functions $(f_n)_{n\in\mathbb{N}}$ and a measurable function f, we have that

$$\mu(\{x \in E : |f_n(x) - f(x)| > \varepsilon\}) \to 0, \quad \text{for all } \varepsilon > 0, \tag{15.2.29}$$

then we say f_n converges to f in measure, denoted as $f_n \xrightarrow{\mu} f$.

Theorem 15.2.14. Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of measurable functions.

(i) Assume that $\mu(E) < \infty$. If $f_n \to 0$ a.e. then $f_n \to 0$ in measure.

(ii) If $f_n \to 0$ in measure then $f_{n_k} \to 0$ a.e. for some subsequence (n_k).

Proof. (i) Suppose $f_n \to 0$ a.e.. For each $\varepsilon > 0$,

$$\mu(|f_n| \le \varepsilon) \ge \underbrace{\mu\left(\bigcap_{m\ge n} \{|f_m| \le \varepsilon\}\right)}_{\text{Lemma } 15.1.10} \uparrow \mu(|f_n| \le \varepsilon \text{ ev.}) \ge \mu(f_n \to 0), \tag{15.2.30}$$

$$\mu(|f_n| > \varepsilon) = \mu(E) - \mu(|f_n| \le \varepsilon) \le \mu(E) - \mu(f_n \to 0) = \mu(f_n \nrightarrow 0) = 0. \tag{15.2.31}$$

Hence $\mu(|f_n| > \varepsilon) \to 0$ and $f_n \to 0$ in measure.

(ii) Suppose $f_n \to 0$ in measure, then $\forall \varepsilon > 0$, $\mu(\{|f_n| > \varepsilon\}) \to 0$ i.e.

$$\forall \varepsilon > 0,\ \delta > 0,\ \exists N,\ \forall n \ge N, \quad \mu(\{|f_n| > \varepsilon\}) < \delta. \tag{15.2.32}$$

so we can find a subsequence (n_k) such that $\varepsilon_k = 1/k$ and $\delta_k = 2^{-k}$,

$$\mu\left(\{|f_{n_k}| > 1/k\}\right) < 2^{-k} \ \Rightarrow\ \sum_k \mu(\{|f_{n_k}| > 1/k\}) < \sum_k 2^{-k} = 1 < \infty. \tag{15.2.33}$$

So, by the first Borel-Cantelli lemma (Lemma 15.1.13),

$$0 = \mu(\{|f_{n_k}| > 1/k \text{ i.o.}\}) = \mu\left(\{|f_{n_k}| \le 1/k \text{ ev.}\}^c\right) = \mu\left(\{f_{n_k} \to 0\}^c\right) \ \Rightarrow\ f_{n_k} \to 0 \text{ a.e.}. \tag{15.2.34}$$

□

Proposition 15.2.15 (uniqueness of limit of convergence in measure)**.** Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of measurable functions and f, g be measurable functions. If $f_n \to f$ in measure and $f_n \to g$ in measure,

$$f = g \text{ a.e.} \quad \text{i.e., } \mu\left(x : f(x) \ne g(x)\right) = 0. \tag{15.2.35}$$

Proof. If $f_n \to f$ in measure and $f_n \to g$ in measure, we have for any ε,

$$\mu\left(|f_n - f| > \varepsilon\right) \to 0, \quad \mu\left(|f_n - g| > \varepsilon\right) \to 0 \tag{15.2.36}$$

as $n \to \infty$. Thus,

$$\mu\left(|f - g| > \varepsilon\right) \le \mu\left(|f_n - f| + |f_n - g| > \varepsilon\right) \le \mu\left(|f_n - f| > \varepsilon/2\right) + \mu\left(|f_n - g| > \varepsilon/2\right) \to 0. \tag{15.2.37}$$

Thus, $\mu\left(|f - g| > \varepsilon\right) = 0$ which imples that $f = g$ a.e.. □

15.3 Integration and Basic Theorems

15.3.1 Definition of integral and basic properties

Definition 15.3.1. For measure space $(E, \mathcal{E}, \mu)$, a simple function is a non-negative one may be written as a finite sum

$$f = \sum_{i=1}^m a_i \mathbb{1}_{A_i} \tag{15.3.1}$$

where $a_i \in [0, \infty]$ and $A_i \in \mathcal{E}$ for all i, and where $m \in \mathbb{N}$.

Definition 15.3.2. For measure space $(E, \mathcal{E}, \mu)$ and simple functions $f = \sum_{i=1}^m a_i \mathbb{1}_{A_i}$ and measure space $(E, \mathcal{E}, \mu)$, we define

$$\mu(f) = \sum_{i=1}^m a_i \mu(A_i), \tag{15.3.2}$$

where we adopt the convention $0 \cdot \infty = 0$.

Although the representation of f is not unique, it is straightforward to check that $\mu(f)$ is well defined and ensure that they yield the same value.

Definition 15.3.3. For measure space $(E, \mathcal{E}, \mu)$ and a simple function f with the form of $f = \sum_{i=1}^m a_i \mathbb{1}_{A_i}$, if $A_1, \ldots, A_m \in \mathcal{E}$ are disjoint sets, then the form is called a normal representation of f.

Lemma 15.3.1. A simple function f has two normal representations:

$$f = \sum_{i=1}^m a_i \mathbb{1}_{A_i} = \sum_{j=1}^n b_j \mathbb{1}_{B_j} \quad \Rightarrow \quad \mu(f) = \sum_{i=1}^m a_i \mu(A_i) = \sum_{j=1}^n b_j \mu(B_j). \tag{15.3.3}$$

Proof. If $\mu(A_i \cap B_j) > 0$ for some i and j, then $A_i \cap B_j \neq \emptyset$, and for any $x \in A_i \cap B_j$

$$f(x) = \sum_{i=1}^m a_i \mathbb{1}_{A_i} = a_i = b_j = \sum_{j=1}^n b_j \mathbb{1}_{B_j}, \tag{15.3.4}$$

for the disjoint sets A_i and disjoint sets B_j. Furthermore, clearly $A_i \subseteq \bigcup_{j=1}^n B_j$ if $a_i \neq 0$, and $B_j \subseteq \bigcup_{i=1}^m A_i$ if $b_j \neq 0$. We conclude that

$$\sum_{i=1}^m a_i \mu(A_i) = \sum_{i=1}^m \sum_{j=1}^n a_i \mu(A_i \cap B_j) = \sum_{j=1}^n \sum_{i=1}^m b_j \mu(A_i \cap B_j) = \sum_{j=1}^n b_j \mu(B_j). \qquad \square$$

Lemma 15.3.2. A simple function f has two representations:

$$f = \sum_{i=1}^m a_i \mathbb{1}_{A_i} = \sum_{j=1}^n b_j \mathbb{1}_{B_j} \quad \Rightarrow \quad \mu(f) = \sum_{i=1}^m a_i \mu(A_i) = \sum_{j=1}^n b_j \mu(B_j). \tag{15.3.5}$$

Proof. For $\varepsilon \in \{0,1\}^m$ define $A_\varepsilon = A_1^{\varepsilon_1} \cap \cdots \cap A_m^{\varepsilon_m}$ where $A_i^0 = A_i^c$, $A_i^1 = A_i$.

For $\delta \in \{0,1\}^n$ define $B_\delta = B_1^{\delta_1} \cap \cdots \cap B_n^{\delta_n}$ where $B_j^0 = B_j^c$, $B_j^1 = B_j$. Then set

$$f_{\varepsilon,\delta} = \begin{cases} \sum_{i=1}^m a_i \varepsilon_i & \text{if } A_\varepsilon \cap B_\delta \neq \emptyset \\ \infty & \text{otherwise.} \end{cases} \tag{15.3.6}$$

We note that the sets A_ε are disjoint and $A_k = \bigcup_{\varepsilon : \varepsilon_k = 1} A_\varepsilon$. Thus, for any measure μ,

$$\mu(A_k) = \sum_\varepsilon \varepsilon_k \mu(A_\varepsilon) = \sum_\delta \sum_\varepsilon \varepsilon_k \mu(A_\varepsilon \cap B_\delta) \tag{15.3.7}$$

Then $\sum_{i=1}^m a_i \mu(A_i) = \sum_{i=1}^m a_i \sum_\delta \sum_\varepsilon \varepsilon_i \mu(A_\varepsilon \cap B_\delta) = \sum_\delta \sum_\varepsilon \mu(A_\varepsilon \cap B_\delta) \sum_{i=1}^m a_i \varepsilon_i = \sum_{\varepsilon,\delta} \mu(A_\varepsilon \cap B_\delta) f_{\varepsilon,\delta}$. If $A_\varepsilon \cap B_\delta \neq \emptyset$, for any point $x \in A_\varepsilon \cap B_\delta$, $f(x) = \sum_{i=1}^m a_i \varepsilon_i = \sum_{j=1}^n b_j \delta_j = f_{\varepsilon,\delta}$. Then by symmetry, we have

$$\sum_{\varepsilon,\delta} \mu(A_\varepsilon \cap B_\delta) f_{\varepsilon,\delta} = \sum_\delta \sum_\varepsilon \mu(A_\varepsilon \cap B_\delta) \sum_{j=1}^n b_j \delta_j = \sum_{j=1}^n b_j \sum_\delta \sum_\varepsilon \delta_j \mu(A_\varepsilon \cap B_\delta) = \sum_{j=1}^n b_j \mu(B_j). \tag{15.3.8}$$

Hence $\mu(f)$ is well-defined. $\square$

Proposition 15.3.3. Every simple function has normal representation.

Proof. Assume $f = \sum_{i=1}^m a_i \mathbb{1}_{A_i}$ and let

$$B_1 = A_i, \qquad b_1 = a_1 + \sum_{i=2}^m a_i \mathbb{1}_{A_1 \cap A_i}, \tag{15.3.9}$$

and then we have $A_j' = A_{j+1} \backslash A_1$, $a_j' = a_{j+1}$, $j = 1, \ldots, m-1$. Repeating the above steps for A_j', we get disjoint set B_i such that

$$f = \sum_{i=1}^m a_i \mathbb{1}_{A_i} = \sum_{j=1}^m b_j \mathbb{1}_{B_j}, \tag{15.3.10}$$

which is normal representation. □

Proposition 15.3.4. For simple functions f, g and constants $\alpha, \beta \in [0, \infty]$, we have

(i) $\mu(\alpha f + \beta g) = \alpha\mu(f) + \beta\mu(g)$,

(ii) $f \le g$ a.e. implies $\mu(f) \le \mu(g)$, $f = g$ a.e. implies $\mu(f) = \mu(g)$,

(iii) $f = 0$ a.e. if and only if $\mu(f) = 0$.

Proof. Let $f = \sum_{i=1}^m a_i \mathbb{1}_{A_i}$ and $g = \sum_{j=1}^n b_j \mathbb{1}_{B_i}$, $a_i, b_i \in [0, \infty]$, where A_i and B_j are disjoint (by Proposition 15.3.3).

(i) We have $\mu(\alpha f + \beta g) = \mu\left(\alpha \sum_{i=1}^m a_i \mathbb{1}_{A_i} + \beta \sum_{j=1}^n b_j \mathbb{1}_{B_i}\right) = \mu\left(\sum_{i=1}^m \alpha a_i \mathbb{1}_{A_i} + \sum_{j=1}^n \beta b_j \mathbb{1}_{B_i}\right)$, then

$$\mu(\alpha f + \beta g) = \sum_{i=1}^m \alpha a_i \mu(A_i) + \sum_{j=1}^n \beta b_j \mu(B_i) = \alpha \sum_{i=1}^m a_i \mu(A_i) + \beta \sum_{j=1}^n b_j \mu(B_i) = \alpha\mu(f) + \beta\mu(g).$$

(ii) We have $g = \sum_{i=1}^m \left(\sum_{j=1}^n b_j \mathbb{1}_{A_i \cap B_j}\right) \mathbb{1}_{A_i} + \sum_{j=1}^n b_j \mathbb{1}_{B_j \setminus \bigcup_{i=1}^n A_i}$ where A_i and $B_j \setminus \bigcup_{i=1}^n A_i$ are $m + n$ disjoint sets. $\forall A_i$, $\forall x \in A_i$, $a_i = f(x) \le g(x) = \sum_{j=1}^n b_j \mathbb{1}_{A_i \cap B_j}$. Hence,

$$\begin{aligned} \mu(f) &= \mu\left(\sum_{i=1}^m a_i \mathbb{1}_{A_i}\right) = \sum_{i=1}^m a_i \mu(A_i) \le \sum_{i=1}^m \left(\sum_{j=1}^n b_j \mathbb{1}_{A_i \cap B_j}\right) \mu(A_i) \\ &\le \sum_{i=1}^m \left(\sum_{j=1}^n b_j \mathbb{1}_{A_i \cap B_j}\right) \mu(A_i) + \sum_{j=1}^n b_j \mu\left(B_j \setminus \bigcup_{i=1}^n A_i\right) = \mu(g). \end{aligned}$$

If $f \le g$ a.e., we have simple functions $f\mathbb{1}_{\{f \le g\}}$ and $f\mathbb{1}_{\{f > g\}}$,

$$\mu(f) = \mu\left(f\mathbb{1}_{\{f \le g\}} + f\mathbb{1}_{\{f > g\}}\right) = \mu\left(f\mathbb{1}_{\{f \le g\}}\right) + \mu\left(f\mathbb{1}_{\{f > g\}}\right). \quad \text{by (i)} \tag{15.3.11}$$

Then we have $f\mathbb{1}_{\{f \le g\}} \le g \Rightarrow \mu\left(f\mathbb{1}_{\{f \le g\}}\right) \le \mu(g)$, and simple functions

$$f\mathbb{1}_{\{f > g\}} \le \left(\sup_{x \in E} f(x)\right) \mathbb{1}_{\{f > g\}} \quad \Rightarrow \quad \mu\left(f\mathbb{1}_{\{f > g\}}\right) \le \mu\left(\left(\sup_{x \in E} f(x)\right) \mathbb{1}_{\{f > g\}}\right). \tag{15.3.12}$$

$$\begin{aligned} \Rightarrow \quad \mu(f) &= \mu\left(f\mathbb{1}_{\{f \le g\}}\right) + \mu\left(f\mathbb{1}_{\{f > g\}}\right) \le \mu(g) + \mu\left(f\mathbb{1}_{\{f > g\}}\right) \le \mu(g) + \mu\left(\left(\sup_{x \in E} f(x)\right) \mathbb{1}_{\{f > g\}}\right) \\ &= \mu(g) + \left(\sup_{x \in E} f(x)\right) \mu\left(\mathbb{1}_{\{f > g\}}\right) \le \mu(g) + \infty \cdot \mu(\{f > g\}) = \mu(g) + \infty \cdot 0 = \mu(g) + 0 = \mu(g). \end{aligned}$$

Furthermore, if $f = g$ a.e., $f \le g$ a.e. and $g \le f$ a.e. gives that $\mu(f) \le \mu(g)$, $\mu(g) \le \mu(f) \Rightarrow \mu(f) = \mu(g)$.

(iii) ($\Rightarrow$) If $f = 0$ a.e., $\mu(\{f \ne 0\}) = 0$,

$$\begin{aligned} \mu(f) &= \mu\left(f\mathbb{1}_{\{f=0\}} + f\mathbb{1}_{\{f \ne 0\}}\right) = \mu\left(f\mathbb{1}_{\{f \ne 0\}}\right) = \mu\left(\left(\sum_{i=1}^m a_i \mathbb{1}_{A_i}\right) \mathbb{1}_{\{f \ne 0\}}\right) = \sum_{i=1}^m a_i \mu(A_i \cap \{f \ne 0\}) \\ &\le \sum_{i=1}^m a_i \mu(\{f \ne 0\}) = 0 \quad \Rightarrow \quad \mu(f) = 0. \end{aligned}$$

($\Leftarrow$) If $\mu(f) = 0$, let $\varepsilon_n = \frac{1}{n} > 0$, by (ii), we have

$$\varepsilon_n \mathbb{1}_{\{f \ge \varepsilon_n\}} \le f \quad \Rightarrow \quad \mu\left(\varepsilon_n \mathbb{1}_{\{f \ge \varepsilon_n\}}\right) \le \mu(f) \quad \Rightarrow \quad \varepsilon_n \mu\left(\mathbb{1}_{\{f \ge \varepsilon_n\}}\right) \le \mu(f) \tag{15.3.13}$$

(by definition of $\mu(f)$ (Definition 15.3.2)) since $\varepsilon_n \mathbb{1}_{\{f \geq \varepsilon_n\}}$ and f are simple functions. Then we have

$$\mu(\{f \geq \varepsilon_n\}) = \mu\left(\mathbb{1}_{\{f \geq \varepsilon_n\}}\right) \leq \frac{1}{\varepsilon_n}\mu(f). \tag{15.3.14}$$

As $\mathbb{1}_{\{f \geq \varepsilon_n\}} \uparrow \mathbb{1}_{\{f \neq 0\}}$, $\{f \geq \varepsilon_n\} \subseteq \{f \neq 0\}$ we have

$$\mu(\{f \geq \varepsilon_n\}) \uparrow \mu(\{f \neq 0\}). \qquad \text{(by fundamental property of measure (Lemma 15.1.10))} \tag{15.3.15}$$

Thus, $\mu(\{f \neq 0\}) \leq \infty \cdot \mu(f) = \infty \cdot 0 = 0 \quad \Rightarrow \quad f = 0$ a.e..

□

Definition 15.3.4. The integral $\mu(f)$ of a non-negative measurable function f by

$$\mu(f) = \sup\{\mu(g) : g \text{ is simple, } g \leq f\}. \tag{15.3.16}$$

Definition 15.3.5. Let $(E, \mathcal{E}, \mu)$ be a measure space. For any measurable function f, set $f^+ = \max\{f, 0\}$ and $f^- = \max\{-f, 0\}$. Then $f = f^+ - f^-$ and $|f| = f^+ + f^-$. Unless both $\mu(f^+)$ and $\mu(f^-)$ are ∞, we define

$$\mu(f) = \mu(f^+) - \mu(f^-). \tag{15.3.17}$$

Definition 15.3.6. Let $(E, \mathcal{E}, \mu)$ be a measure space. We shall define, where possible, for a measurable function $f : E \to [-\infty, \infty]$, the integral of f, to be denoted

$$\mu(f) = \int_E f d\mu = \int_E f(x)\mu(dx). \tag{15.3.18}$$

Here is the key result for the theory of integration.

Theorem 15.3.5 (monotone convergence theorem)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. Let f be a non-negative measurable function and let $(f_n : n \in \mathbb{N})$ be a sequence of such functions. Suppose that $f_n \uparrow f$. Then $\mu(f_n) \uparrow \mu(f)$.

Proof. We discuss in following cases:

Case 1 : If $A_n \uparrow A$, $f_n = \mathbb{1}_{A_n}$, $f = \mathbb{1}_A$ and $f_n \uparrow f$. By fundamental property of measure (Lemma 15.1.10),

$$\mu(f_n) = \mu(\mathbb{1}_{A_n}) = \underbrace{\mu(A_n) \uparrow \mu(A)}_{\text{Lemma 15.1.10}} = \mu(\mathbb{1}_A) = \mu(f) \tag{15.3.19}$$

Case 2 : f_n is simple, $f = \mathbb{1}_A$. Fix $\varepsilon > 0$ and set $A_n = \{f_n > 1 - \varepsilon\}$. Then $A_n \uparrow A$ and

$$(1-\varepsilon)\mathbb{1}_{A_n} \leq f_n \leq \mathbb{1}_A \quad \Rightarrow \quad (1-\varepsilon)\mu(A_n) \leq \mu(f_n) \leq \mu(A). \tag{15.3.20}$$

by Proposition 15.3.4 (ii). But $\mu(A_n) \uparrow \mu(A)$ by Case 1 and $\varepsilon > 0$ was arbitrary, so the result follows.

Case 3 : f_n simple, f simple. We can write f in the form $f = \sum_{k=1}^m a_k \mathbb{1}_{A_k}$ with $a_k > 0$ for all k and the sets A_k disjoint. Then $f_n \uparrow f$ implies

$$\mathbb{1}_{A_k} f_n \uparrow \left(\sum_{k=1}^m a_k \mathbb{1}_{A_k}\right) \mathbb{1}_{A_k} \quad \Rightarrow \quad \mathbb{1}_{A_k} f_n \uparrow a_k \mathbb{1}_{A_k} \quad \Rightarrow \quad a_k^{-1} \mathbb{1}_{A_k} f_n \uparrow \mathbb{1}_{A_k} \tag{15.3.21}$$

so, by Case 2,

$$\mu(f_n) = \sum_k \mu(\mathbb{1}_{A_k} f_n) \uparrow \sum_k a_k \mu(A_k) = \mu(f). \tag{15.3.22}$$

Case 4 : f_n simple, $f \geq 0$ measurable. Let g be simple with $g \leq f$. Then $f_n \uparrow f$ implies $f_n \wedge g \uparrow g$ so, by Case 3,

$$\mu(f_n) \geq \mu(f_n \wedge g) \uparrow \mu(g). \tag{15.3.23}$$

Since g was arbitrary, we have $\lim_n \mu(f_n) \geq \mu(f)$. However, we know that $\mu(f_n) \leq \mu(f)$ (by definition of $\mu(f)$, Definition 15.3.4) as f_n is simple function. Thus, $\lim_n \mu(f_n) = \mu(f)$. With Proposition 15.3.4 (ii), we have $\mu(f_n)$ is increasing, thus $\mu(f_n) \uparrow \mu(f)$.

Case 5 : $f_n \geq 0$ measurable, $f \geq 0$ measurable. Set $g_n = (2^{-n} \lfloor 2^n f_n \rfloor) \wedge n$ then g_n is simple and $g_n \leq f_n \leq f$, so by Theorem 15.3.7 (ii),

$$\mu(g_n) \leq \mu(f_n) \leq \mu(f). \tag{15.3.24}$$

But $f_n \uparrow f$ forces $g_n \uparrow f$, so $\mu(g_n) \uparrow \mu(f)$, by Case 4, and so $\mu(f_n) \uparrow \mu(f)$.

□

Proposition 15.3.6. Let μ and ν be finite Lebesgue measures. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous bounded function on $\mathbb{R}$. Show that f is Lebesgue-integrable with respect to μ and ν. If $\mu(f) = \nu(f)$ for all such f, then $\mu = \nu$.

Proof. Suppose that $|f| \leq M < \infty$. The function f is measurable as it is continuous (Proposition 15.2.3), and $\mu(f) \leq M\mu(\mathbb{R}) < \infty$, so f is moreover integrable.

Suppose that $\mu(f) = \nu(f)$ for all continuous bounded functions f. For any interval A, we can find continuous bounded functions f_n with $0 \leq f_n \uparrow \mathbb{1}_A$ as $n \to \infty$. By monotone convergence theorem (Theorem 15.3.5), we deduce that $\mu(A) = \nu(A)$. Hence $\mu = \nu$ by uniqueness of extension (Theorem 15.1.18). □

Theorem 15.3.7. For all non-negative measurable functions f, g and all constants $\alpha, \beta \in [0, \infty]$,

(i) $\mu(\alpha f + \beta g) = \alpha\mu(f) + \beta\mu(g)$,

(ii) $f \leq g$ a.e. implies $\mu(f) \leq \mu(g)$, $f = g$ a.e. implies $\mu(f) = \mu(g)$,

(iii) $f = 0$ a.e. if and only if $\mu(f) = 0$.

Proof. Define simple functions f_n, g_n by

$$f_n = (2^{-n} \lfloor 2^n f \rfloor) \wedge n, \qquad g_n = (2^{-n} \lfloor 2^n g \rfloor) \wedge n. \tag{15.3.25}$$

Then $f_n \uparrow f$ and $g_n \uparrow g$, so $\alpha f_n + \beta g_n \uparrow \alpha f + \beta g$.

(i) Hence, by monotone convergence theorem,

$$\mu(f_n) \uparrow \mu(f), \quad \mu(g_n) \uparrow \mu(g), \quad \mu(\alpha f_n + \beta g_n) \uparrow \mu(\alpha f + \beta g). \tag{15.3.26}$$

We know that $\mu(\alpha f_n + \beta g_n) = \alpha\mu(f_n) + \beta\mu(g_n)$ by Proposition 15.3.4 (i), so we have

$$\mu(\alpha f + \beta g) = \alpha\mu(f) + \beta\mu(g) \tag{15.3.27}$$

(ii) If $f \leq g$ a.e., then $f_n \leq g_n$ a.e. and $\mu(f_n) \leq \mu(g_n)$ by Proposition 15.3.4 (ii). Also, we have

$$\mu(f_n) \uparrow \mu(f), \quad \mu(g_n) \uparrow \mu(g) \quad \Rightarrow \quad \mu(f) \leq \mu(g). \tag{15.3.28}$$

(iii) ($\Rightarrow$) If $f = 0$ a.e., then $f_n = 0$ a.e., for all n, so by Proposition 15.3.4 (iii), $\mu(f_n) = 0$ for all n and $\mu(f_n) \uparrow \mu(f)$ by monotone convergence theorem. Thus $\mu(f) = 0$.

($\Leftarrow$) If $\mu(f) = 0$, we have $f_n \leq f$, by (ii), we have $\mu(f_n) \leq \mu(f) = 0$ and thus $\mu(f_n) = 0$ for all n, so $f_n = 0$ a.e. for all n by Proposition 15.3.4 (iii) i.e., $\mu\{f_n \neq 0\}) = 0$. Then

$$\{f_n \neq 0\} = \{f \geq 2^{-n}\} \uparrow \{f \neq 0\} \quad \Rightarrow \quad \mu(\{f_n \neq 0\}) \uparrow \mu(\{f \neq 0\}) \tag{15.3.29}$$

by fundamental property of measure (Lemma 15.1.10), then

$$\mu(\{f \neq 0\}) = \lim_n \mu(\{f_n \neq 0\}) = 0 \quad \Rightarrow \quad f = 0 \text{ a.e.}.$$

□

Here are some minor variants on the monotone convergence theorem.

Theorem 15.3.8 (monotone convergence theorem)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. Let f be a non-negative measurable function and $(f_n : n \in \mathbb{N})$ be a sequence of measurable functions, with $f_n \geq 0$ a.e.. Then

$$f_n \uparrow f \text{ a.e. } \Rightarrow \mu(f_n) \uparrow \mu(f). \tag{15.3.30}$$

Remark. Thus the pointwise hypotheses of non-negativity and monotone convergence can be relaxed to hold almost everywhere.

Proof. Consider $\{x : 0 \leq f_n(x) \uparrow f(x)\} \subseteq \{x : f_n(x) \uparrow f(x)\}^c \bigcup (\{x : f_n(x) \uparrow f(x)\} \bigcap (\bigcup_n \{x : f_n(x) < 0\}))$. Then we have

$$\begin{aligned}
\mu(\{x : 0 \leq f_n(x) \uparrow f(x)\}) &\leq \mu\left(\{x : f_n(x) \uparrow f(x)\}^c \bigcup \left(\{x : f_n(x) \uparrow f(x)\} \bigcap \left(\bigcup_n \{x : f_n(x) < 0\}\right)\right)\right) \\
&\leq \mu\left(\{x : f_n(x) \uparrow f(x)\}^c \bigcup \left(\bigcup_n \{x : f_n(x) < 0\}\right)\right) \\
&\leq \mu(\{x : f_n(x) \uparrow f(x)\}^c) + \sum_n \mu(\{x : f_n(x) < 0\}) = 0 + 0 \cdot \infty = 0.
\end{aligned}$$

So we have $0 \leq f_n(x) \uparrow f(x)$ a.e.. Define

$$A = \{x : 0 \leq f_n(x) \uparrow f(x)\} \quad \Rightarrow \quad f_n \mathbb{1}_A \uparrow f \mathbb{1}_A \tag{15.3.31}$$

where $f_n \mathbb{1}_A$ and $f \mathbb{1}_A$ are non-negative measurable functions. Applying monotone convergence theorem (Theorem 15.3.5), we have

$$\mu(f_n \mathbb{1}_A) \uparrow \mu(f \mathbb{1}_A) \tag{15.3.32}$$

We have $f_n \geq 0$ a.s. thus $\mu(f_n^-) = 0$, thus we can have non-negative measurable functions $f_n \mathbb{1}_{\{f_n \geq 0\}} \geq f_n \mathbb{1}_A$,

$$\mu(f_n) = \mu(f_n^+) - \mu(f_n^-) = \mu(f_n^+) = \underbrace{\mu(f_n \mathbb{1}_{\{f_n \geq 0\}}) \geq \mu(f_n \mathbb{1}_A)}_{\text{Theorem 15.3.7 (ii)}} \quad \Rightarrow \quad \mu(f_n) \uparrow \mu(f \mathbb{1}_A). \tag{15.3.33}$$

Also, $f \mathbb{1}_A = f$ a.e. implies $\mu(f \mathbb{1}_A) = \mu(f)$ by Theorem 15.3.7 (ii). Hence, $\mu(f_n) \uparrow \mu(f)$. □

Remark. There are other versions of monotone convergence theorem, i.e. Chung [5], the condition $f_n \geq 0$ a.e. may be weakened to $\mu(f_n) > -\infty$ for some n.

Proposition 15.3.9. Let $(f_n : n \in \mathbb{N})$ be a sequence of non-negative measurable functions. Then

$$\sum_{n=1}^{\infty} \mu(f_n) = \mu\left(\sum_{n=1}^{\infty} f_n\right). \tag{15.3.34}$$

Remark. This reformulation of monotone convergence makes it clear that it is the counterpart for the integration of functions of the countable additivity property of the measure on sets.

Proof. Let $g_n = \sum_{k=1}^n f_k$, then $g_n \leq g_{n+1}$ and g_n is non-negative measurable $\forall n$, thus $g_n \uparrow \sum_{k=1}^{\infty} f_k$ with $\sum_{k=1}^{\infty} f_k$ is non-negative measurable function. Thus, applying monotone convergence theorem (Theorem 15.3.5), we have

$$\mu(g_n) \uparrow \mu\left(\sum_{k=1}^{\infty} f_k\right) \quad \Rightarrow \quad \mu\left(\sum_{k=1}^{\infty} f_k\right) = \sum_{k=1}^{\infty} \mu(f_k).$$ □

Definition 15.3.7. For any measurable function f and $|f| = f^+ + f^-$. If $\mu(|f|) < \infty$, then we say that f is Lebesgue-integrable and define

$$\mu(f) = \mu(f^+) - \mu(f^-). \tag{15.3.35}$$

Remark. Note that $|\mu(f)| \leq \mu(|f|)$ for all integrable functions f. We sometimes define the integral $\mu(f)$ by the same formula, even when f is not integrable, but when either $\mu(f^-)$ or $\mu(f^+)$ is finite. In such cases the integral take the value ∞ or $-\infty$.

Theorem 15.3.10. For all integrable functions f, g and all constants $\alpha, \beta \in \mathbb{R}$,

(i) $\mu(\alpha f + \beta g) = \alpha\mu(f) + \beta\mu(g)$,

(ii) $f \le g$ a.e. implies $\mu(f) \le \mu(g)$, $f = g$ a.e. implies $\mu(f) = \mu(g)$,

(iii) $f = 0$ a.e. implies $\mu(f) = 0$,

(iv) $|\mu(f)| \le \mu\,|f|$.

Proof. We note that $\mu(-f) = -\mu(f)$ (by Definition 15.3.7).

(i) For $\alpha \ge 0$, we have

$$\mu(\alpha f) = \underbrace{\mu\left((\alpha f)^+\right) - \mu\left((\alpha f)^-\right) = \alpha\mu(f^+) - \alpha\mu(f^-)}_{\text{by Theorem 15.3.7 (i) since } f^+ \text{ and } f^- \text{ are non-negative measurable}} = \alpha\mu(f). \tag{15.3.36}$$

For $\alpha \ge 0$, we set $\beta = -\alpha > 0$

$$\mu(\alpha f) = \mu\,(-\beta f) = \underbrace{-\mu\,(\beta f) \;=\; -\,(\beta\mu(f))}_{\text{use the result from the above case}} = \alpha\mu(f). \tag{15.3.37}$$

If $h = f + g$ then $h^+ + f^- + g^- = h^- + f^+ + g^+$, so

$$\mu(h^+) + \mu(f^-) + \mu(g^-) = \mu(h^-) + \mu(f^+) + \mu(g^+) \qquad \text{(by Theorem 15.3.7 (i))} \tag{15.3.38}$$

and so $\mu(h) = \mu(f) + \mu(g)$ (by definition of μ for integrable functions).

(ii) If $f \le g$ a.e., then $f^+ \ge g^+$ a.e. and $g^- \le f^-$ a.e.. By Theorem 15.3.7 (ii),

$$\left\{ \begin{array}{l} \mu(f^+) \le \mu(g^+) \\ \mu(g^-) \le \mu(f^-) \end{array} \right. \quad \Rightarrow \quad \mu(f^+) + \mu(g^-) \le \mu(g^+) + \mu(f^-) \quad \Rightarrow \quad \mu(f) \le \mu(g) \tag{15.3.39}$$

by definition of integral. Thus, we have $f = g$ a.e. implies $\mu(f) = \mu(g)$.

(iii) If $f = 0$ a.e., then $f^\pm = 0$ a.e., so $\mu(f^\pm) = 0$ and thus $\mu(f) = 0$.

(iv) Finally, by (i), $|\mu(f)| = |\mu(f^+) - \mu(f^-)| \le |\mu\,(f^+)| + |\mu\,(f^-)| = \mu(f^+ + f^-) = \mu(|f|)$.

□

15.3.2 Integrals and limits

In the monotone convergence theorem, the hypothesis that the given sequence of functions is non-decreasing is essential. In this section we obtain some results on the integrals of limits of functions without such a hypothesis.

Lemma 15.3.11 (Fatou's Lemma)**.** Let $(f_n : E \to [0, \infty], n \in \mathbb{N})$ be a sequence of non-negative measurable functions. Then

$$\mu\left(\liminf_n f_n\right) \le \liminf_n \mu(f_n). \tag{15.3.40}$$

(Inverse Fatou's Lemma). Additionally, if there exists a non-negative integrable function g (measurable and $\mu(g) < \infty$) such that $f_n \le g$ for all n, then

$$\mu\left(\limsup_n f_n\right) \ge \limsup_n \mu(f_n). \tag{15.3.41}$$

Proof. For $k \ge n$, we have

$$\underbrace{\inf_{m\ge n} f_m \le f_k \quad \Rightarrow \quad \mu\left(\inf_{m\ge n} f_m\right) \le \mu(f_k)}_{\text{by Theorem 15.3.7 (ii) since } f_n \text{ and } \inf f_n \text{ are non-negative measurable}} \qquad \Rightarrow \quad \mu\left(\inf_{m\ge n} f_m\right) \le \inf_{k\ge n} \mu(f_k). \tag{15.3.42}$$

Then we have

$$\mu\left(\inf_{m\ge n} f_m\right) \le \inf_{k\ge n} \mu(f_k) \le \sup_n \inf_{k\ge n} \mu(f_k) = \liminf_n \mu(f_n). \tag{15.3.43}$$

But, as $n \to \infty$,

$$\inf_{m \geq n} f_m \uparrow \sup_n \left(\inf_{m \geq n} f_m \right) = \liminf f_n \quad \Rightarrow \quad \mu \left(\inf_{m \geq n} f_m \right) \uparrow \mu(\liminf f_n) \tag{15.3.44}$$

by monotone convergence theorem. Thus, $\mu(\liminf f_n) \leq \liminf \mu(f_n)$.

For the second inequality, clearly we see that f_n and $\limsup f_n$ are integrable and apply Fatou's lemma to the sequence $g - f_n$,

$$\begin{aligned}
\mu\left(\liminf(g - f_n)\right) &\leq \liminf \mu\left(g - f_n\right) \\
\mu\left(g - \limsup f_n\right) &\leq \liminf \mu(g) - \mu(f_n) \qquad \text{(by Theorem 15.3.10 (i))} \\
\mu\left(g\right) - \mu\left(\limsup f_n\right) &\leq \mu(g) - \limsup \mu(f_n) \qquad \text{(by Theorem 15.3.10 (i))} \\
\limsup \mu(f_n) &\leq \mu(\limsup f_n). \qquad \text{(as } \mu(g) < \infty\text{)}
\end{aligned}$$

□

Theorem 15.3.12 (dominated convergence theorem)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. Let f be a measurable function and let $(f_n : n \in \mathbb{N})$ be a sequence of such functions. Suppose that $f_n(x) \to f(x)$ a.e.. and that $|f_n| \leq g$ a.e. for all n, for some integrable function g. Then f_n and f are integrable, for all n and $\mu(f_n) \to \mu(f)$.

Proof. Clearly, f_n is integrable. The limit f is measurable and $|f| \leq g$ a.e.,

$$\underbrace{|f| \leq g \text{ a.e.} \quad \Rightarrow \quad \mu(|f|) \leq \mu(g)}_{\text{by Theorem 15.3.7 (ii)}} \underbrace{\leq \quad \infty}_{g \text{ is integrable}} \quad \Rightarrow \quad f \text{ is integrable.} \tag{15.3.45}$$

We have $0 \leq g \pm f_n \to g \pm f$ a.e. so certainly $\liminf(g \pm f_n) = g \pm f$ a.e.. By Theorem 15.3.10 (i), (ii) and Fatou's Lemma,

$$\begin{aligned}
\mu(g) + \mu(f) &= \mu(\liminf(g + f_n)) \leq \liminf \mu(g + f_n) = \mu(g) + \liminf \mu(f_n), \\
\mu(g) - \mu(f) &= \mu(\liminf(g - f_n)) \leq \liminf \mu(g - f_n) = \mu(g) - \limsup \mu(f_n).
\end{aligned}$$

Since $\mu(g) < \infty$, we can deduce that

$$\mu(f) \leq \liminf \mu(f_n) \leq \limsup \mu(f_n) \leq \mu(f). \tag{15.3.46}$$

This proves that $\mu(f_n) \to \mu(f)$ as $n \to \infty$ (from Definition 3.5.2 (iii)). □

Remark. (i) The convergence of the sequence and domination by g is relaxed to hold only μ-almost everywhere provided the measure space $(E, \mathcal{E}, \mu)$ is complete or f is chosen as a measurable function which agrees with the μ-almost everywhere existing pointwise limit. Sometimes it is called merely in measure (Chung [5]). (These precautions are necessary, because otherwise there might exist a non-measurable subset of a μ-null set $N \in \mathcal{E}$, hence f might not be measurable.)

(ii) Actually, dominated convergence theorem also implies that $X_n \to X$ in $\mathcal{L}^1(E, \mathcal{E}, \mu)$ by Lemma 15.3.18.

(iii) The condition that there is a dominating integrable function g can be relaxed to uniform integrability of the sequence $\{f_n\}$, see Vitali convergence theorem (Theorem 15.4.25).

Example 15.3.13.

$$\text{(i)} \int_0^\infty \sin(e^x)/(1 + nx^2)dx \to 0 \quad \text{as} \quad n \to \infty, \qquad \text{(ii)} \int_0^1 (n \cos x)/(1 + n^2 x^{\frac{3}{2}})dx \to 0 \quad \text{as} \quad n \to \infty. \tag{15.3.47}$$

Solution (i) Let $f_n(x) = \sin(e^x)/(1 + nx^2) \to 0$ and $g(x) = 1/(1 + x^2)$. It is easy to check that g is measurable and integrable and $|f_n| \leq g$. Applying dominated convergence theorem (Theorem 15.3.12), we have

$$\int_0^\infty \sin(e^x)/(1 + nx^2)dx \to \int_0^\infty 0 \; dx = 0 \quad \text{as } n \to \infty. \tag{15.3.48}$$

(ii) *Approach 1.* Let $f_n(x) = (n\cos x)/(1+n^2x^{\frac{3}{2}}) \to 0$ and $g(x) = x^{-3/4}$. It is easy to check that g is measurable and integrable on $(0,1]$ and

$$|f_n| \le \frac{n}{1+n^2x^{\frac{3}{2}}} = \frac{1}{\frac{1}{n}+nx^{\frac{3}{2}}} \le \frac{1}{2\sqrt{\frac{1}{n}\ nx^{\frac{3}{2}}}} = \frac{1}{2}x^{-\frac{3}{4}} \le g. \tag{15.3.49}$$

Applying dominated convergence theorem (Theorem 15.3.12), we have

$$\int_0^1 (n\cos x)/(1+n^2x^{\frac{3}{2}})dx \to 0 \text{ as } n\to\infty. \tag{15.3.50}$$

Approach 2. Clearly the integral is at most

$$\int_0^1 \frac{n}{1+n^2x^{\frac{3}{2}}}dx$$

Now we can substitute $x \mapsto y/n$ to get

$$\int_0^n \frac{1}{1+n^{\frac{1}{2}}y^{\frac{3}{2}}}dy \le \int_0^1 \frac{1}{1+(yn^{\frac{1}{4}})^2}dy + \int_1^n \frac{1}{1+\sqrt{n}y}dy \le \frac{\tan^{-1}(1)}{n^{\frac{1}{4}}} + \frac{\log(n)}{\sqrt{n}} \to 0. \tag{15.3.51}$$

Note that in Theorem 15.3.10 (iii) we lose the reverse implication. The following result is sometimes useful:

Proposition 15.3.14. Let $\mathcal{A}$ be a π-system containing E and generating $\mathcal{E}$. Then, for any integrable function f,

$$\mu(f\mathbb{1}_A) = 0 \quad \text{for all } A\in\mathcal{A} \ \Rightarrow\ f = 0 \text{ a.e..} \tag{15.3.52}$$

Proof. Consider $\mathcal{D} = \{A\in\mathcal{E} : \mu(f\mathbb{1}_A) = 0\}$. Obviously, $\mathcal{A}\subseteq\mathcal{D}$ and $\mathcal{D}\subseteq\mathcal{E}$. Now we want to prove that $\mathcal{D} = \mathcal{E}$. It suffices to show that $\mathcal{E}\subseteq\mathcal{D}$ and $\mathcal{D}$ is d-system (then $\mathcal{D}$ is a σ-algebra by Dynkin's Lemma (Lemma 15.1.3)).

(i) We know that $\mathcal{A}$ contains E, thus $E\in\mathcal{D}$.

(ii) $\forall A, B\in\mathcal{D}$ with $A\subseteq B$, we have $\mu(f\mathbb{1}_A) = 0,\ \mu(f\mathbb{1}_B) = 0$

$$\underbrace{\mu\left(f\mathbb{1}_{\{B\backslash A\}}\right) = \mu(f\mathbb{1}_B) - \mu\left(f\mathbb{1}_{\{A\cap B\}}\right)}_{f \text{ is integrable}} = \mu(f\mathbb{1}_B) - \mu\left(f\mathbb{1}_A\right) = 0 \ \Rightarrow\ B\backslash A\in\mathcal{D}. \tag{15.3.53}$$

(iii) For increasing sequence $A_n\in\mathcal{D}$ with $A_n\subseteq A_{n+1}$, we have $\mu(f\mathbb{1}_{A_n}) = 0$. Also we have

$$f\mathbb{1}_{A_n} \to f\mathbb{1}_{\left\{\bigcup_n A_n\right\}} \tag{15.3.54}$$

Since f is integrable function, we have that $f_n = f\mathbb{1}_{A_n}$ is bounded by f, ($|f\mathbb{1}_{A_n}| \le |f|$). Then apply dominated convergence theorem (Theorem 15.3.12), we have

$$\mu\left(f\mathbb{1}_{A_n}\right) \to \mu\left(f\mathbb{1}_{\left\{\bigcup_n A_n\right\}}\right) \ \Rightarrow\ \mu\left(f\mathbb{1}_{\left\{\bigcup_n A_n\right\}}\right) = 0 \ \Rightarrow\ \bigcup_n A_n\in\mathcal{D}. \tag{15.3.55}$$

Then we can say that $\mathcal{D} = \mathcal{E}$ and for all $A\in\mathcal{E}$, we have $\mu(f\mathbb{1}_A) = 0$. Thus,

$$\mu(f^+) = \mu\left(f\mathbb{1}_{\{f>0\}}\right) = 0 \ \Rightarrow\ f^+ = 0 \text{ a.e..} \qquad \text{(Theorem 15.3.7 (iii))} \tag{15.3.56}$$

Similarly, we have $f^- = 0$ a.e. and

$$\begin{aligned}\mu(\{f\neq 0\}) &= \mu(\{f>0\} \text{ or } \{f<0\}) = \mu(\{f>0\}) + \mu(\{f<0\}) \\ &= \mu\left(\{f^+\neq 0\}\right) + \mu\left(\{f^-\neq 0\}\right) = 0+0=0 \quad\Rightarrow\quad f = 0 \text{ a.e..}\end{aligned}$$

□

Corollary 15.3.15 (bounded convergence theorem)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. Let f be a measurable function and let $(f_n : n \in \mathbb{N})$ be a sequence of such functions. Suppose that $f_n(x) \to f(x)$ a.e.. and that $|f_n| \leq M$ a.e. for all n, for a constant M. Then for all n and $\mu(f_n) \to \mu(f)$.

Proof. Let $g = M$ (since the constant M is integrable) and apply dominated convergence theorem (Theorem 15.3.12) □

Remark. If we release the condition to $f_n(x) \to f(x)$ in measure with additional condition that μ is finite, we can have another version of Bounded Convergence Theorem (Durrett [8]).

Theorem 15.3.16 (bounded convergence theorem)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space with $\mu(E) < \infty$. Let f be a measurable function and let $(f_n : n \in \mathbb{N})$ be a sequence of such functions. Suppose $f_n \to f$ in measure and $|f_n| \leq M$ for all n, for some constant $M < \infty$. Then $\mu(|f_n - f|) \to 0$, which implies that $\mu(f_n) \to \mu(f)$.

Proof. Let $\mu(E) = C$. By Theorem 15.2.14 (ii), f is the almost everywhere limit of a subsequence, so

$$|f| = |f_{n_k} - f_{n_k} + f| \leq |f_{n_k} - f| + |f_{n_k}| \leq |f_{n_k} - f| + M \to M \text{ a.e.} \quad \Rightarrow \quad f \text{ is integrable.} \tag{15.3.57}$$

For $\varepsilon > 0$, there exists N such that $n \geq N$ implies (by definition of convergence in measure (Definition 15.2.6))

$$\mu(\{|f_n - f| > \varepsilon/(2C)\}) \leq \varepsilon/(4M). \tag{15.3.58}$$

Then $\mu(|f_n - f|) = \mu\left(|f_n - f| \mathbb{1}_{\{|f_n - f| > \varepsilon/(2C)\}}\right) + \mu\left(|f_n - f| \mathbb{1}_{\{|f_n - f| \leq \varepsilon/(2C)\}}\right) \leq 2M(\varepsilon/4M) + \varepsilon/2 = \varepsilon$ implies that

$$\mu(|f_n - f|) \to 0. \tag{15.3.59}$$

Also, by Theorem 15.3.10 (i), (iv), $|\mu(f_n) - \mu(f)| = |\mu(f_n - f)| \leq \mu(|f_n - f|) \to 0 \Rightarrow \mu(f_n) \to \mu(f)$. □

Theorem 15.3.17. Let $(f_n : n \in \mathbb{N})$ be a sequence of integrable functions and suppose that $f_n \to f$ a.e. for some integrable function f. Show that, if $\mu(|f_n|) \to \mu(|f|)$, then $\mu(|f_n - f|) \to 0$.

Proof. We have $\liminf_{n\to\infty} |f_n| = |f|$ a.e., and $\liminf_{n\to\infty} |f_n - f| = 0$ a.e., so by Theorem 15.3.7,

$$\mu(\liminf_{n\to\infty} |f_n|) = \mu(|f|) \quad \text{and} \quad \mu(\liminf_{n\to\infty} |f_n - f|) = 0.$$

Thus, by Fatou's lemma (Lemma 15.3.11) (as $|f| + |f_n| - |f_n - f| \geq 0$) and the fact that $\mu(|f_n|) \to \mu(|f|)$, we have that

$$\begin{aligned}
\mu(\liminf_{n\to\infty}(|f| + |f_n| - |f_n - f|)) &\leq \liminf_{n\to\infty} \mu(|f| + |f_n| - |f_n - f|) \\
\mu\left(\liminf_{n\to\infty} |f|\right) + \mu\left(\liminf_{n\to\infty} |f_n|\right) - \mu\left(\liminf_{n\to\infty} |f_n - f|\right) &\leq \liminf_{n\to\infty} \mu(|f|) + \liminf_{n\to\infty} \mu(|f_n|) - \limsup_{n\to\infty} \mu(|f_n - f|) \\
2\mu(|f|) &\leq 2\mu(|f|) - \limsup_{n\to\infty} \mu(|f_n - f|) \\
\limsup_{n\to\infty} \mu(|f_n - f|) &\leq 0.
\end{aligned}$$

But of course, $0 \leq \liminf_{n\to\infty} \mu(|f_n - f|) \leq \limsup_{n\to\infty} \mu(|f_n - f|)$, whence $\mu(|f_n - f|) \to 0$. □

The above theorems give us Scheffé's Lemma. A different proof is given in Williams [16].P_{55}.

Lemma 15.3.18 (Scheffé's Lemma)**.** let $(f_n : n \in \mathbb{N})$ and f be a sequence of integrable functions. Suppose that $f_n(x) \to f(x)$ a.e..

(i) If f_n and f are non-negative, then $\mu(|f_n - f|) \to 0$ if and only if $\mu(f_n) \to \mu(f)$.

(ii) $\mu(|f_n - f|) \to 0$ if and only if $\mu(|f_n|) \to \mu(|f|)$.

Proof. The 'only if' part of (i) and (ii) is in Theorem 15.3.16.

($\Leftarrow$) (i) Now suppose $\mu(f_n) \to \mu(f)$. Since $(f - f_n)^+ = (f_n - f)^- \leq f$, by dominated convergence theorem (Theorem 15.3.12), $\mu((f_n - f)^-) \to 0$. By Theorem 15.3.10,

$$|\mu((f_n - f)\mathbb{1}_{f_n < f})| = \left|\mu\left((f_n - f)^-\right)\right| \leq \mu\left(\left|(f_n - f)^-\right|\right) \to 0 \tag{15.3.60}$$

Thus,

$$\left|\mu((f_n-f)^+)\right| = \left|\mu\left((f_n-f)\mathbb{1}_{f_n\geq f}\right)\right| = \left|\mu(f_n)-\mu(f)-\mu\left((f_n-f)\mathbb{1}_{f_n<f}\right)\right| \leq |\mu(f_n)-\mu(f)| + \left|\mu\left((f_n-f)\mathbb{1}_{f_n<f}\right)\right| \to 0. \tag{15.3.61}$$

$$\Rightarrow \qquad \mu\left(f_n-f\right) = \mu((f_n-f)^+) - \mu((f_n-f)^-) \to 0 \quad \Rightarrow \quad \mu(f_n)\to\mu(f). \tag{15.3.62}$$

(ii) Since $f_n \to f$ a.e., $f_n^+ \to f^+$ a.e. and $f_n^- \to f^-$ a.e.. Then apply (i) to get the required result. □

15.3.3 Transformations of integrals

Proposition 15.3.19. Let $(E,\mathcal{E},\mu)$ be a measure space and let $A\in\mathcal{E}$. Then the set $\mathcal{E}_A$ of measurable subsets of A is a σ-algebra and the restriction μ_A of μ to $\mathcal{E}_A$ is a measure. Moreover, for any non-negative measurable function f on E, we have

$$\mu(f\mathbb{1}_A) = \mu_A(f|_{\{x\in A\}}). \tag{15.3.63}$$

Proof. For any measurable set $A\in\mathcal{E}$, we define $\mathcal{E} = \{B\in\mathcal{E} : B\subseteq A\}$ and we prove that $\mathcal{E}_A$ is a σ-algebra.

(i) We have $\emptyset\in\mathcal{E}$ and $\emptyset\subseteq A$ imply $\emptyset\in\mathcal{E}_A$. Also, $A\in\mathcal{E}$ and $\emptyset\subseteq A$ imply $A\in\mathcal{E}_A$.

(ii) If $B\in\mathcal{E}_A$, then $B\in\mathcal{E}$ and $B\subseteq A$. So $B_A^c = A\backslash B\subseteq A$ and $B_A^c = A\backslash B\in\mathcal{E}$ as $A\in\mathcal{E},\ B\in\mathcal{E}\ \Rightarrow\ B_A^c\in\mathcal{E}_A$.

(iii) For $A_n\in\mathcal{E}_A$, $n\in\mathbb{N}$, $A_n\subseteq A$ and $A_n\in\mathcal{E}$. Then

$$\begin{cases} A_n\in\mathcal{E}\ \Rightarrow\ \bigcup_n A_n\in\mathcal{E} \\ A_n\subseteq A,\ n\in\mathbb{N}\ \Rightarrow\ \bigcup_n A_n\subseteq A \end{cases} \quad\Rightarrow\quad \bigcup_n A_n\in\mathcal{E}_A. \tag{15.3.64}$$

Second, we prove μ_A, the measure μ to $\mathcal{E}_A$ is a measure on $(A,\mathcal{E}_A)$. Then $\mu_A(\underbrace{\emptyset}_{\in\mathcal{E}_A}) = \mu(\emptyset) = 0$ as μ is a measure.

For disjoint sets $B_n\in\mathcal{E}_A$, $n\in\mathbb{N}$,

$$\mu_A\underbrace{\left(\bigcup_n B_n\right)}_{\in\mathcal{E}_A} = \mu\left(\bigcup_n B_n\right) = \sum_n \mu\left(B_n\right) = \sum_n \mu_A\left(B_n\right) \quad\Rightarrow\quad \mu_A \text{ is a measure.} \tag{15.3.65}$$

Now if f is indicator function $\mathbb{1}_B$, $B\in\mathcal{E}$, we have

$$\mu\left(f\mathbb{1}_A\right) = \mu\left(\mathbb{1}_B\mathbb{1}_A\right) = \mu\underbrace{\left(\mathbb{1}_{B\cap A}\right)}_{\in\mathcal{E}_A} = \mu_A\left(\mathbb{1}_{B\cap A}\right) = \mu_A\left(\mathbb{1}_B|_{\{x\in A\}}\right) = \mu_A\left(f|_{\{x\in A\}}\right). \tag{15.3.66}$$

By linearity, the result also hold for simple function. For non-negative measurable function f, set $f_n = 2^{-n}\lfloor 2^n f\rfloor \wedge n$ and f_n are simple. Then $f_n\mathbb{1}_A\uparrow f\mathbb{1}_A$ and $f_n|_{\{x\in A\}}\uparrow f|_{\{x\in A\}}$. By monotone convergence (Theorem 15.3.5),

$$\mu(f_n\mathbb{1}_A)\uparrow\mu(f\mathbb{1}_A) \quad \text{and} \quad \mu_A(f_n|_{\{x\in A\}})\uparrow\mu_A(f|_{\{x\in A\}}). \tag{15.3.67}$$

Since $\mu(f_n\mathbb{1}_A) = \mu_A(f_n|_{\{x\in A\}})$, the result follows. □

Example 15.3.20. In the case of Lebesgue measure on $\mathbb{R}$, we write, for any interval I with $\inf I = a$ and $\sup I = b$,

$$\underbrace{\int_{\mathbb{R}} f(x)\mathbb{1}_I(x)\mu(dx) = \int_I f(x)\mu(dx)}_{\text{Proposition 15.3.19}} = \underbrace{\int_I f(x)dx}_{\text{Lebesgue measure}} = \int_a^b f(x)dx. \tag{15.3.68}$$

Note that the sets $\{a\}$ and $\{b\}$ have measure zero (by Proposition 15.1.20), so we do not need to specify whether they are included in I or not.

Proposition 15.3.21. Let $(E,\mathcal{E})$ and $(G,\mathcal{G})$ be measurable spaces and let $f: E\to G$ be a measurable function. Given a measure μ on $(E,\mathcal{E})$, define $\nu = \mu\circ f^{-1}$, the image measure on $(G,\mathcal{G})$. Then, for all non-negative measurable functions $g: G\to[0,\infty]$,

$$\nu(g) = \mu(g\circ f). \tag{15.3.69}$$

Proof. If $g = \mathbb{1}_A$, $A \in \mathcal{G}$, $\nu(g) = \nu(\mathbb{1}_A) = \nu(A) = \mu\left(f^{-1}(A)\right) = \mu\left(\mathbb{1}_{\{x:f(x)\in A\}}\right) = \mu(\mathbb{1}_A \circ f) = \mu(g \circ f)$.

By linearity, the result also hold for simple function, $g = \sum_{k=1}^n a_k \mathbb{1}_{A_k}$, $a_k \in [0,\infty]$, with A_k disjoint,

$$\nu\left(\sum_{k=1}^n a_k \mathbb{1}_{A_k}\right) = a_k \sum_{k=1}^n \nu(\mathbb{1}_{A_k}) = a_k \sum_{k=1}^n \mu(\mathbb{1}_{A_k} \circ f) = \mu\left(\sum_{k=1}^n (a_k \mathbb{1}_{A_k} \circ f)\right) = \underbrace{\mu\left(\left(\sum_{k=1}^n a_k \mathbb{1}_{A_k}\right) \circ f\right)}_{A_k \text{ is disjoint}} = \mu(g \circ f) \tag{15.3.70}$$

by Theorem 15.3.7 as $\{f(x) : x \in E\}$ is measurable and hence $\mathbb{1}_{A_k} \circ f = \mathbb{1}_{A_k \cap \{f(x):x\in E\}} = \mathbb{1}_{\{x:f(x)\in A\}}$ is non-negative measurable function. For non-negative measurable function g, set

$$g_n = 2^{-n} \lfloor 2^n g \rfloor \wedge n \tag{15.3.71}$$

and thus g_n are simple. Then $g_n \uparrow g$ and $g_n \circ f \uparrow g \circ f$. By monotone convergence theorem (Theorem 15.3.5),

$$\nu(g_n) \uparrow \nu(g), \qquad \mu(g_n \circ f) \uparrow \mu(g \circ f). \tag{15.3.72}$$

Since $\nu(g_n) = \mu(g_n \circ f)$, $\nu(g) = \mu(g \circ f)$. □

Proposition 15.3.22. Let $(E, \mathcal{E}, \mu)$ be a measure space and let $f : E \to [0,\infty]$ be a non-negative measurable function on E. Define $\nu(A) = \mu(f\mathbb{1}_A)$, $A \in \mathcal{E}$. Then ν is a measure on E and, for all non-negative measurable functions $g : E \to [0,\infty]$,

$$\nu(g) = \mu(fg). \tag{15.3.73}$$

We say that ν has density f (with respect to Lebesgue measure). f is called the density function of ν with respect to μ.

Proof. If $g = \mathbb{1}_A$, $A \in \mathcal{E}$, $\nu(g) = \nu(\mathbb{1}_A) = \nu(A) = \mu(f\mathbb{1}_A) = \mu(fg)$.

By linearity, the result also hold for simple function, $g = \sum_{k=1}^n a_k \mathbb{1}_{A_k}$, $a_k \in [0,\infty]$, with A_k disjoint,

$$\nu\left(\sum_{k=1}^n a_k \mathbb{1}_{A_k}\right) = a_k \sum_{k=1}^n \nu(\mathbb{1}_{A_k}) = a_k \sum_{k=1}^n \mu(f\mathbb{1}_{A_k}) = \mu\left(f \sum_{k=1}^n a_k \mathbb{1}_{A_k}\right) = \mu(fg) \tag{15.3.74}$$

by Theorem 15.3.7. For non-negative measurable function g, set $g_n = 2^{-n} \lfloor 2^n g \rfloor \wedge n$ and thus g_n are simple. Then $g_n \uparrow g$ and $fg_n \uparrow fg$. By monotone convergence theorem (Theorem 15.3.5),

$$\nu(g_n) \uparrow \nu(g), \qquad \mu(fg_n) \uparrow \mu(fg). \tag{15.3.75}$$

Since $\nu(g_n) = \mu(fg_n)$, $\nu(g) = \mu(fg)$. □

Remark. μ and ν are measures on $(E, \mathcal{E})$.

In particular, to each non-negative Borel function f on $\mathbb{R}$, there corresponds a Borel measure ν on $\mathbb{R}$ given by

$$\nu(A) = \int_A f(x)\mu(dx). \tag{15.3.76}$$

Then, for all non-negative Borel functions g,

$$\nu(g) = \int_{\mathbb{R}} g(x)f(x)\mu(dx) = \int_{\mathbb{R}} g(x)f(x)dx. \tag{15.3.77}$$

Theorem 15.3.23 (uniqueness of the density function)**.** Let μ and ν be two measures on $(E, \mathcal{E})$. If f, g are two density functions of ν with respect to μ and ν is σ-finite, then $f = g$, μ-a.e., ν-a.e. as well.

Proof. Assume f, g are two densities of ν with respect to μ. Let $A_n \uparrow E$ with $A_n \in \mathcal{E}$ and

$$B_n = A_n \cap \{f > g\} \in \mathcal{E} \quad \text{as } f, g \text{ is measurable.} \tag{15.3.78}$$

Then $(f-g)\mathbb{1}_{B_n}$ is non-negative measurable, by Theorem 15.3.7 (i),

$$\begin{aligned}\mu\left((f-g)\mathbb{1}_{B_n}\right)+\mu\left(g\mathbb{1}_{B_n}\right) &= \mu\left(f\mathbb{1}_{B_n}\right)\\ \mu\left((f-g)\mathbb{1}_{B_n}\right)+\nu\left(B_n\right) &= \nu\left(B_n\right)\\ \mu\left((f-g)\mathbb{1}_{B_n}\right) &= 0. \qquad (\text{as } \nu(B_n)<\infty)\end{aligned}$$

By Theorem 15.3.7 (iii), $(f-g)\mathbb{1}_{B_n}=0$ μ-a.e., thus,

$$0=\mu\left(\{f\neq g\}\cap B_n\right)=\mu\left(B_n\right) \;\Rightarrow\; \mathbb{1}_{B_n}=0 \text{ } \mu\text{-a.e.} \;\Rightarrow\; \mu\left(B_n\right)=0. \tag{15.3.79}$$

As $\mathbb{1}_{B_n}\uparrow\{f>g\}$, by monotone convergence theorem (Theorem 15.3.8),

$$\mu\left(B_n\right)\uparrow\mu\left(\{f>g\}\right) \quad\Rightarrow\quad 0=\mu\left(\{f>g\}\right). \tag{15.3.80}$$

Similarly, for the case $f<g$, we have $\mu\left(\{f<g\}\right)=0$, and hence

$$\mu\left(\{f\neq g\}\right)=\mu\left(\{f>g\}\right)+\mu\left(\{f<g\}\right)=0+0=0 \quad\Rightarrow\quad f=g \;\; \mu\text{-a.e.} \tag{15.3.81}$$

With the same setting,

$$\begin{aligned}\nu\left((f-g)\mathbb{1}_{B_n}\right)+\nu\left(g\mathbb{1}_{B_n}\right) &= \nu\left(f\mathbb{1}_{B_n}\right)\\ \nu\left((f-g)\mathbb{1}_{B_n}\right)+\mu\left(fg\mathbb{1}_{B_n}\right) &= \mu\left(fg\mathbb{1}_{B_n}\right)\\ \nu\left((f-g)\mathbb{1}_{B_n}\right) &= 0. \qquad (\text{as } fg\mathbb{1}_{B_n}=0 \text{ } \mu\text{-a.e.})\end{aligned}$$

Then we have $f=g$ ν-a.e., with the same argument for μ. □

15.3.4 Relation to Riemann integral

Theorem 15.3.24 (Riemann-Lebesgue Integral)**.** Let $I=[a,b]$ and $f:I\to\mathbb{R}$. Let μ denote the Lebesgue measure. Then f is Lebesgue-integrable on I with integral

$$\int_I f d\mu=\int_a^b f(x)dx. \tag{15.3.82}$$

Proof. Recall that f is said Riemann-integrable with integral R if for all $\varepsilon>0$, there exists $\delta>0$ such that for all finite partitions of I into subintervals $I_1=(a_1,b_1],\ \ldots,\ I_k=(a_k,b_k]$ of mesh $\max_{1\le j\le k}\mu(I_j)=\max_{1\le j\le k}(b_j-a_j)\le\delta$,

$$\left|R-\sum_{j=1}^{k}f(x_j)\mu(I_j)\right|<\varepsilon, \qquad R=\int_a^b f(x)dx \qquad \text{whenever } x_j\in I_j,\ 1\le j\le k. \tag{15.3.83}$$

We may assume without loss of generality that $I=[0,1]$. Consider the dyadic subdivision of I, that is, for $n\ge 1$ and $0\le k\le 2^n-1$, let $I_{k,n}=[k2^{-n},(k+1)2^{-n}]$. Consider the function

$$F^+=\lim_{n\to\infty}\sum_{k=0}^{2^n-1}2^{-n}\sup_{I_{k,n}}f, \qquad F^-=\lim_{n\to\infty}\sum_{k=0}^{2^n-1}2^{-n}\inf_{I_{k,n}}f, \tag{15.3.84}$$

$$\overline{f}_n(x)=\sum_{k=0}^{2^n-1}\sup_{I_{k,n}}f\mathbb{1}_{I_{k,n}}(x), \qquad \underline{f}_n(x)=\sum_{k=0}^{2^n-1}\inf_{I_{k,n}}f\mathbb{1}_{I_{k,n}}(x) \tag{15.3.85}$$

Then note that

$$\overline{f}_n=\sum_{k=0}^{2^n-1}\sup_{I_{k,n}}(f^+-f^-)\mathbb{1}_{I_{k,n}}(x)=\sum_{k=0}^{2^n-1}\left(\sup_{I_{k,n}}f^+-\inf_{I_{k,n}}f^-\right)\mathbb{1}_{I_{k,n}}(x) \tag{15.3.86}$$

is a linear combination of simple functions and is a decreasing sequence of functions, while $\underline{f}_n$ is non-decreasing. Moreover

$$\underline{f}_n\le f\le\overline{f}_n. \tag{15.3.87}$$

Since f is Riemann integrable, we know that $F^+ = F^-$ and therefore f is bounded (i.e. $|f| < M$ for some M, from Definition 10.6.3). Thus

$$\mu\left(\left(\sup_{I_{k,n}} f^+ - \inf_{I_{k,n}} f^-\right)\mathbb{1}_{I_{k,n}}(x)\right) = \mu\left(\sup_{I_{k,n}} f^+\mathbb{1}_{I_{k,n}}(x)\right) - \mu\left(\inf_{I_{k,n}} f^-\mathbb{1}_{I_{k,n}}(x)\right) \tag{15.3.88}$$

by boundedness. Then, we have

$$\begin{aligned} R &= \lim_{n\to\infty}\mu\left(\overline{f}_n\right) = \lim_{n\to\infty}\int_I \overline{f}_n d\mu = \lim_{n\to\infty}\sum_{k=0}^{2^n-1}\left(\sup_{I_{k,n}} f^+ - \inf_{I_{k,n}} f^-\right)2^{-n} = \lim_{n\to\infty}\sum_{k=0}^{2^n-1} 2^{-n}\sup_{I_{k,n}} f \\ &= \lim_{n\to\infty}\mu\left(\underline{f}_n\right) = \lim_{n\to\infty}\int_I \underline{f}_n d\mu = \lim_{n\to\infty}\sum_{k=0}^{2^n-1}\left(\inf_{I_{k,n}} f^+ - \sup_{I_{k,n}} f^-\right)2^{-n} = \lim_{n\to\infty}\sum_{k=0}^{2^n-1} 2^{-n}\inf_{I_{k,n}} f \end{aligned}$$

To see this, use (15.3.83) with x_k such that $f(x_k)$ is arbitrarily close to $\sup_{I_{k,n}} f$ and $\inf_{I_{k,n}} f$ respectively, $0 \le k \le 2^n - 1$ since f is bounded. Since $\overline{f}_n$ and $\underline{f}_n$ are monotone and bounded, by fundamental axiom of real numbers (Axiom 10.2.1), the limit of $\overline{f}_n$ and $\underline{f}_n$ exist, define

$$\overline{f}_n \downarrow \lim \overline{f}_n := \overline{f}, \qquad \underline{f}_n \uparrow \lim \underline{f}_n := \underline{f}. \tag{15.3.89}$$

Then $\overline{f}$ and $\underline{f}$ are measurable as pointwise limits of simple functions linear combination, and by the dominated convergence theorem (Theorem 15.3.12, actually bounded convergence theorem Theorem 15.3.15),

$$\int_I \overline{f} d\mu = \mu\left(\lim \overline{f}_n\right) = \lim_{n\to\infty}\mu\left(\overline{f}_n\right) = R = \lim_{n\to\infty}\mu\left(\underline{f}_n\right) = \mu\left(\lim \underline{f}_n\right) = \int_I \underline{f} d\mu. \tag{15.3.90}$$

Since $\underline{f}$ and $\overline{f}$ are measurable and bounded, they are Lebesgue-integrable. With the fact that $\underline{f} \le \overline{f}$, we have

$$\underbrace{\mu\left(\overline{f} - \underline{f}\right) + \mu\left(\underline{f}\right) = \mu\left(\overline{f}\right)}_{\text{Theorem 15.3.10}} \quad \Rightarrow \quad \mu\left(\overline{f} - \underline{f}\right) = 0 \quad \Leftrightarrow \quad \overline{f} = \underline{f} \text{ a.e..} \tag{15.3.91}$$

Thus, since $\underline{f} \le f \le \overline{f}$, we deduce that $f = \overline{f}$ a.e. and then $\overline{f}_n \to f$ a.e. ($\overline{f}$ is $\mathcal{B}(I)$-measurable and f is $\mathcal{B}(I)^\mu$-measurable, where $\mathcal{B}(I)^\mu$ is Lebesgue completion of $\mathcal{B}(I)$, from Proposition 15.1.9, see Klenke [10]). So by bounded convergence theorem Theorem 15.3.15, f is integrable.

$$\int_I f d\mu = \mu(f) = \lim_{n\to\infty}\mu\left(\overline{f}_n\right) = R, \tag{15.3.92}$$

which proves the result. □

Example 15.3.25. The function $\mathbb{1}_{\{\mathbb{Q}\cap[0,1]\}}$ is Lebesgue-integrable with integral 0 (since $\mu(\mathbb{Q}) = 0$) but is not Riemann-integrable.

15.3.5 Fundamental theorem of calculus

We show that integration with respect to Lebesgue measure on $\mathbb{R}$ acts as an inverse to differentiation. Since we restrict here to the integration of continuous functions, the proof is the same as for the Riemann integral.

Theorem 15.3.26 (fundamental theorem of calculus)**.**

(i) Let $f : [a, b] \to \mathbb{R}$ be a continuous function and set

$$F_a(t) = \int_a^t f(x)dx. \tag{15.3.93}$$

Then F_a is differentiable on (a, b), with $F_a' = f$.

(ii) Let $F : [a, b] \to \mathbb{R}$ be differentiable with continuous derivative f. Then

$$\int_a^b f(x)dx = F(b) - F(a). \tag{15.3.94}$$

Proof. (i) First, f is bounded (from Theorem 10.3.8) and measurable (from the definition), thus integrable. Fix $t \in [a,b)$. Given $\varepsilon > 0$, there exists $\delta > 0$ such that $|f(x) - f(t)| < \varepsilon$ whenever $|x - t| < \delta$ (definition of continuity). So, for $0 < h \le \delta$,

$$\begin{aligned}\left|\frac{F_a(t+h) - F_a(t)}{h} - f(t)\right| &= \frac{1}{h}\left|\int_t^{t+h}(f(x) - f(t))dx\right| = \frac{1}{h}\left|\int_I (f(x) - f(t))dx\right| = \frac{1}{h}\left|\int (f(x) - f(t))\mathbb{1}_I dx\right| \\ &\le \frac{1}{h}\int |(f(x) - f(t))\mathbb{1}_I|\, dx \qquad \text{(Theorem 15.3.10 (iv))} \\ &= \frac{1}{h}\int_t^{t+h} |f(x) - f(t)|dx < \frac{\varepsilon}{h}\int_t^{t+h} dx = \varepsilon.\end{aligned}$$

Hence F_a is differentiable on the right at t with derivative $f(t)$. Similarly, for all $t \in (a,b]$, F_a is differentiable on the left at t with derivative $f(t)$.

(ii) We know that F_a is continuous on $[a,b]$ (by Theorem 10.6.10) and differentiable on (a,b) (by (i)). Thus, $F - F_a$ is continuous on $[a,b]$ and differentiable on (a,b) (by Proposition 10.3.2 and Proposition 10.4.3). Then by the mean value theorem (Theorem 10.4.8), there exists $c \in (a,b)$ such that

$$(F - F_a)(b) - (F - F_a)(a) = (F - F_a)'(c)(b - a) = (f(c) - f(c))(b - a) = 0. \tag{15.3.95}$$

Also, $(F - F_a)'(t) = (f - f)(t) = 0$ for all $t \in (a,b)$ so $F - F_a$ is constant on (a,b) (thus on $[a,b]$ by continuity),

$$F(b) - F(a) = F_a(b) - F_a(a) = \int_a^b f(x)dx. \tag{15.3.96}$$

□

Proposition 15.3.27. Let $\phi : [a,b] \to \mathbb{R}$ be continuously differentiable and strictly increasing. Then, for all non-negative Borel functions g on $[\phi(a), \phi(b)]$,

$$\int_{\phi(a)}^{\phi(b)} g(y)dy = \int_a^b g(\phi(x))\phi'(x)dx. \qquad (*) \tag{15.3.97}$$

Proof. First, the case where g is the indicator function of an interval, $\mathbb{1}_{[\phi(\alpha),\phi(\beta)]}$

$$\begin{aligned}\int_a^b g(\phi(x))\phi'(x)dx &= \int_a^b \mathbb{1}_{\phi(x)\in[\phi(\alpha),\phi(\beta)]}\phi'(x)dx = \int_\alpha^\beta \phi'(x)dx \\ &= \phi(\beta) - \phi(\alpha) \qquad \text{(fundamental theorem of calculus (Theorem 15.3.26 (ii)))} \\ &= \int_{\phi(a)}^{\phi(b)} \mathbb{1}_{[\phi(\alpha),\phi(\beta)]}dy = \int_{\phi(a)}^{\phi(b)} g(y)dy.\end{aligned}$$

Let $(E, \mathcal{E})$ be a measurable space ($E = [a,b]$) and $\mathcal{A}$ be a set of all the intervals (thus π-system generating $\mathcal{E}$). Let $\mathcal{V}$ be a set of bounded, measurable (thus Lebesgue-integrable) function for which $(*)$ holds, then $\mathcal{V}$ is a vector space. We have check that for any interval $A \in \mathcal{A}$, $(*)$ holds for $\mathbb{1}_A$, thus, $\mathbb{1}_A \in \mathcal{V}$. Obviously, $\mathbb{1}_E \in \mathcal{V}$.

Furthermore, if $f_n \in \mathcal{V}$ for all n and f is bounded with $0 \le f_n \uparrow f$, then f is measurable (as f is the limit of f_n). Since ϕ and ϕ' are continuous, ϕ and ϕ' are measurable (by Proposition 15.2.3,).

Therefore functions f_n, f, $(f_n \circ \phi)\phi'$, $(f_n \circ \phi)\phi'$ are measurable as composition of measurable functions is also measurable (Proposition 15.2.6). Thus

$$f_n \uparrow f, \qquad (f_n \circ \phi)\phi' \uparrow (f \circ \phi)\phi' \qquad \text{as} \quad f_n, f \ge 0,\ \phi' > 0\ (\phi \text{ is strictly increasing}). \tag{15.3.98}$$

Thus, by monotone convergence theorem (Theorem 15.3.5)

$$\int_{\phi(a)}^{\phi(b)} f_n(y)dy = \int_a^b f_n(\phi(x))\phi'(x)dx \quad \Rightarrow \quad \int_{\phi(a)}^{\phi(b)} f(y)dy = \int_a^b f(\phi(x))\phi'(x)dx \quad \Rightarrow \quad f \in \mathcal{V}. \tag{15.3.99}$$

Then, by monotone class theorem (Theorem 15.2.9), $\mathcal{V}$ contains every bounded measurable function. Now consider any non-negative Borel function g (which is measurable). Thus $g_n = g \wedge n \in \mathcal{V}$ for all n as g_n is bounded. With $g_n \uparrow g$ and

$(g_n \circ \phi)\phi' \uparrow (g \circ \phi)\phi'$, we have

$$\int_{\phi(a)}^{\phi(b)} g_n(y)dy = \int_a^b g_n(\phi(x))\phi'(x)dx \quad \Rightarrow \quad \int_{\phi(a)}^{\phi(b)} g(y)dy = \int_a^b g(\phi(x))\phi'(x)dx. \tag{15.3.100}$$

□

Proposition 15.3.28. Let u and v be differentiable functions on $[a, b]$ with continuous derivatives u' and v'. Then

$$\int_a^b u(x)v'(x)dx = \{u(b)v(b) - u(a)v(a)\} - \int_a^b u'(x)v(x)dx. \tag{15.3.101}$$

Proof. We know that $(uv)' = uv' + u'v$ and $(uv)'$ is continuous. Thus, apply fundamental theorem of calculus (Theorem 15.3.26 (ii)),

$$\int_a^b (u(x)v(x))'dx = (u(x)v(x))|_a^b = u(b)v(b) - u(a)v(a). \tag{15.3.102}$$

Since $(uv)'$, uv' and $u'v$ are continuous and thus bounded on $[a, b]$, they are Lebesgue-integrable, thus we can apply Theorem 15.3.10 (i) to get the required result. □

15.3.6 Differentiation under integral sign

Integration in one variable and differentiation in another can be interchanged subject to some regularity conditions.

Theorem 15.3.29 (differentiation under integral sign)**.** Let $U \subseteq \mathbb{R}$ be open and $(E, \mathcal{E})$ be a measurable space. Suppose that $f : U \times E \to \mathbb{R}$ satisfies:

(i) $x \mapsto f(t, x)$ is integrable for all t,

(ii) $t \mapsto f(t, x)$ is differentiable for all x,

(iii) for some integrable function g, for all $x \in E$ and all $t \in U$, $\left|\frac{\partial f}{\partial t}(t, x)\right| \leq g(x)$.

Then the function $x \mapsto (\partial f/\partial t)(t, x)$ is integrable for all t. Moreover, the function $F : U \to \mathbb{R}$, defined by

$$F(t) = \int_E f(t, x)\mu(dx) \quad \text{is differentiable and} \quad \frac{d}{dt}F(t) = \int_E \frac{\partial f}{\partial t}(t, x)\mu(dx). \tag{15.3.103}$$

Proof. Take any sequence $h_n \to 0$ and set

$$g_n(x) = \frac{f(t + h_n, x) - f(t, x)}{h_n} - \frac{\partial f}{\partial t}(t, x). \tag{15.3.104}$$

Then $g_n(x) \to 0$ for all $x \in E$ (since t is differentiable) and, by the mean value theorem (Theorem 10.4.8), $\exists c \in (0, h_n)$,

$$\begin{aligned} |g_n| &= \left|\frac{f(t + h_n, x) - f(t, x)}{h_n} - \frac{\partial f}{\partial t}(t, x)\right| \leq \left|\frac{f(t + h_n, x) - f(t, x)}{h_n}\right| + \left|\frac{\partial f}{\partial t}(t, x)\right| \\ &\leq |f'(t + c, x)| + \left|\frac{\partial f}{\partial t}(t, x)\right| \leq g + g = 2g \end{aligned}$$

for all n. In particular, for all t, the limit of measurable functions $(f(t + h_n, x) - f(t, x))/h_n$, the function $x \mapsto (\partial f/\partial t)(t, x)$ is hence measurable, and hence integrable, by (iii).Then, by dominated convergence,

$$\frac{F(t + h_n) - F(t)}{h_n} - \int_E \frac{\partial f}{\partial t}(t, x)\mu(dx) = \int_E g_n(x)\mu(dx) \to 0. \tag{15.3.105}$$

□

15.3.7 Product measure and Fubini's theorem

Definition 15.3.8. Let $(E_1, \mathcal{E}_1, \mu_1)$ and $(E_2, \mathcal{E}_2, \mu_2)$ be finite measure spaces. The set

$$\mathcal{A} = \{A_1 \times A_2 : A_1 \in \mathcal{E}_1, A_2 \in \mathcal{E}_2\} \tag{15.3.106}$$

is a π-system of subsets of $E = E_1 \times E_2$. Define the product σ-algebra

$$\mathcal{E} := \mathcal{E}_1 \otimes \mathcal{E}_2 = \sigma(A). \tag{15.3.107}$$

Remark. To prove a function f is $\mathcal{E}$-measurable, we usually fix $x_2 \in E_2$, then we can see that the function $x_1 \mapsto f(x_1, x_2)$ is $\mathcal{E}_1$-measurable and thus $\mathcal{E}_1 \otimes \mathcal{E}_2$-measurable ($\mathcal{E}$-measurable). Then we can take a union of countable many sets with respect to different x_2 and conclude union is $\mathcal{E}$-measurable. This will imply that f is $\mathcal{E}$-measurable.

Lemma 15.3.30. Let $f : E \to \mathbb{R}$ be $\mathcal{E}$-measurable. Then, for all $x_1 \in E_1$, the function $x_2 \mapsto f(x_1, x_2) : E_2 \to \mathbb{R}$ is $\mathcal{E}_2$-measurable.

Proof. Denote by $\mathcal{V}$ the set of bounded functions f such that for all $x_1 \in E_1$, the function $x_2 \mapsto f(x_1, x_2) : E_2 \to \mathbb{R}$ is $\mathcal{E}_2$-measurable. Clearly, $\mathcal{V}$ is a vector space (Definition 8.1.1).

First, $\mathbb{1}_E = \mathbb{1}_{E_1}\mathbb{1}_{E_2} = 1$, which is bounded. Also, it is $\mathcal{E}_2$-measurable since it is a constant. For the indicator function $\mathbb{1}_A$ of any set $A \in \mathcal{A}$ where $\mathcal{A}$ is a π-system generating $\mathcal{E}$, thus $\mathbb{1}_A$ is bounded. Then $\mathbb{1}_A = \mathbb{1}_{A_1}\mathbb{1}_{A_2}$, where $\mathbb{1}_{A_1}$ can be considered as a constant with respect to $\mathcal{E}_2$. Thus, A_2 is $\mathcal{E}_2$-measurable and so is $\mathbb{1}_{A_2}$. So the $\mathbb{1}_A$ is product of $\mathbb{1}_{A_2}$ and constant, hence $\mathcal{E}_2$-measurable.

Moreover, if $f_n \in \mathcal{V}$ for all n and if f is bounded with $0 \le f_n \uparrow f$ for any $x_1 \in E_1, x_2 \in E_2$, we can fix x_1 and get that the limit f of $\mathcal{E}_2$-measurable functions f_n is also $\mathcal{E}_2$-measurable, thus $f \in \mathcal{V}$.

So, by the monotone class theorem (Theorem 15.2.9), $\mathcal{V}$ contains all bounded $\mathcal{E}$-measurable functions f. Now consider any $\mathcal{E}$-measurable function f, $f_n := (-n) \vee f \wedge n$ is bounded and $\mathcal{E}$-measurable, thus for all $x_1 \in E_1$, the function $x_2 \mapsto f_n(x_1, x_2) : E_2 \to \mathbb{R}$ is $\mathcal{E}_2$-measurable. For all $x_1 \in E_1$, $f_n(x_1, x_2) \uparrow f(x_1, x_2)$ or $f_n(x_1, x_2) \downarrow f(x_1, x_2)$, $f(x_1, x_2)$ is $\mathcal{E}_2$-measurable as a limit of $\mathcal{E}_2$-measurable sequence f_n. □

Lemma 15.3.31. For all bounded $\mathcal{E}$-measurable functions f, the function

$$x_1 \mapsto g(x_1) = \int_{E_2} f(x_1, x_2)\mu_2(dx_2) : E_1 \to \mathbb{R} \tag{15.3.108}$$

is bounded and $\mathcal{E}_1$-measurable.

Proof. From Lemma 15.3.30, we know that for any bounded $\mathcal{E}$-measurable f, $f(x_1, x_2)$ is $\mathcal{E}_2$-measurable for any $x_1 \in E_1$. Also, as f is bounded, $|f| \le M$ for some constant $M > 0$, we have for any $x_1 \in E_1$

$$\underbrace{\mu_2(|f|) \le \mu_2(M)}_{\text{Theorem 15.3.7}} \quad \Rightarrow \quad \mu_2(|f|) \le M\mu_2(E_2) < \infty. \qquad \text{(by finiteness of } \mu_2) \tag{15.3.109}$$

So the integral ($g(x_1)$) is well-defined and bounded, f is Lebesgue-integrable (with respect to μ_2).

If μ_2 is zero measure, the conclusion is obvious as $g(x_1) = 0$ for all $x_1 \in E_1$. The following proof is based on the fact that $\mu_2(E_2) > 0$. Now let $\mathcal{V}$ be the set of bounded measurable functions f such that for all $x_1 \in E_1$,

$$g(x_1) = \int_{E_2} f(x_1, x_2)\mu_2(dx_2) \tag{15.3.110}$$

which is bounded and $\mathcal{E}_1$-measurable. Since f is Lebesgue-integrable, $\mathcal{V}$ is a vector space (Theorem 15.3.10 and Definition 8.1.1).

Clearly, if $f(x_1, x_2) = \mathbb{1}_E$ is bounded and $\mathcal{E}$-measurable, so

$$g(x_1) = \int_{E_2} \mathbb{1}_E \mu_2(dx_2) = \int_{E_2} \mathbb{1}_{E_1 \times E_2}\mu_2(dx_2) = \int_{E_2} \mathbb{1}_{E_1}\mathbb{1}_{E_2}\mu_2(dx_2) = \mathbb{1}_{E_1}\int_{E_2} \mathbb{1}_{E_2}\mu_2(dx_2) = \mathbb{1}_{E_1}\mu_2(E_2) \tag{15.3.111}$$

where $\mathbb{1}_{E_1}\mu_2(E_2)$ is bounded and $\mathcal{E}_1$-measurable function (as $\mu_2(E_2)$ is a constant). So $\mathbb{1}_E \in \mathcal{V}$.

Let $\mathcal{A}$ be the π-system generating $\mathcal{E}$, for any $A \in \mathcal{A} \subseteq \mathcal{E}$, we have $\mathbb{1}_A$ is bounded and $\mathcal{E}$-measurable,

$$g(x_1) = \int_{E_2} \mathbb{1}_A \mu_2(dx_2) = \int_{E_2} \mathbb{1}_{A_1 \times A_2}\mu_2(dx_2) = \int_{E_2} \mathbb{1}_{A_1}\mathbb{1}_{A_2}\mu_2(dx_2) = \mathbb{1}_{A_1}\int_{E_2} \mathbb{1}_{A_2}\mu_2(dx_2) = \mathbb{1}_{A_1}\mu_2(A_2) \tag{15.3.112}$$

where $\mathbb{1}_{A_1}\mu_2(A_2)$ is bounded and $\mathcal{E}_1$-measurable function (as $\mu_2(A_2)$ is a constant). So $\mathbb{1}_A \in \mathcal{V}$.

Moreover, if $f_n \in \mathcal{V}$ for all n and if f is bounded with $0 \le f_n \uparrow f$ for any $x_1 \in E_1$, f_n is $\mathcal{E}$-measurable and thus f is $\mathcal{E}$-measurable. Then

$$g_n(x_1) = \int_{E_2} f_n(x_1, x_2)\mu_2(dx_2) \tag{15.3.113}$$

where g_n is bounded and $\mathcal{E}_1$-measurable for all n. By monotone convergence theorem (Theorem 15.3.5),

$$g_n(x_1) = \int_{E_2} f_n(x_1, x_2)\mu_2(dx_2) \uparrow \int_{E_2} f(x_1, x_2)\mu_2(dx_2) := g(x_1) \tag{15.3.114}$$

Since $g(x_1)$ is the limit of $\mathcal{E}_1$-measurable functions $g_n(x_1)$, it is bounded and $\mathcal{E}_1$-measurable. So $f \in \mathcal{V}$.

Applying the monotone class theorem (Theorem 15.2.9), we have $\mathcal{V}$ contains all bounded $\mathcal{E}$-measurable functions. □

Theorem 15.3.32 (Product Measure)**.** There exists a unique product measure $\mu = \mu_1 \otimes \mu_2$ on $\mathcal{E}$ such that

$$\mu(A_1 \times A_2) = \mu_1(A_1)\mu_2(A_2) \tag{15.3.115}$$

for all $A_1 \in \mathcal{E}_1$ and $A_2 \in \mathcal{E}_2$.

Proof. Uniqueness holds because $\mathcal{A}$ is a π-system generating $\mathcal{E}$ (by Theorem 15.1.18).

For existence, by Lemma 15.3.30 and 15.3.31, we can define for $A \in \mathcal{E}$,

$$\mu(A) = \int_{E_1} \left(\int_{E_2} \mathbb{1}_A(x_1, x_2)\mu_2(dx_2) \right) \mu_1(dx_1) \tag{15.3.116}$$

which is well-defined as $\int_{E_2} \mathbb{1}_A(x_1, x_2)\mu_2(dx_2)$ is $\mathcal{E}_1$-measurable.

Obviously, μ is a set function as $\mu(\emptyset) = 0$. To check the countable additivity, let (A_m) be disjoint sets and $A = \bigcup_m A_m$. Let $f = \mathbb{1}_A$ and $f_n = \mathbb{1}_{\bigcup_{m=1}^n A_m}$, then $f_n \uparrow f$. So

$$\begin{aligned}
\mu\left(\bigcup_n A_n\right) = \mu(A) &= \int_{E_1} \left(\int_{E_2} \mathbb{1}_A \mu_2(dx_2) \right) \mu_1(dx_1) = \int_{E_1} \left(\int_{E_2} f \mu_2(dx_2) \right) \mu_1(dx_1) \\
&= \int_{E_1} \left(\lim_{n\to\infty} \int_{E_2} f_n \mu_2(dx_2) \right) \mu_1(dx_1) \qquad \text{monotone convergence theorem (Theorem 15.3.5)} \\
&= \lim_{n\to\infty} \int_{E_1} \left(\int_{E_2} f_n \mu_2(dx_2) \right) \mu_1(dx_1) \qquad \text{monotone convergence theorem (Theorem 15.3.5)} \\
&= \sum_{n=1}^{\infty} \mu(A_n). \qquad \text{(by definition of } \mu)
\end{aligned}$$

Thus μ is a measure on $\mathcal{E}$. □

Theorem 15.3.33 (Fubini's Theorem)**.** (i) Let f be $\mathcal{E}$-measurable and non-negative. Then

$$\mu(f) = \int_{E_1} \left(\int_{E_2} f(x_1, x_2)\mu_2(dx_2) \right) \mu_1(dx_1). \qquad (*) \tag{15.3.117}$$

(ii) Let f be μ-integrable. Then

(a) $x_1 \mapsto \int_{E_2} f(x_1, x_2)\mu_2(dx_2)$ is μ_1-integrable,

(b) $x_2 \mapsto f(x_1, x_2)$ is μ_2-integrable for μ_1-almost all x_1,

(c) the formula for $\mu(f)$ in (i) holds.

Proof. (i) Denote by $\mathcal{V}$ the set of all bounded $\mathcal{E}$-measurable functions f for which the formula $(*)$ holds. By boundedness of f, we have that $\mathcal{V}$ is a vector space.

Then $\mathcal{V}$ contains the indicator function of every $\mathcal{E}$-measurable set and if $f_n \in \mathcal{V}$ and bounded f with $0 \le f_n \uparrow f$, by monotone convergence theorem (Theorem 15.3.5), we have $f \in \mathcal{V}$. So, by the monotone class theorem (Theorem 15.2.9), $\mathcal{V}$ contains all bounded $\mathcal{E}$-measurable functions. Hence, for all $\mathcal{E}$-measurable functions f, we have

$$\mu(f_n) = \int_{E_1} \left(\int_{E_2} f_n(x_1, x_2)\mu_2(dx_2) \right) \mu_1(dx_1) \qquad (\dagger) \tag{15.3.118}$$

where $f_n = (-n) \vee f \wedge n$.

For f non-negative, we have $f_n \uparrow f$ and can pass to the limit as $n \to \infty$ by monotone convergence to extend the formula to f. That proves (i).

(ii) If f is μ-integrable, then, by (i)

$$\int_{E_1} \left| \int_{E_2} f(x_1, x_2) \mu_2(dx_2) \right| \mu_1(dx_1) \leq \int_{E_1} \left(\int_{E_2} |f(x_1, x_2)| \mu_2(dx_2) \right) \mu_1(dx_1) = \mu(|f|) < \infty. \tag{15.3.119}$$

Hence we obtain $\int_{E_2} f(x_1, x_2) \mu_2(dx_2)$ is μ_1-integrable and $f(x_1, x_2)$ is μ_2-integrable for μ_1-almost all x_1. Then, by dominated convergence theorem (Theorem 15.3.12), we can pass to the limit as $n \to \infty$ in the formula (†) to obtain the desired formula for $\mu(f)$.

□

Proposition 15.3.34. Let $\widehat{\mathcal{E}} = \mathcal{E}_2 \otimes \mathcal{E}_1$ and $\widehat{\mu} = \mu_2 \otimes \mu_1$. For a function f on $E_1 \times E_2$, write $\widehat{f}$ for the function on $E_2 \times E_1$ given by $\widehat{f}(x_2, x_1) = f(x_1, x_2)$. Suppose that f is $\mathcal{E}$-measurable. Then $\widehat{f}$ is $\widehat{\mathcal{E}}$-measurable, and if f is also non-negative or μ-integrable, then $\widehat{\mu}\left(\widehat{f}\right) = \mu(f)$.

Proof. Recall the notation in Fubini's theorem (Theorem 15.3.33 (i), (ii).(c)), if f is non-negative or μ-integrable,

$$\mu(f) = \int_{E_1} \left(\int_{E_2} f(x_1, x_2) \mu_2(dx_2) \right) \mu_1(dx_1). \tag{15.3.120}$$

With the similar argument, we have

$$\widehat{\mu}\left(\widehat{f}\right) = \int_{E_2} \left(\int_{E_1} \widehat{f}(x_2, x_1) \mu_1(dx_1) \right) \mu_2(dx_2) = \int_{E_2} \left(\int_{E_1} f(x_1, x_2) \mu_1(dx_1) \right) \mu_2(dx_2). \tag{15.3.121}$$

If $f = \mathbb{1}_A = \mathbb{1}_{A_1 \times A_2}$, $A = A_1 \times A_2 \in \mathcal{E}$, we have

$$\begin{aligned} \mu(f) &= \int_{E_1} \left(\int_{E_2} \mathbb{1}_{A_1} \mathbb{1}_{A_2} \mu_2(dx_2) \right) \mu_1(dx_1) = \int_{E_1} \mathbb{1}_{A_1} \left(\int_{E_2} \mathbb{1}_{A_2} \mu_2(dx_2) \right) \mu_1(dx_1) = \int_{E_1} \mathbb{1}_{A_1} \mu_2(A_2) \mu_1(dx_1) \\ &= \mu_1(A_1) \mu_2(A_2) = \int_{E_2} \mathbb{1}_{A_2} \mu_1(A_1) \mu_2(dx_2) = \int_{E_2} \mathbb{1}_{A_2} \left(\int_{E_1} \mathbb{1}_{A_1} \mu_1(dx_1) \right) \mu_2(dx_2) \\ &= \int_{E_2} \left(\int_{E_1} \mathbb{1}_{A_2} \mathbb{1}_{A_1} \mu_1(dx_1) \right) \mu_2(dx_2) = \widehat{\mu}\left(\widehat{f}\right). \end{aligned}$$

If f is simple function, we have the same conclusion by Proposition 15.3.4.

If f is non-negative measurable, we define $f_n = (2^{-n} \lfloor 2^n f \rfloor) \wedge n$. Thus f_n are simple functions and $f_n \to f$. We get the result required by applying monotone convergence theorem (Theorem 15.3.5).

If f is μ-integrable, we have that f is measurable and thus f^+, f^- are a non-negative measurable functions (Proposition 15.2.7). So $\mu(f^+) = \widehat{\mu}\left(\widehat{f^+}\right) = \widehat{\mu}\left(\widehat{f}^+\right)$ and $\mu(f^-) = \widehat{\mu}\left(\widehat{f^-}\right) = \widehat{\mu}\left(\widehat{f}^-\right)$ and

$$\widehat{\mu}\left(\left|\widehat{f}\right|\right) = \widehat{\mu}\left(\widehat{f}^+\right) + \widehat{\mu}\left(\widehat{f}^-\right) = \mu(f^+) + \mu(f^-) = \mu(|f|) < \infty \quad \Rightarrow \quad \widehat{f} \text{ is } \widehat{\mu}\text{-integrable.} \tag{15.3.122}$$

Thus $\mu(f) = \mu(f^+) - \mu(f^-) = \widehat{\mu}\left(\widehat{f}^+\right) - \widehat{\mu}\left(\widehat{f}^-\right) = \widehat{\mu}\left(\widehat{f}\right)$ as $\widehat{\mu}\left(\widehat{f}\right)$ is well-defined by integrability of $\widehat{f}$. □

Remark. Note that the iterated integral in Fubini's theorem (i) (Theorem 15.3.33) is well defined, for all bounded or non-negative measurable functions f, by Lemmas 15.3.30 and 15.3.31. Note also that, in combination wih Proposition 15.3.34, Fubini's theorem (Theorem 15.3.33) allows us to interchange the order of integration in multiple integrals, whenever the integrand is non-negative or μ-integrable.

Remark. The existence of product measure and Fubini's theorem extend easily to σ-finite measure spaces (Definition 15.1.17 as we can break up σ-finite spaces into countable unions of disjoint finite blocks). More important, it is crucial to have σ-finite.

Example 15.3.35. Let f_n be a sequence of functions on some finite measure space $(E, \mathcal{E}, \mu)$. Now consider $g(n, x) = f_n(x)$ and a σ-finite measure space $(\mathbb{N}, \mathcal{P}(\mathbb{N}), \nu)$ where $\nu(A) = \#A$ (the number of integers in the set $A \subseteq \mathbb{N}$). It is easy to prove

that ν is a measure. Then define on $G = \mathbb{N} \times E$, product σ-algebra $\mathcal{G} = \mathcal{P}(\mathbb{N}) \otimes \mathcal{E}$, product measure (by Theorem 15.3.32)

$$\lambda(A) = \int_{\mathbb{N}} \left(\int_E \mathbb{1}_A(n,x)\mu(dx) \right) \nu(dn) = \sum_{n=1}^{\infty} \left(\int_E \mathbb{1}_A(n,x)\mu(dx) \right) \tag{15.3.123}$$

Assume that

$$\lambda(|f|) = \sum_{n=1}^{\infty} \left(\int_E |f(n,x)|\, \mu(dx) \right) = \sum_{n=1}^{\infty} \int |f_n|\, d\mu < \infty, \tag{15.3.124}$$

then f is λ-integrable. Thus, by Fubini's theorem (Theorem 15.3.33 (ii)), we have

$$\lambda(f) = \sum_{n=1}^{\infty} \left(\int_E f(n,x)\mu(dx) \right) \quad \Rightarrow \quad \sum_{n=1}^{\infty} \int f_n d\mu = \int \left(\sum_{n=1}^{\infty} f_n \right) d\mu. \qquad \text{(Proposition 15.3.34)} \tag{15.3.125}$$

Example 15.3.36. Take $(E_1, \mathcal{E}_1) = (E_2, \mathcal{E}_2) = ([0,1], \mathcal{B}([0,1]))$ and let μ_1 be Lebesgue measure and $\mu_2(A) = \#A$ (number of real numbers in A) for $A \in \mathcal{B}$. Note that μ_2 is not σ-finite. Consider the $\mathcal{E}$-measurable function

$$f(x,y) = \mathbb{1}_{y=x} = \underbrace{\mathbb{1}_{E_1}}_{\in \mathcal{E}_1} \underbrace{\mathbb{1}_{y=x}}_{\text{for fixed } x, \{y=x\} \in \mathcal{E}_2}, \tag{15.3.126}$$

$$\int_{E_1} \left(\int_{E_2} f(x,y)\mu_2(dy) \right) \mu_1(dx) = \int_{E_1} \left(\int_{E_2} \mathbb{1}_{y=x}\mu_2(dy) \right) \mu_1(dx) = \int_{E_1} 1\mu_1(dx) = \mu_1(E_1) = 1, \tag{15.3.127}$$

since there is only a point to make $\mathbb{1}_{y=x} = 1$. On the other hand,

$$\int_{E_2} \left(\int_{E_1} f(x,y)\mu_1(dx) \right) \mu_2(dy) = \int_{E_2} \underbrace{\left(\int_{E_1} \mathbb{1}_{y=x}\mu_1(dx) \right)}_{\mathbb{1}_{y=x}=0 \text{ a.e. for fixed y}} \mu_2(dy) = \int_{E_2} \underbrace{0}_{\text{Theorem 15.3.7 (iii)}} \mu_2(dy) = 0 \cdot \infty = 0. \tag{15.3.128}$$

Thus, we can see σ-finiteness is essential for Fubini's theorem.

Remark. The operation of taking the product of two measure spaces is associative,

$$\mu_1 \otimes (\mu_2 \otimes \mu_3) = (\mu_1 \otimes \mu_2) \otimes \mu_3 \tag{15.3.129}$$

by a π-system uniqueness argument as

$$\mu(A) = \mu(A_1)\mu(A_2)\mu(A_3), \qquad A = A_1 \times A_2 \times A_3 \text{ is a } \pi\text{-system.} \tag{15.3.130}$$

So we can, by induction, take the product of a finite number, without specifying the order. Again, σ-finite is essential for the argument. In particular, the n-fold product of Lebesgue measure on $\mathbb{R}$ is called Lebesgue measure on $\mathbb{R}^n$. The corresponding integral is written

$$\int_{\mathbb{R}^n} f(x)dx = \int_{\mathbb{R}} \dots \int_{\mathbb{R}} f(x_1, \dots, x_n) dx_n \dots dx_1. \tag{15.3.131}$$

Proposition 15.3.37. Let $\mathcal{B}(\mathbb{R}^n)$ be the Borel set of $\mathbb{R}^n$ and $\mathcal{E} = \mathcal{B}(\mathbb{R})^n = \mathcal{B}(\mathbb{R}) \otimes \cdots \otimes \mathcal{B}(\mathbb{R})$. Then $\mathcal{E} = \mathcal{B}(\mathbb{R}^n)$.

Proof. To prove $\mathcal{E} \subseteq \mathcal{B}(\mathbb{R}^n)$, we have two approaches:

Approach 1. $\mathcal{B}(\mathbb{R}^n)$ is constructed from the topological space $(\mathbb{R}^n, \mathcal{T})$. Now, if $f_i : \mathbb{R}^n \to \mathbb{R}$ is the ith coordinate map:

$$f_i(x_1, x_2, \dots, x_n) = x_i, \tag{15.3.132}$$

then f_i is continuous[8], and hence $\mathcal{B}(\mathbb{R}^n)$-measurable (Proposition 15.2.3). Thus,

$$\mathcal{B}(\mathbb{R})^n = \sigma\left(f_i : 1 \le i \le n\right) \subseteq \mathcal{B}(\mathbb{R}^n) \tag{15.3.133}$$

Approach 2. Assume $n = 2$ and let $A_1 \in \mathcal{B}(\mathbb{R})$, $A_2 \in \mathcal{B}(\mathbb{R})$, we want to show that $A_1 \times A_2 \in \mathcal{B}(\mathbb{R}^2)$.

[8] need checking

Let C be an open interval in $\mathbb{R}$, then $\{B : C \times B \in \mathcal{B}(\mathbb{R}^2)\}$ is a d-system[9] containing finite unions of open intervals. Hence it contains $\mathcal{B}(\mathbb{R})$, so it contains A_2.

As a consequence, $\{A : A \times A_2 \in \mathcal{B}(\mathbb{R}^2)\}$ is a d-system containing open intervals (and hence finite unions), so contains $\mathcal{B}(\mathbb{R})$. Thus, we have $A_1 \times A_2 \in \mathcal{B}(\mathbb{R}^2)$ and $\mathcal{A} \subseteq \mathcal{B}(\mathbb{R}^2)$, $\mathcal{A}$ is π-system, so by Dynkin's lemma (Lemma 15.1.3), $\mathcal{E} \in \mathcal{B}(\mathbb{R}^2)$. Then we have the conclusion by induction.

On the other hand, $\mathcal{B}(\mathbb{R}^n)$ is generated by the open subsets of $\mathbb{R}^n$, and every such open subsets is a countable union of open 'hypercubes' of the form

$$\prod_{1\le i\le n} (a_i, b_i) \tag{15.3.134}$$

and such products are in $\mathcal{B}(\mathbb{R})^n$. Hence, $\mathcal{B}(\mathbb{R}^n) \subseteq \mathcal{B}(\mathbb{R})^n$ by Dynkin's lemma (Lemma 15.1.3). Thus, $\mathcal{B}(\mathbb{R}^n) = \mathcal{B}(\mathbb{R})^n$[10]. □

Remark. $\mathcal{B}(\mathbb{R}^n)$ is not a topology. Let $A \subseteq \mathbb{R}^n$ such that $A \notin \mathcal{B}(\mathbb{R}^n)$. If $\mathcal{B}(\mathbb{R}^n)$ were a topology, then it would be closed under arbitrary unions. As $\{x\} \in \mathcal{B}(\mathbb{R}^n)$ for all $x \in \mathbb{R}^n$, we would get the contradiction $A = \bigcup_{x\in A}\{x\} \in \mathcal{B}(\mathbb{R}^n)$ since A is an uncountable union (Klenke [10].P_9).

Proposition 15.3.38. Let $(E, \mathcal{E})$ be measurable space and μ be a σ-finite measure, then for any non-negative measurable function $f : E \to \mathbb{R}$,

$$\mu(f) = \int_0^\infty \mu(f \ge t)dt. \tag{15.3.135}$$

Proof. With Fubini theorem (Theorem 15.3.33),

$$\int_0^\infty \mu(f \ge t)dt = \int_0^\infty \mu\left(\mathbb{1}_{\{f\ge t\}}\right)dt = \int_0^\infty \int_E \mathbb{1}_{\{f\ge t\}} d\mu dt = \int_E \int_0^\infty \mathbb{1}_{\{f\ge t\}} dt d\mu = \int_E \int_0^f dt d\mu = \int_E f d\mu = \mu(f), \tag{15.3.136}$$

as required. □

15.3.8 Applications

Example 15.3.39. The function $f(x) = \sin x/x$ is not Lebesgue-integrable over $[1, \infty)$ but that the following limit does exist:

$$\lim_{N\to\infty} \int_1^N \frac{\sin x}{x} dx. \tag{15.3.137}$$

Solution *Approach 1.* Set $a_n = \int_{n\pi}^{(n+1)\pi} \frac{\sin x}{x} dx$. Then $\operatorname{sgn}(a_n) = (-1)^n$ and

$$|a_n| \ge \frac{1}{(n+1)\pi}\left|\int_{n\pi}^{(n+1)\pi} \sin x dx\right| = \frac{1}{(n+1)\pi}, \quad |a_n| \le \int_{n\pi}^{(n+1)\pi} \frac{1}{x} dx \le \frac{1}{n\pi}\int_{n\pi}^{(n+1)\pi} dx = \frac{1}{n} \qquad (*) \tag{15.3.138}$$

Thus,

$$\lim_{N\to\infty} \int_1^N \left|\frac{\sin x}{x}\right| dx = \int_1^\pi \left|\frac{\sin x}{x}\right| dx + \sum_{n=1}^\infty |a_n| \ge \int_1^\pi \left|\frac{\sin x}{x}\right| dx + \frac{1}{\pi}\sum_{n=2}^\infty \frac{1}{n} = \infty. \tag{15.3.139}$$

Also, we can see that $\operatorname{sgn}(a_n) = (-1)^n$ and $|a_n|$ is a decreasing sequence. Thus, with alternatiing series theorem, we have

$$\lim_{N\to\infty} \int_1^N \frac{\sin x}{x} dx = \int_1^\pi \frac{\sin x}{x} dx + \sum_{n=1}^\infty a_n \quad \text{converges.} \tag{15.3.140}$$

Approach 2. We need to show that the integral of $\left|\frac{\sin x}{x}\right|$ over $[1, \infty)$ is infinite. But by considering n triangles with vertices $(j\pi, 0)$, $\left(\frac{(2j+1)\pi}{2}, \frac{2}{(2j+1)\pi}\right)$, $((j+1)\pi, 0)$, $j = 1, \ldots, n$ (draw a picture), we see that

$$\int_1^{(n+1)\pi} \left|\frac{\sin x}{x}\right| dx > \sum_{j=1}^n \frac{1}{2j+1}$$

[9] need checking
[10] need proof

Since the RHS tends to ∞ as $n \to \infty$, the LHS must also tend to ∞. Then by monotone convergence, we see that

$$\int_1^\infty \left|\frac{\sin x}{x}\right| dx = \infty.$$

For the second part of the question, note that

$$\int_{j\pi}^{(j+1)\pi} \frac{\sin x}{x} dx$$

changes sign as j is odd or even, and then use the alternating series test.

Example 15.3.40. The Lebesgue integral $\int_0^\infty (\sin x/x)\, dx$ does not exist. However,

$$\lim_{N\to\infty} \int_0^N \frac{\sin x}{x} dx = \frac{\pi}{2}. \tag{15.3.141}$$

Solution From Example 15.3.39, we know that (from $(*)$)

$$\int_0^\infty \left(\frac{\sin x}{x}\right)^+ dx > \sum_{n=1}^\infty \frac{1}{2n} = \infty, \qquad \int_0^\infty \left(\frac{\sin x}{x}\right)^- dx \geq \sum_{n=1}^\infty \frac{1}{2n-1} = \infty. \tag{15.3.142}$$

Thus, the Lebesgue integral is not well-defined. The calculation of $\lim_{N\to\infty} \int_0^N (\sin x/x) dx$ is given in Example 11.0.4.

15.4 $\mathcal{L}^p$ Space, L^p Space and Convergence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$

15.4.1 $\mathcal{L}^p$-norms

Definition 15.4.1 ($\mathcal{L}^p$ Norm)**.** Let $(E, \mathcal{E}, \mu)$ be a measure space. For $1 \leq p < \infty$, we denote by $\mathcal{L}^p = \mathcal{L}^p(E, \mathcal{E}, \mu)$ the set of measurable functions f with finite $\mathcal{L}^p$-norm:

$$\|f\|_p = \left(\int_E |f|^p d\mu\right)^{1/p} < \infty. \tag{15.4.1}$$

Definition 15.4.2 (essential supremum)**.** We denote by $\mathcal{L}^\infty = \mathcal{L}^\infty(E, \mathcal{E}, \mu)$ the set of measurable functions f with the essential supremum of f:

$$\|f\|_\infty := \operatorname{esssup}(f) = \inf\{\lambda : |f| \leq \lambda \text{ a.e.}\} = \inf\{\lambda : \mu(x : |f(x)| > \lambda) = 0\}. \tag{15.4.2}$$

Remark. Note that $\|f\|_p \leq \mu(E)^{1/p} \|f\|_\infty$ for all $1 \leq p < \infty$.

Example 15.4.1. For $\alpha \in (0, \infty)$ and $p \in [1, \infty)$ and for

$$f_\alpha(x) = x^{-\alpha}, \quad x > 0. \tag{15.4.3}$$

For $0 < a < b < \infty$ by the fundamental theorem of calculus (Theorem 15.3.26), we have over intervals $[a, b]$,

$$\int_a^b x^{-\alpha p} dx = \frac{b^{1-\alpha p} - a^{1-\alpha p}}{1 - \alpha p}. \tag{15.4.4}$$

Now note that $f_\alpha \mathbb{1}_{[\frac{1}{n},1]} \uparrow f_\alpha \mathbb{1}_{[0,1]}$, $f_\alpha \mathbb{1}_{[1,n]} \uparrow f_\alpha \mathbb{1}_{[1,\infty)}$ and then with monotone convergence theorem (Theorem 15.3.5)by passing to the limits $a \downarrow 0$ with $b = 1$ and $b \uparrow \infty$ with $a = 1$, we have

$$f_\alpha \in \mathcal{L}^p((0, 1], dx) \;\Leftrightarrow\; \alpha p < 1, \qquad f_\alpha \in \mathcal{L}^p([1, \infty), dx) \;\Leftrightarrow\; \alpha p > 1.$$

Definition 15.4.3. For $1 \leq p \leq \infty$ and $f_n \in \mathcal{L}^p$, we say that f_n converges to f in $\mathcal{L}^p$ if $\|f_n - f\|_p \to 0$.

15.4.2 Chebyshev's inequality

Theorem 15.4.2. Let f be a non-negative measurable function and let $\lambda \geq 0$. Then $\lambda\mu(f \geq \lambda) \leq \mu(f)$.

Proof. We use the notation $\{f \geq \lambda\}$ for the set $\{x \in E : f(x) \geq \lambda\}$. Then $\lambda \mathbb{1}_{\{f \geq \lambda\}} \leq f \Rightarrow \lambda\mu(f \geq \lambda) \leq \mu(f)$, by Theorem 15.3.7. □

Now let g be any measurable function. We can deduce inequalities for g by choosing some non-negative measurable function ϕ and applying Chebyshev's inequality (Theorem 15.4.2) to $f = \phi \circ g$.

For example, if $g \in \mathcal{L}^p$, $p < \infty$ and $\lambda > 0$, then $\mu(|g| \geq \lambda) = \mu(|g|^p \geq \lambda^p) \leq \lambda^{-p}\mu(|g|^p) < \infty$.

So we obtain the tail estimate $\mu(|g| \geq \lambda) = O(\lambda^{-p})$, as $\lambda \to \infty$.

15.4.3 Jensen's inequality

Definition 15.4.4. Let $I \subseteq \mathbb{R}$ be an interval. A function $f : I \to \mathbb{R}$ is convex if, for all $x, y \in I$ and $t \in [0, 1]$,

$$f(tx + (1-t)y) \leq tf(x) + (1-t)f(y). \tag{15.4.5}$$

Lemma 15.4.3. Let $f : I \to \mathbb{R}$ be convex and let m be a point in the interior of I. Then there exist $a, b \in \mathbb{R}$ such $f(x) \geq ax + b$ for all x, with equality at $x = m$.

Proof. By convexity, for $m, x, y \in I$ with $x < m < y$, we have

$$\frac{f(m) - f(x)}{m - x} \leq \frac{f(y) - f(m)}{y - m}. \tag{15.4.6}$$

So, fixing an interior point m, there exists $a \in \mathbb{R}$ such that, for all $x < m$ and all $y > m$

$$\frac{f(m) - f(x)}{m - x} \leq a \leq \frac{f(y) - f(m)}{y - m}. \tag{15.4.7}$$

Then $f(x) \geq a(x - m) + f(m)$, for all $x \in I$. □

Theorem 15.4.4 (Jensen's inequality)**.** For measure space $(E, \mathcal{E}, \mu)$ with $\mu(E) = 1$, let g be an integrable function with values in I and $f : I \to \mathbb{R}$ be convex. Then $\mu(f \circ g)$ is well defined and

$$\mu(f \circ g) \geq f(\mu(g)). \tag{15.4.8}$$

The equality holds when f is not strictly convex, e.g. when it is a straight line, or when g follows a degenerate distribution, i.e. $g = \mu(g)$ a.e..

Remark. (i) Note that this won't hold for finite measure ($\mu(E) < \infty$). We can think about the case g equals to some constant c a.e.. as we can not tell that $f(c)\mu(E) \geq f(c\mu(E))$.

(ii) Jensen's inequality also gets other versions, i.e., alternative finite form[11].

Proof. If f is a stright line, it is easy to have the equality.

For the case where g is almost everywhere constant. We say $g = c$ a.e., then $\mu(g) = c\mu(E) = c$ by Theorem 15.3.10.

Otherwise, $m = \mu(g)$ must lie in the interior of I (if not the equality $m = \mu(g)$ does not hold). Choose $a, b \in \mathbb{R}$ as in Lemma 15.4.3, then $f \circ g \geq ag + b$ a.e. with equality at $g = m = \mu(g)$ a.e.. In particular,

$$f \circ g \geq ag + b \quad \Rightarrow \quad (f \circ g)^- \leq (ag + b)^-. \tag{15.4.9}$$

and $(ag + b)^-$ is a convex function, thus for $t \in [0, 1]$

$$(ag + b)^- \leq t(ag)^- + (1-t)b^- \leq t\left((ag)^- + (ag)^+\right) + (1-t)\left(b^- + b^+\right) = t\,|ag| + (1-t)\,|b|\,. \tag{15.4.10}$$

Then by Theorem 15.3.7, $\mu((f \circ g)^-) \leq |a|\mu(|g|) + |b| < \infty$, since g is μ-integrable.

So $\mu(f \circ g)$ is well defined (as existence of one of $\mu\left((f \circ g)^+\right)$ and $\mu\left((f \circ g)^-\right)$ implies the existence of $\mu(f \circ g)$ in Remark 15.3.1). If $f \circ g$ is not μ-integrable, we have $\mu(f \circ g) = \infty$ which satisfies the inequality. Moreover, if $f \circ g$ is μ-integrable, by Theorem 15.3.10 (ii),

$$\mu(f \circ g) \geq a\mu(g) + b = am + b = f(m) = f(\mu(g)) \tag{15.4.11}$$

[11] see wikipedia

with equality at $g = \mu(g)$ a.e..

Finally, note that for the equality to be held, $\mu(g \neq \mu(g)) > 0$ can not be the case since this will give different values of $ag + b$. □

We deduce from Jensen's inequality the monotonicity of $\mathcal{L}^p(E, \mathcal{E}, \mu)$-norms with respect to a measure.

Proposition 15.4.5. Let $1 \leq p < q < \infty$ and $\mu(E) = 1$. For any real-valued function $g \in \mathcal{L}^p(E, \mathcal{E}, \mu)$, $\|g\|_p \leq \|g\|_q$. Moreover, $\mathcal{L}^q(E, \mathcal{E}, \mu) \subseteq \mathcal{L}^p(E, \mathcal{E}, \mu)$.

Proof. First, set $f(x) = |x|^{q/p}$, then f is convex. Since g^p is real-valued integrable function, by Jensen's inequality (Theorem 15.4.4),

$$\|g\|_p = (\mu|g|^p)^{1/p} = (f(\mu|g|^p))^{1/q} \leq (\mu f(|g|^p))^{1/q} = (\mu|g|^q)^{1/q} = \|g\|_q . \tag{15.4.12}$$

Then $\forall g \in \mathcal{L}^q(E, \mathcal{E}, \mu)$, set $g_n = |g| \wedge n$. Thus, g_n is bounded real-valued function and thus integrable, so is g_n^q. So, by Jensen's inequality (Theorem 15.4.4),

$$\|g_n\|_p = (\mu|g_n|^p)^{1/p} = (f(\mu|g_n|^p))^{1/q} \leq (\mu f(|g_n|^p))^{1/q} = (\mu|g_n|^q)^{1/q} = \|g_n\|_q \leq \|g\|_q < \infty. \tag{15.4.13}$$

Since $g_n \uparrow |g|$, with monotone convergence theorem (Theorem 15.3.5), we have $\|g_n\|_p \uparrow \|g\|_p$, thus, $\|g\|_p \leq \|g\|_q < \infty$, $g \in \mathcal{L}^p(E, \mathcal{E}, \mu)$. Hence $\mathcal{L}^q(E, \mathcal{E}, \mu) \subseteq \mathcal{L}^p(E, \mathcal{E}, \mu)$. □

Remark. This statement is not ture for infinite measure, for example, $f(x) = \frac{1}{x}$,

$$\begin{aligned} \|f\|_1 = \mu(|f|) &= \int_1^\infty \frac{1}{x} dx = \log x|_1^\infty \quad \Rightarrow \quad f \notin \mathcal{L}^1([1,\infty), \mathcal{B}([1,\infty)), \text{Leb}) \\ \|f\|_2 = \mu(|f|^2)^{1/2} &= \left(\int_1^\infty \frac{1}{x^2} dx\right)^2 = \left(-\frac{1}{x}\Big|_1^\infty\right)^{1/2} = 1 < \infty \ \Rightarrow \ f \in \mathcal{L}^2([1,\infty), \mathcal{B}([1,\infty)), \text{Leb}) \end{aligned}$$

15.4.4 Hölder's inequality and Minkowski's inequality

Definition 15.4.5. For $p, q \in [1, \infty]$, we say that p and q are conjugate indices if

$$\frac{1}{p} + \frac{1}{q} = 1. \tag{15.4.14}$$

Theorem 15.4.6 (Hölder's inequality)**.** Let $p, q \in [1, \infty]$ be conjugate indices. Then, for all measurable functions $f \in \mathcal{L}^p(\mathbb{E}, \mathcal{E}, \mu)$ and $g \in \mathcal{L}^q(\mathbb{E}, \mathcal{E}, \mu)$, fg is integrable and

$$\mu(|fg|) \leq \|f\|_p \|g\|_q . \tag{15.4.15}$$

(i) For $p, q \in (1, \infty)$, Hölder's inequality becomes an equality if and only if $|f|^p$ and $|g|^q$ are linearly dependent in $\mathcal{L}^1(E, \mathcal{E}, \mu)$, i.e., for $f \in \mathcal{L}^p(\mathbb{E}, \mathcal{E}, \mu)$ and $g \in \mathcal{L}^q(\mathbb{E}, \mathcal{E}, \mu)$, there exist real number $\alpha, \beta \geq 0$ such that $\alpha |f|^p = \beta |g|^q$ a.e.

(ii) For $p, q \in \{1\} \cup \{\infty\}$, Hölder's inequality becomes an equality if and only if $p = 1$ and $g = \|g\|_\infty$ a.e. or $q = 1$ and $f = \|f\|_\infty$ a.e..

Proof. Consider the case that $p, q \in (1, \infty)$. If $\|f\|_p = 0$, we have

$$\left(\int_E |f|^p d\mu\right)^{1/p} = 0 \quad \Rightarrow \quad \left(\int_E |f|^p d\mu\right) = 0 \quad \Rightarrow \quad |f|^p = 0 \ \text{ a.e.} \quad \text{(by Theorem 15.3.7)} \tag{15.4.16}$$

Thus, $|f| = 0$ a.e. $|fg| = 0$ a.e.. This is because

$$\{|fg| > 0\} = \bigcup_{n \in \mathbb{Z}^+} \left\{|fg| > \frac{1}{n}\right\} = \bigcup_{n \in \mathbb{Z}^+} \bigcup_{q \in \mathbb{R}^+} \left\{|f| > \frac{1}{nq}\right\} \cap \{|g| > q\} \subseteq \bigcup_{n \in \mathbb{Z}^+} \bigcup_{q \in \mathbb{R}^+} \left\{|f| > \frac{1}{nq}\right\} \tag{15.4.17}$$

is a sum of countable zero-measure sets. This implies that $\mu(\{|fg| > 0\}) = 0$. Thus, $|fg| = 0$ a.e. and by Theorem 15.3.7, $\mu(|fg|) = 0$ and the inequality holds.

If $\|f\|_p \in (0,\infty)$, let $\|f\|_p = a$. So we can define a finite measure ν on $\mathcal{E}$ by

$$\nu(A) = \frac{1}{a^p}\int_A |f|^p d\mu = \frac{1}{a^p}\mu\left(|f|^p \mathbb{1}_A\right). \tag{15.4.18}$$

Obviously, $\nu(E) = 1$ and for simple function h ($h \geq 0$), we have $a^p\nu(h) = \mu(h|f|^p)$. Thus, for non-negative measurable function h, by monotone convergence theorem (Theorem 15.3.5), we have $a^p\nu(h) = \mu(h|f|^p)$. Or we can have this by Proposition 15.3.22.

Now for the non-negative measurable function h, if it is ν-integrable, $h < \infty$ a.e.. Thus,

$$\nu(h) = \underbrace{\nu\left(h\mathbb{1}_{\{h<\infty\}}\right) + \nu\left(h\mathbb{1}_{\{h=\infty\}}\right)}_{\text{Theorem 15.3.7}} \leq \underbrace{\nu\left(h^q\mathbb{1}_{\{h<\infty\}}\right)^{1/q} + \nu\left(h\mathbb{1}_{\{h=\infty\}}\right)}_{\text{Proposition 15.4.5}} \leq \underbrace{\nu\left(h^q\right)^{1/q} + 0}_{\text{as } h<\infty \text{ a.e.}} = \nu\left(h^q\right)^{1/q} \qquad (*).$$

Note that $q(p-1) = p$ and $1 + \frac{p}{q} = p$. Then use $(*)$ and Jensen's inequality (Theorem 15.4.4)

$$\mu(|fg|) = \mu\left(\frac{|g|}{|f|^{p-1}}|f|^p\right) = a^p\nu\left(\frac{|g|}{|f|^{p-1}}\right) \leq aa^{p/q}\nu\left(\frac{|g|^q}{|f|^{q(p-1)}}\right)^{1/q} = a\mu(|g|^q)^{1/q} = \|f\|_p \|g\|_q. \tag{15.4.19}$$

with equality when $\frac{|g|}{|f|^{p-1}} = c$ a.e. for some $c \geq 0$ as $l(x) = x^q$ is strictly convex. So the equality holds when

$$|g| = c|f|^{p-1} \text{ a.e. } \Rightarrow \ |g|^q = c^q|f|^{q(p-1)} = c^q|f|^p \text{ a.e.}. \tag{15.4.20}$$

If $p, q = 1$ or ∞. Let $p = 1$ and $q = \infty$, we have $\|g\|_\infty = \inf\{\lambda \geq 0 : |g| \leq \lambda \text{ a.e.}\} \Rightarrow \mu(g) \leq \|g\|_\infty$ (by Theorem 15.3.7). If $\|g\|_\infty < \infty$, $|f||g| \leq |f|\|g\|_\infty$ a.e.,

$$\mu(|fg|) = \mu(|f||g|) \leq \mu(|f|\|g\|_\infty) = \mu(|f|)\|g\|_\infty = \|f\|_1\|g\|_\infty. \tag{15.4.21}$$

Obviously, the eqaulity holds for $|g| = \|g\|_\infty$ a.e. □

Remark. Hölder's inequality can also be proved by Young's inequality. See Klenke [10].P_{150}.

If $p = q = 2$, Hölder's inequality is Cauchy-Schwarz inequality (Theorem 15.4.7). Hölder's inequality also holds for complex-valued functions f and g on E[12].

Theorem 15.4.7 (Cauchy-Schwarz inequality)**.** Let $(E, \mathcal{E}, \mu)$ be a probability space. Then for all measurable functions $f, g \in \mathcal{L}^2(E, \mathcal{E}, \mu)$, fg is integrable and

$$(\mu(fg))^2 \leq (\mu|fg|)^2 \leq \mu\left(f^2\right)\mu\left(g^2\right). \tag{15.4.22}$$

The equality holds when $\alpha f = \beta g$ for some $\alpha, \beta \in \mathbb{R}$ a.e..

Remark. The first inequality is given by Theorem 15.3.10.(iv) and second is given by Theorem 15.4.6

Theorem 15.4.8 (Minkowski's inequality)**.** For $p \in [1,\infty]$ and measurable functions $f, g \in \mathcal{L}^p(E, \mathcal{E}, \mu)$, we have

$$\|f+g\|_p \leq \|f\|_p + \|g\|_p. \tag{15.4.23}$$

For $p \in (1,\infty)$, the equality holds if and only if $f = cg$ or $g = cf$ for some $c \geq 0$ a.e..

Proof. If $p = 1$, $|f+g| = |f^+ - f^- + g^+ - g^-| \leq |f^+ + f^-| + |g^+ + g^-| = |f| + |g|$, then

$$\mu(|f+g|) \leq \mu(|f|) + \mu(|g|) \qquad \text{(by Theorem 15.3.7 (ii))}. \tag{15.4.24}$$

If $p = \infty$, we let $\|f\|_\infty = \lambda_f$ and $\|g\|_\infty = \lambda_g$,

$$|f| \leq \lambda_f \text{ a.e.}, \quad |g| \leq \lambda_g \text{ a.e.} \quad \Rightarrow \quad |f| + |g| \leq \lambda_f + \lambda_g \text{ a.e.} \quad \Rightarrow \quad |f+g| \leq \lambda_f + \lambda_g \text{ a.e.}. \tag{15.4.25}$$

Thus, $\|f+g\|_\infty = \inf\{\lambda : |f+g| \leq \lambda \text{ a.e.}\} \leq \lambda_f + \lambda_g = \|f\|_\infty + \|g\|_\infty$, so the inequality holds for $p = \infty$.

Now consider the case $p \in (1,\infty)$. If $\|f\|_p = \infty$ or $\|g\|_p = \infty$, the inequality holds obviously.

[12] need checking

So we consider the case that $p > 1$ and $\|f\|_p < \infty$ or $\|g\|_p < \infty$, then

$$\left|\frac{f+g}{2}\right|^p \leq \left|\frac{|f|+|g|}{2}\right|^p \leq |\max\{|f|,|g|\}|^p \leq (|f|^p + |g|^p) \quad \Rightarrow \quad |f+g|^p \leq 2^p\left(|f|^p + |g|^p\right) \tag{15.4.26}$$

By Theorem 15.3.7 (ii), $\mu(|f+g|^p) \leq 2^p\left(\mu(|f|^p) + \mu(|g|^p)\right) < \infty$ $(*)$.

The case where $\|f+g\|_p = 0$ is clear, so let us assume $\|f+g\|_p > 0$. Observe that

$$\left\||f+g|^{p-1}\right\|_q = \mu\left(|f+g|^{(p-1)q}\right)^{1/q} = \mu\left(|f+g|^p\right)^{1-1/p} \qquad (\dagger). \tag{15.4.27}$$

Also, we can see that $|f+g|^{p-1} \in \mathcal{L}^q(E,\mathcal{E},\mu)$ as $\left\||f+g|^{p-1}\right\|_q = \mu\left(|f+g|^p\right)^{1-1/p} < \infty$ by $(*)$. So, by Hölder's inequality (Theorem 15.4.6),

$$\begin{aligned}\mu(|f+g|^p) &\overset{**}{\leq} \mu\left(|f||f+g|^{p-1}\right) + \mu\left(|g||f+g|^{p-1}\right) \\ &\leq \left(\|f\|_p + \|g\|_p\right)\left\||f+g|^{p-1}\right\|_q = \left(\|f\|_p + \|g\|_p\right)\mu\left(|f+g|^p\right)^{1-1/p}.\end{aligned}$$

As $\mu(|f+g|^p) < \infty$ $(*)$, we can divide both sides by $\left\||f+g|^{p-1}\right\|_q = \mu\left(|f+g|^p\right)^{1-1/p}$ $(\dagger)$, then the result follows.

For $p \in (1,\infty)$, we have the equality holds when

$$\alpha_1|f|^p = \beta_1|f+g|^{p-1} \text{ a.e., } \alpha_2|g|^p = \beta_2|f+g|^{p-1} \text{ a.e.} \quad \text{for some } \alpha_1,\alpha_2,\beta_1,\beta_2 \geq 0. \tag{15.4.28}$$

by Hölder's inequality (Theorem 15.4.6. Then we have $|f| = c|g|$ for some $c \geq 0$ a.e.. Also, we can see that f and g must have the same sign to imply the equality $(**)$. Thus, the equality holds when $f = cg$ or $g = cf$ for some $c \geq 0$ a.e.. □

15.4.5 Completeness of $\mathcal{L}^p$

Theorem 15.4.9 (Completeness of $\mathcal{L}^p$)**.** Let $p \in [1,\infty]$. Let $(f_n : n \in \mathbb{N})$ be a sequence in $\mathcal{L}^p$ such that

$$\|f_n - f_m\|_p \to 0 \quad \text{as } n,m \to \infty. \tag{15.4.29}$$

Then there exists $f \in \mathcal{L}^p$ such that

$$\|f_n - f\|_p \to 0 \quad \text{as } n \to \infty. \tag{15.4.30}$$

Proof. f_n is Cauchy sequence in $\mathcal{L}^p$, then $\forall \varepsilon > 0$ we can find $N \in \mathbb{N}$ and $\exists m,n \geq N$ such that $\|f_n - f_m\|_p < \varepsilon$. So we can find a subsequence $(n_k)_{k\geq 1}$ such that

$$\left\|f_{n_{k+1}} - f_{n_k}\right\|_p < \frac{1}{2^k} \quad \Rightarrow \quad S = \sum_{k=1}^{\infty}\left\|f_{n_{k+1}} - f_{n_k}\right\|_p < 1 < \infty. \tag{15.4.31}$$

By Minkowski's inequality, for any $K \in \mathbb{N}$, $\left\|\sum_{k=1}^{K}\left|f_{n_{k+1}} - f_{n_k}\right|\right\|_p \leq \sum_{k=1}^{K}\left\|f_{n_{k+1}} - f_{n_k}\right\|_p \leq S < \infty$. Then we have two cases:

(i) For the case that $p < \infty$, by monotone convergence theorem (Theorem 15.3.5), this bound holds also for $K = \infty$, as

$$\sum_{k=1}^{K}\left|f_{n_{k+1}} - f_{n_k}\right| \uparrow \sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right| \quad \Rightarrow \quad \left\|\sum_{k=1}^{K}\left|f_{n_{k+1}} - f_{n_k}\right|\right\|_p \uparrow \left\|\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right\|_p. \tag{15.4.32}$$

$$\text{So} \quad \left\|\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right\|_p < \infty \quad \Rightarrow \quad \int\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p d\mu = \mu\left(\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p\right) < \infty. \tag{15.4.33}$$

Then for any $\lambda \geq 0$, by Theorem 15.3.7 (ii),

$$\lambda\mathbb{1}_{\left\{\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p \geq \lambda\right\}} \leq \left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p \quad \Rightarrow \quad \lambda\mu\left(\mathbb{1}_{\left\{\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p \geq \lambda\right\}}\right) \leq \mu\left(\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}} - f_{n_k}\right|\right)^p\right).$$

Let $\lambda = \infty$, we have

$$\infty \cdot \mu\left(\mathbb{1}_{\left\{\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right|\right)^p=\infty\right\}}\right) \leq \mu\left(\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right|\right)^p\right) < \infty \tag{15.4.34}$$

which gives $\mu\left(\mathbb{1}_{\left\{\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right|\right)^p=\infty\right\}}\right) = 0 \;\Rightarrow\; \sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right| < \infty$ a.e..

(ii) If $p=\infty$, $\left\|\sum_{k=1}^{K}\left|f_{n_{k+1}}-f_{n_k}\right|\right\|_p = \inf\left\{\lambda : \left|\sum_{k=1}^{K}\left|f_{n_{k+1}}-f_{n_k}\right|\right| \leq \lambda \text{ a.e.}\right\} \leq S \;\Rightarrow\; \mu\left(\left|\sum_{k=1}^{K}\left|f_{n_{k+1}}-f_{n_k}\right|\right|\right) \leq S$.

Then by monotone convergence (Theorem 15.3.5),

$$\sum_{k=1}^{K}\left|f_{n_{k+1}}-f_{n_k}\right| \uparrow \sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right| \quad \Rightarrow \quad \mu\left(\sum_{k=1}^{K}\left|f_{n_{k+1}}-f_{n_k}\right|\right) \uparrow \mu\left(\sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right|\right) \leq S < \infty. \tag{15.4.35}$$

Using the same argument, we have the same result that $\sum_{k=1}^{\infty}\left|f_{n_{k+1}}-f_{n_k}\right| < \infty$ a.e..

Hence, for both cases, by completeness of $\mathbb{R}$ (Theorem 3.6.1), f_{n_k} converges a.e. (as f_{n_k} is a cauchy sequence a.e.). We define a measurable function f by

$$f(x) = \begin{cases} \lim f_{n_k}(x) & \text{if the limit exists} \\ 0 & \text{otherwise} \end{cases} \tag{15.4.36}$$

Given $\varepsilon > 0$, we can find N so that $n \geq N$ implies

$$\|f_n - f_m\|_p = \begin{cases} \mu(|f_n - f_m|^p) < \varepsilon & p \in [1,\infty) \\ \inf\{\lambda : |f_n - f_m| \leq \lambda \text{ a.e.}\} < \varepsilon & p = \infty \end{cases} \quad \text{for all } m \geq n, \tag{15.4.37}$$

(i) For $p \in [1,\infty)$, $\mu(|f_n - f_{n_k}|^p) < \varepsilon$ for all sufficiently large k. Hence, for $n \geq N$, $|f_n - f|^p \geq 0$ and $|f_n - f| = |f_n - \lim_{k\to\infty} f_{n_k}|$ a.e., by Theorem 15.3.7 (ii)

$$\begin{aligned} \mu(|f_n - f|^p) &= \mu\left(\left|f_n - \lim_{k\to\infty} f_{n_k}\right|^p\right) = \mu\left(\lim_{k\to\infty}|f_n - f_{n_k}|^p\right) \\ &= \mu\left(\liminf_{k\to\infty}|f_n - f_{n_k}|^p\right) \quad \text{(Definition 3.5.2 (iii))} \\ &\leq \liminf_{k\to\infty}\mu\left(|f_n - f_{n_k}|^p\right) < \varepsilon. \quad \text{(Fatou's lemma, Lemma 15.3.11)} . \end{aligned}$$

Thus, $\|f_n - f\|_p \to 0$.

(ii) If $p = \infty$, $\inf\{\lambda : |f_n - f_{n_k}| \leq \lambda \text{ a.e.}\} < \varepsilon$ for all sufficiently large k and $\mu(|f_n - f_{n_k}|) < \varepsilon$. Hence, for $n \geq N$, $|f_n - f| \geq 0$ and $|f_n - f| = |f_n - \lim_{k\to\infty} f_{n_k}|$ a.e., for arbitrarily small δ,

$$\begin{aligned} \inf\{\lambda : |f_n - f| \leq \lambda \text{ a.e.}\} &= \inf\left\{\lambda : \left|f_n - \lim_{k\to\infty} f_{n_k}\right| \leq \lambda \text{ a.e.}\right\} \\ &\leq \mu\left(\left|f_n - \lim_{k\to\infty} f_{n_k}\right|\right) + \delta \qquad \text{(Definition 2.7.1, infimum)} \\ &\leq \liminf \mu\left(|f_n - f_{n_k}|\right) + \delta < \varepsilon + \delta. \qquad \text{(Fatou's lemma, Lemma 15.3.11)} \end{aligned}$$

Thus, $\|f_n - f\|_\infty \to 0$.

Furthermore, we need to show that $f \in \mathcal{L}^p$. For $p \in [1,\infty)$,

$$\underbrace{\mu\left(|f|^p\right) = \mu\left(\lim_{k\to\infty}|f_{n_k}|^p\right)}_{\text{Theorem 15.3.7 (ii)}} = \mu\left(\liminf|f_{n_k}|^p\right) \leq \liminf \mu\left(|f_{n_k}|^p\right) < \infty. \tag{15.4.38}$$

For $p = \infty$, $\mu(|f_{n_k}|) \leq \inf\{\lambda : |f_{n_k}| \leq \lambda \text{ a.e.}\} < \infty$. For arbitrarily small δ,

$$\inf\{\lambda : |f| \leq \lambda \text{ a.e.}\} = \inf\{\lambda : \lim|f_{n_k}| \leq \lambda \text{ a.e.}\} \underbrace{\leq \mu(\lim|f_{n_k}|) + \delta}_{\text{Definition 2.7.1 (infimum)}} \leq \underbrace{\liminf \mu(|f_{n_k}|) + \delta}_{\text{Fatou lemma (Lemma 15.3.11)}} < \infty. \tag{15.4.39}$$

Hence, $f \in \mathcal{L}^p$ and, since $\varepsilon > 0$ was arbitrarily small, $\|f_n - f\|_p \to 0$. □

Proposition 15.4.10. The sequence f_n is a Cauchy sequence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$ if and and only if f_n converges in $\mathcal{L}^p$ to $f \in \mathcal{L}^p(E, \mathcal{E}, \mu)$.

15.4.6 L^p space

Recall the definitions of norm (Definition 10.8.1) and inner product (Definition 10.9.1). Minkowski's inequality shows that each L^p space is a vector space and that the $\mathcal{L}^p$-norms satisfy condition (i), (iii) and (iv), but condition (ii) fails, because $\|f\|_p = 0$ does not imply that $f = 0$, only that $f = 0$ a.e..

However, it is possible to make the $\mathcal{L}^p$-norms into true norms by quotienting out by the subspace of measurable functions vanishing a.e.. This quotient will be denoted L^p.

The notion of convergence in $\mathcal{L}^p$ defined in previous section is the usual notion of convergence in a normed space. We can define a equivalence relation

$$u \sim v \quad \Leftrightarrow \quad u = v \text{ a.e.} \tag{15.4.40}$$

Then this quotienting gives us a complete space. Usually, we do not do this quotienting in probability theory.

Note that, for $f \in L^2$, we have $\|f\|_2^2 = \langle f, f \rangle$, where $\langle \cdot, \cdot \rangle$ is the symmetric bilinear form on L^2 given by

$$\langle f, g \rangle = \int_E f g d\mu. \tag{15.4.41}$$

Thus L^2 is an inner product space.

A normed vector space V is complete if every Cauchy sequence in V converges, that is to say, given any sequence $(v_n : n \in \mathbb{N})$ in V such that $\|v_n - v_m\| \to 0$ as $n, m \to \infty$, there exists $v \in V$ such that $\|v_n - v\| \to 0$ as $n \to \infty$. A complete normed vector space is called a Banach space (Definition 14.0.3). A complete inner product space is called a Hilbert space. Such spaces have many useful properties, which makes the following result important.

Corollary 15.4.11. We have

(a) $L^p(E, \mathcal{E}, \mu)$ is a Banach space, for all $1 \leq p \leq \infty$,

(b) $L^2(E, \mathcal{E}, \mu)$ is a Hilbert space.

15.4.7 Orthogonal Projection

We shall apply some general Hilbert space arguments to $\mathcal{L}^2$. First, we have

Proposition 15.4.12. Pythagoras' rule

$$\|f + g\|_2^2 = \|f\|_2^2 + 2\langle f, g \rangle + \|g\|_2^2 \tag{15.4.42}$$

and the parallelogram law

$$\|f + g\|_2^2 + \|f - g\|_2^2 = 2\left(\|f\|_2^2 + \|g\|_2^2\right). \tag{15.4.43}$$

Definition 15.4.6. If $\langle f, g \rangle = 0$, then we say that f and g are orthogonal. For any subset $V \subseteq \mathcal{L}^2$, we define[13]

$$V^\perp = \{f \in \mathcal{L}^2 : \langle f, v \rangle = 0 \text{ for all } v \in V\}. \tag{15.4.44}$$

Definition 15.4.7. A subset $V \subseteq \mathcal{L}^2$ is closed if, for every sequence $(f_n : n \in \mathbb{N})$ in V, with $f_n \to f$ in $\mathcal{L}^2$, we have $f = v$ a.e., for some $v \in V$.

Theorem 15.4.13 (Orthogonal Projection)**.** Let V be a complete subspace of $\mathcal{L}^2$. Then each $f \in \mathcal{L}^2$ has a decomposition $f = g + h$, with $g \in V$ and $h \in V^\perp$. Moreover, $\|f - g\|_2 \leq \|f - u\|_2$ for all $u \in V$, $f - g \perp v$ for all $v \in V$ with equality only if $g = u$ a.e..

The function g is called the orthogonal projection of f on V.

[13] could be introduced earlier

Proof. Choose a sequence $g_n \in V$ such that

$$\|f - g_n\|_2 \to d(f, V) = \inf\{\|f - u\|_2 : u \in V\}. \tag{15.4.45}$$

By the parallelogram law,

$$\|2(f - (g_n + g_m)/2)\|_2^2 + \|g_n - g_m\|_2^2 = 2\left(\|f - g_n\|_2^2 + \|f - g_m\|_2^2\right). \tag{15.4.46}$$

But $\|2(f - (g_n + g_m)/2)\|_2^2 \geq 4d(f, V)^2$, so we must have $\|g_n - g_m\|_2 \to 0$ as $n, m \to \infty$. So g_n is a Cauchy sequence in $\mathcal{L}^2$. By completeness of $\mathcal{L}^2$, $\|g_n - g\|_2 \to 0$, for some $g \in \mathcal{L}^2$.

Hence, $\|f - g\|_2 \leq \|f - g_n\| + \|g_n - g\|_2$ implies that $\|f - g\|_2 = \inf\{\|f - u\|_2 : u \in V\}$.

Now, for any $v \in V$ and $t \in \mathbb{R}$, we have

$$d(f, V)^2 \leq \|f - (g + tv)\|_2^2 = d(f, V)^2 - 2t\langle f - g, v\rangle + t^2\|v\|_2^2. \tag{15.4.47}$$

So we must have $\langle f - g, v\rangle = 0$ for arbitrarily small t. Hence $h = f - g \in V^\perp$, as required.

If $g = u$ a.e., i.e., $\|g - u\|_2 = 0$ for some $u \in V$, then

$$\|f - u\|_2 \leq \|g - u\|_2 + \|f - g\|_2 = 0 + d(f, V) = d(f, V). \tag{15.4.48}$$

Thus, the equality holds. □

Proposition 15.4.14. Let $(E, \mathcal{E}, \mu)$ be a measure space and let $V_1 \subseteq V_2 \subseteq \dots$ be an increasing sequence of closed subspaces of $\mathcal{L}^2 = \mathcal{L}^2(E, \mathcal{E}, \mu)$ for $f \in \mathcal{L}^2$, denoted by f_n the orthogonal projection of f on V_n. Show that f_n converges in $\mathcal{L}^2$.

Proof. Since $\mathcal{L}^2$ is complete, we need only show that the f_n are Cauchy. We have, for $m \leq n$,

$$\|f_m - f_n\|_2^2 = \|(f - f_n) - (f - f_n)\|_2^2 = \|f - f_n\|_2^2 - 2\langle f - f_n, f - f_m\rangle + \|f - f_m\|_2^2. \tag{15.4.49}$$

By the definition of orthogonal projection (Theorem 15.4.13), we have

$$\|f - f_n\|_2^2 + \|f_n\|_2^2 = \|f\|_2^2 \qquad (*) \tag{15.4.50}$$

Using this, and also noting that $f - f_n \in V_n^\perp \subseteq V_m^\perp$, we get

$$\|f_m - f_n\|_2^2 = 2\|f\|_2^2 - \|f_m\|_2^2 - \|f_n\|_2^2 - 2\langle f - f_n, f - f_m\rangle \tag{15.4.51}$$

$$= 2\|f\|_2^2 - \|f_m\|_2^2 - \|f_n\|_2^2 - 2(\|f\|_2^2 - \|f_n\|_2^2) = \|f_n\|_2^2 - \|f_m\|_2^2 \qquad (\dagger) \tag{15.4.52}$$

Thus f_n is Cauchy if $\|f_n\|_2^2$ is Cauchy. But $(\dagger)$ shows that the $\|f_n\|^2$ are increasing, and $(*)$ shows they are bounded above by $\|f\|_2^2$. Thus $\|f_n\|_2$ converges and is therefore Cauchy. □

15.4.8 Uniform integrable

Lemma 15.4.15. For a measure space $(E, \mathcal{E}, \mu)$, let f be an integrable measurable function and set

$$I_f(\delta) = \sup\{\mu(|f|\mathbb{1}_A) : A \in \mathcal{E}, \mu(A) \leq \delta\} \quad \Rightarrow \quad I_f(\delta) \downarrow 0 \text{ as } \delta \downarrow 0. \tag{15.4.53}$$

Proof. Suppose not. Then, for some $\varepsilon > 0$, there exists $A_n \in \mathcal{E}$, with $\mu(A_n) \leq 2^{-n}$ and $\mu(|f|\mathbb{1}_{A_n}) \geq \varepsilon$ for all n. By the first Borel-Cantelli lemma (Lemma 15.1.13), $\mu(A_n \text{ i.o.}) = 0$. But then, by dominated convergence theorem ,

$$|f|\mathbb{1}_{\{\bigcup_{m\geq n} A_m\}} \to |f|\mathbb{1}_{\{A_n \text{ i.o.}\}} \quad \Rightarrow \quad \varepsilon \leq \mu\left(|f|\mathbb{1}_{\{\bigcup_{m\geq n} A_m\}}\right) \to \mu\left(|f|\mathbb{1}_{\{A_n \text{ i.o.}\}}\right) = 0 \tag{15.4.54}$$

which is a contradiction. □

Definition 15.4.8. For a measure space $(E, \mathcal{E}, \mu)$, let $\{f_\alpha\}$ be a collection of measurable functions. For $1 \leq p \leq \infty$, we say that $\{f_\alpha\}$ is bounded in $\mathcal{L}^p(E, \mathcal{E}, \mu)$ if

$$\sup_{f \in \{f_\alpha\}} \|f\|_p < \infty. \tag{15.4.55}$$

Definition 15.4.9. Let $(E, \mathcal{E}, \mu)$ be a measure space. Define

$$I_{\{f_\alpha\}}(\delta) = \sup\{\mu(|f|\mathbb{1}_A) : f \in \{f_\alpha\}, A \in \mathcal{E}, \mu(A) \le \delta\}. \tag{15.4.56}$$

We say that $\{f_\alpha\}$ is uniformly integrable or UI if $\{f_\alpha\}$ is bounded in $\mathcal{L}^1(E, \mathcal{E}, \mu)$ and

$$I_{\{f_\alpha\}}(\delta) \downarrow 0 \text{ as } \delta \downarrow 0, \quad \text{i.e., } \forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } I_{\{f_\alpha\}}(\delta) < \varepsilon. \tag{15.4.57}$$

Proposition 15.4.16. Let $(E, \mathcal{E}, \mu)$ be a measure space. If $\mu(E) < \infty$ and a collection of measurable function, $\{f_\alpha\}$ is bounded in $\mathcal{L}^p(E, \mathcal{E}, \mu)$, for some $p \in (1, \infty]$, then $\{f_\alpha\}$ is UI.

Proof. By Hölder's inequality (Theorem 15.4.6), for conjugate indices $p \in (1, \infty]$, $q \in [1, \infty)$,

$$\mu(|f|\mathbb{1}_A) \le \|f\|_p (\mu(A))^{1/q}. \tag{15.4.58}$$

Hence, if $\{f_\alpha\}$ is bounded in $\mathcal{L}^p(E, \mathcal{E}, \mu)$, $\|f\|_p (\mu(A))^{1/q} \le \sup_{f \in \{f_\alpha\}} \|f\|_p (\mu(E))^{1/q} < \infty$, then $\{f_\alpha\}$ is UI. □

Example 15.4.17. The sequence $f_n = n\mathbb{1}_{(0,1/n)}$ is bounded in $\mathcal{L}^1(E, \mathcal{E}, \mu)$ for Lebesgue measure on $(0, 1]$, but not uniformly integrable as for all n, $\sup \mathbb{E}\left(n\mathbb{1}_{(0,1/n)}\right) = 1$.

Proposition 15.4.18. Any single integrable measurable function is uniformly integrable. This extends easily to any finite collection of integrable measurable functions.

Proof. Direct result from Lemma 15.4.15 and Hölder's inequality (Theorem 15.4.6). □

Proposition 15.4.19. For any integrable measurable function g, the set

$$\{f_\alpha\} = \{f : f \text{ is a measurable function}, |f| \le g\} \quad \text{is UI.} \tag{15.4.59}$$

Proof. First, $\mu(|f|1_A) \le \mu(g1_A)$ for all A. By Proposition 15.4.18, we have $\{f_\alpha\}$ is UI. □

Lemma 15.4.20. Let $(E, \mathcal{E}, \mu)$ be a measure space with $\mu(E) < \infty$. Let $\{f_\alpha\}$ be a family of measurable functions. Then $f \in \{f_\alpha\}$ is UI if and only if

$$\sup\{\mu(|f|\mathbb{1}_{|f| \ge K}) : f \in \{f_\alpha\}\} \to 0, \quad \text{as } K \to \infty. \tag{15.4.60}$$

Proof. Suppose $\{f_\alpha\}$ is UI. Given $\varepsilon > 0$, choose $\delta > 0$ so that $I_{\{f_\alpha\}}(\delta) < \varepsilon$, then choose $K < \infty$ so that $\sup_{f \in \{f_\alpha\}} \mu(|f|) \le K\delta$ since $\{f_\alpha\}$ is bounded in $\mathcal{L}^1$ by the definition of UI. Then, for $f \in \{f_\alpha\}$ and $A = \{|f| \ge K\}$, we have

$$\mu(A) = \underbrace{\mu(|f| \ge K) \le \frac{\mu(|f|)}{K}}_{\text{Chebyshev's inequality (Theorem 15.4.2)}} \le \frac{\sup \mu(|f|)}{K} \le \frac{\delta K}{K} = \delta, \tag{15.4.61}$$

so $\mu(|f|\mathbb{1}_A) < \varepsilon$. Hence, as $K \to \infty$, $\sup\{\mu(|f|1_{\{|f| \ge K\}}) : f \in \{f_\alpha\}\} \to 0$.

On the other hand, if this condition holds, then, since

$$|f| = |f|\,\mathbb{1}_{\{|f|<K\}} + |f|\,\mathbb{1}_{\{|f| \ge K\}} \quad \Rightarrow \quad \underbrace{\mu(|f|) \le \mu\left(|f|\,\mathbb{1}_{\{|f|<K\}}\right) + \mu|f|\mathbb{1}_{\{|f| \ge K\}}}_{\text{Minkowski's inequality, Theorem 15.4.8}} \quad \Rightarrow \quad \mu(|f|) < K\mu(E) + \mu|f|\mathbb{1}_{\{|f| \ge K\}}$$

Thus, take $\varepsilon = 1$, we can choose K

$$\sup_{f \in \{f_\alpha\}} \mu(|f|) < K\mu(E) + \sup_{f \in \{f_\alpha\}} \mu|f|\mathbb{1}_{\{|f| \ge K\}} < K\mu(E) + 1 < \infty \quad \Rightarrow \quad \{f_\alpha\} \text{ is bounded in } \mathcal{L}^1. \tag{15.4.62}$$

Given $\varepsilon > 0$, choose $K < \infty$ so that $\mu(|f|\mathbb{1}_{\{|f| \ge K\}}) < \varepsilon/2$ for all $f \in \{f_\alpha\}$. Then choose $\delta > 0$ so that $K\delta < \varepsilon/2$. For all $f \in \{f_\alpha\}$ and $A \in \mathcal{E}$ with $\mu(A) < \delta$, we have

$$\mu(|f|\mathbb{1}_A) \le \mu(|f|\mathbb{1}_{\{|f| \ge K\}}\mathbb{1}_A) + \mu(|f|\mathbb{1}_{\{|f|<K\}}\mathbb{1}_A) < \mu(|f|\mathbb{1}_{\{|f| \ge K\}}) + K\mu(A) < \varepsilon. \tag{15.4.63}$$

Hence $\{f_\alpha\}$ is UI. □

Alternative definition of uniformly integrable is given by the following theorem.

Theorem 15.4.21. Let $(E,\mathcal{E},\mu)$ be a measure space. A collection of measurable functions $\{f_\alpha\}$ is uniformly integrable, it is equivalent to either of the following two conditions:

$$\text{(i)} \inf_{0\le g\in\mathcal{L}^1(E,\mathcal{E},\mu)} \sup_{f\in\{f_\alpha\}} \mu\left(|f|\,\mathbb{1}_{|f|>g}\right)=0, \qquad \text{(ii)} \inf_{0\le g\in\mathcal{L}^1(E,\mathcal{E},\mu)} \sup_{f\in\{f_\alpha\}} \mu\left((|f|-g)^+\right)=0. \tag{15.4.64}$$

If $\mu(E)<\infty$, then uniformly integrability is equivalent to either of the following two conditions:

$$\text{(iii)} \inf_{a\in[0,\infty)} \sup_{f\in\{f_\alpha\}} \mu\left(|f|\,\mathbb{1}_{|f|>a}\right)=0, \qquad \text{(iv)} \inf_{a\in[0,\infty)} \sup_{f\in\{f_\alpha\}} \mu\left((|f|-a)^+\right)=0. \tag{15.4.65}$$

Proof. Klenke [10].P_{135}.[14] □

15.4.9 Convergence in $\mathcal{L}^p(E,\mathcal{E},\mu)$

Definition 15.4.10. Let $(E,\mathcal{E},\mu)$ be a measure space. We say the sequence of measurable functions f_n converges in $\mathcal{L}^p$ to f, for some $p\in[1,\infty)$, denoted by $f_n \overset{\mathcal{L}^p}{\to} f$, if $f,f_n\in\mathcal{L}^p(E,\mathcal{E},\mu)$ for all n and

$$\mu\,|f_n-f|^p\to 0 \ \text{ as } n\to\infty. \tag{15.4.66}$$

If $p=\infty$, we say f_n converges in $\mathcal{L}^\infty$ to f, if $f,f_n\in\mathcal{L}^\infty(E,\mathcal{E},\mu)$ for all n and

$$\|f_n-f\|_\infty\to 0 \ \text{ as } n\to\infty. \tag{15.4.67}$$

Proposition 15.4.22. Let $(E,\mathcal{E},\mu)$ be a measure space and $\mu(E)=1$. For $p=[1,\infty)$, if $f_n \overset{\mathcal{L}^p}{\to} f$, then for any $q\in[1,p)$, $f_n \overset{\mathcal{L}^q}{\to} f$.

Proof. This is direct result from Proposition 15.4.5. □

Proposition 15.4.23. Let $(E,\mathcal{E},\mu)$ be a measure space. For $p=[1,\infty)$, if $f_n \overset{\mathcal{L}^p}{\to} f$, then $f_n \overset{\mu}{\to} f$.

Proof. If $f_n \overset{\mathcal{L}^p}{\to} f$, $\forall\varepsilon>0$, and then $\varepsilon\mathbb{1}_{\{|f_n-f|\ge\varepsilon\}}\le|f_n-f|$,

$$\mu\left(\{|f_n-f|\ge\varepsilon\}\right)^{1/p}=\frac{1}{\varepsilon}\left\|\varepsilon\mathbb{1}_{\{|f_n-f|\ge\varepsilon\}}\right\|_p \underbrace{\le \frac{1}{\varepsilon}\|f_n-f\|_p}_{\text{by Theorem 15.3.10}} \to \frac{1}{\varepsilon}0=0 \quad\Rightarrow\quad \mu\left(\{|f_n-f|\ge\varepsilon\}\right)\to 0 \ \text{ as } \ n\to\infty.$$

Thus, f_n converges to f in measure. □

Theorem 15.4.24 (bounded convergence theorem)**.** Let $(E,\mathcal{E},\mu)$ be a measure space with $\mu(E)<\infty$. Let f be a measurable function and let $(f_n : n\in\mathbb{N})$ be a sequence of such functions. Suppose $f_n\to f$ in measure and $|f_n|\le M$ for all n, for some constant $M<\infty$. Then for $p\in[1,\infty)$. $f_n \overset{\mathcal{L}^p}{\to} f$.

Remark. When $p=1$, this is Theorem 15.3.16.

Proof. Let $\mu(E)=C$. Since $|f_n|\le M$ for all n, we have $f_n\in\mathcal{L}^p(E,\mathcal{E},\mu)$. By Theorem 15.2.14 (ii), f is the almost everywhere limit of a subsequence, so

$$|f|=|f_{n_k}-f_{n_k}+f|\le|f_{n_k}-f|+|f_{n_k}|\le|f_{n_k}-f|+M\to M \ \text{ a.e. } \Rightarrow\ |f|^p\le M^p \text{ a.e. } \Rightarrow\ f\in\mathcal{L}^p(E,\mathcal{E},\mu). \tag{15.4.68}$$

For $\varepsilon>0$, there exists N such that $n\ge N$ implies (by definition of convergence in measure (Definition 15.2.6))

$$\mu\left(\{|f_n-f|^p>\varepsilon/(2C)\}\right)\le\varepsilon/(2^{p+1}M^p). \qquad (*) \tag{15.4.69}$$

[14] need proof

Then by Theorem 15.3.10.(ii),

$$\begin{aligned}\mu|f_n - f|^p &= \mu\left(|f_n - f|^p \mathbb{1}_{\{|f_n-f|^p>\varepsilon/(2C)\}}\right) + \mu\left(|f_n - f|^p \mathbb{1}_{\{|f_n-f|^p\le\varepsilon/(2C)\}}\right)\\ &\le \mu\left(2^p M^p \mathbb{1}_{\{|f_n-f|^p>\varepsilon/(2C)\}}\right) + \mu\left(\varepsilon/(2C)\right)\\ &= 2^p M^p \mu\left(\mathbb{1}_{\{|f_n-f|^p>\varepsilon/(2C)\}}\right) + \frac{\varepsilon}{2C}\mu(E)\\ &\le 2^p M^p \varepsilon/(2^{p+1}M^p) + \varepsilon/2 = \varepsilon, \quad \text{by } (*)\end{aligned}$$

which implies that $\mu(|f_n - f|^p) \to 0$. Hence, $f_n \overset{\mathcal{L}^p}{\to} f$. □

Theorem 15.4.25 (Vitali Convergence Theorem)**.** Let $f_1, f_2, \dots$ be $\mathcal{L}^p(E, \mathcal{E}, \mu)$-integrable functions, for $1 \le p < \infty$. Then the sequence f_n is a Cauchy sequence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$ if and and only if

(i) the sequence f_n is a Cauchy sequence in measure,

(ii) the collection of functions, $\{|f_n|^p\}$ is uniformly integrable,

(iii) for every $\varepsilon > 0$, there exists a set A of finite measure, such that $\|f_n \mathbb{1}_{A^c}\|_p < \varepsilon$ for all n.

Remark. The statement "f_n is a Cauchy sequence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$" can be replaced by "$f_n$ is convergent in $\mathcal{L}^p(E, \mathcal{E}, \mu)$" by Proposition 15.4.10. Also, "f_n is convergent in $\mathcal{L}^p(E, \mathcal{E}, \mu)$" can imply strong statement "f_n is convergent in measure" by Proposition 15.4.23.

Note that if the sequence f_n is a Cauchy sequence in measure, then there exists f such that f_n converges to f in measure[15].

Proof. ($\Rightarrow$) Assume f_n is Cauchy sequence in $\mathcal{L}^p(E, \mathcal{E}, \mu)$, then given $\varepsilon > 0$, there exists N, $\|f_m - f_n\|_p < \varepsilon$ for all $m, n \ge N$ i.e., $\|f_m - f_n\|_p \to 0$ as $m, n \to \infty$

(i) Fix $\eta > 0$, and then $\eta \mathbb{1}_{\{|f_m-f_n|\ge\eta\}} \le |f_m - f_n|$,

$$\mu\left(\{|f_m - f_n| \ge \eta\}\right)^{1/p} = \frac{1}{\eta}\left\|\eta \mathbb{1}_{\{|f_m-f_n|\ge\eta\}}\right\|_p \underbrace{\le \frac{1}{\eta}\|f_m - f_n\|_p}_{\text{by Theorem 15.3.10}} \to \frac{1}{\eta}0 = 0 \quad \Rightarrow \quad \mu\left(\{|f_m - f_n| \ge \eta\}\right) \to 0 \text{ as } m, n \to \infty.$$

Thus, f_n is a Cauchy sequence in measure.

(ii) Given $\varepsilon > 0$, select N such that $\|f_n - f_N\|_p < \varepsilon$ when $n \ge N$. The family $\{f_\alpha^N\} = \{|f_1|^p, \dots, |f_{N-1}|^p, |f_N|^p\}$ is uniformly integrable because it consists of only finitely many integrable functions.

So for every $\varepsilon > 0$, there is $\delta > 0$ such that $\mu(A) \le \delta$ implies $\|f_n \mathbb{1}_A\|_p < \varepsilon$ for $n \le N$ by the fact that $\{f_\alpha^N\}$ is UI. On the other hand, for $n > N$,

$$\|f_n \mathbb{1}_A\|_p \le \|(f_n - f_N)\mathbb{1}_A\|_p + \|f_N \mathbb{1}_A\|_p \le \|f_n - f_N\|_p + \|f_N \mathbb{1}_A\|_p < 2\varepsilon \tag{15.4.70}$$

for the same sets A, and thus the entire infinite sequence $\{|f_n|^p\}$ is uniformly integrable too.

(iii) Given ε, select N such that $\|f_n - f_N\|_p < \varepsilon$ for all $n \ge N$. Then let

$$\varphi_m = 2^{-m}\left\lfloor 2^m f_N^+ \right\rfloor \wedge m - 2^{-m}\left\lfloor 2^m f_N^- \right\rfloor \wedge m = \sum_{i=1}^m a_i \mathbb{1}_{A_i} - \sum_{j=1}^m b_j \mathbb{1}_{B_j}. \tag{15.4.71}$$

where $a_i, b_j \in [0, \infty)$ and A_i, B_j are disjoint sets. Note that the integral of φ_m is well-definted since f_N is integrable. Since $\varphi_m \to f_N \Rightarrow (\varphi_m - f_N)^p \to 0$, by dominated convergence theorem (Theorem 15.3.12), we have some $\varphi^N := \varphi_k$ in the sequence (φ_m) s.t. $\left\|f_N - \varphi^N\right\|_p < \varepsilon$. Then by Minkowski's inequality (Theorem 15.4.8), we have

$$\left\|f_n - \varphi^N\right\|_p \le \|f_n - f_N\|_p + \left\|f_N - \varphi^N\right\|_p < 2\varepsilon \quad \text{for all } n \ge N. \tag{15.4.72}$$

[15] need proof

Let $S_N = \{\varphi^N \neq 0\}$ be the support of φ^N,

$$\begin{aligned}\mu(S_N) &\leq \underbrace{\max_{1\leq i\leq k}\{a_i, b_i : a_i, b_i \neq 0\}}_{\text{finite many}} \mu\left(\left\{\bigcup_{i=1}^{k}(A_i \cup B_i) : a_i, b_i \neq 0\right\}\right) \\ &\leq \frac{\max_{1\leq i\leq k}\{a_i, b_i : a_i, b_i \neq 0\}}{\min_{1\leq i\leq k}\{a_i, b_i : a_i, b_i \neq 0\}}\mu\left(|\varphi^N|\right) \leq \frac{\max_{1\leq i\leq k}\{a_i, b_i : a_i, b_i \neq 0\}}{\min_{1\leq i\leq k}\{a_i, b_i : a_i, b_i \neq 0\}}\mu\left(|f_N|\right) < \infty\end{aligned}$$

since f_N is integrable. Hence S_N must have finite measure. Then we have

$$\left\|f_n \mathbb{1}_{S_N^c}\right\|_p = \|f_n - f_n\mathbb{1}_{S_N}\|_p \underbrace{\leq \left\|f_n - \varphi^N\right\|_p + \left\|\varphi^N - f_n\mathbb{1}_{S_N}\right\|_p}_{\text{Minkowski's inequality (Theorem 15.4.8)}} = \left\|f_n - \varphi^N\right\|_p + \left\|(\varphi^N - f_n)\mathbb{1}_{A_N}\right\|_p < 2\varepsilon + 2\varepsilon = 4\varepsilon. \tag{15.4.73}$$

For each $n < N$, we can similarly construct φ^n (as we did for φ^N), such that $\|f_n - \varphi^n\|_p < 2\varepsilon$ and let $S_n = \{\varphi^n \neq 0\}$ of finite measure,

$$\left\|f_n \mathbb{1}_{S_n^c}\right\|_p = \|f_n - f_n\mathbb{1}_{S_n}\|_p \underbrace{\leq \|f_n - \varphi^n\|_p + \|\varphi^n - f_n\mathbb{1}_{S_n}\|_p}_{\text{Minkowski's inequality (Theorem 15.4.8)}} = \|f_n - \varphi^n\|_p + \|(\varphi^n - f_n)\mathbb{1}_{S_n}\|_p < 2\varepsilon + 2\varepsilon = 4\varepsilon. \tag{15.4.74}$$

Then we set $A = S_1 \cup \cdots \cup S_{N-1} \cup S_N$, a finite union, then A has finite measure, and clearly

$$\|f_n \mathbb{1}_{A^c}\|_p < 4\varepsilon \text{ for any } n. \tag{15.4.75}$$

($\Leftarrow$) We show $\|f_m - f_n\|_p$ to be small for large m, n by a multi-step estimate: fix $\eta > 0$, we have (by Minkowski's inequality, Theorem 15.4.8),

$$\|f_m - f_n\|_p \leq \left\||f_m - f_n|\,\mathbb{1}_{A\setminus\{|f_m - f_n|\geq\eta\}}\right\|_p + \left\||f_m - f_n|\,\mathbb{1}_{\{|f_m - f_n|\geq\eta\}}\right\|_p + \left\||f_m - f_n|\,\mathbb{1}_{E\setminus A}\right\|_p. \tag{15.4.76}$$

Use condition (iii) to choose A of finite measure such that

$$\|f_n \mathbb{1}_{A^c}\|_p < \varepsilon \text{ for all } n \quad \Rightarrow \quad \||f_m - f_n|\,\mathbb{1}_{A^c}\|_p < 2\varepsilon. \tag{15.4.77}$$

Let $\eta = \varepsilon/\mu(A)^{1/p} > 0$ and $A_{mn} = \{|f_m - f_n| \geq \eta\}$. By condition (ii), choose $\delta > 0$ s.t.

$$\|f_n \mathbb{1}_{A_{mn}}\|_p < \varepsilon \quad \text{whenever } \mu(A_{mn}) < \delta \quad \Rightarrow \quad \||f_m - f_n|\,\mathbb{1}_{A_{mn}}\|_p < 2\varepsilon. \tag{15.4.78}$$

Then by condition (i), exists N such that $\mu(A_{mn}) < \delta$ if $m, n \geq N$. Thus,

$$\begin{aligned}\|f_m - f_n\|_p &\leq \left\||f_m - f_n|\,\mathbb{1}_{A\setminus\{|f_m - f_n|\geq\eta\}}\right\|_p + \left\||f_m - f_n|\,\mathbb{1}_{\{|f_m - f_n|\geq\eta\}}\right\|_p + \||f_m - f_n|\,\mathbb{1}_{A^c}\|_p \\ &< \|\eta\mathbb{1}_A\|_p + \||f_m - f_n|\,\mathbb{1}_{A_{mn}}\|_p + \||f_m - f_n|\,\mathbb{1}_{A^c}\|_p \\ &= \frac{\varepsilon}{\mu(A)^{1/p}}\|\mathbb{1}_A\|_p + \||f_m - f_n|\,\mathbb{1}_{A_{mn}}\|_p + \||f_m - f_n|\,\mathbb{1}_{A^c}\|_p < \varepsilon + 2\varepsilon + 2\varepsilon = 5\varepsilon.\end{aligned}$$

Hence, $\|f_m - f_n\|_p < 5\varepsilon$ for $m, n \geq N$. □

Remark. This theorem can be used as a replacement for the more well-known dominated convergence theorem (Theorem 15.3.12), when a dominating factor cannot be found for the functions f_n to be integrated. (If this theorem is known, the dominated convergence theorem can be derived as a special case.)

In a finite measure space, condition (iii) is trivial. In fact, condition (iii) is the tool used to reduce considerations in the general case to the case of a finite measure space.

In probability theory, the definition of 'uniform integrability' (in fact, the definition is Lemma 15.4.20) is slightly different from its definition in general measure theory. The special case is Theorem 19.3.36.

15.4.10 Dense property

Definition 15.4.11. A stepfunction $f : \mathbb{R} \to \mathbb{R}$ is any finite linear combination of indicator functions of finite intervals.

Proposition 15.4.26. The set of stepfunctions $\mathcal{J}$ is dense in $\mathcal{L}^p(\mathbb{R}, \mathcal{B}(\mathbb{R}), \mu)$ for all $p \in [1, \infty)$, i.e., for all $f \in \mathcal{L}^p(\mathbb{R}, \mathcal{B}(\mathbb{R}), \mu)$ and all $\varepsilon > 0$ there exists $g \in \mathcal{J}$ such that $\|f - g\|_p < \varepsilon$.

Proof. Let $f \in \mathcal{L}^p(\mathbb{R}, \mathcal{B}(\mathbb{R}), \mu)$ and assume first, for simplicity, that $f \geq 0$. Given $\varepsilon > 0$, there exists $N_1 \in \mathbb{R}$ such that

$$\left\|f - f\mathbb{1}_{[-N_1,N_1]}\right\|_p < \frac{\varepsilon}{3} \qquad (*) \tag{15.4.79}$$

To see this, note that $|f|^p \geq \left|f - f\mathbb{1}_{[-n,n]}\right|^p \to 0$ as $n \to \infty$, and use dominated convergence (Theorem 15.3.12).

Now, set $f_n = 2^{-n}\left\lfloor 2^n f\mathbb{1}_{[-N_1,N_1]}\right\rfloor \wedge n$, so f_n simple and $\left|f_n - f\mathbb{1}_{[-N_1,N_1]}\right|^p \to 0$. Again, by dominated convergence, there exists $N_2 \in \mathbb{N}$ with

$$\left\|f\mathbb{1}_{[-N_1,N_1]} - f_{N_2}\right\|_p < \frac{\varepsilon}{3} \qquad (\dagger) \tag{15.4.80}$$

Suppose $f_{N_2} = \sum_{k=1}^m a_k \mathbb{1}_{A_k}$, for Borel sets A_k containted in $[-N_1, N_1]$, and positive reals a_k, $k = 1, \ldots, m$. By Proposition 15.1.21, for each A_k one can find a finite collection of finite, disjoint intervals $B_{1,k}, \ldots, B_{l_k,k}$, contained in $[-N_1, N_1]$, such that

$$\mu\left(A_k \triangle \bigcup_{j=1}^{l_k} B_{j,k}\right) = \left\|\mathbb{1}_{A_k} - \mathbb{1}_{\left\{\bigcup_{j=1}^{l_k} B_{j,k}\right\}}\right\|_p < \frac{\varepsilon}{3m \max_k a_k} \tag{15.4.81}$$

Set $g = \sum_{k=1}^m \left(a_k \sum_{j=1}^{l_k} \mathbb{1}_{B_{j,k}}\right)$, so g is a stepfunction. Thus,

$$\|f_{N_2} - g\|_p < \left\|\sum_{k=1}^m a_k \mathbb{1}_{A_k} - \sum_{k=1}^m \left(a_k \sum_{j=1}^{l_k} \mathbb{1}_{B_{j,k}}\right)\right\|_p \leq m \max_k a_k \left\|\mathbb{1}_{A_k} - \mathbb{1}_{\left\{\bigcup_{j=1}^{l_k} B_{j,k}\right\}}\right\|_p < \frac{\varepsilon}{3} \qquad (\ddagger) \tag{15.4.82}$$

Combining $(*)$ and $(\dagger)$, and $(\ddagger)$ using Minkowski's inequality (Theorem 15.4.8), we have that

$$\|f - g\|_p \leq \left\|f - f\mathbb{1}_{[-N_1,N_1]}\right\|_p + \left\|f\mathbb{1}_{[-N_1,N_1]} - f_{N_2}\right\|_p + \|f_{N_2} - g\|_p < \varepsilon.$$

Finally for general $f \in \mathcal{L}_p(\mathbb{R}, \mathcal{B}(\mathbb{R}), \mu)$ and $\varepsilon > 0$, we set $f = f^+ - f^-$. From the above, we can find stepfunctions g_1, g_2 such that $\|f^+ - g_1\|_p, \|f^- - g_2\|_p < \frac{\varepsilon}{2}$. But then by Minkowski's inequality again,

$$\|f - (g_1 - g_2)\|_p \leq \left\|f^+ - g_1\right\|_p + \|f^- - g_2\|_p < \epsilon, \tag{15.4.83}$$

and $g_1 - g_2$ is of course a stepfunction. □

15.4.11 Fourier transform

Definition 15.4.12. For a finite Borel measure μ on $\mathbb{R}^n$, we define the Fourier transform

$$\widehat{\mu}(u) = \int_{\mathbb{R}^n} e^{i\langle u,x\rangle} \mu(dx), \quad u \in \mathbb{R}^n. \tag{15.4.84}$$

Remark. Here, $\langle \cdot, \cdot \rangle$ denotes the usual inner product on $\mathbb{R}^n$. Note that $\widehat{\mu}$ is in general complex-valued, with $\overline{\widehat{\mu}(u)} = \widehat{\mu}(-u)$, and $\|\widehat{\mu}\|_\infty = \widehat{\mu}(0) = \mu(\mathbb{R}^n)$.

Proposition 15.4.27. The Fourier transform of a finite Borel measure is a bounded continuous function.

Proof. First we have $\forall u \in \mathbb{R}^n$

$$|\widehat{\mu}(u)| = \left|\int_{\mathbb{R}^n} e^{i\langle u,x\rangle} \mu(dx)\right| \leq \int_{\mathbb{R}^n} \left|e^{i\langle u,x\rangle}\right| \mu(dx) = \int_{\mathbb{R}^n} \mu(dx) = \mu(\mathbb{R}^n) < \infty. \tag{15.4.85}$$

Moreover, for any sequence $u_n \to u$ and $\forall x \in \mathbb{R}^n$, we have $e^{i\langle u_n,x\rangle} \to e^{i\langle u,x\rangle}$. Then

$$|\widehat{\mu}(u_n) - \widehat{\mu}(u)| = \left|\int_{\mathbb{R}^n} \left(e^{i\langle u_n,x\rangle} - e^{i\langle u,x\rangle}\right) \mu(dx)\right| \to 0 \tag{15.4.86}$$

by bounded convergence theorem (Theorem 15.3.15, $\left|e^{i\langle u_n,x\rangle}-e^{i\langle u,x\rangle}\right|<2$). Thus, $\widehat{\mu}$ is continuous on $\mathbb{R}^n$. □

Proposition 15.4.28. For a finite Borel measure μ on $\mathbb{R}$ and $\int |x|^k d\mu(x)<\infty$, then the Fourier transform $\hat{\mu}$ of μ has a kth continuous derivative, which at 0 is given by

$$\hat{\mu}^{(k)}(0)=i^k\int x^k d\mu(x). \tag{15.4.87}$$

Proof. Note that if $\int |x|^k \mu(dx)<\infty$ and μ finite, by Hölder's inequality (Theorem 15.4.6), for all $n\le k$,

$$\int_{\mathbb{R}} |x|^n \mu(dx)\le\left(\int_{\mathbb{R}} |x|^k \mu(dx)\right)^{\frac{n}{k}} \mu(\mathbb{R})^{1-\frac{n}{k}}<\infty \tag{15.4.88}$$

Thus we have

(i) $x\mapsto e^{iux}$ is integrable for all u.

(ii) $u\mapsto e^{iux}$ is infintely differentiable for all x.

(iii) $\left|\frac{\partial^n}{\partial u^n}e^{iux}\right|\le|x|^n$, which is integrable for $n\le k$.

These properties allow for differention k times under the integral (Theorem 15.3.29). Thus, by Hölder's inequality (Theorem 15.4.6)

$$\left|\widehat{\mu}^{(k)}(u)\right|=\left|\int_{\mathbb{R}} i^k x^k e^{iux}\mu(dx)\right|\le\int_{\mathbb{R}}\left|x^k e^{iux}\right|\mu(dx)=\int_{\mathbb{R}}\left|x^k\right|\mu(dx)<\infty. \tag{15.4.89}$$

Thus, for any sequence $u_n\to u$ and $\forall x\in\mathbb{R}$, we have $x^k e^{iu_n x}\to x^k e^{iux}$. Then

$$\left|\widehat{\mu}^{(k)}(u_n)-\widehat{\mu}^{(k)}(u)\right|=\left|\int_{\mathbb{R}^n} x^k\left(e^{iu_n x}-e^{iux}\right)\mu(dx)\right|\to 0 \tag{15.4.90}$$

by bounded convergence theorem (Theorem 15.3.15, $\left|e^{i\langle u_n,x\rangle}-e^{i\langle u,x\rangle}\right|<2$). Thus, $\widehat{\mu}^{(k)}$ is continuous on $\mathbb{R}$. In particular,

$$\widehat{\mu}^{(k)}(0)=\int_{\mathbb{R}} i^k x^k e^{i0x}\mu(dx)=i^k\int_{\mathbb{R}} x^k\mu(dx). \tag{15.4.91}$$

Simiarly, the conclusion holds for all $n\le k$. □

Lemma 15.4.29 (Riemann-Lebesgue lemma)**.** Suppose that μ is a finite Borel measure on $\mathbb{R}$ which has a density f with respect to Lebesgue measure. Show that its Fourier transform

$$\widehat{\mu}(t)=\int_{-\infty}^{\infty} e^{itx}f(x)dx\to 0\ \text{ as } |t|\to\infty. \tag{15.4.92}$$

Proof. For any real numbers a, b one has $\int_a^b e^{itx}dx\to 0$ as $|t|\to\infty$.

$$\int_a^b e^{itx}dx=\int_a^b\cos txdx+i\int_a^b\sin txdx=\frac{\sin tb-\sin ta}{t}+i\frac{\cos ta-\cos tb}{t}\to 0 \tag{15.4.93}$$

as $|t|\to\infty$. Thus, we can have that

$$\widehat{f}(t)\to 0\ \text{ as }\ |t|\to\infty\quad\text{whenever } f \text{ is a stepfunction (see Definition 15.4.11)} \tag{15.4.94}$$

Now given any $f\in\mathcal{L}^1(E,\mathcal{E},Leb)$, and $\varepsilon>0$, we can pick a stepfunction g with $\|f-g\|_1<\varepsilon/2$. Then pick $T\in\mathbb{R}$ such that for all $t:|t|\ge T$, $\widehat{g}(t)<\varepsilon/2$. Hence,

$$\begin{aligned}\left|\int_{-\infty}^{\infty} e^{itx}f(x)dx\right| &\le \left|\int_{-\infty}^{\infty} e^{itx}(f(x)-g(x)+g(x))dx\right|\le\left|\int_{-\infty}^{\infty} e^{itx}(f(x)-g(x))dx\right|+\left|\int_{-\infty}^{\infty} e^{itx}g(x)dx\right|\\ &\le \int_{-\infty}^{\infty}|f(x)-g(x)|\,dx+\left|\int_{-\infty}^{\infty} g(x)dx\right|=\|f-g\|_1+|\widehat{g}(t)|<\varepsilon/2+\varepsilon/2=\varepsilon\end{aligned}$$

as required. □

Proposition 15.4.30. Suppose that μ is a finite Borel measure on $\mathbb{R}$ which has a density f with respect to Lebesgue measure. Suppose f has an integrable and continuous derivative f'. Show that

$$\hat{\mu}(t) = o(t^{-1}), \quad \text{i.e.,} \quad t\hat{\mu}(t) \to 0 \text{ as } |t| \to \infty. \tag{15.4.95}$$

Proof. By Proposition 15.3.28 (integration by parts, note the integrand is continuous). For any N, we have

$$e^{itx} f(x)\Big|_{-N}^{N} = it \int_{-N}^{N} e^{itx} f(x)\, dx + \int_{-N}^{N} e^{itx} f'(x)\, dx \tag{15.4.96}$$

We see that the LHS tends to 0 as $N \to \infty$[16]. Now $\left|e^{itx} f'(x) \mathbb{1}_{[-N,N]}(x)\right| \leq f'(x)$, and f' is integrable (given). Therefore, by dominated convergence theorem,

$$\lim_{N\to\infty} \int_{-N}^{N} e^{itx} f'(x)\, dx = \lim_{N\to\infty} \int_{-\infty}^{\infty} e^{itx} f'(x) \mathbb{1}_{[-N,N]}(x)\, dx = \int_{-\infty}^{\infty} \lim_{N\to\infty} e^{itx} f'(x) \mathbb{1}_{[-N,N]}(x)\, dx = \int_{-\infty}^{\infty} e^{itx} f'(x)\, dx$$

Similarly,

$$it \lim_{N\to\infty} \int_{-N}^{N} e^{itx} f(x)\, dx = it \int_{-\infty}^{\infty} e^{itx} f(x)\, dx.$$

Thus we have

$$\int_{-\infty}^{\infty} e^{itx} f'(x)\, dx = -it \int_{-\infty}^{\infty} e^{itx} f(x)\, dx$$

Now $f' \in \mathcal{L}^1(E, \mathcal{E}, Leb)$, so by the result in Lemma 15.4.29, the LHS tends to 0 as $|t| \to \infty$. Then of course, we have $t\hat{\mu}(t) \to 0$ as $|t| \to \infty$. The extension to higher derivatives is similar. □

15.5 Convergence of Measures

15.5.1 Weak convergence and vague convergence

We have a variety of notions of convergence for measurable functions, including almost everywhere convergence, convergence in $\mathcal{L}^p$, and convergence in measure. All these notions depend on the measurable function themselves. Weak convergence is a notion of convergence for measures.

If $(\mu_n, n \geq 0)$ is a sequence of measures on $(E, \mathcal{E})$, we could say that $\mu_n \to \mu$ if $\mu_n(A) \to \mu(A)$ for all $A \in \mathcal{E}$, but this form of convergence (i.e. pointwise convergence) is very rigid. Instead we use the following definition.

Definition 15.5.1. Let (E, d) be a metric space and endow it with its Borel σ-algebra $\mathcal{B}(E)$. Let μ be a finite measure and $(\mu_n, n \geq 1)$ be a sequence of finite measures defined on $(E, \mathcal{E})$. We say that (μ_n) converges weakly to μ if for every continuous bounded function $f : E \to \mathbb{R}$, $\mu_n(f) \to \mu(f)$ as $n \to \infty$, denoted by $\mu_n \xrightarrow{w} \mu$, i.e.,

$$\int f d\mu_n \to \int f d\mu \quad \text{as } n \to \infty, \quad \mu, \mu_n \in \mathcal{M}_f(E), \quad \forall f \in C_b(E), \tag{15.5.1}$$

Example 15.5.1. (i) $x_n \to x$ in $\mathbb{R}$ if and only if $\delta_{x_n} \xrightarrow{w} \delta_x$. Indeed, the latter is equivalent to requiring that $f(x_n) \to f(x)$ for every continuous bounded function f.

(ii) Let $\mu_n = \frac{1}{n} \sum_{k=0}^{n-1} \delta_{\frac{k}{n}}$ on $[0, 1]$. Then $\mu_n \xrightarrow{w} dx$, Lebesgue measure on $[0, 1]$. Indeed, $\mu_n(f)$ is a Riemann sum of f.

Also, we give vague convergence. Recall the definition of compact support (Definition 2.7.3),

Definition 15.5.2. Let (E, d) be a metric space and endow it with its σ-algebra $\mathcal{B}(E)$. Let μ be a Radon measure and $(\mu_n, n \geq 1)$ be a sequence of Radon measures defined on $(E, \mathcal{E})$. We say that (μ_n) converges vaguely to μ if for every continuous function with compact support, $f : E \to \mathbb{R}$, $\mu_n(f) \to \mu(f)$ as $n \to \infty$, denoted by $\mu_n \xrightarrow{v} \mu$, i.e.,

$$\int f d\mu_n \to \int f d\mu \quad \text{as } n \to \infty, \quad \mu, \mu_n \in \mathcal{M}_R(E), \quad \forall f \in C_c(E), \tag{15.5.2}$$

Theorem 15.5.2 (Portemanteau Theorem)**.** Let Let $(\mu_n, n \geq 1)$ and μ be finite Borel measures on E, i.e., $\mu, \mu_n \in \mathcal{M}_f(E)$. Let U_f be the set of points of discontinuity of f. The following are equivalent:

[16] need details

(i) $\mu_n \xrightarrow{w} \mu$.

(ii) For every $G \subseteq E$ open, $\liminf_n \mu_n(G) \geq \mu(G)$.

(iii) For every $F \subseteq E$ closed, $\limsup_n \mu_n(F) \leq \mu(F)$.

(iv) For every $A \subseteq E$ Borel such that $\mu(\partial A) = 0$, $\lim_n \mu_n(A) = \mu(A)$.

(v) $\int f d\mu_n \to \int f d\mu$ as $n \to \infty$ for all bounded Lipschitz continuous f.

(vi) $\int f d\mu_n \to \int f d\mu$ as $n \to \infty$ for all bounded measurable f with $\mu(U_f) = 0$.

The idea is the mass can be 'won or lost' only through the boundary.[17]

Proof. (i) $\Rightarrow$ (ii): Let G be an open set and introduce the sequence of functions $f_k(x) := 1 \wedge kd(x, G^c)$ (for $x \in E$). For each $k \geq 1$, f_k is continuous and bounded (in fact, uniformly continuous), so $\mu_n(f_k) \to \mu(f_k)$.

As G is open, $x \in G$ if and only if $d(x, G^c) > 0$. Thus $f_k \uparrow \mathbb{1}_G$ pointwise as $k \to \infty$. For every n, $\mu_n(G) = \mu_n(\mathbb{1}_G) \geq \mu_n(f_k)$ by fundamental property of measure (Lemma 15.1.10), so $\liminf_n \mu_n(G) \geq \mu(f_k)$ for all k. By the monotone convergence theorem (Theorem 15.3.5), taking $k \to \infty$ we have $\liminf_n \mu_n(G) \geq \mu(G)$.

(ii) $\Rightarrow$ (iii): Let F be a closed set and thus F^c is open. Then by (ii)

$$\mu(F) = 1 - \mu(F^c) \geq 1 - \liminf_n \mu_n(F^c) = \limsup_n (1 - \mu_n(F^c)) = \limsup_n \mu_n(F). \tag{15.5.3}$$

(ii) + (iii) $\Rightarrow$ (iv): Let A be a Borel set such that $\mu(\partial A) = 0$. Then $\overline{A}$ is closed and $\mathring{A}$ is open

$$\limsup_n \mu_n(A) \quad \leq \quad \limsup_n \mu_n(\bar{A}) \leq \mu(\bar{A}) = \mu(\mathring{A} \cup \partial A) = \mu(\mathring{A}) \leq \liminf_n \mu_n(\mathring{A}) \leq \liminf_n \mu_n(A).$$

It follows that the limit exists and equals to $\mu(A)$.

(iv) $\Rightarrow$ (i): Let $f \in C_b^+(E)$. We must show that $\mu_n(f) \to \mu(f)$ as $n \to \infty$. Write $f \leq K$, so by Proposition 15.3.38

$$\mu(f) = \int_0^\infty \mu(f \geq t)dt = \int_0^K \mu(f \geq t)dt, \qquad \mu_n(f) = \int_0^\infty \mu_n(f \geq t)dt = \int_0^K \mu_n(f \geq t)dt. \qquad (*) \tag{15.5.4}$$

Note that the set $A := \{f \geq t\} = f^{-1}([t, \infty))$ is closed, while the set $\{f > t\}$ is open, so $\partial A = \partial\{f \geq t\} \subseteq \{f = t\}$. The set $B := \{t | \mu(\{f = t\}) > 0\}$ is countable since it is equal to $\bigcup_{n \geq 1} \{t | \mu(\{f = t\}) \geq n^{-1}\mu(E)\}$, and each set in the union is finite since μ is a finite measure (for fixed n, the number of t such that $\mu(f = t) \geq n^{-1}\mu(E)$ is smaller than n). Therefore $\mu(B) = 0$, since the whole set is uncountable. Then $\mu(A) \leq \mu(B) = 0$, so by given condition (iv), $\mu_n(A) \to \mu(A)$ as $n \to \infty$. Thus,

$$\mu_n(f) \underbrace{= \int_0^K \mu_n(f \geq t)dt}_{\text{by } (*)} \qquad \underbrace{\to \int_0^K \mu(f \geq t)dt}_{\text{dominated convergence theorem (Theorem 15.3.12)}} \qquad \underbrace{= \mu(f)}_{\text{by } (*)} \tag{15.5.5}$$

Then check the definition of weak convergence, decompose elements of $C_b(E)$ into positive and negative parts.

(vi) $\Rightarrow$ (i) $\Rightarrow$ (v): It is trivial since all the bounded continuous function satisfies (vi) and all bounded Lipschitz continuous satisfies (i) by Definition 12.0.10.

(v) $\Rightarrow$ (iii): For closed set F and any $\varepsilon > 0$, we can construct a Lipschitz continuous function $\rho_{F,\varepsilon}$ as in Lemma 12.0.10. Thus, use the same argument in Fatou's lemma (Lemma 15.3.11), for $k \geq n$ and non-negative function g, we have

$$\inf_{m \geq n} g_m \leq g_k \quad \Rightarrow \quad \mu\left(\inf_{m \geq n} g_m\right) \leq \mu(g_k) \quad \Rightarrow \quad \mu\left(\inf_{m \geq n} g_m\right) \leq \inf_{k \geq n} \mu(g_k). \qquad (\dagger) \tag{15.5.6}$$

We know that $\mathbb{1}_F \leq \rho_{F,\varepsilon}$, so $\mathbb{1}_F \leq \lim_{\varepsilon \downarrow 0} \rho_{F,\varepsilon} = \inf_{\varepsilon > 0} \rho_{F,\varepsilon}$, which gives $\mu_n(F) \leq \mu_n\left(\inf_{\varepsilon > 0} \rho_{F,\varepsilon}\right) \leq \inf_{\varepsilon > 0} \mu_n(\rho_{F,\varepsilon})$ by (†), then for fixed n, we have

$$\sup_{m \geq n} \left(\inf_{\varepsilon > 0} \mu_m(\rho_{F,\varepsilon})\right) \leq \sup_{m \geq n} (\mu_m(\rho_{F,\varepsilon})) \quad \Rightarrow \quad \sup_{m \geq n} \left(\inf_{\varepsilon > 0} \mu_m(\rho_{F,\varepsilon})\right) \leq \inf_{\varepsilon > 0} \sup_{m \geq n} (\mu_m(\rho_{F,\varepsilon})) \tag{15.5.7}$$

[17] for vague convergence part check Klenke [10].P_{253}

$$\limsup_n \mu_n(F) = \inf_n \sup_{m\geq n} \mu_m(F) \leq \inf_n \sup_{m\geq n} \left(\inf_{\varepsilon>0} \mu_m\left(\rho_{F,\varepsilon}\right)\right) \leq \inf_n \inf_{\varepsilon>0} \sup_{m\geq n} \mu_m\left(\rho_{F,\varepsilon}\right) \leq \inf_{\varepsilon>0} \inf_n \sup_{m\geq n} \mu_m\left(\rho_{F,\varepsilon}\right). \tag{15.5.8}$$

But we know that (v) $\lim_{n\to\infty} \mu_n(f) = \mu(f)$ for all bounded Lipschitz continuous functions f, i.e., the limit of $\mu_n(f)$ exists, and $\lim_{n\to\infty} \mu_n(f) = \limsup_n \mu_n(f) = \inf_n \sup_{m\geq n} \mu_m(f)$. Then with condition (v), we have

$$\limsup_n \mu_n(F) \leq \inf_{\varepsilon>0} \lim_{n\to\infty} \mu_n(\rho_{F,\varepsilon}) = \inf_{\varepsilon>0} \mu(\rho_{F,\varepsilon}) = \lim_{\varepsilon\downarrow 0} \mu(\rho_{F,\varepsilon}) = \mu(F), \tag{15.5.9}$$

by dominited convergence theorem (Theorem 15.3.12) as $\rho_{F,\varepsilon}$ is bounded. □

15.5.2 Tightness

Definition 15.5.3. Let $(\mu_i)_{i\in I}$ be a family of finite measures on (E,d). We say that $(\mu_i)_{i\in I}$ is tight if for all $\varepsilon > 0$ there is $K \subseteq E$ compact such that $\sup_{i\in I} \mu_i(E\backslash K) < \varepsilon$.

Remark. The intuitive idea is that a given collection of measures does not "escape to infinity".

Proposition 15.5.3. If E is a compact space, then every collection of (possibly complex) measures on E is tight.

Proof. [18] □

15.6 Ergodic theory

15.6.1 Measure-preserving transformations

Definition 15.6.1. Let $(E,\mathcal{E},\mu)$ be a measure space. A measurable function $\theta : E \to E$ is called a measure-preserving transformation if

$$\mu(\theta^{-1}(A)) = \mu(A), \quad \text{for all } A \in \mathcal{E}. \tag{15.6.1}$$

A set $A \in \mathcal{E}$ is invariant if $\theta^{-1}(A) = A$. A measurable function $f : E \to \mathbb{R}$ is invariant if $f = f \circ \theta$.

Proposition 15.6.1. Let $(E,\mathcal{E},\mu)$ be a measure space and $\theta : E \to E$ a measure-preserving transformation. Then the class of all invariant sets forms a σ-algebra, which we denote by

$$\mathcal{E}_\theta := \{A \in \mathcal{E} : \theta^{-1}(A) = A\} \tag{15.6.2}$$

Then f is invariant if and only if f is $\mathcal{E}_\theta$-measurable.

Proof. Checking that $\mathcal{E}_\theta$ is a σ-algebra by Definition 15.1.2,

(i) $\emptyset \in \mathcal{E}_\theta$ since $\theta^{-1}(\emptyset) = \emptyset$.

(ii) If $A \in \mathcal{E}_\theta$, by Proposition 2.6.1, $\theta^{-1}(A^c) = \theta^{-1}(E\backslash A) = E\backslash\theta^{-1}(A) = E\backslash A = A^c$. Thus, $A^c \in \mathcal{E}_\theta$.

(iii) If $A_n \in \mathcal{E}_\theta$, by Proposition 2.6.1, $\theta^{-1}\left(\bigcup_n A_n\right) = \bigcup_n \theta^{-1}(A_n) = \bigcup_n A_n$. Thus, $\bigcup_n A_n \in \mathcal{E}_\theta$.

Thus, $\mathcal{E}_\theta$ is a σ-algebra.

Now suppose that f is invariant ($f = f \circ \theta$). Then, for all $B \in \mathcal{B}(\mathbb{R})$, we have

$$f^{-1}(B) = (f\circ\theta)^{-1}(B) = \theta^{-1}\left(f^{-1}(B)\right) \;\Rightarrow\; f^{-1}(B) \in \mathcal{E}_\theta. \tag{15.6.3}$$

Conversely, suppose f is $\mathcal{E}_\theta$-measurable. Then, for all $x \in \mathbb{R}$ ($\{x\} \in \mathcal{B}(\mathbb{R})$), we have $f^{-1}(\{x\}) \in \mathcal{E}_\theta$ (by Definition 15.2.1), i.e.,

$$f^{-1}(\{x\}) = \theta^{-1}\left(f^{-1}(\{x\})\right) = (f\circ\theta)^{-1}(\{x\}) \tag{15.6.4}$$

Thus, $\forall y \in E$, $\exists x \in \mathbb{R}$ such that $f(y) = x$. Then $f^{-1}(\{x\}) \neq \emptyset$, thus we have $y \in f^{-1}(\{x\}) = (f\circ\theta)^{-1}(\{x\})$. So

$$f(y) = x = f\circ\theta(y) \;\Rightarrow\; f \text{ is invariant.} \tag{15.6.5}$$

□

[18] need proof

Here are two simple examples of measure preserving transformations:

Example 15.6.2. (i) Translation map on the torus. Take $E = [0,1)^n$ with Lebesgue measure on its Borel σ-algebra, and consider addition modulo 1 in each coordinate. For $a \in E$ set

$$\theta_a(x_1, \ldots, x_n) = (x_1 + a_1, \ldots, x_n + a_n). \tag{15.6.6}$$

(ii) Bakers' map. Take $E = [0,1)$ with Lebesgue measure. Set

$$\theta(x) = 2x - \lfloor 2x \rfloor . \tag{15.6.7}$$

Proposition 15.6.3. Let $(E, \mathcal{E}, \mu)$ be a measure space. If f is integrable and θ is measure-preserving, then $f \circ \theta$ is integrable and

$$\int_E f d\mu = \int_E f \circ \theta d\mu. \tag{15.6.8}$$

Proof. First assume $f = \mathbb{1}_A$ where $A \in \mathcal{E}$. We have that

$$\mu(f \circ \theta) = \mu\left(\mathbb{1}_A \circ \theta\right) = \mu\left(\mathbb{1}_{\theta^{-1}(A)}\right) = \mu\left(\theta^{-1}(A)\right). \tag{15.6.9}$$

Then by Definition 15.6.1,

$$\mu\left(\theta^{-1}(A)\right) = \mu(A) = \mu\left(\mathbb{1}_A\right) = \mu(f) < \infty \tag{15.6.10}$$

since f is integrable. By lineality, we have $f \circ \theta$ is integrable and $\mu(f) = \mu(f \circ \theta)$ for simple f of the form

$$f = \sum_{k=1}^{m} a_k \mathbb{1}_{A_k}, \quad m \in \mathbb{N},\ a_k \geq 0. \tag{15.6.11}$$

For non-negative measurable function f, let $f_n = 2^{-n} \lfloor 2^n f \rfloor$, $g_n = 2^{-n} \lfloor 2^n f \circ \theta \rfloor$. Thus f_n and g_n are simple and

$$f_n \uparrow f, \quad g_n \uparrow f \circ \theta. \tag{15.6.12}$$

Thus by monotone converge theorem (Theorem 15.3.5), we have

$$\mu(f_n) \uparrow \mu(f), \quad \mu(g_n) \uparrow \mu(f \circ \theta). \tag{15.6.13}$$

But by the previous results for simpe f, $\mu(f_n) = \mu(g_n)$ since they are simple. Thus, $\mu(f \circ \theta) = \mu(f) < \infty$ and $f \circ \theta$ is integrable.

For integrable f, we know that $f = f^+ - f^-$ where f^+ and f^- are non-negative measurable and integrable. Thus,

$$\mu\left(|f \circ \theta|\right) = \mu\left(\left(f^+ + f^-\right) \circ \theta\right) = \mu\left(f^+ \circ \theta\right) + \mu\left(f^- \circ \theta\right) = \mu\left(f^+\right) + \mu\left(f^-\right) = \mu\left(|f|\right) < \infty \tag{15.6.14}$$

by Theorem 15.3.7 and previous results for non-negative measurable f. □

15.6.2 Ergodic measure-preserving transformation

Definition 15.6.2. Let $(E, \mathcal{E}, \mu)$ be a measure space and $\theta : E \to E$ a measure-preserving transformation. We say that θ is ergodic if $\mathcal{E}_\theta$ contains only sets of measure zero and their complements.

Proposition 15.6.4. $(E, \mathcal{E}, \mu)$ is a measure space. If θ is ergodic and f is invariant, then $f = c$ a.e., for some constant c.

Proof. f is $\mathcal{E}_\theta$-measurable since f is invariant (by Proposition 15.6.1). Let

$$c = \sup\{a : \mu(f < a) = 0\} = \sup\{a : \mu(f \geq a) \neq 0\} \qquad (*) \tag{15.6.15}$$

but we must check that the set over which we are taking the supremum on $\mathbb{R}$ or $\emptyset$ does not pose any problems.

First suppose $\{a : \mu(f < a) = 0\} = \mathbb{R}$. Then by Proposition 15.1.8.(ii),

$$\mu(E) = \mu\left(\bigcup_{n \in \mathbb{N}} \{f < n\}\right) \leq \sum_{n \in \mathbb{N}} \mu(f < n) = 0 \tag{15.6.16}$$

So, trivially, we have that for any c, $\mu(f \neq c) \leq \mu(E) = 0$.

Now assume $\{a : \mu(f < a) = 0\} = \emptyset$. This means that $\mu(f < a) > 0$ for all a. Since f is $\mathcal{E}_\theta$ measurable, and $\mathcal{E}_\theta$ contains only null sets and their complements, we must have that $\mu(f \geq a) = 0$ for all a. Then by Proposition 15.1.8.(ii),

$$\mu(E) = \mu\left(\bigcup_{n\in\mathbb{N}} \{f \geq -n\}\right) \leq \sum_{n\in\mathbb{N}} \mu(f \geq -n) = 0$$

which contradicts $\mu(f > a) > 0$.

Thus we can follow through with our initial idea and define s as in $(*)$. Since $\mathcal{E}_\theta$ is ergodic, $\forall n \in \mathbb{N}$ we have that

$$\mu\left(\left\{f \leq c + \frac{1}{n}\right\}\right) \neq 0 \;\Rightarrow\; \mu\left(\left\{f > c + \frac{1}{n}\right\}\right) = 0. \tag{15.6.17}$$

by definition of c. Also, there exists arbitary small $\varepsilon \leq \frac{1}{n}$,

$$\mu\left(f \geq c - \frac{1}{n}\right) \geq \mu\left(f \geq c - \varepsilon\right) \neq 0 \;\Rightarrow\; \mu\left(f < c - \frac{1}{n}\right) = 0 \tag{15.6.18}$$

Then

$$\mu\left(\{f \neq c\}\right) = \mu\left(\bigcup_{n\in\mathbb{N}} \left\{f < c - \tfrac{1}{n}\right\} \cup \left\{f > c + \tfrac{1}{n}\right\}\right) \leq \sum_{n\in\mathbb{N}} \left(\mu\left(\left\{f < c - \tfrac{1}{n}\right\}\right) + \mu\left(\left\{f > c + \tfrac{1}{n}\right\}\right)\right) = 0 \tag{15.6.19}$$

by Proposition 15.1.8.(i),(ii). □

15.6.3 Birkhoff's and von Neumann's ergodic theorems

Throughout this section, $(E, \mathcal{E}, \mu)$ will denote a measure space, on which is given a measure-preserving transformation θ. Given an measurable function f, set $S_0 = 0$ and define, for $n \geq 1$,

$$S_n = S_n(f) = f + f \circ \theta + \cdots + f \circ \theta^{n-1}. \tag{15.6.20}$$

Lemma 15.6.5 (maximal ergodic lemma)**.** Let $\theta : E \to E$ be a measure-preserving transformation (Note that θ does not need to be ergodic). Let f be an integrable function on E. Set $S^* = \sup_{n\geq 0} S_n(f)$. Then

$$\int_{\{S^*>0\}} f d\mu \geq 0. \tag{15.6.21}$$

Proof. Set $S_n^* = \max_{0\leq m\leq n} S_m$ and $A_n = \{S_n^* > 0\}$. Note that $S_n^* \geq 0$. Then, for $m = 1, \ldots, n$,

$$S_m = f + S_{m-1} \circ \theta \leq f + S_n^* \circ \theta. \tag{15.6.22}$$

On A_n, we have $S_n^* = \max_{1\leq m\leq n} S_m$, so

$$S_n^* \leq f + S_n^* \circ \theta. \tag{15.6.23}$$

On A_n^c, we have

$$S_n^* = 0 \leq S_n^* \circ \theta. \tag{15.6.24}$$

So, integrating and adding (by Theorem 15.3.7 since both sides are non-negative), we obtain

$$\int_E S_n^* d\mu \leq \int_{A_n} f d\mu + \int_E S_n^* \circ \theta d\mu. \tag{15.6.25}$$

But S_n^* is integrable (since $S_m,\ m = 1, \ldots n$ are integrable by Proposition 15.6.3), so

$$\int_E S_n^* \circ \theta d\mu = \int_E S_n^* d\mu < \infty \quad \Rightarrow \quad \int_{A_n} f d\mu \geq 0. \tag{15.6.26}$$

As $n \to \infty$, $A_n \uparrow \{S^* > 0\}$ so, by dominated convergence, with dominating function $|f|$,

$$\int_{\{S^*>0\}} f d\mu = \lim_{n\to\infty} \int_{A_n} f d\mu \geq 0. \tag{15.6.27}$$

□

Theorem 15.6.6 (Birkhoff's almost everywhere ergodic theorem)**.** Assume that $(E, \mathcal{E}, \mu)$ is σ-finite and that f is an integrable function on E. Let $\theta : E \to E$ be a measure-preserving transformation (Note that θ does not need to be ergodic). Then there exists an invariant function $\overline{f}$, with $\mu(|\overline{f}|) \leq \mu(|f|)$, such that $S_n(f)/n \to \overline{f}$ a.e. as $n \to \infty$.

Proof. We know that

$$S_n \circ \theta = S_{n+1} - f \;\Rightarrow\; \frac{S_n}{n} \circ \theta = \frac{S_{n+1}}{n+1}\frac{n+1}{n} - \frac{f}{n}. \tag{15.6.28}$$

Taking lim inf on both sides, we have

$$\left(\liminf_n \frac{S_n}{n}\right) \circ \theta = \liminf_n \frac{S_{n+1}}{n+1}\frac{n+1}{n} - 0 = \liminf_n \frac{S_n}{n}. \tag{15.6.29}$$

Thus, the functions $\liminf_n(S_n/n)$ is invariant. Similarly, $\limsup_n(S_n/n)$ is also invariant.

Therefore, for $a < b$, so is the following set

$$D = D(a,b) = (a,b), \qquad \liminf_n(S_n/n) < a < b < \limsup_n(S_n/n). \tag{15.6.30}$$

We shall show that $\mu(D) = 0$.

First, f is integrable on E, thus f is integrable on D since $\mu(|f|\,\mathbb{1}_D) \leq \mu(|f|) < \infty$.

Thus, we make the following argument on D. Note that either $b > 0$ or $a < 0$. We can interchange the two cases by replacing f by $-f$. Let us assume then that $b > 0$.

Let $B \in \mathcal{E}$ with $\mu(B) < \infty$, then $g = f - b\mathbb{1}_B$ is integrable (since $\mathbb{1}_B$ is integrable) and, for each $x \in D$, for some n,

$$S_n(g)(x) = S_n(f - b\mathbb{1}_B)(x) = S_n(f)(x) - bS(\mathbb{1}_B)(x) \geq S_n(f)(x) - nb. \tag{15.6.31}$$

Hence $S^*(g) \geq \limsup_n S_n(f) - nb > 0$ everywhere in D and, by the maximal ergodic lemma (Lemma 15.6.5),

$$0 \leq \int_D (f - b\mathbb{1}_B) d\mu = \int_D f d\mu - b\mu(B). \tag{15.6.32}$$

Since μ is σ-finite (see Definition 15.1.17), there is a sequence of sets $B_n \in \mathcal{E}$, with $\mu(B_n) < \infty$ for all n and $B_n \uparrow D$. Hence, by fundamental property of measure (Lemma 15.1.10),

$$b\mu(D) = \lim_{n\to\infty} b\mu(B_n) \leq \int_D f d\mu < \infty \tag{15.6.33}$$

since f is integrable on D. In particular, we see that $\mu(D) < \infty$.

Similarly, $h = a\mathbb{1}_B - f$ is also integrable for each $x \in D$, for some n. Let $B = D$, then

$$S_n(h)(x) = S_n(a\mathbb{1}_B - f)(x) = an\mathbb{1}_D - S_n(f)(x) = an - S_n(f)(x). \tag{15.6.34}$$

Hence $S^*(h) \geq an - \liminf_n S_n(f) > 0$ everywhere in D, and by the maximal ergodic lemma (Lemma 15.6.5),

$$\int_D (a - f) d\mu \geq 0 \;\Rightarrow\; a\mu(D) \geq \int_D f d\mu \quad\Rightarrow\quad b\mu(D) \leq \int_D f d\mu \leq a\mu(D). \tag{15.6.35}$$

by Theorem 15.3.10.(i). Since $a < b$ and the integral is finite, this forces $\mu(D) = 0$. Set

$$\Delta = \left\{\liminf_n(S_n/n) < \limsup_n(S_n/n)\right\} \tag{15.6.36}$$

then Δ is invariant (by Proposition 15.2.5 since $\liminf_n(S_n/n)$ and $\limsup_n(S_n/n)$ are invariant ($\mathcal{E}_\theta$-measurable)). Also,

$$\Delta = \bigcup_{a,b\in\mathbb{Q},a<b} D(a,b), \tag{15.6.37}$$

so by Proposition 15.1.8.(ii),

$$\mu(\Delta) = \mu\left(\bigcup_{a,b\in\mathbb{Q},a<b} D(a,b)\right) \leq \sum_{a,b\in\mathbb{Q},a<b} \mu(D(a,b)) = 0. \tag{15.6.38}$$

On the complement of Δ, S_n/n converges in $[-\infty,\infty]$, so we can define an invariant function $\overline{f}$ by

$$\overline{f} = \begin{cases} \lim_n(S_n/n) & \text{on } \Delta^c, \\ 0 & \text{on } \Delta. \end{cases} \qquad \text{i.e. } \overline{f} = \lim_n(S_n/n)\mathbb{1}_{\Delta^c} \tag{15.6.39}$$

Finally, $\mu(|f\circ\theta^n|) = \mu(|f|)$ by Proposition 15.6.3 since f is integrable on E, so

$$\mu(|S_n|) \leq \mu(|f|) + \mu(|f\circ\theta|) + \cdots + \mu(\left|f\circ\theta^{n-1}\right|) = n\mu(|f|) \tag{15.6.40}$$

for all n. Since $\overline{f} = \lim\lim_n(S_n/n)$ on Δ^c, we have $\left|\overline{f}\right| = \lim\lim_n|S_n/n|$ on Δ^c. Hence, by Fatou's lemma (Lemma 15.3.11),

$$\mu(|\overline{f}|) = \mu\left(\lim_n|S_n/n|\right) = \mu\left(\liminf_n|S_n/n|\right) \leq \liminf_n \mu(|S_n/n|) \leq \mu(|f|). \tag{15.6.41}$$

□

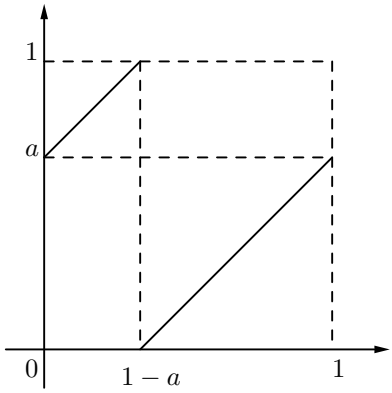
Example 15.6.7. For $E=[0,1)$, $a\in E$ and $\mu(dx)=dx$, define

$$\theta(x) = x + a \pmod 1. \tag{15.6.42}$$

It is measure-preserving and θ is not guaranteed to be ergodic for all $a\in[0,1)$.

First we have

$$\theta(x) = \begin{cases} x+a & x\in[0,1-a) \\ x+a-1 & x\in[1-a,1) \end{cases}$$



Thus, $\forall b<c\in[0,1)$ and $A=(b,c)$, then $\mu\left(\theta^{-1}(A)\right) = \mu\left((b,c)\right)$. So $\mu\circ\theta^{-1}=\mu$ on intervals of the form (b,c), which form a π-system generating $\mathcal{B}([0,1))$. Then by uniqueness of extension theorem (Theorem 15.1.18, $\mu(E)=1<\infty$ since μ is Lebesgue measure and $E=[0,1)$), $\mu\circ\theta^{-1}=\mu$ on $\mathcal{B}([0,1))$. Thus, θ is measure-preserving.

First we show that θ is not ergodic when a is rational. Indeed, suppose $a=p/q$, with $p,q\in\mathbb{N}$ and p,q coprime. Then set

$$A := \bigcup_{k=0}^{q-1}\left[\frac{k}{q}, \frac{k}{q}+\frac{1}{2q}\right) = \left[0,\frac{1}{2q}\right) \cup \left[\frac{2}{2q},\frac{3}{2q}\right) \cup \cdots \cup \left[\frac{2q-2}{2q},\frac{2q-1}{2q}\right) \tag{15.6.43}$$

It is easy to see that $\mu(A)=\frac{1}{2}$, but A is invariant. So θ is not ergodic. Also, as θ^q is the identity ($\theta^q(x)=x+p\pmod 1 = x$), we have

$$\begin{aligned} \frac{S_n(f)}{n} &= \frac{1}{n}(f + f\circ\theta + \cdots + f\circ\theta^{n-1}) \\ &= \frac{\left\lfloor\frac{n}{q}\right\rfloor}{n}(f + f\circ\theta + \cdots + f\circ\theta^{q-1}) + \frac{1}{n}(f + f\circ\theta + \cdots + f\circ\theta^{n-q\left\lfloor\frac{n}{q}\right\rfloor-1}) \end{aligned}$$

so by Birkhoff's theorem (Theorem 15.6.6),

$$\overline{f} \overset{\text{a.e.}}{=} \lim_{n\to\infty} \frac{S_n(f)}{n} \overset{\text{a.e.}}{=} \frac{1}{q}(f + f\circ\theta + \cdots + f\circ\theta^{q-1}). \tag{15.6.44}$$

since $f + f\circ\theta + \cdots + f\circ\theta^{q-1}$ is finite a.e.. Equivalently,

$$\overline{f} = \frac{1}{q}\sum_{k=0}^{q-1} f\left(\left(x + k\frac{p}{q}\right) \pmod 1\right) \quad \text{a.e..} \tag{15.6.45}$$

Now suppose $a \in [0,1)\backslash\mathbb{Q}$ and f is invariant. Then the Fourier coefficients of f will be

$$\begin{aligned} a_n &= \int_0^1 f(x)e^{-i2\pi nx}dx = \int_0^1 f\left((x+a) \pmod 1\right) e^{-i2\pi n((x+a)\,(\bmod\ 1))}dx \\ &= \int_0^1 f(x)e^{-i2\pi n((x+a)\,(\bmod\ 1))}dx = \int_0^1 f(x)e^{-i2\pi nx}e^{-i2\pi na} = a_n e^{-i2\pi na}. \end{aligned}$$

Thus, $a_n = 0$, $\forall n \neq 0$ (since $a \notin \mathbb{Q}$). So f is a constant. If there exists $A \in \mathcal{E}_\theta$ such that $\mu(A) \in (0,1)$, then the function $\mathbb{1}_A$ must be $\mathcal{E}_\theta$-measurable (Proposition 15.2.5) and thus invariant (Proposition 15.6.4). However, $\mathbb{1}_A$ is not constant. Contradiction. Thus, all the sets in $\mathcal{E}_\theta$ are of measure 0 or 1. That is, θ is ergodic for irrational a.

Thus, for an integrable function f, by Birkhoff's almost everywhere ergodic theorem (Theorem 15.6.6), there exists an integrable, invariant function $\overline{f}$, such that, for some constant c (since $\overline{f}$ is invariant),

$$c = \overline{f} = \lim_{n\to\infty} \frac{S_n(f)}{n} = \frac{1}{n}(f + f\circ\theta + \cdots + f\circ\theta^{n-1}) \quad \text{a.e..} \tag{15.6.46}$$

Thus, since f is integrable, by Proposition 15.6.3, $f\circ\theta^n$ is integrable for all n,

$$\int_E f\circ\theta^n(x)dx = \int_E f(x)dx \;\Rightarrow\; \int \frac{S_n(f)}{n}(x) = \int_E f(x)dx \tag{15.6.47}$$

Then by Dominated convergence theorem (Theorem 19.3.8),

$$c = \int_E c dx = \lim_{n\to\infty}\int_E \frac{S_n(f)}{n}(x)dx = \int_E f(x)dx = \int_0^1 f(x)dx. \tag{15.6.48}$$

Thus, $\overline{f} = \int_0^1 f(x)dx$.

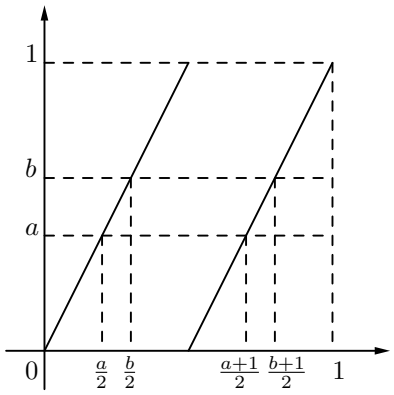
Example 15.6.8. For $E = [0,1)$ and $\mu(dx) = dx$, define Bakers' map,

$$\theta(x) = 2x - \lfloor 2x \rfloor = 2x \pmod 1. \tag{15.6.49}$$

It is a measure-preserving transformation of Lebesgue measure on $[0,1)$, and that θ is ergodic.

First we have

$$\theta(x) = \begin{cases} 2x & x \in [0, \frac{1}{2}) \\ 2x-1 & x \in [\frac{1}{2}, 1) \end{cases}$$



Thus, $\forall a < b \in [0,1)$ and $A = (a,b)$, then $\theta^{-1}(A) = \left(\frac{a}{2}, \frac{b}{2}\right) \cup \left(\frac{a+1}{2}, \frac{b+1}{2}\right)$. Then

$$\begin{aligned} \mu\left(\theta^{-1}(A)\right) &= \mu\left(\theta^{-1}(a,b)\right) = \mu\left(\left(\frac{a}{2}, \frac{b}{2}\right)\right) + \mu\left(\left(\frac{a+1}{2}, \frac{b+1}{2}\right)\right) \\ &= \frac{b-a}{2} + \frac{b+1}{2} - \frac{a+1}{2} = b - a = \mu\left((a,b)\right). \end{aligned}$$

Thus, $\mu \circ \theta^{-1} = \mu$ on intervals of the form (a,b), which form a π-system generating $\mathcal{B}([0,1))$. Then by uniqueness of extension theorem (Theorem 15.1.18, $\mu(E) = 1 < \infty$ since μ is Lebesgue measure and $E = [0,1)$), $\mu \circ \theta^{-1} = \mu$ on $\mathcal{B}([0,1))$. Thus, θ is measure-preserving.

Now to each $x \in [0,1)$, we may assign a unique binary representation $x = 0.x_1x_2x_3\ldots$, provided we do not allow an infinite string of 1's. Then we see that $\theta(x) = 0.x_2x_3\ldots$. Define random variables $X_n(x) = x_n$ (the probability triple is $([0,1), \mathcal{B}([0,1)), \mu)$). Then the X_n are the Rademacher functions, and are i.i.d. Bin$(1, \frac{1}{2})$. Now

$$\theta^{-n}(\{X_1 = \varepsilon_1, \ldots, X_k = \varepsilon_k\}) = \{X_{n+1} = \varepsilon_1, \ldots X_{n+k} = \varepsilon_k\} \in \mathcal{T}_n$$

where $\mathcal{T}_n = \sigma(X_k : k \geq n+1)$. Since $\mathcal{B}([0,1)) = \sigma(X_n : n \in \mathbb{N})$ (check this), we have that $\theta^{-n}(B) \in \mathcal{T}_n$ for all $B \in \mathcal{B}([0,1))$. Now if A is invariant then $A \in \mathcal{E}_\theta$ and thus $\theta^{-n}(A) = A$ for all n. Thus

$$\mathcal{E}_\theta \subset \bigcap_n \mathcal{T}_n =: \mathcal{T}_\infty$$

Since $\mathcal{T}_\infty$ is the tail σ-algebra, by Kolmogorov's 0-1 Law (Theorem 19.2.12), $\mathcal{E}_\theta$ can contain only events of measure 1 or 0, so θ is ergodic.

For an integrable function f, by Birkhoff's almost everywhere ergodic theorem (Theorem 15.6.6), there exists an integrable, invariant function $\overline{f}$, such that,

$$\overline{f} = \lim_{n\to\infty} \frac{1}{n}(f + f \circ \theta + \cdots + f \circ \theta^{n-1}) \text{ a.e..} \tag{15.6.50}$$

As θ is ergodic, $\overline{f}$ is invariant, then $\overline{f}$ is a constant c almost everywhere (Proposition 15.6.4), so

$$c = \overline{f} = \lim_{n\to\infty} \frac{S_n(f)}{n}(x) \text{ a.e..} \tag{15.6.51}$$

Thus, since f is integrable, by Proposition 15.6.3, $f \circ \theta^n$ is integrable for all n,

$$\int_E f \circ \theta^n(x)dx = \int_E f(x)dx \;\Rightarrow\; \int \frac{S_n(f)}{n}(x) = \int_E f(x)dx \tag{15.6.52}$$

Then by Dominated convergence theorem (Theorem 19.3.8),

$$c = \int_E c dx = \lim_{n\to\infty} \int_E \frac{S_n(f)}{n}(x)dx = \int_E f(x)dx = \int_0^1 f(x)dx. \tag{15.6.53}$$

Thus, $\overline{f} = \int_0^1 f(x)dx$ a.e..

Theorem 15.6.9 (von Neumann's $\mathcal{L}^p$ ergodic theorem)**.** Assume that $\mu(E) < \infty$. Let $p \in [1,\infty)$. Let $\theta : E \to E$ be a measure-preserving transformation (Note that θ does not need to be ergodic). Then, for all $f \in \mathcal{L}^p(E, \mathcal{E}, \mu)$, $S_n(f)/n \to \overline{f}$ in $\mathcal{L}^p(E, \mathcal{E}, \mu)$.

Proof. We have (by Proposition 15.6.3),

$$\|f \circ \theta^n\|_p = \left(\int_E |f|^p \circ \theta^n d\mu\right)^{1/p} = \left(\int_E |f|^p d\mu\right)^{1/p} = \|f\|_p. \tag{15.6.54}$$

So, by Minkowski's inequality (Theorem 15.4.8),

$$\|S_n(f)\|_p \leq \|f\|_p + \cdots + \left\|f \circ \theta^{n-1}\right\|_p = n\|f\|_p \;\Rightarrow\; \|S_n(f)/n\|_p \leq \|f\|_p. \tag{15.6.55}$$

Given $\varepsilon > 0$, choose $K < \infty$ so that $\|f - g\|_p < \varepsilon/3$, where $g = (-K) \vee f \wedge K$. Note that $g \in \mathcal{L}^p(E, \mathcal{E}, \mu)$.

By Birkhoff's theorem (Theorem 15.6.6), $S_n(g)/n \to \overline{g}$ a.e.. We have $|S_n(g)/n| \le K$ for all n so, by bounded convergence theorem (Theorem 15.4.24), $S_n(g)/n, \overline{g} \in \mathcal{L}^p(E, \mathcal{E}, \mu)$ and there exists N such that, for $n \ge N$,

$$\|S_n(g)/n - \overline{g}\|_p < \varepsilon/3. \tag{15.6.56}$$

Since $(f - g \in \mathcal{L}^p(E, \mathcal{E}, \mu)$ and by Proposition 15.6.3), $\mu(|(f-g)\circ\theta^n|^p) = \mu(|f-g|^p)$ for all n. Then by Minkowski's inequality (Theorem 15.4.8),

$$\begin{aligned}
\mu(|S_n(f-g)|^p)^{1/p} = \|S_n(f-g)\|_p &\le \|f-g\|_p + \|(f-g)\circ\theta\| + \ldots \left\|(f-g)\circ\theta^{n-1}\right\|_p \\
&= \mu(|f-g|^p)^{1/p} + \mu(|(f-g)\circ\theta|^p)^{1/p} + \cdots + \mu(\left|(f-g)\circ\theta^{n-1}\right|^p)^{1/p} \\
&= n\mu(|f-g|^p)^{1/p} = n\|f-g\|_p .
\end{aligned}$$

Thus, we have

$$\mu(|S_n(f-g)/n|^p) \le \mu(|f-g|^p) = \|f-g\|_p^p . \tag{15.6.57}$$

By Birkhoff's theorem (Theorem 15.6.6), $\overline{f} = \lim_n (S_n(f)/n)$ a.e. then $\left|\overline{f}\right| = \lim_n |S_n(f)/n|$ a.e.. Similary, we have

$$\overline{f} - \overline{g} = \lim_n (S_n(f-g)/n) \text{ a.e.} \quad \Rightarrow \quad \left|\overline{f} - \overline{g}\right| = \lim_n |S_n(f-g)/n| \text{ a.e. .} \tag{15.6.58}$$

By Fatou's lemma (Lemma 15.3.11),

$$\left\|\overline{f} - \overline{g}\right\|_p^p = \mu\left(\lim_n |S_n(f-g)/n|^p\right) = \mu\left(\liminf_n |S_n(f-g)/n|^p\right) \le \liminf_n \mu(|S_n(f-g)/n|^p) \le \|f-g\|_p^p \tag{15.6.59}$$

Hence, for $n \ge N$, by Minkowski's inequality (Theorem 15.4.8),

$$\begin{aligned}
\left\|S_n(f)/n - \overline{f}\right\|_p &\le \|S_n(f-g)/n\|_p + \|S_n(g)/n - \overline{g}\|_p + \left\|\overline{g} - \overline{f}\right\|_p \\
&\le \|S_n(f-g)/n\|_p + \|S_n(g)/n - \overline{g}\|_p + \|g-f\|_p \\
&< \varepsilon/3 + \varepsilon/3 + \varepsilon/3 = \varepsilon.
\end{aligned}$$

□

15.7 Signed Measure

15.8 Problems

Part IV

Dynamics

Chapter 16

Differential Equations

16.1 Some literature reviews

There is a striking difference between ordinary differential equations and partial differential equations. A classical result of Peano states that the ordinary differential equation $dy/dx = f(x, y)$ has a solution under a single condition of the continuity of the function f. This result has also been extended to equations of higher order or to systems of equations. However, for partial differential equations, the situation is entirely different (see [17].P_{182}).

16.2 Modified Bessel functions

16.2.1 Definition

Definition 16.2.1. The solutions of

$$z^2\frac{d^2w}{dz^2} + z\frac{dw}{dz} - (z^2+\nu^2)w = 0 \tag{16.2.1}$$

are $I_{\pm\nu}(z)$ and $K_\nu(z)$.

Proposition 16.2.1.

$$I_\nu(z) = \left(\frac{1}{2}z\right)^\nu \sum_{k=0}^{\infty} \frac{\left(\frac{1}{4}z^2\right)^k}{k!\Gamma(\nu+k+1)}. \tag{16.2.2}$$

Proposition 16.2.2.

$$K_\nu(z) = \frac{1}{2}\pi\frac{I_{-\nu}(z) - I_\nu(z)}{\sin(\nu\pi)}. \tag{16.2.3}$$

Remark. By this proposition, we have that $K_\nu(z) = K_{-\nu}(z)$.

16.2.2 General case ν

Proposition 16.2.3. When ν is fixed and $z \to 0$,

$$I_\nu(z) \sim \left(\frac{1}{2}z\right)^\nu \Big/ \Gamma(\nu+1), \qquad \nu \neq -1, -2, \ldots. \tag{16.2.4}$$

Proposition 16.2.4.

$$I_{\nu-1}(z) - I_{\nu+1}(z) = \frac{2\nu}{z}I_\nu(z). \tag{16.2.5}$$

Proposition 16.2.5. When ν is fixed and $z \to 0$,

$$K_0(z) \sim -\ln z, \qquad K_\nu(z) \sim \frac{1}{2}\Gamma(\nu)\left(\frac{1}{2}z\right)^{-\nu}, \quad \Re\nu > 0. \tag{16.2.6}$$

Proposition 16.2.6.

$$K_\nu(z) = \frac{\sqrt{\pi}\left(\frac{1}{2}z\right)^\nu}{\Gamma(\nu+1/2)}\int_0^\infty e^{-z\cosh t}\sinh^{2\nu}t\,dt = \frac{\sqrt{\pi}\left(\frac{1}{2}z\right)^\nu}{\Gamma(\nu+1/2)}\int_1^\infty e^{-zt}(t^2-1)^{\nu-\frac{1}{2}}dt, \qquad \Re\nu > -\frac{1}{2},\ x > 0,\ |\arg z| < \frac{1}{2}\pi.$$

Proposition 16.2.7.

$$K_\nu(z) = \int_0^\infty e^{-z\cosh t}\cosh(\nu t)dt, \qquad |\arg z| < \frac{1}{2}\pi. \tag{16.2.7}$$

Proposition 16.2.8.

$$K_\nu(xz) = \frac{\Gamma(\nu+1/2)(2z)^\nu}{\sqrt{\pi}x^\nu}\int_0^\infty \frac{\cos(xt)dt}{(t^2+z^2)^{\nu+\frac{1}{2}}}, \qquad \Re\nu > -\frac{1}{2},\ x>0,\ |\arg z| < \frac{1}{2}\pi. \tag{16.2.8}$$

Proposition 16.2.9.

$$e^{(\nu-1)\pi i}K_{\nu-1}(z) - e^{(\nu+1)\pi i}K_{\nu+1}(z) = \frac{2\nu}{z}e^{\nu\pi i}K_\nu(z). \tag{16.2.9}$$

16.2.3 Special case ν

Proposition 16.2.10.

$$\sqrt{\frac{1}{2}\pi/z}\,I_{1/2}(z) = \frac{\sinh z}{z}, \qquad \sqrt{\frac{1}{2}\pi/z}\,I_{3/2}(z) = -\frac{\sinh z}{z^2} + \frac{\cosh z}{z}, \qquad \sqrt{\frac{1}{2}\pi/z}\,I_{5/2}(z) = \left(\frac{3}{z^3}+\frac{1}{z}\right)\sinh z - \frac{3}{z^2}\cosh z,$$
$$\sqrt{\frac{1}{2}\pi/z}\,I_{-1/2}(z) = \frac{\cosh z}{z}, \qquad \sqrt{\frac{1}{2}\pi/z}\,I_{-3/2}(z) = \frac{\sinh z}{z} - \frac{\cosh z}{z^2}, \qquad \sqrt{\frac{1}{2}\pi/z}\,I_{-5/2}(z) = -\frac{3}{z^2}\sinh z + \left(\frac{3}{z^3}+\frac{1}{z}\right)\cosh z.$$

This is from [2].P_{443}.

Proposition 16.2.11.

$$K_{1/2}(z) = K_{-1/2}(z) = \sqrt{\frac{1}{2}\pi z}\frac{e^{-z}}{z}, \qquad K_{3/2}(z) = K_{-3/2}(z) = \sqrt{\frac{1}{2}\pi z}\left(\frac{1}{z}+\frac{1}{z^2}\right)e^{-z}, \tag{16.2.10}$$

$$K_{5/2}(z) = K_{-5/2}(z) = \sqrt{\frac{1}{2}\pi z}\left(\frac{1}{z}-\frac{3}{z^2}+\frac{3}{z^3}\right)e^{-z}. \tag{16.2.11}$$

Part V

Geometry

Chapter 17

Geometry

Chapter 18

Differential Geometry

18.1

Part VI

Probability

Chapter 19

Probability

19.1 Basic Concepts

19.1.1 Sample spaces, events and probability

Definition 19.1.1. We will deal with a experiment which has a "random" outcome, the possible outcomes being, say, $\omega_1, \omega_2, \ldots$. The set of all possible outcomes $\Omega = \{\omega_1, \omega_2, \ldots\}$ is the sample space of the experiment. A particular point $\omega \in \Omega$ is an observation.

Example 19.1.1. We have the following experiments

(i) Tossing a normal six-faced die, $\Omega = \{1, 2, \ldots, 6\}$.

(ii) Picking a card from a standard pack, Ω is the pack of 52 cards.

(iii) Administer a drug to 20 patients. For simplicity assume there are only two possible outcomes for each patient, R if the patient recovers, D otherwise. Then

$$\Omega = \{(i_1, \ldots, i_{20}) : i_j = R \text{ or } D\} \tag{19.1.1}$$

where i_j is R or D according as patient j recovers or not, so has 2^{20} points.

(iv) Pick a point from the unit interval, $[0, 1]$, then $\Omega = [0, 1]$.

All but (iv) are examples of discrete sample spaces.

Definition 19.1.2 (event)**.** A subset A of Ω, $A \subset \Omega$ is called an event. If the experiment is performed with outcome ω and $\omega \in A$, the event A is said to occur.

Remark. In Example 19.1.1 (i), A might be the event that "the outcome is even", so that $A = \{2, 4, 6\}$, in which case A occurs if one of 2,4,6 is shown on the die.

Example 19.1.2. Let A, B, C be three events. we express the following in symbols:

(i) only A occurs, $A \cap (B \cup C)^c = A \cap B^c \cap C^c$.

(ii) all three events occur, $A \cap B \cap C$.

(iii) at least one event occurs, $A \cup B \cup C$.

(iv) one and only one event occurs, $(A \cap (B \cup C)^c) \cup (B \cap (A \cup C)^c) \cup (C \cap (A \cup B)^c)$.

(v) no event occurs, $(A \cup B \cup C)^c = A^c \cap B^c \cap C^c$.

(vi) not more than two events occurs, $(A \cap B \cap C)^c = A^c \cup B^c \cup C^c$.

Definition 19.1.3. Let $(E, \mathcal{E}, \mu)$ be a measure space (Definition 15.1.15). If $\mu(E) = 1$, the measure space is a probability space. Usually the probability space is denoted as $(\Omega, \mathcal{F}, \mathbb{P})$, wihch has the following interpretation:

- Ω is the sample space, the set of possible outcomes,
- $\mathcal{F}$ is the set of observable sets of outcomes, or events A_i,
- $\mathbb{P}(A)$ is the probability of the event $A \in \mathcal{F}$ ($A \subseteq \Omega$).

In addition, we say that an event $A \in \mathcal{F}$ occurs almost surely (often abbreviated a.s.) if $\mathbb{P}(A) = 1$.

Definition 19.1.4. Furthermore, certain set-theoretic notions have special interpretations in probability.

- The complement in Ω of the event A, A^c is the event "not A", and occurs if and only if A does not occur.
- The union $A \cup B$ of two events A and B is the event "at least one of A or B occurs".
- The intersection $A \cap B$ is the event "both A and B occur".
- The inclusion relation $A \subseteq B$ means "the occurrence of A implies the occurrence of B".
- Events A and B are said to be mutually exclusive if they are disjoint, $A \cap B = \emptyset$, and so both cannot occur together.

Example 19.1.3 (Classical probability)**.** Classical probability was concerned with modelling situations where there are just a finite number of possible outcomes of the experiment and each of these outcomes is "equally likely". For example, tossing a fair coin or an unloaded die, or picking a card from a standard well-shued pack. Here Ω is a finite set with N points, say, $\Omega = \{\omega_1, \dots, \omega_N\}$, and attached to each event $A \subseteq \Omega$ is a measure of how "likely" the event A is to occur.

Here we take $\mathbb{P}(A)$, the probability of the event A to be

$$\mathbb{P}(A) = \frac{N_A}{N} = \frac{\text{number of points in } A}{\text{number of points in } \Omega} \tag{19.1.2}$$

where N_A is the number of points in A. Thus the probability $\mathbb{P}(\cdot)$ is just a real-valued function defined on subsets A of Ω.

Example 19.1.4. Consider $\Omega = [0, 2\pi)$, $\mathcal{F}$ the Borel σ-algebra, and $\mathbb{P}(A) = \mu(A)/2\pi$ where μ is the Lebesgue measure. Then $(\Omega, \mathcal{F}, \mathbb{P})$ may serve as a probability space for choosing a point uniformly at random on the unit circle. e.g., if $A = [0, 2\pi)\backslash\mathbb{Q}$ then $\mathbb{P}(A) = 1$ so almost surely, the angle of the point is irrational.

Example 19.1.5. Infinite coin-tossing. Let

$$\Omega = \{0, 1\}^{\mathbb{N}} = \{\omega = (\omega_1, \dots) \text{ with } \omega_n \in \{0, 1\} \text{ for all } n \geq 1\}. \tag{19.1.3}$$

We interpret the event $\{\omega_n = 1\}$ as the event that the nth toss results in a heads. We take for the σ-algebra $\mathcal{F}$ the σ-algebra generated by events of the form

$$A = \{\omega_1 = \varepsilon_1, \dots, \omega_n = \varepsilon_n\} \tag{19.1.4}$$

for any fixed sequence $(\varepsilon_1, \dots) \in \{0, 1\}^{\mathbb{N}}$. We will soon define a probability measure $\mathbb{P}$ on $(\Omega, \mathcal{F})$ under which the outcomes of the tosses are independent.

Recall Definitions 15.1.10, 15.1.11, 15.1.12, 15.1.13, 15.1.15, 19.1.3 and Proposition 15.1.8 we have the following properites:

Proposition 19.1.6. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a measure space, $\forall A, B \in \mathcal{F}$,

(i) $\mathbb{P}(\emptyset) = 0$, $\mathbb{P}(\Omega) = 1$.

(ii) $0 \leq \mathbb{P}(A) \leq 1$, $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$.

(iii) If $A \cap B = \emptyset$, then $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$. If $A_n \in \mathcal{F}$, $n \in \mathbb{N}$ are disjoint, $\mathbb{P}\left(\bigcup_n A_n\right) = \sum_n \mathbb{P}(A_n)$.

(iv) If $A \subseteq B$ then $\mathbb{P}(A) \leq \mathbb{P}(B)$.

(v) $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B) \leq \mathbb{P}(A) + \mathbb{P}(B)$.

(vi) (inclusion-exclusion formula.) $\forall A_n \in \mathcal{F}$, $n \in \mathbb{N}$,

$$\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n \mathbb{P}(A_i) - \sum_{1 \leq i_1 < i_2 \leq n} \mathbb{P}(A_{i_1} \cap A_{i_2}) + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \mathbb{P}(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \cdots + (-1)^{n-1} \mathbb{P}\left(\bigcap_{i=1}^n A_i\right). \tag{19.1.5}$$

(vii) $\mathbb{P}\left(\bigcup_n A_n\right) \leq \sum_n \mathbb{P}(A_n)$.

Corollary 19.1.7 (Bonferroni's inequalities)**.** For any events $A_1, A_2, \ldots, A_n$ and for any r, $1 \leq r \leq n$,

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \begin{array}{c} \leq \\ \text{or} \\ \geq \end{array} \sum_i \mathbb{P}(A_i) - \sum_{i_1<i_2} \mathbb{P}(A_{i_1} \cap A_{i_2}) + \sum_{i_1<i_2<i_3} \mathbb{P}(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \cdots + (-1)^{r-1} \sum_{i_1<\cdots<i_r} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_r}),$$

according as r is odd or even. That is, if the sum in the inclusion-exclusion formula is truncated after r terms it overestimates or underestimates the probability of the union of the n events according as r is odd or even.

Proof. The proof proceeds by induction on n. Assume it is true for n, then for $n+1$ events it is true when $r = n+1$, by the inclusion-exclusion formula, and for $r \leq n$, apply the inductive hypothesis to probability of the two unions of n events in relation (19.1.5) to get the result. □

Example 19.1.8. We now consider that how many of the number 1,...,500 are not divisible by 7 but are divisible by 3 or 5.

Let A be the event that number $1 \sim 500$ that divisible by 7, B be the event that the number divisible by 3, C be the event that the number divisible by 5. so

$$\begin{aligned} A &= \{7, 14, \ldots, 497\}, |A| = 71, \\ B &= \{3, 6, \ldots, 498\}, |B| = 166, \\ C &= \{5, 10, \ldots, 500\}, |C| = 100, \\ A \cap B &= \{21, 42, \ldots, 483\}, |A \cap B| = 23 \\ A \cap C &= \{35, 70, \ldots, 490\}, |A \cap C| = 14 \\ B \cap C &= \{15, 30, \ldots, 495\}, |B \cap C| = 33 \\ A \cap B \cap C &= \{105, 210, \ldots, 420\}, |A \cap B \cap C| = 4 \end{aligned}$$

so by inclusion-exclusion formula (Proposition 19.1.6.(vi)), we have $166 + 100 - 33 - 23 - 14 + 4 = 200$.

19.1.2 Combinatorial analysis

Fundamental rule: There are r multiple choices to be made in sequence: there are m_1 possibilities for the first choice, after making the first choice there are m_2 possibilities for the second choice, after making the first two choices there are m_3 possibilities for the third choice, and so on until after making the first $r-1$ choices there are m_r possibilities for the rth choice. Then the total number of different possibilities for the set of choices is $m_1 m_2 \ldots m_r$.

Example 19.1.9. A restaurant menu has 6 starters, 7 main courses and 6 puddings. The total number of different three-course meals that may be served is $6 \times 7 \times 6 = 252$.

Example 19.1.10 (Sampling models)**.** Many of the standard calculations that arise in classical probability where outcomes need to be counted may be put in a standard framework of sampling. Think of drawing m balls from an urn which initially contains n distinguishable balls (they are numbered 1 to n, say). This may be done in a number of ways:

(i) **Sampling with replacement and with ordering.** The balls are replaced between successive draws and the order in which balls are drawn is noted. Then the Fundamental Rule shows that there are n^m possible ways.

(ii) **Sampling without replacement and with ordering ($m \leq n$).** The balls are not replaced after drawing and the order is noted. Then the number of ways is

$$n(n-1)\ldots(n-m+1) = \frac{n!}{(n-m)!} = P_m^n. \tag{19.1.6}$$

The symbol P_m^n represents the number of permutations of n objects m at a time. An important special case occurs when $n = m$. We get the number of permutations of n distinguishable objects (that is the number of distinguishable ways they may be laid out in a line, say) is $n!$.

(iii) **Sampling without replacement and without ordering.** If we take m balls from n and they were ordered there would be $n(n-1)\dots(n-m+1) = n!/(n-m)!$ ways but each unordered selection may be permuted in $m!$ different ways (or give $m!$ ordered arrangements) so that the total number of unordered ways is

$$\frac{n!}{(n-m)!m!} = \binom{n}{m} = C_m^n. \tag{19.1.7}$$

The symbol $\binom{n}{m}$ is the binomial coecient, usually read "n choose m", and represents the number of ways of picking m objects from n, note that $\binom{n}{m}$ is the coecient of x^m in the expansion of $(1+x)^n$ using the binomial theorem.

Suppose that, of the n balls, m_1 are of colour 1, m_2 are of colour 2 and so on up to m_k balls of colour k, where $n = m_1 + \dots + m_k$. Consider the number of permutations of the n balls when the balls are distinguishable only by colour. For example, if $n = 4$ and there are two black balls and two white balls then there are 6 possible arrangements:

$$BBWW \quad BWBW \quad BWWB \quad WBBW \quad WBWB \quad WWBB \tag{19.1.8}$$

If the balls are distinguishable then there are $n!$ permutations, but within colour i there are $m_i!$ ways of permuting the balls so the Fundamental Rule gives that for each distinguishable arrangement there are $\prod_{i=1}^k (m_i!)$ ways of permuting the balls leaving the arrangement the same if the balls are distinguishable only by colour. Thus the number of arrangements distinguishable only by colour is

$$\frac{n!}{m_1!m_2!\dots m_k!} = \binom{n}{m_1 \dots m_k}, \tag{19.1.9}$$

which is the multinomial coefficient (the coefficient of $x_1^{m_1}x_2^{m_2}\dots x_k^{m_k}$ in the expansion of $(x_1 + \dots + x_k)^n$). An alternative way of seeing this is to think of first choosing the positions for the balls of colour 1, which can be done in $\binom{n}{m_1}$ ways, then choose the positions for the balls of colour 2 in $\binom{n-m_1}{m_2}$ ways and so on to see that the total number of ways, using the Fundamental Rule, is

$$\binom{n}{m_1}\binom{n-m_1}{m_2}\binom{n-m_1-m_2}{m_3}\cdots\binom{n-m_1-\dots-m_{k-1}}{m_k} = \binom{n}{m_1\dots m_k}. \tag{19.1.10}$$

(iv) **Sampling with replacement and without ordering.** Draw m balls one after another, each time noting the number of the ball and replacing it before the next draw,

Ball No.	1	2	3	4	...	n
Times drawn	$\surd$	$\surd\surd$	$\surd$	$\surd\surd$	...	$\surd$

so that the number of $\surd$ is the number of times the ball is drawn. The number of ways is then the number of ways that $n-1$ vertical lines may be put between m $\surd$ which is

$$\binom{n+m-1}{n-1}. \tag{19.1.11}$$

think of choosing $n-1$ slots for the vertical lines out of $n+m-1$ slots and then the checks go in the remainder.

Example 19.1.11 (Allocation models)**.** An alternative way of thinking of these counting schemes is to think about allocating m tokens (labelled $1,\dots,m$) to n boxes (labelled $1,\dots,n$). The four cases considered previously correspond to:

(i) Each box may contain any number of tokens and the labels on the tokens are observed.

(ii) No box may contain more than one token and the labels on the tokens are observed.

(iii) No box may contain more than one token and the labels on the the tokens are not observed.

(iv) Each box may contain any number of tokens and the labels on the tokens are not observed.

In the next examples in which each outcome in the probability space is equally likely we will calculate the probability of the event A by computing the number of points N in the sample space Ω and then computing the number N_A of points in A. In each case the probability will then be

$$\mathbb{P}(A) = \frac{N_A}{N} \tag{19.1.12}$$

Example 19.1.12. What is the probability that a Poker hand shows five different face values? (A poker hand contains 5 cards.) One way to do this is to think of consisting of all possible poker hands, that is, unordered sets of five cards chosen from a standard pack of 52. We have $N = \binom{52}{5}$ and A consists of those hands showing five different face values so that

$$N_A = \binom{13}{5} \times 4^5 \tag{19.1.13}$$

since we may think of first choosing the unordered sets of 5 face values and then the different suits for each value, and use the Fundamental Rule. An alternative way in this problem, and in other situations involving sampling without replacement, is to think of comprising all ordered sets of 5 cards (imagine the cards being dealt in sequence). Then $N = 52\times51\times50\times49\times48$ and $N_A = 52\times48\times44\times40\times36$, thinking of the possible choices for the first card, second card in the hand and so on to give 5 different face values. You should check that these two different approaches give the same probabilities. Either approach is fine, but remember to be consistent - if your sample space has unordered (respectively, ordered) points then the points in A must be unordered (respectively, ordered).

Example 19.1.13. What is the probability that a Bridge hand (13 cards) contains 5 spades (♠), 3 hearts (♡), 4 diamonds (♢) and 1 club (♣)? Take Ω to be the set of unordered Bridge hands, so we have $N = \binom{52}{13}$ while

$$N_A = \binom{13}{5} \times \binom{13}{3} \times \binom{13}{4} \times \binom{13}{1}. \tag{19.1.14}$$

since we may think of choosing in sequence the spades, hearts, diamonds and club and then use the Fundamental Rule to get the total number of ways.

Example 19.1.14. If there are r people in a room, what is the probability that at least two have the same birthday? In this case the number of points in the sample space Ω is $N = (365)^r$, since the sample space consists of all possible r-tuples of birthdays. If A is the required event, this is a case where it is easier to calculate the number of points in A^c, the complement of A, since A^c is just the event that no two of the r people share a birthday. We then have

$$N_{A^c} = 365 \times 364 \times 363 \times \cdots \times (365 - r + 1) \quad \Rightarrow \quad \mathbb{P}(A) = 1 - P(A^c) = 1 - \frac{365 \times 364 \times 363 \times \cdots \times (365 - r + 1)}{(365)^r} = p_r.$$

It is interesting to note the following values

r	10	15	20	21	22	23	24	25	30	40	55
p_r	0.12	0.25	0.41	0.44	0.48	0.51	0.54	0.57	0.71	0.89	0.99

which shows the well known fact that if there are 23 or more people in a room there is higher than evens chances that at least 2 share a birthday.

Example 19.1.15. What is the probability that in a round of Bridge at least one player holds exactly two aces and two kings? Let Ω be the sample space of all possible (unordered) hands for 4 players, then the number of points in Ω is $N = \binom{52}{13\ 13\ 13\ 13}$. For each player i, $i = 1, 2, 3, 4$, let A_i be the event that player i holds exactly two aces and two kings. Then

$$\mathbb{P}(A_i) = \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9}\binom{39}{13\ 13\ 13}}{\binom{52}{13\ 13\ 13\ 13}} = \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9}}{\binom{52}{13}}. \tag{19.1.15}$$

think of choosing the aces for player i, then the kings and then 9 other cards and finally distributing the remaining 39 cards among the other three players. If $i \neq j$, then

$$\mathbb{P}(A_i \cap A_j) = \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9\ 9\ 26}\binom{26}{13}}{\binom{52}{13\ 13\ 13\ 13}} = \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9\ 9\ 26}}{\binom{52}{13\ 13\ 26}}, \tag{19.1.16}$$

as before, think of picking the aces and kings for player i with the remaining aces and kings going to player j, and then picking 9 other cards for each of i and j. If i, j, k are unequal then $A_i \cap A_j \cap A_k = \emptyset$, so that by inclusion exclusion we have the required probability is

$$\mathbb{P}\left(\bigcup_{i=1}^{4} A_i\right) = 4 \times \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9}}{\binom{52}{13}} - \binom{4}{2} \times \frac{\binom{4}{2}\binom{4}{2}\binom{44}{9\ 9\ 26}}{\binom{52}{13\ 13\ 26}}. \tag{19.1.17}$$

Example 19.1.16. Suppose that n students leave their n coats outside a lecture room and when they leave they pick up their coats at random. What is the probability that at least one student has his own coat? Let Ω consist of all permutations of $1, \ldots, n$, so that if $(i_1, \ldots, i_n) \in \Omega$ then i_j is the index of the coat got by student j. Denote by A_i the event that student i gets his own coat. Then for $i_1 < i_2 < \cdots < i_r$, the probability that all of the students $i_1, \ldots, i_r$ get their own coats is

$$\mathbb{P}\left(\bigcap_{k=1}^{r} A_{ik}\right) = \frac{(n-r)!}{n!}, \tag{19.1.18}$$

since the numerator is the number of ways that the remaining $n - r$ coats may be permuted among the remaining $n - r$ students. Then by inclusion-exclusion we have

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{r=1}^{n}\left[(-1)^{r-1}\sum_{i_1<\cdots<i_r}\mathbb{P}\left(\bigcap_{k=1}^{r} A_{ik}\right)\right] = \sum_{r=1}^{n}(-1)^{r-1}\binom{n}{r}\frac{(n-r)!}{n!} = \sum_{r=1}^{n}(-1)^{r-1}\frac{1}{r!}, \tag{19.1.19}$$

so that for large n the probability is approximately equal to

$$1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \cdots = 1 - e^{-1} \approx 0.632. \tag{19.1.20}$$

19.1.3 Independence and Borel-Cantelli lemmas

Relative to measure theory, probability theory is enriched by the significance attached to the notion of independence.

Definition 19.1.5. Let I be a countable set. Say that events A_i, $i \in I$, are independent if, for all finite subsets $J \subseteq I$,

$$\mathbb{P}\left(\bigcap_{i\in J} A_i\right) = \prod_{i\in J}\mathbb{P}(A_i). \tag{19.1.21}$$

Example 19.1.17. Roll a die twice and let A be the event that a 1 is obtained on the first roll and B be the event that a 5 is obtained on the second roll. The sample space $\Omega = \{(i, j) : 1 \le i \le 6, 1 \le j \le 6\}$ has 36 points, all of which have the same probability $\frac{1}{36}$. Then $A \cap B$ is just the outcome $(1, 5)$ and $\mathbb{P}(A) = \frac{1}{6} = \mathbb{P}(B)$ so we can conclude that A and B are independent.

Proposition 19.1.18. If A and B are independent then so are

$$\text{(i) } A \text{ and } B^c, \qquad \text{(ii) } A^c \text{ and } B^c, \qquad \text{(iii) } A^c \text{ and } B. \tag{19.1.22}$$

Proof. For (i), $\mathbb{P}(A \cap B^c) = \mathbb{P}(A) - \mathbb{P}(A \cap B) = \mathbb{P}(A) - \mathbb{P}(A)\mathbb{P}(B) = \mathbb{P}(A)(1 - \mathbb{P}(B)) = \mathbb{P}(A)\mathbb{P}(B^c)$.
(ii) and (iii) follow from (i). □

The Definition 19.1.5 implies that if we take any two of the events A_i and A_j (i distinct from j) then they are independent, so the events are said to be pairwise independent. However, it should be noted that pairwise independence does not imply independence as the next example shows.

Example 19.1.19. Suppose that a fair coin is tossed twice (by a fair coin we mean the 4 possible outcomes HH, HT, TH and TT are equally likely and equal to $\frac{1}{4}$, so that a Head or a Tail on either toss has probability $\frac{1}{2}$). Let A_1 be the event that a head is obtained on the first toss, A_2 the event that there is a head on the second toss and A_3 the event that exactly 1 head is obtained. Then $\mathbb{P}(A_i) = \frac{1}{2}$ for $i = 1, 2, 3$. It may be seen that the events are pairwise independent since, for example,

$$\mathbb{P}(A_1 \cap A_3) = \mathbb{P}(A_1 \cap A_2^c) = \frac{1}{4} = \mathbb{P}(A_1)\mathbb{P}(A_3), \tag{19.1.23}$$

and similarly for A_2 and A_3 (and A_1 and A_2). But

$$\mathbb{P}(A_1 \cap A_2 \cap A_3) = 0 \neq \mathbb{P}(A_1)\mathbb{P}(A_2)\mathbb{P}(A_3) = \frac{1}{8}, \tag{19.1.24}$$

so the three events are not independent.

More than the independence of events, we give the independence of σ-algebra.

Definition 19.1.6. σ-algebras $\mathcal{A}_i \subseteq \mathcal{F}$, $i \in I$, are independent if A_i, $i \in I$, are independent whenever $A_i \in \mathcal{A}_i$ for all i.

Here is a useful way to establish the independence of two σ-algebras.

Theorem 19.1.20. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be π-systems contained in $\mathcal{F}$ and suppose that

$$\mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1)\mathbb{P}(A_2) \tag{19.1.25}$$

whenever $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$. Then $\sigma(\mathcal{A}_1)$ and $\sigma(\mathcal{A}_2)$ are independent.

Proof. Fix $A_1 \in \mathcal{A}_1$ and define for $A \in \mathcal{F}$, $\mu(A) = \mathbb{P}(A_1 \cap A)$, $\nu(A) = \mathbb{P}(A_1)\mathbb{P}(A)$. Then μ and ν are measures which agree on the π-system $\mathcal{A}_2$, with $\mu(\Omega) = \nu(\Omega) = \mathbb{P}(A_1) < \infty$. So, by uniqueness of extension, for all $A_2 \in \sigma(\mathcal{A}_2)$,

$$\mathbb{P}(A_1 \cap A_2) = \mu(A_2) = \nu(A_2) = \mathbb{P}(A_1)\mathbb{P}(A_2). \tag{19.1.26}$$

Now fix $A_2 \in \sigma(\mathcal{A}_2)$ and repeat the argument with

$$\mu'(A) = \mathbb{P}(A \cap A_2), \qquad \nu'(A) = \mathbb{P}(A)\mathbb{P}(A_2) \tag{19.1.27}$$

to show that, for all $A_1 \in \sigma(\mathcal{A}_1)$, $\mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1)\mathbb{P}(A_2)$. □

Then we extend the above theorem.

Theorem 19.1.21. Let $\mathcal{A}_i, i \in I$ be π-systems contained in $\mathcal{F}$. I is a countable set and $J \subseteq I$ is a finite set. Suppose that

$$\mathbb{P}\left(\bigcap_{i\in J} A_i\right) = \prod_{i\in J} \mathbb{P}(A_i) \tag{19.1.28}$$

whenever $A_i \in \mathcal{A}_i$. Then $\sigma(\mathcal{A}_i), i \in I$ are independent.

Proof. We prove this by induction. First assume that for π-systems $\mathcal{A}_i, i \leq k$ and $A_i \in \mathcal{A}_i, i \leq k$,

$$\mathbb{P}\left(\bigcap_{i\leq k} A_i\right) = \prod_{i\leq k} \mathbb{P}(A_i) \;\Rightarrow\; \sigma(\mathcal{A}_i), i \leq k \text{ are independent.} \tag{19.1.29}$$

Thus, Fix $A_i \in \mathcal{A}_i, i \leq k$ and define for $A \in \mathcal{F}$,

$$\mu(A) = \mathbb{P}\left(\left(\bigcap_{i\leq k} A_i\right) \bigcap A\right), \qquad \nu(A) = \left(\prod_{i\leq k} \mathbb{P}(A_i)\right) \mathbb{P}(A) \tag{19.1.30}$$

Then μ and ν are measures which agree on the π-system $\mathcal{A}_{k+1}$, with $\mu(\Omega) = \nu(\Omega) = \mathbb{P}\left(\bigcap_{i\leq k} A_i\right) < \infty$. So by uniqueness of extension, for all $A_{k+1} \in \sigma(\mathcal{A}_{k+1})$, $\mathbb{P}\left(\bigcap_{i\leq k+1} A_i\right) = \mu(A_{k+1}) = \nu(A_{k+1}) = \prod_{i\leq k+1} \mathbb{P}(A_i) \;\Rightarrow\; \sigma(\mathcal{A}_i), i \leq k+1$ are independent. □

Proposition 19.1.22. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $A_n, n \in \mathbb{N}$, a sequence of events. Then $A_n, n \in \mathbb{N}$ are independent if and only if the σ-algebras they generate

$$\sigma(A_n) = \{\emptyset, A_n, A_n^c, \Omega\} \quad \text{ are independent.} \tag{19.1.31}$$

Proof. ($\Leftarrow$) Recall the definition that σ-algebras $\mathcal{A}_i \subseteq \mathcal{F}$, $i \in I$ are independent if A_i, $i \in I$ are independent whenever $A_i \in \mathcal{A}_i$ for all i.

($\Rightarrow$) We take $\mathcal{A}_n = \{\emptyset, A_n\}$. It is easy to check that $\mathcal{A}_n$ is a π-system. Thus, by Theorem 19.1.21, the independence of A_n implies the independence of $\sigma(A_n)$, the σ-algebras they generate. □

Theorem 19.1.23. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Suppose $(\mathcal{F}_{i,j})_{1\leq i\leq n, 1\leq j\leq m(i)}$ are independent and let $\mathcal{G}_i = \sigma\left(\bigcup_j \mathcal{F}_{i,j}\right)$. Then $\mathcal{G}_1, \ldots, \mathcal{G}_n$ are independent.

Proof. Let $\mathcal{A}_i$ be the collection of sets of the form $\bigcap_j A_{i,j}$ where $A_{i,j} \in \mathcal{F}_{i,j}$. Thus, $\mathcal{A}_i$ is π-system of σ-algebra $\sigma\left(\bigcup_j \mathcal{F}_{i,j}\right) = \mathcal{G}_i$. Also, $\mathcal{A}_i$ are independent as $\mathcal{F}_{i,j}$ are independent, i.e.,

$$\mathbb{P}\left(\bigcap_i \bigcap_j A_{ij}\right) = \prod_{i=1}^{n} \mathbb{P}\left(\bigcap_j A_{ij}\right). \tag{19.1.32}$$

Hence, $\sigma(\mathcal{A}_i) = \mathcal{G}_i$ are independent by Theorem 19.1.21. □

Lemma 19.1.24 (first Borel-Cantelli lemma)**.** Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a measure space. For sequence $A_n \subseteq \Omega$, if $\sum_n \mathbb{P}(A_n) < \infty$, then $\mathbb{P}(A_n \text{ i.o.}) = 0$. (That is almost surely, A_n^c occurs eventually.)

We note that first Borel-Cantelli lemma (Lemma 15.1.13) is valid whether or not μ is a probability measure. The converse is not true, but if we add the independence, then it is true, which is the second lemma.

Lemma 19.1.25 (second Borel-Cantelli lemma)**.** Assume that the events $(A_n : n \in \mathbb{N})$ are independent. If $\sum_n \mathbb{P}(A_n) = \infty$, then $\mathbb{P}(A_n \text{ i.o.}) = 1$. Hence, almost surely, A_n holds infinitely often.

Proof. We use the inequality $1 - a \leq e^{-a}$. Set $a_n = \mathbb{P}(A_n)$. Then, for all n we have

$$\mathbb{P}\left(\bigcap_{m \geq n} A_m^c\right) = \prod_{m \geq n} (1 - a_m) \leq \exp\left(-\sum_{m \geq n} a_m\right) = 0 \quad \Rightarrow \quad \mathbb{P}(A_n \text{ i.o.}) = 1 - \mathbb{P}\left(\bigcup_n \bigcap_{m \geq n} A_m^c\right) = 1. \qquad \square$$

Example 19.1.26. Infinite coin-toss. Let $0 < p < 1$. We will soon construct a probability measure $\mathbb{P}$ on the infinite coin-toss measurable space $(\Omega, \mathcal{F})$ such that the events $\{\omega_n = 1\}$, $n \in \mathcal{N}$ are independent and for all $n \geq 1$, $\mathbb{P}(\omega_n = 1) = p$. Then

$$\sum_n \mathbb{P}(\omega_n = 1) = \infty, \tag{19.1.33}$$

hence, since these events are independent, we may apply the second Borel-Cantelli lemma (Lemma 19.1.25): almost surely, there are infinitely many heads in the coin-tossing experiment (no matter how small p is).

19.2 Random variables

Recall the definition in measure theory, we have the following definitions:

19.2.1 Random variables

Definition 19.2.1. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and let $(E, \mathcal{E})$ be a measurable space. A measurable function $X : \Omega \to E$ is called a random variable in E.

It has the interpretation of a quantity, or state, determined by chance. Where no space E is mentioned, it is assumed that X takes values in $\mathbb{R}$.

Example 19.2.1. Recall Definition 15.2.3. A real-valued random variable which takes on just the two values 0 and 1 is known as an indicator random variable, suppose that the event on which it takes the value 1 is $A \subseteq \Omega$ and otherwise 0, then the random variable is denoted by $\mathbb{1}_A$.

Definition 19.2.2. The image measure $\mu_X = \mathbb{P} \circ X^{-1}$ is called the law or distribution of X. For real-valued random variables ($E = \mathbb{R}$), μ_X is uniquely determined by its values on the π-system of intervals $(-\infty, x]$, $x \in \mathbb{R}$, given by

$$F_X(x) = \mu_X((-\infty, x]) = \mathbb{P}(X \leq x) = \mathbb{P}\left(\{\omega : X(\omega) \leq x\}\right). \tag{19.2.1}$$

Then μ_X is unique for any measurable $A \in \mathcal{B}(\mathbb{R})$ by uniqueness of extension (by Theorem 15.1.18). The function F_X is called the distribution function of X.

Remark. F_X is right-continuous since for $\varepsilon > 0$ and let $\varepsilon = \frac{1}{n}$, $\bigcap_n \left(x, x + \frac{1}{n}\right] = \emptyset$,

$$F_X(x + \varepsilon) - F_X(x) = \mu_X((-\infty, x + \varepsilon]) - \mu_X((-\infty, x]) = \mu_X\left((x, x + \varepsilon]\right) \to \mu_X\left(\bigcap_n \left(x, x + \frac{1}{n}\right]\right) = \mu_X(\emptyset) = 0 \tag{19.2.2}$$

by Corollary 15.1.11. However, F_X is not left-continuous since

$$F_X(x+\varepsilon) - F_X(x) = \mu_X((-\infty, x-\varepsilon]) - \mu_X((-\infty, x]) = -\mu_X\left((x-\varepsilon, x]\right) \to -\mu_X\left(\bigcap_n \left(x - \frac{1}{n}, x\right]\right) = -\mu_X(\{x\}), \quad (19.2.3)$$

which could be an atom (Definition 19.2.3).

Definition 19.2.3. If $\mathbb{P}(X = c) > 0$, then the law μ_X of X is said to have an atom at c, and the distribution function F_X of X has a discontinuity at c:

$$\mu_X(\{c\}) = F_X(c) - F_X(c^-) = \mathbb{P}(X = c). \qquad (\text{as } F_X \text{ is right-continuous}) \quad (19.2.4)$$

Remark. μ can have at most n atoms of mass at least $1/n$, so that the number of atoms of μ is at most countable. So we have,

Proposition 19.2.2. given $x \in \mathbb{R}$, the set of non-atoms is dense, i.e. there exists a sequence (y_n) of reals with $y_n \downarrow x$ such that every y_n is a non-atom of μ (equivalently a point of continuity of F_X), and then by right-continuous of F_X, $F_X(y_n) \downarrow F_X(x)$.

Proof. [1]. □

Definition 19.2.4. Similarly, the law μ_X on $(\mathbb{R}^n, \mathcal{B}(\mathbb{R}^n))$ is

$$\mu_X(A) = \mathbb{P}\left(X_1 \le x_1, \ldots, X_n \le x_n\right), \quad (19.2.5)$$

where $A = \bigotimes_{i=1}^{n}(-\infty, x_i] := (-\infty, x_1] \times \ldots (-\infty, x_n],\ x_i \in \mathbb{R}$. Then μ_X is unique for any measurable $A \in \mathcal{B}(\mathbb{R}^n)$.

Definition 19.2.5. If an increasing and right-continuous function $F : \mathbb{R} \to [0, 1]$ satisfies the following conditions

$$\lim_{x \to -\infty} F(x) = 0, \qquad \lim_{x \to \infty} F(x) = 1, \quad (19.2.6)$$

we call it distribution function.

Remark. For any distribution function F, set $\Omega = (0, 1]$ and $\mathcal{F} = \mathcal{B}((0, 1])$. Let $\mathbb{P}$ denote the restriction of Lebesgue measure to $\mathcal{F}$. Then $(\Omega, \mathcal{F}, \mathbb{P})$ is a probability space. Let F be any distribution function. Define $X : \Omega \to \mathbb{R}$ by

$$X(\omega) = \inf\{x : \omega \le F(x)\}. \quad (19.2.7)$$

Then, by Lemma 15.2.10, X is a random variable and $X(\omega) \le x$ if and only if $\omega \le F(x)$. So

$$F_X(x) = \mathbb{P}(X \le x) = \mathbb{P}((0, F(x)]) = F(x) - 0 = F(x). \qquad (\mathbb{P} \text{ is Lebesgue measure}) \quad (19.2.8)$$

Alternatively, from 15.2.11, we know that there exists a unique Borel measure μ_X (F implies X and thus implies μ_X) such that

$$F_X(x) = \underbrace{\mu_X((-\infty, x])}_{dg((a,b])} = \mathbb{P}(X \le x) = \underbrace{F(x)}_{g(b)} - \underbrace{\lim_{x \to -\infty} F(x)}_{g(a)} = F(x). \quad (19.2.9)$$

Thus, we have following proposition:

Proposition 19.2.3. Every distribution function F is the distribution function F_X of a random variable X.

Remark. Furthermore, μ_X is non-zero Radon measure [2] in $\mathbb{R}$ (since $\mathbb{P}(X \le x) \in [0, 1]$). Thus, this unique non-zero Radon measure μ_X is Lebesgue-Stieltjes measure associated with F (by Theorem 15.2.11).

[1] need proof
[2] need sort out

Example 19.2.4. Let C_n denote the nth approximation to the Cantor set C: thus $C_0 = [0,1]$, $C_1 = \left[1, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$, $C_2 = \left[1, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right]$, etc. and $C_n \downarrow C$ as $n \to \infty$. Denote by F_n the distribution function of a random variable uniformly distributed (see Definition 19.8.4) on C_n. Note that F_n is given recursively by

$$F_{n+1}(x) = \begin{cases} \frac{1}{2}F_n(3x) & 0 \le x \le \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} \le x \le \frac{2}{3} \\ \frac{1}{2} + \frac{1}{2}F_n(3x-2) & \frac{2}{3} \le x \le 1 \end{cases} \tag{19.2.10}$$

so

$$|F_{n+1}(x) - F_n(x)| \le \frac{1}{2} \sup_x |F_n(x) - F_{n-1}(x)| \le 2^{-n}. \tag{19.2.11}$$

Hence F_n converges uniformly with continuous limit F. If $x \notin C$ then $x \notin C_n$ for some n and $F = F_n$ =constant in a neightbourhood of x, so F is differentiable at x with $F'(x) = 0$. The Lebesgue measure of C is zero.

Proposition 19.2.5 (Skorokhod representation of a random variable with prescribed distribution function)**.** Let $F : \mathbb{R} \to [0,1]$ be distribution function. For probability space $(\Omega, \mathcal{F}, \mathbb{P}) = ([0,1], \mathcal{B}[0,1], \text{Leb})$, define

$$X^+(\omega) := \inf\{x : F(x) > \omega\} = \sup\{y : F(y) \le \omega\}, \qquad X^-(\omega) := \inf\{x : F(x) \ge \omega\} = \sup\{y : F(y) < \omega\}. \tag{19.2.12}$$

Then, the random variable X^- has distribution function F, and almost surely, $X^+ = X^-$.

Proof. By definition of X^-, we have

$$\{\omega \le F(c)\} \;\Rightarrow\; \left\{X^-(\omega) \le c\right\}. \tag{19.2.13}$$

Also,

$$\left\{x > X^-(\omega)\right\} \;\Rightarrow\; \{F(x) \ge \omega\}, \tag{19.2.14}$$

so, by the right-continuity of F, $F(X^-(\omega)) \ge \omega$, and

$$\left\{X^-(\omega) \le c\right\} \;\Rightarrow\; \left\{\omega \le F(X^-(\omega)) \le F(c)\right\}. \tag{19.2.15}$$

Thus, $\{\omega \le F(c)\} \Leftrightarrow \{X^-(\omega) \le c\}$, so that $\mathbb{P}(X^-(\omega) \le c) = F_c$, i.e., the random variable X^- has distribution function F.

By definition of X^+,

$$\{\omega < F(c)\} \;\Rightarrow\; \left\{X^+(\omega) \le c\right\}. \tag{19.2.16}$$

so that $F(c) \le \mathbb{P}(X^+(\omega) \le c)$. SInce $X^- \le X^+$, it is clear that

$$\left\{X^- \ne X^+\right\} = \bigcup_{c \in \mathbb{Q}} \left\{X^- \le c < X^+\right\}. \tag{19.2.17}$$

But, for every $c \in \mathbb{R}$,

$$\mathbb{P}\left(\left\{X^- \le c \le X^+\right\}\right) = \mathbb{P}\left(\left\{X^- \le c\right\} \setminus \left\{X^+ \le c\right\}\right) \le F(c) - F(c) = 0. \tag{19.2.18}$$

Since $\mathbb{Q}$ is countable, the result follows.[3] □

19.2.2 Independence of random variables

Definition 19.2.6. Recall Definition 15.2.2, given a countable family of random variables $X_i : \Omega \to G, i \in I$, the σ-algebra generated by $(X_i : i \in I)$ is

$$\sigma(X_i, i \in I) = \sigma\left(X_i^{-1}(A) : A \in \mathcal{G}, i \in I\right). \tag{19.2.19}$$

Definition 19.2.7. A countable family of random variables $(X_i : i \in I)$ is said to be independent (or X_i are independent) if the σ-algebras $(\sigma(X_i) : i \in I)$ are independent.

Proposition 19.2.6. If $\mathcal{F}$ and $\mathcal{G}$ are independent and random variables X is $\mathcal{F}$-measurable, Y is $\mathcal{G}$-measurable, then X and Y are independent.

[3] need graph in Williams [16].P_{34}

Proof. First we have $\sigma(X) \subseteq \mathcal{F}$ and $\sigma(Y) \subseteq \mathcal{G}$. Then $\forall A \in \sigma(X), B \in \sigma(Y)$, we have

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B) \tag{19.2.20}$$

since $A \in \mathcal{F}, B \in \mathcal{G}$ and $\mathcal{F}, \mathcal{G}$ are independent. □

Proposition 19.2.7. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Let X and Y be two random variables. If X is independent of $\mathcal{F}$ and Y is $\mathcal{F}$-measurable, then X and Y are independent.

Proof. Y is $\mathcal{F}$-measurable, i.e., $\sigma(Y) \subseteq \mathcal{F}$. Since X is independent of $\mathcal{F}$, i.e., for any $A \in \sigma(X)$, $B \in \mathcal{F}$

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B). \tag{19.2.21}$$

Since $\sigma(Y) \subseteq \mathcal{F}$, the equation holds for all $A \in \sigma(X)$ and $B \in \sigma(Y)$, thus X and Y are independent (by Definition 19.2.7). □

Theorem 19.2.8. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. If $(X_{i,j})_{1 \le i \le n, 1 \le j \le m(i)}$ are independent and $f_i : \mathbb{R}^{m(i)} \to \mathbb{R}$ are measurable then $f_i(X_{i,1}, \dots, X_{i,m(i)})$ are independent.

Proof. Let $\mathcal{F}_{i,j} = \sigma(X_{i,j})$ and $\mathcal{G}_i = \sigma\left(\bigcup_j \mathcal{F}_{i,j}\right)$. Then by Theorem 19.1.23, $\mathcal{G}_i$ are independent. Since $f_i(X_{i,1}, \dots, X_{i,m(i)})$ is $\mathcal{G}_i$-measurable (as f_i are measurable[4]), we have $f_i(X_{i,1}, \dots, X_{i,m(i)})$ are independent by Proposition 19.2.6. □

Remark. What if $(X_{i,j})_{1 \le j \le m(i)}$ are not independent?[5]

Proposition 19.2.9. Let $(X_n : n \in \mathbb{N})$ be a sequence of real-valued random variables on $(\Omega, \mathcal{F}, \mathbb{P})$ and suppose that for all for all $x_1, \dots, x_n \in \mathbb{R}$ and all n,

$$\mathbb{P}(X_1 \le x_1, \dots, X_n \le x_n) = \mathbb{P}(X_1 \le x_1) \dots \mathbb{P}(X_n \le x_n) \tag{19.2.22}$$

if and only if $X_1, \dots, X_n$ are independent.

Remark. The equation is equivalent to $\mathbb{P}(X_1 \in dx_1, \dots, X_n \in dx_n) = \mathbb{P}(X_1 \in dx_1) \dots \mathbb{P}(X_n \in dx_n)$.

Proof. ($\Leftarrow$) It the direct result from Definition 19.1.5, 19.2.6 and 19.2.7.

($\Rightarrow$) X_i are independent means that $\sigma(X_i)$ are independent. From 19.1.21, we know that if $\mathcal{A}_i$ are π-systems for which

$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \mathbb{P}(A_i), \qquad A_i \in \mathcal{A}_i \tag{19.2.23}$$

whenever $A_i \in \mathcal{A}_i$. Then $\sigma(\mathcal{A}_i)$ are independent. Clearly, $\{\{\omega : X(\omega) \le x\},\ x \in \mathbb{R}\}$ is a π-system since

$$\begin{cases} A := \{\{\omega : X(\omega) \le x\},\ x \in \mathbb{R}\} \in \mathcal{A} \\ B := \{\{\omega : X(\omega) \le y\},\ y \in \mathbb{R}\} \in \mathcal{A} \end{cases} \Rightarrow\ \emptyset \in \mathcal{A},\ A \cap B = A \text{ or } B \in \mathcal{A}. \tag{19.2.24}$$

Thus, It suffices to show that

$$\{\{\omega : X(\omega) \le x\},\ x \in \mathbb{R}\} = \{X^{-1}(-\infty, x],\ x \in \mathbb{R}\} \quad \text{generates} \quad \sigma(X) = \sigma(\{X^{-1}(B), B \in \mathcal{B}\}) \tag{19.2.25}$$

where $\mathcal{B}$ is Borel σ-algebra on $\mathbb{R}$. It is equivalent to show that

$$\sigma\left(\{X^{-1}(B), B \in \mathcal{B}\}\right) \subseteq \sigma\left(\{X^{-1}(-\infty, x],\ x \in \mathbb{R}\}\right) \tag{19.2.26}$$

Then it suffices to show that

$$\mathcal{A} := \left\{B : X^{-1}(B) \in \sigma\left(\{X^{-1}(-\infty, x],\ x \in \mathbb{R}\}\right),\ B \in \mathcal{B}\right\} \supseteq \mathcal{B} = \sigma\left(\{(-\infty, x],\ x \in \mathbb{R}\}\right) \tag{19.2.27}$$

Then it is obvious that $\{(-\infty, x],\ x \in \mathbb{R}\} \subseteq \mathcal{A}$.

Thus, it is enough to show that $\mathcal{A}$ is a σ-algebra. (This follows by Proposition 2.6.1.)

[4] need details
[5] need proof

(i) $B = \emptyset \in \mathcal{B}$, then $X^{-1}(B) = \emptyset \in \sigma\left(\{X^{-1}(-\infty, x],\ x \in \mathbb{R}\}\right)$. So $\emptyset \in \mathcal{A}$.

(ii) If $B \in \mathcal{A}$, $X^{-1}(B) \in \sigma\left(\{X^{-1}(-\infty, x,\ x \in \mathbb{R}\}\right)$ and $B \in \mathcal{B}$. Then

$$B^c \in \mathcal{B}, \quad X^{-1}(B^c) = \left(X^{-1}(B)\right)^c \in \sigma\left(\{X^{-1}(-\infty, x],\ x \in \mathbb{R}\}\right) \ \Rightarrow\ B^c \in \mathcal{A} \tag{19.2.28}$$

(iii) If $B_n \in \mathcal{A} \ \Rightarrow\ B_n \in \mathcal{B}$, $\bigcup_n B_n \in \mathcal{B}$ and

$$X^{-1}\left(\bigcup_n B_n\right) = \bigcup_n X^{-1}(B_n) \in \sigma\left(\{X^{-1}(-\infty, x],\ x \in \mathbb{R}\}\right) \ \Rightarrow\ \bigcup_n B_n \in \mathcal{A}. \tag{19.2.29}$$

Hence, $\mathcal{A}$ is a σ-algebra. □

Remark. A sequence of random variables $(X_n : n \geq 0)$ is often regarded as a process evolving in time. The σ-algebra generated by $X_0, \ldots, X_n$, $\mathcal{F}_n = \sigma(X_0, \ldots, X_n)$ contains those events depending (measurably) on $X_0, \ldots, X_n$ and represents what is known about the process by time n.

Proposition 19.2.10. Let $X_1, X_2, \ldots$ be independent random variables with distribution uniform on $[0, 1]$. Let A_n be the event that a record occurs at time n, that is,

$$X_n > X_m \quad \text{for all } m < n. \tag{19.2.30}$$

Then $A_1, A_2, \ldots$ are independent. Also, with probability one, infinitely many records occur.

Proof. $\mathbb{P}(A_n)$ means the probability that the maximum of n appears at n, then $\mathbb{P}(A_n) = 1/n$. Also

$$A_1 \cap A_2 \cap \cdots \cap A_n \ \Rightarrow\ X_1 < X_2 < \cdots < X_n \tag{19.2.31}$$

which is a increasing order. Then we have $\mathbb{P}(A_1 \cap A_2 \cap A_n) = 1/n!$. Thus, it is obvious that

$$\mathbb{P}(A_1 \cap A_2 \cap A_n) = \prod_n \mathbb{P}(A_n) \ \Rightarrow\ A_1, A_2, \ldots \text{ are independent.} \tag{19.2.32}$$

With Second Borel-Cantelli lemma (Lemma 19.1.25), we have $\sum_n \mathbb{P}(A_n) = \sum_n \frac{1}{n} = \infty$, then $\mathbb{P}(A_n \text{ i.o.}) = 1$. □

19.2.3 Rademacher functions

We continue with the particular choice of probability space $(\Omega, \mathcal{F}, \mathbb{P})$ made in the preceding section. Provided that we forbid infinite sequences of 0's, each $\omega \in \Omega$ has a unique binary expansion

$$\omega = 0.\omega_1\omega_2\omega_3 \ldots \tag{19.2.33}$$

Define random variables $R_n : \Omega \to \{0, 1\}$ by $R_n(\omega) = \omega_n$. Then

$$R_1 = \mathbb{1}_{(\frac{1}{2}, 1]}, \quad R_2 = \mathbb{1}_{(\frac{1}{4}, \frac{1}{2}]} + \mathbb{1}_{(\frac{3}{4}, 1]}, \quad R_3 = \mathbb{1}_{(\frac{1}{8}, \frac{1}{4}]} + \mathbb{1}_{(\frac{3}{8}, \frac{1}{2}]} + \mathbb{1}_{(\frac{5}{8}, \frac{3}{4}]} + \mathbb{1}_{(\frac{7}{8}, 1]}. \tag{19.2.34}$$

These are called the Rademacher functions. The random variables $R_1, R_2, \ldots$ are independent and Bernoulli, that is to say

$$\mathbb{P}(R_n = 0) = \mathbb{P}(R_n = 1) = 1/2. \tag{19.2.35}$$

Let $E = \{0, 1\}^{\mathbb{N}}$ and let $\mathcal{E}$ denote the σ-algebra generated by events of the form

$$A = \{\omega \in E : \omega_1 = y_1, \ldots, \omega_n = y_n\},\ n \in \mathbb{N},\ y_i \in \{0, 1\}. \tag{19.2.36}$$

Let $R = (R_1, \ldots,) \in E$. Then R is a random variable in $(E, \mathcal{E})$. The distribution μ of R is then a probability measure on $(E, \mathcal{E})$, under which the events $\{\omega_n = y_n\}, n \in \mathbb{N}$, are independent. This is the infinite (fair) coin-toss measure.

We now use a trick involving the Rademacher functions to construct on $\Omega = (0, 1]$, not just one random variable, but an infinite sequence of independent random variables with given distribution functions.

Proposition 19.2.11. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be the probability space of Lebesgue measure on the Borel subsets of $(0,1]$. Let $(F_n : n \in \mathbb{N})$ be a sequence of distribution functions. Then there exists a sequence $(X_n : n \in \mathbb{N})$ of independent random variables on $(\Omega, \mathcal{F}, \mathbb{P})$ such that X_n has distribution function $F_{X_n} = F_n$ for all n.

Proof. Choose a bijection $m : \mathbb{N}^2 \to \mathbb{N}$ and set $Y_{k,n} = R_{m(k,n)}$, where R_m is the mth Rademacher function. Set

$$Y_n = \sum_{k=1}^{\infty} 2^{-k} Y_{k,n}. \tag{19.2.37}$$

Then $Y_1, Y_2, \dots$ are independent and, for all n, for $i2^{-k} = 0.y_1 \dots y_k$, we have

$$\mathbb{P}(i2^{-k} < Y_n \leq (i+1)2^{-k}) = \mathbb{P}(Y_{1,n} = y_1, \dots, Y_{k,n} = y_k) = 2^{-k} \tag{19.2.38}$$

so $\mathbb{P}(Y_n \leq x) = x$ for all $x \in (0,1]$. Set

$$G_n(y) = \inf\{x : y \leq F_n(x)\} \tag{19.2.39}$$

then, by Lemma 15.2.10, G_n is Borel and $G_n(y) \leq x$ if and only if $y \leq F_n(x)$. So, if we set $X_n = G_n(Y_n)$, then $X_1, X_2, \dots$ are independent random variables on Ω and

$$\mathbb{P}(X_n \leq x) = \mathbb{P}(G_n(Y_n) \leq x) = \mathbb{P}(Y_n \leq F_n(x)) = F_n(x). \tag{19.2.40}$$

Thus, X_n has distribution function $F_{X_n} = F_n$ for all n. □

19.2.4 Tail events

Definition 19.2.8 (tail σ-algebra)**.** Let $(X_n : n \in \mathbb{N})$ be a sequence of random variables. Define

$$\mathcal{T}_n = \sigma(X_m : m \geq n+1) = \sigma(X_{n+1}, X_{n+2}, \dots), \quad \mathcal{T}_\infty = \bigcap_n \mathcal{T}_n. \tag{19.2.41}$$

Then $\mathcal{T}_\infty$ is a σ-algebra, called the tail σ-algebra of $(X_n : n \in \mathbb{N})$. It contains the events which depend only on the limiting behaviour of the sequence.

Theorem 19.2.12 (Kolmogorov's 0-1 law)**.** Suppose that $(X_n : n \in \mathbb{N})$ is a sequence of independent random variables. Then the tail σ-algebra $\mathcal{T}_\infty$ of $(X_n : n \in \mathbb{N})$ contains only events of probability 0 or 1. Moreover, any $\mathcal{T}_\infty$-measurable random variable is almost surely constant.

Proof. Set $\mathcal{F}_n = \sigma(X_1, \dots, X_n)$. Then $\mathcal{F}_n$ is generated by the π-system of events

$$A = \{X_1 \leq x_1, \dots, X_n \leq x_n\} \tag{19.2.42}$$

whereas $\mathcal{T}_n$ is generated by the π-system of events

$$B = \{X_{n+1} \leq x_{n+1}, \dots, X_{n+k} \leq x_{n+k}\}, \quad k \in \mathbb{N}. \tag{19.2.43}$$

We have $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$ for all such A and B, by independence. Hence $\mathcal{F}_n$ and $\mathcal{T}_n$ are independent, by Theorem 19.1.20 (Independence). It follows that $\mathcal{F}_n$, $n \in \mathbb{N}$ and $\mathcal{T}_\infty$ are independent since $\forall A_n \in \mathcal{F}_n$, $\forall B \in \mathcal{T} \subseteq \mathcal{T}_n$,

$$\mathbb{P}(A_n \cap B) = \mathbb{P}(A_n)\mathbb{P}(B). \qquad \text{(by independence of } \mathcal{F}_n \text{ and } \mathcal{T}_n) \tag{19.2.44}$$

Now $\bigcup_n \mathcal{F}_n$ is a π-system which generates the σ-algebra $\mathcal{F}_\infty = \sigma(X_n : n \in \mathbb{N})$. So by Theorem 19.1.20 again, $\mathcal{F}_\infty$ and $\mathcal{T}_\infty$ are independent, since $\forall A \in \mathcal{F}_\infty$, $\forall B \in \mathcal{T}_\infty$, we can find that $A \in \mathcal{F}_m$ for some $m \in \mathbb{N}$,

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B). \qquad \text{(by independence of } \mathcal{F}_m \text{ and } \mathcal{T}_\infty) \tag{19.2.45}$$

But $T \subseteq \mathcal{F}_\infty$. So, if $A \in \mathcal{T}_\infty$,

$$\mathbb{P}(A) = \mathbb{P}(A \cap A) = \mathbb{P}(A)\mathbb{P}(A) \;\Rightarrow\; \mathbb{P}(A) \in \{0,1\}. \tag{19.2.46}$$

Finally, if Y is any $\mathcal{T}_\infty$-measurable random variable, then $F_Y(y) = \mathbb{P}(Y \le y)$ takes values in $\{0,1\}$, so $\mathbb{P}(Y = c) = 1$, where $c = \inf\{y : F_Y(y) = 1\}$. □

Example 19.2.13. Let U be a uniform random variable on $(0,1)$ (see Definition 19.8.4) and let R_n be its binary expansion. Then R_n are independent and identically distributed (i.i.d.). The strong law of large numbers (Theorem 19.9.9) applies here to show that $n^{-1}\sum_{i=1}^n R_i$ converges to $1/2$, almost surely. Reformulating this using the canonical probability space $(\Omega, \mathcal{F}, \mathbb{P})$,

$$\mathbb{P}\left(\left\{\omega \in (0,1] : \frac{|\{k \le n : \omega_k = 1\}|}{n} \to \frac{1}{2}\right\}\right) = \mathbb{P}\left(\frac{R_1 + \cdots + R_n}{n} \to \frac{1}{2}\right) = 1. \tag{19.2.47}$$

This is called Borel's normal number theorem (Theorem 3.6.2).

19.2.5 Large values in sequences of IID random variables

Consider a sequence $(X_n : n \in \mathbb{N})$ of independent random variables, all having the same distribution function F. Assume that $F(x) < 1$ for all $x \in \mathbb{R}$. Then, almost surely, the sequence $(X_n : n \in \mathbb{N})$ is unbounded above, so $\limsup_n X_n = \infty$. A way to describe the occurrence of large values in the sequence is to find a function $g : \mathbb{N} \to (0,\infty)$ such that, almost surely,

$$\limsup_n X_n / g(n) = 1. \tag{19.2.48}$$

Example 19.2.14. We now show that $g(n) = \log n$ is the right choice when $F(x) = 1 - e^{-x}$. The same method adapts to other distributions.

Fix $\alpha > 0$ and consider the event $A_n = \{X_n \ge \alpha \log n\}$. Then

$$\mathbb{P}(A_n) = e^{-\alpha \log n} = n^{-\alpha}, \tag{19.2.49}$$

so the series $\sum_n \mathbb{P}(A_n)$ converges if and only if $\alpha > 1$. By the Borel-Cantelli lemmas (Lemma 15.1.13, 19.1.25), we deduce that, for all $\varepsilon > 0$,

$$\mathbb{P}(X_n/\log n \ge 1 \text{ i.o.}) = 1, \qquad \mathbb{P}(X_n/\log n \ge 1 + \varepsilon \text{ i.o.}) = 0. \tag{19.2.50}$$

Hence, almost surely,

$$\limsup_n X_n / \log n = 1. \tag{19.2.51}$$

Example 19.2.15. Let $X_1, X_2, \ldots$ be independent $\mathcal{N}(0,1)$ random variables. Let

$$A = \left\{\omega : \limsup_n \left\{X_n(\omega) \Big/ \sqrt{2\log n} \ge 1\right\}\right\}, \quad B = \left\{\omega : \limsup_n \left\{X_n(\omega) \Big/ \sqrt{2\log n} > 1\right\}\right\} \tag{19.2.52}$$

We want to show that $\mathbb{P}(A) = 1$ and $\mathbb{P}(B) = 0$. First, consider the event $\left\{X_n(\omega)\big/\sqrt{2\log n} \ge \alpha\right\}$

$$\begin{aligned}
\sum_n \mathbb{P}\left(X_n(\omega) \Big/ \sqrt{2\log n} \ge \alpha\right) &= \sum_n \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \mathbb{1}_{\left\{x \ge \alpha\sqrt{2\log n}\right\}} dx \qquad \text{(standard Gaussian density (Definition 19.5.2))} \\
&= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \sum_n \mathbb{1}_{\left\{n \le \exp\left\{\frac{1}{2}\frac{x^2}{\alpha^2}\right\}\right\}} dx \qquad \text{(by Fubini's theorem (Theorem 15.3.33))} \\
&= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \left\lfloor e^{\frac{1}{2}x^2/\alpha^2} \right\rfloor dx < \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2\left(1-\frac{1}{\alpha^2}\right)} dx < \infty \;\Leftrightarrow\; \alpha > 1.
\end{aligned}$$

Thus, let $\alpha = 1$,

$$\begin{aligned}
\sum_n \mathbb{P}\left(X_n(\omega) \Big/ \sqrt{2\log n}\right) &= \sum_n \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \mathbb{1}_{\left\{x \ge \sqrt{2\log n}\right\}} dx = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \left\lfloor e^{\frac{1}{2}x^2} \right\rfloor dx \\
&> \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \left(e^{\frac{1}{2}x^2} - 1\right) dx = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dx - 1 = \infty.
\end{aligned}$$

With Second Borel-Cantelli lemma (Lemma 19.1.25), we have $\mathbb{P}(A) = 1$.

Also, we have $\alpha = 1 + 1/m,\ m \in \mathbb{N}$, $\sum_n \mathbb{P}\left(X_n(\omega)\big/\sqrt{2\log n} \ge \alpha\right) < \infty$. Then by First Borel-Cantelli lemma (Lemma 15.1.13),

$$\mathbb{P}\left(\left\{\omega : X_n(\omega) \Big/ \sqrt{2\log n} \ge 1 + 1/m\right\} \text{ i.o.}\right) = 0 \tag{19.2.53}$$

and since $B = \bigcup_{m\in\mathbb{N}} \left(\left\{\omega : X_n(\omega)\big/\sqrt{2\log n} \geq 1 + 1/m\right\} \text{ i.o.}\right)$, we have

$$\mathbb{P}(B) \leq \sum_n \mathbb{P}\left(\left\{\omega : X_n(\omega)\Big/\sqrt{2\log n} \geq 1 + 1/m\right\} \text{ i.o.}\right) = 0 \;\Rightarrow\; \mathbb{P}(B) = 0. \tag{19.2.54}$$

Thus, $\limsup_n (X_n/\sqrt{2\log n}) = 1$ a.s.

19.2.6 Convergence almost surely and convergence in probability

Recall Definitions 15.2.5 and 15.2.6, we have the following two definitions.

Definition 19.2.9. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. We say a sequence of random variables $(X_n : n \in \mathbb{N})$ converges to X a.s. if

$$\mathbb{P}\left(\{\omega \in \Omega : X_n(\omega) \nrightarrow X(\omega)\}\right) = 0 \quad \Leftrightarrow \quad \mathbb{P}\left(\{\omega \in \Omega : X_n(\omega) \to X(\omega)\}\right) = 1, \qquad \text{denoted as } X_n \to X \text{ a.s.} \tag{19.2.55}$$

Definition 19.2.10. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and X be a random variable. We say a random variable Y is a version of X if $X = Y$ a.s.

Definition 19.2.11. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. For a sequence of random variables $(X_n : n \in \mathbb{N})$, we have that

$$\mathbb{P}\left(\{\omega \in \Omega : |X_n(\omega) - X(\omega)| > \varepsilon\}\right) \to 0, \quad \text{for all } \varepsilon > 0, \tag{19.2.56}$$

then we say X_n converges to X in probability, denoted as $X_n \xrightarrow{p} X$.

Recall Theorem 15.2.14, we have particular theorem for probability.

Theorem 19.2.16. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $(X_n : n \in \mathbb{N})$ be a sequence of random variables.

(i) If $X_n \to 0$ a.s. then $X_n \xrightarrow{p} 0$.

(ii) If $X_n \xrightarrow{p} 0$ then $X_{n_k} \to 0$ a.s. for some subsequence (n_k).

For more general case, we define convergence in probability by

Definition 19.2.12. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. For a sequence of random variables $(X_n : n \in \mathbb{N})$ on metric space (Ω, d), we have that

$$\mathbb{P}\left(\{\omega \in \Omega : d\left(X_n(\omega), X(\omega)\right) > \varepsilon\}\right) \to 0, \quad \text{for all } \varepsilon > 0, \tag{19.2.57}$$

then we say X_n converges to X in probability, denoted as $X_n \xrightarrow{p} X$.

Recalling Propsoition 15.2.15, we have

Proposition 19.2.17 (uniqueness of limit of convergence in probability)**.** Let $(X_n)_{n\in\mathbb{N}}$ be a sequence of random variables and X, Y be random variables. If $X_n \xrightarrow{p} X$ and $X_n \xrightarrow{p} Y$,

$$X = Y \text{ a.s.} \quad \text{ i.e., } \mathbb{P}\left(X = Y\right) = 1. \tag{19.2.58}$$

19.3 Expectation and Convergence in $\mathcal{L}^p\left(\Omega, \mathcal{F}, \mathbb{P}\right)$

19.3.1 Expectation

Recall Definition 15.3.6, in particular,

Definition 19.3.1. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. We shall define, where possible, for a random variable $X : \Omega \to [-\infty, \infty]$, the expectation of X, to be denoted

$$\mathbb{E}(X) = \int_\Omega X d\mathbb{P} = \int_\Omega X(\omega)\mathbb{P}(d\omega). \tag{19.3.1}$$

Remark. For any random variable X denote by $X^+ = \max\{X, 0\}$, the positive part of X, and $X^- = \max\{-X, 0\}$, the negative part of X are non-negative random variables, for which so that $X = X^+ - X^-$ and $|X| = X^+ + X^-$. Provided not both $\mathbb{E}X^+ = \infty$ and $\mathbb{E}X^- = \infty$, we define the expectation of X to be

$$\mathbb{E}X = \mathbb{E}X^+ - \mathbb{E}X^-, \tag{19.3.2}$$

if both $\mathbb{E}X^+$ and $\mathbb{E}X^-$ are infinite then the expectation of X is not defined. In the following, when we write $\mathbb{E}X$ for a random variable X, it may be assumed that the expectation of X is well defined (see Definition 15.3.5).

Recall Definition 15.3.2, Theorem 15.3.7 and Theorem 15.3.10, we have

Proposition 19.3.1 (properties of expectation)**.** Let X, Y be random variables and $\mathbb{E}X$, $\mathbb{E}Y$ are well-defined. Then

(i) For the indicator of any event $A \subseteq \Omega$ we have $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$.

(ii) If $X \geq 0$, then $\mathbb{E}X \geq 0$, and $\mathbb{E}X = 0$ implies that $X = 0$ a.s..

(iii) If $X, Y \geq 0$ and $a, b \in [0, \infty]$, then $\mathbb{E}(aX + bY) = a\mathbb{E}X + b\mathbb{E}Y$.

(iv) If X, Y are integrable and $a, b \in \mathbb{R}$, $\mathbb{E}(aX + bY) = a\mathbb{E}X + b\mathbb{E}Y$.

Definition 19.3.2 (moment of random variable)**.** For a random variable X, the expected values of powers of X are known as moments of X, thus $\mathbb{E}(X^r)$ (assuming it is well defined) is the rth moment of X and $\mathbb{E}(|X|^r)$ is the rth absolute moment of X.

Example 19.3.2. Let $X_1, X_2, \ldots$ be random variables with

$$X_n = \begin{cases} n^2 - 1 & \text{with probability } 1/n^2 \\ -1 & \text{with probability } 1 - 1/n^2 \end{cases} \tag{19.3.3}$$

Thus,

$$\mathbb{E}X_n = (n^2 - 1)\frac{1}{n^2} + (-1)\left(1 - \frac{1}{n^2}\right) = 0 \;\Rightarrow\; \mathbb{E}\left(\frac{X_1 + \cdots + X_n}{n}\right) = 0 \tag{19.3.4}$$

Also, we consider the event

$$\left\{\frac{X_1 + \cdots + X_n}{n} \nrightarrow -1\right\} = \left\{X_n = n^2 - 1 \;\text{ i.o.}\right\} \tag{19.3.5}$$

However, with First Borel-Cantelli lemma (Lemma 19.1.24), we have

$$\sum_n \mathbb{P}(X_n = n^2 - 1) = \sum_n \frac{1}{n^2} < \infty \quad \Rightarrow \quad \mathbb{P}\left(X_n = n^2 - 1 \;\text{ i.o.}\right) = 0. \tag{19.3.6}$$

Example 19.3.3 (Another proof of inclusion-exclusion formula.)**.** For events $A_1, \ldots, A_n$, use $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$ (Definition 15.3.2 and Proposition 19.3.1), the expression for the product of indicators (Proposition 15.2.4) and linearity of the expectation (Theorem 15.3.10.(i)),

$$\begin{aligned}
\mathbb{P}(A_1 \cup \cdots \cup A_n) &= \mathbb{E}(\mathbb{1}_{A_1 \cup A_2 \cup \cdots \cup A_n}) = \mathbb{E}\left(1 - \prod_{i=1}^n (1 - \mathbb{1}_{A_i})\right) \\
&= \mathbb{E}\left(\sum_i \mathbb{1}_{A_i} - \sum_{i_1 < i_2} \mathbb{1}_{A_{i_1} \cap A_{i_2}} + \sum_{i_1 < i_2 < i_3} \mathbb{1}_{A_{i_1} \cap A_{i_2} \cap A_{i_3}} - \cdots + (-1)^{n-1} \mathbb{1}_{A_1 \cap \cdots \cap A_n}\right) \\
&= \sum_i \mathbb{E}(\mathbb{1}_{A_i}) - \sum_{i_1 < i_2} \mathbb{E}\left(\mathbb{1}_{A_{i_1} \cap A_{i_2}}\right) + \cdots + (-1)^{n-1} \mathbb{E}\left(\mathbb{1}_{A_1 \cap \cdots \cap A_n}\right) \\
&= \sum_i \mathbb{P}(A_i) - \sum_{i_1 < i_2} \mathbb{P}\left(A_{i_1} \cap A_{i_2}\right) + \cdots + (-1)^{n-1} \mathbb{P}(A_1 \cap \cdots \cap A_n),
\end{aligned}$$

which is the required expression for the inclusion-exclusion formula.

Example 19.3.4. Let X be a non-negative integer-valued random variable. We have

$$\sum_{n=1}^\infty \mathbb{P}(X \geq n) = \sum_{n=1}^\infty \sum_{k=n}^\infty \mathbb{P}(X = k) = \sum_{k=1}^\infty \sum_{n=1}^k \mathbb{P}(X = k) = \sum_{k=1}^\infty k\mathbb{P}(X = k) = \mathbb{E}(X). \tag{19.3.7}$$

If $\mathbb{E}(X) = \infty$, let $X_1, X_2, \dots$ is a sequence of independent random variables with the same distribution as X, then let $A_n = \{X_n \geq n\}$. Since $\sum_{n=1}^{\infty} \mathbb{P}(A_n) = \mathbb{E}(X) = \infty$, By the second Borel-Cantelli lemma (Lemma 19.1.25), we have then

$$\mathbb{P}(A_n \text{ i.o.}) = \mathbb{P}(X_n \geq n \text{ i.o.}) = 1 \;\Rightarrow\; \limsup(X_n/n) \geq 1 \quad \text{a.s.} \tag{19.3.8}$$

Hence, if $\mathbb{E}(X) = \infty$, $\mathbb{E}(X/k) = \infty$, with the same argument we have

$$\limsup(X_n/(kn)) \geq 1 \quad \text{a.s.} \;\Rightarrow\; \limsup(X_n/n) \geq k \quad \text{a.s.} \;\Rightarrow\; \limsup(X_n/n) = \infty \quad \text{a.s.} \tag{19.3.9}$$

Now suppose that $Y_1, Y_2, \dots$ is any sequence of independent identically distributed random variables with $\mathbb{E}|Y_1| = \infty$. Now let $X_n = |Y_n|$. We have

$$\limsup(|Y_n|/n) = \infty \quad \text{a.s.} \tag{19.3.10}$$

Also, we know that

$$|Y_n| \leq |Y_1 + \cdots + Y_n| + |Y_1 + \cdots + Y_{n-1}| \;\Rightarrow\; \limsup(|Y_1 + \cdots + Y_n|/n) \geq \frac{1}{2} \limsup(|Y_n|/n) = \infty \quad \text{a.s.} \tag{19.3.11}$$

Proposition 19.3.5. Let X be a random variable and let $1 \leq p < q < \infty$. Then

$$\mathbb{E}(|X|^p) = \int_0^{\infty} p\lambda^{p-1}\mathbb{P}(|X| \geq \lambda)d\lambda \qquad \text{and} \qquad X \in \mathcal{L}^q(\mathbb{P}) \;\Rightarrow\; \mathbb{P}(|X| \geq \lambda) = O(\lambda^{-q}) \;\Rightarrow\; X \in \mathcal{L}^p(\mathbb{P}). \tag{19.3.12}$$

Remark. We can get the special version of Proposition 15.4.5

Proof. We have

$$\begin{aligned}
\int_0^{\infty} p\lambda^{p-1}\mathbb{P}(|X| \geq \lambda)d\lambda &= \int_0^{\infty} p\lambda^{p-1}\mathbb{E}(\mathbb{1}_{\{|X|\geq\lambda\}})\, d\lambda = \int_0^{\infty} p\lambda^{p-1} \int_{\Omega} \mathbb{1}_{\{\omega' : |X(\omega')| \geq \lambda\}}(\omega)\, \mathbb{P}(d\omega)\, d\lambda \\
&= \int_{\Omega}\int_0^{\infty} p\lambda^{p-1}\mathbb{1}_{\{\omega' : |X(\omega')| \geq \lambda\}}(\omega)\, d\lambda\, \mathbb{P}(d\omega) \qquad \text{(Fubini theorem, Theorem 15.3.33)} \\
&= \int_{\Omega}\int_0^{|X(\omega)|} p\lambda^{p-1}\, d\lambda\, \mathbb{P}(d\omega) = \int_{\Omega} |X(\omega)|^p\; \mathbb{P}(d\omega) = \mathbb{E}(|X|^p)
\end{aligned}$$

Now if $X \in L^q(\mathbb{P})$, $\mathbb{E}(|X|^q) < \infty$ by definition. We want to be able to say that since

$$\int_0^{\infty} p\lambda^{q-1}\lambda^{-q}\, d\lambda = \infty$$

we must have that $\mathbb{P}(|X| \geq \lambda) = \mathcal{O}(\lambda^{-q})$. To make this argument rigorous, we first note that if $\mathbb{P}(|X| \geq \lambda) \neq \mathcal{O}(\lambda^{-q})$, then for each $n \in \mathbb{N}$, there exits λ_n such that $\mathbb{P}(|X| \geq \lambda_n) > n\lambda_n^{-q}$. Since $\mathbb{P}(|X| \geq \lambda)$ is non-increasing as a function of λ, this means that

$$\mathbb{P}(|X| \geq \lambda) > \lambda^{-q} \quad \text{for} \quad \lambda \in [\lambda_n^-, \lambda_n] \quad n = 1, 2, \dots$$

where $\lambda_n^- := \frac{\lambda_n}{n^{1/q}}$. Thus, for all $n \in \mathbb{N}$, we have that

$$\mathbb{E}(|X|^q) > q\int_{\lambda_n^-}^{\lambda_n} \lambda^{-1}\, d\lambda = \log(n)$$

and so $\mathbb{E}(|X|^q) = \infty$. Alternatively, we could have used Chebyshev's inequality.

Now if $\mathbb{P}(|X| \geq \lambda) \leq C\lambda^{-q}$, some C, then

$$\mathbb{E}(|X|^p) \leq C\int_0^{\infty} p\lambda^{p-1}\lambda^{-q}\, d\lambda < \infty.$$

This is special of Proposition 15.3.38. □

19.3.2 Convergence Theorems for probability

From measure theory, we have the following special theorems:

Theorem 19.3.6 (monotone convergence theorem)**.** Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Let X be a non-negative random variable and $(X_n : n \in \mathbb{N})$ be a sequence of random variables, with $X_n \geq 0$ a.s. Then

$$X_n \uparrow X \text{ a.s. } \Rightarrow \mathbb{E}(X_n) \uparrow \mathbb{E}(X). \tag{19.3.13}$$

Lemma 19.3.7 (Fatou's lemma)**.** Let $(X_n)_{n\in\mathbb{N}}$ be a sequence of non-negative random variables. Then

$$\mathbb{E}(\liminf X_n) \leq \liminf \mathbb{E}(X_n). \tag{19.3.14}$$

(Inverse Fatou's Lemma). Additionally, if there exists a non-negative integrable random variable Y such that $X_n \leq Y$ for all n, then

$$\mathbb{E}(\limsup X_n) \geq \limsup \mathbb{E}(X_n). \tag{19.3.15}$$

Theorem 19.3.8 (dominated convergence theorem)**.** Let $(\Omega, \mathcal{F}, \mathbb{P})$ be probability space. Let X be a random variable and let $(X_n : n \in \mathbb{N})$ be a sequence of such random variables. Suppose that $X_n(\omega) \to X(\omega)$ a.s. and that $|X_n| \leq Y$ a.s. for all n, for some integrable random variable Y. Then X_n and X are integrable, for all n and $\mathbb{E}X_n \to \mathbb{E}X$.

Remark. Actually, dominated convergence theorem also implies that $X_n \to X$ in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ by Lemma 19.3.11.

Example 19.3.9. Let $(X_n : n \in \mathbb{N})$ be an identically distributed sequence in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. for $\varepsilon > 0$,

$$n\mathbb{P}(|X| > \epsilon\sqrt{n}) = n\mathbb{P}\left(\frac{X_1^2}{\epsilon^2} > n\right) = \mathbb{E}\left(n\mathbb{1}\left(\left\{\tfrac{X_1^2}{\epsilon^2} > n\right\}\right)\right) \leq \frac{1}{\epsilon^2}\mathbb{E}(X_1^2) < \infty \tag{19.3.16}$$

Now $n\mathbb{1}\left(\left\{\frac{X_1^2}{\epsilon^2} > n\right\}\right) \to 0$ as $n \to \infty$, so by dominated convergence, $n\mathbb{P}(|X| > \epsilon\sqrt{n}) \to 0$.

$$\mathbb{P}\left(n^{-\frac{1}{2}} \max_{k\leq n} |X_k| > \epsilon\right) = \mathbb{P}\left(\bigcup_{k\leq n} \{|X_k| > \epsilon\sqrt{n}\}\right) \leq n\,\mathbb{P}(|X| > \epsilon\sqrt{n}) \to 0 \qquad \left(n^{-\frac{1}{2}} \max_{k\leq n} |X_k| \xrightarrow{p} 0\right) \tag{19.3.17}$$

where we have used countable subadditivity (Lemma 15.1.6 since $\mathbb{P}$ is a measure) and the fact that the X_n are i.i.d. in the final line.

Theorem 19.3.10 (bounded convergence theorem)**.** Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a measure space. Let X be a random variable and let $(X_n : n \in \mathbb{N})$ be a sequence of such functions. Suppose $X_n \to X$ in probability and $|X_n| \leq M$ for all n, for some constant $M < \infty$. Then $\mathbb{E}\,|X_n - X| \to 0$, which implies that $\mathbb{E}X_n \to \mathbb{E}X$.

Lemma 19.3.11 (Scheffé's Lemma)**.** let X and $(X_n : n \in \mathbb{N})$ integrable random variables. Suppose that $X_n(\omega) \to X(\omega)$ a.s., then $\mathbb{E}\,|X_n - X| \to 0$ if and only if $\mathbb{E}\,|X_n| \to \mathbb{E}\,|X|$.

Proposition 19.3.12. For independent random variables X and Y, $\mathbb{E}|XY| = \mathbb{E}|X|\mathbb{E}|Y|$ and that if both X and Y are integrable then

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y). \tag{19.3.18}$$

Proof. Let X and Y be random variables. If $X = \mathbb{1}_A$ and $Y = \mathbb{1}_B$, then

$$\mathbb{E}(XY) = \mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B) = \mathbb{E}(X)\mathbb{E}(Y). \tag{19.3.19}$$

The identity extends to simple random variables by linearity, if $X = \sum_{k=1}^{m} a_k \mathbf{1}_{A_k}$ and $Y = \sum_{j=1}^{n} b_j \mathbf{1}_{B_j}$ (A_k and B_j are disjoint respectively),

$$\mathbb{E}(XY) = \sum_{k=1}^{m}\sum_{j=1}^{n} a_k b_j \mathbb{P}\left(A_k \cap B_j\right) = \sum_{k=1}^{m}\sum_{j=1}^{n} a_k b_j \mathbb{P}(A_k)\mathbb{P}(B_j) = \mathbb{E}(X)\mathbb{E}(Y). \tag{19.3.20}$$

then it extends to non-negative random variables by monotone convergence theorem (Theorem 19.3.6, by using the approximation $X_n = 2^{-n}\lfloor 2^n X \rfloor$).

For X, Y integrable we have $\mathbb{E}(|XY|) = \mathbb{E}(|X|)\mathbb{E}(|Y|) < \infty \Rightarrow XY$ is integrable. Hence, as X^+ and Y are independent, $\mathbb{E}(XY) = \mathbb{E}\left((X^+ - X^-)(Y^+ - Y^-)\right) = \left(\mathbb{E}(X^+) - \mathbb{E}(X^-)\right)\left(\mathbb{E}(Y^+) - \mathbb{E}(Y^-)\right) = \mathbb{E}(X)\mathbb{E}(Y)$. □

Then, we have the following proposition by extending to n random variables.

Proposition 19.3.13. For independent random variables $X_1, \ldots, X_n$, $\mathbb{E}\left(\prod_{i=1}^n |X_i|\right) = \prod_{i=1}^n \mathbb{E}\,|X_i|$ and that if all X_i are integrable then

$$\mathbb{E}\left(\prod_{i=1}^n X_i\right) = \prod_{i=1}^n \mathbb{E}(X_i). \tag{19.3.21}$$

19.3.3 Transformations of expectations and density function

Recall Definition 19.2.2, Proposition 15.3.21, 15.3.22, we have the following propositions:

Theorem 19.3.14. Let $(\Omega, \mathcal{F})$ and $(G, \mathcal{G})$ be measurable spaces and let $X : \Omega \to G$ be a random variable. Given a probability $\mathbb{P}$ on $(\Omega, \mathcal{F})$, define $\mu_X = \mathbb{P} \circ X^{-1}$, the image measure on $(G, \mathcal{G})$. Then, for all non-negative measurable functions $g : G \to [0, \infty]$,

$$\mu_X(g) = \mathbb{E}(g \circ X) = \mathbb{E}(g(X)). \tag{19.3.22}$$

Theorem 19.3.15 (density function)**.** Let $(\mathbb{R}^n, \mathcal{B}(\mathbb{R}^n), \mu)$ be a Lebesgue measure space and let $f_X : \mathbb{R}^n \to [0, \infty]$ be a non-negative μ-integrable function on $\mathbb{R}^n$. For real-valued random variable $X \in \mathbb{R}^n$, define

$$\mu_X(A) = \mathbb{P}(X \in A) := \int_{\mathbb{R}^n} \mathbb{1}_A(x) f_X(x) \mu(dx) = \int_A f_X(x) dx, \tag{19.3.23}$$

$A \in \mathcal{B}(\mathbb{R}^n)$ and $\mathbb{P}(\mathbb{R}^n) = 1$. Then $\mathbb{P}$ is a probablity on $\mathcal{B}(\mathbb{R}^n)$ and, for all non-negative measurable functions $g : \mathbb{R}^n \to [0, \infty]$,

$$\mu_X(g) = \int_{\mathbb{R}^n} g(x) f_X(x) dx. \tag{19.3.24}$$

f_X is called the density function of random variable X. As $\mathbb{P}(\Omega) = 1 < \infty$, we have that f is Lebesgue-integrable a.e. by Theorem 15.3.23.

Proposition 19.3.16. Combine the above results

$$\int_\Omega g(X(\omega)) \mathbb{P}(d\omega) = \mathbb{E}(g(X)) = \mu_X(g) = \int_{\mathbb{R}^n} g(x) f_X(x) dx. \tag{19.3.25}$$

Example 19.3.17. Let X be an exponential random variable. That is, its distribution function satisfies $F(t) = 1 - e^{-t}$, $t \geq 0$. Therefore, by the fundamental theorem of calculus (Theorem 15.3.26),

$$\mathbb{P}(X \leq t) = 1 - e^{-t} = \int_0^t e^{-x} dx = \int_0^\infty e^{-x} \mathbb{1}_{[0,t]}(x) dx. \tag{19.3.26}$$

For any interval $(a, b]$, the set $\{(a, b], a < b\}$ is π-system and

$$\mathbb{P}(X \in (a, b]) = \underbrace{\mathbb{P}(X \in (0, b]) - \mathbb{P}(X \in (0, a])}_{\mathbb{P} \text{ is a measure}} = F(b) - F(a) = \int_a^b f(x) dx = \int_0^\infty f(x) \mathbb{1}_{(a,b]} dx \tag{19.3.27}$$

where $f_X(x) = e^{-x} \mathbb{1}_{[0,\infty)}(x)$. Then by uniqueness of extension (Lemma 15.1.18), it follows that for all Borel set A,

$$\mathbb{P}(X \in A) = \int f_X(x) \mathbb{1}_A(x) dx. \tag{19.3.28}$$

Note that F need not differentiate to f everywhere (e.g. uniform distribution in $[a, b]$), all that is required is that f integrate properly (equation (19.3.28)). On the other hand, if F does differentiate to f and f is continuous, it follows by the fundamental theorem of calculus (Theorem 15.3.26) that f is indeed a density for F Billingsley [4].

Thus μ_X has a density function f_X. Hence, by Proposition 15.3.21 and 15.3.22,

$$\mathbb{E}(X^2) = \int x^2 f_X(x) dx = \int_0^\infty x^2 e^{-x} dx = \Gamma(3) = 2. \tag{19.3.29}$$

Proposition 19.3.18. Let μ and ν be probability measures on $(E, \mathcal{E})$ and suppose that, for some measurable function $f : E \to [0, R]$,

$$\nu(A) = \int_A f d\mu, \quad A \in \mathcal{E}. \tag{19.3.30}$$

Let $(X_n)_{n\in\mathbb{N}}$ be a sequence of independent random variables in E with law μ and let $(U_n)_{n\in\mathbb{N}}$ be a sequence of independent $U[0,1]$ random variables. Set

$$T = \min\{n \in \mathbb{N} : RU_n \le f(X_n)\}, \quad Y = X_T. \tag{19.3.31}$$

Then Y has law ν.

Remark. This is important in applications, where one wishes to simulate a random variable whose density function is difficult to integrate numerically.

Proof. To make this question work, we shall assume that $f(X_1)$ is positive with positive probability, to ensure that

$$\{n \in \mathbb{N} : RU_n \le f(X_n)\} \neq \emptyset \quad \text{a.s.}$$

We may define T as taking the value ∞ and Y in an arbitrary way on the null set for which equality holds in the above. Then, for any $A \in \mathcal{E}$,

$$\mathbb{P}(Y \in A) = \mathbb{P}(X_T \in A) = \sum_{n\in\mathbb{N}} \mathbb{P}(X_n \in A, T = n) = \sum_{n\in\mathbb{N}} \mathbb{P}(X_n \in A, RU_n \le f(X_n), T \ge n) \tag{19.3.32}$$

since $\{RU_n \le f(X_n)\} = \{T \le n\}$. But

$$\{T \ge n\} = \bigcup_{m<n} \{RU_m > f(X_m)\}$$

Thus the events $\{X_n \in A, RU_n \le f(X_n)\}$ and $\{T \ge n\}$ are independent. Therefore, taking $\mathbb{E}(T) = C$, say, we have

$$\begin{aligned}
\mathbb{P}(Y \in A) =& C\,\mathbb{P}(X_1 \in A, RU_1 \le f(X_1)) \\
=& C \int_E \int_0^1 \mathbb{1}\{(x', u') : x' \in A, Ru' \le f(x')\}(x, u)\, du\, \mu(dx) \\
=& \frac{C}{R} \int_E f \mathbb{1}_A d\mu = \frac{C}{R}\nu(A)
\end{aligned}$$

In particular,

$$1 = \mathbb{P}(Y \in E) = \frac{C}{R}\nu(E)$$

But ν is a probability measure so $\frac{C}{R} = 1$, and $\mathbb{P}(Y \in A) = \nu(A)$ as required. □

Now we give the joint distribution function and joint density function. To start with, to keep the notation simpler, consider just the case of two random variables. Then these definitions can be extended to multi-dimensional case.

Definition 19.3.3 (joint distribution function, joint density function, marginal probability density functions)**.** The joint distribution function of $X \in \mathbb{R}^m$ and $Y \in \mathbb{R}^n$ is

$$F(x, y) = \mu_{X,Y} := \mu = \mathbb{P}\left(X \le x, Y \le y\right), \quad x \in \mathbb{R}^m, y \in \mathbb{R}^n, \tag{19.3.33}$$

so that $F : \mathbb{R}^{m+n} \to [0, 1]$. If there exists a Lebesgue-integrable (μ-integrable) function $f(\cdot, \cdot)$ a.e. (by Theorem 19.3.15) with

$$F(x, y) = \int_{Y\le y} \int_{X\le x} f(x, y)dxdy, \tag{19.3.34}$$

so that $dF(x, y) = f(x, y)dxdy := f_{X,Y}(x, y)dxdy$. Then f is the joint probability density function of X and Y.

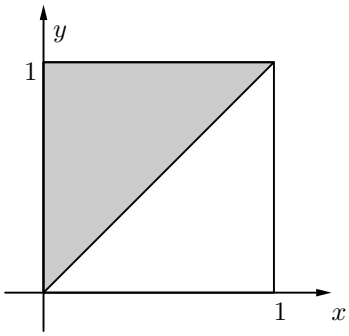
Furthermore,

$$f_X(x) = \int_{\mathbb{R}^n} f_{X,Y}(x, y)dy, \qquad f_Y(y) = \int_{\mathbb{R}^m} f_{X,Y}(x, y)dx, \tag{19.3.35}$$

are the marginal density functions of X and Y, respectively. Note that the marginal density function are well-definied and integrable (with respect to Lebesgue-dx or Lebesgue-dy a.e.) by Fubini theorem (Theorem 15.3.33.(ii).(a))

Example 19.3.19. Consider the joint density for X and Y given by

$$f(x,y) = \begin{cases} 8xy & 0 \le x \le y \le 1, \\ 0 & \text{otherwise.} \end{cases}$$



Here, (X, Y) are distributed over the upper half of the unit square as illustrated in the diagram. You should check that this is indeed a joint p.d.f. in that it integrates to 1 over the region.

We now compute the marginal densities of X and Y,

$$f_X(x) = \int_x^1 8xy dy = 4x(1-x^2) \quad \text{and} \quad f_Y(y) = \int_0^y 8xy dx = 4y^3, \tag{19.3.36}$$

for $0 \le x \le 1$ and $0 \le y \le 1$. Calculate that

$$\mathbb{E}X = \int_0^1 x f_X(x) dx = \int_0^1 4x^2(1-x^2) dx = 4\left(\frac{1}{3} - \frac{1}{5}\right) = \frac{8}{15} \tag{19.3.37}$$

and similarly $\mathbb{E}Y = \frac{4}{5}$.

19.3.4 Inequalities and orthogonal projection

Apply Definition 15.4.1, 15.4.2, Theorem 15.4.2, 15.4.4, 15.4.6, 15.4.8 in probability space, we have

Theorem 19.3.20 (Markov's inequality)**.** If X is any random variable and $a > 0$, then

$$\mathbb{P}(|X| \ge a) \le \frac{\mathbb{E}|X|}{a}. \tag{19.3.38}$$

Theorem 19.3.21 (Chebyshev's inequality)**.** If X is any random variable and $a > 0$, then

$$\mathbb{P}(|X - \mathbb{E}(X)| \ge a) \le \frac{\mathrm{Var}(X)}{a^2}. \tag{19.3.39}$$

Theorem 19.3.22 (Jensen's inequality)**.** For probability space $(\Omega, \mathcal{F}, \mathbb{P})$, let X be an integrable function with values in I and let $f : I \to \mathbb{R}$ be convex. Then $\mathbb{E}(f(X))$ is well defined and

$$\mathbb{E}(f(X)) \ge f(\mathbb{E}(X)). \tag{19.3.40}$$

The equality holds when f is not strictly convex, e.g. when it is a straight line, or when X follows a degenerate distribution, i.e. $X = \mathbb{E}X$ a.s..

Example 19.3.23 (arithmetic-geometric mean inequality)**.** For positive real numbers $x_1, \ldots, x_n$,

$$\left(\prod_{i=1}^n x_i\right)^{1/n} \le \frac{1}{n}\sum_{i=1}^n x_i. \tag{19.3.41}$$

This follows by Jensen's inequality (Theorem 19.3.22) applied to the convex function $f(x) = -\log x$, and the random variable X which takes the value x_i with probability $\frac{1}{n}$, so that

$$-\frac{1}{n}\sum_{i=1}^n \log x_i = \mathbb{E}(-\log(X)) \ge -\log(\mathbb{E}X) = -\log\left(\frac{1}{n}\sum_{i=1}^n x_i\right) \tag{19.3.42}$$

from which we see that

$$\log\left(\left(\prod_{i=1}^{n} x_i\right)^{1/n}\right) \leq \log\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right), \tag{19.3.43}$$

which gives the result, since log is an increasing function.

Theorem 19.3.24 (Hölder's inequality)**.** Let $p, q \in [1, \infty]$ be conjugate indices. Then, for all random variables $X \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ and $Y \in \mathcal{L}^q(\Omega, \mathcal{F}, \mathbb{P})$, we have

$$\mathbb{E}(|XY|) \leq \left(\mathbb{E}\,|X|^p\right)^{1/p} \left(\mathbb{E}\,|Y|^q\right)^{1/q}. \tag{19.3.44}$$

(i) Hölder's inequality becomes an equality if and only if $|X|^p$ and $|Y|^q$ are linearly dependent in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, i.e., for $X \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ and $Y \in \mathcal{L}^q(\Omega, \mathcal{F}, \mathbb{P})$, there exist real number $a, b \geq 0$ such that $a\,|X|^p = b\,|Y|^q$ a.s..

(ii) For $p, q \in \{1\} \cup \{\infty\}$, Hölder's inequality becomes an equality if and only if $p = 1$ and $Y = \|Y\|_\infty$ a.e. or $q = 1$ and $X = \|X\|_\infty$ a.s..

Theorem 19.3.25 (Cauchy-Schwarz inequality)**.** For all random variables $X, Y \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, we have that XY is integrable and

$$\left(\mathbb{E}\,(XY)\right)^2 \leq \left(\mathbb{E}\,|XY|\right)^2 \leq \mathbb{E}X^2\mathbb{E}Y^2. \tag{19.3.45}$$

The equality holds when $aX = bY$ for some $a, b \in \mathbb{R}$ a.s., i.e., X, Y are linearly dependent.

Remark. The first inequality is given by Theorem 15.3.10.(iv) and the second is given by Theorem 19.3.24.

Theorem 19.3.26 (Minkowski's inequality)**.** For $p \in [1, \infty]$ and random variables $X, Y \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, we have

$$\left(\mathbb{E}\,|X+Y|^p\right)^{1/p} \leq \left(\mathbb{E}\,|X|^p\right)^{1/p} + \left(\mathbb{E}\,|Y|^p\right)^{1/p}. \tag{19.3.46}$$

For $p \in (1, \infty)$, the equality holds if and only if $X = cY$ or $Y = cX$ for some $c \geq 0$ a.s..

Applying Definition 15.4.7 and Theorem 15.4.13 for probabilty space, we have

Definition 19.3.4. A subset $V \subseteq \mathcal{L}^2$ is closed if, for every random variable sequence $(X_n : n \in \mathbb{N})$ in V, with $X_n \to X$ in $\mathcal{L}^2$, we have $X = Y$ a.s., for some $Y \in V$.

Theorem 19.3.27 (Orthogonal Projection)**.** Let $\mathcal{K}$ be a complete subspace of $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. Then each $X \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ has a decomposition $X = Y + Z$, with $Y \in \mathcal{K}$ and $Z \in \mathcal{K}^\perp$. Moreover, $\|X - Y\|_2 \leq \|X - V\|_2$ for all $V \in \mathcal{K}$, $X - Y \perp Z$ for all $Z \in \mathcal{K}$ with equality only if $X = Y$ a.s.

The random variable Y is called (a version of) the orthogonal projection of X on E.

19.3.5 Bounded in $\mathcal{L}^p$ and uniform integrability

Recall Definition 15.4.8, 15.4.9, we give

Definition 19.3.5. For a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, let $\mathcal{X}$ be a collection of random variables. For $1 \leq p \leq \infty$, we say that $\mathcal{X}$ is bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ if

$$\sup_{X \in \mathcal{X}} \|X\|_p < \infty. \tag{19.3.47}$$

Proposition 19.3.28. Let $1 \leq p < q < \infty$. If $\mathcal{X}$ is bounded in $\mathcal{L}^q(\Omega, \mathcal{F}, \mathbb{P})$, then it is also bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$.

Proof. By Proposition 15.4.5, we have

$$\|X\|_p \leq \|X\|_q \;\Rightarrow\; \sup_{X \in \mathcal{X}} \|X\|_p \leq \sup_{X \in \mathcal{X}} \|X\|_q. \tag{19.3.48}$$

Thus, if $\mathcal{X}$ is boudned $\mathcal{L}^q(\Omega, \mathcal{F}, \mathbb{P})$, then it is also boudned $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. □

Definition 19.3.6. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Define

$$I_{\mathcal{X}}(\delta) = \sup\{\mathbb{E}(|X|\mathbb{1}_A) : X \in \mathcal{X}, A \in \mathcal{F}, \mathbb{P}(A) \leq \delta\}. \tag{19.3.49}$$

We say that $\mathcal{X}$ is uniformly integrable or UI if $\mathcal{X}$ is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and

$$I_{\mathcal{X}}(\delta) \downarrow 0 \text{ as } \delta \downarrow 0, \quad \text{i.e.,} \quad \forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } I_{\mathcal{X}}(\delta) < \varepsilon. \tag{19.3.50}$$

Then, from Lemma 15.4.20 and Theorem 15.4.21, we have

Theorem 19.3.29. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. A collection of random variables $\mathcal{X}$ is uniformly integrable, it is equivalent to either of the following two conditions:

$$\text{(i)} \inf_{K \in [0,\infty)} \sup_{X \in \mathcal{X}} \mathbb{E}\left(|X| \mathbb{1}_{|X|>K}\right) = 0, \quad \text{i.e.,} \quad \sup_{X \in \mathcal{X}} \mathbb{E}\left(|X| \mathbb{1}_{|X|>K}\right) \to 0 \text{ as } K \to \infty. \tag{19.3.51}$$

$$\text{(ii)} \inf_{K \in [0,\infty)} \sup_{X \in \mathcal{X}} \mathbb{E}\left((|X| - K)^+\right) = 0, \quad \text{i.e.,} \quad \sup_{X \in \mathcal{X}} \mathbb{E}\left((|X| - K)^+\right) \to 0 \text{ as } K \to \infty. \tag{19.3.52}$$

Proof. This is special case for Theorem 15.4.21. □

Proposition 19.3.30. Any single integrable random variable is uniformly integrable. This extends easily to any finite collection of integrable random variables.

Proof. See Proposition 15.4.18. □

Proposition 19.3.31. For any integrable random variable Y, the set

$$\mathcal{X} = \{X : X \text{ is a random variable}, |X| \le Y\} \quad \text{is UI.} \tag{19.3.53}$$

Proof. See Proposition 15.4.19. □

Proposition 19.3.32. If a random variable family $\mathcal{X}$ is bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, for $p \in (1, \infty]$, then it is UI.

Proof. Direct result of Proposition 15.4.16. □

Example 19.3.33. Take uniformly distributed random variable $X \sim U[0,1]$ and consider the sequence

$$X_{n,k} = n \mathbb{1}_{\{X \in (k/n^2, (k+1)/n^2]\}}, \quad k = 0, 1, \ldots, n-1. \tag{19.3.54}$$

The sequence is: $X_{1,0}, X_{2,0}, X_{2,1}, X_{3,0}, X_{3,1}, X_{3,2}, \ldots$. Thus, $X_n \in \{X_{n,k}\}$, $k = 0, 1, \ldots, n-1$ and

$$\mathbb{P}(X_{n,k} = n) = \frac{1}{n^2} \;\Rightarrow\; X_n \to 0 \text{ a.s. as } n \to \infty \tag{19.3.55}$$

It is also UI since

$$\begin{aligned}
\lim_{K\to\infty} \sup_n \mathbb{E}\left(|X_n| \mathbb{1}_{\{|X_n|>K\}}\right) &= \lim_{K\to\infty} \sup_n \mathbb{E}\left(n \mathbb{1}_{\{X \in (k/n^2,(k+1)/n^2]\}} \mathbb{1}_{\{n>K\}}\right) \\
&= \lim_{K\to\infty} \sup_n n\mathbb{P}\left(\left\{X \in (k/n^2, (k+1)/n^2]\right\}\right) \mathbb{1}_{\{n>K\}} \\
&= \lim_{K\to\infty} \sup_{n>K} n\mathbb{P}\left(\left\{X \in (k/n^2, (k+1)/n^2]\right\}\right) \\
&= \lim_{K\to\infty} \sup_{n>K} n \cdot \frac{1}{n^2} = \lim_{K\to\infty} \sup_{n>K} \frac{1}{n} = \lim_{K\to\infty} \frac{1}{\lceil K \rceil} = 0.
\end{aligned}$$

For $U \in \left(0, \frac{1}{n}\right]$, we have $|X_n| = n$, thus we can find m such that $\forall n \ge m$, $|X_m| \ge \frac{1}{U}$. Then

$$\mathbb{E}\left(\sup_n |X_n|\right) \ge \mathbb{E}\left(\frac{1}{U}\right) = \int_0^1 \frac{1}{u} du = \infty. \tag{19.3.56}$$

Remark. Note that $\sup_n \mathbb{E}|X_n| \neq \mathbb{E}(\sup_n |X_n|)$ in general.

19.3.6 Convergence in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$

Recalling Definition 15.4.10, Proposition 15.4.22 and Proposition 15.4.23, we have

Definition 19.3.7. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. We say that the sequence of random variables X_n converges in $\mathcal{L}^p$ (or in the p-th mean) to X, for some $p \in [1, \infty)$, if $X, X_n \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ for all n and

$$\mathbb{E}\,|X_n - X|^p \to 0 \ \text{ as } n \to \infty. \tag{19.3.57}$$

If $p = \infty$, we say X_n converges in $\mathcal{L}^\infty$ to X, if $X, X_n \in \mathcal{L}^\infty(\Omega, \mathcal{F}, \mathbb{P})$ for all n and

$$\|X_n - X\|_\infty \to 0 \ \text{ as } n \to \infty. \tag{19.3.58}$$

Proposition 19.3.34. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. For $p = [1, \infty)$, if $X_n \overset{\mathcal{L}^p}{\to} X$, then for any $q \in [1, p)$, $X_n \overset{\mathcal{L}^q}{\to} X$.

Proposition 19.3.35. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. For $p = [1, \infty)$, if $X_n \overset{\mathcal{L}^p}{\to} X$, then $X_n \overset{p}{\to} X$.

Theorem 19.3.36. Let X be a random variable and let $(X_n : n \in \mathbb{N})$ be a sequence of random variables. The following are equivalent:

(i) $X_n \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ for all n, $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $X_n \to X$ in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$,

(ii) $\{X_n : n \in \mathbb{N}\}$ is UI and $X_n \to X$ in probability.

Remark. This is the special case of Vitali convergence theorem (Theorem 15.4.25)

Proof. Suppose (i) holds. By Chebyshev's inequality (Theorem 15.4.2), for $\varepsilon > 0$,

$$\mathbb{P}(|X_n - X| > \varepsilon) \le \varepsilon^{-1}\mathbb{E}(|X_n - X|) \to 0 \tag{19.3.59}$$

so $X_n \to X$ in probability. Moreover, given $\varepsilon > 0$, there exists N such that $\mathbb{E}(|X_n - X|) < \varepsilon/2$ whenever $n \ge N$. Then we can find $\delta > 0$ so that $\mathbb{P}(A) < \delta$ implies $\mathbb{E}(|X|\mathbb{1}_A) < \varepsilon/2$ by Lemma 15.4.15.

Then, for $n \ge N$ and $\mathbb{P}(A) \le \delta$,

$$\mathbb{E}(|X_n|\mathbb{1}_A) \le \mathbb{E}(|X_n - X|) + \mathbb{E}(|X|\mathbb{1}_A) < \varepsilon. \tag{19.3.60}$$

Hence $\{X_n : n \in \mathbb{N}\}$ is UI. We have shown that (i) implies (ii).

Suppose, on the other hand, that (ii) holds. Then there is a subsequence (n_k) such that $X_{n_k} \to X$ a.s. by Theorem 15.2.14 (ii). So, by Fatou's lemma,

$$\mathbb{E}(|X|) = \mathbb{E}\left(\liminf_k |X_{n_k}|\right) \le \underbrace{\liminf_k \mathbb{E}(|X_{n_k}|) < \infty}_{\text{Definition 15.4.8, 15.4.9}} \quad \Rightarrow \quad X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P}). \tag{19.3.61}$$

Thus, X is integrable, then by Lemma 15.4.15, $I_X(\delta) \downarrow 0$ as $\delta \downarrow 0$. So $\{X_n, n \in \mathbb{N}\} \cup X$ is UI.

Now, given $\varepsilon > 0$, there exists $K < \infty$ such that, for all n,

$$\mathbb{E}(|X_n|\mathbb{1}_{\{|X_n| \ge K\}}) < \varepsilon/3, \qquad \mathbb{E}(|X|\mathbb{1}_{\{|X| \ge K\}}) < \varepsilon/3. \qquad \text{(Lemma 15.4.20)} \tag{19.3.62}$$

Consider the uniformly bounded sequence $X_n^K = (-K) \vee X_n \wedge K$ and set $X^K = (-K) \vee X \wedge K$. Then

$$\left\{\left|X_n^K - X^K\right| > \varepsilon\right\} \subseteq \{|X_n - X| > \varepsilon\} \quad \Rightarrow \quad \mathbb{P}\left(\left|X_n^K - X^K\right| > \varepsilon\right) \le \mathbb{P}\left(|X_n - X| > \varepsilon\right) \to 0. \tag{19.3.63}$$

Thus $X_n^K \to X^K$ in probability, so by bounded convergence theorem (Theorem 15.3.16, $\left|X_n^K\right| \le K$), there exists N such that, for all $n \ge N$, $\mathbb{E}|X_n^K - X^K| < \varepsilon/3$. But then, for all $n \ge N$,

$$\begin{aligned} \mathbb{E}|X_n - X| &\le \mathbb{E}|X_n - X_n^K| + \mathbb{E}|X_n^K - X^K| + \mathbb{E}|X - X^K| \\ &\le \mathbb{E}(|X_n|\mathbb{1}_{\{|X_n| \ge K\}}) + \mathbb{E}|X_n^K - X^K| + \mathbb{E}(|X|\mathbb{1}_{\{|X| \ge K\}}) < \varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ was arbitrary, we have shown that (ii) implies (i). □

Proposition 19.3.37. Let $(X_n)_{n\in\mathbb{N}}$ be an identically distributed sequence in $\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$. Then

$$\mathbb{E}\left(\max_{k\le n}|X_k|\Big/\sqrt{n}\right)\to 0 \text{ as } n\to\infty. \tag{19.3.64}$$

Proof. First we have for some constant M

$$\mathbb{E}\left(\max_{k\le n}X_k^2/n\right)\le\frac{1}{n}\mathbb{E}\left(\sum_{k=1}^n X_k^2\right)=\mathbb{E}(X_1^2)\le M \;\Rightarrow\; \left\{\max_{k\le n}|X_k|\Big/\sqrt{n}\right\}_n \text{ is bounded in } \mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P}). \tag{19.3.65}$$

So it is UI by Proposition 19.3.32 (as $\sup\|\max_{k\le n}|X_k|/\sqrt{n}\|_2\le M<\infty$). Also, by Example 19.3.9, it converges to 0 in probability.

Hence, we can have

$$\max_{k\le n}|X_k|\Big/\sqrt{n}\to 0 \text{ in } \mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P}) \;\Rightarrow\; \mathbb{E}\left(\max_{k\le n}|X_k|\Big/\sqrt{n}\right)\to 0 \text{ as } n\to\infty \tag{19.3.66}$$

by Theorem 19.3.36. □

Since probability is finite measure, (iii) of Theorem 15.4.25 is automatically satisfied, so we have probability version of 15.4.25:

Theorem 19.3.38. Let $X_1, X_2, \ldots$ be $\mathcal{L}^p(\Omega,\mathcal{F},\mathbb{P})$-integrable random variables, for $1\le p<\infty$. Then the sequence X_n converges in $\mathcal{L}^p(\Omega,\mathcal{F},\mathbb{P})$ if and and only if

(i) the sequence X_n converges in probability,

(ii) the collection of random variables, $\{|X_n|^p\}$ is uniformly integrable,

Proof. We can use Theorem 19.3.36. □

Remark. This theorem is Theorem 19.3.36 when $p=1$.

19.3.7 Variance and covariance

Now we look at some $\mathcal{L}^2$ notions relevant to probability.

Definition 19.3.8 (variance)**.** For $X\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$, with mean $\mathbb{E}X$ (this is well-defined as $\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})\subseteq\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$, see Proposition 19.3.5), we define variance

$$\mathrm{Var}(X)=\mathbb{E}\left((X-\mathbb{E}X)^2\right). \tag{19.3.67}$$

Remark. The variance is a measure of how much the distribution of X is spread out around the mean, the smaller the distribution the more the distribution of X is concentrated close to $\mathbb{E}X$. The quantity $\sqrt{\mathrm{Var}(X)}$ is known as the standard deviation of X. When we use the notation $\mathrm{Var}(X)$ we will assume implicitly that it is a finite quantity.

Proposition 19.3.39 (properties of $\mathrm{Var}(X)$)**.** Let $X\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$.

(i) $\mathrm{Var}(X)=\mathbb{E}X^2-(\mathbb{E}X)^2$.

(ii) If c is a constant, $\mathrm{Var}(cX)=c^2\,\mathrm{Var}(X)$.

(iii) If c is a constant, $\mathrm{Var}(X+c)=\mathrm{Var}(X)$.

(iv) $\mathrm{Var}(X)\ge 0$, and $\mathrm{Var}(X)=0$ if and only if $X=\mathbb{E}X$ a.s..

(v) The expression $\mathbb{E}(X-c)^2$ is minimized over constants c when $c=\mathbb{E}X$, so that $\mathbb{E}(X-c)^2\ge\mathrm{Var}(X)$, for all c, with equality when $c=\mathbb{E}X$.

Proof. (i)-(iii) are from definition directly.

(iv) By Proposition 19.3.1.(ii),

$$(X-\mathbb{E}X)^2=0 \text{ a.s.} \;\Rightarrow\; X=\mathbb{E}X \text{ a.s..} \tag{19.3.68}$$

(v) Expand out the expression

$$\mathbb{E}(X-c)^2 = \mathbb{E}\left(X^2 - 2cX + c^2\right) = \mathbb{E}X^2 - 2c\mathbb{E}X + c^2, \tag{19.3.69}$$

and minimize the right-hand side in c to see that the minimum occurs at $c = \mathbb{E}X$.

□

Definition 19.3.9 (covariance)**.** For $X, Y \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, with means $\mathbb{E}X, \mathbb{E}Y$ (well-defined), covariance of X and Y is

$$\mathrm{Cov}(X,Y) = \mathbb{E}\left((X - \mathbb{E}X)(Y - \mathbb{E}Y)\right). \tag{19.3.70}$$

Remark. We shall see that this is a measure of the dependence between the random variables X and Y.

For a random variable $X = (X_1, \ldots, X_n)$ in $\mathbb{R}^n$, we define its covariance matrix

$$V = \mathrm{Cov}(X) = (\mathrm{Cov}(X_i, X_j))_{i,j=1}^n, \quad \text{i.e., } \mathrm{Cov}(X_i, X_j) = V_{ij}. \tag{19.3.71}$$

Proposition 19.3.40. For two independent random variables $X, Y \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, with means $\mathbb{E}X, \mathbb{E}Y$ (well-defined), we have $\mathrm{Cov}(X,Y) = 0$.

Proof. This is from Definition 19.3.9 and Proposition 19.3.12. □

Remark. The converse is generally false. One special case is multivariate Gaussian random variables (see Theorem 19.8.20.(v)).

Example 19.3.41. [Covariance equal to 0 does not imply independence] Suppose that X is a random variable with distribution determined by

x	2	1	-1	-2
$\mathbb{P}(X=x)$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

and let $Y = X^2$. Then $\mathbb{E}X = 0$ and $\mathbb{E}(X^3) = 0$ so that $\mathrm{Cov}(X,Y) = \mathbb{E}(X^3) = 0$, but

$$\mathbb{P}(X=2, Y=4) = \frac{1}{4} \neq \mathbb{P}(X=2)\mathbb{P}(Y=4) = \frac{1}{4} \times \frac{1}{2}, \tag{19.3.72}$$

so that X and Y are not independent.

Example 19.3.42. Let $(X,Y) = (\cos\theta, \sin\theta)$ where $\theta = \frac{K\pi}{4}$ and K is a random variable such that $\mathbb{P}(K=r) = 1/8,\ r = 0, 1, \ldots, 7$.

K	0	1	2	3	4	5	6	7
X	1	$\frac{1}{\sqrt{2}}$	0	$-\frac{1}{\sqrt{2}}$	-1	$-\frac{1}{\sqrt{2}}$	0	$\frac{1}{\sqrt{2}}$
Y	0	$\frac{1}{\sqrt{2}}$	1	$\frac{1}{\sqrt{2}}$	0	$-\frac{1}{\sqrt{2}}$	-1	$-\frac{1}{\sqrt{2}}$

so that it is immediate that $\mathrm{Cov}(X,Y) = 0$. We also have

$$\mathbb{P}\left(X = 1/\sqrt{2}\right) = \mathbb{P}\left(Y = 1/\sqrt{2}\right) = \frac{1}{4} \tag{19.3.73}$$

but

$$\mathbb{P}\left(X = 1/\sqrt{2}, Y = 1/\sqrt{2}\right) = \frac{1}{8} \neq \mathbb{P}\left(X = 1/\sqrt{2}\right)\mathbb{P}\left(Y = 1/\sqrt{2}\right) \tag{19.3.74}$$

so that X and Y are not independent.

Proposition 19.3.43 (properties of covariance)**.** Let $X, Y, Z \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. Then

(i) $\mathrm{Cov}(X,Y) = \mathrm{Cov}(Y,X)$.

(ii) $\mathrm{Cov}(X,Y) = \mathbb{E}(XY) - (\mathbb{E}X)(\mathbb{E}Y)$.

(iii) $\mathrm{Cov}(X,X) = \mathrm{Var}(X)$.

(iv) $\mathrm{Var}(X+Y) = \mathrm{Var}(X) + \mathrm{Var}(Y) + 2\,\mathrm{Cov}(X,Y)$.

(v) If c is a constant, $\mathrm{Cov}(X,c) = 0$.

(vi) If c is a constant, $\mathrm{Cov}(X+c,Y)=\mathrm{Cov}(X,Y)$.

(vii) If c is a constant, $\mathrm{Cov}(cX,Y)=c\,\mathrm{Cov}(X,Y)$.

(viii) $\mathrm{Cov}(X+Z,Y)=\mathrm{Cov}(X,Y)+\mathrm{Cov}(Z,Y)$. These last two generalize to the case of random variables $X_1,\ldots,X_n\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$ and $Y_1,\ldots,Y_n\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$ and constants $c_1,\ldots,c_n$ and $d_1,\ldots,d_n$ to give, by induction,

$$\mathrm{Cov}\left(\sum_{i=1}^n c_iX_i,\sum_{j=1}^n d_jY_j\right)=\sum_{i=1}^n\sum_{j=1}^n c_id_j\,\mathrm{Cov}(X_i,Y_j). \tag{19.3.75}$$

(ix) Using (iii), we see that a special case of this is

$$\mathrm{Var}\left(\sum_{i=1}^n X_i\right)=\sum_{i=1}^n\mathrm{Var}(X_i)+\sum_{i=1}^n\sum_{j\neq i}\mathrm{Cov}(X_i,X_j),\qquad(*) \tag{19.3.76}$$

for any random variables $X_1,\ldots,X_n$.

(x) Using (viii), if $X_1,\ldots,X_n$ are independent, we have

$$\mathrm{Var}\left(\sum_{i=1}^n c_iX_i\right)=\sum_{i=1}^n c_i^2\,\mathrm{Var}(X_i). \tag{19.3.77}$$

Proof. This is obvious from Definitions 19.3.9, 19.3.9. □

Proposition 19.3.44. Every covariance matrix is non-negative definite.

Proof. For any $a\in\mathbb{R}^n$ and covariance matrix $\mathrm{Var}\,(X)$.

$$a^T\,\mathrm{Var}(X)a=\mathrm{Var}(a^TX)\geq 0\quad\Rightarrow\quad\mathrm{Var}\,(X)\text{ is non-negative definite.}$$ □

Definition 19.3.10 (correlation)**.** For $X,Y\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$, with means $\mathbb{E}X,\mathbb{E}Y$ (well-defined), then correlation of X and Y is

$$\mathrm{Corr}(X,Y)=\mathrm{Cov}(X,Y)/\sqrt{\mathrm{Var}(X)\,\mathrm{Var}(Y)}. \tag{19.3.78}$$

Note that the $\mathrm{Cov}(X,Y)\in[-1,1]$. This is implied by Cauchy-Schwarz inequality (Theorem 19.3.25).

Remark. It may be further seen that $|\mathrm{Corr}(X,Y)|=1$ if and only if $X=aY+b$ for some constants a and b. One property of correlation that we should note is that for constants a, b, c and d with $ac\neq 0$, we have

$$\mathrm{Corr}(aX+b,cY+d)=\begin{cases}\mathrm{Corr}(X,Y) & ac>0,\\ -\mathrm{Corr}(X,Y) & ac<0.\end{cases} \tag{19.3.79}$$

This follows easily from the definition of correlation and the properties of the covariance and variance, notice that when $ac=0$, $\mathrm{Cov}(aX+b,cY+d)=0$, and the correlation is not defined because at least one of $\mathrm{Var}(aX+b)=0$ or $\mathrm{Var}(cY+d)=0$.

Notice that one consequence of this fact is that the correlation between two random variables is scale invariant - if we multiply the observation of X and Y by positive constants we do not alter the correlation.

19.4 Conditional Expectation

19.4.1 Elementary conditional probabilities of events

Definition 19.4.1. Let $(\Omega,\mathcal{F},\mathbb{P})$ be a probability space. Let $A,B\in\mathcal{F}$ and suppose that $\mathbb{P}(B)>0$. The conditional probability of A with respect to B is

$$\mathbb{P}(A|B)=\frac{\mathbb{P}(A\cap B)}{\mathbb{P}(B)}. \tag{19.4.1}$$

Remark. The conditional probability is interpreted as the probability of event A happening given that event B has happened.

Proposition 19.4.1. The first thing to observe is that $\mathbb{P}(\cdot|B)$ is a probability distribution on the sample space B, because it satisfies the following

(i) For $C \subseteq B$, $\mathbb{P}(C|B) = \mathbb{P}(C)/\mathbb{P}(B)$, so that $0 \leq \mathbb{P}(C|B) \leq 1$.

(ii) $\mathbb{P}(B|B) = \mathbb{P}(B)/\mathbb{P}(B) = 1$.

(iii) For countable disjoint events $C_1, C_2, \ldots$ in B,

$$\mathbb{P}\left(\bigcup_{i=1}^{\infty} C_i \middle| B\right) = \frac{\mathbb{P}\left(\bigcup_{i=1}^{\infty} C_i \cap B\right)}{\mathbb{P}(B)} = \frac{\mathbb{P}\left(\bigcup_{i=1}^{\infty} C_i\right)}{\mathbb{P}(B)} = \frac{\sum_{i=1}^{\infty} \mathbb{P}(C_i)}{\mathbb{P}(B)} = \sum_{i=1}^{\infty} \mathbb{P}(C_i|B). \tag{19.4.2}$$

(iv) The next thing to notice is the multiplication rule that

$$\mathbb{P}(A \cap B) = \mathbb{P}(A|B)P(B), \tag{19.4.3}$$

so that the probability of two events occurring can be broken up into calculating successive probabilities – firstly the probability that B occurs and then given that B has occurred the probability that A occurs. This is one of two central procedures for calculating probabilities (the second is the Law of Total Probability (19.4.6)).

Example 19.4.2. What is the probability that a Bridge hand contains the ace of hearts given that it contains exactly 5 hearts? Let A be the event that the hand contains the ace of hearts and B the event that the hand contains exactly 5 hearts. Then

$$\mathbb{P}(B) = \frac{\binom{13}{5}\binom{39}{8}}{\binom{52}{13}}, \quad \mathbb{P}(A \cap B) = \frac{\binom{12}{4}\binom{39}{8}}{\binom{52}{13}} \quad \Rightarrow \quad \mathbb{P}(A|B) = \frac{\binom{12}{4}}{\binom{13}{5}} = \frac{5}{13}. \tag{19.4.4}$$

Example 19.4.3. Suppose that two students are selected, without replacement, from a class of 5 women and 13 men. What is the probability that the first student selected is a man and the second is a woman? Let B be the event that the first is a man and A the event that the second is a woman, then $\mathbb{P}(A \cap B) = \mathbb{P}(A|B)\mathbb{P}(B) = \frac{5}{17} \times \frac{13}{18}$.

More generally we can write down the multiplication rule for events $A_1, \ldots, A_n$,

$$\mathbb{P}(A_1 \cap A_2 \cdots \cap A_n) = \mathbb{P}(A_1)\mathbb{P}(A_2|A_1)\mathbb{P}(A_3|A_1 \cap A_2) \ldots \mathbb{P}(A_n|A_1 \cap \cdots \cap A_{n-1}). \tag{19.4.5}$$

Example 19.4.4. In drawing three cards without replacement from a pack what is the probability of three successive aces? Here A_i would be the event that an ace is obtained on draw i, $i = 1, 2, 3$, then

$$\mathbb{P}(A_1 \cap A_2 \cap A_3) = \mathbb{P}(A_1)\mathbb{P}(A_2|A_1)\mathbb{P}(A_3|A_1 \cap A_2) = \frac{4}{52} \times \frac{3}{51} \times \frac{2}{50}. \tag{19.4.6}$$

Example 19.4.5. For $s > 1$ define the zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Let X and Y be independent random variables with

$$\mathbb{P}(X = n) = \mathbb{P}(Y = n) = n^{-s}/\zeta(s). \tag{19.4.7}$$

Let A_n be the event $\{n \text{ divides } X\}$ then

$$\mathbb{P}(A_n) = \mathbb{P}\left(\bigcup_m \{X = mn\}\right) = \sum_m \mathbb{P}(X = mn) = \sum_m (mn)^{-s}/\zeta(s) = n^{-s}. \tag{19.4.8}$$

Let $p_1, \ldots, p_k$ be distinct primes

$$\prod_{j=1}^{k} p_j = n \;\Leftrightarrow\; p_j \text{ divides } n \text{ for all } j \leq k \quad \Rightarrow \quad \mathbb{P}\left(\bigcap_{j=1}^{k} A_{p_j}\right) = \mathbb{P}\left(A_{(p_1 \ldots p_k)}\right) = (p_1 \ldots p_k)^{-s} = \prod_{j=1}^{k} \mathbb{P}(A_{p_j}). \tag{19.4.9}$$

Thus, the events $(A_p, p \text{ is prime})$ are independent. Hence the events $\left(A_p^c, p \text{ is prime}\right)$ are also independent (from Proposition 19.1.22). Then

$$\prod_p \left(1 - \frac{1}{p^s}\right) = \prod_p \left(A_p^c\right) = \mathbb{P}\left(\bigcap_p A_p^c\right) = \mathbb{P}\left(\left(\bigcup_p A_p\right)^c\right) = \mathbb{P}(X \text{ has no prime factors}) = \mathbb{P}(X = 1) = \frac{1}{\zeta(s)}. \tag{19.4.10}$$

which is Euler's formula. The same argument show that the events $\left(A^c_{p^2}, p \text{ is prime}\right)$ are independent

$$\mathbb{P}(X \text{ is square-free}) = \prod_p \left(1 - \frac{1}{p^{2s}}\right) = \frac{1}{\zeta(2s)}. \tag{19.4.11}$$

Next, we have the event $\{H = n\} = A^X_n \cap A^Y_n \cap \left(\bigcup_p A^X_{pn} \cap A^Y_{pn}\right)^c$, where $\left(\bigcup_p A^X_{pn} \cap A^Y_{pn}\right)$ means that there exists a prime p s.t. X and Y have a bigger common factor pn. Thus,

$$\mathbb{P}(\{H = n\}) = \mathbb{P}\left(A^X_n \cap A^Y_n \cap \left(\bigcup_p A^X_{pn} \cap A^Y_{pn}\right)^c\right) = \mathbb{P}\left(A^X_n \cap A^Y_n \cap \left(\bigcap_p \left(A^X_{pn} \cap A^Y_{pn}\right)^c\right)\right) \tag{19.4.12}$$

Also, we check the event $(A_{pn}|A_n)$ (note that $\mathbb{P}(A_{kn}|A_n) = k^{-s}$)

$$\mathbb{P}\left(\bigcap_{j=1}^k \left(A_{p_j n}|A_n\right)\right) = \mathbb{P}\left(\bigcap_{j=1}^k A_{p_j n}\middle| A_n\right) = \mathbb{P}\left(A_{(p_1 \ldots p_j n)}\middle| A_n\right) = (p_1 \ldots p_k)^{-s} = \prod_{j=1}^k \mathbb{P}(A_{p_j n}|A_n). \tag{19.4.13}$$

Thus, we say that $((A_{pn}|A_n), p \text{ is prime})$ are independent. The similar argument for $\left(A^X_{pn} \cap A^Y_{pn}|A^X_n \cap A^Y_n\right)$. Then

$$\begin{aligned}
\mathbb{P}(\{H = n\}) &= \mathbb{P}\left(A^X_n \cap A^Y_n \cap \left(\bigcap_p \left(A^X_{pn} \cap A^Y_{pn}\right)^c\right)\right) = \mathbb{P}\left(\bigcap_p \left(A^X_{pn} \cap A^Y_{pn}\right)^c \middle| A^X_n \cap A^Y_n\right) \mathbb{P}\left(A^X_n \cap A^Y_n\right) \\
&= \mathbb{P}\left(A^X_n \cap A^Y_n\right) \prod_p \mathbb{P}\left(\left(A^X_{pn} \cap A^Y_{pn}\right)^c \middle| A^X_n \cap A^Y_n\right) = \mathbb{P}\left(A^X_n \cap A^Y_n\right) \prod_p \left(1 - \mathbb{P}\left(\left(A^X_{pn} \cap A^Y_{pn}\right)\middle| A^X_n \cap A^Y_n\right)\right) \\
&= \mathbb{P}\left(A^X_n\right) \mathbb{P}\left(A^Y_n\right) \prod_p \left(1 - \mathbb{P}\left(A^X_{pn}\middle| A^X_n\right) \mathbb{P}\left(A^Y_{pn}\middle| A^Y_n\right)\right) = n^{-2s} \prod_p \left(1 - p^{-2s}\right) = n^{-2s}/\zeta(2s).
\end{aligned}$$

Theorem 19.4.6 (law of total probability)**.** A countable collection $\{B_i\}_{i=1}^\infty$ of disjoint events for which $\bigcup_{i=1}^\infty B_i = \Omega$ is said to be a partition of the sample space Ω. For any partition of the sample space, $\{B_i\}$, and for any event A, we may write

$$\mathbb{P}(A) = \sum_{i=1}^\infty \mathbb{P}(A \cap B_i) = \sum_i \mathbb{P}(A|B_i)\mathbb{P}(B_i), \tag{19.4.14}$$

where the second summation extends only over those events B_i in the partition for which $\mathbb{P}(B_i) > 0$. The identity in (19.4.14) is known as the law of total probability.

Proof. It follows immediately from 19.4.1.(iii),(iv), because the event A may be represented as $A = \bigcup_{i=1}^\infty (A \cap B_i)$. □

Example 19.4.7. An urn contains b black balls and r red balls from which two balls are drawn without replacement. What is the probability that the second ball drawn is black? Let A represent the event that the second ball is black and B the event that the first ball is black. Then B and B^c form a partition of the sample space (think of the other events in the partition as being $\emptyset$). Then

$$\mathbb{P}(A) = \mathbb{P}(A|B)\mathbb{P}(B) + \mathbb{P}(A|B^c)\mathbb{P}(B^c) = \left(\frac{b-1}{b+r-1}\right)\left(\frac{b}{b+r}\right) + \left(\frac{b}{b+r-1}\right)\left(\frac{r}{b+r}\right) = \frac{b}{b+r}. \tag{19.4.15}$$

This probability may be seen to be the same as the probability that the second ball is black when sampling with replacement.

Example 19.4.8. A survey of US voters shows the following figures for proportions of voters registered with the main parties and the proportions of voters registered for each of the parties who declare an intention to vote for Dubya.

	Registered	Proportion for Bush
Democratic	45%	10%
Republican	35%	60%
Not affiliated	20%	40%

Suppose that a voter is chosen at random, what is the probability (s)he is a Bush voter? Here the partition of the sample

space is D (Democrat), R (Republican) and NA (No affiliation), and if B is the event the voter is a Bush supporter then

$$\mathbb{P}(B) = \mathbb{P}(B|D)\mathbb{P}(D) + \mathbb{P}(B|R)\mathbb{P}(R) + \mathbb{P}(B|NA)\mathbb{P}(NA) = 0.1 \times 0.45 + 0.6 \times 0.35 + 0.4 \times 0.2 = 0.335. \tag{19.4.16}$$

Theorem 19.4.9 (Bayes' Theorem)**.** For any events A and B, for which $\mathbb{P}(A) > 0$ and $\mathbb{P}(B) > 0$, we have

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A|B)\mathbb{P}(B)}{\mathbb{P}(A)}. \tag{19.4.17}$$

Example 19.4.10. In Example 19.4.8, given that the voter chosen is a Bush supporter, what is the probability that (s)he is a Republican?

$$\mathbb{P}(R|B) = \frac{\mathbb{P}(B|R)\mathbb{P}(R)}{\mathbb{P}(B)} = 0.6 \times 0.35/0.335 \approx 0.63. \tag{19.4.18}$$

Combining the law of total probability (Theorem 19.4.9) with the statement in (19.4.9), gives the general statement of Bayes' Theorem:

Theorem 19.4.11 (Bayes' Theorem)**.** Suppose that $\{B_i\}_i$ is a partition of the sample space and that A is an event for which $\mathbb{P}(A) > 0$. Then for any event, B_i, in the partition with $\mathbb{P}(B_i) > 0$, we have

$$\mathbb{P}(B_i|A) = \frac{\mathbb{P}(A|B_i)\mathbb{P}(B_i)}{\sum_j \mathbb{P}(A|B_j)\mathbb{P}(B_j)}, \tag{19.4.19}$$

where the summation in the denominator extends over all j for which $\mathbb{P}(B_j) > 0$.

Example 19.4.12. Consider a diagnostic test for some disease for which the outcome of the test is either positive, +, or negative, -, and which is 99% accurate, so that if D represents the event that the patient has the disease then

$$\mathbb{P}(+|D) = 0.99 = \mathbb{P}(-|D^c). \tag{19.4.20}$$

Suppose that 0.1% of patients have the disease. A patient is chosen at random and tests positive, what is the probability that (s)he has the disease? Then from Bayes' Theorem

$$\mathbb{P}(D|+) = \frac{\mathbb{P}(+|D)\mathbb{P}(D)}{\mathbb{P}(+|D)\mathbb{P}(D) + \mathbb{P}(+|D^c)\mathbb{P}(D^c)} = \frac{0.99 \times 0.001}{0.99 \times 0.001 + 0.01 \times 0.999} \approx 0.09. \tag{19.4.21}$$

At first sight this conclusion, that the probability that someone testing positive has a somewhat low probability of having the disease, may be counter intuitive. It arises because the probability of a 'false positive', $\mathbb{P}(+|D^c)$, is large compared to the probability of the disease in the population, $\mathbb{P}(D)$. Notice that

$$\mathbb{P}(D|+) = \frac{1}{1 + (\mathbb{P}(+|D^c)\mathbb{P}(D^c)/\mathbb{P}(+|D)\mathbb{P}(D))}. \tag{19.4.22}$$

typically $\mathbb{P}(D^c)$ and $\mathbb{P}(+|D)$ will be close to 1 so that $\mathbb{P}(D|+)$ will be large or small according as the ratio $\mathbb{P}(+|D^c) = \mathbb{P}(D)$ is small or large. This becomes less mysterious when you consider a population of 1,000 patients with just one person suffering from the disease. Of the 999 not suffering from the disease there will be about 10 who will test positive so there will be about 11 in the population who will test positive, given that 17 the person selected has tested positive then there is about a 1 in 11 chance that the person is the one suffering from the disease. A similar calculation to the above shows that $\mathbb{P}(D|-) \approx 0.000001$.

Example 19.4.13 (Simpson's paradox)**.** One example of conditional probability that appears counter-intuitive when first seen is the following situation which can arise frequently. Consider one individual chosen at random from 50 men and 50 women applicants to a particular College. Figures on the 100 applicants are given in the following table indicating whether they were educated at a state school or at an independent school and whether they were admitted or rejected.

All applicants	Admitted	Rejected	% Admitted
State	25	25	50%
Independent	28	22	56%

Note that overall the probability that an applicant is admitted is 0.53, but conditional on the candidate being from an independent school the probability is 0.56 while conditional on being from a state school the probability is lower at 0.50. Suppose that when we break down the figures for men and women we have the following figures.

Men only	Admitted	Rejected	% Admitted
State	15	22	41%
Independent	5	8	38%

Women only	Admitted	Rejected	% Admitted
State	10	3	77%
Independent	23	14	62%

It may now be seen that now for both men and women the conditional probability of being admitted is higher for state school applicants, at 0.41 and 0.77, respectively. This may seem to be a surprising result in that while the aggregate data suggests that independent school applicants have a better chance of being admitted, the individual tables for both men and women show that in both cases state school applicants have a higher acceptance rate. A 18 result of this type in tables of this sort (called contingency tables in statistics) is known as Simpson's paradox. Strictly, it is not a paradox in that it has an easy explanation. Note that overall women have a much higher acceptance rate (66%) than men (40%) whereas the proportion of men from state schools is 74% with 26% from independent schools while those proportions are reversed for women. This situation is known in statistics as confounding, it occurs when figures for two separate and different populations are aggregated to give misleading conclusions. It may be difficult or impossible to determine whether data such as that presented in the first table arise from two disparate populations and so confounding is present.

The example shows that if A, B, C are three events it is possible to have the three inequalities

$$\mathbb{P}(A|B\cap C) > \mathbb{P}(A|B\cap C^c), \qquad \mathbb{P}(A|B^c\cap C) > \mathbb{P}(A|B^c\cap C^c), \qquad \mathbb{P}(A|C^c) > \mathbb{P}(A|C), \tag{19.4.23}$$

holding simultaneously. In this example, A would be the event 'being admitted', B the event 'being a man' (with B^c being a woman) and C being 'state school' (with C^c being independent school). One situation where the three inequalities in (19.4.23) cannot hold simultaneously is when

$$\mathbb{P}(B|C) = \mathbb{P}(B|C^c) \tag{19.4.24}$$

To see this, suppose that (19.4.23) and (19.4.24) hold, then we see that

$$\mathbb{P}(A\cap B|C) > \mathbb{P}(A\cap B|C^c), \qquad \mathbb{P}(A\cap B^c|C) > \mathbb{P}(A\cap B^c|C^c) \tag{19.4.25}$$

and then adding and observing that, for example,

$$\mathbb{P}(A\cap B|C) + \mathbb{P}(A\cap B^c|C) = \mathbb{P}(A|C), \tag{19.4.26}$$

we obtain $\mathbb{P}(A|C) > \mathbb{P}(A|C^c)$, which contradicts (19.4.23). In this example it would not be possible to engineer that (19.4.24) holds, but consider the situation where a clinical trial of a new drug for some illness is being conducted to test its eectiveness against a standard drug. Then A would be the event that a patient recovers from the illness and C would be the event that the patient receives the new drug (C^c the event that (s)he receives the standard drug), again B or B^c would correspond to the patient being a man or woman, respectively. Then to avoid the sort of situation described in this example, (19.4.24) would require that the trial be designed so that the relative proportions of men and women that receive the new drug are the same as the relative proportions that receive the standard drug.

19.4.2 Elementary conditional probabilities of random variables

Definition 19.4.2. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. If $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ then the conditional expectation of X given B is

$$\mathbb{E}\,(X|B) = \frac{\mathbb{E}(X\mathbb{1}_B)}{\mathbb{P}(B)}. \tag{19.4.27}$$

Comparing with Definition 19.4.2, we define more general conditional expectation:

Definition 19.4.3. $(\Omega, \mathcal{F}, \mathbb{P})$ is a probability space. Let $(B_i)_{i\in I}$ be a partition of Ω i.e., (B_i) are disjoint and $\bigcup_{i\in I} B_i = \Omega$ such that $B_i \in \mathcal{F}$ for all $i \in I$ where I is a countable set. Let $\mathcal{G} = \sigma(B_i, i \in I)$ and for $X \in \mathcal{L}^1$ define the conditional expectation of X with respect to $\mathcal{G}$ to be

$$Y := \mathbb{E}\,(X|\mathcal{G}) = \sum_{i\in I} \mathbb{E}\,(X|B_i)\,\mathbb{1}_{B_i}, \qquad (\text{i.e., } \mathbb{E}\,(X|\mathcal{G}) = \mathbb{E}\,(X|B_i) \;\Leftrightarrow\; \omega \in B_i) \tag{19.4.28}$$

with the convention that $E(X|B_i) = 0$ if $\mathbb{P}(B_i) = 0$. Also, if Z is a random variable, $\mathbb{E}(X|Z) = \mathbb{E}(X|\sigma(Z))$.

Lemma 19.4.14. Let $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $(B_i)_{i\in I}$ be a partition of Ω. The conditional expectation with respect to $\mathcal{G} = \sigma(B_i, i \in I)$ satisfies

(i) $\mathbb{E}(X|\mathcal{G})$ is $\mathcal{G}$-measurable,

(ii) $\mathbb{E}(X|\mathcal{G}) \in \mathcal{L}^1(\Omega, \mathcal{G}, \mathbb{P})$,

(iii) $\mathbb{E}(X\mathbb{1}_A) = \mathbb{E}(\mathbb{E}(X|\mathcal{G})\mathbb{1}_A)$ for all $A \in \mathcal{G}$.

Proof. (i) Let f be the map $f : \Omega \to I$ with $f(\omega) = i \Leftrightarrow \omega \in B_i$. For any $J \subseteq I$, we have $f^{-1}(J) = \bigcup_{j\in J} B_j \in \mathcal{G}$, as $B_j \in \mathcal{G}, j \in J$. Thus, f is $\mathcal{G}$-measurable (by Definition 15.2.1). Further, let $g : I \to \mathbb{R}, i \mapsto \mathbb{E}(X|B_i)$. Since I is discrete, g is measurable. Then

$$\mathbb{E}(X|\mathcal{G}) = g \circ f(\omega) \quad \text{is } \mathcal{G}\text{-measurable (by Proposition 15.2.6).} \tag{19.4.29}$$

(ii) Let $I' := \{i \in I : \mathbb{P}(B_i) > 0\}$, by Definition 19.4.3 and Fubini theorem (Theorem 15.3.33),

$$\begin{aligned}
\mathbb{E}(|\mathbb{E}(X|\mathcal{G})|) &= \mathbb{E}\left(\left|\sum_{i\in I}\mathbb{E}(X|B_i)\mathbb{1}_{B_i}\right|\right) = \mathbb{E}\left(\left|\sum_{i\in I}\frac{\mathbb{E}(X\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\mathbb{1}_{B_i}\right|\right) \le \mathbb{E}\left(\sum_{i\in I}\frac{|\mathbb{E}(X\mathbb{1}_{B_i})|}{\mathbb{P}(B_i)}\mathbb{1}_{B_i}\right) \\
&\le \mathbb{E}\left(\sum_{i\in I'}\frac{\mathbb{E}(|X|\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\mathbb{1}_{B_i}\right) = \sum_{i\in I'}\frac{\mathbb{E}(|X|\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\mathbb{E}(\mathbb{1}_{B_i}) = \mathbb{E}\left(|X|\,\mathbb{1}_{\{\bigcup_{i\in I'}B_i\}}\right) \le \mathbb{E}(|X|) < \infty.
\end{aligned}$$

(iii) For every $A \in \mathcal{G}$, we have $J \subseteq I$ with $A = \bigcup_{j\in J} B_j$. Let $J' := \{i \in J : \mathbb{P}(B_i) > 0\}$. So, we have $\mathbb{1}_A = \mathbb{1}_{\{\bigcup_{i\in J'}B_i\}}$ a.s., which gives that $X\mathbb{1}_A = X\mathbb{1}_{\{\bigcup_{i\in J'}B_i\}} = X\sum_{i\in J'}\mathbb{1}_{B_i}$ a.s. Hence,

by Definition 19.4.3 and Fubini theorem (Theorem 15.3.33),

$$\begin{aligned}
\mathbb{E}(\mathbb{E}(X|\mathcal{G})\mathbb{1}_A) &= \int_A \mathbb{E}(X|\mathcal{G})\,d\mathbb{P}(\omega) = \int_A\left(\sum_{i\in I}\mathbb{E}(X|B_i)\mathbb{1}_{B_i}\right)d\mathbb{P}(\omega) = \int_A\left(\sum_{i\in I}\frac{\mathbb{E}(X\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\mathbb{1}_{B_i}\right)d\mathbb{P}(\omega) \\
&= \int_\Omega\left(\sum_{i\in I}\frac{\mathbb{E}(X\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\mathbb{1}_{A\cap B_i}\right)d\mathbb{P}(\omega) = \sum_{i\in J'}\frac{\mathbb{E}(X\mathbb{1}_{B_i})}{\mathbb{P}(B_i)}\int_\Omega \mathbb{1}_{B_i}d\mathbb{P}(\omega) = \sum_{i\in J'}\mathbb{E}(X\mathbb{1}_{B_i}) \\
&= \mathbb{E}\left(\sum_{i\in J'}X\mathbb{1}_{B_i}\right) = \mathbb{E}\left(X\sum_{i\in J'}\mathbb{1}_{B_i}\right) = \mathbb{E}(X\mathbb{1}_A). \qquad \text{(Theorem 15.3.10)}
\end{aligned}$$

You can see the proof in Klenke [10].P_{172}. □

Proposition 19.4.15. Let $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $(B_i)_{i\in I}$ (I is a countable set) be a partition of Ω. The conditional expectation with respect to $\mathcal{G} = \sigma(B_i, i \in I)$ satisfies

$$\mathbb{E}X = \sum_{i\in I}\mathbb{E}(X|B_i)\,\mathbb{P}(B_i). \tag{19.4.30}$$

Proof. Direct result from Definition 19.4.3 and the proof of Lemma 19.4.14.(iii). □

Example 19.4.16. Let $X_1, \ldots, X_n$ be n independent random variable with

$$\mathbb{P}(X_n = 0) = \mathbb{P}(X_n = 1) = \frac{1}{2}, \qquad S_n = \sum_{i=1}^n X_i, \qquad \mathcal{G} := \sigma(S_n). \tag{19.4.31}$$

For $0 \le k \le n$, let $G_k = \{S_n = k\}$, then $\bigcup_{k=0}^n G_k = \Omega$, and G_k are pairwise disjoint. Thus $\mathcal{G} := \sigma(G_0, \ldots, G_n)$. So

$$\mathbb{E}(X_1|\mathcal{G}) = \sum_{k=0}^n \mathbb{E}(X_1|G_k)\,\mathbb{1}_{G_k}. \tag{19.4.32}$$

Now, $\mathbb{E}(X_1|G_k) = \mathbb{P}(X_1 = 1|S_n = k)$, $\quad \mathbb{P}(S_n = k) = \binom{n}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k} = \binom{n}{k}2^{-n}$.

Hence

$$\mathbb{P}\left(X_1=1|S_n=k\right)=\frac{\mathbb{P}\left(X_1=1,S_n=k\right)}{\mathbb{P}(S_n=k)}=\frac{\frac{1}{2}\binom{n-1}{k-1}\left(\frac{1}{2}\right)^{n-1}}{\binom{n}{k}2^{-n}}=\frac{k}{n}\quad\Rightarrow\quad\mathbb{E}\left(X_1|\mathcal{G}\right)=\sum_{k=0}^{n}\frac{k}{n}\mathbb{1}_{S_n=k}=\frac{S_n}{n}. \tag{19.4.33}$$

Example 19.4.17. Let $X\in\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$ and let Y be a r.v. taking values in some countable set E. Then $\Omega=\bigcup_{y\in E}\{Y=y\}$ is a partition of Ω which generates $\sigma(Y)$, and

$$\mathbb{E}\left(X|Y\right):=\mathbb{E}\left(X|\sigma(Y)\right)=\sum_{y\in E}\mathbb{E}\left(X|\{Y=y\}\right)\mathbb{1}_{\{Y=y\}}. \tag{19.4.34}$$

19.4.3 Conditional expectation

We now define the conditional expectation with respect to a sub-σ-algebra so that it satisfies the same properties as conditional expectation with respect to $\mathcal{G}=\sigma(B_i,i\in I)$ (as Definition 19.4.3). The following definition and theorem are due to Kolmogorov.

Theorem 19.4.18. Let $X\in\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$ and $\mathcal{G}\subseteq\mathcal{F}$ be a sub-σ-algebra. Then there exists an integrable r.v. Y such that

(i) Y is $\mathcal{G}$-measurable,

(ii) $Y\in\mathcal{L}^1(\Omega,\mathcal{G},\mathbb{P})$,

(iii) $\mathbb{E}\left(X\mathbb{1}_A\right)=\mathbb{E}\left(Y\mathbb{1}_A\right)$ for all $A\in\mathcal{G}$.

Moreover, if $\widetilde{Y}$ is another such r.v. then $Y=\widetilde{Y}$ a.s. We write $Y=\mathbb{E}\left(X|\mathcal{G}\right)$, a.s.

Remark. Note that if $\mathcal{G}$ is the trivial σ-algebra $\{\emptyset,\Omega\}$ (which contains no information), then $\mathbb{E}\left(X|\mathcal{G}\right)=\mathbb{E}(X)$ for all ω.

Proof of Almost sure uniqueness of $\mathbb{E}\left(X|\mathcal{G}\right)$. Suppose that $X\in\mathcal{L}^1$ and that Y and $\widetilde{Y}$ are versions of $\mathbb{E}\left(X|\mathcal{G}\right)$. Then, $Y,\widetilde{Y}\in\mathcal{L}^1\left(\Omega,\mathcal{G},\mathbb{P}\right)$, and for all $A\in\mathcal{G}$

$$\mathbb{E}\left(Y\mathbb{1}_A\right)=\mathbb{E}\left(X\mathbb{1}_A\right)=\mathbb{E}\left(\widetilde{Y}\mathbb{1}_A\right)\quad\Rightarrow\quad\mathbb{E}\left(\left(Y-\widetilde{Y}\right)\mathbb{1}_A\right)=0.\quad(*)\quad\text{(Theorem 15.3.10)} \tag{19.4.35}$$

Suppose that Y and $\widetilde{Y}$ are not almost surely equal. We may assume that the labelling is such that $\mathbb{P}(Y>\widetilde{Y})>0$. Since

$$\left\{Y>\widetilde{Y}+\frac{1}{n}\right\}\uparrow\left\{Y>\widetilde{Y}\right\}, \tag{19.4.36}$$

we see that $\mathbb{P}\left(Y-\widetilde{Y}>\frac{1}{n}\right)>0$ for some n. But the set $\left\{Y-\widetilde{Y}>\frac{1}{n}\right\}$ is in $\mathcal{G}$, because Y and $\widetilde{Y}$ are $\mathcal{G}$-measurable and

$$\mathbb{E}\left(\left(Y-\widetilde{Y}\right)\mathbb{1}_{Y-\widetilde{Y}>\frac{1}{n}}\right)\geq\frac{1}{n}\mathbb{P}\left(\left\{Y-\widetilde{Y}>\frac{1}{n}\right\}\right)>0, \tag{19.4.37}$$

a contradiction with $(*)$. Hence $Y=\widetilde{Y}$ a.s. □

Existence of $\mathbb{E}(X|\mathcal{G})$ for $X\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$. Suppose that $X\in\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$. Let $\mathcal{G}$ be a sub-σ-algebra of $\mathcal{F}$, then $\mathcal{L}^2(\Omega,\mathcal{G},\mathbb{P})$ is complete by Theorem 15.4.9. Then by orthogonal projection theorem (Theorem 19.3.27, there exists $Y\in\mathcal{L}^2(\Omega,\mathcal{G},\mathbb{P})$ such that

$$\mathbb{E}\left((X-Y)^2\right)=\inf\left\{\mathbb{E}\left((X-W)^2\right):W\in\mathcal{L}^2(\Omega,\mathcal{G},\mathbb{P})\right\},\qquad\langle X-Y,Z\rangle=0,\quad Z\in\mathcal{L}^2(\Omega,\mathcal{G},\mathbb{P}). \tag{19.4.38}$$

Now, if $A\in\mathcal{G}$, then $Z:=\mathbb{1}_A\in\mathcal{L}^2(\Omega,\mathcal{G},\mathbb{P})$, we have $\mathbb{E}\left((X-Y)Z\right)=0\ \Rightarrow\ \mathbb{E}\left(Y\mathbb{1}_A\right)=\mathbb{E}\left(X\mathbb{1}_A\right)$. Thus, Y is a version of $\mathbb{E}(X|\mathcal{G})$. □

Before proving the existence for the case that $X\in\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$, we have the following lemma:

Lemma 19.4.19. Let $(\Omega,\mathcal{F},\mathbb{P})$ be a probability measure and X be a non-negative bounded random variable, then

$$\mathbb{E}\left(X|\mathcal{G}\right)\geq 0\qquad\text{a.s.} \tag{19.4.39}$$

Proof. Since X is non-negative bounded, we have $X \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, thus, $\mathbb{E}(X|\mathcal{G})$ exists. Let Y be a version of $\mathbb{E}(X|\mathcal{G})$. If $\mathbb{P}(Y < 0) > 0$, then for some n, the set

$$A := \left\{ Y < -\frac{1}{n} \right\} \in \mathcal{G} \quad \text{has positive probability,} \quad \Rightarrow \quad 0 \leq \mathbb{E}\left(X \mathbb{1}_A\right) = \mathbb{E}\left(Y \mathbb{1}_A\right) < -\frac{1}{n}\mathbb{P}(A) < 0. \tag{19.4.40}$$

The contradiction finishes the proof. □

Existence of $\mathbb{E}(X|\mathcal{G})$ for $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. By splitting X as $X = X^+ - X^-$, we see that it is enough to deal with the case when $X \in \left(\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})\right)^+$. We can now choose bounded variables $X_n = X \wedge n$ with $0 \leq X_n \uparrow X$. Since X_n is bounded and thus in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, we can choose a version Y_n of $\mathbb{E}(X_n|\mathcal{G})$.

Since X_n is non-negative bounded random variable, from Lemma 19.4.19, $Y_n \geq 0$ a.s. Also, $X_{n+1} - X_n \geq 0$ implies that $Y_{n+1} \geq Y_n$ a.s.

$$\{0 \leq Y_n \uparrow\}^c = \left(\bigcap_n \{Y_{n+1} - Y_n \geq 0\} \right)^c = \bigcup_n \{Y_{n+1} - Y_n < 0\} \tag{19.4.41}$$

Thus,

$$\mathbb{P}\left(\{0 \leq Y_n \uparrow\}^c\right) = \mathbb{P}\left(\bigcup_n \{Y_{n+1} - Y_n < 0\} \right) \leq \sum_n \mathbb{P}\left(\{Y_{n+1} - Y_n < 0\}\right) = 0 \cdot \underbrace{\infty}_{\text{countable}} = 0 \quad \Rightarrow \quad 0 \leq Y_n \uparrow \quad \text{a.s..} \tag{19.4.42}$$

Then we set $Y(\omega) := \lim_n Y_n(\omega),\ \omega \in \{0 \leq Y_n \uparrow\}$, thus

$$Y \text{ is } \mathcal{G}\text{-measurable since } Y_n \text{ is measurable (by Theorem 15.2.7), and } Y_n \uparrow Y \text{ a.s..} \tag{19.4.43}$$

For any $A \in \mathcal{G}$, $\mathbb{E}\left(X_n \mathbb{1}_A\right) = \mathbb{E}\left(Y_n \mathbb{1}_A\right)$, also by monotone convergence theorem (Theorem 19.3.6),

$$\mathbb{E}\left(X_n \mathbb{1}_A\right) \to \mathbb{E}\left(X \mathbb{1}_A\right), \qquad \mathbb{E}\left(Y_n \mathbb{1}_A\right) \to \mathbb{E}\left(Y \mathbb{1}_A\right) \quad \Rightarrow \quad \mathbb{E}\left(X \mathbb{1}_A\right) = \mathbb{E}\left(Y \mathbb{1}_A\right). \tag{19.4.44}$$

Finally, we let $A = \Omega$, $\mathbb{E}\,|Y| = \mathbb{E}Y = \mathbb{E}\left(Y \mathbb{1}_\Omega\right) = \mathbb{E}\left(X \mathbb{1}_\Omega\right) = \mathbb{E}X < \infty$, thus $Y \in \mathcal{L}^1(\Omega, \mathcal{G}, \mathbb{P})$. □

Remark. The condition (iii) in Theorem 19.4.18 can be generalized to

$$\text{(iii')} \quad \mathbb{E}\left(ZX\right) = \mathbb{E}\left(ZY\right) \quad \text{for every bounded } \mathcal{G}\text{-measurable r.v. } Z. \tag{19.4.45}$$

To prove (iii') from (i), (ii) and (iii), first prove it for simple functions Z and then approximate general Z.

Proposition 19.4.20. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $\mathcal{G} \in \mathcal{F}$,

(i) If $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathcal{G} \subseteq \mathcal{F}$, then $\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)\right) = \mathbb{E}X$.

(ii) If X is $\mathcal{G}$-measurable and $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ then $\mathbb{E}\left(X|\mathcal{G}\right) = X$ a.s.

(iii) If $X, Y \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $a, b \in \mathbb{R}$ then $\mathbb{E}\left(aX + bY|\mathcal{G}\right) = a\mathbb{E}\left(X|\mathcal{G}\right) + b\mathbb{E}\left(Y|\mathcal{G}\right)$ a.s.

(iv) If $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ then $\left|\mathbb{E}\left(X|\mathcal{G}\right)\right| \leq \mathbb{E}\left(|X|\,|\mathcal{G}\right)$ a.s., which implies that $\mathbb{E}\left(\left|\mathbb{E}\left(X|\mathcal{G}\right)\right|\right) \leq \mathbb{E}\,|X|$.

(v) If $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $X \geq 0$ then $\mathbb{E}\left(X|\mathcal{G}\right) \geq 0$ a.s.

Proof. (i) Use Theorem 19.4.18 and let $\Omega = A \in \mathcal{G}$. Let Y be a version of $\mathbb{E}\left(X|\mathcal{G}\right)$, $\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)\right) = \mathbb{E}\left(Y \mathbb{1}_\Omega\right) = \mathbb{E}\left(X \mathbb{1}_\Omega\right) = \mathbb{E}X$.

(ii) Recall Theorem 19.4.18 and let $Y = X$, then $\mathbb{E}\left(Y \mathbb{1}_A\right) = \mathbb{E}\left(X \mathbb{1}_A\right)$ for any $A \in \mathcal{G}$, thus X is a version of $\mathbb{E}\left(X|\mathcal{G}\right)$, so $X = \mathbb{E}\left(X|\mathcal{G}\right)$ a.s.

(iii) Let X' be a version of $\mathbb{E}(X|\mathcal{G})$, Y' be a version of $\mathbb{E}(Y|\mathcal{G})$, for any $A \in \mathcal{G}$, by Theorem 15.3.10 as X' and Y' are integrable,

$$\mathbb{E}\left(X' \mathbb{1}_A\right) = \mathbb{E}\left(X \mathbb{1} A\right), \quad \mathbb{E}\left(Y' \mathbb{1}_A\right) = \mathbb{E}\left(Y \mathbb{1}_A\right) \quad \Rightarrow \quad \mathbb{E}\left(\left(aX' + bY'\right) \mathbb{1}_A\right) = \mathbb{E}\left(\left(aX + bY\right) \mathbb{1}_A\right). \tag{19.4.46}$$

then $aX' + bY'$ is a version of $\mathbb{E}\left(aX + bY|\mathcal{G}\right)$. Thus, $\mathbb{E}\left(aX + bY|\mathcal{G}\right) = a\mathbb{E}\left(X|\mathcal{G}\right) + b\mathbb{E}\left(Y|\mathcal{G}\right)$ a.s.

(iv) Let Y be a version of $\mathbb{E}(X|\mathcal{G})$, then

$$|\mathbb{E}(X|\mathcal{G})| = \left|\mathbb{E}\left(X^+ - X^-|\mathcal{G}\right)\right| \overset{\text{a.s.}}{=} \left|\mathbb{E}\left(X^+|\mathcal{G}\right) - \mathbb{E}\left(X^-|\mathcal{G}\right)\right| \leq \left|\mathbb{E}\left(X^+|\mathcal{G}\right)\right| + \left|\mathbb{E}\left(X^-|\mathcal{G}\right)\right|. \tag{19.4.47}$$

Since $X^+, X^- \geq 0$, we have $|\mathbb{E}(X^+|\mathcal{G})| + |\mathbb{E}(X^-|\mathcal{G})| \overset{\text{a.s.}}{=} \mathbb{E}(X^+ + X^-|\mathcal{G}) = \mathbb{E}(|X||\mathcal{G})$. so

$$|\mathbb{E}(X|\mathcal{G})| \leq \mathbb{E}(|X||\mathcal{G}) \quad \text{a.s.} \quad \Rightarrow \quad \mathbb{E}(|\mathbb{E}(X|\mathcal{G})|) \leq \mathbb{E}(\mathbb{E}(|X||\mathcal{G})) = \mathbb{E}|X| \quad \text{(by Theorem 15.3.10 and (i))} \tag{19.4.48}$$

(v) We can use the same as Lemma 19.4.19.

□

19.4.4 Non-negative conditional expectation

With Theorem 19.4.18, we actually built an object $\mathbb{E}(X|\mathcal{G})$ as the a.s. increasing limit of $\mathbb{E}(X \wedge n|\mathcal{G})$ for any non-negative random variable X, not necessarily integrable. This random variable enjoys similar properties as $\mathcal{L}^1$ case:

Theorem 19.4.21. Let X be a non-negative random variable and $\mathcal{G} \subseteq \mathcal{F}$ be a sub-σ-algebra. Then there exists a r.v. $Y \geq 0$ such that

(i) Y is $\mathcal{G}$-measurable,

(ii) $\mathbb{E}(ZX) = \mathbb{E}(ZY)$ for all non-negative $\mathcal{G}$-measurable random variable Z.

Moreover, if $\widetilde{Y}$ is another such r.v. then $Y = \widetilde{Y}$ a.s. We write $Y = \mathbb{E}(X|\mathcal{G})$, a.s.

Proof. Existence. Let $Y_n = \mathbb{E}(X \wedge n|\mathcal{G})$ a.s. and Y_n is $\mathcal{G}$-measurable (by Theorem 19.4.18 since $X \wedge n$ is bounded and thus integrable). Also, we know that $Y_n \geq 0$ a.s. by Lemma 19.4.19. Now let

$$Y = \begin{cases} \limsup_n Y_n & Y_n \geq 0 \\ 0 & Y_n < 0 \end{cases} \quad \text{i.e.,} \quad Y = \limsup_n Y_n \mathbb{1}_{\bigcap_n \{Y_n \geq 0\}}. \tag{19.4.49}$$

Thus $Y \geq 0$ is $\mathcal{G}$-measurable by Theorem 15.2.8. Then let $Z_n = Z \wedge n$, we have $Y_n Z \uparrow YZ$ a.s. for any non-negative random variable Z. Thus, by monontone convergence theorem (Theorem 19.3.6)

$$\mathbb{E}(Y_n Z_n) \uparrow \mathbb{E}(YZ). \tag{19.4.50}$$

Also $X_n Z_n \uparrow XZ$ implies $E(X_n Z_n) \uparrow \mathbb{E}(XZ)$ by monontone convergence theorem (Theorem 19.3.6). With Theorem 19.4.18 (iii'), we have

$$\mathbb{E}(X_n Z_n) = \mathbb{E}(Y_n Z_n) \quad \Rightarrow \quad \mathbb{E}(XZ) = \mathbb{E}(YZ). \tag{19.4.51}$$

Uniqueness. If Y and $\widetilde{Y}$ are non-negative and satisfy (i) and (ii). For any $a < b \in \mathbb{Q}^+$, by letting $B = \left\{Y \leq a < b \leq \widetilde{Y}\right\} \in \mathcal{G}$ since Y and $\widetilde{Y}$ are $\mathcal{G}$-measurable, we obtain

$$b\mathbb{P}(B) \leq \mathbb{E}(\widetilde{Y}\mathbb{1}_B) = \mathbb{E}(X\mathbb{1}_B) = \mathbb{E}(Y\mathbb{1}_B) \leq a\mathbb{P}(B) \tag{19.4.52}$$

which entails that $\mathbb{P}(B) = 0$, so that

$$\left\{Y < \widetilde{Y}\right\} = \underbrace{\bigcup_{a<b\in\mathbb{Q}^+} \left\{Y \leq a < b \leq \widetilde{Y}\right\}}_{\text{countable many}} \quad \Rightarrow \quad \mathbb{P}\left(Y < \widetilde{Y}\right) = 0 \tag{19.4.53}$$

Similarly, $\mathbb{P}\left(\widetilde{Y} < Y\right) = 0$, thus $Y = \widetilde{Y}$ a.s. □

Now we can generalize Proposition 19.4.20

Proposition 19.4.22. For $(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathcal{G} \subseteq \mathcal{F}$ be a sub-σ-algebra. If $0 \leq X \leq Y$, then $0 \leq \mathbb{E}(X|\mathcal{G}) \leq \mathbb{E}(Y|\mathcal{G})$ a.s.

Proof. First by Theorem 19.4.21, $\mathbb{E}(X|\mathcal{G})$ and $\mathbb{E}(Y|\mathcal{G})$ are well-defined. We can use the same as Lemma 19.4.19 to show that $\mathbb{E}(X|\mathcal{G}) \geq 0$ a.s. and $\mathbb{E}(Y|\mathcal{G}) \geq 0$ a.s.

Now let X' be a non-negative version of $\mathbb{E}(X|\mathcal{G})$ and Y' be a non-negative version of $\mathbb{E}(Y|\mathcal{G})$. If $\mathbb{P}(Y' < X') > 0$, then for some n, the set

$$A := \left\{ Y' < X' - \frac{1}{n} \right\} = \left\{ Y' + \frac{1}{n} < X' \right\} \in \mathcal{G} \quad \text{has positive probability,}$$

Then by Theorem 15.3.7 (ii), since $Y'\mathbb{1}_A + \frac{1}{n}\mathbb{1}_A \leq X'\mathbb{1}_A$,

$$\mathbb{E}\left(Y'\mathbb{1}_A\right) + \frac{1}{n}\mathbb{P}(A) \leq \mathbb{E}\left(X'\mathbb{1}_A\right) = \mathbb{E}\left(X\mathbb{1}_A\right) \leq \mathbb{E}\left(Y\mathbb{1}_A\right) = \mathbb{E}\left(Y'\mathbb{1}_A\right). \tag{19.4.54}$$

The contradiction finishes the proof. □

19.4.5 Specific theorems of conditional expectation

Theorem 19.4.23 (conditional monotone convergence Theorem)**.** Let $X_n \geq 0 (n \geq 0)$ be such that $X_n \uparrow X$ a.s. Then

$$\mathbb{E}\left(X_n|\mathcal{G}\right) \uparrow \mathbb{E}\left(X|\mathcal{G}\right) \text{ a.s.} \tag{19.4.55}$$

Proof. Note that if $0 \leq X \leq Y$ then $0 \leq \mathbb{E}\left(X|\mathcal{G}\right) \leq \mathbb{E}\left(Y|\mathcal{G}\right)$ a.s. (by Proposition 19.4.22). Let $Y_n = \mathbb{E}\left(X_n|\mathcal{G}\right)$ a.s., then Y_n increases with n a.s., so let $Y = \lim_{n\to\infty} Y_n$. Then for any $A \in \mathcal{G}$, by Theorem 19.3.6,

$$\mathbb{E}\left(X_n\mathbb{1}_A\right) \uparrow \mathbb{E}\left(X\mathbb{1}_A\right), \qquad \mathbb{E}\left(Y_n\mathbb{1}_A\right) \uparrow \mathbb{E}\left(Y\mathbb{1}_A\right) \tag{19.4.56}$$

so $\mathbb{E}\left(Y\mathbb{1}_A\right) = \mathbb{E}\left(X\mathbb{1}_A\right)$ and $Y = \mathbb{E}\left(X|\mathcal{G}\right)$ a.s. by uniqueness. □

Theorem 19.4.24 (Conditional Fatou's Lemma)**.** Let $X_n \geq 0$, $n \geq 0$. Then

$$\mathbb{E}\left(\liminf_{n\to\infty} X_n \middle| \mathcal{G}\right) \leq \liminf_{n\to\infty} \mathbb{E}\left(X_n|\mathcal{G}\right) \quad \text{a.s.} \tag{19.4.57}$$

(Inverse Conditional Fatou's Lemma). Additionally, if there exists a non-negative integrable random variable Y such that $X_n \leq Y$ for all n, then

$$\mathbb{E}\left(\limsup_{n} X_n \middle| \mathcal{G}\right) \geq \limsup_{n} \mathbb{E}(X_n|\mathcal{G}) \quad \text{a.s.} \tag{19.4.58}$$

Proof. For $k \geq n$, we have

$$\underbrace{\inf_{m\geq n} X_m \leq X_k \quad \Rightarrow \quad \mathbb{E}\left(\inf_{m\geq n} X_m \middle| \mathcal{G}\right) \leq \mathbb{E}(X_k|\mathcal{G}) \quad \text{a.s.}}_{\text{by Proposition 19.4.20 (v) since } X_n \text{ and } \inf X_n \text{ are non-negative measurable}} \quad \Rightarrow \quad \mathbb{E}\left(\inf_{m\geq n} X_m \middle| \mathcal{G}\right) \leq \inf_{k\geq n} \mathbb{E}(X_k|\mathcal{G}) \quad \text{a.s.} \tag{19.4.59}$$

Then we have

$$\mathbb{E}\left(\inf_{m\geq n} X_m \middle| \mathcal{G}\right) \leq \inf_{k\geq n} \mathbb{E}(X_k|\mathcal{G}) \leq \sup_{n} \inf_{k\geq n} \mathbb{E}(X_k|\mathcal{G}) = \liminf_{n} \mathbb{E}(X_n|\mathcal{G}) \quad \text{a.s.} \tag{19.4.60}$$

But, as $n \to \infty$,

$$\inf_{m\geq n} X_m \uparrow \sup_{n}\left(\inf_{m\geq n} X_m\right) = \liminf_{n} X_n \quad \Rightarrow \quad \mathbb{E}\left(\inf_{m\geq n} X_m \middle| \mathcal{G}\right) \uparrow \mathbb{E}\left(\liminf_{n} X_n \middle| \mathcal{G}\right) \quad \text{a.s.} \tag{19.4.61}$$

by conditional monotone convergence theorem (Theorem 19.4.23). Thus, $\mathbb{E}\left(\liminf_n X_n | \mathcal{G}\right) \leq \liminf \mathbb{E}(X_n|\mathcal{G})$.

For the second inequality, clearly we see that X_n and $\limsup X_n$ are integrable and apply Fatou's lemma to the sequence

$Y - X_n$,

$$\begin{aligned}
\mathbb{E}\left(\liminf_n (Y - X_n)\middle|\mathcal{G}\right) &\leq \liminf_n \mathbb{E}\left(Y - X_n|\mathcal{G}\right) \quad \text{a.s.} \\
\mathbb{E}\left(Y - \limsup X_n|\,\mathcal{G}\right) &\leq \liminf \mathbb{E}(Y|\mathcal{G}) - \mathbb{E}(X_n|\mathcal{G}) \quad \text{a.s.} \quad \text{(by Proposition 19.4.20 (iii))} \\
\mathbb{E}\left(Y|\mathcal{G}\right) - \mathbb{E}\left(\limsup_n X_n\middle|\,\mathcal{G}\right) &\leq \mathbb{E}(Y|\mathcal{G}) - \limsup \mathbb{E}(X_n|\mathcal{G}) \quad \text{a.s.} \quad \text{(by Proposition 19.4.20 (iii))} \\
\limsup_n \mathbb{E}(X_n|\mathcal{G}) &\leq \mathbb{E}\left(\limsup_n X_n\middle|\,\mathcal{G}\right) \quad \text{a.s.} \quad (\mathbb{E}\left(Y|\mathcal{G}\right) \text{ is integrable } (\mathbb{E}\left(Y|\mathcal{G}\right) < \infty \text{ a.s.}) \text{ by Theorem 19.4.18})
\end{aligned}$$

□

Theorem 19.4.25 (conditional dominated convergence theorem)**.** Let $X_n \to X$ a.s., and assume that $\sup_{n\geq 0}|X_n| \leq Y$ for some integral random variable Y. Then $\mathbb{E}\left(X|\mathcal{G}\right)$ is integrable and

$$\mathbb{E}\left(X_n|\mathcal{G}\right) \to \mathbb{E}\left(X|\mathcal{G}\right) \text{ a.s.} \tag{19.4.62}$$

Proof. Consider $Y - X_n$, $Y + X_n \geq 0$. By Proposition 19.4.20 (iii) and conditional Fatou's lemma (Lemma 19.4.24),

$$\mathbb{E}\left(Y - X|\mathcal{G}\right) \leq \liminf_{n\to\infty}(\mathbb{E}\left(Y|\mathcal{G}\right) - \mathbb{E}\left(X_n|\mathcal{G}\right)) \text{ a.s.}, \qquad \mathbb{E}\left(Y + X|\mathcal{G}\right) \leq \liminf_{n\to\infty}(\mathbb{E}\left(Y|\mathcal{G}\right) + \mathbb{E}\left(X_n|\mathcal{G}\right)) \text{ a.s.} \tag{19.4.63}$$

As $\mathbb{E}\left(Y|\mathcal{G}\right)$ is integrable, we get

$$\liminf_{n\to\infty} \mathbb{E}\left(X_n|\mathcal{G}\right) \geq \mathbb{E}\left(X|\mathcal{G}\right) \geq \limsup_{n\to\infty} \mathbb{E}\left(X_n|\mathcal{G}\right) \text{ a.s.} \quad \Rightarrow \quad \mathbb{E}(X|\mathcal{G}) = \lim_{n\to\infty} \mathbb{E}\left(X_n|\mathcal{G}\right) \text{ a.s.}$$ □

Theorem 19.4.26 (conditional Jensen inequality)**.** Let $c : I \to \mathbb{R}$ with $I \subseteq \mathbb{R}$ be a convex function, $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, and assume that $c(X) \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ or $c \geq 0$. Then

$$c(\mathbb{E}\left(X|\mathcal{G}\right)) \leq \mathbb{E}\left(c(X)|\mathcal{G}\right) \text{ a.s.}^6 \tag{19.4.64}$$

Proof. Since $c(X) \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, $\mathbb{E}\left(c(X)|\mathcal{G}\right)$ is well-defined. From Lemma 15.4.3, we have that there exist $a, b \in \mathbb{R}$ such that $c(x) \geq ax + b$ for all x. Furthermore, there exists a countable sequence (a_n, b_n) of points in $\mathbb{R}^2$ such that

$$c(x) \geq a_n x + b_n, \qquad c(x) = \sup_n (a_n x + b_n),\ x \in \mathbb{R}. \tag{19.4.65}$$

For $c(X) \in \mathcal{L}^1$, $c(x) - a_n x - b_n \geq 0$. Thus, by Proposition 19.4.20 (v), $\mathbb{E}\left(c(X) - a_n X - b_n|\mathcal{G}\right) \geq 0$ a.s. $\Rightarrow$ $\mathbb{E}\left(c(X)|\mathcal{G}\right) \geq \mathbb{E}\left(a_n X + b_n|\mathcal{G}\right)$ a.s. since $X \in \mathcal{L}^1$.

If $c \geq 0$, there exist $a_n x + b_n \geq 0$ and with Proposition 19.4.22, we also have $\mathbb{E}\left(c(X)|\mathcal{G}\right) \geq \mathbb{E}\left(a_n X + b_n|\mathcal{G}\right)$ a.s.

Therefore, by Proposition 19.4.20, $\mathbb{E}\left(a_n X + b_n|\mathcal{G}\right) = a_n \mathbb{E}\left(X|\mathcal{G}\right) + b_n$ a.s. Thus,

$$\mathbb{E}\left(c(X)|\mathcal{G}\right) \geq \sup_n \left\{a_n \mathbb{E}\left(X|\mathcal{G}\right) + b_n\right\} \text{ a.s.} \tag{19.4.66}$$

But $\sup_n \left\{a_n \mathbb{E}\left(X|\mathcal{G}\right) + b_n\right\} = c(\mathbb{E}\left(X|\mathcal{G}\right))$. So we have $\mathbb{E}\left(c(X)|\mathcal{G}\right) \geq c(\mathbb{E}\left(X|\mathcal{G}\right))$ a.s. □

Corollary 19.4.27. For probability space $(\Omega, \mathcal{F}, \mathbb{P})$, $\mathcal{G} \subseteq \mathcal{F}$ and $p \in [1, \infty)$, if $X \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, then

$$\left\|\mathbb{E}\left(X|\mathcal{G}\right)\right\|_p \leq \left\|X\right\|_p. \tag{19.4.67}$$

Proof. Let $c(x) = |x|^p$. It clear that $c(x)$ is convex. Since $X \notin \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, we have $\left\|X\right\|_p < \infty$. If $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, we use conditional Jensen's inequality (Theorem 19.4.26) to get

$$|\mathbb{E}\left(X|\mathcal{G}\right)|^p \leq \mathbb{E}\left(|X|^p\,|\mathcal{G}\right) \text{ a.s.} \tag{19.4.68}$$

[6] need the condition for equality.

We know that $\mathbb{E}\left(|X|^p|\mathcal{G}\right) \geq 0$ a.s., thus construct the non-negative random variable

$$Y = \begin{cases} \mathbb{E}\left(|X|^p|\mathcal{G}\right) & \mathbb{E}\left(|X|^p|\mathcal{G}\right) \geq 0 \\ 0 & \mathbb{E}\left(|X|^p|\mathcal{G}\right) < 0 \end{cases} \quad \Rightarrow \quad |\mathbb{E}\left(X|\mathcal{G}\right)|^p \leq Y \text{ a.s.} \tag{19.4.69}$$

Thus, by Theorem 15.3.7, we have

$$\mathbb{E}\left(|\mathbb{E}\left(X|\mathcal{G}\right)|^p\right) \leq \mathbb{E}Y = \mathbb{E}\left(\mathbb{E}\left(|X|^p|\mathcal{G}\right)\right) = \mathbb{E}\left(|X|^p\right) \qquad \text{(Proposition 19.4.20 (i))} \tag{19.4.70}$$

which gives the inequality $\left\|\mathbb{E}\left(X|\mathcal{G}\right)\right\|_p \leq \left\|X\right\|_p$. □

Remark. We can see that $X \mapsto \mathbb{E}\left(X|\mathcal{G}\right)$ is a continuous linear operator on $\mathcal{L}^p$ of (operator) norm (by Definition 10.3.2).

Proposition 19.4.28. Let $\mathcal{G} \subseteq \mathcal{F}$, then

(i) (tower property) If $\mathcal{H} \subseteq \mathcal{G}$ and either $X \in \mathcal{L}^1\left(\Omega, \mathcal{F}, \mathbb{P}\right)$ or $X \geq 0$, then $\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right) = \mathbb{E}\left(X|\mathcal{H}\right)$ a.s.

(ii) ('take out what is known') If Z is $\mathcal{G}$-measurable and bounded, $X \in \mathcal{L}^1\left(\Omega, \mathcal{F}, \mathbb{P}\right)$, then $\mathbb{E}\left(ZX|\mathcal{G}\right) = Z\mathbb{E}\left(X|\mathcal{G}\right)$ a.s.

(iii) If $p > 1$, $\frac{1}{p} + \frac{1}{q} = 1$, $X \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ and $Z \in \mathcal{L}^q(\Omega, \mathcal{G}, \mathbb{P})$, then $\mathbb{E}\left(ZX|\mathcal{G}\right) = Z\mathbb{E}\left(X|\mathcal{G}\right)$ a.s.

(iv) If either $X \in \mathcal{L}^1\left(\Omega, \mathcal{F}, \mathbb{P}\right)$ $ZX \in \mathcal{L}^1\left(\Omega, \mathcal{F}, \mathbb{P}\right)$ or $X, Z \geq 0$, then if Z is $\mathcal{G}$-measurable, $\mathbb{E}\left(ZX|\mathcal{G}\right) = Z\mathbb{E}\left(X|\mathcal{G}\right)$ a.s.

(v) (role of independence) If $\mathcal{H}$ is independent of $\sigma(\sigma(X), \mathcal{G})$ and $X \in \mathcal{L}^1\left(\Omega, \mathcal{F}, \mathbb{P}\right)$, then

$$\mathbb{E}\left(X|\sigma(\mathcal{G}, \mathcal{H})\right) = \mathbb{E}\left(X|\mathcal{G}\right) \text{ a.s.} \tag{19.4.71}$$

In particular, if X is independent of $\mathcal{H}$ then $\mathbb{E}\left(X|\mathcal{H}\right) = \mathbb{E}\left(X\right)$ a.s.

(vi) Let $\mathcal{G}$ be any σ-algebra and $\mathcal{N}$ be set of all the $\mathbb{P}$-null sets. If X is an integrable random variable, then

$$\mathbb{E}\left(X|\sigma(\mathcal{G}, \mathcal{N})\right) = \mathbb{E}\left(X|\mathcal{G}\right) \text{ a.s.} \tag{19.4.72}$$

Proof. (i) If $X \in \mathcal{L}^1$, let $A \in \mathcal{H} \subseteq \mathcal{G}$, then by Theorem 19.4.18,

$$\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{H}\right)\mathbb{1}_A\right) = \mathbb{E}\left(X\mathbb{1}_A\right) = \mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)\mathbb{1}_A\right) = \mathbb{E}\left(\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right)\mathbb{1}_A\right) \tag{19.4.73}$$

so both $\mathbb{E}\left(X|\mathcal{H}\right)$ and $\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right)$ are version of $\mathbb{E}\left(X|\mathcal{H}\right)$, thus $\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right) = \mathbb{E}\left(X|\mathcal{H}\right)$ a.s. by uniqueness (Theorem 19.4.18).

If $X \geq 0$, let W be any non-negative $\mathcal{H}$-measurable random variable, by Theorem 19.4.21,

$$\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{H}\right)W\right) = \mathbb{E}\left(XW\right) = \mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)W\right) = \mathbb{E}\left(\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right)W\right) \tag{19.4.74}$$

(ii) Since Z is bounded, we have $ZX \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, so $\mathbb{E}\left(ZX|\mathcal{G}\right)$ is well-defined. Thus, let Y be a version of $\mathbb{E}(X|\mathcal{G})$, it is enough to show that for any $A \in \mathcal{G}$,

$$\mathbb{E}\left(\mathbb{E}\left(ZX|\mathcal{G}\right)\mathbb{1}_A\right) = \mathbb{E}\left(ZX\mathbb{1}_A\right) \overset{\text{need to show}}{=} \mathbb{E}\left(ZY\mathbb{1}_A\right) = \mathbb{E}\left(Z\mathbb{E}\left(X|\mathcal{G}\right)\mathbb{1}_A\right) \qquad (*) \tag{19.4.75}$$

If $Z = \mathbb{1}_B$ where $B \in \mathcal{G}$, we have

$$\mathbb{E}\left(ZX\mathbb{1}_A\right) = \underbrace{\mathbb{E}\left(X\mathbb{1}_{A\cap B}\right) = \mathbb{E}\left(Y\mathbb{1}_{A\cap B}\right)}_{\text{definition of condition expectation}} = \mathbb{E}\left(ZY\mathbb{1}_A\right) \tag{19.4.76}$$

If Z is a simple function, we have the same result by Proposition 19.4.20 (iii). For any non-negative Z, we have the same result by letting $Z_n = 2^{-n}\left\lfloor 2^n Z\right\rfloor$ thus $Z_n \uparrow Z$ and apply monotone convergence theorem (Theorem 19.3.6). For general bounded Z, we can split $Z = Z^+ - Z^-$ then apply Proposition 19.4.20 (iii) again.

(iii) With Hölder's inequality (Theorem 19.3.24), we have

$$\mathbb{E}(|ZX|) \leq \|Z\|_q \|X\|_p < \infty \quad \Rightarrow \quad ZX \text{ is integrable.} \tag{19.4.77}$$

Let Y be a version of $\mathbb{E}(X|\mathcal{G})$, with the fact that $X \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ and $Y \in \mathcal{L}^p(\Omega, \mathcal{G}, \mathbb{P})$ (by Corollary 19.4.27, so YZ is integrable by Hölder's inequality (Theorem 19.3.24) and $\mathbb{E}(YZ)$ is well-defined) we can apply the same argument (*) in (ii).

(iv) Let Y be a version of $\mathbb{E}(X|\mathcal{G})$.

With the assumption, we know that XZ is integrable, also and YZ is non-negative a.s. as $Y \geq 0$ a.s. (by Proposition 19.4.20 (v)). Thus, we can choose any non-negative version of $\mathbb{E}(X|\mathcal{G})$, Y' such that $\mathbb{E}(Y'Z)$ is well-defined. Again, we can apply the argument (*) in (ii).

Let W be any non-negative $\mathcal{G}$-measurable random variable, then ZW is non-negative $\mathcal{G}$-measurable, by Theorem 19.4.21,

$$\mathbb{E}\left(X(ZW)\right) = \mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)(ZW)\right) \Rightarrow \mathbb{E}\left(XZ(W)\right) = \mathbb{E}\left(YZ(W)\right) \Rightarrow \mathbb{E}\left(XZ|\mathcal{G}\right) = Z\mathbb{E}\left(X|\mathcal{G}\right) \text{ a.s.} \tag{19.4.78}$$

by uniqueness of Theorem 19.4.21.

(v) Without loss of generality, we assume that $X \geq 0$. For $G \in \mathcal{G}$, $H \in \mathcal{H}$, $X\mathbb{1}_G$ and H are independent (by Definition 19.2.7), then by Proposition 19.3.12,

$$\mathbb{E}\left(X\mathbb{1}_{G\cap H}\right) = \mathbb{E}\left(\left(X\mathbb{1}_G\right)\mathbb{1}_H\right) = \mathbb{E}(X\mathbb{1}_G)\mathbb{P}(H). \tag{19.4.79}$$

Now let Y be a version of $\mathbb{E}(X|\mathcal{G})$. Since Y is $\mathcal{G}$-measurable, $Y\mathbb{1}_G$ is independent of $\mathcal{H}$ so that

$$\mathbb{E}\left(\left(Y\mathbb{1}_G\right)\mathbb{1}_H\right) = \mathbb{E}\left(Y\mathbb{1}_G\right)\mathbb{P}(H) \Rightarrow \mathbb{E}\left(X\mathbb{1}_{G\cap H}\right) = \mathbb{E}\left(Y\mathbb{1}_{G\cap H}\right). \tag{19.4.80}$$

Thus, consider two finite measures on $(\Omega, \sigma(\mathcal{G}, \mathcal{H}))$ where $\sigma(\mathcal{G}, \mathcal{H})$ has π-system with form $G \cap H$, $G \in \mathcal{G}, H \in \mathcal{H}$.

$$\mu_1(A) := \mathbb{E}\left(X\mathbb{1}_A\right), \quad \mu_2(A) := \mathbb{E}\left(Y\mathbb{1}_A\right), \quad \forall A = G \cap H,\ G \in \mathcal{G},\ H \in \mathcal{H}. \tag{19.4.81}$$

We know that $\mu_1(\Omega) = \mu_2(\Omega) < \infty$ since X is integrable and two measures agree on the π-system generating $\sigma(\mathcal{G}, \mathcal{H})$. Thus, by uniqueness of extension (Theorem 15.1.18), we have $\mu_1 = \mu_2$ on $\sigma(\mathcal{G}, \mathcal{H})$. Hence, $\forall A \in \sigma(\mathcal{G}, \mathcal{H})$

$$\mathbb{E}\left(\mathbb{E}(X|\sigma(\mathcal{G}, \mathcal{H}))\mathbb{1}_A\right) = \mathbb{E}\left(X\mathbb{1}_A\right) = \mu_1(A) = \mu_2(A) = \mathbb{E}\left(Y\mathbb{1}_A\right). \tag{19.4.82}$$

Then uniqueness of conditional expectation (Theorem 19.4.18) gives that

$$\mathbb{E}(X|\sigma(\mathcal{G}, \mathcal{H})) = Y \text{ a.s.} \Rightarrow \mathbb{E}(X|\sigma(\mathcal{G}, \mathcal{H})) = \mathbb{E}(X|\mathcal{G}) \text{ a.s.} \tag{19.4.83}$$

Now let $\mathcal{G} = \{\emptyset, \Omega\}$, we have $\mathbb{E}(X|\mathcal{H}) = X$ a.s.

(vi) It suffices to show that $\forall G \in \mathcal{G}, N \in \mathcal{N}$, for $Z = \mathbb{E}(X|\mathcal{G})$, $\mathbb{E}(X\mathbb{1}_{G\cap N}) = \mathbb{E}(Z\mathbb{1}_{G\cap N})$ (since $G \cap N$ is π-system of $\sigma(\mathcal{G}, \mathcal{N})$). Since X is integrable and $X\mathbb{1}_G\mathbb{1}_N = 0 = Z\mathbb{1}_G\mathbb{1}_N$ a.s., we can apply Theorem 15.3.10,

$$\mathbb{E}(X\mathbb{1}_{G\cap N}) = 0 = \mathbb{E}(Z\mathbb{1}_{G\cap N}). \tag{19.4.84}$$

□

Remark. (v) does not hold if we assume that $\sigma(X)$ is independent of $\mathcal{H}$ and $\mathcal{G}$ is independent of $\mathcal{H}$[7].

Proposition 19.4.29. If $\mathcal{H} \subseteq \mathcal{G} \subseteq \mathcal{F}$ and $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, then

$$\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{G}\right)|\mathcal{H}\right) = \mathbb{E}\left(\mathbb{E}\left(X|\mathcal{H}\right)|\mathcal{G}\right) \text{ a.s.} \tag{19.4.85}$$

[7] see example sheet

Proof. We can get the required result by combining Proposition 19.4.28.(i) and Proposition 19.4.20.(ii). □

19.4.6 Uniformly integrable property and multivariable conditional expectation

Theorem 19.4.30. Let $\mathcal{X}$ be a UI family of random variables on probability space $(\Omega, \mathcal{F}, \mathbb{P})$ Then, the set

$$\{\mathbb{E}(X|\mathcal{G}), X \in \mathcal{X}, \mathcal{G} \subseteq \mathcal{F}\} \quad \text{is also UI.} \tag{19.4.86}$$

Proof. Recalling Theorem 19.3.29, $\mathcal{X}$ is UI iff

$$\sup_{X\in\mathcal{X}} \mathbb{E}\left(|X| \mathbb{1}_{|X|>K}\right) \to 0 \text{ as } K \to \infty. \tag{19.4.87}$$

By Definition 19.3.6, we have that if $\mathcal{X}$ is UI then $X \in \mathcal{X}$ is bounded in $\mathcal{L}^1$, so for all $X \in \mathcal{X}$, we have $\mathbb{E}|X| < M$ where M is a constant. By Definition 19.3.6 again, $\mathcal{X}$ is UI then for any $\varepsilon > 0$, there exists $\delta > 0$ such that for any $A \in \mathcal{F}$ with $\mathbb{P}(A) < \delta$,

$$\sup_{X\in\mathcal{X}} \{\mathbb{E}(|X| \mathbb{1}_A)\} < \varepsilon. \tag{19.4.88}$$

Let $Y = \mathbb{E}(X|\mathcal{G})$. If set $c(x) = |x|$, with Jensen's inequality (Theorem 19.4.26, as $|X|$ is integrable),

$$|Y| = |\mathbb{E}(X|\mathcal{G})| \le \mathbb{E}(|X||\mathcal{G}) \text{ a.s. } (*) \quad \Rightarrow \quad |Y| \mathbb{1}_{\{|Y|>K\}} \le \mathbb{E}(|X||\mathcal{G}) \mathbb{1}_{\{|Y|>K\}} \text{ a.s. } (\dagger) \tag{19.4.89}$$

Now take $K = M/\delta$, let $A = \{|Y| > K\}$, we have (by Chebyshev inequality (Theorem 15.4.2)),

$$\mathbb{P}(A) = \mathbb{P}(\{|Y| > K\}) \le \frac{1}{K}\mathbb{E}|Y| \overset{(*)}{\le} \frac{1}{K}\mathbb{E}(\mathbb{E}(|X||\mathcal{G})) = \frac{1}{K}\mathbb{E}|X| \le \frac{M}{K} = \delta \quad \Rightarrow \quad \sup_{X\in\mathcal{X}} \{\mathbb{E}(|X| \mathbb{1}_A)\} < \varepsilon. \tag{19.4.90}$$

Also, with (†), we have (by Theorem 15.3.10),

$$\mathbb{E}\left(|Y| \mathbb{1}_{\{|Y|>K\}}\right) \le \mathbb{E}\left(\mathbb{E}(|X||\mathcal{G}) \mathbb{1}_{\{|Y|>K\}}\right) = \mathbb{E}\left(\mathbb{E}\left(|X| \mathbb{1}_{\{|Y|>K\}}|\mathcal{G}\right)\right) \tag{19.4.91}$$

by Proposition 19.4.28 (ii) since $\mathbb{1}_{\{|Y|>K\}}$ is $\mathcal{G}$-measurable and bounded (as $Y = \mathbb{E}(X|\mathcal{G})$ is $\mathcal{G}$-measurable). Then,

$$\mathbb{E}\left(|Y| \mathbb{1}_{\{|Y|>K\}}\right) \le \mathbb{E}\left(\mathbb{E}\left(|X| \mathbb{1}_{\{|Y|>K\}}|\mathcal{G}\right)\right) = \underbrace{\mathbb{E}\left(|X| \mathbb{1}_{\{|Y|>K\}}\right)}_{\text{Proposition 19.4.20 (i)}} < \varepsilon. \tag{19.4.92}$$

Thus, $Y = \mathbb{E}(X|\mathcal{G})$ is UI. □

Corollary 19.4.31. If X is $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ random variable on a probability space Ω, then the set of all of its condition expectations,

$$\{\mathbb{E}(X|\mathcal{G}) : \mathcal{G} \subseteq \mathcal{F}\} \quad \text{is UI.} \tag{19.4.93}$$

Proof. It is the direct result from Proposition 15.4.18 and Theorem 19.4.30. □

Proposition 19.4.32. Let X and Y be random variables and g be a non-negative measurable function with $g(X, Y) \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Let $\mathcal{G} \subseteq \mathcal{F}$ be a sub-σ-algebra, and assume that Y is $\mathcal{G}$-measurable and $\sigma(X)$ is independent of $\mathcal{G}$. Then

$$\mathbb{E}[g(X, Y)|\mathcal{G}] = \int g(x, Y)\mathbb{P}_X(dx). \tag{19.4.94}$$

Here $\mathbb{P}_X$ is the law of X, i.e. $\mathbb{P}_X(A) := \mathbb{P}(X \in A)$.

Proof. Let Z be $\mathbb{1}_A$ where $A \in \mathcal{G}$ thus Z is $\mathcal{G}$-measurable. Then (by Theorem 19.3.14)

$$\mathbb{E}(Zg(X, Y)) = \int zg(x, y)\mathbb{P}_{X,Y,Z}(dx, dy, dz) \tag{19.4.95}$$

But X is independent of (Z, Y) (Proposition 19.2.7), so (by Proposition 19.2.9)

$$\mathbb{P}_{X,Y,Z}(dx, dy, dz) = \mathbb{P}_X(dx)\mathbb{P}_{Y,Z}(dy, dz). \tag{19.4.96}$$

By Fubini's Theorem (Theorem 15.3.33),

$$\int zg(x,y)\mathbb{P}_{X,Y,Z}(dx,dy,dz) = \int \left(\int zg(x,y)\mathbb{P}_{Y,Z}(dy,dz) \right) \mathbb{P}_X(dx) = \int \mathbb{E}\left(Zg(x,Y)\right) \mathbb{P}_X(dx) = \mathbb{E}\left(Z \int g(x,Y)\mathbb{P}_X(dx) \right).$$

Thus,

$$\mathbb{E}\left(g(X,Y)\mathbb{1}_A\right) = \mathbb{E}\left(\int g(x,Y)\mathbb{P}_X(dx)\mathbb{1}_A \right). \tag{19.4.97}$$

Since $\int g(x,Y)\mathbb{P}_X(dx)$ is $\mathcal{G}$-measurable (Lemma 15.3.31) and integrable (Theorem 15.3.33), it is $\mathbb{E}\left(g(X,Y)|\mathcal{G}\right)$ by uniqueness (Theorem 19.4.18). □

19.4.7 Conditional probability density function

Definition 19.4.4 (Conditional density function)**.** Let $f_{X,Y}(x,y)$ be the joint distribution function of $X \in \mathbb{R}^m$ and $Y \in \mathbb{R}^n$ and

$$f_Y(y) = \int_{\mathbb{R}^m} f_{X,Y}(x,y)dx \tag{19.4.98}$$

be the marginal density function of Y (see Definition 19.3.3). Note that f_Y is Lebesgue-dy-integrable by Fubini theorem (Theorem 15.3.33.(ii).(a)).

Define the conditional probability density function of X given Y:

$$f_{X|Y}(x|y) := \begin{cases} f_{X,Y}(x,y)/f_Y(y) & f_Y(y) \neq 0 \\ 0 & \text{otherwise} \end{cases}. \tag{19.4.99}$$

Proposition 19.4.33. Let $X \in \mathbb{R}^m$ and $Y \in \mathbb{R}^n$ be two random variables. Let $f_{X|Y}(x,y)$ be the conditional probability density function of X given Y and h be Borel function on $\mathbb{R}^m$ such that $h(X)$ is integrable, i.e.,

$$\mathbb{E}\left|h(X)\right| = \int_{\mathbb{R}} \left|h(x)\right| f_X(x)dx < \infty, \tag{19.4.100}$$

where $f_X(x) = \int_{\mathbb{R}} f_{X,Y}(x,y)dy$. Set function $g : \mathbb{R}^n \to \mathbb{R}$,

$$g(y) = \int_{\mathbb{R}^m} h(x) f_{X|Y}(x|y)dx. \tag{19.4.101}$$

Then $Z := g(Y)$ is a version of the conditional expectation of $h(X)$ given $\mathcal{G} := \sigma(Y)$. That is,

$$\mathbb{E}\left(\, h(X)|\, \sigma(Y)\right) = \mathbb{E}\left(\, h(X)|\, \mathcal{G}\right) = \int_{\mathbb{R}} h(x) f_{X|Y}(x|Y)dx \text{ a.s..} \tag{19.4.102}$$

Remark. When $Y = y$, we have

$$\mathbb{E}\left(\, h(X)|\, Y = y\right) = \int_{\mathbb{R}^m} h(x) f_{X|Y}(x|y)dx \text{ a.s..} \tag{19.4.103}$$

Let $\nu(Y,dx)$ be the measure with density $f_{X|Y}(x|Y)$ with respect to Lebesgue measure dx. Then $\mathbb{E}\left(h(X)|Y\right) = \int_{x\in\mathbb{R}} h(x)\nu(Y,dx)$. When we have such a formula, we say that $\nu(Y,dx)$ is the conditional distribution of X given Y. Sometimes $\nu(y,dx)$ is called the conditional distribution of X given $Y = y$. These are defined only up a set of zero measure for y. We also say that $f_{X|Y}(x|y)$ is the conditional density function of X given $Y = y$.

Proof. For any $A \in \sigma(Y)$, for $x \in \mathbb{R}^m$ and $y \in \mathbb{R}^n$,

$$\mathbb{E}\left(h(X)\mathbb{1}_A\right) = \int h(x)\mathbb{1}_A(y) f_{X,Y}(x,y)dxdy = \underbrace{\int \left(\int h(x)\frac{f_{X,Y}(x,y)}{f_Y(y)}dx \right) \mathbb{1}_A(y) f_Y(y)dy}_{\text{Fubini theorem (Theorem 15.3.33}} = \mathbb{E}\left(g(Y)\mathbb{1}_A\right). \tag{19.4.104}$$

Since $\mathbb{E}(h(X)) = \int\int h(X) f_{X,Y}(x,y)dxdy < \infty$, $h(X)f_{X,Y}(x,y)$ is $dx \otimes dy$-integrable, and $f_{X,Y}(x,y)$ is also $dx \otimes dy$-integrable. Thus, by Fubini theorem (Theorem 15.3.33) (ii).(a), the following two integrals

$$\int_{\mathbb{R}^m} h(X) f_{X,Y}(x,Y)dx, \qquad \int_{\mathbb{R}^m} f_{X,Y}(x,Y)dx, \tag{19.4.105}$$

are $\mathcal{G}$-integrable. Thus, if $f_{X|Y}(x|Y) = 0$, then $g(Y) = 0$, is $\mathcal{G}$-measurable. Otherwise, by Theorem 15.3.7,

$$g(Y) = \int_{\mathbb{R}^m} h(x) f_{X|Y}(x|Y) dx = \int_{\mathbb{R}^m} \frac{h(X) f_{X,Y}(x,Y)}{f_Y(Y)} dx = \frac{\int_{\mathbb{R}^m} h(X) f_{X,Y}(x,Y) dx}{f_Y(Y)} = \frac{\int_{\mathbb{R}^m} h(X) f_{X,Y}(x,Y) dx}{\int_{\mathbb{R}^m} f_{X,Y}(x,y) dx}. \quad (19.4.106)$$

So both of denominator and numerator are $\mathcal{G}$-measurable, so $g(Y)$ is $\mathcal{G}$-measurable. Hence $g(Y)$ is a version of $\mathbb{E}(h(X)|\mathcal{G})$. □

Example 19.4.34. Recalling Example 19.3.19, the conditional densities are

$$f_{X|Y}(x|y) = \frac{8xy}{4y^3} = \frac{2x}{y^2}, \qquad f_{Y|X}(y|x) = \frac{8xy}{4x(1-x^2)} = \frac{2y}{1-x^2}, \quad (19.4.107)$$

for $0 \le x \le y \le 1$. We then have

$$\mathbb{E}(X|Y=y) = \int_0^y x \frac{2x}{y^2} dx = \frac{2y}{3} \text{ a.s.}, \qquad \mathbb{E}(Y|X=x) = \int_x^1 y \frac{2y}{1-x^2} dx = \frac{2(1-x^3)}{3(1-x^2)} \text{ a.s.}. \quad (19.4.108)$$

We see that $\mathbb{E}(X|Y) = 2Y/3$ a.s. and $\mathbb{E}(Y|X) = 2\left(1-X^3\right) / \left(3\left(1-X^2\right)\right)$ a.s.. Then we have

$$\begin{aligned} \mathbb{E}\left(\mathbb{E}(X|Y)\right) &= \int_0^1 \frac{2y}{3} f_Y(y) dy = \int_0^1 \frac{8y^4}{3} dy = \frac{8}{15} = \mathbb{E}X, \\ \mathbb{E}\left(\mathbb{E}(Y|X)\right) &= \int_0^1 \frac{2(1-x^3)}{3(1-x^2)} f_X(x) dx = \int_0^1 \frac{8x(1-x^3)}{3} dx = \frac{4}{5} = \mathbb{E}Y, \end{aligned}$$

which are consistent with results in Example 19.3.19.

19.5 Characteristic Function and Moment Generating Function

19.5.1 Characteristic function

Definition 19.5.1 (Characteristic Function)**.** For a random variable X in $\mathbb{R}^n$, we define the characteristic function

$$\phi_X(u) = \mathbb{E}\left(e^{i\langle u, X\rangle}\right) = \int_\Omega e^{i\langle u, X(\omega)\rangle} \mathbb{P}(d\omega), \quad u \in \mathbb{R}^n. \quad (19.5.1)$$

Thus $\phi_X = \widehat{\mu}_X$ (Fourier transform (Definition 15.4.12) of μ_X and Theorem 19.3.14), where μ_X is the law of X. Also, $\overline{\phi_X(u)} = \phi_X(-u)$.

Definition 19.5.2. A random variable X in $\mathbb{R}^n$ is standard Gaussian if

$$\mathbb{P}(X \in A) = \int_A \frac{1}{(2\pi)^{n/2}} e^{-|x|^2/2} dx, \quad A \in \mathcal{B}(\mathbb{R}^n). \quad (19.5.2)$$

Proposition 19.5.1 (The characteristic function of a standard Gaussian random variable X in $\mathbb{R}$)**.** We have

$$\phi_X(u) = \int_{\mathbb{R}} e^{iux} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx = e^{-u^2/2} I \qquad \text{where} \quad I = \int_{\mathbb{R}} \frac{1}{\sqrt{2\pi}} e^{-(x-iu)^2/2} dx. \quad (19.5.3)$$

The integral I can be evaluated by considering the integral of the analytic function $e^{-z^2/2}$ around the rectangular contour with corners R, $R-iu$, $-R-iu$, $-R$: by Cauchy's residue theorem (Theorem 11.0.3), the integral round the contour vanishes, as do, in the limit $R \to \infty$, the contributions from the vertical sides of the rectangle. We deduce that

$$I = \int_{\mathbb{R}} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx = 1 \quad \Rightarrow \quad \phi_X(u) = e^{-u^2/2}. \quad (19.5.4)$$

We now show that a finite Borel measure is determined uniquely by its Fourier transform and obtain, where possible, an inversion formula by which to compute the measure from its transform.

Definition 19.5.3 (heat kernel)**.** Define, for $t > 0$ and $x, y \in \mathbb{R}^n$, the heat kernel (or transition density of n-dimensional Brownian motion (starts from x)),

$$p_t(x,y) = \frac{1}{(2\pi t)^{n/2}} e^{-|y-x|^2/2t} = \prod_{k=1}^{n} \frac{1}{\sqrt{2\pi t}} e^{-|y_k - x_k|^2/2t}. \tag{19.5.5}$$

Remark. This is the fundamental solution for the heat equation $\left(\partial/\partial t - \frac{1}{2}\Delta\right) p = 0$ in $\mathbb{R}^n$, where $\Delta = \sum_{i=1}^n \frac{\partial^2}{\partial x_i^2}$. But we shall not pursue this property here.[8]

Lemma 19.5.2. Let Z be a standard Gaussian random variable in $\mathbb{R}^n$. Let $x \in \mathbb{R}^n$ and $t \in (0,\infty)$. Then

(i) the random variable $Y = x + \sqrt{t}Z$ has density function $p_t(x,\cdot)$ on $\mathbb{R}^n$,

(ii) for all $y \in \mathbb{R}^n$, we have

$$p_t(x,y) = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^n} e^{i\langle u,x\rangle} e^{-|u|^2 t/2} e^{-i\langle u,y\rangle} du. \tag{19.5.6}$$

Proof. The component random variables $Y_k = x_k + \sqrt{t}Z_k$ are independent Gaussians with mean x_k and variance t. So Y_k has density

$$\frac{1}{\sqrt{2\pi t}} e^{-|y_k - x_k|^2/2t} \tag{19.5.7}$$

and we obtain the claimed density function for Y as the product of the marginal densities.

For $u \in \mathbb{R}$ and $t \in (0,\infty)$, we know that

$$\int_{\mathbb{R}} e^{iux} \frac{1}{\sqrt{2\pi t}} e^{-|x|^2/2t} dx = \mathbb{E}\left(e^{iu\sqrt{t}Z_1}\right) = e^{-u^2 t/2}. \tag{19.5.8}$$

let $u_k = tx$, $x_k - y_k = u/t$, thus $x_k, y_k, u_k \in \mathbb{R}$ and $t \in (0,\infty)$,

$$\int_{\mathbb{R}} e^{iu_k(x_k - y_k)} \frac{\sqrt{t}}{\sqrt{2\pi}} e^{-t|u_k|^2/2} du_k = e^{-(x_k - y_k)^2/2t} \quad \Rightarrow \quad \frac{1}{\sqrt{2\pi t}} e^{-|y_k - x_k|^2/2t} = \frac{1}{2\pi} \int_{\mathbb{R}} e^{iu_k x_k} e^{-u_k^2 t/2} e^{-iu_k y_k} du_k. \tag{19.5.9}$$

On taking the product over $k \in \{1,\ldots,n\}$, we obtain the claimed formula for $p_t(x,y)$. □

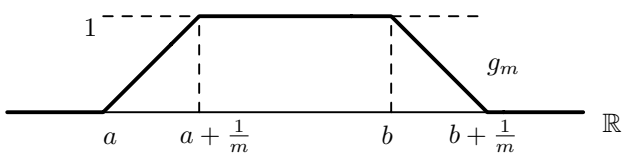
Theorem 19.5.3 (The inversion formula for densities)**.** Let X be a random variable in $\mathbb{R}^n$. The law μ_X of X is uniquely determined by its characteristic function ϕ_X. Moreover, if ϕ_X is integrable, and we define

$$f_X(x) = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^n} \phi_X(u) e^{-i\langle u,x\rangle} du, \tag{19.5.10}$$

then f_X is a bounded, continuous and real, non-negative function, which is a density function for X, i.e., if $n = 1$

$$\mathbb{P}(a < X \le b) = \int_a^b f_X(x) dx, \qquad \text{for all } -\infty < a < b < \infty. \tag{19.5.11}$$

Proof. Let $m \in \mathbb{N}$ and let $g_m : \mathbb{R} \to \mathbb{R}$ be the function graphed below:



Let Z be a standard Gaussian random variable in $\mathbb{R}^n$, independent of X, and for any $t \in (0,\infty)$. Let $X_t = X + \sqrt{t}Z$, from Lemma 19.5.2, random variable $x + \sqrt{t}Z$ has density function

$$p_t(x,y) = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^n} e^{i\langle u,x\rangle} e^{-|u|^2 t/2} e^{-i\langle u,y\rangle} du. \tag{19.5.12}$$

[8] in sfm

by Fubini's theorem (Theorem 15.3.33 since g is bounded and thus integrable),

$$\mathbb{E}(g_m(X+\sqrt{t}Z)) = \frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} g_m(x+\sqrt{t}z)e^{-|z|^2/2}dz\mu_X(dx). \tag{19.5.13}$$

Then we have (by Theorem 19.3.15)

$$\begin{aligned}\int_{\mathbb{R}^n} g_m(x+\sqrt{t}z)\frac{1}{(2\pi)^n}e^{-|z|^2/2}dz &= \mathbb{E}(g_m(x+\sqrt{t}Z)) = \int_{\mathbb{R}^n} g_m(y)p_t(x,y)dy \\ &= \frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} e^{i\langle u,x\rangle}e^{-|u|^2t/2}e^{-i\langle u,y\rangle}du g_m(y)dy,\end{aligned}$$

so, by Fubini theorem again,

$$\begin{aligned}\mathbb{E}\left(g_m(X_t)\right) &= \int_{\mathbb{R}^n}\left(\frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\left(\int_{\mathbb{R}^n} e^{i\langle u,x\rangle}\mu_X(dx)\right)e^{-|u|^2t/2}e^{-i\langle u,y\rangle}du\right)g_m(y)dy \\ &= \int_{\mathbb{R}^n}\left(\frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\phi_X(u)e^{-|u|^2t/2}e^{-i\langle u,y\rangle}du\right)g_m(y)dy. \quad (*)\end{aligned}$$

Let Y be another random variable with characteristic function ϕ_Y. If $\phi_X = \phi_Y$, let $Y_t = Y + \sqrt{t}Z$, thus, with the same argument for $(*)$, we have

$$\int_{\mathbb{R}^n}\left(\frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\phi_X(u)e^{-|u|^2t/2}e^{-i\langle u,y\rangle}du\right)g_m(y)dy = \int_{\mathbb{R}^n}\left(\frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\phi_Y(u)e^{-|u|^2t/2}e^{-i\langle u,y\rangle}du\right)g_m(y)dy = \mathbb{E}\left(g_m(Y_t)\right).$$

Note that the integral (expectation) of left hand side is well defined since g_m is bounded. So by Theorem 19.3.14 we have

$$\mu_{X_t}(g_m) = \mathbb{E}\left(g_m(X_t)\right) = \mathbb{E}\left(g_m(Y_t)\right) = \mu_{Y_t}(g_m). \tag{19.5.14}$$

Then by bounded convergence theorem (Theorem 19.3.10),

$$\mu_{X_t}(g_m) = \mathbb{E}\left(g_m(X_t)\right) \to \mathbb{E}\left(g(X_t)\right) \to \mathbb{E}\left(g(X)\right) = \mu_X((a,b]). \qquad \text{(similar for } Y_t\text{)} \tag{19.5.15}$$

Let $a = -\infty$, we have $\mu_{X_t}(g_m) \to \mu_X((-\infty,b])$. Thus $\mu_X((-\infty,b]) = \mu_Y((-\infty,b])$. Since $(-\infty,b]$ forms a π-system and thus

$$\mu_X(A) = \mu_Y(A) \quad \forall A \in \mathcal{B}(\mathbb{R}^n) \quad \Rightarrow \quad \text{Thus, } \phi_X \text{ determines } \mu_X \text{ uniquely.} \tag{19.5.16}$$

Now if ϕ_X is integrable, $f_X(x)$ exists since

$$\int_{\mathbb{R}^n}\left|e^{-i\langle u,x\rangle}\phi_X(u)\right|du = \int_{\mathbb{R}^n}|\phi_X(u)|\,du < \infty. \tag{19.5.17}$$

f_X is bounded since

$$(2\pi)^n|f_X(x)| = \left|\int_{\mathbb{R}^n} e^{-i\langle u,x\rangle}\phi_X(u)du\right| \le \int_{\mathbb{R}^n}|\phi_X(u)|\,du < \infty. \tag{19.5.18}$$

To show that f_X is continuous, i.e. $f(x_n) \to f(x)$, as $x_n \to x$. That is

$$\frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\phi_X(u)e^{-i\langle u,x_n\rangle}du \to \frac{1}{(2\pi)^n}\int_{\mathbb{R}^n}\phi_X(u)e^{-i\langle u,x\rangle}du. \tag{19.5.19}$$

This follows from the dominated convergence theorem (Theorem 19.3.8), since

$$\phi_X(u)e^{-i\langle u,x_n\rangle} \to \phi_X(u)e^{-i\langle u,x\rangle} \qquad \text{for all } u \in \mathbb{R}, \qquad \text{and} \qquad \int_{\mathbb{R}^n}\left|\phi_X(u)e^{-i\langle u,x_n\rangle}\right| \le \int_{\mathbb{R}^n}|\phi_X(u)| < \infty. \tag{19.5.20}$$

Since $\overline{\phi_X(u)} = \phi_X(-u)$, we have $\overline{f}_X = f_X$, so f_X is real-valued. Since f_X is continuous, if it took a negative value anywhere, it would do so on an open interval of positive length, I say. There would exist a continuous function g, positive on I and vanishing outside I. Then we would have $\mathbb{E}(g(X)) \ge 0$ and $\int_{\mathbb{R}^n} g(x)f_X(x)dx < 0$, a contradiction. Hence, f_X is non-negative.

Now consider the case $n = 1$, from $(*)$ and Propositions 19.3.14,

$$\mu_{X_t}(g_m) = \mathbb{E}\left(g_m(X_t)\right) = \int_\Omega g_m\left(X_t(\omega)\right)\mathbb{P}(d\omega) = \int_{\mathbb{R}} g_m(x) f_t(x) dx. \tag{19.5.21}$$

where

$$f_t(x) := \frac{1}{2\pi}\int_{\mathbb{R}} \phi_X(u) e^{-u^2 t/2} e^{-i\langle u,x\rangle} du. \qquad (\dagger) \tag{19.5.22}$$

We have as $t \to 0$, by bounded convergence theorem (Theorem 19.3.10)

$$\int_{\mathbb{R}} g_m\left(X_t(\omega)\right)\mathbb{P}(d\omega) \to \int_{\mathbb{R}} g_m\left(X(\omega)\right)\mathbb{P}(d\omega) \quad \text{since} \quad g_m\left(X_t(\omega)\right) \to g_m\left(X(\omega)\right) \text{ and } \left|g_m\left(X_t(\omega)\right)\right| \le 1. \tag{19.5.23}$$

Also, by dominated convergence theorem (Theorem 19.3.8)

$$\int_{\mathbb{R}} g_m(x) f_t(x) dx \to \int_{\mathbb{R}} g_m(x) f(x) dx \tag{19.5.24}$$

since by $(\dagger)$, $f_t(x) \to f(x)$,

$$g_m(x) f_t(x) \to g_m(x) f(x) \text{ and } \int \left|g_m(x) f_t(x)\right| dx \le \left|\int g_m(x) dx\right| \sup\left|f_t(x)\right| \le (b+1-a)\int_{\mathbb{R}} \left|\phi(u)\right| du < \infty.$$

Thus, we get

$$\mathbb{E}\left(g_m(X)\right) = \int_\Omega g_m\left(X(\omega)\right)\mathbb{P}(d\omega) = \int_{\mathbb{R}} g_m(x) f(x) dx. \tag{19.5.25}$$

Since $g_m \to g = \mathbb{1}_{(a,b]}$ pointwise and boundedly, by bounded convergence theorem (Theorem 19.3.10), we have

$$\int_\Omega g_m\left(X(\omega)\right)\mathbb{P}(d\omega) \to \int_\Omega g\left(X(\omega)\right)\mathbb{P}(d\omega) \quad \text{since} \quad g_m\left(X(\omega)\right) \to g\left(X(\omega)\right) \text{ and } \left|g_m\left(X(\omega)\right)\right| \le 1. \tag{19.5.26}$$

Also, by dominated convergence theorem (Theorem 19.3.8)

$$\int_{\mathbb{R}} g_m(x) f(x) dx \to \int_{\mathbb{R}} g(x) f(x) dx \qquad \text{since} \tag{19.5.27}$$

$$g_m(x) f(x) \to g(x) f(x) \text{ and } \int \left|g_m(x) f(x)\right| dx \le \left|\int g_m dx\right| \sup\left|f(x)\right| \le (b+1-a)\int_{\mathbb{R}} \left|\phi(u)\right| du < \infty.$$

Then, we have

$$\mathbb{E}\left(g(X)\right) = \int_\Omega g\left(X(\omega)\right)\mathbb{P}(d\omega) = \int_{\mathbb{R}} g(x) f(x) dx = \int_{\mathbb{R}} \mathbb{1}_{(a,b]} f(x) dx = \int_a^b f(x) dx. \tag{19.5.28}$$

The proof of higher dimensional case is similar. □

The relation of law, distribution function, characteristic function and density function From the previous results, we have the law of random variable (distribution function) determines the characteristic function (Definition 19.5.1). Then characteristic function determines the law (no matter integrable or not) and density function if it is integrable (Theorem 19.5.3). Since the law is unique, the characteristic function and density function are unique as well.

Remark. Binomal, Poisson, $U[0,1]$ distributions do not have continuous density function so cannot have integrable characteristic functions.

19.5.2 Characteristic functions and independence

Theorem 19.5.4. Let $X = (X_1, \ldots, X_n)$ be a random variable in $\mathbb{R}^n$. Then the following are equivalent:

(i) $X_1, \ldots, X_n$ are independent,

(ii) $\mu_X = \mu_{X_1} \otimes \cdots \otimes \mu_{X_n}$,

(iii) $\mathbb{E}\left(\prod_k f_k(X_k)\right) = \prod_k \mathbb{E}(f_k(X_k))$, for all bounded Borel functions $f_1, \ldots, f_n$,

(iv) $\phi_X(u) = \prod_k \phi_{X_k}(u_k)$, for all $u = (u_1, \ldots, u_n) \in \mathbb{R}^n$,

(v) $f_X(x) = \prod_k f_{X_k}(x_k)$, Leb^n-a.e. for the density functions $f_X, f_{X_1}, \ldots, f_{X_n}$.

Proof. If (i) holds, then by Proposition 19.2.9, for all $x_i \in \mathbb{R}$,

$$\mathbb{P}(X_1 \leq x_1, \ldots, X_n \leq x_n) = \mathbb{P}(X_1 \leq x_1) \ldots \mathbb{P}(X_n \leq x_n). \tag{19.5.29}$$

Then by Definitions 19.2.2, 19.2.4,

$$\mu_X(A_1 \times \cdots \times A_n) = \prod_k \mu_{X_k}(A_k) \tag{19.5.30}$$

for all Borel sets $A_1, \ldots, A_n$, so (ii) holds, since this formula characterizes the product measure (Theorem 15.3.32).

If (ii) holds, then, for $f_1, \ldots, f_n$ bounded Borel functions (thus μ_{X_i}-integrable),

$$\mathbb{E}\left(\prod_k f_k(X_k)\right) \underbrace{= \int_{\mathbb{R}^n} \prod_k f_k(x_k) \mu_X(dx)}_{\text{Theorem 19.3.15}} \underbrace{= \prod_k \int_{\mathbb{R}} f_k(x_k) \mu_{X_k}(dx_k)}_{\text{Fubini's theorem (Theorem 15.3.33)}} \underbrace{= \prod_k \mathbb{E}(f_k(X_k))}_{\text{Theorem 19.3.15}}, \tag{19.5.31}$$

so (iii) holds. Statement (iv) is a special case of (iii) since (by Definition 19.5.1)

$$\phi_X = \mathbb{E}\left(e^{i\langle u, X\rangle}\right), \qquad \text{where} \quad e^{i\langle u,x\rangle} \text{ is bounded, } x \in \mathbb{R}^n. \tag{19.5.32}$$

Suppose that (iv) holds and take independent random variables $\widetilde{X}_1, \ldots, \widetilde{X}_n$ with $\mu_{\widetilde{X}_k} = \mu_{X_k}$ for all k. We know that (i) implies (iv), $\phi_{\widetilde{X}_k}(u_k) = \phi_{X_k}(u_k)$ so

$$\phi_{\widetilde{X}}(u) = \prod_k \phi_{\widetilde{X}_k}(u_k) = \prod_k \phi_{X_k}(u_k) = \phi_X(u) \tag{19.5.33}$$

so $\mu_{\widetilde{X}} = \mu_X$ by Theorem 19.5.3. Thus, $\forall x_i \in \mathbb{R}, i = 1, \ldots, n$,

$$\begin{aligned}
\mathbb{P}(X_1 \leq x_1, \ldots, X_n \leq x_n) &= \mu_X\left(\bigotimes_{i=1}^n (-\infty, x_i]\right) \qquad \text{(Definition 19.2.4)} \\
&= \mu_{\widetilde{X}}\left(\bigotimes_{i=1}^n (-\infty, x_i]\right) = \mu_{\widetilde{X}_1}((-\infty, x_1]) \otimes \cdots \otimes \mu_{\widetilde{X}_n}((-\infty, x_n]) \quad \text{by (ii)} \\
&= \mu_{X_1}((-\infty, x_1]) \otimes \cdots \otimes \mu_{X_n}((-\infty, x_n]) \\
&= \mathbb{P}(X_1 \leq x_1) \ldots \mathbb{P}(X_n \leq x_n). \qquad \text{(Definition 19.2.2)}
\end{aligned}$$

Then by Proposition 19.2.9, $X_1, \ldots, X_n$ are independent. Hence (i) holds.

Finally, if (ii) holds, we have by Theorem 15.3.32,

$$\mu_X\left(\bigotimes_k (-\infty, y_k]\right) = \mu_{X_1}((-\infty, y_1]) \ldots \mu_{X_n}((-\infty, y_n]) \tag{19.5.34}$$

which is equivalent to

$$\int_{\bigotimes_k (-\infty, y_k]} f_X(x)dx = \int_{-\infty}^{y_1} f_{X_1}(x_1)dx_1 \ldots \int_{-\infty}^{y_n} f_{X_n}(x_n)dx_n = \int_{\bigotimes_k (-\infty, y_k]} \prod_k f_{X_k}(x_k)dx \qquad (*) \tag{19.5.35}$$

by Theorem 19.3.15. Thus since f is non-negative, by Theorem 15.3.7, it holds if $f_X(x) = \prod_k f_{X_k}(x_k)$ a.e. (with respect to Lebesgue measure). If $(*)$ holds, then $f_X(x) = \prod_k f_{X_k}(x_k)$ a.e. by uniqueness of density function (Theorem 15.3.23) as $f_X(x)$ and $\prod_k f_{X_k}(x_k)$ are density function. Hence (v) holds. □

Example 19.5.5. We will show that there do not exist independent identically distributed random variables X, Y such

that

$$X - Y \sim \mathcal{U}[-1,1]^9. \tag{19.5.36}$$

Using the fact that X and Y are i.i.d., we have by Definition 19.5.1 and Theorem 19.5.4,

$$\phi_{X-Y} = \phi_X \phi_{-Y} = \phi_X \overline{\phi_Y} = \phi_X \overline{\phi_X} = |\phi_X|^2 \geq 0 \tag{19.5.37}$$

However,

$$\phi_{X-Y}(u) = \mathbb{E}\left(e^{iu(X-Y)}\right) = \frac{1}{2}\int_{-1}^{1} e^{iux} dx = \frac{\sin u}{u}. \tag{19.5.38}$$

When $u = 3\pi/2$ the right hand side is negative. So the characteristic function of $\mathcal{U}[-1,1]$ is not non-negative everywhere.

Proposition 19.5.6. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be probability space and $\mathcal{E}$ be a σ-algebra. The the random variable vector $X = (X_1, \ldots, X_k)$ is independent of $\mathcal{E}$ if and only if for any $A \in \mathcal{E}$ and any continuous bounded function $f : \mathbb{R}^n \to \mathbb{R}$,

$$\mathbb{E}\left(\mathbb{1}_A f(X_1, \ldots, X_k)\right) = \mathbb{P}(A)\mathbb{E}\left(f(X_1, \ldots, X_k)\right) \qquad (*). \tag{19.5.39}$$

Proof. Since $A \in \mathcal{E}$, $\mathbb{1}_A$ is $\mathcal{E}$-measurable, so we have $\mathbb{1}_A$ and X are independent by Proposition 19.2.7. Then by Theorem 19.5.4.(iii), for any bounded continuous function f,

$$\mathbb{E}\left(\mathbb{1}_A f(X_1, \ldots, X_k)\right) = \mathbb{E}\left(\mathbb{1}_A\right)\mathbb{E}(f(X_1, \ldots, X_k)) = \mathbb{P}(A)\mathbb{E}\left(f(X_1, \ldots, X_k)\right). \tag{19.5.40}$$

Now suppose for any $A \in \mathcal{F}$, $(*)$ holds. Let $B \in \mathcal{A}$ where $\mathcal{A}$ is the π-system generating $\sigma(X_1, \ldots, X_k)$. Thus, B is of the form $\bigcap_{i=1}^k B_i = \bigcap_{i=1}^k \{\omega : X_i(\omega) \leq y_i\}$. Thus, we define continuous bounded functions f_n,

$$f_n(x_1, \ldots, x_k) = \prod_{i=1}^k f_{n,i}, \qquad \text{where } f_{n,i} = \begin{cases} 1 & x_i \leq y_i \\ \frac{x_i - y_i}{\frac{1}{n}} & y_i \leq x_i \leq y_i + \frac{1}{n} \\ 0 & x_i \geq y_i + \frac{1}{n} \end{cases}, \quad i = 1, \ldots, k. \tag{19.5.41}$$

Then by the assumption, we have

$$\mathbb{E}\left(\mathbb{1}_A f_n(X_1, \ldots, X_k)\right) = \mathbb{P}(A)\mathbb{E}\left(f_n(X_1, \ldots, X_k)\right) \tag{19.5.42}$$

Also, we can see that $f_n(X_1, \ldots, X_1) \to \mathbb{1}_B$ as $n \to \infty$. Thus, by bounded convergence theorem (Theorem 19.3.10), we have

$$\mathbb{E}\left(\mathbb{1}_A \mathbb{1}_B\right) = \mathbb{P}(A)\mathbb{E}\left(\mathbb{1}_B\right) = \mathbb{P}(A)\mathbb{P}(B). \tag{19.5.43}$$

Since B is arbitary set in the π-system generating $\sigma(X_1, \ldots, X_k)$, we have for any $A \in \mathcal{E}$ and $B \in \sigma(X_1, \ldots, X_k)$ (by Theorem 19.1.20), $\mathbb{E}\left(\mathbb{1}_A \mathbb{1}_B\right) = \mathbb{P}(A)\mathbb{P}(B)$. This means that X is independent of $\mathcal{E}$. □

Corollary 19.5.7. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be probability space and $\mathcal{G}$ be a σ-algebra. The the random variable vector $X = (X_1, \ldots, X_k)$ is independent of $\mathcal{G}$ if and only if for any continuous bounded Borel function $f : \mathbb{R}^n \to \mathbb{R}$,

$$\mathbb{E}\left(f(X_1, \ldots, X_k)|\mathcal{G}\right) = \mathbb{E}\left(f(X_1, \ldots, X_k)\right) \text{ a.s..} \tag{19.5.44}$$

Remark. Note that when f is continuous bounded Borel function, the statement is actually the inverse of Proposition 19.4.28.(v).

Proof. Let $Y = \mathbb{E}\left(f(X_1, \ldots, X_k)|\mathcal{G}\right)$ a.s.. Then by Definition of conditional expectation, for any $A \in \mathcal{G}$ (as $f(X_1, \ldots, X_k)$ is bounded and thus integrable),

$$\mathbb{E}\left(Y\mathbb{1}_A\right) = \mathbb{E}\left(f(X_1, \ldots, X_k)\mathbb{1}_A\right) \underbrace{= \mathbb{P}(A)\mathbb{E}\left(f(X_1, \ldots, X_k)\right)}_{\text{Proposition 19.5.6}} = \mathbb{E}\left(\mathbb{1}_A \mathbb{E}\left(f(X_1, \ldots, X_k)\right)\right). \tag{19.5.45}$$

This equality holds if and only if $Y = \mathbb{E}\left(f(X_1, \ldots, X_k)\right)$ a.s. by Theorem 19.4.18. □

[9] see Definition 19.8.4

Theorem 19.5.8. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be probability space and $\mathcal{G}$ be a σ-algebra. The the random variable vector $X = (X_1, \ldots, X_k)^T$ is independent of $\mathcal{G}$ if and only if

$$\mathbb{E}\left(e^{i\langle u, X\rangle}|\mathcal{G}\right) = \mathbb{E}\left(e^{i\langle u, X\rangle}\right) \text{ a.s.. } (*) \tag{19.5.46}$$

Proof. The only if part is implied by Proposition 19.4.28.(v).

Now we prove the if part. For any $A \in \mathcal{G}$, we have $u \in \mathbb{R}^k$ and $v = \left(u^T, u_{k+1}\right)^T$ where $u_{k+1} \in \mathbb{R}$, and $Y = \left(X^T, \mathbb{1}_A\right)$

$$\begin{aligned}
\phi_Y(v) &= \mathbb{E}\left(e^{i\langle v, Y\rangle}\right) = \mathbb{E}\left(e^{i\langle u, X\rangle} e^{iu_{k+1}\mathbb{1}_A}\right) = \mathbb{E}\left(e^{i\langle u, X\rangle} e^{iu_{k+1}}\mathbb{1}_A\right) \\
&= e^{iu_{k+1}}\mathbb{E}\left(e^{i\langle u, X\rangle}\mathbb{1}_A\right) = e^{iu_{k+1}}\mathbb{E}\left(e^{i\langle u, X\rangle}\right)\mathbb{E}\left(\mathbb{1}_A\right) \qquad \text{(by } (*)\text{)} \\
&= \mathbb{E}\left(e^{i\langle u, X\rangle}\right)\mathbb{E}\left(e^{iu_{k+1}}\mathbb{1}_A\right) = \mathbb{E}\left(e^{i\langle u, X\rangle}\right)\mathbb{E}\left(e^{iu_{k+1}\mathbb{1}_A}\right) = \phi_X(u)\phi_{\mathbb{1}_A}(u_{k+1}).
\end{aligned}$$

Thus, we can see that X is independent of $\mathbb{1}_A$ by Theorem 19.5.4. Then we can say that X is independent of $\mathcal{G}$. □

19.5.3 Moment generating function

Definition 19.5.4 (moment generating function)**.** The moment generating function M_X of a real-valued random variable X is defined by

$$M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right), \quad \theta \in \mathbb{R}. \tag{19.5.47}$$

Example 19.5.9. The set $I = \{\theta : M_X(\theta) < \infty\}$ is an interval (i.e., $\mathbb{R}$, $\{0\}$ and $(-\infty, 1)$).

Suppose $M_X(a)$ and $M_X(b)$ are both finite with $a < b$. Then for all $c \in (a, b)$,

$$M_X(c) \le \mathbb{E}\left(\max\left\{e^{aX}, e^{bX}\right\}\right) < M_X(a) + M_X(b) < \infty. \tag{19.5.48}$$

(i) For $I = \mathbb{R}$, we can take X with $X(\omega) = 1$ for all ω as $M_X(\theta) = e^\theta < \infty$, $\forall \theta \in \mathbb{R}$.

(ii) For $I = \{0\}$, we can take X with a Cauchy distribution (i.e. density $1/(\pi(1+x^2)$, see Definition 19.8.8) since for $\theta \neq 0$,

$$\begin{aligned}
M_X(\theta) &= \int_{-\infty}^{\infty} \frac{e^{\theta x}}{\pi(1+x^2)} dx = \int_0^{\infty} \frac{e^{\theta x} + e^{-\theta x}}{\pi(1+x^2)} dx \ge \int_0^{\infty} \frac{e^{|\theta| x}}{\pi(1+x^2)} dx \ge \int_0^{\infty} \frac{e^{|\theta| x}}{\pi(1+x)^2} dx \\
&\ge e^{-|\theta|} \int_1^{\infty} \frac{e^{|\theta| x}}{\pi x^2} dx = \frac{e^{-|\theta|}}{\pi} \int_1^{\infty} \left(\frac{1}{x^2} + \frac{1}{x} + \frac{1}{2} + \frac{x}{3!} + \frac{x^2}{4!} + \ldots\right) dx = \infty
\end{aligned}$$

and $M_X(0) = 1 < \infty$.

(iii) For $I = (-\infty, 1)$, we can take $X \sim \mathcal{E}(1)$ (i.e. density e^{-x} on $[0, \infty)$) since $\theta \neq 1$ ($M_X(1) = \infty$ when $\theta = 1$),

$$M_X(\theta) = \int_0^{\infty} e^{\theta x} e^{-x} dx = \int_0^{\infty} e^{(\theta-1)x} dx = \frac{1}{\theta - 1} e^{(\theta-1)x}\Big|_0^{\infty} < \infty \text{ only if } \theta < 1.$$

Proposition 19.5.10. Let $\theta \in I = \{\theta : M_X(\theta) < \infty\}$ and I contains a neighbourhood of 0 then X has finite moments of all orders given by

$$\mathbb{E}(X^n) = \left(\frac{d^n M_X(\theta)}{d\theta^n}\right)\Big|_{\theta=0}. \tag{19.5.49}$$

Proof. For all θ, we have that

$$\sum_{n=0}^{N} \frac{(\theta X)^n}{n!} \to e^{\theta X} \text{ pointwise as } N \to \infty. \tag{19.5.50}$$

Now take $\varepsilon \in I$ with $\varepsilon > 0$ and $M_X(-\varepsilon) < \infty$. Then for all $\theta \in (-\varepsilon, \varepsilon)$, we have that

$$\left|\sum_{n=0}^{N} \frac{(\theta X)^n}{n!}\right| \le \sum_{n=0}^{N} \frac{|\theta X|^n}{n!} \le e^{|\varepsilon X|} \le e^{\varepsilon X} + e^{-\varepsilon X} \tag{19.5.51}$$

for all N. Thus,

$$\mathbb{E}\left|\sum_{n=0}^{N} \frac{(\theta X)^n}{n!}\right| \le \mathbb{E}\left(e^{\varepsilon X} + e^{-\varepsilon X}\right) < \infty \Rightarrow \sum_{n=0}^{N} \frac{(\theta X)^n}{n!} \text{ is integrable.} \tag{19.5.52}$$

Hence by dominated convergence theorem (Theorem 19.3.8), $e^{\theta X}$ is integrable and

$$M_X(\theta) = \mathbb{E}(e^{\theta X}) = \mathbb{E}\left(\lim_{N\to\infty}\sum_{n=0}^{N}\frac{(\theta X)^n}{n!}\right) = \lim_{N\to\infty}\mathbb{E}\left(\sum_{n=0}^{N}\frac{(\theta X)^n}{n!}\right) = \sum_{n=0}^{\infty}\frac{\theta^n\mathbb{E}(X^n)}{n!}. \quad (*) \tag{19.5.53}$$

by Fubini theorem (Theorem 15.3.33). Also, for each n

$$\frac{\theta^n\mathbb{E}(|X|^n)}{n!} < \infty \;\Rightarrow\; \mathbb{E}\left(|X|^n\right) < \infty. \tag{19.5.54}$$

Using standard results for power series,

$$\sum_{n=0}^{\infty}\frac{\theta^n\mathbb{E}(X^n)}{n!} \quad (\dagger) \tag{19.5.55}$$

is infinitely differentiable for all θ within its radius of convergence, so in particular for all $\theta \in (-\varepsilon, \varepsilon)$. The nth derivative at 0 is given by $\mathbb{E}(X^n)$. By the relationship in $(*)$, this also equals $\left(\frac{d^n M_X(\theta)}{d\theta^n}\right)\Big|_{\theta=0}$. □

Definition 19.5.5 (skewness)**.** The skewness of a random variable X with mean μ and variance σ^2 is defined as

$$\text{Skew}(X) = \mathbb{E}\left(\left(\frac{X-\mu}{\sigma}\right)^3\right) = \frac{\mathbb{E}(X-\mu)^3}{\left(\mathbb{E}(X-\mu)^2\right)^{3/2}}. \tag{19.5.56}$$

Remark. If skewness is positive, the distribution tends to lean to left.

Definition 19.5.6 (kurtosis)**.** The kurtosis of a random variable X with mean μ and variance σ^2 is defined as

$$\text{Kurt}(X) = \frac{\mathbb{E}(X-\mu)^4}{\left(\mathbb{E}(X-\mu)^2\right)^2} - 3 = \frac{\mathbb{E}(X-\mu)^4}{\sigma^4} - 3. \tag{19.5.57}$$

Remark. If kurtosis is positive, it means that the distribution has 'fat tail'.

Theorem 19.5.11. Let X and Y be two random variables. If their moment generatring functions exist, say $M_X(\theta)$ and $M_Y(\theta)$ with $M_X(\theta) = M_Y(\theta) < \infty$. Then we have that X and Y have the same distribution. In other words, M_X determines the law μ_X uniquely.

Proof. Apply the same argument in proof of Theorem 19.5.3. □

Corollary 19.5.12. Let A be an event and X be a random variable satisfies that

$$\mathbb{E}\left(e^{\theta X}\mathbb{1}_A\right) = \mathbb{E}\left(e^{\theta X}\right)\mathbb{P}(A). \tag{19.5.58}$$

where $e^{\theta X}$ is bounded. Then X is independent of A.

Proof. Let X' be a random variable independent of A with

$$\mathbb{P}\left(X \le x, \mathbb{1}_A \le a\right) = \mathbb{P}\left(X' \le x, \mathbb{1}_A \le a\right). \tag{19.5.59}$$

In other words, they have the same joint law. Therefore,

$$\mathbb{E}\left(e^{\theta X}\mathbb{1}_A\right) = \mathbb{E}\left(e^{\theta X'}\mathbb{1}_A\right) = \mathbb{E}\left(e^{\theta X'}\right)\mathbb{P}(A) \tag{19.5.60}$$

by Theorem 19.5.4.(iii) since X' is independent of A. Also, we know that by assumption

$$\mathbb{E}\left(e^{\theta X}\right)\mathbb{P}(A) = \mathbb{E}\left(e^{\theta X}\mathbb{1}_A\right) \;\Rightarrow\; \mathbb{E}\left(e^{\theta X}\right)\mathbb{P}(A) = \mathbb{E}\left(e^{\theta X'}\right)\mathbb{P}(A). \tag{19.5.61}$$

Hence, we have that $M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right) = \mathbb{E}\left(e^{\theta X'}\right) = M_{X'}(\theta) < \infty$ as $e^{\theta X}$ is bounded. Then by Theorem 19.5.11, we have that $X \sim X'$. Therefore,

$$\mathbb{P}\left(X \le x, \mathbb{1}_A \le a\right) = \mathbb{P}\left(X' \le x, \mathbb{1}_A \le a\right) = \mathbb{P}\left(X' \le x\right)\mathbb{P}\left(\mathbb{1}_A \le a\right) = \mathbb{P}\left(X \le x\right)\mathbb{P}\left(\mathbb{1}_A \le a\right) \tag{19.5.62}$$

by Proposition 19.2.9 and the fact that $X \sim X'$. Hence, we have that X is independent of A by Proposition 19.2.9. □

Proposition 19.5.13. Let $X_1, X_2, \ldots, X_n$ be random variables with $e^{\theta_1 X_1}, \ldots, e^{\theta_n X_n}$ bounded. Then $X_1, \ldots, X_n$ are independent if and only if for moment generating functions $M_{X_1}, \ldots, M_{X_n}$,

$$\mathbb{E}\left(e^{\theta_1 X_1 + \cdots + \theta_n X_n}\right) = \mathbb{E}\left(e^{\theta_1 X_1}\right) \ldots \mathbb{E}\left(e^{\theta_n X_n}\right). \tag{19.5.63}$$

Proof. Direct result from Theorem 19.5.4 □

19.6 Convergence in Distribution and Weak Convergence

19.6.1 Convergence in distribution for random variables

Definition 19.6.1. Let F be a distribution function on $\mathbb{R}$ and let $(F_n : n \in \mathbb{N})$ be a sequence of such distribution functions. We say that $F_n \to F$ as distribution functions if $F_n(x) \to F(x)$ at every point $x \in \mathbb{R}$ where F is continuous.

Definition 19.6.2. Let X be a random variable and let $(X_n : n \in \mathbb{N})$ be a sequence of random variables. We say that $X_n \to X$ in distribution (denoted by $X_n \xrightarrow{d} X$) if $F_{X_n} \to F_X$.

Lemma 19.6.1. If $X_n \to X$ in probability then $X_n \to X$ in distribution.

Proof. Suppose $X_n \xrightarrow{p} X$ and write

$$F_n(x) = \mathbb{P}(X_n \le x), \qquad F(x) = \mathbb{P}(X \le x), \tag{19.6.1}$$

for the distribution functions of X_n and X respectively. $\forall \varepsilon > 0$,

$$F_n(x) = \mathbb{P}(X_n \le x) = \mathbb{P}(X_n \le x, X \le x + \varepsilon) + \mathbb{P}(X_n \le x, X > x + \varepsilon) \le F(x + \varepsilon) + \mathbb{P}\left(|X_n - X| > \varepsilon\right). \tag{19.6.2}$$

Similarly,

$$F(x - \varepsilon) = \mathbb{P}(X \le x - \varepsilon) = \mathbb{P}(X \le x - \varepsilon, X_n \le x) + \mathbb{P}(X \le x - \varepsilon, X_n > x) \le F_n(x) + \mathbb{P}\left(|X_n - X| > \varepsilon\right). \tag{19.6.3}$$

Thus,

$$F(x - \varepsilon) - \mathbb{P}\left(|X_n - X| > \varepsilon\right) \le F_n(x) \le F(x + \varepsilon) + \mathbb{P}\left(|X_n - X| > \varepsilon\right) \tag{19.6.4}$$

Let $n \to \infty$ to obtain (as $\mathbb{P}\left(|X_n - X| > \varepsilon\right) \to 0$)

$$F(x - \varepsilon) \le \liminf_{n \to \infty} F_n(x) \le \limsup_{n \to \infty} F_n(x) \le F(x + \varepsilon), \tag{19.6.5}$$

If F is continuous at x then

$$F(x - \varepsilon) \uparrow F(x), \qquad F(x + \varepsilon) \downarrow F(x) \quad \text{as } \varepsilon \downarrow 0. \tag{19.6.6}$$

Thus, $\lim F_n(x) = F(x)$ for all continuous points, known as $X_n \to X$ in distribution. □

Remark. The inverse of above lemma is not true.

Example 19.6.2. Let X be a Bernoulli variable taking values 0 and 1 with equal probability $\frac{1}{2}$. Let $X_1, X_2, \ldots$ be indentical random variables given by $X_n = X$ for all n. The X_n are certainly not independent, but $X_n \xrightarrow{d} X$. Let $Y = 1 - X$. Clearly $X_n \xrightarrow{d} Y$, since X and Y have the same distribution. However, X_n cannot converge to Y in any other mode because $|X_n - Y| = 1$ always.

However, we have the following proposition:

Proposition 19.6.3. Let X_n, X be r.v.'s. If $X_n \to X$ in probability, i.e.

$$\lim_{n \to \infty} \mathbb{P}(d(X_n, X) > \varepsilon) \to 0 \text{ for all } \varepsilon > 0 \tag{19.6.7}$$

then $X_n \to X$ in distribution. If $X_n \to c$ in distribution for some constant c then $X_n \to c$ in probability.

Proof. [10] □

Theorem 19.6.4 (Skorokhod Representation Theorem)**.** Suppose that $(F_n : n \in \mathbb{N})$ is a sequence of distribution function on $\mathbb{R}$, and F is a distribution function on $\mathbb{R}$ that $F_n(x) \to F(x)$ at every point x of continuity of F.

Then there exists a probability triple $(\Omega, \mathcal{F}, \mathbb{P})$ carring a sequence (X_n) of random variables and also a random variable X such that

$$F_n = F_{X_n}, \quad F = F_X, \qquad \text{and} \quad X_n \to X \text{ a.s.} \tag{19.6.8}$$

Remark. This is a kind of 'converse' to Lemma 19.6.7.

Proof. Take $(\Omega, \mathcal{F}, \mathbb{P}) = ([0,1], \mathcal{B}([0,1]), \text{Leb})$, define

$$X^+(\omega) := \inf\{x : F(x) > \omega\}, \quad X^-(\omega) := \inf\{x : F(x) \geq \omega\}, \tag{19.6.9}$$

similarly,

$$X_n^+(\omega) := \inf\{x : F_n(x) > \omega\}, \quad X_n^-(\omega) := \inf\{x : F_n(x) \geq \omega\}. \tag{19.6.10}$$

Thus, from Proposition 19.2.5, we have $\mathbb{P}(X^+ = X^-) = 1$.

Now fix ω. Let x be a non-atom of F with $x > X^+(\omega)$. Then $F(z) > \omega$ and hence, for large n, $F_n(x) > \omega$ (since $F_n \to F$ as distributio function), so that $X_n^+(\omega) \leq x$. So $\limsup_n X_n^+(\omega) \leq x$. Also we can choose $x \downarrow X^+(\omega)$ (remark of Definition 19.2.3). Hence

$$\limsup_n X_n^+(\omega) \leq X^+(\omega), \tag{19.6.11}$$

and by similar arguments,

$$\limsup_n X_n^-(\omega) \geq X^-(\omega). \tag{19.6.12}$$

Since $X_n^- \leq X_n^+$ and $\mathbb{P}(X^+ = X^-) = 1$, we have

$$\limsup_n X_n^+ = \liminf_n X_n^+ = \lim_n X_n^+ = X^+ \text{ a.s.}, \qquad \limsup_n X_n^- = \liminf_n X_n^- = \lim_n X_n^- = X^- \text{ a.s.}, \tag{19.6.13}$$

Thus, $\mathbb{P}(X_n^+ = X_n^-) = 1$. Define

$$X_n = \begin{cases} X_n^- & X_n^+ = X_n^- \\ 0 & \text{otherwise} \end{cases}, \qquad X = \begin{cases} X^+ & X^+ = X^- \\ 0 & \text{otherwise} \end{cases} \tag{19.6.14}$$

we have $F_n(x) = \mathbb{P}(X_n \leq x)$ and $F(x) = \mathbb{P}(X \leq x)$ (since $X_n^- = X_n$ a.s. and $X^- = X$ a.s.) and $\mathbb{P}(\lim_n X_n \to X) = 1$ since $X^- = X$ a.s., $X_n^- = X_n$ a.s. and $X_n^- \to X^-$ a.s. □

19.6.2 Weak convergence

Definition 19.6.3 (weak convergence)**.** Let μ be a Borel probability measure on $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ and let $(\mu_n : n \in \mathbb{N})$ be a sequence of such measures. We say that $\mu_n \to \mu$ weakly or $\mu_n \xrightarrow{w} \mu$ if $\mu_n(f) \to \mu(f)$ for all continuous bounded functions f on $\mathbb{R}$.

Lemma 19.6.5. Suppose X, $(X_n : n \in \mathbb{N})$ are random variables such that $X_n \to X$ in probability. Then μ and $(\mu_n : n \in \mathbb{N})$ are the law (Borel probability measures on $\mathbb{R}$) corresponding to distribution function F_X and F_{X_n}, i.e.

$$\mu((-\infty, x]) = F_X(x), \qquad \mu_n((-\infty, x]) = F_{X_n}(x). \tag{19.6.15}$$

Then we have $\mu_n \xrightarrow{w} \mu$.

Proof. Suppose that $X_n \to X$ in probability, for any bounded continuous function f on $\mathbb{R}$, $\forall \varepsilon > 0$, there exists $\delta > 0$, s.t. $|X_n - X| < \delta$, $|f(X_n) - f(X)| < \varepsilon$ (by definition of continuity (Definition 10.3.2)). Let

$$A := \{|f(X_n) - f(X)| < \varepsilon\}, \quad B := \{|X_n - X| < \delta\} \quad \Rightarrow \quad B \subseteq A \Rightarrow A^c \subseteq B^c. \tag{19.6.16}$$

Thus, $\mathbb{P}(\{|f(X_n) - f(X)| \geq \varepsilon\}) = \mathbb{P}(A^c) \leq \mathbb{P}(B^c) = \mathbb{P}(\{|X_n - X| \geq \delta\}) \to 0$. So $f(X_n) \to f(X)$ in probability. Then by bounded convergence theorem (Theorem 19.3.10) and Theorem 19.3.14, we have

[10] need proof

$$\mu_n(f) = \mathbb{E}(f(X_n)) \to \mathbb{E}(f(X)) = \mu(f) \quad \Rightarrow \quad \mu_n \xrightarrow{w} \mu. \qquad \square$$

We check the fact that F_n does not converge to F at discontinuous points of F.

Example 19.6.6. Suppose that $X_n = \frac{1}{n}$, $X = 0$ (F is not continuous at 0). Let μ_n be the law of X_n, so that μ_n is the unite mass at $\frac{1}{n}$, and let μ be the law of X. Then, for any bounded continuous function on $\mathbb{R}$, $f \in C_b(\mathbb{R})$,

$$\mu_n(f) = \underbrace{f\left(\frac{1}{n}\right) \to f(0)}_{\text{by continuity}} = \mu(f) \quad \Rightarrow \quad \mu_n \xrightarrow{w} \mu. \tag{19.6.17}$$

However, $F_n(0) = 0 \nrightarrow 1 = F(0)$.

Lemma 19.6.7. If $\mu_n \xrightarrow{w} \mu$, then for the corresponding distribution functions $F_n(x) = \mu_n((-\infty, x])$ and $F = \mu((-\infty, x])$,

$$\lim_n F_n(x) = F(x) \tag{19.6.18}$$

for every non-atom (that is, every point of continuity) x of F.

Proof. Suppose that $\mu_n \xrightarrow{w} \mu$, let $x \in \mathbb{R}$, and let $\delta > 0$. Construct bounded continuous function f

$$f(y) := \begin{cases} 1 & y \le x \\ 1 - \delta^{-1}(y - x) & x < y < x + \delta \\ 0 & y \ge x + \delta \end{cases} \tag{19.6.19}$$

Then $\mu_n(f) \to \mu(f)$. Now,

$$F_n(x) = \mu_n((-\infty, x]) \le \mu_n(h), \quad \mu(h) \le \mu((-\infty, x + \delta]) = F(x + \delta) \quad \Rightarrow \quad \limsup_n F_n(x) \le F(x + \delta). \tag{19.6.20}$$

However, F is right-continuous, so we may let $\delta \downarrow 0$ to obtain

$$\limsup_n F_n(x) \le F(x), \quad \forall x \in \mathbb{R}. \quad (*) \tag{19.6.21}$$

In similar fashion, working with $y \to h(y + \delta)$, we find that for $x \in \mathbb{R}$ and

$$\liminf F_n(x) \le F(x - \delta) \quad \Rightarrow \quad \liminf F_n(x) \le F(x-), \quad \forall x \in \mathbb{R}. \quad (\dagger) \tag{19.6.22}$$

If F is continuous at x, then we have $F(x^-) = F(x)$, which gives us that

$$\limsup_n F_n(x) \le \liminf_n F_n(x) \quad \Rightarrow \lim_n F_n(x) = F(x), \tag{19.6.23}$$

as required. $\square$

Now we can merge Lemma 19.6.5 and 19.6.7,

Theorem 19.6.8. Let μ_n, μ be probability measures on $\mathbb{R}$. F_n and F are corresponding distribution functions $F_n(x) = \mu_n((-\infty, x])$ and $F = \mu((-\infty, x])$,. The following are equivalent.

(i) $\mu_n \to \mu$ weakly.

(ii) $F_n(x) \to F(x)$ for every $x \in \mathbb{R}$ that is a continuity point of F.

Remark. Of course, this theorem can be proved by previous argument, but we give the proof implied by the results in measure theory.

Proof. (i) $\Rightarrow$ (ii): This is (i) $\Rightarrow$ (iv) in Theorem 15.5.2 ($E = \mathbb{R}$). Indeed, $\partial(-\infty, x] = \{x\}$, so if F continuous at x then $\mu(\{x\}) = 0$.

(ii) $\Rightarrow$ (i): Let G be open in $\mathbb{R}$. We may write $G = \bigcup_{k\geq 0}(a_k, b_k)$ for pairwise disjoint intervals (a_k, b_k). Then $\mu_n(G) = \sum_{k\geq 0}\mu_n(a_k, b_k)$ by countable additivity. Now,

$$\mu_n(a_k, b_k) = F_n(b_k^-) - F_n(a_k) \geq F_n(b) - F_n(a) \tag{19.6.24}$$

for every $a_k < a < b < b_k$. Choosing a and b to be continuity points of F (such points are dense in $\mathbb{R}$ (given $x \in \mathbb{R}$, there exists a sequence (y_n) of reals with $y_n \downarrow x$ such that every y_n is a non-atom of μ) by Proposition 19.2.2), we obtain

$$\liminf \mu_n(a_k, b_k) \geq \liminf (F_n(b) - F_n(a)) = F(b) - F(a). \qquad \text{(by (ii))} \tag{19.6.25}$$

Letting $a \downarrow a_k$ and $b \uparrow b_k$ along continuity points of F (since the set of continuity points of F is dense), we obtain

$$\liminf \mu_n(a_k, b_k) \geq \underbrace{F(b_k^-)}_{F \text{ is increasing}} - \underbrace{F(a_k)}_{F \text{ is right-continuous}} = \mu(a_k, b_k). \qquad (*) \tag{19.6.26}$$

Finally, applying the idea in proof of Fatou's lemma (Lemma 15.3.11),

$$\begin{aligned} \inf_{m\geq n}\mu_m(a_k, b_k) \leq \mu_m(a_k, b_k) \quad &\Rightarrow \quad \sum_{k\geq 0}\inf_{m\geq n}\mu_m(a_k, b_k) \leq \sum_{k\geq 0}\mu_m(a_k, b_k) \\ &\Rightarrow \quad \sum_{k\geq 0}\inf_{m\geq n}\mu_m(a_k, b_k) \leq \inf_{m\geq n}\sum_{k\geq 0}\mu_m(a_k, b_k). \qquad (**) \end{aligned}$$

Clearly,

$$\sum_{k\geq 0}\sup_n\left(\inf_{m\geq n}\mu_m(a_k, b_k)\right) \leq \sup_n\sum_{k\geq 0}\left(\inf_{m\geq n}\mu_m(a_k, b_k)\right). \qquad (\dagger) \tag{19.6.27}$$

Thus,

$$\begin{aligned} \liminf_n \mu_n(G) \quad &= \quad \liminf_n \sum_{k\geq 0}\mu_n(a_k, b_k) = \sup_n \inf_{m\geq n}\sum_{k\geq 0}\mu_m(a_k, b_k) \overset{(**)}{\geq} \sup_n \sum_{k\geq 0}\inf_{m\geq n}\mu_m(a_k, b_k) \\ &\overset{(\dagger)}{\geq} \quad \sum_{k\geq 0}\sup_n\inf_{m\geq n}\mu_m(a_k, b_k) = \sum_{k\geq 0}\liminf_n \mu_n(a_k, b_k) \overset{(*)}{\geq} \sum_{k\geq 0}\mu(a_k, b_k) = \mu(G). \end{aligned}$$

This is actually (ii) in Theorem 15.5.2, which is equivalent to (i). □

Then by Definition 19.6.2, Theorem 19.6.8 and Theorem 19.3.14,

Corollary 19.6.9. $X_n \overset{d}{\to} X$ if and only if $\mathbb{E}(f(X_n)) \to \mathbb{E}(f(X))$ for all bounded continous functions, $f \in C_b(E)$.

Example 19.6.10. (i) If $X_n = x_n$ is constant and $x_n \to x$ then $X_n \overset{d}{\to} X$ since $\delta_{x_n} \overset{w}{\to} \delta_x$.

(ii) Let U be a uniform r.v. (see Definition 19.8.4) in $[0, 1]$, and write $X_n = n^{-1}\lfloor U \rfloor$. Then $X_n \to U$ a.s., so $X_n \overset{d}{\to} U$. Indeed, $\mu_{X_n} = \frac{1}{n}\sum_{k=0}^{n-1}\delta_{\frac{k}{n}} \overset{w}{\to} dx = \mu_X(U)$.

(iii) Central Limit Theorem (see Theorem 19.9.10). Let $X_1, X_2, \ldots$ be i.i.d. r.v.'s in $\mathcal{L}^2(\mathbb{R})$. If $\mu := \mathbb{E}[X]$ and $\sigma^2 := \mathrm{Var}(X) = \mathbb{E}[X^2]$ then for all $a < b$,

$$\mathbb{P}\left(a < \frac{X_1 + \cdots + X_n - n\mu}{\sigma\sqrt{n}} < b\right) \to \int_a^b \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}dx \tag{19.6.28}$$

which is saying that $\frac{X_1+\cdots+X_n-n\mu}{\sigma\sqrt{n}} \overset{d}{\to} \mathcal{N}(0, 1)$ in distribution, where $\mathcal{N}(0, 1)$ is a Gaussian random variable with mean 0 and variance 1.

19.6.3 Tightness and Lévy's convergence theorem

Recall Definition 15.5.3,

Definition 19.6.4. Let $(\mu_i)_{i\in I}$ be a family of probability measures on (E, d). We say that $(\mu_i)_{i\in I}$ is tight if for all $\varepsilon > 0$ there is $K \subseteq E$ compact such that $\sup_{i\in I}\mu_i(E\backslash K) < \varepsilon$.

Theorem 19.6.11 (Prokhorov's Theorem)**.** Let $(\mu_n, n \geq 0)$ be probability measures on (E, d). If $(\mu_n, n \geq 0)$ is tight. Then there is a subsequence $(\mu_{n_k}, k \geq 0)$ and a probability measure μ such that $\mu_{n_k} \xrightarrow{w} \mu$ as $k \to \infty$.

To motivate this theorem, notice that for (δ_{x_n}), tightness is exactly the requirement that the x_n are contained in a compact set, so Prokhorov's Theorem may (loosely) be seen as a generalization of the Bolzano-Weierstrass Theorem.

Proof. We prove the case $E = \mathbb{R}$. Consider $(F_n(q), n \geq 0) \subseteq [0,1]$ for q a rational number. There exists a subsequence n_k^q such that $F_{n_k^q}(q) \to F(q)$ (i.e. the subsequence has a limit in $[0,1]$ since it is bounded by Bolzano-Weierstrass theorem (Theorem 10.2.36)). Since $\mathbb{Q}$ is countable, by a diagonal procedure[11], we can find $(n_k, k \geq 0)$ such that $F_{n_k}(q) \to F(q)$ for all $q \in \mathbb{Q}$. Then F is non-decreasing on $\mathbb{Q}$, so extend it to $\mathbb{R}$ via $F(t) = \lim_{q \downarrow t, q \in \mathbb{Q}} F(q)$ and F is non-decreasing on $\mathbb{R}$. Thus, F is càdlàg(it is right-continuous by definition of $F(t)$ and its left limit exists since F is bounded and non-decreasing.)

Check that for every continuity point t of F, $F_{n_k}(t) \to F(t)$ as $k \to \infty$. $\forall \varepsilon > 0$, and pick $\eta > 0$ such that $F(t+\eta) \leq F(t) + \varepsilon$ and $t + \eta \in \mathbb{Q}$ (since F is countinous at point t). Then $F_{n_k}(t+\eta) \to F(t+\eta) \leq F(t) + \varepsilon$. Thus, since $\limsup F_{n_k}(q) = \lim F_{n_k}(q)$ for all $q \in \mathbb{Q}$,

$$\limsup_k F_{n_k}(t) \leq \limsup_k F_{n_k}(t+\eta) = F(t+\eta) \leq F(t) + \varepsilon \quad \Rightarrow \quad \limsup F_{n_k}(t) \leq F(t),$$

by infimum defnition (Definition 2.7.1). Similarly we get that $F(t) \leq \liminf F_{n_k}(t)$. Thus, $\lim_{k \to \infty} F_{n_k}(t) \to F(t)$, $(*)$ by Definition 3.5.2.

We want to show that F is the corresponding distribution function of some probability measure μ. It is sufficient to check that $F(t) \to 0, 1$ as $t \to -\infty, +\infty$ (since we alrealy know that F is non-decreasing and càdlàg).

By tightness given ε, we can find compact set $K = [A, B]$ such that $\mu_n((B, \infty)) < \varepsilon - \mu_n((-\infty, A))$ for all $n \geq 0$. But $\varepsilon > \mu_{n_k}((B, \infty)) = 1 - F_{n_k}(B)$ and $\varepsilon > \mu_{n_k}((-\infty, A)) = F_{n_k}(A^-)$. Then we can pick continuous points A' and B' of F such that $A' < A < B < B'$. Thus, by $(*)$,

$$\varepsilon > 1 - F_{n_k}(B) > 1 - F_{n_k}(B') \to 1 - F(B'), \qquad \varepsilon > F_{n_k}(A^-) \geq F_{n_k}(A') \to F(A'). \tag{19.6.29}$$

as required. Therefore, $F_{n_k} \to F$ at every continuity point of F. Then by Theorem 19.6.8, $\mu_{n_k} \to \mu$ weakly. □

Lemma 19.6.12. Let X be a random variable with values in $\mathbb{R}^n$. Then for any norm $\|\cdot\|$ on $\mathbb{R}^n$, there exists a constant $C > 0$ (depending on n and on the choice of the norm but not depending on X) such that

$$\mathbb{P}(\|X\| \geq K) \leq CK^n \int_{[0, \frac{1}{K}]^n} (1 - \Re\phi_X(u)) du. \tag{19.6.30}$$

Proof. Indeed, $\Re\phi_X(u) = \Re\mathbb{E}\left(e^{i\langle u, X\rangle}\right) = \mathbb{E}(\cos(uX))$. By Fubini's Theorem,

$$K^n \int_{[0, \frac{1}{K}]^n} (1 - \Re\phi_X(u)) du \quad = \quad \mathbb{E}\left(1 - K^n \int_{[0, \frac{1}{K}]^n} \prod_{i=1}^n \cos(u_i X_i) du\right) = \mathbb{E}\left(1 - \prod_{i=1}^n \frac{\sin(\frac{X_i}{K})}{\frac{X_i}{K}}\right). \qquad (*)$$

Define the norm $\|u\| = \sup_{1 \leq i \leq n} |u_i|$, $u \in \mathbb{R}^n$. Then the continuous function $\operatorname{sinc} : t \in \mathbb{R} \to \frac{1}{t}\sin t$ is such that there exists $0 < c < 1$ such that $|\operatorname{sinc} t| \leq c$ for every $t \geq 1$, so that function $f : u \in \mathbb{R}^d \mapsto \prod_{i=1}^n \sin u_i / u_i$ satisfies that $|f(u)| \leq c$ if any $u_i \geq 1$, i.e., we need $\|u\| \geq 1$ to have that $1 - |f(u)| \geq 1 - c$. Then take $C = (1-c)^{-1}$, we have $\mathbb{1}_{\|u\| \geq 1} \leq C(1 - f(u))$. Then let $u = \frac{X}{K}$, since $\mathbb{1}_{\|u\| \geq 1}$ and $C(1 - f(u))$ are non-negative, by Theorem 15.3.7, we have

$$\mathbb{P}(\|X\| \geq K) = \mathbb{E}\left(\mathbb{1}_{\|\frac{X}{K}\| \geq 1}\right) \leq C\mathbb{E}\left(1 - \frac{\sin(\frac{X}{K})}{\frac{X}{K}}\right) \overset{(*)}{=} CK^n \int_{[0, \frac{1}{K}]^n} (1 - \Re\phi_X(u)) du. \tag{19.6.31}$$

Then this result holds for any norm on $\mathbb{R}^n$ by the equivalence of norms in finite-dimensional vector spaces. Note that C does not depend on the law of X. □

Theorem 19.6.13 (Lévy's convergence theorem)**.** (i) Let $(X_n, n \in \mathbb{N})$, X be r.v.'s such that $X_n \xrightarrow{d} X$. Then $\phi_{X_n}(u) \to \phi_X(u)$ for all $u \in \mathbb{R}^d$.

[11] need to check

(ii) Let $(X_n, n \in \mathbb{N})$ be r.v.'s such that $\phi_{X_n}(u) \to \phi(u)$ for all $u \in \mathbb{R}^d$ for some function $\phi : \mathbb{R}^d \to \mathbb{C}$ that is continuous at 0. There is a r.v. X such that $\phi = \phi_X$ and $X_n \xrightarrow{d} X$.

Proof. (i) Recall Corollary 19.6.9, $X_n \xrightarrow{d} X$ if and only if $\mathbb{E}[f(X_n)] \to \mathbb{E}[f(X)]$ for all $f \in C_b(\mathbb{R}^d)$. Since, $e^{i\langle u, X_n\rangle} \in C_b(\mathbb{R}^d)$,

$$\phi_{X_n}(u) = \mathbb{E}\left(e^{i\langle u, X_n\rangle}\right) \to \mathbb{E}\left(e^{i\langle u, X\rangle}\right) = \phi_X(u) \quad \forall u \in \mathbb{R}^d. \tag{19.6.32}$$

(ii) From Lemma 19.6.12, we know that for any norm on $\mathbb{R}^d$, there exists a universal constant $C > 0$ such that for all r.v. X_n taking values in $\mathbb{R}^d$,

$$\mathbb{P}(\|X_n\| \geq K) \leq CK^d \int_{\left[0, \frac{1}{K}\right]^d} (1 - \Re\phi_{X_n}(u))du. \tag{19.6.33}$$

Thus, since $\phi_{X_n}(u) \to \phi(u)$, $\Re\phi_{X_n}(u) \to \Re\phi(u)$ and $1 - \Re\phi_{X_n}(u)$ is bounded. By dominated convergence theorem (Theorem 19.3.8),

$$\mathbb{P}(\|X_n\| \geq K) \leq CK^d \int_{\left[0, \frac{1}{K}\right]^d} (1 - \Re\phi_{X_n}(u))du \to CK^d \int_{\left[0, \frac{1}{K}\right]^d} (1 - \Re\phi(u))du \tag{19.6.34}$$

Since ϕ is continuous at zero and $\phi(0) = 1$, for any $\varepsilon > 0$ there is K large enough such that $|1 - \Re\phi(u)| \leq \frac{\varepsilon}{2C}$ for any $u \in [0, \frac{1}{K}]^d$. Thus, for such K,

$$\limsup_n \mathbb{P}(\|X_n\| \geq K) \leq \frac{\varepsilon}{2}. \tag{19.6.35}$$

Thus there is N_ε such that for all $n > N_\varepsilon$, $\mathbb{P}(\|X_n\| \geq K) \leq \varepsilon$. Up to taking K even larger, we may assume that

$$\sup_{1 \leq n \leq N_\varepsilon} \mathbb{P}(\|X_n\| \geq K) \leq \varepsilon. \tag{19.6.36}$$

Now for such K, $\sup_n \mathbb{P}(\|X_n\| \geq K) \leq \varepsilon$ (for all n), but we know that $\left\{\sup_{1 \leq i \leq d} X_n^i \geq K\right\} = \left\{X_n \in (-K, K)^d\right\}^c$

$$\sup_n \mathbb{P}(\|X_n\| \geq K) \leq \varepsilon \quad \Leftrightarrow \quad \sup_n \mu_n\left(\left\{(-K, K)^d\right\}^c\right) \leq \varepsilon \quad \Rightarrow \quad \sup_n \mu_n\left(\left\{[-K, K]^d\right\}^c\right) \leq \varepsilon \tag{19.6.37}$$

where μ_n is the law of X_n. Since $[-K, K]^d$ is a compact set, then $(\mu_n, n \geq 1)$ is a tight family of measures.

By Prokhorov's theorem (Theorem 19.6.11), there is a subsequence such that $\mu_{n_k} \xrightarrow{w} \mu$, for some probability measure μ on $\mathbb{R}$. Hence $X_{n_k} \xrightarrow{d} X$ for some r.v. X (by Theorem 19.6.8).

But by part (i), $\phi_{X_{n_k}} \to \phi_X$ pointwise, so $\phi = \phi_X$ is the characteristic function of a r.v. Let us assume that X_n does not converge in distribution to X. Then we could find $f \in C_b(\mathbb{R})$ such that $\mathbb{E}[f(X_n)]$ does not converge to $\mathbb{E}[f(X)]$ (by Corollary 19.6.9). Thus we could find an extraction n_k and $\varepsilon > 0$ such that $|\mathbb{E}\left(f(X_{n_k})\right) - \mathbb{E}\left(f(X)\right)| \geq \varepsilon$.

But $(\mu_{n_k}, k \geq 1)$ is tight (since it is contained in a tight family), so we can further extract a subsequence such that $X_{n_{k_r}} \to X'$ in distribution for some r.v. X'. Similarly, $\phi_X = \phi_{X'}$, so X and X' have the same distribution (by Theorem 19.5.3), i.e., $\mu_X = \mu_{X'}$, Then $\mathbb{E}\left(f(X_{n_{k_r}})\right) \to \mathbb{E}\left(f(X')\right) = \mu_{X'}(f) = \mu_X(f) = \mathbb{E}[f(X)]$ by Theorem 19.3.14 since $f \in C_b(\mathbb{R})$. Contradiction.

□

Now combine Theorem 19.6.8, 19.6.4 and 19.6.13, we have:

Theorem 19.6.14 (Equivalent modes of convergence)**.** Suppose we are given a sequence of Borel probability measures $(\mu_n : n \in \mathbb{N})$ on $\mathbb{R}$ and a further such measure μ. Write F_n and F for the corresponding distribution functions,

$$F_n(x) = \mu_n((-\infty, x]), \qquad F(x) = \mu((-\infty, x]) \tag{19.6.38}$$

and write ϕ_n and ϕ for the corresponding Fourier transforms (Definition 15.4.12)

$$\phi_n(u) = \int e^{iux}\mu_n(dx), \qquad \phi(u) = \int e^{iux}\mu(dx). \tag{19.6.39}$$

On the probability space $([0,1), \mathcal{B}([0,1)), dx)$ (with Lebesgue measure), define random variables

$$X_n(\omega) = \inf\{x \in \mathbb{R} : \omega \leq F_n(x)\}, \qquad X(\omega) = \inf\{x \in \mathbb{R} : \omega \leq F(x)\}, \tag{19.6.40}$$

Recall that $X_n \sim \mu_n$ and $X \sim \mu$. The following are equivalent:

(i) $\mu_n \to \mu$ weakly,

(ii) $F_n \to F$ as distribution functions,

(iii) $\phi_n(u) \to \phi(u)$ for all $u \in \mathbb{R}$,

(iv) $X_n \to X$ a.s.

19.7 Discrete Random Variables

19.7.1 Discrete random variable and probability generating function

Definition 19.7.1 (discrete random variable, discrete probability distribution, probability mass function)**.** A discrete probability distribution shall be understood as a probability distribution characterized by a probability mass function. Thus, the distribution of a random variable X is discrete, and X is then called a discrete random variable, if

$$\sum_{u_k} \mathbb{P}(X = u_k) = 1 \tag{19.7.1}$$

as u_k ($\{u_k\}_k$ is countable) runs through the set of all possible values of X. $\mathbb{P}(X = u_k)$ is called probability mass function. It follows that such a random variable can assume only a countable (finite or countably infinite) number of values.

Remark. If the probability distribution of X is a standard distribution such as the binomial distribution (or Poisson, or geometric), we say that X is a binomial (respectively, Poisson, or geometric) random variable.

Example 19.7.1. Suppose that two standard dice are rolled so that the sample space is $\Omega = \{(i,j) : 1 \leq i,j \leq 6\}$, and we are interested in the sum of the numbers shown so that the random variable $X : \Omega \to \mathbb{R}$ is given by $X(i,j) = i + j$. The probability of each point in Ω is $\frac{1}{36}$ with the set of possible values taken on by X being $\Omega_X = \{2, 3, \ldots, 12\}$ and, for example,

$$\mathbb{P}(X = 6) = \mathbb{P}(\{(1,5),(2,4),(3,3),(4,2),(5,1)\}) = \frac{5}{36}. \tag{19.7.2}$$

If we set $p_j = \mathbb{P}(X = j)$, for $j = 2, \ldots, 12$, then the table

j	2	3	4	5	6	7	8	9	10	11	12
p_j	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

gives the full probability distribution of the random variable X.

Definition 19.7.2 (probability generating function)**.** If X is a discrete random variable taking values in the non-negative integers $\{0, 1, \ldots\}$, then the probability generating function of X is defined by

$$G_X(z) = \mathbb{E}\left(z^X\right) = \sum_{k=0}^{\infty} \mathbb{P}(X = k) z^k = \sum_{k=0}^{\infty} p_k z^k, \quad z \in [0,1]. \tag{19.7.3}$$

Remark. Note that $G_X(z) \in [0,1]$ as $G_X(1) = \sum_{k=0}^{\infty} \mathbb{P}(X = k) = 1$.

Theorem 19.7.2. The probability generating function of X, $G(z)$, $0 \leq z \leq 1$, determines the probability distribution of X uniquely.

Remark. We can prove this by letting $\theta = \log z$ and applying Theorem 19.5.11.

Proof. Suppose that

$$G(z) = \sum_{r=0}^{\infty} p_r z^r = \sum_{r=0}^{\infty} q_r z^r, \text{ for all } 0 \leq z \leq 1, \tag{19.7.4}$$

where $p_r \geq 0$, and $q_r \geq 0$ for each r, and $\sum_{r=0}^{\infty} p_r = 1 = \sum_{r=0}^{\infty} q_r$. We will show by induction on n that $p_n = q_n$ for all n. First see, by setting $z = 0$, that $p_0 = q_0$. Now assume that $p_i = q_i$ for $0 \leq i \leq n$, then for $0 < z < 1$

$$\sum_{r=n+1}^{\infty} p_r z^r = \sum_{r=n+1}^{\infty} q_r z^r. \tag{19.7.5}$$

Divide through both sides by z^{n+1} and let $z \downarrow 0$ (as z^n is continuous at 0) to see that $p_{n+1} = q_{n+1}$ to complete the induction. □

In addition to determining the distribution uniquely, the probability generating function may be used to compute moments of the random variable by evaluating derivatives of the function.

Proposition 19.7.3. Let $X_1, \ldots, X_n$ be independent random variable taking values in $\{0, 1, \ldots\}$. Then for $z_1, \ldots, z_n \in [0, 1]$,

$$H(z) := \mathbb{E}\left(\prod_{i=1}^{n} z_i^{X_i}\right) = \prod_{i=1}^{n} G_{X_i}(z_i). \tag{19.7.6}$$

In particular, for $X = X_1 + \cdots + X_n$, we have $G_X(z) = \prod_{i=1}^{n} G_{X_i}(z)$.

Proof. Direct result from Proposition 19.5.13 by letting $\theta_i = \log z_i$ as $H(z)$ is bounded. □

Theorem 19.7.4. Let X be a random variable with probability generating function $G(z)$, then

$$\mathbb{P}(X = k) = \frac{G^{(k)}(0)}{k!}. \tag{19.7.7}$$

Proof. We know that $G(z) = \sum_{k=0}^{\infty} p_k z^k$ is convergent in $z \in [0, 1]$. Then by Lemma 10.5.5 and Theorem 10.5.7, for $z \in (0, 1)$, we have

$$G^{(k)}(z) = \sum_{n=k}^{\infty} p_n \frac{n! z^{n-k}}{(n-k)!} \;\Rightarrow\; G^{(k)}(0) = \lim_{z \downarrow 0} G^{(k)}(z) = p_k k! \;\Rightarrow\; \mathbb{P}(X = k) = p_k = \frac{G^{(k)}(0)}{k!}. \tag{19.7.8}$$

as z^n is continuous at 0. □

Theorem 19.7.5. Let X be a random variable with probability generating function $G(z)$, then

$$\mathbb{E}\left(\frac{X!}{(X-k)!}\right) = \lim_{z \uparrow 1} G^{(k)}(z) = G^{(k)}(1^-). \tag{19.7.9}$$

In particular,

$$\mathbb{E}X = \lim_{z \uparrow 1} G'(z) = G'(1^-), \qquad \mathrm{Var}(X) = G''(1^-) + G'(1^-) - (G'(1^-))^2. \tag{19.7.10}$$

Proof. First we see that $\mathbb{E}\left(\frac{X!}{(X-k)!}\right)$ is well-defined as it is non-negative.

First assume that $\mathbb{E}\left(\frac{X!}{(X-k)!}\right) < \infty$. For $0 < z < 1$, by Lemma 10.5.5 and Theorem 10.5.7

$$G^{(k)}(z) = \sum_{r=1}^{\infty} \frac{r!}{(r-k)!} p_r z^{r-k} \leq \sum_{r=1}^{\infty} \frac{r!}{(r-k)!} p_r = \mathbb{E}\left(\frac{X!}{(X-k)!}\right). \tag{19.7.11}$$

We see that $G^{(k)}(z)$ is non-decreasing in z so that $\lim_{z \uparrow 1} G^{(k)}(z) \leq \mathbb{E}\left(\frac{X!}{(X-k)!}\right)$.

Take $\varepsilon > 0$, and choose N so that $\sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r \geq \mathbb{E}\left(\frac{X!}{(X-k)!}\right) - \varepsilon$. Then

$$\lim_{z \uparrow 1} G^{(k)}(z) \geq \lim_{z \uparrow 1} \sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r z^{r-k} = \sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r \geq \mathbb{E}X - \varepsilon. \tag{19.7.12}$$

Note that $(*)$ holds because it takes the limit of the sum of finite items, having the form of z^n. This is true for each $\varepsilon > 0$, whence $\lim_{z \uparrow 1} G^{(k)}(z) \geq \mathbb{E}X$ and it follows that $G^{(k)}(1^-) = \lim_{z \uparrow 1} G^{(k)}(z) = \mathbb{E}\left(\frac{X!}{(X-k)!}\right)$.

If $\mathbb{E}\left(\frac{X!}{(X-k)!}\right) = \infty$, then for any $M > 0$ choose N so that $\sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r \geq M$, and, as above, see that

$$\lim_{z\uparrow 1} G^{(k)}(z) \geq \lim_{z\uparrow 1} \sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r z^{r-1} = \sum_{r=1}^{N} \frac{r!}{(r-k)!} p_r \geq M, \tag{19.7.13}$$

this is true for any M, whence $G^{(k)}(1^-) = \lim_{z\uparrow 1} G^{(k)}(z) = \infty$ and $\mathbb{E}\left(\frac{X!}{(X-k)!}\right) = G^{(k)}(1^-)$.

Accordingly, we have $\mathbb{E}X = G'(1^-)$ and

$$\mathrm{Var}(X) = \mathbb{E}\left(X^2\right) - (\mathbb{E}X)^2 = \mathbb{E}\left(X(X-1)\right) + \mathbb{E}X - (\mathbb{E}X)^2 = G''(1^-) + G'(1^-) - (G'(1^-))^2, \tag{19.7.14}$$

as required. □

Remark. Here we can not write $G(1)$ as z^n is NOT continuous at 1 when $n \to \infty$.

19.7.2 Bernoulli random variables

Definition 19.7.3 (Bernoulli random variable)**.** A random variable X in $\{0, 1\}$ is Bernoulli distributed if, for some $p \in [0, 1]$ and $q = 1 - p$, has probability mass function

$$\mathbb{P}(X = k) = \begin{cases} p & k = 1 \\ q & k = 0 \end{cases} \tag{19.7.15}$$

We write $X \sim \mathrm{Ber}(p)$. The cumulative distribution function of Bernoulli distribution is given by

$$F(x) = \begin{cases} 0 & x < 0 \\ q & 0 \leq x < 1 \\ 1 & x \geq 1 \end{cases} \tag{19.7.16}$$

Example 19.7.6 (Bernoulli distribution)**.** Consider a sample space with just two points $\Omega = \{H, T\}$, where the two points may be thought of as $H =$ "heads", and $T =$ "tails", so we are modelling a coin toss where we will take p as the probability of heads and $1 - p$ as the probability of tails. Then $p = \mathbb{P}(H)$ and $1 - p = \mathbb{P}(T)$, with $0 \leq p \leq 1$.

Proposition 19.7.7. Suppose $X \sim \mathrm{Ber}(p)$. Then for $\theta, t \in \mathbb{R}$,

$$G_X(z) = (1-p) + pz, \qquad M_X(\theta) = (1-p) + pe^{\theta}, \qquad \phi_X(t) = (1-p) + pe^{it}. \tag{19.7.17}$$

Proof. From Definition 19.7.2, 19.5.4,

$$\begin{aligned} G_X(z) &= \mathbb{E}\left(z^X\right) = \mathbb{P}(X=1)z^1 + \mathbb{P}(X=0)z^0 = pz + q, \\ M_X(\theta) &= \mathbb{E}\left(e^{\theta X}\right) = \mathbb{P}(X=1)e^{\theta} + \mathbb{P}(X=0)\cdot 1 = pe^{\theta} + q, \\ \phi_X(t) &= \mathbb{E}\left(e^{itX}\right) = \mathbb{P}(X=1)e^{it} + \mathbb{P}(X=0)\cdot 1 = pe^{it} + q. \end{aligned}$$

□

Proposition 19.7.8. Suppose $X \sim \mathrm{Ber}(p)$. Then

$$\text{(i) } \mathbb{E}X = p, \qquad \text{(ii) } \mathrm{Var}\, X = p(1-p), \qquad \text{(iii) } \mathrm{Skew}(X) = \frac{1-2p}{\sqrt{p(1-p)}}, \qquad \text{(iv) } \mathrm{Kurt}(X) = \frac{1-6p(1-p)}{p(1-p)}. \tag{19.7.18}$$

Proof. Let $q = 1 - p$,

$$\mathbb{E}X = \sum_{k=0}^{1} \mathbb{P}(X=k)k = p, \qquad \mathbb{E}X^2 = \sum_{k=0}^{1} \mathbb{P}(X=k)k^2 = p \;\Rightarrow\; \mathrm{Var}\, X = p - p^2 = pq. \tag{19.7.19}$$

$$\mathbb{E}(X-p)^3 = \sum_{k=0}^{1} \mathbb{P}(X=k)(k-p)^3 = p(1-p)^3 + q(0-p)^3 = pq^3 - qp^3 = pq(q-p). \tag{19.7.20}$$

$$\mathrm{Skew}(X) = \frac{pq(q-p)}{(pq)^{3/2}} = \frac{q-p}{\sqrt{pq}}. \tag{19.7.21}$$

$$\begin{aligned}\mathbb{E}(X-p)^4 &= \sum_{k=0}^{1} \mathbb{P}(X=k)(k-p)^4 = p(1-p)^4 + q(0-p)^4 = pq^4 + qp^4 \\ &= pq(p^2 - pq + q^2) = pq(p^2 + 2pq + q^2 - 3pq) = pq(1-3pq).\end{aligned}$$

$$\mathrm{Kurt}(X) = \frac{pq(1-3pq)}{p^2q^2} - 3 = \frac{1-3pq}{pq} - 3 = \frac{1-6pq}{pq}. \tag{19.7.22}$$

We can also apply Theorem 19.7.5,

$$\mathbb{E}X = G'(1^-) = p, \quad \mathrm{Var}(X) = G''(1^-) + G'(1^-) - \left(G'(1^-)\right)^2 = 0 + p - p^2 = p(1-p) = pq. \tag{19.7.23}$$

□

19.7.3 Binomial random variables

Definition 19.7.4 (Binomial random variable)**.** A random variable X in $\{0, 1, \ldots, n\}$ is Binomial distributed if, for some $n \in \mathbb{Z}^+$ and $p \in [0, 1]$, has probability mass function

$$\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}, \qquad k \in \{0, 1, \ldots, n\}. \tag{19.7.24}$$

We write $X \sim \mathrm{Bin}(n, p)$.

Remark. This models the number of heads obtained in n successive tosses of the coin. Note that if $n = 1$, $X \sim \mathrm{Ber}(p)$.

Proposition 19.7.9. Suppose $X \sim \mathrm{Bin}(n, p)$. Then for $\theta, t \in \mathbb{R}$,

$$G_X(z) = \left((1-p) + pz\right)^n, \qquad M_X(\theta) = \left((1-p) + pe^{\theta}\right)^n, \qquad \phi_X(t) = \left((1-p) + pe^{it}\right)^n. \tag{19.7.25}$$

Proof. From Definition 19.7.2, 19.5.4,

$$\begin{aligned}G_X(z) &= \mathbb{E}\left(z^X\right) = \sum_{k=0}^{n} \mathbb{P}(X=k) z^k = \sum_{k=0}^{n} \binom{n}{k} (zp)^k (1-p)^{n-k} = \left((1-p) + pz\right)^n, \\ M_X(\theta) &= \mathbb{E}\left(e^{\theta X}\right) = \sum_{k=0}^{n} \mathbb{P}(X=k) e^{\theta k} = \sum_{k=0}^{n} \binom{n}{k} (e^{\theta}p)^k (1-p)^{n-k} = \left((1-p) + pe^{\theta}\right)^n.\end{aligned}$$

and similarly for $\phi_X(t)$. □

Remark. By Proposition 19.7.3, we can see that $X \sim \mathrm{Bin}(n, p)$ is sum of $X_1, \ldots, X_n \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(p)$ by assuming $\theta = \log z$.

Proposition 19.7.10. Suppose $X \sim \mathrm{Bin}(n, p)$. Then

$$\text{(i) } \mathbb{E}X = np, \qquad \text{(ii) } \mathrm{Var}\, X = np(1-p), \qquad \text{(iii) } \mathrm{Skew}(X) = \frac{1-2p}{\sqrt{np(1-p)}}, \qquad \text{(iv) } \mathrm{Kurt}(X) = \frac{1-6p(1-p)}{np(1-p)}. \tag{19.7.26}$$

Proof.

$$\mathbb{E}X = \sum_{k=0}^{n} \mathbb{P}(X=k)k = \sum_{k=1}^{n} \binom{n}{k} p^k (1-p)^{n-k} k = np \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} (1-p)^{n-k} = np. \tag{19.7.27}$$

$$\begin{aligned}\mathbb{E}X^2 &= \sum_{k=0}^{n} \mathbb{P}(X=k)k^2 = \sum_{k=1}^{n} \binom{n}{k} p^k (1-p)^{n-k} (k^2 - k + k) \\ &= n(n-1)p^2 \sum_{k=2}^{n} \binom{n-2}{k-2} p^{k-2} (1-p)^{n-k} + np = n(n-1)p^2 + np.\end{aligned}$$

Then $\operatorname{Var} X = n(n-1)p^2 + np - n^2p^2 = np - np^2 = np(1-p)$. Furthermore,

$$\begin{aligned}
\mathbb{E}(X-np)^3 &= \sum_{k=0}^{n} \mathbb{P}(X=k)(k-np)^3 = \sum_{k=0}^{n} \mathbb{P}(X=k)k^3 - 3np\sum_{k=0}^{n} \mathbb{P}(X=k)k^2 + 3n^2p^2\sum_{k=0}^{n} \mathbb{P}(X=k)k - n^3p^3 \\
&= \sum_{k=0}^{n} \mathbb{P}(X=k)\left(k(k-1)(k-2) + 3k^2 - 2k\right) - 3np\sum_{k=0}^{n} \mathbb{P}(X=k)k^2 + 3n^2p^2\sum_{k=0}^{n} \mathbb{P}(X=k)k - n^3p^3 \\
&= n(n-1)(n-2)p^3 + (3-3np)\left(n(n-1)p^2 + np\right) + \left(-2 + 3n^2p^2\right)np - n^3p^3 \\
&= np(1-2p)(1-p).
\end{aligned}$$

and

$$\mathbb{E}X^3 = n(n-1)(n-2)p^3 + 3\left(n(n-1)p^2 + np\right) - 2np = np\left((n-1)(n-2)p^2 + 3(n-1)p + 1\right). \tag{19.7.28}$$

Therefore,

$$\operatorname{Skew}(X) = \frac{np(1-2p)(1-p)}{(np(1-p))^{3/2}} = \frac{1-2p}{\sqrt{np(1-p)}}. \tag{19.7.29}$$

$$\mathbb{E}(X-np)^4 = \sum_{k=0}^{n} \mathbb{P}(X=k)k^4 - 4np\sum_{k=0}^{n} \mathbb{P}(X=k)k^3 + 6n^2p^2\sum_{k=0}^{n} \mathbb{P}(X=k)k^2 - 4n^3p^3\sum_{k=0}^{n} \mathbb{P}(X=k)k + n^4p^4$$

and $\mathbb{E}X^4 = \sum_{k=0}^{n} \mathbb{P}(X=k)\left(k(k-1)(k-2)(k-3) + 6k^3 - 11k^2 + 6k\right)$. Therefore,

$$\begin{aligned}
\mathbb{E}(X-np)^4 &= n(n-1)(n-2)(n-3)p^4 + (6-4np)np\left((n-1)(n-2)p^2 + 3(n-1)p + 1\right) \\
&\quad + (-11 + 6n^2p^2)\left(n(n-1)p^2 + np\right) + (6 - 4n^3p^3)np + n^4p^4 \\
&= np\left((3n-6)p^3 + (-6n+12)p^2 + (3n-7)p + 1\right) = np(1-p)\left((3n-6)p(1-p) + 1\right).
\end{aligned}$$

Thus,

$$\operatorname{Kurt}(X) = \frac{np(1-p)\left((3n-6)p(1-p)+1\right)}{n^2p^2(1-p)^2} - 3 = \frac{(3n-6)p(1-p)+1}{np(1-p)} - 3 = \frac{1-6p(1-p)}{np(1-p)}. \tag{19.7.30}$$

□

19.7.4 Geometric random variables

Definition 19.7.5 (geometric random variable)**.** A random variable X in $\{0, 1, \dots\}$ is geometric distributed if, for some $p \in [0,1]$, has probability mass function

$$\mathbb{P}(X=k) = (1-p)^k p, \quad k \in \{0, 1, \dots\} \tag{19.7.31}$$

We write $X \sim \operatorname{Geo}(p)$. The cumulative distribution function of geometric distribution is given by

$$F(x) = 1 - (1-p)^{x+1}. \tag{19.7.32}$$

Proposition 19.7.11. Suppose $X \sim \operatorname{Geo}(p)$. Then for $\theta, t \in \mathbb{R}$,

$$G_X(z) = \frac{p}{1-(1-p)z}, \qquad M_X(\theta) = \frac{p}{1-(1-p)e^{\theta}}, \qquad \phi_X(t) = \frac{p}{1-(1-p)e^{it}}. \tag{19.7.33}$$

Proof. From Definition 19.7.2, 19.5.4,

$$\begin{aligned}
G_X(z) &= \mathbb{E}\left(z^X\right) = \sum_{k=0}^{\infty} \mathbb{P}(X=k)z^k = \sum_{k=0}^{\infty} (1-p)^k pz^k = p\sum_{k=0}^{\infty} (1-p)^k z^k = \frac{p}{1-(1-p)z}, \\
M_X(\theta) &= \mathbb{E}\left(e^{\theta X}\right) = \sum_{k=0}^{\infty} \mathbb{P}(X=k)e^{\theta k} = p\sum_{k=0}^{\infty} (1-p)^k \left(e^{\theta}\right)^k = \frac{p}{1-(1-p)e^{\theta}}.
\end{aligned}$$

and similarly for $\phi_X(t)$. □

Proposition 19.7.12. Suppose $X \sim \text{Geo}(p)$. Then

$$\text{(i) } \mathbb{E}X = \frac{1-p}{p}, \qquad \text{(ii) } \operatorname{Var} X = \frac{1-p}{p^2}, \qquad \text{(iii) } \operatorname{Skew}(X) = \frac{2-p}{\sqrt{1-p}}, \qquad \text{(iv) } \operatorname{Kurt}(X) = 6 + \frac{p^2}{1-p}. \tag{19.7.34}$$

Proof.

$$\mathbb{E}X = \sum_{k=0}^{\infty} \mathbb{P}(X=k)k = \sum_{k=0}^{\infty} (1-p)^k pk = \sum_{k=0}^{\infty} (1-p)^k p(k+1-1) = -p\left(\frac{1-p}{p}\right)' - 1 = \frac{1-p}{p}. \tag{19.7.35}$$

$$\begin{aligned} \mathbb{E}X^2 &= \sum_{k=0}^{\infty} \mathbb{P}(X=k)k^2 = \sum_{k=0}^{\infty} (1-p)^k pk^2 = \sum_{k=0}^{\infty} (1-p)^k p(k^2+3k+2-3k-2) \\ &= p\left(\frac{(1-p)^2}{p}\right)'' - 3\frac{1-p}{p} - 2 = \frac{(1-p)(2-p)}{p^2}. \end{aligned}$$

Therefore,

$$\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \frac{(1-p)(2-p)}{p^2} - \left(\frac{1-p}{p}\right)^2 = \frac{1-p}{p^2}. \tag{19.7.36}$$

$$\begin{aligned} \mathbb{E}X^3 &= \sum_{k=0}^{\infty} \mathbb{P}(X=k)k^3 = \sum_{k=0}^{\infty} (1-p)^k pk^3 = \sum_{k=0}^{\infty} (1-p)^k p(k^3+6k^2+11k+6-6k^2-11k-6) \\ &= -p\left(\frac{(1-p)^3}{p}\right)''' - 6\frac{(1-p)(2-p)}{p^2} - 11\frac{1-p}{p} - 6 = \frac{(1-p)(6-6p+p^2)}{p^3}. \end{aligned}$$

$$\mathbb{E}\left(X - \frac{1-p}{p}\right)^3 = \frac{(1-p)(6-6p+p^2)}{p^3} - 3\frac{1-p}{p}\frac{(1-p)(2-p)}{p^2} + 2\left(\frac{1-p}{p}\right)^3 = \frac{(1-p)(2-p)}{p^3}. \tag{19.7.37}$$

$$\operatorname{Skew}(X) = \frac{(1-p)(2-p)/p^3}{(1-p)^{3/2}/p^3} = \frac{2-p}{\sqrt{1-p}}. \tag{19.7.38}$$

Furthermore,

$$\begin{aligned} \mathbb{E}X^4 &= \sum_{k=0}^{\infty} \mathbb{P}(X=k)k^4 = \sum_{k=0}^{\infty} (1-p)^k pk^4 = \sum_{k=0}^{\infty} (1-p)^k p(k^4+10k^3+35k^2+50k+24-10k^3-35k^2-50k-24) \\ &= p\left(\frac{(1-p)^4}{p}\right)'''' - 10\frac{(1-p)(6-6p+p^2)}{p^3} - 35\frac{(1-p)(2-p)}{p^2} - 50\frac{1-p}{p} - 24 = \frac{(1-p)(2-p)(12-12p+p^2)}{p^4}. \end{aligned}$$

$$\begin{aligned} \mathbb{E}\left(X - \frac{1-p}{p}\right)^4 &= \frac{(1-p)(2-p)(12-12p+p^2)}{p^4} - 4\frac{1-p}{p}\frac{(1-p)(6-6p+p^2)}{p^3} + 6\left(\frac{1-p}{p}\right)^2\frac{(1-p)(2-p)}{p^2} - 3\left(\frac{1-p}{p}\right)^4 \\ &= \frac{(1-p)(9-9p+p^2)}{p^4}. \end{aligned}$$

$$\operatorname{Kurt}(X) = \frac{(1-p)(9-9p+p^2)/p^4}{(1-p)^2/p^4} - 3 = \frac{p^2}{1-p} + 9 - 3 = 6 + \frac{p^2}{1-p}. \tag{19.7.39}$$

□

19.7.5 Negative binomial random variables

Suppose there is a sequence of independent Bernoulli trials, each trial having two potential outcomes called "success" and "failure". In each trial the probability of failure is p and of success is $1-p$. We are observing this sequence until a predefined

number r of failures has occurred. Then the random number of successes we have seen, X, will have the negative binomial (or Pascal) distribution.

Definition 19.7.6 (negative binomial random variable)**.** A random variable X in $\{0, 1, \dots\}$ is negative binomial distributed if, for some $p \in [0, 1]$ and $r \in \mathbb{R}^+$ (extended version), has probability mass function

$$\mathbb{P}(X = k) = \binom{k+r-1}{k} \cdot (1-p)^k p^r, \quad k \in \{0, 1, \dots\} \tag{19.7.40}$$

We write $\mathrm{NB}(r, p)$.

First, we need to make sure that the probability mass function makes sence.

Theorem 19.7.13. For $r \in \mathbb{R}^+$,

$$\sum_{k=0}^{\infty} \mathbb{P}(X = k) = \sum_{k=0}^{\infty} \binom{k+r-1}{k} \cdot (1-p)^k p^r = 1. \tag{19.7.41}$$

Proof.

$$\begin{aligned} \binom{k+r-1}{k} &= \frac{(k+r-1)!}{k!\,(r-1)!} = \frac{(k+r-1)(k+r-2)\cdots(r)}{k!} \\ &= \frac{(k+r-1)\cdots(r)}{k!} = (-1)^k \frac{(-r)(-r-1)(-r-2)\cdots(-r-k+1)}{k!} = (-1)^k \binom{-r}{k} \qquad (*). \end{aligned}$$

Then by Definition 4.4.1 and $(*)$,

$$p^{-r} = (1-(1-p))^{-r} = \sum_{k=0}^{\infty} \binom{-r}{k} (-(1-p))^k = \sum_{k=0}^{\infty} \binom{k+r-1}{k} (1-p)^k \tag{19.7.42}$$

as required. □

Proposition 19.7.14. Suppose $X \sim \mathrm{NB}(r, p)$. Then for $|z| < \frac{1}{p}$, $\theta < -\log p$ and $t \in \mathbb{R}$,

$$G_X(z) = \left(\frac{p}{1-(1-p)z}\right)^r, \qquad M_X(\theta) = \left(\frac{p}{1-(1-p)e^{\theta}}\right)^r, \qquad \phi_X(t) = \left(\frac{p}{1-(1-p)e^{it}}\right)^r. \tag{19.7.43}$$

Remark. By Proposition 19.7.3, we can see that $X \sim \mathrm{NB}(n, p)$ is sum of $X_1, \dots, X_n \overset{\text{i.i.d.}}{\sim} \mathrm{Geo}(p)$ by assuming $\theta = \log z$.

Proof. From Definition 19.7.2,

$$\begin{aligned} G_X(z) &= \mathbb{E}\left(z^X\right) = \sum_{k=0}^{\infty} \mathbb{P}(X = k) z^k = \sum_{k=0}^{\infty} \binom{k+r-1}{k} \cdot (1-p)^k p^r z^k \\ &= p^r \sum_{k=0}^{\infty} \binom{k+r-1}{k} \cdot ((1-p)z)^k = \left(\frac{p}{1-(1-p)z}\right)^r. \end{aligned}$$

and similarly for $M_X(\theta)$ and $\phi_X(t)$. □

Proposition 19.7.15. Suppose $X \sim \mathrm{NB}(r, p)$. Then

(i) $\mathbb{E}X = \dfrac{r(1-p)}{p}$, (ii) $\mathrm{Var}\, X = \dfrac{r(1-p)}{p^2}$, (iii) $\mathrm{Skew}(X) = \dfrac{2-p}{\sqrt{r(1-p)}}$, (iv) $\mathrm{Kurt}(X) = \dfrac{6}{r} + \dfrac{p^2}{r(1-p)}$.

Proof. From proof of Theorem 19.7.13,

$$\binom{k+r-1}{k} k = (-1)^k \frac{(-r)(-r-1)(-r-2)\cdots(-r-k+1)}{(k-1)!} = r(-1)^{k-1} \frac{(-r-1)(-r-2)\cdots(-r-k+1)}{(k-1)!} = r\binom{k+r-1}{k-1}.$$

Thus,

$$\mathbb{E}X = \sum_{k=0}^{\infty} \binom{k+r-1}{k} \cdot (1-p)^k p^r k = \frac{r(1-p)}{p} \sum_{k=1}^{\infty} \binom{k+r-1}{k-1} \cdot (1-p)^{k-1} p^{r+1} = \frac{r(1-p)}{p}. \tag{19.7.44}$$

$$\begin{aligned}
\mathbb{E}X^2 &= \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r k^2 = \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r (k^2-k+k) \\
&= r(r+1)\left(\frac{1-p}{p}\right)^2\sum_{k=2}^{\infty}\binom{k+r-1}{k-2}\cdot(1-p)^{k-2}p^{r+2} + \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r k \\
&= r(r+1)\left(\frac{1-p}{p}\right)^2 + \frac{r(1-p)}{p} = \frac{r(1-p)}{p}\left(\frac{r+1-rp}{p}\right).
\end{aligned}$$

Therefore,

$$\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \frac{r(1-p)}{p}\left(\frac{r+1-rp}{p}\right) - \left(\frac{r(1-p)}{p}\right)^2 = \frac{r(1-p)}{p^2}. \tag{19.7.45}$$

$$\begin{aligned}
\mathbb{E}X^3 &= \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r k^3 = \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r (k^3-3k^2+2k+3k^2-2k) \\
&= r(r+1)(r+2)\left(\frac{1-p}{p}\right)^3 + 3\frac{r(1-p)}{p}\left(\frac{r+1-rp}{p}\right) - 2\frac{r(1-p)}{p} \\
&= \frac{r(1-p)}{p}\frac{r^2p^2-(r+1)(2r+1)p+(r+1)(r+2)}{p^2}.
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left(X-\frac{r(1-p)}{p}\right)^3 &= \frac{r(1-p)}{p}\frac{r^2p^2-(r+1)(2r+1)p+(r+1)(r+2)}{p^2} - 3\frac{r(1-p)}{p}\frac{r(1-p)}{p}\left(\frac{r+1-rp}{p}\right) + 2\left(\frac{r(1-p)}{p}\right)^3 \\
&= \frac{r(1-p)}{p}\frac{(2-p)}{p^2} = \frac{r(1-p)(2-p)}{p^3}.
\end{aligned}$$

$$\operatorname{Skew}(X) = \frac{r(1-p)(2-p)/p^3}{r^{3/2}(1-p)^{3/2}/p^3} = \frac{2-p}{\sqrt{r(1-p)}}. \tag{19.7.46}$$

Furthermore,

$$\begin{aligned}
\mathbb{E}X^4 &= \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r k^4 = \sum_{k=0}^{\infty}\binom{k+r-1}{k}\cdot(1-p)^k p^r (k^4-6k^3+11k^2-6k+6k^3-11k^2+6k) \\
&= \frac{r(1-p)}{p}\left((r+1)(r+2)(r+3)\left(\frac{1-p}{p}\right)^3 + 6\frac{r^2p^2-(r+1)(2r+1)p+(r+1)(r+2)}{p^2} - 11\left(\frac{r+1-rp}{p}\right) + 6\right) \\
&= \frac{r(1-p)}{p}\frac{(r+1)(r+2)(r+3)-3(r+1)^2(r+2)p+(r+1)(3r^2+3r+1)p^2-r^3p^3}{p^3}.
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left(X-\frac{r(1-p)}{p}\right)^4 &= \frac{r(1-p)}{p}\left(\frac{(r+1)(r+2)(r+3)-3(r+1)^2(r+2)p+(r+1)(3r^2+3r+1)p^2-r^3p^3}{p^3}\right. \\
&\qquad -4\left(\frac{r(1-p)}{p}\right)\frac{r^2p^2-(r+1)(2r+1)p+(r+1)(r+2)}{p^2} \\
&\qquad \left. +6\left(\frac{r(1-p)}{p}\right)^2\left(\frac{r+1-rp}{p}\right) - 3\left(\frac{r(1-p)}{p}\right)^3\right) \\
&= \frac{r(1-p)}{p}\left(\frac{3(r+2)-(3r+6)\,p+p^2}{p^3}\right).
\end{aligned}$$

$$\operatorname{Kurt}(X) = \frac{r(1-p)(3(r+2)-(3r+6)\,p+p^2)/p^4}{r^2(1-p)^2/p^4} - 3 = \frac{6}{r} + \frac{p^2}{r(1-p)}. \tag{19.7.47}$$

□

19.7.6 Poisson random variables

Definition 19.7.7 (Poisson random variable)**.** A random variable X in $\{0, 1, \dots\}$ is poisson distributed if, for some $p \in [0, 1]$ and $r \in \mathbb{R}^+$ (extended version), has probability mass function

$$\mathbb{P}(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}, \qquad k \in \{0, 1, \dots\}. \tag{19.7.48}$$

We write $\text{Poi}(\lambda)$.

Proposition 19.7.16. Suppose $X \sim \text{Poi}(\lambda)$. Then for $z, \theta, t \in \mathbb{R}$,

$$G_X(z) = \exp(\lambda(z-1)), \qquad M_X(\theta) = \exp(\lambda(e^\theta - 1)), \qquad \phi_X(t) = \exp(\lambda(e^{it} - 1)). \tag{19.7.49}$$

Proof. From Definition 19.7.2,

$$G_X(z) = \mathbb{E}\left(z^X\right) = \sum_{k=0}^{\infty} \mathbb{P}(X = k) z^k = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} z^k = e^{\lambda z - \lambda} \sum_{k=0}^{\infty} \frac{(\lambda z)^k e^{-\lambda z}}{k!} = e^{\lambda(z-1)}. \tag{19.7.50}$$

and similarly for $M_X(\theta)$ and $\phi_X(t)$. □

Proposition 19.7.17. Suppose $X \sim \text{Poi}(\lambda)$. Then

$$\text{(i) } \mathbb{E}X = \lambda, \qquad \text{(ii) } \operatorname{Var} X = \lambda, \qquad \text{(iii) } \operatorname{Skew}(X) = \lambda^{-1/2}, \qquad \text{(iv) } \operatorname{Kurt}(X) = \lambda^{-1}.$$

Proof.

$$\mathbb{E}X = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} k = \lambda \sum_{k=1}^{\infty} \frac{\lambda^{k-1} e^{-\lambda}}{(k-1)!} = \lambda. \tag{19.7.51}$$

$$\mathbb{E}X^2 = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} k^2 = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} (k^2 - k + k) = \lambda^2 \sum_{k=2}^{\infty} \frac{\lambda^{k-2} e^{-\lambda}}{(k-2)!} + \lambda = \lambda^2 + \lambda. \tag{19.7.52}$$

Therefore, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \lambda^2 + \lambda - \lambda^2 = \lambda$.

$$\mathbb{E}X^3 = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} k^3 = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} (k^3 - 3k^2 + 2k + 3k^2 - 2k) = \lambda^3 + 3(\lambda^2 + \lambda) - 2\lambda = \lambda^3 + 3\lambda^2 + \lambda. \tag{19.7.53}$$

$$\mathbb{E}\left(X - \lambda\right)^3 = \lambda^3 + 3\lambda^2 + \lambda - 3\lambda(\lambda^2 + \lambda) + 2\lambda^3 = \lambda \;\Rightarrow\; \operatorname{Skew}(X) = \frac{\lambda}{\lambda^{3/2}} = \lambda^{-1/2}. \tag{19.7.54}$$

Furthermore,

$$\begin{aligned} \mathbb{E}X^4 &= \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} k^4 = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} (k^4 - 6k^3 + 11k^2 - 6k + 6k^3 - 11k^2 + 6k) \\ &= \lambda^4 + 6\left(\lambda^3 + 3\lambda^2 + \lambda\right) - 11\left(\lambda^2 + \lambda\right) + 6\lambda = \lambda^4 + 6\lambda^3 + 7\lambda^2 + \lambda. \end{aligned}$$

$$\mathbb{E}\left(X - \lambda\right)^4 = \lambda^4 + 6\lambda^3 + 7\lambda^2 + \lambda - 4\lambda\left(\lambda^3 + 3\lambda^2 + \lambda\right) + 6\lambda^2\left(\lambda^2 + \lambda\right) - 3\lambda^4 = 3\lambda^2 + \lambda. \tag{19.7.55}$$

$$\operatorname{Kurt}(X) = \frac{\lambda(3\lambda + 1)}{\lambda^2} - 3 = \lambda^{-1}. \tag{19.7.56}$$

□

Proposition 19.7.18 (sums of independent Poisson random variables)**.** Let $X_1, \dots, X_n$ with $X_i \sim \text{Poi}(\lambda_i)$ where $\lambda_i > 0$ be independent random variables. Then

$$X := X_1 + \cdots + X_n \sim \text{Poi}\left(\sum_{i=1}^{n} \lambda_i\right). \tag{19.7.57}$$

Proof. The probability generating function of X_i is $e^{-\lambda_i(1-z)}$. Then by Proposition 19.7.3,

$$G_X(z) = \prod_{i=1}^{n} G_{X_i}(z) = \prod_{i=1}^{n} e^{-\lambda_i(1-z)} = e^{-(1-z)\sum_{i=1}^{n}\lambda_i}. \tag{19.7.58}$$

Thus, X is a Poisson random variables with parameter $\sum_{i=1}^{n}\lambda_i$. □

Proposition 19.7.19 (sums of independent Poisson random variables for fixed number)**.** Let $X \sim \text{Poi}(\lambda)$ and $Y \sim \text{Poi}(\mu)$ where $\lambda, \mu > 0$ be independent random variables. Then given that $X + Y = n$, for $0 \le k \le n$,

$$X_{X+Y=n} \sim \text{Bin}\left(n, \frac{\lambda}{\lambda+\mu}\right). \tag{19.7.59}$$

Proof. By Proposition 19.7.18, $X + Y \sim \text{Poi}(\lambda + \mu)$. For $0 \le k \le n$,

$$\begin{aligned}
\mathbb{P}(X = k | X + Y = n) &= \frac{\mathbb{P}(X = k, X + Y = n)}{\mathbb{P}(X + Y = n)} = \frac{\mathbb{P}(X = k, Y = n - k)}{\mathbb{P}(X + Y = n)} \\
&= \frac{\mathbb{P}(X = k)\mathbb{P}(Y = n - k)}{\mathbb{P}(X + Y = n)} = \frac{e^{-\lambda}\frac{\lambda^k}{k!}e^{-\mu}\frac{\mu^{n-k}}{(n-k)!}}{e^{-(\lambda+\mu)}\frac{(\lambda+\mu)^n}{n!}} \\
&= \binom{n}{k}\left(\frac{\lambda}{\lambda+\mu}\right)^k\left(1 - \frac{\lambda}{\lambda+\mu}\right)^{n-k}
\end{aligned}$$

as required. □

19.8 Continuous Random Variables

19.8.1 Continuous random variable

Definition 19.8.1 (continuous random variable)**.** [12]

Definition 19.8.2 (median)**.** The median m of a continuous random variable X with density function f is the point which satisfies

$$\mathbb{P}(X \ge m) = \int_m^\infty f(x)dx = \int_{-\infty}^m f(x)dx = \mathbb{P}(X \le m) = \frac{1}{2}. \tag{19.8.1}$$

Thus half the distribution lies on one side of m and half on the other. For a discrete random variable, X, a median m is a point satisfying

$$\mathbb{P}(X \ge m) \ge \frac{1}{2} \quad \text{and} \quad \mathbb{P}(X \le m) \ge \frac{1}{2}. \tag{19.8.2}$$

Remark. Note that for the normal distribution $\mathcal{N}(\mu, \sigma^2)$ (see Definition 19.8.6) the mean is equal to the median (and this is true for any symmetric distribution).

Definition 19.8.3 (mode)**.** A mode of a continuous random variable, with density function f, is a point m for which $f(m) \ge f(x)$ for all x, that is the density function is maximized at a mode.

For a discrete random variable a mode is a point, m, for which $\mathbb{P}(X = m) \ge \mathbb{P}(X = x)$ for all possible values x.

Remark. In the case of the normal distribution function (see Definition 19.8.6), the mean and median are also the mode. For example, for the $\mathcal{E}(\lambda)$ distribution with density function $\lambda e^{-\lambda x}$ for $x > 0$, we have seen that the mean is $1/\lambda$, it is easy to check that the median is $\log 2/\lambda$ and the mode is 0.

19.8.2 Uniform random variables

Definition 19.8.4 (uniform random variable)**.** A random variable X in $\mathbb{R}$ is uniformly distributed if, for some $a < b \in \mathbb{R}$, X has density function

$$f_X(x) = \begin{cases} \frac{1}{b-a} & \text{for } x \in [a, b] \\ 0 & \text{otherwise} \end{cases} \tag{19.8.3}$$

[12] need definition.

We write $X \sim \mathcal{U}(a,b)$. The cumulative distribution function of uniform distribution is given by

$$F(x) = \begin{cases} 0 & \text{for } x < a \\ \frac{x-a}{b-a} & \text{for } x \in [a,b) \\ 1 & \text{for } x \geq b \end{cases} \tag{19.8.4}$$

A result that is important for computer simulation of random variables is the following.

Theorem 19.8.1. Suppose that $U \sim \mathcal{U}[0,1]$, then for any continuous distribution function F, the random variable $X = F^{-1}(U)$ has distribution function F.

Proof. Note that for $u \in [0,1]$, $\mathbb{P}(U \leq u) = u$, so we have

$$\mathbb{P}(X \leq x) = \mathbb{P}\left(F^{-1}(U) \leq x\right) = \mathbb{P}(U \leq F(x)) = F(x), \tag{19.8.5}$$

which gives the result. □

Remark. As a consequence, in order to simulate any random variable it is only necessary to use a random number generator to provide a random number uniform in $[0,1]$ and then use the above procedures in the continuous and discrete cases.

Proposition 19.8.2. Suppose $X \sim \mathcal{U}(a,b)$. Then for $\theta, t \in \mathbb{R}$,

$$M_X(\theta) = \frac{e^{\theta b} - e^{\theta a}}{\theta(b-a)}, \qquad \phi_X(t) = \frac{e^{itb} - e^{ita}}{it(b-a)}. \tag{19.8.6}$$

Proof. From Definition 19.5.4,

$$M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right) = \int_a^b e^{\theta x} \frac{1}{b-a} dx = \frac{1}{\theta(b-a)} \int_a^b de^{\theta x} = \frac{e^{\theta b} - e^{\theta a}}{\theta(b-a)}. \tag{19.8.7}$$

$$\phi_X(t) = \mathbb{E}\left(e^{itX}\right) = \int_a^b e^{itx} \frac{1}{b-a} dx = \frac{1}{it(b-a)} \int_a^b de^{itx} = \frac{e^{itb} - e^{ita}}{it(b-a)}. \tag{19.8.8}$$

□

Proposition 19.8.3. Suppose $X \sim \mathcal{U}(a,b)$. Then

$$\text{(i) } \mathbb{E}X = \frac{1}{2}(b+a), \qquad \text{(ii) } \operatorname{Var} X = \frac{1}{12}(b-a)^2, \qquad \text{(iii) } \operatorname{Skew}(X) = 0, \qquad \text{(iv) } \operatorname{Kurt}(X) = -\frac{6}{5}. \tag{19.8.9}$$

Proof. With Propositions 19.8.2, 19.5.10, with L'Hôpital Rule[13]

$$\mathbb{E}X = \left.\frac{dM_X(\theta)}{d\theta}\right|_{\theta=0} = \left.\frac{(\theta b - 1)e^{\theta b} - (\theta a - 1)e^{\theta a}}{\theta^2(b-a)}\right|_{\theta=0} = \left.\frac{\theta b^2 e^{\theta b} - \theta a^2 e^{\theta a}}{2\theta(b-a)}\right|_{\theta=0} = \left.\frac{b^2 e^{\theta b} - a^2 e^{\theta a}}{2(b-a)}\right|_{\theta=0} = \frac{1}{2}(b+a).$$

$$\begin{aligned} \mathbb{E}X^2 &= \left.\frac{d^2 M_X(\theta)}{d\theta^2}\right|_{\theta=0} = \left.\frac{\theta^2\left(\theta b^2 e^{\theta b} - \theta a^2 e^{\theta a}\right) - 2\theta\left((\theta b - 1)e^{\theta b} - (\theta a - 1)e^{\theta a}\right)}{\theta^4(b-a)}\right|_{\theta=0} \\ &= \left.\frac{\left(\theta^2 b^2 - 2\theta b + 2\right)e^{\theta b} - \left(\theta^2 a^2 - 2\theta a + 2\right)e^{\theta a}}{\theta^3(b-a)}\right|_{\theta=0} = \left.\frac{\theta^2 b^3 e^{\theta b} - \theta^2 a^3 e^{\theta a}}{3\theta^2(b-a)}\right|_{\theta=0} \\ &= \frac{b^3 - a^3}{3(b-a)} = \frac{1}{3}\left(b^2 + ab + a^2\right). \end{aligned}$$

[13] need theorem

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \frac{1}{3}\left(b^2+ab+a^2\right) - \frac{1}{4}(b^2+2ab+a^2) = \frac{1}{12}(b-a)^2$. Also,

$$\begin{aligned}
\mathbb{E}X^3 &= \left.\frac{d^3M_X(\theta)}{d\theta^3}\right|_{\theta=0} = \left.\frac{\theta^3\left(\theta^2b^3e^{\theta b}-\theta^2a^3e^{\theta a}\right)-3\theta^2\left(\left(\theta^2b^2-2\theta b+2\right)e^{\theta b}-\left(\theta^2a^2-2\theta a+2\right)e^{\theta a}\right)}{\theta^6(b-a)}\right|_{\theta=0} \\
&= \left.\frac{\left(\theta^3b^3-3\theta^2b^2+6\theta b-6\right)e^{\theta b}-\left(\theta^3a^3-3\theta^2a^2+6\theta a-6\right)e^{\theta a}}{\theta^4(b-a)}\right|_{\theta=0} = \left.\frac{\theta^3b^4e^{\theta b}-\theta^3a^4e^{\theta a}}{4\theta^3(b-a)}\right|_{\theta=0} \\
&= \frac{b^4-a^4}{4(b-a)} = \frac{1}{4}\left(b^3+b^2a+ba^2+a^3\right).
\end{aligned}$$

Thus,

$$\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = \frac{1}{4}\left(b^3+b^2a+ba^2+a^3\right) - \frac{3}{2}(b+a)\frac{1}{3}\left(b^2+ab+a^2\right) + \frac{2}{8}(b+a)^3 = 0.$$

By Definition 19.5.5, $\operatorname{Skew}(X) = 0$. Furthermore,

$$\begin{aligned}
\mathbb{E}X^4 &= \left.\frac{d^4M_X(\theta)}{d\theta^4}\right|_{\theta=0} = \left.\frac{\theta^4\left(\theta^3b^4e^{\theta b}-\theta^3a^4e^{\theta a}\right)-4\theta^3\left(\left(\theta^3b^3-3\theta^2b^2+6\theta b-6\right)e^{\theta b}-\left(\theta^3a^3-3\theta^2a^2+6\theta a-6\right)e^{\theta a}\right)}{\theta^8(b-a)}\right|_{\theta=0} \\
&= \left.\frac{\left(\theta^4b^4-4\theta^3b^3+12\theta^2b^2-24\theta b+24\right)e^{\theta b}-\left(\theta^4a^4-4\theta^3a^3+12\theta^2a^2-24\theta a+24\right)e^{\theta a}}{\theta^5(b-a)}\right|_{\theta=0} \\
&= \left.\frac{\theta^4b^5e^{\theta b}-\theta^4a^5e^{\theta a}}{5\theta^4(b-a)}\right|_{\theta=0} = \frac{b^5-a^5}{5(b-a)} = \frac{1}{5}\left(b^4+b^3a+b^2a^2+ba^3+a^4\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
&\mathbb{E}\left(X-\mu\right)^4 = \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 \\
=\ & \frac{1}{5}\left(b^4+b^3a+b^2a^2+ba^3+a^4\right) - \frac{4}{2}(b+a)\frac{1}{4}\left(b^3+b^2a+ba^2+a^3\right) + \frac{6}{4}(b+a)^2\frac{1}{3}\left(b^2+ab+a^2\right) - \frac{4}{16}(b+a)^4 + \frac{1}{16}(b+a)^4 \\
=\ & \frac{1}{80}(b-a)^4
\end{aligned}$$

By Definition 19.5.6, we have $\operatorname{Kurt}(X) = \frac{(b-a)^4/80}{(b-a)^4/144} - 3 = -\frac{6}{5}$. □

In deed, we can have more general result.

Proposition 19.8.4. Suppose $X \sim \mathcal{U}(a,b)$. Then with $\mu = \frac{1}{2}(a+b)$, for $n \in \mathbb{N}$

$$\mathbb{E}X^n = \frac{b^{n+1}-a^{n+1}}{(n+1)(b-a)}, \qquad \mathbb{E}(X-\mu)^n = \begin{cases} \frac{(b-a)^n}{(n+1)2^n} & n \text{ is even} \\ 0 & n \text{ is odd} \end{cases}. \tag{19.8.10}$$

Proof. We know that $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$ with Taylor expansion. Thus, by Proposition 19.8.2, 19.5.10,

$$\begin{aligned}
\mathbb{E}X^n &= \left.\frac{d^nM_X(\theta)}{d\theta^n}\right|_{\theta=0} = \left.\left(\frac{d^n}{d\theta^n}\left(\frac{e^{\theta b}-e^{\theta a}}{\theta(b-a)}\right)\right)\right|_{\theta=0} = \frac{1}{b-a}\left.\left(\frac{d^n}{d\theta^n}\left(\sum_{n=0}^{\infty}\frac{(\theta b)^n-(\theta a)^n}{\theta n!}\right)\right)\right|_{\theta=0} \\
&= \frac{1}{b-a}\frac{n!(b^{n+1}-a^{n+1})}{(n+1)!} = \frac{b^{n+1}-a^{n+1}}{(n+1)(b-a)}.
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}(X-\mu)^n &= \sum_{k=0}^{n}C_n^k\mathbb{E}X^{n-k}(-\mu)^k = \sum_{k=0}^{n}\frac{n!}{(n-k)!k!}\frac{b^{n-k+1}-a^{n-k+1}}{(n-k+1)(b-a)}(-\mu)^k = \sum_{k=0}^{n}\frac{(n+1)!}{(n-k+1)!k!}\frac{b^{n-k+1}-a^{n-k+1}}{(n+1)(b-a)}(-\mu)^k \\
&= \frac{1}{(n+1)(b-a)}\left(\sum_{k=0}^{n}C_{n+1}^kb^{n-k+1}(-\mu)^k - \sum_{k=0}^{n}C_{n+1}^ka^{n-k+1}(-\mu)^k\right) \\
&= \frac{1}{(n+1)(b-a)}\left((b-\mu)^{n+1}-(-\mu)^{n+1}-(a-\mu)^{n+1}+(-\mu)^{n+1}\right) = \frac{1}{(n+1)(b-a)}\left((b-\mu)^{n+1}-(a-\mu)^{n+1}\right)
\end{aligned}$$

Since $\mu = \frac{1}{2}(a+b)$, then $\mathbb{E}(X-\mu)^n = 0$ if n is odd. If n is even,

$$\mathbb{E}(X-\mu)^n = \frac{1}{(n+1)(b-a)}\left(\left(\frac{b-a}{2}\right)^{n+1} - \left(-\frac{b-a}{2}\right)^{n+1}\right) = \frac{(b-a)^n}{(n+1)2^n}. \tag{19.8.11}$$

Thus, Proposition 19.8.3 can be derived easily. □

Proposition 19.8.5. Let $X_1, \ldots, X_n \overset{\text{i.i.d.}}{\sim} \mathcal{U}[0,1]$. Then define

$$Y := \max\{X_1, \ldots, X_n\}, \qquad Z := \min\{X_1, \ldots, X_n\}. \tag{19.8.12}$$

Then

$$\begin{aligned} M_Y(\theta) &= n!e^\theta\left(\frac{1}{\theta(n-1)!} - \frac{1}{\theta^2(n-2)!} + \cdots + \frac{(-1)^{n-1}}{\theta^n}\right) + \frac{(-1)^n n!}{\theta^n}, \\ M_Z(\theta) &= \frac{n!}{\theta^n}e^\theta - n!\left(\frac{1}{\theta(n-1)!} + \frac{1}{\theta^2(n-2)!} + \cdots + \frac{1}{\theta^n}\right) \end{aligned}$$

In particular,

$$\mathbb{E}Y^m = \frac{n}{n+m}, \qquad \mathbb{E}Z^m = \frac{n!m!}{(n+m)!}. \tag{19.8.13}$$

Also,

$$\mathrm{Cov}(Y,Z) = \frac{1}{(n+1)^2(n+2)}, \quad \mathrm{Corr}(Y,Z) = \frac{1}{n}. \tag{19.8.14}$$

Remark. That Y and Z have positive correlation make sense since when Z becomes large, Y tends to become large as well ($Y \geq Z$).

Proof. First, we have (as $X_1, \ldots, X_n$ are i.i.d.)

$$\begin{aligned} \mathbb{P}(Y \leq y) &= \mathbb{P}(\max\{X_1, \ldots, X_n\} \leq y) = \mathbb{P}(X_1 \leq y, \ldots, X_n \leq y) = \mathbb{P}(X_1 \leq y)\ldots\mathbb{P}(X_n \leq y) = y^n, \\ \mathbb{P}(Z \leq z) &= \mathbb{P}(\min\{X_1, \ldots, X_n\} \leq z) = 1 - \mathbb{P}(X_1 \geq z, \ldots, X_n \geq z) = 1 - \mathbb{P}(X_1 \geq z)\ldots\mathbb{P}(X_n \geq z) = 1 - (1-z)^n. \end{aligned}$$

Taking differentiation,

$$f_Y(y) = ny^{n-1}, \qquad f_Z(z) = n(1-z)^{n-1}. \tag{19.8.15}$$

Therefore, for $\theta \neq 0$. Let $I(n) = \int_0^1 e^{\theta y}y^n dy$ and thus $M_Y(\theta) = nI(n-1)$. Then $I(0) = \frac{1}{\theta}\left(e^\theta - 1\right)$ and

$$I(1) = \int_0^1 e^{\theta y}ydy = \frac{1}{\theta}\int_0^1 yde^{\theta y} = \frac{1}{\theta}\left(e^\theta - I(0)\right) = e^\theta\left(\frac{1}{\theta} - \frac{1}{\theta^2}\right) + \frac{1}{\theta^2} \tag{19.8.16}$$

$$\begin{aligned} I(n) &= \int_0^1 e^{\theta y}y^n dy = \frac{1}{\theta}\int_0^1 y^n de^{\theta y} = \frac{1}{\theta}\left(y^n e^{\theta y}\big|_0^1 - n\int_0^1 e^{\theta y}y^{n-1}dy\right) \\ &= \frac{1}{\theta}\left(e^\theta - n\int_0^1 e^{\theta y}y^{n-1}dy\right) = \frac{1}{\theta}\left(e^\theta - nI(n-1)\right). \end{aligned}$$

Let $J(n) := \theta^n I(n)/n!$. Then

$$J(n) = \frac{\theta^{n-1}e^\theta}{n!} - J(n-1). \tag{19.8.17}$$

Therefore,

$$\begin{aligned}
J(n) &= \frac{\theta^{n-1}e^{\theta}}{n!} - \frac{\theta^{n-2}e^{\theta}}{(n-1)!} + \cdots + (-1)^n J(0) \\
\theta^n I(n)/n! &= \frac{\theta^{n-1}e^{\theta}}{n!} - \frac{\theta^{n-2}e^{\theta}}{(n-1)!} + \cdots + (-1)^n I(0) = \frac{\theta^{n-1}e^{\theta}}{n!} - \frac{\theta^{n-2}e^{\theta}}{(n-1)!} + \cdots + (-1)^n \frac{1}{\theta}\left(e^{\theta}-1\right) \\
I(n) &= n!e^{\theta}\left(\frac{1}{\theta n!} - \frac{1}{\theta^2(n-1)!} + \cdots + \frac{(-1)^n}{\theta^{n+1}}\right) + \frac{(-1)^{n+1}n!}{\theta^{n+1}} \\
I(n) &= \frac{n!e^{\theta}}{\theta^{n+1}}\left(\frac{\theta^n}{n!} - \frac{\theta^{n-1}}{(n-1)!} + \cdots + (-1)^n\right) + \frac{(-1)^{n+1}n!}{\theta^{n+1}} \\
I(n) &= \frac{(-1)^n n!e^{\theta}}{\theta^{n+1}}\left(1 + \frac{(-\theta)}{1!} + \cdots + \frac{(-\theta)^{n-1}}{(n-1)!} + \frac{(-\theta)^n}{n!}\right) + \frac{(-1)^{n+1}n!}{\theta^{n+1}}
\end{aligned}$$

Therefore,

$$\begin{aligned}
M_Y(\theta) = nI(n-1) &= \frac{(-1)^{n-1}n!e^{\theta}}{\theta^n}\left(1 + \frac{(-\theta)}{1!} + \cdots + \frac{(-\theta)^{n-1}}{(n-1)!}\right) + \frac{(-1)^n n!}{\theta^n} \\
&= n!e^{\theta}\left(\frac{1}{\theta(n-1)!} - \frac{1}{\theta^2(n-2)!} + \cdots + \frac{(-1)^{n-1}}{\theta^n}\right) + \frac{(-1)^n n!}{\theta^n} \qquad (*)
\end{aligned}$$

Then taking differentiation of $(*)$,

$$\begin{aligned}
\frac{dM_Y(\theta)}{d\theta} &= n!e^{\theta}\left(\frac{1}{\theta(n-1)!} - \frac{1}{\theta^2(n-2)!} + \cdots + \frac{(-1)^{n-1}}{\theta^n} + \frac{-1}{\theta^2(n-1)!} + \cdots + \frac{(-1)^{n-1}(n-1)}{\theta^n} + \frac{(-1)^n n}{\theta^{n+1}}\right) + \frac{n(-1)^{n+1}n!}{\theta^{n+1}} \\
&= n!e^{\theta}\left(\frac{n}{\theta n!} - \frac{n}{\theta^2(n-1)!} + \cdots + \frac{n(-1)^{n-1}}{\theta^n 1!} + \frac{n(-1)^n}{\theta^{n+1}}\right) + \frac{n(-1)^{n+1}n!}{\theta^{n+1}} \qquad (**) \\
&= \frac{n(-1)^n n!e^{\theta}}{\theta^{n+1}}\left(1 + \frac{(-\theta)}{1!} + \frac{(-\theta)^2}{2!} + \cdots + \frac{(-\theta)^n}{n!}\right) + \frac{n(-1)^{n+1}n!}{\theta^{n+1}} \\
&= \frac{n(-1)^n n!e^{\theta}}{\theta^{n+1}}\left(e^{-\theta} - \frac{(-1)^{n+1}\theta^{n+1}}{(n+1)!} - \text{other following Taylor expansions}\right) + \frac{n(-1)^{n+1}n!}{\theta^{n+1}} \\
&= -n(-1)^n n!\frac{(-1)^{n+1}}{(n+1)!} + O(\theta) = \frac{n!n}{(n+1)!} + O(\theta) = \frac{n}{n+1} + O(\theta).
\end{aligned}$$

Letting $\theta = 0$, we have

$$\mathbb{E}Y = \left.\frac{dM_Y(\theta)}{d\theta}\right|_{\theta=0} = \frac{n}{n+1}. \tag{19.8.18}$$

Taking differentiation of $(**)$,

$$\begin{aligned}
\frac{d^2M_Y(\theta)}{d\theta^2} &= n!e^{\theta}n\left(\frac{1}{\theta n!} - \frac{1}{\theta^2(n-1)!} + \cdots + \frac{(-1)^{n-1}}{\theta^n 1!} + \frac{(-1)^n}{\theta^{n+1}} - \frac{1}{\theta^2 n!} + \frac{2}{\theta^3(n-1)!} - \cdots + \frac{n(-1)^n}{\theta^{n+1}1!} + \frac{(n+1)(-1)^{n+1}}{\theta^{n+2}}\right) \\
&\quad + \frac{n(n+1)(-1)^{n+2}n!}{\theta^{n+2}} \\
&= n!e^{\theta}n\left(\frac{n+1}{\theta(n+1)!} - \frac{n+1}{\theta^2 n!} + \cdots + \frac{(n+1)(-1)^n}{\theta^{n+1}1!} + \frac{(n+1)(-1)^{n+1}}{\theta^{n+2}}\right) + \frac{n(n+1)(-1)^{n+2}n!}{\theta^{n+2}} \\
&= \frac{n(n+1)(-1)^{n+1}n!e^{\theta}}{\theta^{n+2}}\left(1 + \frac{(-\theta)}{1!} + \frac{(-\theta)^2}{2!} + \cdots + \frac{(-\theta)^{n+1}}{(n+1)!}\right) + \frac{n(n+1)(-1)^{n+2}n!}{\theta^{n+2}} \\
&= \frac{n(n+1)(-1)^{n+1}n!e^{\theta}}{\theta^{n+2}}\left(e^{-\theta} - \frac{(-1)^{n+2}\theta^{n+2}}{(n+2)!} - \text{other following Taylor expansions}\right) + \frac{n(n+1)(-1)^{n+2}n!}{\theta^{n+2}} \\
&= -n(n+1)(-1)^{n+1}n!\frac{(-1)^{n+2}}{(n+2)!} + O(\theta) = \frac{n(n+1)n!}{(n+2)!} + O(\theta) = \frac{n}{n+2} + O(\theta).
\end{aligned}$$

Letting $\theta = 0$, we have

$$\mathbb{E}Y^2 = \left.\frac{d^2 M_Y(\theta)}{d\theta^2}\right|_{\theta=0} = \frac{n}{n+2} \;\Rightarrow\; \operatorname{Var} Y = \frac{n}{n+2} - \left(\frac{n}{n+1}\right)^2 = \frac{n}{(n+1)^2(n+2)}. \tag{19.8.19}$$

Similarly, we can see that

$$\mathbb{E}Y^m = \frac{n}{n+m} = \int_0^1 n x^{n+m-1} dx = \int_0^1 x^m n x^{n-1} dx. \tag{19.8.20}$$

For Z, we have

$$\begin{aligned} M_Z(\theta) = \mathbb{E}\left(e^{\theta Z}\right) &= \int_0^1 e^{\theta z} n(1-z)^{n-1} dz = \int_0^1 e^{\theta(1-z)} n z^{n-1} dz = e^{\theta}\int_0^1 e^{-\theta z} n z^{n-1} dz = e^{\theta} M_Y(-\theta) \\ &= n!\left(\frac{1}{(-\theta)(n-1)!} - \frac{1}{(-\theta)^2 (n-2)!} + \cdots + \frac{(-1)^{n-1}}{(-\theta)^n}\right) + \frac{(-1)^n n!}{(-\theta)^n} e^{\theta} \\ &= -n!\left(\frac{1}{\theta(n-1)!} + \frac{1}{\theta^2(n-2)!} + \cdots + \frac{1}{\theta^n}\right) + \frac{n!}{\theta^n} e^{\theta} \qquad (\dagger) \end{aligned}$$

Then taking differentiation of (†),

$$\begin{aligned} \frac{dM_Z(\theta)}{d\theta} &= n!\left(\frac{1}{\theta^2(n-1)!} + \frac{2}{\theta^3(n-2)!} + \cdots + \frac{n}{\theta^{n+1}}\right) + n! e^{\theta}\left(\frac{1}{\theta^n} - \frac{n}{\theta^{n+1}}\right) \\ &= \frac{n!}{\theta^{n+1}}\left(\frac{\theta^{n-1}}{(n-1)!} + \frac{2\theta^{n-2}}{(n-2)!} + \cdots + n\right) \\ &\qquad + n!\left(1 + \theta + \frac{\theta^2}{2} + \cdots + \frac{\theta^n}{n!} + \frac{\theta^{n+1}}{(n+1)!} + \text{other following Taylor expansions}\right)\frac{\theta - n}{\theta^{n+1}} \\ &= \frac{n!}{\theta^{n+1}}\left(\frac{\theta^{n-1}}{(n-1)!} + \frac{2\theta^{n-2}}{(n-2)!} + \cdots + n + \theta + \theta^2 + \frac{\theta^3}{2} + \cdots + \frac{\theta^{n+1}}{n!} - n - n\theta - \frac{n\theta^2}{2} - \cdots - \frac{n\theta^{n+1}}{(n+1)!} + O(\theta^{n+2})\right) \\ &= \frac{n!}{\theta^{n+1}}\left(\frac{\theta^n}{(n-1)!} + \frac{\theta^{n+1}}{n!} - \frac{n\theta^n}{n!} - \frac{n\theta^{n+1}}{(n+1)!} + O(\theta^{n+2})\right) = \frac{1}{n+1} + O(\theta). \end{aligned}$$

Letting $\theta = 0$, we have

$$\mathbb{E}Z = \left.\frac{dM_Z(\theta)}{d\theta}\right|_{\theta=0} = \frac{1}{n+1}. \tag{19.8.21}$$

Similarly, by Proposition 4.6.1

$$\mathbb{E}Z^m = \int_0^1 z^m n(1-z)^{n-1} dz = n\int_0^1 z^m (1-z)^{n-1} dz = n\frac{\Gamma(m+1)\Gamma(n)}{\Gamma(m+n+1)} = \frac{m!n!}{(m+n)!}. \tag{19.8.22}$$

In particular, $\operatorname{Var} Z = \frac{n!2}{(n+2)!} - \left(\frac{1}{n+1}\right)^2 = \frac{2(n+1)-(n+2)}{(n+1)^2(n+2)} = \frac{n}{(n+1)^2(n+2)}$.

Second, we have for $z \le y$,

$$\mathbb{P}(Y \le y, Z \ge z) = \mathbb{P}(z \le X_1 \le y, \ldots, z \le X_n \ge y) = \mathbb{P}(z \le X_1 \le y)\ldots\mathbb{P}(z \le X_n \le y) = (y-z)^n \tag{19.8.23}$$

and

$$\mathbb{P}(Y \le y, Z \le z) = \mathbb{P}(Y \le y) - \mathbb{P}(Y \le y, Z \ge z) = y^n - (y-z)^n \tag{19.8.24}$$

Thus,

$$f_{Y,Z}(y,z) = \frac{\partial^2 (y^n - (y-z)^n)}{\partial y \partial z} = n(n-1)(y-z)^{n-2}. \tag{19.8.25}$$

Thus, by Definition 4.6.1 and Proposition 4.6.1

$$\begin{aligned}
\mathbb{E}(YZ) &= \int_0^1\int_z^1 yzn(n-1)(y-z)^{n-2}dydz = \int_0^1\int_z^1 (y-z+z)zn(n-1)(y-z)^{n-2}dydz \\
&= \int_0^1\int_z^1 n(n-1)(y-z)^{n-1}zdydz + \int_0^1\int_z^1 n(n-1)(y-z)^{n-2}z^2dydz \\
&= \int_0^1 (n-1)(1-z)^n zdz + \int_0^1 n(1-z)^{n-1}z^2dz = (n-1)\int_0^1 (1-z)^{n-1}zdz + \int_0^1 (1-z)^{n-1}z^2dz \\
&= (n-1)B(n,2) + B(n,3) = (n-1)\frac{\Gamma(n)\Gamma(2)}{\Gamma(n+2)} + \frac{\Gamma(n)\Gamma(3)}{\Gamma(n+3)} \\
&= \frac{(n-1)(n-1)!}{(n+1)!} + \frac{(n-1)!2!}{(n+2)!} = \frac{(n-1)}{n(n+1)} + \frac{2}{n(n+1)(n+2)} = \frac{(n-1)(n+2)+2}{n(n+1)(n+2)} = \frac{1}{n+2}.
\end{aligned}$$

Thus,

$$\mathrm{Cov}(Y,Z) = \mathbb{E}(YZ) - \mathbb{E}Y\mathbb{E}Z = \frac{1}{n+2} - \frac{1}{n+1}\frac{n}{n+1} = \frac{1}{(n+1)^2(n+2)}. \tag{19.8.26}$$

Thus

$$\mathrm{Corr}(Y,Z) = \frac{\mathrm{Cov}(Y,Z)}{\sqrt{\mathrm{Var}\,Y\,\mathrm{Var}\,Z}} = \frac{\frac{1}{(n+1)^2(n+2)}}{\frac{n}{(n+1)^2(n+2)}} = \frac{1}{n}. \tag{19.8.27}$$

□

19.8.3 Exponential random variables

Definition 19.8.5 (exponential random variable)**.** A random variable X in $\mathbb{R}$ is exponential distributed if, for some $\lambda > 0, \lambda \in \mathbb{R}$, X has density function

$$f_X(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0, \\ 0, & x < 0. \end{cases} \tag{19.8.28}$$

We write $X \sim \mathcal{E}(\lambda)$. The cumulative distribution function of exponential distribution is given by

$$F(x) = \begin{cases} 1 - e^{-\lambda x}, & x \geq 0, \\ 0, & x < 0. \end{cases} \tag{19.8.29}$$

Proposition 19.8.6. Suppose $X \sim \mathcal{E}(\lambda)$. Then for $\theta < \lambda$ and $t \in \mathbb{R}$,

$$M_X(\theta) = \frac{\lambda}{\lambda - \theta}, \qquad \phi_X(t) = \frac{\lambda}{\lambda - it}. \tag{19.8.30}$$

Proof. From Definition 19.5.4,

$$M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right) = \int_0^\infty \lambda e^{\theta x}e^{-\lambda x}dx = \frac{\lambda}{\theta - \lambda}\int_0^\infty de^{(\theta-\lambda)x} = \frac{\lambda}{\lambda - \theta}. \tag{19.8.31}$$

$$\phi_X(t) = \mathbb{E}\left(e^{itX}\right) = \int_0^\infty \lambda e^{itx}e^{-\lambda x}dx = \int_0^\infty \lambda e^{-\lambda x}\left(\cos tx + i\sin tx\right)dx. \tag{19.8.32}$$

Therefore,

$$\begin{aligned}
I = \int_0^\infty \lambda e^{-\lambda x}\left(\cos tx\right)dx &= -\left(e^{-\lambda x}\cos tx\big|_0^\infty + t\int_0^\infty e^{-\lambda x}\sin txdx\right) = -\left(-1 - \frac{t}{\lambda}\int_0^\infty \sin txde^{-\lambda x}\right) \\
&= -\left(-1 - \frac{t}{\lambda}\left(\sin txde^{-\lambda x}\big|_0^\infty - t\int_0^\infty e^{-\lambda x}\cos txdx\right)\right) = 1 - \frac{t^2}{\lambda^2}I.
\end{aligned}$$

Thus, $\lambda^2 I = \lambda^2 - t^2 I \Rightarrow I = \frac{\lambda^2}{\lambda^2+t^2}$. Similarly,

$$\begin{aligned} J = \int_0^\infty \lambda e^{-\lambda x} (\sin tx)\, dx &= -\left(e^{-\lambda x} \sin tx \Big|_0^\infty - t \int_0^\infty e^{-\lambda x} \cos tx dx \right) = -\left(\frac{t}{\lambda} \int_0^\infty \cos tx de^{-\lambda x} \right) \\ &= -\left(\frac{t}{\lambda} \left(\cos tx de^{-\lambda x} \Big|_0^\infty + t \int_0^\infty e^{-\lambda x} \sin tx dx \right) \right) = \frac{t}{\lambda} \left(1 - \frac{t}{\lambda} J \right). \end{aligned}$$

Thus, $\lambda^2 J = \lambda t - t^2 J \Rightarrow J = \frac{\lambda t}{\lambda^2+t^2}$. Thus,

$$\phi_X(t) = \frac{\lambda^2}{\lambda + t^2} + \frac{i\lambda t}{\lambda + t^2} = \frac{\lambda^2(\lambda + it)}{\lambda^2 + t^2} = \frac{\lambda}{\lambda - it}. \tag{19.8.33}$$

□

Proposition 19.8.7. Suppose $X \sim \mathcal{E}(\lambda)$. Then

$$\text{(i) } \mathbb{E}X = \frac{1}{\lambda}, \qquad \text{(ii) } \operatorname{Var} X = \frac{1}{\lambda^2}, \qquad \text{(iii) } \operatorname{Skew}(X) = 2, \qquad \text{(iv) } \operatorname{Kurt}(X) = 6, \qquad \text{(v)} \mathbb{E}X^n = \frac{n!}{\lambda^n}. \tag{19.8.34}$$

Proof. With Propositions 19.8.6, 19.5.10,

$$\mathbb{E}X = \left. \frac{dM_X(\theta)}{d\theta} \right|_{\theta=0} = \left. \frac{\lambda}{(\lambda-\theta)^2} \right|_{\theta=0} = \frac{\lambda}{\lambda^2} = \frac{1}{\lambda}, \qquad \mathbb{E}X^2 = \left. \frac{d^2 M_X(\theta)}{d\theta^2} \right|_{\theta=0} = \left. \frac{2\lambda}{(\lambda-\theta)^3} \right|_{\theta=0} = \frac{2}{\lambda^2}.$$

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \frac{2}{\lambda^2} - \frac{1}{\lambda^2} = \frac{1}{\lambda^2}$. Also,

$$\mathbb{E}X^3 = \left. \frac{d^3 M_X(\theta)}{d\theta^3} \right|_{\theta=0} = \left. \frac{6\lambda}{(\lambda-\theta)^4} \right|_{\theta=0} = \frac{6}{\lambda^3}. \tag{19.8.35}$$

Thus,

$$\mathbb{E}(X-\mu)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = \frac{6}{\lambda^3} - 3\frac{1}{\lambda}\frac{2}{\lambda^2} + 3\frac{1}{\lambda^2}\frac{1}{\lambda^2} - \frac{1}{\lambda^3} = \frac{2}{\lambda^3}. \tag{19.8.36}$$

By Definition 19.5.5, $\operatorname{Skew}(X) = \frac{2/\lambda^3}{1/\lambda^3} = 2$. Furthermore,

$$\mathbb{E}X^4 = \left. \frac{d^4 M_X(\theta)}{d\theta^4} \right|_{\theta=0} = \left. \frac{24\lambda}{(\lambda-\theta)^5} \right|_{\theta=0} = \frac{24}{\lambda^4}. \tag{19.8.37}$$

Thus,

$$\mathbb{E}(X-\mu)^4 = \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 = \frac{24}{\lambda^4} - 4\frac{1}{\lambda}\frac{6}{\lambda^3} + 6\frac{1}{\lambda^2}\frac{2}{\lambda^2} - 4\frac{1}{\lambda^3}\frac{1}{\lambda} + \frac{1}{\lambda^4} = \frac{9}{\lambda^4}. \tag{19.8.38}$$

By Definition 19.5.6, we have $\operatorname{Kurt}(X) = \frac{9/\lambda^4}{1/\lambda^4} - 3 = 6$.
For (v), we know that $\frac{d^n M_X(\theta)}{d\theta^n} = \lambda n!/(\lambda-\theta)^{n+1}$,

$$\mathbb{E}X^n = \left. \frac{d^n M_X(\theta)}{d\theta^n} \right|_{\theta=0} = \frac{\lambda n!}{\lambda^{n+1}} = \frac{n!}{\lambda^n}. \tag{19.8.39}$$

□

The exponential distribution is sometimes used to model the lifetime of a component.

Proposition 19.8.8 (memoryless property of the exponential distribution)**.** Let $X \sim \mathcal{E}(\lambda)$. Then for $x > 0$ and $y > 0$,

$$\mathbb{P}(X > x + y | X > y) = e^{-\lambda x}. \tag{19.8.40}$$

Remark. So that, given the component has survived a length of time y the probability that it will survive a further time x is the same as if it has just been installed. This property, which is crucial to the study of stochastic processes, is known as the lack of memory property of the exponential distribution.

Proof. We have that

$$\mathbb{P}(X > x+y | X > y) = \frac{\mathbb{P}(X > x+y, X > y)}{\mathbb{P}(X > y)} = \frac{\mathbb{P}(X > x+y)}{\mathbb{P}(X > y)} = \frac{e^{-\lambda(x+y)}}{e^{-\lambda y}} = e^{-\lambda x}, \tag{19.8.41}$$

as required. □

Proposition 19.8.9 (minimum of independent exponentials is exponential)**.** Suppose that $X_i \sim \mathcal{E}(\lambda_i)$, $i = 1, \ldots, n$ are independent. Then $\min(X_1, \ldots, X_n) \sim \mathcal{E}(\sum_i \lambda_i)$.

Proof. Using the independence, we see that for $x \geq 0$,

$$\begin{aligned} \mathbb{P}\left(\min_i X_i \leq x\right) &= 1 - \mathbb{P}\left(\min_i X_i > x\right) = 1 - \mathbb{P}(X_1 > x, \ldots, X_n > x) \\ &= 1 - \prod_{i=1}^{n} \mathbb{P}(X_i > x) = 1 - \prod_{i=1}^{n} e^{-\lambda_i x} = 1 - e^{-x\sum_i \lambda_i}, \end{aligned}$$

so that $\min(X_1, \ldots, X_n) \sim \mathcal{E}(\sum_i \lambda_i)$. □

Proposition 19.8.10. Let $X_1, X_2, \cdots \overset{\text{i.i.d.}}{\sim} \mathcal{E}(\lambda)$ and $Y = \max\{n : X_1 + X_2 + \cdots + X_n \leq 1\}$. Then $Y \sim \text{Poi}(\lambda)$.

Proof. We define $Z = X_1 + \cdots + X_n \sim \Gamma(n, \lambda)$. Then

$$\begin{aligned} \mathbb{P}(Y = n) &= \mathbb{P}(X_1 + \cdots + X_n \leq 1, X_1 + \cdots + X_n + X_{n+1} > 1) = \mathbb{P}(Z \leq 1, Z + X_{n+1} > 1) \\ &= \int_0^1 \mathbb{P}(X > 1 - z) f_Z(z) dz = \int_0^1 e^{-\lambda(1-z)} \frac{\lambda^n}{e^{-\lambda z} z^{n-1}} (n-1)! dz \\ &= \int_0^1 \frac{\lambda^n}{e^{-\lambda} z^{n-1}} (n-1)! dz = \frac{\lambda^n e^{-\lambda}}{n!} \end{aligned}$$

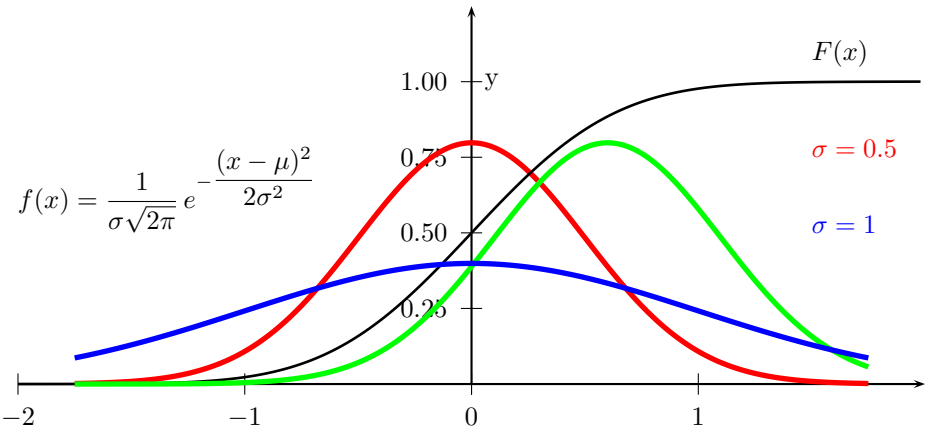
as required. □

19.8.4 Gaussian random variables

Definition 19.8.6 (Gaussian random variable)**.** A random variable X in $\mathbb{R}$ is Gaussian distributed if, for some $\mu \in \mathbb{R}$ and some $\sigma^2 \in (0, \infty)$, X has density function

$$f_X(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(x-\mu)^2/2\sigma^2}. \tag{19.8.42}$$

We also admit as Gaussian any random variable X with $X = \mu$ a.s., this degenerate case corresponding to taking $\sigma^2 = 0$. We write $X \sim \mathcal{N}(\mu, \sigma^2)$.



Proposition 19.8.11. Suppose $X \sim \mathcal{N}(\mu, \sigma^2)$. Then $M_X(\theta) = e^{\mu\theta + \sigma^2\theta^2/2}$.

Proof. From Definition 19.5.4, we have

$$\begin{aligned} M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right) &= \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} e^{\theta x} e^{-\frac{(x-\mu)^2}{2\sigma^2}}\,dx = \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} e^{-\frac{x^2-2\mu x+\mu^2}{2\sigma^2}} e^{\frac{2\sigma^2\theta x}{2\sigma^2}}\,dx \\ &= \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} e^{-\frac{x^2-2(\sigma^2\theta+\mu)x+\mu^2}{2\sigma^2}}\,dx = \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} e^{-\frac{(x-\sigma^2\theta-\mu)^2+\mu^2-(\sigma^2\theta+\mu)^2}{2\sigma^2}}\,dx \\ &= e^{-\frac{\mu^2-(\sigma^2\theta+\mu)^2}{2\sigma^2}}\frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} e^{-\frac{(x-\sigma^2-\mu)^2}{2\sigma^2}}\,dx = e^{\frac{(\sigma^2\theta+\mu)^2}{2\sigma^2}-\mu^2} = e^{\mu\theta+\sigma^2\theta^2/2}. \end{aligned}$$

□

Proposition 19.8.12. Suppose $X \sim \mathcal{N}(\mu, \sigma^2)$. Then

$$\text{(i) } \mathbb{E}X = \mu, \qquad \text{(ii) } \operatorname{Var} X = \sigma^2, \qquad \text{(iii) } \operatorname{Skew}(X) = 0, \qquad \text{(iv) } \operatorname{Kurt}(X) = 0. \tag{19.8.43}$$

Proof. With Propositions 19.8.11, 19.5.10,

$$\mathbb{E}X = \left.\frac{dM_X(\theta)}{d\theta}\right|_{\theta=0} = \left.\left(\mu+\sigma^2\theta\right)e^{\mu\theta+\sigma^2\theta^2/2}\right|_{\theta=0} = \mu. \tag{19.8.44}$$

$$\mathbb{E}X^2 = \left.\frac{d^2M_X(\theta)}{d\theta^2}\right|_{\theta=0} = \left.\left(\left(\mu+\sigma^2\theta\right)^2+\sigma^2\right)e^{\mu\theta+\sigma^2\theta^2/2}\right|_{\theta=0} = \mu^2+\sigma^2. \tag{19.8.45}$$

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \mu^2+\sigma^2-\mu^2 = \sigma^2$. Also,

$$\mathbb{E}X^3 = \left.\frac{d^3M_X(\theta)}{d\theta^3}\right|_{\theta=0} = \left.\left(\left(\mu+\sigma^2\theta\right)^3+3\sigma^2\left(\mu+\sigma^2\theta\right)\right)e^{\mu\theta+\sigma^2\theta^2/2}\right|_{\theta=0} = \mu^3+3\mu\sigma^2. \tag{19.8.46}$$

Thus,

$$\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = \mu^3+3\mu\sigma^2-3\mu\left(\mu^2+\sigma^2\right)+3\mu^3-\mu^3 = 0. \tag{19.8.47}$$

By Definition 19.5.5, $\operatorname{Skew}(X) = 0$. Furthermore,

$$\mathbb{E}X^4 = \left.\frac{d^4M_X(\theta)}{d\theta^4}\right|_{\theta=0} = \left.\left(\left(\mu+\sigma^2\theta\right)^4+6\sigma^2\left(\mu+\sigma^2\theta\right)^2+3\sigma^4\right)e^{\mu\theta+\sigma^2\theta^2/2}\right|_{\theta=0} = \mu^4+6\mu^2\sigma^2+3\sigma^4. \tag{19.8.48}$$

Thus,

$$\begin{aligned} \mathbb{E}\left(X-\mu\right)^4 &= \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 \\ &= \mu^4+6\mu^2\sigma^2+3\sigma^4-4\mu\left(\mu^3+3\mu\sigma^2\right)+6\mu^2\left(\mu^2+\sigma^2\right)-3\mu^4 = 3\sigma^4. \end{aligned}$$

By Definition 19.5.6, we have $\operatorname{Kurt}(X) = \frac{3\sigma^4}{\sigma^4} - 3 = 0$. □

Proposition 19.8.13. Let k be a positive integer and let $X \sim \mathcal{N}(0,1)$. Then

$$\mathbb{E}X^k = \begin{cases} 0 & k \text{ is odd} \\ \frac{(2k)!}{2^k k!} & k \text{ is even} \end{cases} \tag{19.8.49}$$

Proof. We have

$$\mathbb{E}X^k = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} x^k e^{-x^2/2}dx \tag{19.8.50}$$

If k is odd, then $\mathbb{E}X^k = 0$. If k is even,

$$\begin{aligned} \mathbb{E}X^k &= \left[\frac{1}{\sqrt{2\pi}}\left(-x^{k-1}\right)e^{-x^2/2}\right]_{-\infty}^{\infty} + \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}(k-1)x^{k-2}e^{-x^2/2}dx \\ &= (k-1)\mathbb{E}(X^{k-2}) = (k-1)(k-3)\cdots\mathbb{E}(X^0) = \frac{(2k)!}{2^k k!} \end{aligned}$$

□

Proposition 19.8.14. Suppose $X \sim \mathcal{N}(\mu, \sigma^2)$ and $a, b \in \mathbb{R}$. Then

$$\text{(i) } aX + b \sim \mathcal{N}(a\mu + b, a^2\sigma^2), \qquad \text{(ii) } \phi_X(u) = e^{iu\mu - u^2\sigma^2/2}. \tag{19.8.51}$$

Proof. For (i), note that

$$F_{aX+b}(x) = \mathbb{P}(aX + b \le x) = \mathbb{P}\left(X \le \frac{x-b}{a}\right) = F_X\left(\frac{x-b}{a}\right)$$

so

$$f_{aX+b}(x) = \frac{d}{dx}F_{aX+b}(x) = \frac{1}{a}f_X\left(\frac{x-b}{a}\right) = \frac{1}{\sqrt{2\pi(a\sigma)^2}}\exp\left(-\frac{(x-(a+b\mu))^2}{2(a\sigma)^2}\right).$$

Thus $aX + b \sim \mathcal{N}(a\mu + b, a\sigma)$.

For part (ii), note that from (i), we have that if $Z \sim \mathcal{N}(0,1)$, then X and $\mu + \sigma Z$ have the same distribution. Thus

$$\mathbb{E}(e^{iuX}) = e^{iu\mu}\mathbb{E}(e^{iu\sigma Z}) = e^{iu\mu}\phi_Z(u\sigma) = e^{iu\mu - u^2\sigma^2/2}.$$ □

Proposition 19.8.15. Suppose $X \sim \mathcal{N}\left(\mu, \sigma^2\right)$, Then

$$\mathbb{E}\,|X| = \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \mu\left(2\Phi\left(\frac{\mu}{\sigma}\right) - 1\right), \qquad \text{where} \quad \Phi(x) = \int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right)dx. \tag{19.8.52}$$

Proof. We know the density function is $\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$, thus

$$\begin{aligned}
\mathbb{E}\,|X| &= \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty}|x|\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)dx = \frac{1}{\sqrt{2\pi}\sigma}\left(\int_0^\infty x\exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right)dx + \int_0^\infty x\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)dx\right)\\
&= \frac{1}{\sqrt{2\pi}\sigma}\left(\int_0^\infty (x+\mu)\exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right)dx + \int_0^\infty (x-\mu)\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)dx\right.\\
&\qquad \left. +\mu\int_0^\infty\left(\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) - \exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right)\right)dx\right)
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathbb{E}\,|X| &= \frac{\sigma}{\sqrt{2\pi}}\left(-\exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right) - \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)\right)\Big|_0^\infty + \frac{\mu}{\sqrt{2\pi}\sigma}\int_0^\infty\left(\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) - \exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right)\right)dx\\
&= \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \frac{\mu}{\sqrt{2\pi}\sigma}\int_0^\infty\left(\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) - \exp\left(-\frac{(x+\mu)^2}{2\sigma^2}\right)\right)dx\\
&= \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \frac{\mu}{\sqrt{2\pi}\sigma}\left(\int_{-\mu}^\infty\exp\left(-\frac{x^2}{2\sigma^2}\right)dx - \int_{\mu}^\infty\exp\left(-\frac{x^2}{2\sigma^2}\right)dx\right)\\
&= \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \frac{\mu}{\sqrt{2\pi}}\left(\int_{-\frac{\mu}{\sigma}}^\infty\exp\left(-\frac{x^2}{2}\right)dx - \int_{\frac{\mu}{\sigma}}^\infty\exp\left(-\frac{x^2}{2}\right)dx\right)\\
&= \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \mu\left(\Phi\left(\frac{\mu}{\sigma}\right) - \Phi\left(-\frac{\mu}{\sigma}\right)\right) = \sqrt{\frac{2}{\pi}}\sigma\exp\left(-\frac{\mu^2}{2\sigma^2}\right) + \mu\left(2\Phi\left(\frac{\mu}{\sigma}\right) - 1\right)
\end{aligned}$$

as required. □

Proposition 19.8.16. Let X be a standard Gaussian random variable. Then for any $x \in \mathbb{R}\setminus\{0\}$,

$$\frac{x^{-1} - x^{-3}}{\sqrt{2\pi}}e^{-x^2/2} \le \mathbb{P}\left(X > x\right) \le \frac{x^{-1}}{\sqrt{2\pi}}e^{-x^2/2} \tag{19.8.53}$$

Proof. It is equivalent to prove that

$$\left(x^{-1} - x^{-3}\right)e^{-x^2/2} \le \int_x^\infty e^{-t^2/2}dt \le x^{-1}e^{-x^2/2}. \tag{19.8.54}$$

First, we have

$$\begin{aligned}\int_x^\infty e^{-t^2/2}dt &= \int_x^\infty e^{-x^2/2}e^{-(t-x)^2/2}e^{-(t-x)x}dt = e^{-x^2/2}\int_0^\infty e^{-t^2/2-tx}dt = x^{-1}e^{-x^2/2}\int_0^\infty -e^{-t^2/2}de^{-tx} \\ &= x^{-1}e^{-x^2/2}\left(-e^{-t^2/2}e^{-tx}\Big|_0^\infty - \int_0^\infty e^{-tx}e^{-t^2/2}tdt\right) = x^{-1}e^{-x^2/2}\left(1-\int_0^\infty te^{-tx}e^{-t^2/2}dt\right) \geq x^{-1}e^{-x^2/2} \qquad (*)\end{aligned}$$

as the integrand is positive. If we do the integral by parts again, then the second part of the above equation is

$$\begin{aligned}x^{-1}e^{-x^2/2}\int_0^\infty te^{-tx}e^{-t^2/2}dt &= x^{-2}e^{-x^2/2}\int_0^\infty -te^{-t^2/2}de^{-tx} = x^{-2}e^{-x^2/2}\left(-te^{-t^2/2}e^{-tx}\Big|_0^\infty + \int_0^\infty e^{-tx}d\left(te^{-t^2/2}\right)\right) \\ &= x^{-2}e^{-x^2/2}\left(-te^{-t^2/2}e^{-tx}\Big|_0^\infty + \int_0^\infty e^{-tx}d\left(te^{-t^2/2}\right)\right) \\ &= x^{-2}e^{-x^2/2}\left(0-\int_0^\infty t^2e^{-tx}e^{-t^2/2}dt + \int_0^\infty e^{-tx}e^{-t^2/2}dt\right) \\ &= -x^{-3}e^{-x^2/2}\int_0^\infty e^{-t^2/2}de^{-tx} - x^{-2}e^{-x^2/2}\int_0^\infty t^2e^{-tx}e^{-t^2/2}dt \\ &= x^{-3}e^{-x^2/2}\left(-e^{-t^2/2}e^{-tx}\Big|_0^\infty - \int_0^\infty te^{-tx}e^{-t^2/2}dt\right) - x^{-2}e^{-x^2/2}\int_0^\infty t^2e^{-tx}e^{-t^2/2}dt \\ &= x^{-3}e^{-x^2/2} - x^{-3}e^{-x^2/2}\int_0^\infty te^{-tx}e^{-t^2/2}dt - x^{-2}e^{-x^2/2}\int_0^\infty t^2e^{-tx}e^{-t^2/2}dt \\ &\leq x^{-3}e^{-x^2/2}\end{aligned}$$

as the integrands are positive. Thus, we have

$$\int_x^\infty e^{-t^2/2}dt \geq \left(x^{-1}-x^{-3}\right)e^{-x^2/2}. \qquad (\dagger) \tag{19.8.55}$$

Combining $(*)$ and $(\dagger)$, we have the required result. □

Proposition 19.8.17. Let $(X_n)_{n\in\mathbb{N}}$ be a sequence of Gaussian random variables with bounded means $(\mu_n)_{n\in\mathbb{N}}$ and variances $(\sigma_n^2)_{n\in\mathbb{N}}$. If $X_n \xrightarrow{d} X$. Then X is also a Gaussian random variable.

Proof. Since $(\mu_n)_{n\in\mathbb{N}}$ and $(\sigma_n^2)_{n\in\mathbb{N}}$ are bounded, we can apply Bolzano-Weierstrass theorem 10.2.36 to pick converging subsequence of n_k such that (μ_{n_k}) and $(\sigma_{n_k}^2)$ are converging to μ and σ^2.

By Lévy convergence theorem (Theorem 19.6.13), we have characteristic functions $\phi_{X_n}(t) \to \phi_X(t)$. Then we have

$$\left|\phi_{X_{n_k}}(t)\right| \to |\phi(t)| \;\Rightarrow\; \left|e^{i\mu_{n_k}t-\sigma_{n_k}^2t^2/2}\right| = \left|e^{-\sigma_{n_k}^2t^2/2}\right| \to |\phi(t)|\,. \tag{19.8.56}$$

Thus, $e^{-\sigma^2t^2/2} = |\phi(t)|$ and therefore, $e^{-\sigma^2/2} = |\phi(1)|$. Hence, σ^2 is uniquely determined. Then

$$e^{i\mu_{n_k}t-\sigma_{n_k}^2t^2/2} \to \phi_X(t) \;\Rightarrow\; e^{i\mu t} = \phi_X(t)e^{\sigma^2t^2/2},\ \forall t\in\mathbb{R}. \tag{19.8.57}$$

Thus, μ is also uniquely determined. Thus, we have that $\phi_X(t) = e^{i\mu t-\sigma^2t^2/2}$ and X is a Gaussian. □

Definition 19.8.7 (multivariate Gaussian random variables)**.** A random variable $X = (X_1,\ldots,X_n)$ in $\mathbb{R}^n$ is Gaussian if $\langle u, X\rangle$ is Gaussian, for all $u \in \mathbb{R}^n$ and $X_1,\ldots,X_n$ are multivariate Gaussian random variables. That is, any linear combination of multivariate Gaussian random variables is still a Gassian random variable.

Example 19.8.18. An example of such a random variable is provided by $X = (X_1,\ldots,X_n)$, where $X_1,\ldots,X_n$ are independent $\mathcal{N}(0,1)$ random variables. To see this, we note that

$$\mathbb{E}e^{i\langle u,X\rangle} = \mathbb{E}\prod_k e^{iu_kX_k} = e^{-|u|^2/2} \tag{19.8.58}$$

so $\langle u, X\rangle$ is $\mathcal{N}(0,|u|^2)$ for all $u \in \mathbb{R}^n$.

Example 19.8.19 (bivariate Gaussian random variables)**.** In the 2-dimensional nonsingular case ($k = \mathrm{r}(\Sigma) = 2$), the

probability density function of a vector $[X, Y]^T$ is

$$f(x,y) = \frac{1}{2\pi\sigma_x\sigma_y\sqrt{1-\rho^2}} \exp\left(-\frac{1}{2(1-\rho^2)}\left[\frac{(x-\mu_x)^2}{\sigma_x^2} + \frac{(y-\mu_y)^2}{\sigma_y^2} - \frac{2\rho(x-\mu_x)(y-\mu_y)}{\sigma_x\sigma_y}\right]\right), \tag{19.8.59}$$

where ρ is the correlation between X and Y and where $\sigma_x > 0$ and $\sigma_y > 0$. In this case,

$$\mu = \begin{pmatrix}\mu_x \\ \mu_y\end{pmatrix}, \quad \Sigma = \begin{pmatrix}\sigma_x^2 & \rho\sigma_x\sigma_y \\ \rho\sigma_x\sigma_y & \sigma_y^2\end{pmatrix}. \tag{19.8.60}$$

Theorem 19.8.20. Let $X = (X_1, \ldots, X_n)$ be a Gaussian random variable in $\mathbb{R}^n$ with mean μ and variance Σ, i.e., $X_1, \ldots, X_n$ are multivariate Gaussian random variables. Then

(i) $AX + b$ is a Gaussian random variable in $\mathbb{R}^m$, for all $m \times n$ matrices A and all $b \in \mathbb{R}^m$. That is, $AX + b \sim \mathcal{N}(A\mu + b, A\Sigma A^T)$[14].

(ii) $X \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ and its distribution is determined by its mean μ and its covariance matrix V.

(iii) $\phi_X(u) = e^{i\langle u,\mu\rangle - \langle u,\Sigma u\rangle/2}$, $M_X(\theta) = e^{\langle\theta,\mu\rangle + \langle\theta,\Sigma\theta\rangle/2}$.

(iv) if V is invertible, then X has a density function on $\mathbb{R}^n$, given by

$$f_X(x) = (2\pi)^{-n/2}(\det\Sigma)^{-1/2}\exp\left(-\left\langle x-\mu, \Sigma^{-1}(x-\mu)\right\rangle/2\right). \tag{19.8.61}$$

(v) suppose $X = (X_1, X_2)$, with X_1 in $\mathbb{R}^{n_1}$ and X_2 in $\mathbb{R}^{n_2}$, then

$$\mathrm{Cov}(X_1, X_2) = 0 \quad \Rightarrow \quad X_1,\ X_2 \text{ are independent.} \tag{19.8.62}$$

Remark. Note that (v) is only true for multivariate Gaussian random variables.

Proof. For $u \in \mathbb{R}^n$, we have $\langle u, AX + b\rangle = \left\langle A^T u, X\right\rangle + \langle u, b\rangle$ so $\langle u, AX + b\rangle$ is Gaussian, by Proposition 19.8.14. This proves (i).

Each component X_k is Gaussian, so $X \in \mathcal{L}^2$. Set $\mu = \mathbb{E}(X)$ and $\Sigma = \mathrm{Var}(X)$. For $u \in \mathbb{R}^n$ we have $\mathbb{E}(\langle u, X\rangle) = \langle u, \mu\rangle$ and

$$\mathrm{Var}(\langle u, X\rangle) = \mathrm{Cov}(\langle u, X\rangle, \langle u, X\rangle) = \langle u, \Sigma u\rangle. \tag{19.8.63}$$

Since $\langle u, X\rangle$ is Gaussian, by Proposition 19.8.14, we must have

$$\langle u, X\rangle \sim \mathcal{N}(\langle u, \mu\rangle, \langle u, \Sigma u\rangle), \qquad \phi_X(u) = \mathbb{E}e^{i\langle u,X\rangle} = e^{i\langle u,\mu\rangle - \langle u,\Sigma u\rangle/2}. \tag{19.8.64}$$

This is (iii) and (ii) follows by uniqueness of characteristic functions. Similarly, we get the moment generating function.

Let $Y_1, \ldots, Y_n$ be independent $\mathcal{N}(0,1)$ random variables. Then $Y = (Y_1, \ldots, Y_n)$ has density

$$f_Y(y) = (2\pi)^{-n/2}\exp\left(-|y|^2/2\right). \tag{19.8.65}$$

Set $\widetilde{X} = \Sigma^{1/2}Y + \mu$, then $\widetilde{X}$ is Gaussian, with $\mathbb{E}(\widetilde{X}) = \mu$ and $\mathrm{Var}(\widetilde{X}) = \Sigma$, so $\widetilde{X} \sim X$. If Σ is invertible, then $\widetilde{X}$ and hence X has the density claimed in (iv), by a linear change of variables in $\mathbb{R}^n$.

Finally, if $X = (X_1, X_2)$ with $\mathrm{Cov}(X_1, X_2) = 0$, then, for $u = (u_1, u_2)$, we have

$$\langle u, \Sigma u\rangle = \langle u_1, \Sigma_{11}u_1\rangle + \langle u_2, \Sigma_{22}u_2\rangle, \tag{19.8.66}$$

where $\Sigma_{11} = \mathrm{Var}(X_1)$ and $\Sigma_{22} = \mathrm{Var}(X_2)$. Then $\phi_X(u) = \phi_{X_1}(u_1)\phi_{X_2}(u_2)$ so X_1 and X_2 are independent by Theorem 19.5.4. □

Example 19.8.21. Let (X, Y) be a Gaussian random vector in $\mathbb{R}^2$ (so $\lambda X + \mu Y$ is Gaussian for all $\lambda, \mu \in \mathbb{R}$). What is $\mathbb{E}(X|Y)$? Let $X' = aY + b$, where a and b are chosen so that

$$\text{(i) } \mathrm{Cov}(X - X', Y) = 0, \qquad \text{(ii) } \mathbb{E}X' = \mathbb{E}X. \tag{19.8.67}$$

[14] need proof

In this case $X - X'$ and Y are independent (by Theorem 19.8.20.(v), this is a property of Gaussian random vectors). Then by Proposition 19.3.12,

$$\mathbb{E}\left((X - X')\mathbb{1}_A(Y)\right) = \mathbb{E}\left(X - X'\right)\mathbb{P}(Y \in A) = 0, \tag{19.8.68}$$

so $X' = \mathbb{E}\left(X|Y\right)$ since $X \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ by Theorem 19.8.20 (ii). Notice that

$$\mathrm{Cov}(X, Y) = \mathrm{Cov}(aY + b, Y) = a \operatorname{Var} Y \quad \Rightarrow \quad a = \frac{\mathrm{Cov}(X, Y)}{\operatorname{Var} Y}, \tag{19.8.69}$$

Then, $\mathbb{E}X = \mathbb{E}X' = a\mathbb{E}Y + b \quad \Rightarrow \quad b = \mathbb{E}X - a\mathbb{E}Y$, thus

$$\mathbb{E}\left(X|Y\right) = \mathbb{E}X + \frac{\mathrm{Cov}(X, Y)}{\mathrm{Var}(Y)}(Y - \mathbb{E}Y). \tag{19.8.70}$$

Example 19.8.22. Suppose that $X_1, \ldots, X_n$ are jointly Gaussian random variables with

$$\mathbb{E}(X_i) = \mu_i, \mathrm{Cov}(X_i, X_j) = \Sigma_{ij} \tag{19.8.71}$$

and that the matrix $\Sigma = (\Sigma_{ij})$ is invertible. Set $Y = \Sigma^{-\frac{1}{2}}(X - \mu)$.

Then

$$\begin{aligned} \mathbb{E}Y &= \Sigma^{-1/2}\mathbb{E}(X - \mu) = 0 \\ \operatorname{Var} Y &= \Sigma^{-1/2} \operatorname{Var}\left(X\right) \Sigma^{-1/2} = I. \end{aligned}$$

Hence $\mathrm{Cov}(Y_i, Y_j) = \delta_{ij}$, so $Y_1, \ldots, Y_n$ are independent $\mathcal{N}(0, 1)$ random variables.

If $Z = X_2 - aX_1$ then (X_1, Z) is Gaussian, so Z and X_1 willbe independent provided

$$0 = \mathrm{Cov}(Z, X_1) = \Sigma_{12} - a\Sigma_{11}. \tag{19.8.72}$$

If $\Sigma_{11} \neq 0$, take $a = \Sigma_{12}/\Sigma_{11}$. If $\Sigma_{11} = 0$, then $X_1 = \mu_1$ a.s. so X_1 and X_2 are independent and we can take $a = 0$. Then Z is Gaussian and

$$\mathbb{E}Z = \mu_2 - a\mu_1, \quad \operatorname{Var} Z = \Sigma_{22} - 2a\Sigma_{12} + a^2\Sigma_{11}. \tag{19.8.73}$$

Example 19.8.23. Let $X_1, \ldots, X_n$ be independent $\mathcal{N}(0, 1)$ random variables. We will show that

$$\left(\overline{X},\ \sum_{m=1}^{n}(X_m - X)^2\right), \qquad \left(X_n/\sqrt{n},\ \sum_{m=1}^{n-1} X_m^2\right) \tag{19.8.74}$$

have the same distribution, where $\overline{X} = (X_1 + \cdots + X_n)/n$.

Both $\overline{X}$ and $X_n/\sqrt{n}$ are $\mathcal{N}(0, 1)$. Since $\mathbb{E}\left(\overline{X}(X_m - \overline{X})\right) = 0$ for all m, $\overline{X}$ and $(X_1 - \overline{X}, \ldots, X_n - \overline{X})$ are independent, so $\overline{X}$ and $\sum_{m=1}^{n}\left(X_m - \overline{X}\right)^2$ are independent. Set $\phi(u) = \mathbb{E}\left(e^{iuX_1^2}\right)$ and note that

$$n\overline{X}^2 + \sum_{m=1}^{n}\left(X_m - \overline{X}\right)^2 = \sum_{m=1}^{n} X_m^2 \ \Rightarrow\ \phi(u)\mathbb{E}\left(\exp\left(iu\sum_{m=1}^{n}(X_m - \overline{X})^2\right)\right) = \phi(u)^n. \tag{19.8.75}$$

Thus, $\sum_{m=1}^{n}(X_m - \overline{X})^2$ and $\sum_{m=1}^{n-1} X_m^2$ have the same characteristic function and hence the same distribution.

19.8.5 Cauchy random variables

Definition 19.8.8. A random variable X is called standard Cauchy random variable if its density function is for $d > 0$,

$$f_X(x) = \frac{d}{\pi(d^2 + x^2)}, \quad x \in \mathbb{R}. \tag{19.8.76}$$

The distribution is called standard Cauchy distribution.

Remark. Note that the moment generating function, mean, variance, etc. are undefined.

Proposition 19.8.24. The characteristic function of standard Cauchy random variable is

$$\phi(u) = e^{-|du|}, \quad u \in \mathbb{R}. \tag{19.8.77}$$

Proof. Since $e^{-|u|}$ is integrable, by Theorem 19.5.3 we can compute the inverse Fourier transform

$$\frac{1}{2\pi}\int_{\mathbb{R}} e^{-iux}e^{-|du|}du = \frac{1}{2\pi}\left(\int_0^\infty e^{-(d+ix)u}du + \int_{-\infty}^0 e^{(d-ix)u}du\right) = \frac{1}{2\pi}\left(\frac{1}{d+ix}+\frac{1}{d-ix}\right) = \frac{d}{\pi(d^2+x^2)}. \tag{19.8.78}$$

A direct computation of the transform of $d/\pi(d^2+x^2)$ can be made by Cauchy's residue theorem (Theorem 11.0.3)[15]. □

Proposition 19.8.25. If $X_1, \ldots, X_n$ are independent standard Cauchy random variables, then $\frac{X_1+\cdots+X_n}{n}$ is also Cauchy.

Proof. By Theorem 19.5.4.(iii),

$$\mathbb{E}\left(e^{iu(X_1+\cdots+X_n)/n}\right) = \left(\mathbb{E}\left(e^{i(du/n)X_n}\right)\right)^n = \left(e^{-|du|/n}\right)^n = e^{-|du|}. \tag{19.8.79}$$

Hence, $(X_1+\cdots+X_n)/n$ is also standard Cauchy. □

Remark. Neither the strong law of large numbers nor the central limit theorem apply here, as the mean of a Cauchy random variable is not well-defined.

Note that we can not apply Proposition 19.5.13 as $e^{\theta X_i}$ is not bounded.

Proposition 19.8.26. Let X and Y be two independent standard Gaussian random variables. Then X/Y is standard Cauchy distributed.

Proof. We see that by symmetry of Gaussian distribution (see Definition 19.8.6), for any $k \geq 0$

$$\mathbb{P}\left(\frac{X}{Y} \leq k\right) = \frac{2}{2\pi}\int_0^\infty \int_0^{ky} e^{-\frac{x^2}{2}}e^{-\frac{y^2}{2}}dxdy. \tag{19.8.80}$$

Let $X = r\sin\theta$ and $Y = r\cos\theta$, thus,

$$\mathbb{P}\left(\frac{X}{Y} \leq k\right) = \frac{2}{2\pi}\int_0^\infty \int_{-\pi/2}^{\arctan k} e^{-r^2/2}rdrd\theta = \frac{1}{2}+\frac{1}{\pi}\arctan k. \tag{19.8.81}$$

Then taking differentiation wrt k, we have the density function is

$$f(k) = \left(\frac{1}{2}+\frac{1}{\pi}\arctan k\right)' = \frac{1}{\pi(1+k^2)}. \tag{19.8.82}$$

Similarly, we have the same result for $k \leq 0$

$$\mathbb{P}\left(\frac{X}{Y} \leq k\right) = \frac{2}{2\pi}\int_0^\infty \int_{-\infty}^{ky} e^{-\frac{x^2}{2}}e^{-\frac{y^2}{2}}dxdy = \frac{2}{2\pi}\int_0^\infty \int_{-\pi/2}^{\arctan k} e^{-r^2/2}rdrd\theta = \frac{1}{2}+\frac{1}{\pi}\arctan k. \tag{19.8.83}$$

Taking differentiation wrt k, we have the same density function. Thus, X/Y is standard Cauchy distributed. □

19.8.6 Gamma random variables

Definition 19.8.9 (Gamma random variable)**.** A random variable X in $\mathbb{R}^+$ is called Gamma-distributed if, for some $n > 0$ and $\lambda > 0$, its density function is

$$f_X(x) = \frac{1}{\Gamma(k)}\lambda^k x^{k-1}e^{-\lambda x}, \tag{19.8.84}$$

where k is shape parameter, λ is rate parameter and $\Gamma(x)$ is Gamma function. We write $X \sim \Gamma(k,\lambda)$.

Remark. If $k = 1$, Gamma distribution is exponential distribution with parameter λ, i.e., $\Gamma(1,\lambda) \sim \mathcal{E}(\lambda)$.

If $k \in \mathbb{Z}^+$, then Gamma distributed random variable $X \sim \Gamma(k,\lambda)$ is the summation of k independent exponential distributed random variables $\mathcal{E}(\lambda)$ with the same parameter λ (see Proposition 19.8.28).

[15] need details

Proposition 19.8.27. Suppose $X \sim \Gamma(k, \lambda)$. Then for $\theta < \lambda$ and $t \in \mathbb{R}$,

$$M_X(\theta) = \left(\frac{\lambda}{\lambda - \theta}\right)^k, \qquad \phi_X(t) = \left(\frac{\lambda}{\lambda - it}\right)^k. \tag{19.8.85}$$

Proof. From Definition 19.5.4,

$$M_X(\theta) = \mathbb{E}\left(e^{\theta X}\right) = \int_0^\infty e^{\theta x} \frac{1}{\Gamma(k)} \lambda^k x^{k-1} e^{-\lambda x} dx = \frac{\lambda^k}{(\lambda-\theta)^k} \int_0^\infty \frac{1}{\Gamma(k)} (\lambda-\theta)^k x^{k-1} e^{-(\lambda-\theta)x} dx = \left(\frac{\lambda}{\lambda-\theta}\right)^k. \tag{19.8.86}$$

For $\phi_X(t)$, we have $e^{itx} = \sum_{n=0}^{+\infty} \frac{(itx)^n}{n!}$ and thus

$$\phi_X(t) = \mathbb{E}\left(e^{itX}\right) = \int_0^\infty e^{itx} \frac{1}{\Gamma(k)} \lambda^k x^{k-1} e^{-\lambda x} dx = \int_0^\infty \frac{1}{\Gamma(k)} \lambda^k x^{k-1} e^{-\lambda x} \sum_{n=0}^{\infty} \frac{(itx)^n}{n!} dx. \tag{19.8.87}$$

Therefore,

$$\phi_X(t) = \int_0^\infty \sum_{n=0}^{\infty} \frac{1}{\Gamma(k)} \lambda^k x^{k-1} e^{-\lambda x} \frac{(itx)^n}{n!} dx = \sum_{n=0}^{\infty} \frac{(it)^n}{n!} \int_0^\infty \frac{1}{\Gamma(k)} \lambda^k x^{n+k-1} e^{-\lambda x} dx$$

by Fubini Theorem (Theorem 15.3.33) since $\left|\mathbb{E}\left(e^{itX}\right)\right| \leq \mathbb{E}\left|e^{itX}\right| = 1 < \infty$. Thus,

$$\phi_X(t) = \sum_{n=0}^{\infty} \frac{(it)^n}{n!} \frac{\Gamma(n+k)}{\lambda^n \Gamma(k)} \int_0^\infty \frac{1}{\Gamma(n+k)} \lambda^{n+k} x^{n+k-1} e^{-\lambda x} dx = \sum_{n=0}^{\infty} \frac{(it)^n}{\lambda^n n!} \frac{\Gamma(n+k)}{\Gamma(k)} = \sum_{n=0}^{\infty} \binom{n+k-1}{n} \left(\frac{it}{\lambda}\right)^n \tag{19.8.88}$$

Then by Theorem 19.7.13, $\phi_X(t) = \frac{1}{(1-it/\lambda)^k} = \left(\frac{\lambda}{\lambda - it}\right)^k$. □

Proposition 19.8.28. Let $X_i \sim \mathcal{E}(\lambda)$ be independently distributed for $i = 1, \ldots, k$ with $k \in \mathbb{Z}^+$. Then $\sum_{i=1}^k X_i$ is a Gamma distributed random variable with parameters k and λ, i.e., $\sum_{i=1}^k X_i \sim \Gamma(k, \lambda)$.

Proof. Direct result from Proposition 19.8.27, Proposition 19.8.6 and Theorem 19.5.11. □

Proposition 19.8.29. Suppose $X \sim \Gamma(k, \lambda)$. Then

(i) $\mathbb{E}X = \frac{k}{\lambda}$, (ii) $\operatorname{Var} X = \frac{k}{\lambda^2}$, (iii) $\operatorname{Skew}(X) = \frac{2}{\sqrt{k}}$, (iv) $\operatorname{Kurt}(X) = \frac{6}{k}$, (v) $\mathbb{E}X^n = \frac{k(k+1)\ldots(n+k-1)}{\lambda^n}$.

Proof. With Propositions 19.8.27, 19.5.10,

$$\mathbb{E}X = \left.\frac{dM_X(\theta)}{d\theta}\right|_{\theta=0} = \left.\frac{k\lambda^k}{(\lambda-\theta)^{k+1}}\right|_{\theta=0} = \frac{k\lambda^k}{\lambda^{k+1}} = \frac{k}{\lambda}, \qquad \mathbb{E}X^2 = \left.\frac{d^2M_X(\theta)}{d\theta^2}\right|_{\theta=0} = \left.\frac{k(k+1)\lambda^k}{(\lambda-\theta)^{k+2}}\right|_{\theta=0} = \frac{k(k+1)}{\lambda^2}.$$

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \frac{k(k+1)}{\lambda^2} - \frac{k^2}{\lambda^2} = \frac{k}{\lambda^2}$. Also,

$$\mathbb{E}X^3 = \left.\frac{d^3M_X(\theta)}{d\theta^3}\right|_{\theta=0} = \left.\frac{k(k+1)(k+2)\lambda^k}{(\lambda-\theta)^{k+3}}\right|_{\theta=0} = \frac{k(k+1)(k+2)}{\lambda^3}. \tag{19.8.89}$$

Thus,

$$\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = \frac{k(k+1)(k+2)}{\lambda^3} - 3\frac{k}{\lambda}\frac{k(k+1)}{\lambda^2} + 3\frac{k^3}{\lambda^3} - \frac{k^3}{\lambda^3} = \frac{2k}{\lambda^3}. \tag{19.8.90}$$

By Definition 19.5.5, $\operatorname{Skew}(X) = \frac{2k/\lambda^3}{k^{3/2}/\lambda^3} = \frac{2}{\sqrt{k}}$. Furthermore,

$$\mathbb{E}X^4 = \left.\frac{d^4M_X(\theta)}{d\theta^4}\right|_{\theta=0} = \left.\frac{k(k+1)(k+2)(k+3)\lambda^k}{(\lambda-\theta)^{k+4}}\right|_{\theta=0} = \frac{k(k+1)(k+2)(k+3)}{\lambda^4}. \tag{19.8.91}$$

Thus,

$$\begin{aligned}\mathbb{E}\,(X-\mu)^4 &= \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 \\ &= \frac{k(k+1)(k+2)(k+3)}{\lambda^4} - 4\frac{k}{\lambda}\frac{k(k+1)(k+2)}{\lambda^3} + 6\frac{k^2}{\lambda^2}\frac{k(k+1)}{\lambda^2} - 4\frac{k^3}{\lambda^3}\frac{k}{\lambda} + \frac{k^4}{\lambda^4} = \frac{3k^2+6k}{\lambda^4}.\end{aligned}$$

By Definition 19.5.6, we have $\mathrm{Kurt}(X) = \frac{3k(k+2)/\lambda^4}{k^2/\lambda^4} - 3 = \frac{6}{k}$.

For (v), we know that $\frac{d^n M_X(\theta)}{d\theta^n} = \lambda^k k(k+1)\dots(n+k-1)/(\lambda-\theta)^{n+k}$,

$$\mathbb{E}X^n = \left.\frac{d^n M_X(\theta)}{d\theta^n}\right|_{\theta=0} = \frac{k(k+1)\dots(n+k-1)}{\lambda^n}. \tag{19.8.92}$$

□

19.8.7 Beta random variables

Definition 19.8.10 (beta random variable)**.** A random variable X in $[0,1]$ is called beta-distributed if, for some $a, b > 0$, its density function is

$$f_X(x) = \frac{x^{a-1}(1-x)^{b-1}}{B(a,b)}, \tag{19.8.93}$$

where $B(a,b)$ is Beta function. We write $X \sim \mathrm{B}(a,b)$.

Proposition 19.8.30. Suppose $X \sim \mathrm{B}(a,b)$. Then

$$\text{(i) } \mathbb{E}X = \frac{a}{a+b}, \quad \text{(ii) } \mathrm{Var}\,X = \frac{ab}{(a+b)^2(a+b+1)}, \quad \text{(iii) } \mathrm{Skew}(X) = \frac{2(b-a)\sqrt{a+b+1}}{(a+b+2)\sqrt{ab}},$$

$$\text{(iv) } \mathrm{Kurt}(X) = \frac{6\left((a-b)^2(a+b+1) - ab(a+b+2)\right)}{ab(a+b+2)(a+b+3)}.$$

Proof. [16]

□

19.9 Sums of independent random variables

19.9.1 Weak Law of large numbers

Theorem 19.9.1 (weak law of large numbers)**.** Let $X_1, X_2, \dots$ be independent, identically distributed random variables with $\mathbb{E}X_1 = \mu$ and $\mathrm{Var}(X_1) < \infty$. For any constant $\varepsilon > 0$,

$$\mathbb{P}\left(\left|\frac{X_1+\cdots+X_n}{n} - \mu\right| > \varepsilon\right) \to 0, \quad \text{as } n \to \infty. \tag{19.9.1}$$

Proof. By Chebyshev's inequality (Theorem 19.3.21) we have

$$\begin{aligned}\mathbb{P}\left(\left|\frac{X_1+\cdots+X_n}{n} - \mu\right| > \varepsilon\right) &\le \frac{1}{\varepsilon^2}\mathbb{E}\left(\frac{X_1+\cdots+X_n}{n} - \mu\right)^2 = \frac{1}{n^2\varepsilon^2}\mathbb{E}(X_1+\cdots+X_n-n\mu)^2 \\ &= \frac{1}{n^2\varepsilon^2}\mathrm{Var}(X_1+\cdots+X_n) = \frac{n}{n^2\varepsilon^2}\mathrm{Var}(X_1) = \frac{1}{n\varepsilon^2}\mathrm{Var}(X_1) \to 0,\end{aligned}$$

as required. □

Remark. (i) This is proved first by Jacob Bernoulli[17] in 1713.

[16] need proof.

[17] need mathematician link

(ii) The statement in Theorem 19.9.1 is normally referred to by saying that the random variable $(X_1+\cdots+X_n)/n$ 'converges in probability' to μ, written

$$\frac{X_1+\cdots+X_n}{n} \xrightarrow{p} \mu \text{ as } n\to\infty. \tag{19.9.2}$$

(iii) This result should be distinguished from the strong law of large numbers which states that

$$\mathbb{P}\left(\frac{X_1+\cdots+X_n}{n} \to \mu \text{ as } n\to\infty\right) = 1. \tag{19.9.3}$$

As the name implies, the strong law of large numbers implies the weak law (by Theorem 19.2.16). The mode of convergence in the strong law is referred to as 'convergence with probability one' or 'almost sure convergence'.

(iv) Notice that the requirement that the random variables in the weak law be independent is not one that we may dispense with. For example, suppose that $\Omega=\{\omega_1,\omega_2\}$ has just two points and let $X_n(\omega_1)=1$ and $X_n(\omega_2)=0$ for each n, so that the random variables are identically distributed, but not of course independent. Let $p=\mathbb{P}(\{\omega_1\})=1-\mathbb{P}(\{\omega_2\})$, where $0<p<1$, then $\mathbb{E}X_1=p$, and we have

$$\frac{X_1(\omega_1)+\cdots+X_n(\omega_1)}{n}=1, \qquad \frac{X_1(\omega_2)+\cdots+X_n(\omega_2)}{n}=0, \quad \text{for all } n, \tag{19.9.4}$$

so that the conclusion of Theorem 19.9.1 cannot hold.

(v) It should be noticed that the weak law of large numbers is 'distribution free' in that the particular distribution of the summands $\{X_i\}$ only influences the result through the mean, μ, (and, in the form we have stated it, through the fact that the variance is finite) but otherwise the underlying distribution does not enter the conclusion of the Theorem.

Example 19.9.2. The weak law of large numbers underlies the 'frequentist' interpretation of probability. Suppose that we have independent repetitions of an experiment, and we set $X_i=1$ if a particular outcome occurs on the ith repetition (e.g., 'Heads'), and $X_i=0$, otherwise (e.g., 'Tails'). Then $\mathbb{E}X_i=p$, say, where $p=\mathbb{P}(X_i=1)$ is the probability of the outcome. Then $(X_1+\cdots+X_n)/n$ is the average number of occurrences of the outcome in n repetitions and this converges in the above sense to $\mathbb{E}X_i=p$, thus the probability p is the long-run proportion of times that the outcome occurs.

By giving a more refined argument it is possible to dispense with the requirement in the statement of the Theorem that $\mathrm{Var}(X_1)<\infty$. The conclusion still holds provided $\mathbb{E}\,|X_1|<\infty$.

Theorem 19.9.3 (weak law of large numbers)**.** Let $X_1, X_2, \ldots$ be independent, identically distributed random variables with $\mathbb{E}X_1=\mu$ and $\mathbb{E}\,|X_1|<\infty$. For any constant $\varepsilon>0$,

$$\mathbb{P}\left(\left|\frac{X_1+\cdots+X_n}{n}-\mu\right|>\varepsilon\right)\to 0, \quad \text{as } n\to\infty. \tag{19.9.5}$$

Proof. By Taylor's theorem for complex functions[18], the characteristic function of any random variable, X, with finite mean μ, can be written as

$$\phi_X(t)=1+it\mu+o(t), \quad t\to 0. \tag{19.9.6}$$

All $X_1, X_2, \ldots$ have the same characteristic function, so we will simply denote this ϕ_X. Among the basic properties of characteristic functions there are

$$\phi_{\frac{1}{n}X}(t)=\phi_X\left(\frac{t}{n}\right), \quad \phi_{X+Y}(t)=\phi_X(t)\phi_Y(t) \quad \text{if } X \text{ and } Y \text{ are independent.} \tag{19.9.7}$$

These rules can be used to calculate the characteristic function of $\overline{X}_n := \frac{1}{n}\sum_{i=1}^n X_i$ in terms of ϕ_X:

$$\phi_{\overline{X}_n}(t)=\left[\phi_X\left(\frac{t}{n}\right)\right]^n=\left[1+i\mu\frac{t}{n}+o\left(\frac{t}{n}\right)\right]^n\to e^{it\mu}, \quad \text{as } n\to\infty. \tag{19.9.8}$$

The limit $e^{it\mu}$ is the characteristic function of the constant random variable μ, and hence by Lévy's convergence theorem (Theorem 19.6.13), $\overline{X}_n$ converges in distribution to μ:

$$\overline{X}_n \xrightarrow{d} \mu \text{ as } n\to\infty. \tag{19.9.9}$$

[18] need link

μ is a constant, which implies that convergence in distribution to μ and convergence in probability to μ are equivalent (Proposition 19.6.3) Therefore,

$$\overline{X}_n \xrightarrow{p} \mu \text{ as } n \to \infty. \tag{19.9.10}$$

□

19.9.2 Strong law of large numbers for finite fourth moment

The result we obtain in this section will be largely superseded in the next. We include it because its proof is much more elementary than that needed for the definitive version of the strong law which follows.

Theorem 19.9.4 (strong law of large numbers)**.** Let $(X_n : n \in \mathbb{N})$ be a sequence of independent random variables such that, for some constants $\mu \in \mathbb{R}$ and $M < \infty$,

$$\mathbb{E}(X_n) = \mu, \quad \mathbb{E}(X_n^4) \leq M \quad \text{for all } n. \tag{19.9.11}$$

Set $S_n = X_1 + \cdots + X_n$. Then

$$S_n/n \to \mu \text{ a.s., } \quad \text{as } n \to \infty. \tag{19.9.12}$$

Proof. Consider $Y_n = X_n - \mu$. Then $Y_n^4 \leq 2^4(X_n^4 + \mu^4)$, so

$$\mathbb{E}(Y_n^4) \leq 16(M + \mu^4) \tag{19.9.13}$$

and it suffices to show that $(Y_1 + \cdots + Y_n)/n \to 0$ a.s. So we are reduced to the case where $\mu = 0$.

Note that X_n, X_n^2, X_n^3 are all integrable since X_n^4 is. Since $\mu = 0$, by independence,

$$\mathbb{E}(X_i X_j^3) = \mathbb{E}(X_i X_j X_k^2) = \mathbb{E}(X_i X_j X_k X_l) = 0 \tag{19.9.14}$$

for distinct indices i, j, k, l. Hence

$$\mathbb{E}(S_n^4) = \mathbb{E}\left(\sum_{1 \leq i \leq n} X_k^4 + 6 \sum_{1 \leq i < j \leq n} X_i^2 X_j^2 \right). \tag{19.9.15}$$

Now for $i < j$, by independence and the Cauchy-Schwarz inequality (Theorem 19.3.25),

$$\mathbb{E}(X_i^2 X_j^2) = \mathbb{E}(X_i^2)\mathbb{E}(X_j^2) \leq \mathbb{E}(X_i^4)^{1/2}\mathbb{E}(X_j^4)^{1/2} \leq M. \tag{19.9.16}$$

So we get the bound

$$\mathbb{E}(S_n^4) \leq nM + 3n(n-1)M \leq 3n^2 M. \tag{19.9.17}$$

Thus

$$\mathbb{E}\left(\sum_n (S_n/n)^4 \right) \leq 3M \sum_n 1/n^2 < \infty \quad \Rightarrow \quad \sum_n (S_n/n)^4 < \infty \text{ a.s.} \tag{19.9.18}$$

and hence $S_n/n \to 0$ a.s.. □

Proposition 19.9.5. Let $(X_n : n \in \mathbb{N})$ be a sequence of independent random variables such that, for some constants $\mu \in \mathbb{R}$ and $M < \infty$,

$$\mathbb{E}(X_n) = \mu, \quad \mathbb{E}(X_n^4) \leq M \quad \text{for all } n. \tag{19.9.19}$$

Set $S_n = X_1X_2 + X_2X_3 + \cdots + X_{n-1}X_n$. Then

$$P_n/n \to \mu^2 \text{ a.s., } \quad \text{as } n \to \infty. \tag{19.9.20}$$

Proof. Consider

$$Y_n = X_{2n-1}X_{2n}, \quad Z_n = X_{2n}X_{2n+1}. \tag{19.9.21}$$

Then since $(X_n : n \in \mathbb{N})$ are independent, Y_n and Z_n are independent and

$$\mathbb{E}(Y_n) = \mathbb{E}\left(X_{2n-1}\right)\mathbb{E}\left(X_{2n}\right) = \mu^2, \quad \mathbb{E}(Z_n) = \mathbb{E}\left(X_{2n}\right)\mathbb{E}\left(X_{2n+1}\right) = \mu^2, \quad \mathbb{E}(Y_n^4), \mathbb{E}(Z_n^4) \leq M^2. \tag{19.9.22}$$

Set $S_n = Y_1 + \cdots + Y_n$ and $T_n = Z_1 + \cdots + Z_n$. By Theorem 19.9.4, we have

$$S_n/n \to \mu^2, \quad T_n/n \to \mu^2 \text{ a.s. .} \tag{19.9.23}$$

Then

$$\frac{P_{2n}}{2n} = \frac{S_n + T_{n-1}}{2n} \to \mu^2, \quad \frac{P_{2n+1}}{2n+1} = \frac{S_n + T_n}{2n+1} \to \mu^2, \text{ a.s..} \tag{19.9.24}$$

Thus, $P_n/n \to \mu^2$ a.s.. □

19.9.3 Canonical probability space

Definition 19.9.1 (canonical probability space)**.** Consider a sequence of random variable $(X_n : n \in \mathbb{N})$ and the infinite product space

$$E = \mathbb{R}^{\mathbb{N}} = \{x = (x_n : n \in \mathbb{N}) : x_n \in \mathbb{R} \text{ for all } n\} \tag{19.9.25}$$

and the σ-algebra $\mathcal{E}$ on E generated by the coordinate functions $f_n(x) = x_n$

$$\mathcal{E} = \sigma(f_n : n \in \mathbb{N}) = \sigma\left(f_n^{-1}(A) : A \in \mathcal{B}(\mathbb{R}), n \in \mathbb{N}\right) = \sigma\left(\bigotimes_{k=1}^{n-1} \mathbb{R} \times A \times \bigotimes_{k>n} \mathbb{R} : A \in \mathcal{B}(\mathbb{R}), n \in \mathbb{N}\right). \tag{19.9.26}$$

Note that $\mathcal{E}$ is also generated by the π-system

$$\mathcal{A} = \left\{\bigotimes_{n\in\mathbb{N}} A_n : A_n \in \mathcal{B} \text{ for all } n,\ A_n = \mathbb{R} \text{ for sufficiently large } n\right\}. \tag{19.9.27}$$

Define $X : \Omega \to E$ by $X(\omega) = (X_n(\omega) : n \in \mathbb{N})$

$$\begin{aligned} X : (\Omega, \mathcal{F}, \mathbb{P}) &\longrightarrow (E, \mathcal{E}) \\ \omega &\longmapsto (X_1(\omega), X_2(\omega), \ldots) \end{aligned}$$

Then for any set in π-system, $A = \bigotimes_{n\in\mathbb{N}} A_n \in \mathcal{A}$, $A_n \in \mathcal{B}(\mathbb{R})$. Thus, $B_n = X_n^{-1}(A_n) \in \mathcal{F}$ since X_n are random variables (measurable). Thus, $X^{-1}(A) = \bigcap_n B_n \in \mathcal{F}$, so by Proposition 15.2.1, Y is measurable.

Also the image measure $\mu = \mathbb{P} \circ X^{-1}$. By uniqueness of extension (Theorem 15.1.18), μ is the unique measure on $\mathcal{E}$ having this property.

The probability space $(E, \mathcal{E}, \mu)$ is called the canonical probability space for such sequences.

Definition 19.9.2 (shift map)**.** Define the shift map $\theta : E \to E$ by

$$\theta(x_1, x_2, \ldots) = (x_2, x_3, \ldots). \tag{19.9.28}$$

Theorem 19.9.6. The shift map is an ergodic measure-preserving transformation if the sequence $(X_n : n \in \mathbb{N})$ are i.i.d.

Proof. Let m be a probability measure on $\mathbb{R}$. In subsection 19.2.3, we constructed a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ on which there exists a sequence of independent random variables $(X_n : n \in \mathbb{N})$, all having distribution m.

$\forall A \in \mathcal{A}$ of the form $A = \bigotimes_{k=1}^n A_k \times \bigotimes_{k>n} \mathbb{R}$ for n sufficiently large, then

$$\theta^{-1}(A) = \mathbb{R} \times \bigotimes_{k=1}^{n} A_k \times \bigotimes_{k>n} \mathbb{R} \in \mathcal{A} \subseteq \mathcal{E}. \tag{19.9.29}$$

Thus, by Proposition 15.2.1, θ is measurable. Also, $\mu = \mathbb{P} \circ X^{-1}$, for $A = \bigotimes_{n\in\mathbb{N}} A_n \in \mathcal{A}$,

$$\mu(A) = \prod_{n\in\mathbb{N}} m(A_n) \tag{19.9.30}$$

since $(X_n : n \in \mathbb{N})$ are independent (by Theorem 19.5.4.(ii)). Thus,

$$\mu(A) = \prod_{k=1}^{n} m(A_n), \quad \mu(\theta^{-1}(A)) = \prod_{k=1}^{n} m(A_n) \ \Rightarrow\ \mu(A) = \mu(\theta^{-1}(A)) = (\mu \circ \theta^{-1})(A) \tag{19.9.31}$$

Note that $\mu \circ \theta^{-1}$ is also a probability measure. Thus, by uniqueness of extension (Theorem 15.1.18),

$$\mu(A) = \mu(\theta^{-1}(A)),\ \forall A \in \mathcal{E} \ \Rightarrow\ \theta \text{ is measure-preserving transformation.} \tag{19.9.32}$$

To see that θ is ergodic, we recall the definition of the tail σ-algebras (Definition 19.2.8),

$$\mathcal{T}_n = \sigma(X_m : m \geq n+1), \qquad \mathcal{T}_\infty = \bigcap_n \mathcal{T}_n. \tag{19.9.33}$$

For $A = \bigotimes_{n\in\mathbb{N}} A_n \in \mathcal{A}$ we have

$$\theta^{-n}(A) = \{X_{n+k} \in A_k \text{ for all } k\} \in \mathcal{T}_n. \tag{19.9.34}$$

Since $\mathcal{T}_n$ is a σ-algebra, it follows that $\theta^{-n}(A) \in \mathcal{T}_n$ for all $A \in \mathcal{E}$, so by Proposition 15.6.1,

$$\left\{A \in \mathcal{E} : \theta^{-1}(A) = A\right\} = \mathcal{E}_\theta \subseteq \mathcal{T}_\infty. \tag{19.9.35}$$

Hence θ is ergodic by Kolmogorov's 0-1 law (Theorem 19.2.12) since the sequence X_n are independent. □

19.9.4 Stationary sequence of random variables

Definition 19.9.3 (stationary sequence of random variables)**.** A sequence of random variables $(X_n : n \in \mathbb{N})$ on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ is stationary if for each $n, k \in \mathbb{N}$ the random vectors $(X_1, \ldots, X_n)$ and $(X_{k+1}, \ldots, X_{k+n})$ have the same distribution: for $A_1, \ldots, A_n \in \mathcal{B}(\mathbb{R})$,

$$\mathbb{P}(X_1 \in A_1, \ldots, X_n \in A_n) = \mathbb{P}(X_{k+1} \in A_1, \ldots, X_{k+n} \in A_n). \tag{19.9.36}$$

Remark. Note that $(X_n : n \in \mathbb{N})$ are not independent.

Proposition 19.9.7. If $(X_n : n \in \mathbb{N})$ is a stationary sequence and $X_1 \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, for some $p \in [1, \infty)$, then

$$\frac{1}{n}\sum_{i=1}^{n} X_i \to Y \quad \text{a.s. and in } \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}), \tag{19.9.37}$$

for some random variable $Y \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ with $\mathbb{E}(Y) = \mathbb{E}(X_1)$.

Proof. Let $(E, \mathcal{E}, \mu)$ be the canoncial probability space of $(X_n : n \in \mathbb{N})$ and θ be the shift map (see Definition 19.9.2). $\forall A \in \mathcal{A}$ of the form $A = \bigotimes_{k=1}^{n} A_k \times \bigotimes_{k>n} \mathbb{R}$ for n sufficiently large, then

$$\begin{aligned}
\mu(\theta^{-1}(A)) &= \mathbb{P} \circ X^{-1}\left(\theta^{-1}(A)\right) = \mathbb{P}\left(\theta(X) \in A\right) = \mathbb{P}\left(X \in \theta^{-1}(A)\right) = \mathbb{P}(X_2 \in A_1, \ldots, X_{n+1} \in A_n) \\
&= \mathbb{P}(X_1 \in A_1, \ldots, X_n \in A_n) \qquad (X_n : n \in \mathbb{N}) \text{ is stationary} \\
&= \mathbb{P}\left(X \in A\right) = \mu(A).
\end{aligned}$$

So probability measures $\mu \circ \theta^{-1}$ and μ agree on $\mathcal{A}$, so they must agree on $\mathcal{E}$. Thus, θ is measure-preserving.
Now let $f : (E, \mathcal{E}, \mu) \to (\mathbb{R}, \mathcal{B}(\mathbb{R}))$ be the first coordinate map. Then

$$f \circ X = X_1\ (f(x) = x_1), \quad f \circ \theta \circ X = X_2\ (f \circ \theta(x) = x_2), \quad \ldots \tag{19.9.38}$$

Thus,

$$\mu\left(|f|^p\right) = \mathbb{E}\left(|X_1|^p\right) < \infty \qquad \text{since } X_1 \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}) \ \Rightarrow\ f \in \mathcal{L}^p(E, \mathcal{E}, \mu). \tag{19.9.39}$$

Then by Birkhoff's ergodic theorem (Theorem 15.6.6 since f is integrable by Proposition 15.4.5) and von Neumann's ergodic theorem (Theorem 15.6.9), we have that

$$\frac{1}{n}(f + f \circ \theta + \cdots + f \circ f^{n-1}) = S_n(f)/n \to \bar{f} \quad \text{a.e. and in } \mathcal{L}^p(E, \mathcal{E}, \mu), \tag{19.9.40}$$

for some $\overline{f} \in \mathcal{L}^p(E, \mathcal{E}, \mu)$. Set $Y = \overline{f} \circ X$, so $Y : (\Omega, \mathcal{F}, \mathbb{P}) \to (\mathbb{R}, \mathcal{B}(\mathbb{R}))$. Then

$$\mathbb{E}\left(|Y|^p\right) = \mathbb{E}\left(\left|\overline{f}\right|^p \circ X\right) = \mu\left(\left|\overline{f}\right|^p\right) < \infty \ \Rightarrow\ Y \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}). \tag{19.9.41}$$

Then we have that,

$$\begin{aligned} 1 = \mu\left(S_n(f)/n \to \bar{f}\right) &= \mathbb{P} \circ X^{-1}\left(\left\{x \in E : \frac{1}{n} S_n(f)(x) \to \bar{f}(x)\right\}\right) = \mathbb{P}\left(\left\{\omega : \frac{1}{n} S_n(f)(X(\omega)) \to \overline{f}(X(\omega))\right\}\right) \\ &= \mathbb{P}\left(\left\{\omega : \frac{1}{n}\left(f \circ X(\omega) + f \circ \theta \circ X(\omega) + \cdots + f \circ \theta^{n-1} \circ X(\omega)\right)\right) \to \overline{f}(X(\omega))\right\}\right) \\ &= \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i(\omega) \to Y(\omega)\right). \end{aligned}$$

$$\mathbb{E}\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i - Y\right|^p\right) = \mathbb{E}(\left|S_n(f)/n - \overline{f}\right|^p \circ X) = \mu\left(\left|S_n(f)/n - \overline{f}\right|^p\right) \to 0. \tag{19.9.42}$$

Hence,

$$\frac{1}{n}\sum_{i=1}^{n} X_i \to Y \quad \text{a.s. and in } \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}). \tag{19.9.43}$$

Finally, by Proposition 19.3.34,

$$\frac{1}{n}\sum_{i=1}^{n} X_i \to Y \ \text{ in } \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P}) \ \Rightarrow \ \mathbb{E}(Y) = \lim_{n\to\infty} \mathbb{E}\left(\frac{1}{n}\sum_{i=1}^{n} X_i\right) = \mathbb{E}(X_1) \tag{19.9.44}$$

by dominated convergence theorem (Theorem 19.3.8). □

19.9.5 Strong law of large numbers

Theorem 19.9.8. Let m be a probability measure on $\mathbb{R}$, with

$$\int_{\mathbb{R}} |x_n| m(dx_n) < \infty, \qquad \int_{\mathbb{R}} x_n m(dx_n) = \nu, \qquad n \in \mathbb{N} \tag{19.9.45}$$

Let $(E, \mathcal{E}, \mu)$ be the canonical model for a sequence of independent random variables with law m. Then

$$\mu(\{x \in \mathbb{R}^{\mathbb{N}} : (x_1 + \cdots + x_n)/n \to \nu \text{ as } n \to \infty\}) = 1. \tag{19.9.46}$$

Proof. By Theorem 19.9.6, the shift map θ on E is measure-preserving and ergodic. The coordinate function $f(x) = x_1, x \in \mathbb{R}^{\mathbb{N}}$ is integrable (since $\int |f|\, d\mu = \int_{\mathbb{R}} |x_1| m(dx_1) < \infty$) and

$$S_n(f)(x) = f(x) + f \circ \theta(x) + \cdots + f \circ \theta^{n-1}(x) = x_1 + \cdots + x_n. \tag{19.9.47}$$

Also by Proposition 15.6.3,

$$\mu(f \circ \theta^{n-1}(x)) = \mu(f(x)) = m(x_1) = \nu \ \Rightarrow \ \mu\left(S_n(f)(x)/n\right) = n\mu(f(x))/n = \nu. \quad (*) \tag{19.9.48}$$

So $S_n(f)/n \to \overline{f}$ a.e. and in $\mathcal{L}^1(E, \mathcal{E}, \mu)$, for some invariant function $\overline{f}$, by Birkhoff's theorem (Theorem 15.6.6) and von Neumann's $\mathcal{L}^p$ ergodic theorem (Theorem 15.6.9). Since θ is ergodic, $\overline{f} = c$ a.e., for some constant c by Proposition 15.6.4. Also, $\mu\left(S_n(f)/n\right) \to \mu\left(\overline{f}\right)$ by dominated convergence theorem (Theorem 19.3.8).

Then by Theorem 15.3.10,

$$c = \mu(\overline{f}) = \lim_n \mu(S_n(f)/n) = \lim_n \nu = \nu. \quad (\text{by } (*)) \tag{19.9.49}$$

□

Theorem 19.9.9 (strong law of large numbers)**.** Let $(Y_n : n \in \mathbb{N})$ be a sequence of independent, identically distributed, integrable random variables with mean ν. Set $S_n = Y_1 + \cdots + Y_n$. Then

$$S_n/n \to \nu \text{ a.s. as } n \to \infty. \tag{19.9.50}$$

Proof. In the notation of Theorem 19.9.8, take m to be the law of the random variables Y_n. Then $\mu = P \circ Y^{-1}$, where

$Y : \Omega \to E$ is given by $Y(\omega) = (Y_n(\omega) : n \in \mathbb{N})$. Hence

$$\begin{aligned}\mathbb{P}(S_n/n \to \nu \text{ as } n \to \infty) &= \mathbb{P}\left((Y_1(\omega) + \cdots + Y_n(\omega))/n \to \nu \text{ as } n \to \infty\right) \\ &= \mu(\{x : (x_1 + \cdots + x_n)/n \to \nu \text{ as } n \to \infty\}) = 1.\end{aligned}$$

□

19.9.6 Central limit theorem

Theorem 19.9.10 (central limit theorem)**.** Let $(X_n : n \in \mathbb{N})$ be a sequence of independent, identically distributed (i.i.d.), random variables with mean 0 and variance 1. Set $S_n = X_1 + \cdots + X_n$. Then, for all $a < b$, as $n \to \infty$,

$$\mathbb{P}\left(\frac{S_n}{\sqrt{n}} \in [a, b]\right) \to \int_a^b \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy, \quad \text{i.e.,} \quad \frac{S_n}{\sqrt{n}} \to \mathcal{N}(0, 1). \tag{19.9.51}$$

Remark. The alternative form[19] is: $(X_n)_{n\in\mathbb{N}}$ are i.i.d. with mean μ and variance σ^2 and $S_n = X_1 + \cdots + X_n$. Then

$$\frac{S_n - n\mu}{\sigma\sqrt{n}} \xrightarrow{d} \mathcal{N}(0, 1). \tag{19.9.52}$$

Proof. Set $\phi(u) = \mathbb{E}(e^{iuX_1})$ where $\phi(u)$ is the characteristic function (Definition 19.5.1). Since e^{iuX_1} is bounded and $\mathbb{E}(X_1^2) = 1 < \infty$, we can differentiate $\mathbb{E}(e^{iuX_1})$ twice under the expectation by Theorem 15.3.29. It is shown that

$$\phi(0) = \mathbb{E}\left(e^0\right) = 1, \quad \phi'(0) = \mathbb{E}\left(iX_1 e^0\right) = 0, \quad \phi''(0) = \mathbb{E}\left(-X_1^2 e^0\right) = -1. \tag{19.9.53}$$

Hence, by Taylor's theorem (Theorem 10.4.15), as $u \to 0$,

$$\phi(u) = 1 - u^2/2 + o(u^2). \tag{19.9.54}$$

So, for the characteristic function ϕ_n of $S_n/\sqrt{n}$, by Theorem 19.5.4.(iii),

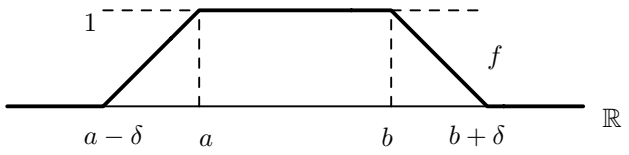
$$\phi_n(u) = \mathbb{E}\left(e^{iu(X_1+\cdots+X_n)/\sqrt{n}}\right) = \left(\mathbb{E}\left(e^{i(u/\sqrt{n})X_1}\right)\right)^n = (1 - u^2/2n + o(u^2/n))^n. \tag{19.9.55}$$

The complex logarithm satisfies, as $z \to 0$, $\log(1 + z) = z + o(|z|)$. So for each $u \in \mathbb{R}$, as $n \to \infty$,

$$\log \phi_n(u) = n \log\left(1 - u^2/2n + o(u^2/n)\right) = -u^2/2 + o(1). \tag{19.9.56}$$

Hence $\phi_n(u) \to e^{-u^2/2}$ for all u. But $e^{-u^2/2}$ is the characteristic function of the $\mathcal{N}(0, 1)$ distribution, so $S_n/\sqrt{n} \to \mathcal{N}(0, 1)$ in distribution by Lévy's convergence theorem (Theorem 19.6.13), as required. □

Alternative Proof. Take a random variable $Y \sim \mathcal{N}(0, 1)$, independent of the sequence $(X_n : n \in \mathbb{N})$. Fix $a < b$ and $\delta > 0$ and consider the function f which interpolates linearly the points $(-\infty, 0)$, $(a - \delta, 0)$, $(a, 1)$, $(b, 1)$, $(b + \delta, 0)$, $(\infty, 0)$.



Note that $|f(x + y) - f(x)| \le |y|/\delta$ for all x, y. So, given $\varepsilon > 0$, for $t = (\pi/2)(\varepsilon\delta/3)^2$ and any random variable Z, by Theorem 15.3.10.(iv) and Proposition 19.8.15,

$$\left|\mathbb{E}(f(Z + \sqrt{t}Y)) - \mathbb{E}(f(Z))\right| \le \mathbb{E}(\sqrt{t}|Y|)/\delta = \varepsilon/3. \tag{19.9.57}$$

Recall from the proof of the Fourier inversion formula ((*) in the proof of Theorem 19.5.3) that

$$\mathbb{E}\left(f\left(\frac{S_n}{\sqrt{n}} + \sqrt{t}Y\right)\right) = \int_{\mathbb{R}} \left(\frac{1}{2\pi}\int_{\mathbb{R}} \phi_n(u) e^{-u^2 t/2} e^{-iuy} du\right) f(y) dy. \tag{19.9.58}$$

[19] details needed

Consider a second sequence of independent random variables $(\overline{X}_n : n \in \mathbb{N})$, also independent of Y, and with $\overline{X}_n \sim \mathcal{N}(0,1)$ for all n. Note that $\overline{S}_n/\sqrt{n} \sim \mathcal{N}(0,1)$ for all n. So

$$\mathbb{E}\left(f\left(\frac{\overline{S}_n}{\sqrt{n}} + \sqrt{t}Y\right)\right) = \int_{\mathbb{R}} \left(\frac{1}{2\pi}\int_{\mathbb{R}} e^{-u^2/2} e^{-u^2 t/2} e^{-iuy} du\right) f(y) dy. \tag{19.9.59}$$

Now $e^{-u^2 t/2} f(y) \in \mathcal{L}^1(\mathbb{R}^2, \mathcal{B}(\mathbb{R}^2), du \otimes dy)$ and ϕ_n is bounded, with $\phi_n(u) \to e^{-u^2/2}$ for all u as $n \to \infty$, so, by bounded convergence theorem (Theorem 19.3.10) for n sufficiently large,

$$\left|\mathbb{E}\left(f\left(\frac{S_n}{\sqrt{n}} + \sqrt{t}Y\right)\right) - \mathbb{E}\left(f\left(\frac{\overline{S}_n}{\sqrt{n}} + \sqrt{t}Y\right)\right)\right| \leq \varepsilon/3. \tag{19.9.60}$$

$$\begin{aligned}
\left|\mathbb{E}\left(f\left(S_n/\sqrt{n}\right)\right) - \mathbb{E}\left(f\left(\overline{S}_n/\sqrt{n}\right)\right)\right| &\leq \left|\mathbb{E}\left(f\left(S_n/\sqrt{n}\right)\right) - \mathbb{E}\left(f\left(S_n/\sqrt{n} + \sqrt{t}Y\right)\right)\right| \\
&\quad + \left|\mathbb{E}\left(f\left(\overline{S}_n/\sqrt{n} + \sqrt{t}Y\right)\right) - \mathbb{E}\left(f\left(S_n/\sqrt{n} + \sqrt{t}Y\right)\right)\right| \\
&\quad + \left|\mathbb{E}\left(f\left(\overline{S}_n/\sqrt{n}\right)\right) - \mathbb{E}\left(f\left(\overline{S}_n/\sqrt{n} + \sqrt{t}Y\right)\right)\right| \\
&\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.
\end{aligned}$$

But $\overline{S}_n/\sqrt{n} \sim Y$ for all n and $\varepsilon > 0$ is arbitrary, so we have shown that

$$\mathbb{E}(f(S_n/\sqrt{n})) \to \mathbb{E}(f(Y)) \quad \text{as } n \to \infty. \tag{19.9.61}$$

The same argument applies to the function g, defined like f, but with a, b replaced by $a + \delta$, $b - \delta$ respectively. Now $g \leq \mathbb{1}_{[a,b]} \leq f$, so by Theorem 15.3.10.(ii),

$$\mathbb{E}\left(g\left(\frac{S_n}{\sqrt{n}}\right)\right) \leq \mathbb{P}\left(\frac{S_n}{\sqrt{n}} \in [a,b]\right) \leq \mathbb{E}\left(f\left(\frac{S_n}{\sqrt{n}}\right)\right). \tag{19.9.62}$$

On the other hand, as $\delta \downarrow 0$, by dominated convergence theorem (Theorem 19.3.8),

$$\mathbb{E}(g(Y)) \uparrow \int_a^b \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy, \qquad \mathbb{E}(f(Y)) \downarrow \int_a^b \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy \tag{19.9.63}$$

so we must have, as $n \to \infty$,

$$\mathbb{P}\left(\frac{S_n}{\sqrt{n}} \in [a,b]\right) \to \int_a^b \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy. \tag{19.9.64}$$

□

Example 19.9.11 (normal approximation to the binomial distribution)**.** If the random variable $Y \sim \text{Bin}(n,p)$, we may think of the distribution of Y as being the same as that of the sum of n i.i.d. random variables each of which has the Bernoulli distribution, thus the random variable $(Y - np)/\sqrt{np(1-p)}$ has approximately the $\mathcal{N}(0,1)$ distribution for large n.

Note that here p is being held fixed and $n \to \infty$, unlike the situation we described in the Poisson approximation to the binomial where $n \to \infty$ and $p \to 0$ in such a way that the product $np \to \lambda > 0$.

Example 19.9.12 (normal approximation to the Poisson distribution)**.** When the random variable $Y \sim \text{Poi}(n)$, where $n \geq 1$ is an integer, we may think of Y as having the same distribution as that of the sum of n i.i.d. random variables each with the Poi(1) distribution. Thus $(Y - n)/\sqrt{n}$ has approximately the $\mathcal{N}(0,1)$ distribution for large n. The same conclusion is true for $Y \sim \text{Poi}(\lambda)$ for non-integer λ, that is, $(Y - \lambda)/\sqrt{\lambda}$ is approximately $\mathcal{N}(0,1)$ for λ large.

Example 19.9.13 (opinion polls)**.** Suppose that the proportion of voters in the population who vote Labour is p, where p is unknown. A random sample of n voters is taken and it is found that S voters in the sample vote Labour and we estimate p by S/n. We want to ensure that $|S/n - p| < \varepsilon$, for some small given ε, with high probability, ≥ 0.95, say. How large must n be? Note that $S \sim \text{Bin}(n,p)$, so that $\mathbb{E}S = np$ and $\text{Var}(S) = np(1-p)$. Then by central limit theorem (Theorem 19.9.10),

we require

$$\begin{aligned}\mathbb{P}\left(\left|\frac{S}{n}-p\right|<\varepsilon\right) &= \mathbb{P}\left(-\varepsilon\sqrt{\frac{n}{p(1-p)}}<\frac{S-np}{\sqrt{np(1-p)}}<\varepsilon\sqrt{\frac{n}{p(1-p)}}\right)\\ &\approx \Phi\left(\varepsilon\sqrt{\frac{n}{p(1-p)}}\right)-\Phi\left(-\varepsilon\sqrt{\frac{n}{p(1-p)}}\right)\\ &= 2\Phi\left(\varepsilon\sqrt{\frac{n}{p(1-p)}}\right)-1\geq 0.95, \qquad \text{since } \Phi(x)=1-\Phi(-x),\end{aligned}$$

so that we need $\varepsilon\sqrt{n/p(1-p)}>1.96$, that is

$$n\geq (1.96)^2 p(1-p)/\varepsilon^2. \tag{19.9.65}$$

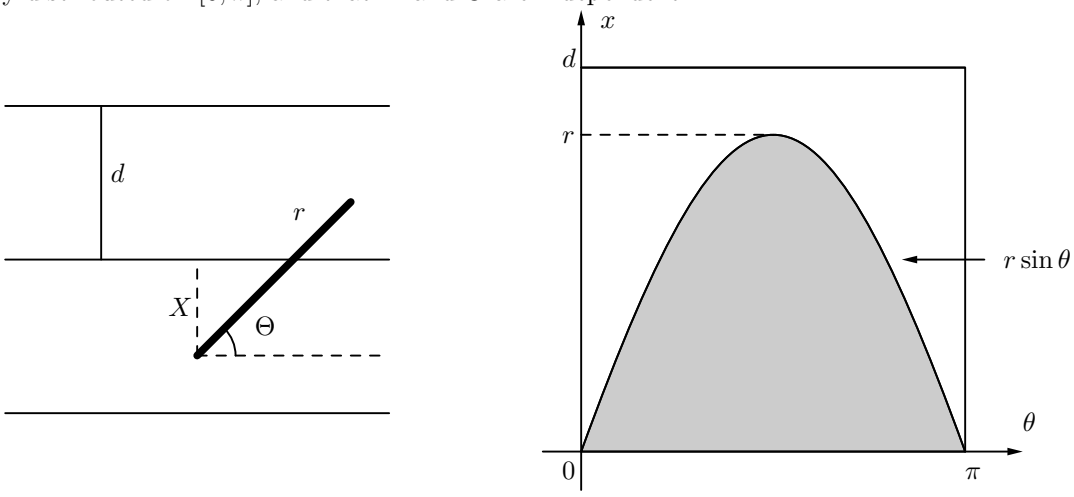
We do not know the value of p, but it is always the case that $p(1-p)\leq \frac{1}{4}$, with equality occurring when $p=\frac{1}{2}$, so to ensure that we have the required bound we need $n\geq (1.96/2\varepsilon)^2$. For example, if we take $\varepsilon=0.02$, so that the estimate of the percentage of Labour voters is accurate to within 2 percentage points with 95% probability we would need to take a sample with $n\geq 2401$. The typical sample size in opinion polls is $n\approx 1000$ which corresponds to an error $\varepsilon\approx 0.03$.

19.10 Geometric probability

19.10.1 Buffon's needle

Consider a needle of length r which is thrown at random on to a plane surface on which there are parallel straight lines at distance $d>r$ apart. What is the probability that the needle intersects one of the lines?

Think of the parallel lines running West-East and let X be the distance from the point representing the Southern end of the needle to the nearest line North of that point, if the needle is parallel to the lines, take the right-hand end point. Let Θ be the angle that the needle makes with the West-East lines. Then we will assume that X is uniformly distributed on $[0,d)$ and Θ is uniformly distributed on $[0,\pi]$, and that X and Θ are independent.



The joint probability density of (X,Θ) is

$$f(x,)=\begin{cases}\frac{1}{\pi d}, & 0\leq x<d,\ 0\leq\theta\leq\pi,\\ 0 & \text{otherwise.}\end{cases} \tag{19.10.1}$$

Then if A is the shaded area in the $x-\theta$ plane illustrated, the probability that the needle intersects a line is

$$\mathbb{P}(X\leq r\sin\Theta)=\int\int_A f(x,\theta)dxd\theta=\int_0^\pi\int_0^{r\sin\theta}\frac{1}{\pi d}dxd\theta=\frac{r}{\pi d}\int_0^\pi\sin\theta d\theta=\frac{2r}{\pi d}. \tag{19.10.2}$$

This probability was derived in 1777 by the French mathematician and naturalist Georges Louis Leclerc, Comte de Buffon, who suggested a method of approximating the value of π by repeatedly dropping a needle and estimating the probability that a line is intersect (and hence the value of π) by recording the proportion of times that the needle crosses a line. First

note that if $X \sim \mathcal{N}(\mu, \sigma^2)$, where σ^2 is small, and $g : \mathbb{R} \to \mathbb{R}$ then

$$g(X) = g(\mu) + (X - \mu)g'(\mu) + \cdots \sim \mathcal{N}\left(g(\mu), (g'(\mu))^2\sigma^2\right), \tag{19.10.3}$$

where the symbol $\simeq$ may be read as "approximately distributed as". Now, if $S_n = X_1 + \cdots + X_n$ denotes the total number of times that the needle intersects a line in n drops of the needle, where X_i is the indicator of the event that a line is intersected on the ith drop, then $S_n \sim \text{Bin}(n, p)$ where $p = 2r/(\pi d)$. By the Central Limit Theorem we have that $S_n/n \sim \mathcal{N}(p, p(1-p)/n)$. Let $g(x) = 2r/(xd)$, so that $g(p) = \pi$ and $g'(p) = -\pi^2 d/(2r)$. We see that an estimate of π is given by $\widehat{\pi} = g(S_n/n)$, where

$$\widehat{\pi} \sim \mathcal{N}\left(\pi, \frac{\pi^2}{2rn}(\pi d - 2r)\right). \tag{19.10.4}$$

One small difficulty that arises when one tries to replicate Buffon's procedure for estimating π on a computer is how to do the simulation without using the value of π to take random samples of Θ from the uniform distribution on $(0, \pi]$. One way around this is to generate a sample (X, Y) which has the uniform distribution over a quadrant of the circle centre the origin and of unit radius as follows:

Step 1. generate independent X and Y each with the uniform distribution on $[0, 1]$,

Step 2. if $X^2 + Y^2 > 1$ repeat Step 1, otherwise take (X, Y).

Now set $\Theta = 2\arctan(Y/X)$, which will be uniform on $(0, \pi)$.

19.10.2 Bertrand's Paradox

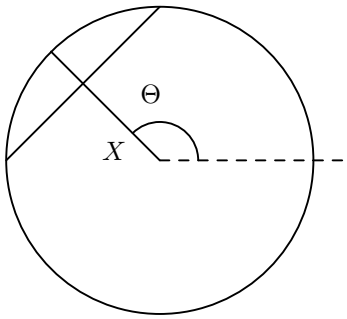
This results from the following question posed by Bertrand in 1889: What is the probability that a chord chosen at random joining two points of a circle of radius r has length $\leq r$?

The difficulty with the question is that there is not a unique interpretation of what it means for a chord to be chosen 'at random', there are different ways to do this and they lead to different probabilities for the length, C, of the chord being less than r. We will consider two approaches.

Approach 1. Let X be a random variable having the uniform distribution on $(0, r)$ and let Θ be a random variable, independent of X, with the uniform distribution on $(0, 2\pi)$.

The length of the chord is

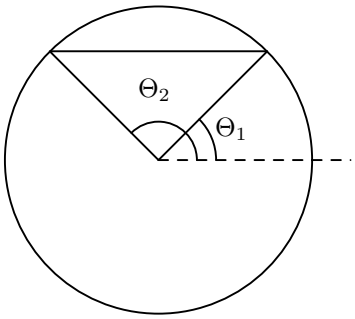
$C = 2\sqrt{r^2 - X^2}$

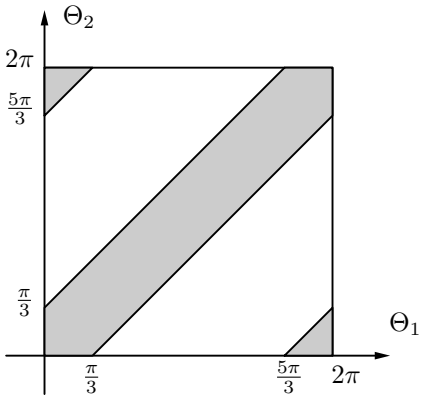


Construct the chord by taking a reference line (the x-axis, say) and drawing the radius at angle Θ with the line. Then take the chord at right angles to this radius at distance X from the centre of the circle. We then have

$$\mathbb{P}(C \leq r) = \mathbb{P}\left(4(r^2 - X^2) \leq r^2\right) = \mathbb{P}\left(\sqrt{3}r/2 \leq X\right) = 1 - \sqrt{3}/2 \approx 0.134. \tag{19.10.5}$$

Approach 2. Let Θ_1 and Θ_2 be independent random variables each with the uniform distribution on $(0, 2\pi)$. Take the end points of the chord as the points $(r\cos\Theta_i, r\sin\Theta_i)$, $i = 1, 2$, on the circumference of the circle, where the angles are measured from some reference line. The length of the chord is $C = 2r\sin\left(\frac{|\Theta_1 - \Theta_2|}{2}\right)$.





The probability is then

$$\mathbb{P}(C \le r) = \mathbb{P}\left(\sin\left(\frac{|\Theta_1 - \Theta_2|}{2}\right) \le \frac{1}{2}\right) = \mathbb{P}\left(|\Theta_1 - \Theta_2| \le \frac{\pi}{3} \text{ or } |\Theta_1 - \Theta_2| \ge \frac{5\pi}{3}\right), \tag{19.10.6}$$

this probability is the area of the shaded region in the square divided by $(2\pi)^2$ which gives the probability to be $\frac{1}{3} \approx 0.3333$. This probability is the same as when you take one end of the chord as fixed (say on the reference line) and take the other end at a point at angle Θ uniformly distributed on $(0, 2\pi)$.

It should be noted that both probabilities may arise as the outcomes of physical experiments which are choosing the chord 'at random'. For example, the probability in Approach 1 would be found if a circular disc of radius r is thrown randomly onto a table on which parallel lines at distance $2r$ are drawn, the chord would be determined by the unique line intersecting the circle and the distribution of the distance of center of the circle to the nearest line would be uniform on $(0, r)$. By contrast, the probability in Approach 2 is obtained if the disc is pivoted on a point on its circumference, which is on a given straight line and the disc is spun around that point, then the chord would be determined by the intersection of the given line and the circumference of the disc.

19.11 Problems

19.11.1 Classical probability

Problem 19.11.1. From a table of random digits, k are chosen. What are the probabilities that for $0 \le r \le 9$, (i) no digit exceed r? (ii) r is the greatest digit drawn?

Solution. Let $\Omega = \{\{i_1, \ldots, i_k\}, 0 \le i_j \le 9, j = 1, \ldots, k\}$.

(i) $\mathbb{P}(\text{no digit exceed } r) = \mathbb{P}(\text{all } i_j \le r) = \left(\frac{r+1}{10}\right)^k$.

(ii) $\mathbb{P}(r \text{ is the greatest digit drawn} = \mathbb{P}(\text{all } i_j \le r, \text{ but not all} \le r-1) = \mathbb{P}(\text{all } i_j \le r) - \mathbb{P}(\text{all } i_j \le r-1) = \left(\frac{r+1}{10}\right)^k - \left(\frac{r}{10}\right)^k$.

Problem 19.11.2. Five mices are chosen (without replacement) from a litter, three of which are tagged A, B and C. The probability that all three tagged mice are chosen is twice the probability that A is the only tagged mouse chosen. How many mice are three in the litter?

Solution. The probability all three tagged mice are chosen is $\binom{n-3}{2} / \binom{n}{5}$, while the probability only A is chosen is $\binom{n-3}{4} / \binom{n}{5}$. This leads to the equation

$$\frac{(n-3)(n-4)}{2!} = 2\frac{(n-3)(n-4)(n-5)(n-6)}{4!} \tag{19.11.1}$$

which gives $6 = n^2 - 11n + 30$, or $n^2 - 11n + 24 = 0$, so that $n = 8$ or $n = 3$; the latter cannot happen so we conlude that $n = 8$.

Problem 19.11.3. Two cards are taken at random from an ordinary pack of 52 cards. Find the probabilities that

(i) both cards are aces (event A).

(ii) the pair of cards includes an ace (event B).

(iii) the pair of cards includes the ace of hearts (event C).

Show that $\mathbb{P}(A|B) \neq \mathbb{P}(A|C)$.

Solution. (i)-(iii)

$$\mathbb{P}(A) = \frac{\binom{4}{2}}{\binom{52}{2}} = \frac{4\times 3}{52\times 51} = \frac{1}{221}, \quad \mathbb{P}(B) = 1 - \frac{\binom{48}{2}}{\binom{52}{2}} = \frac{48\times 47}{52\times 51} = \frac{33}{221}, \quad \mathbb{P}(C) = 1 - \frac{\binom{51}{1}}{\binom{52}{2}} = \frac{2\times 51}{52\times 51} = \frac{1}{26}. \tag{19.11.2}$$

Also, we have

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(A\cap B)}{\mathbb{P}(B)} = \frac{\mathbb{P}(A)}{\mathbb{P}(B)} = \frac{1}{33}, \quad \mathbb{P}(A|C) = \frac{\mathbb{P}(A\cap C)}{\mathbb{P}(C)} = \frac{3}{\binom{52}{2}} / \frac{1}{26} = \frac{1}{17}. \tag{19.11.3}$$

Thus, $\mathbb{P}(A|B) \neq \mathbb{P}(A|C)$.

Problem 19.11.4. Sarah collects figures from cornflakes packets. Each packet contains one figure, and n distinct figures make a complete set. Show that the expected number of packets Sarah needs to buy to collect a complete set is $n\sum_{i=1}^{n} i^{-1}$. How much easier is it to collet half the set than the complete set?

Solution. The total number is $N = 1 + \sum_{i=1}^{n-1} X_i$, where $\mathbb{P}(X_i = k) = (i/n)^{k-1}(1-i/n)$, for $k = 1, 2, \ldots$. We have

$$\mathbb{E}X_i = \sum_{k=1}^{\infty} k\left(\frac{i}{n}\right)^{k-1}\left(1-\frac{i}{n}\right) = \frac{n}{n-i}. \tag{19.11.4}$$

It follows that $\mathbb{E}N = n\sum_{i=1}^{n}\frac{1}{i}$.

The expected number of packets Sarah needs to buy to collet half is

$$\sum_{i=n/2}^{n}\frac{n}{i} = n\sum_{i=n/2}^{n}\frac{1}{n}\frac{1}{i/n} \approx n\int_{1/2}^{1}\frac{1}{x}dx = n\ln 2. \tag{19.11.5}$$

Problem 19.11.5. Mary tosses two coins and John tosses one coin. What is the probability that Mary gets strictly more heads than John? Answer the same question if Mary tosses three coins and John tosses two. Make a conjecture for the same probability when Mary tosses $n+1$ coins and John tosses n. Can you prove your conjecture?

Solution. If M_H and J_H denote the number of heads for Mary and John, respectively, then in the first case

$$\mathbb{P}(M_H > J_H) = \mathbb{P}(M_H = 2) + \mathbb{P}(M_H = 1, J_H = 0) = 1/4 + 1/4 = 1/2 \tag{19.11.6}$$

Similarly you may see that the probability for 3 and 2 coins is 1/2, so the conjecture is that for the general case it is the same. With the obvious notation, $M_H + M_T = n+1$ and $J_H + J_T = n$ so that the event

$$\{M_H > J_H\}^c = \{n+1-M_T \leq n - J_T\} = \{1 + J_T \leq M_T\} = \{J_T < M_T\} \tag{19.11.7}$$

that is, exactly one of the events 'Mary get more heads' and 'Mary gets more tails' must occur, but these must have equal probabilities.

19.11.2 Theoretical problems

Problem 19.11.6. Let X be a positive random variable taking only finitely many values in $\mathbb{R}^+$. Show that

$$\mathbb{E}\left(\frac{1}{X}\right) \geq \frac{1}{\mathbb{E}X} \tag{19.11.8}$$

and that the inequality is strict unless $\mathbb{P}(X = \mathbb{E}X) = 1$.

Solution. Since $\frac{1}{X}$ is convext, we can use Jensen's inequality (Theorem 19.3.22) to get the $\mathbb{E}\left(\frac{1}{X}\right) \geq \frac{1}{\mathbb{E}X}$.

Let $x_i, i = 1, \ldots, n$ be Ω of X, each with probability p_i. Thus, $\mathbb{E}\left(\frac{1}{X}\right) = \frac{1}{\mathbb{E}X}$ gives us

$$\sum_{i=1}^{n}\frac{p_i}{x_i} = \frac{1}{\sum_{j=1}^{n} p_j x_j} \;\Rightarrow\; \sum_{i=1}^{n}\frac{p_i\prod_{k\neq i} x_k}{\prod_{k=1}^{n} x_k} = \frac{1}{\sum_{j=1}^{n} p_j x_j} \;\Rightarrow\; \prod_{k=1}^{n} x_k = \sum_{j=1}^{n} p_j x_j\left(\sum_{i=1}^{n} p_i \prod_{k\neq i} x_k\right) \tag{19.11.9}$$

After the expansion, we have

$$\begin{aligned}\prod_{k=1}^{n} x_k &= \sum_{j=1}^{n} p_j^2 \prod_{i=1}^{n} x_i + \sum_{j=1}^{n}\sum_{i\neq j} p_i p_j \frac{x_j}{x_i} \prod_{k=1}^{n} x_k \\ \left(\sum_{j=1}^{n} p_j\right)^2 &= \sum_{j=1}^{n} p_j^2 + \sum_{j=1}^{n}\sum_{i>j} p_i p_j \left(\frac{x_j}{x_i} + \frac{x_i}{x_j}\right) \\ 0 &= \sum_{j=1}^{n}\sum_{i>j} p_i p_j \left(\frac{x_j}{x_i} + \frac{x_i}{x_j} - 2\right) = \sum_{j=1}^{n}\sum_{i>j} p_i p_j \frac{(x_i - x_j)^2}{x_i x_j} \end{aligned} \tag{19.11.10}$$

Since $x_i > 0$, we have $x_i = x_j, \forall i, j$ which implies that $\mathbb{P}(X = \mathbb{E}X) = 1$.

Problem 19.11.7. How large a random sample should be taken from a distribution in order for the probability to be at least 0.99 that the sample mean will be within two standard deviations of the mean of the distribution? Use Chebyshev's inequality to determine a sample size that will be sufficient, whatever the distribution.

Solution. Chebyshev's inequality (Theorem 19.3.21) says

$$\mathbb{P}\left(|X - \mu| \geq k\sigma\right) \leq \frac{1}{k^2} \tag{19.11.11}$$

Now $\hat{\mu} = \frac{1}{N}\sum_{i=1}^{N} X_i \sim \mathcal{D}(\mu, \frac{\sigma^2}{N})$ if we let X_i be i.i.d. Then we need

$$\mathbb{P}\left(|\hat{\mu} - \mu| \geq 2\sigma\right) = \mathbb{P}\left(|\hat{\mu} - \mu| \geq 2\sqrt{N}\frac{\sigma}{\sqrt{N}}\right) \leq \frac{1}{4N} = 1 - 0.99 = 0.01 \tag{19.11.12}$$

Thus a sufficient sample space has size 25.

Problem 19.11.8. Let X and Y be integrable random variables and suppose that

$$\mathbb{E}\left(X|Y\right) = Y \quad \text{and} \quad \mathbb{E}\left(Y|X\right) = X \text{ a.s.} \tag{19.11.13}$$

Show that $X = Y$ a.s.

Solution. Fix $c \in \mathbb{R}$. As $\{Y \leq c\} \in \sigma(Y)$ and $\mathbb{E}\left(X|Y\right) = Y$ a.s., $\mathbb{E}\left(X\mathbb{1}_{\{Y\leq c\}}\right) = \mathbb{E}\left(Y\mathbb{1}_{\{Y\leq c\}}\right)$, and hence

$$0 = \mathbb{E}\left((X-Y)\mathbb{1}_{\{Y\leq c\}}\right) = \mathbb{E}\left((X-Y)\mathbb{1}_{\{X>c, Y\leq c\}}\right) + \mathbb{E}\left((X-Y)\mathbb{1}_{\{X\leq c, Y\leq c\}}\right) \tag{19.11.14}$$

By symmetry, we also have that

$$0 = \mathbb{E}\left((Y-X)\mathbb{1}_{\{X\leq c\}}\right) = \mathbb{E}\left((Y-X)\mathbb{1}_{\{X\leq c, Y>c\}}\right) + \mathbb{E}\left((Y-X)\mathbb{1}_{\{X\leq c, Y\leq c\}}\right) \tag{19.11.15}$$

By adding these equations, we then see that

$$0 = \mathbb{E}\left((X-Y)\mathbb{1}_{\{X>c, Y\leq c\}}\right) + \mathbb{E}\left((Y-X)\mathbb{1}_{\{X\leq c, Y>c\}}\right) \tag{19.11.16}$$

Each of these terms is itself nonnegative and therefore, from the above, equal to 0. It follows that $\mathbb{P}\left(X > c, Y \leq c\right) = 0$ and $\mathbb{P}\left(X \leq c, Y > c\right) = 0$. As $c \in \mathbb{R}$ was arbitrary, we conclude from these equations that $X = Y$ a.s..

Problem 19.11.9 (coprime numbers)**.** Given two randomly chosen integers a and b, it is reasonable to ask how likely it is that a and b are coprime.

Solution. In this determination, it is convenient to use the characterization that a and b are coprime if and only if no prime number divides both of them (see Fundamental theorem of arithmetic[20]).

Informally, the probability that any number is divisible by a prime (or in fact any integer) p is $1/p$; for example, every 7th integer is divisible by 7. Hence the probability that two numbers are both divisible by this prime is $1/p^2$, and the probability that at least one of them is not is $1 - 1/p^2$. For distinct primes, these divisibility events are mutually independent. For

[20] need link

example, in the case of two events, a number is divisible by p and q if and only if it is divisible by pq; the latter event has probability $1/pq$. (Independence does not hold for numbers in general, but holds for prime numbers.) Thus the probability that two numbers are coprime is given by a product over all primes,

$$\prod_p^\infty \left(1 - \frac{1}{p^2}\right) = \left(\prod_p^\infty \frac{1}{1-p^{-2}}\right)^{-1} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.607927102 \approx 61\%. \tag{19.11.17}$$

Here ζ refers to the Riemann zeta function[21], the identity relating the product over primes to $\zeta(2)$ is an example of an Euler product, and the evaluation of $\zeta(2)$ as $\pi^2/6$ is the Basel problem, solved by Leonhard Euler in 1735. In general, the probability of k randomly chosen integers being coprime is $1/\zeta(k)$.

The notion of a 'randomly chosen integer' in the preceding paragraphs is not rigorous. One rigorous formalization is the notion of natural density: choose the integers a and b randomly between 1 and an integer N. Then, for each upper bound N, there is a probability P_N that two randomly chosen numbers are coprime. This will never be exactly $6/\pi^2$, but in the limit as $N \to \infty$, the probability P_N approaches $6/\pi^2$. This theorem was proved by Ernesto Cesro in 1881. For a more rigorous proof, see Hardy-Wright [1].

Problem 19.11.10. Let f be a bounded continuous function on $(0,\infty)$, having Laplace transform

$$\hat{f}(\lambda) = \int_0^\infty e^{-\lambda x} f(x)dx, \quad \lambda \in (0,\infty). \tag{19.11.18}$$

Let $(X_n : n \in \mathbb{N})$ be a sequence of independent exponential random variables, of parameter λ. Show that $\hat{f}$ has derivatives of all orders on $(0,\infty)$ and that, for all $n \in \mathbb{N}$, for some $C(\lambda, n) \neq 0$ independent of f, we have

$$(d/d\lambda)^{n-1}\hat{f}(\lambda) = C(\lambda, n)\mathbb{E}(f(S_n)) \tag{19.11.19}$$

where $S_n = X_1 + \cdots + X_n$. Deduce that if $\hat{f} \equiv 0$ then also $f \equiv 0$.

Solution. Let $\epsilon > 0$. Then

(i) $x \mapsto e^{-\lambda x} f(x)$ is integrable on for all $\lambda \in (\epsilon, \infty)$.

(ii) $\lambda \mapsto e^{-\lambda x} f(x)$ is infinitely differentiable on (ϵ, ∞) for all x.

(iii) $x \mapsto \frac{\partial}{\partial \lambda^n}(e^{-\lambda x} f(x)) = (-x)^n e^{-\lambda x} f(x)$ is integrable (on $\mathbb{R}_+$) for all $\lambda \in (\epsilon, \infty)$, as $\left|(-x)^n e^{-\lambda x} f(x)\right| \leq x^n e^{-\epsilon x}$, and $x^n e^{-\epsilon x}$ is integrable.

These conditions allow for differentiation under the integral sign any number of times (by Theorem 15.3.29), for all $\lambda \in (\epsilon, \infty)$. But ϵ was arbitrary so the same is true for $\lambda \in (0, \infty)$. Thus

$$\frac{d^{n-1}\hat{f}(\lambda)}{d\lambda^{n-1}} = \int_0^\infty (-x)^{n-1} e^{-\lambda x} f(x)dx$$

Now $S_n \sim \Gamma(n, \lambda)$ which has pdf $e^{-\lambda x}\lambda^n x^{n-1}/(n-1)!$. So by Proposition 19.3.16,

$$\frac{d^{n-1}\hat{f}(\lambda)}{d\lambda^{n-1}} = \frac{(n-1)!(-1)^{n-1}}{\lambda^n} \int_0^\infty \frac{\lambda^n x^{n-1}}{(n-1)!} e^{-\lambda x} f(x)dx = \frac{(n-1)!(-1)^{n-1}}{\lambda^n}\mathbb{E}(f(S_n)). \tag{19.11.20}$$

Moreover, since $S_n/n \sim \Gamma(n, n\lambda)$, we have

$$\left.\frac{d\hat{f}}{d\lambda^{n-1}}\right|_{n\lambda} = \int_0^\infty (-x)^{n-1} e^{-n\lambda x} f(x)dx = \frac{(n-1)!(-1)^{n-1}}{(n\lambda)^n}\mathbb{E}(f(S_n/n))$$

Thus if $\hat{f} \equiv 0$ then $\mathbb{E}(f(S_n/n)) = 0$ for all n. But by the strong law of large numbers (Theorem 19.9.9), since $\mathbb{E}(X) = \frac{1}{\lambda}$,

$$1 = \mathbb{P}(S_n/n \to 1/\lambda) = \mathbb{P}(f(S_n/n) \to f(1/\lambda)), \tag{19.11.21}$$

[21] need link

where in the last step we have used the fact that f is continuous. As f is bounded, by bounded convergence theorem (Theorem 19.3.10) we have

$$0 = \lim_{n\to\infty} \mathbb{E}(f(S_n/n)) = \mathbb{E}\left(\lim_{n\to\infty} f(S_n/n)\right) = f(1/\lambda).$$

This is true for all λ, so $f \equiv 0$.

Problem 19.11.11. For each $n \in \mathbb{N}$, there is a unique probability measure μ_n on the unit sphere $S^{n-1} = \{x \in \mathbb{R}^n : |x| = 1\}$ such that $\mu_n(A) = \mu_n(UA)$ for all Borel sets A and all orthogonal $n \times n$ matrices U. Fix $k \in \mathbb{N}$ and, for $n \geq k$, let γ_n denote the probability measure on $\mathbb{R}^k$ which is the law of $\sqrt{n}(x_1, \ldots, x_k)$ under μ_n. Show

(i) if $X \sim \mathcal{N}(0, I_n)$ then $X/|X| \sim \mu_n$,

(ii) if $(X_n : n \in \mathbb{N})$ is a sequence of independent $\mathcal{N}(0,1)$ random variables and if $R_n = (X_1^2 + \cdots + X_n^2)^{\frac{1}{2}}$ then $R_n/\sqrt{n} \to 1$ a.s.,

(iii) for all bounded continuous functions f on $\mathbb{R}^k$, $\gamma_n(f) \to \gamma(f)$, where γ is the standard Gaussian distribution on $\mathbb{R}^k$.

Solution. (i) Since $U^{-1}X \sim \mathcal{N}(0, I_n)$ (U is orthogonal) and $|X| = \left|U^{-1}X\right|$,

$$\mu_{X/|X|}(A) = \mathbb{P}(X/|X| \in A) = \mathbb{P}(U^{-1}X/\left|U^{-1}X\right| \in A) = \mathbb{P}(U^{-1}X/|X| \in A) = \mathbb{P}(X/|X| \in UA) = \mu_{X/|X|}(UA).$$

(ii) By of the strong law of large number,

$$\frac{X_1^2 + \cdots + X_n^2}{n} \to 1, \quad \text{a.s..} \tag{19.11.22}$$

Also, with the fact that $\sqrt{\cdot}$ is continuous, we have $R_n/\sqrt{n} \to 1$ a.s..

(iii) Let $g : x \mapsto \sqrt{n}(x_1, \ldots, x_k)$. Then

$$\gamma_n(f) = \mu_n(f \circ g) = \mu_{X/|X|}(f \circ g) = \mathbb{E}(f \circ g(X/|X|)) = \mathbb{E}\left(f\left(\frac{X_1}{\left(\frac{R_n}{\sqrt{n}}\right)}, \ldots, \frac{X_k}{\left(\frac{R_n}{\sqrt{n}}\right)}\right)\right). \tag{19.11.23}$$

By the continuity of f and (ii),

$$f\left(\frac{X_1}{\left(\frac{R_n}{\sqrt{n}}\right)}, \ldots, \frac{X_k}{\left(\frac{R_n}{\sqrt{n}}\right)}\right) \to f\left(\frac{X_1}{\left(\lim_{n\to\infty}\frac{R_n}{\sqrt{n}}\right)}, \ldots, \frac{X_k}{\left(\lim_{n\to\infty}\frac{R_n}{\sqrt{n}}\right)}\right) = f(X_1, \ldots, X_k) \quad \text{a.s..} \tag{19.11.24}$$

Then by bounded convergence theorem (Theorem 19.3.10),

$$\lim \gamma_n(f) = \lim_{n\to\infty} \mathbb{E}\left(f\left(\frac{X_1}{\left(\frac{R_n}{\sqrt{n}}\right)}, \ldots, \frac{X_k}{\left(\frac{R_n}{\sqrt{n}}\right)}\right)\right) = \mathbb{E}(f(X_1), \ldots, f(X_k)) = \gamma(f). \tag{19.11.25}$$

Problem 19.11.12. Let (X_k) be a sequence of independent, identically distributed random variables, each with mean μ and variance σ^2. Show that

$$\sum_{k=1}^n \left(X_k - \overline{X}\right)^2 = \sum_{k=1}^n (X_k - \mu)^2 - n\left(\overline{X} - \mu\right)^2 \tag{19.11.26}$$

where $\overline{X} = n^{-1}\sum_{k=1}^n X_k$. Prove that, if $\mathbb{E}\left[(X_1 - \mu)^4\right] < \infty$, then for every $\epsilon > 0$

$$\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^n \left(X_k - \overline{X}\right)^2 - \sigma^2\right| > \epsilon\right\} \to 0 \text{ as } n \to \infty. \tag{19.11.27}$$

Solution. We have $\sum_{k=1}^n (X_k - \overline{X})^2 = \sum_{k=1}^n X_k^2 + n\overline{X}^2 - 2\overline{X}\sum_{k=1}^n X_k = \sum_{k=1}^n X_k^2 - n\overline{X}^2$, thus,

$$\sum_{k=1}^n (X_k - \mu)^2 - n\left(\overline{X} - \mu\right)^2 = \sum_{k=1}^n X_k^2 + n\mu^2 - 2\mu\sum_{k=1}^n X_k - n\overline{X}^2 + 2n\mu\overline{X} - n\mu^2 = \sum_{k=1}^n X_k^2 - n\overline{X}^2 = \sum_{k=1}^n (X_k - \overline{X})^2$$

Hence we have

$$\begin{aligned}
&\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}\left(X_k-\overline{X}\right)^2-\sigma^2\right|>\epsilon\right\}\\
=\;&\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}(X_k-\mu)^2-\sigma^2-(\overline{X}-\mu)^2\right|>\epsilon\right\}\le\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}(X_k-\mu)^2-\sigma^2\right|+(\overline{X}-\mu)^2>\epsilon\right\}\\
=\;&\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}(X_k-\mu)^2-\sigma^2\right|+(\overline{X}-\mu)^2>\epsilon,(\overline{X}-\mu)^2>\frac{\epsilon}{2}\right\}+\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}(X_k-\mu)^2-\sigma^2\right|+(\overline{X}-\mu)^2>\epsilon,(\overline{X}-\mu)^2\le\frac{\epsilon}{2}\right\}\\
\le\;&\mathbb{P}\left\{(\overline{X}-\mu)^2>\frac{\epsilon}{2}\right\}+\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}(X_k-\mu)^2-\sigma^2\right|>\frac{\epsilon}{2}\right\}
\end{aligned}$$

Applying Chebyshev's inequality (Theorem 19.3.21), we have

$$\mathbb{P}\left\{\left|\frac{1}{n}\sum_{k=1}^{n}\left(X_k-\overline{X}\right)^2-\sigma^2\right|>\epsilon\right\}\le\frac{\mathbb{E}\left[(\overline{X}-\mu)^2\right]}{\epsilon/2}+\frac{2\mathbb{E}\left[(X_1-\mu)^4\right]}{n\epsilon}=\frac{2\operatorname{Var}X_1}{n\epsilon}+\frac{2\mathbb{E}\left[(X_1-\mu)^4\right]}{n\epsilon}\to 0 \tag{19.11.28}$$

19.11.3 Random variables

Problem 19.11.13. Find approximately the probability that the number of 6's in 12000 rolls of a fair die is between 1900 and 2150.

Solution. Let N be the number of 6's, then

$$N\sim\operatorname{Bin}(12000,1/6)\approx\mathcal{N}(2000,10000/6)\quad(\mathcal{N}(np,np(1-p))) \tag{19.11.29}$$

by central limit theorem (Theorem 19.9.10). So that if $Z\sim\mathcal{N}(0,1)$,

$$\mathbb{P}(1900\le N\le 2150)=\mathbb{P}\left(-\frac{100}{\sqrt{10000/6}}\le\frac{N-2000}{\sqrt{10000/6}}\le\frac{150}{\sqrt{10000/6}}\right)=\mathbb{P}\left(-2.45\le Z\le 3.67\right)=\Phi(3.67)-\Phi(-2.45)$$

which is $0.9999-(1-0.9929)\approx 0.9928$.

Problem 19.11.14. Find the number c such that the probability is about $\frac{1}{2}$ that in 1000 tosses of a fair coin the number of heads lie between 490 and c.

Solution. The number $N\sim\operatorname{Bin}(1000,1/2)\approx\mathcal{N}(500,250)$, so that if $Z\sim\mathcal{N}(0,1)$,

$$\mathbb{P}(490\le N\le c)=\mathbb{P}\left(-\frac{10}{\sqrt{250}}\le\frac{N-500}{\sqrt{250}}\le\frac{c-500}{\sqrt{250}}\right)\approx\mathbb{P}\left(-0.6324\le Z\le\frac{c-500}{\sqrt{250}}\right), \tag{19.11.30}$$

which gives is $\Phi((c-500)/\sqrt{250})-0.2643=0.5$, so that $c=500+0.72\sqrt{250}\approx 511$.

Problem 19.11.15. If X, Y and Z are independent random variables each uniformly distributed on $(0,1)$, show that $(XY)^Z$ is also uniformly distributed on $(0,1)$.

Solution. It is sufficient to show that $-\log\left((XY)^Z\right)=Z(-\log X-\log Y)$ has the exponential distribution with parameter 1. Equivalently, show that if random variables $X\sim U(0,1)$ and $Y\sim\Gamma(2,1)$ are independent then $XY\sim\mathcal{E}(1)$. The joint pdf of X and Y is

$$f(x,y)=\begin{cases}ye^{-y} & 0<x<1,y>0\\ 0 & \text{otherwise}\end{cases} \tag{19.11.31}$$

Now put $U=XY,V=X/Y$, so that $X=\sqrt{UV}$ and $Y=\sqrt{U/V}$, and the Jacobian of the transformation is

$$\begin{vmatrix}\frac{\partial x}{\partial u} & \frac{\partial x}{\partial v}\\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v}\end{vmatrix}=\begin{vmatrix}\frac{1}{2}\sqrt{\frac{v}{u}} & \frac{1}{2}\sqrt{\frac{u}{v}}\\ \frac{1}{2\sqrt{uv}} & -\frac{\sqrt{u}}{2v^{3/2}}\end{vmatrix}=-\frac{1}{4v}-\frac{1}{4v}=-\frac{1}{2v} \tag{19.11.32}$$

and the joint density of U and V is

$$g(u,v) = \frac{\sqrt{u}}{2v^{3/2}} e^{-\sqrt{u/v}}, \quad 0 < uv < 1 \tag{19.11.33}$$

Integrating out v we get that the marginal density of U is

$$\int_0^{1/u} \frac{\sqrt{u}}{2v^{3/2}} e^{-\sqrt{u/v}} dv = \int_u^{\infty} e^{-z} dz = e^{-u}, \tag{19.11.34}$$

after making the substitution $z = \sqrt{u/v}$.

Problem 19.11.16. $X_1, X_2, \ldots$ from a sequence of independent random variables, each uniformly distributed on $(0,1)$. Let $N = \min\{n : X_1 + X_2 + \cdots + X_n \geq 1\}$. Calculate $\mathbb{P}(N \geq k)$ for each $k \geq 1$ and show that $\mathbb{E}N = e$.

Solution. For $x \leq 1$ let $a_n(x) = \mathbb{P}(X_1 + \cdots + X_n < x)$. Show by induction on n that $a_n(x) = x^n/n!$. It is true for $n = 1$ and then

$$a_{n+1}(x) \quad = \quad \int_0^1 \mathbb{P}(X_1 + \cdots + X_{n+1} < x | X_{n+1} = y) dy = \int_0^x a_n(x-y) dy = \int_0^x ((x-y)^n/n!) dy = x^{n+1}/(n+1)!$$

We then have $\mathbb{P}(N \geq k) = a_{k-1}(1) = 1/(k-1)!$ and

$$\mathbb{E}N = \sum_{k=1}^{\infty} \mathbb{P}(N \geq k) = \sum_{k=1}^{\infty} \frac{1}{(k-1)!} = e. \tag{19.11.35}$$

Problem 19.11.17. Derive the distribution of the sum of n independent random variables each having the Poisson distribution with parameter 1. Use the central limit theorem to prove that

$$e^{-n}\left(1 + \frac{n}{1!} + \frac{n^2}{2!} + \cdots + \frac{n^n}{n!}\right) \to \frac{1}{2} \quad \text{as } n \to \infty \tag{19.11.36}$$

Solution. For random variables $\{N_i\}$ which are i.i.d. with the Poisson distribution mean 1, let $M_n = N_1 + N_2 + \cdots + N_n$, then M_n has the Poisson distribution with mean n and by the central limit theorem (Theorem 19.9.10), for any x,

$$\lim_{n\to\infty} \mathbb{P}\left(\frac{M_n - n}{\sqrt{n}} \leq x\right) = \Phi(x), \tag{19.11.37}$$

where $\Phi(x)$ is the standard normal distribution function. Take $x = 0$, then $\Phi(x) = \frac{1}{2}$, and the left-hand side is

$$\lim_{n\to\infty} \mathbb{P}(M_n \leq n) = \lim_{n\to\infty} e^{-n}\left(1 + \frac{n}{1!} + \frac{n^2}{2!} + \cdots + \frac{n^n}{n!}\right). \tag{19.11.38}$$

Problem 19.11.18. How large a random sample should be taken from a normal distribution in order for the probability to be at least 0.99 that the sample mean will be within one standard deviation of the mean of the distribution? [Hint: $\Phi(2.58) = 0.995$.]

Solution. $X \sim \mathcal{N}(\mu, \sigma^2) \;\Rightarrow\; \bar{X} \sim \mathcal{N}(\mu, \sigma^2/n)$. Thus

$$\mathbb{P}\left(|\bar{X} - \mu| < \sigma\right) \geq 0.99 \;\Rightarrow\; \mathbb{P}\left(-\sqrt{n} < \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} < \sqrt{n}\right) \geq 0.99 = \Phi(2.58) - \Phi(-2.58) \tag{19.11.39}$$

So we get $\sqrt{n} \geq 2.58 \;\Rightarrow\; n \geq 7$.

Problem 19.11.19. Let X, Y be two independent Bernoulli random variables with parameter $p \in (0,1)$. Let $Z = \mathbb{1}_{\{X+Y=0\}}$. Compute $\mathbb{E}(X|Z)$ and $\mathbb{E}(Y|Z)$.

Solution. By symmetry $\mathbb{E}(X|Z) = \mathbb{E}(Y|Z)$ a.s., so it is enough to find just one. Note that, as $\{Z = 0\}$ and $\{Z = 1\}$ are non-null events that partition our sample space, it follows that (by Definition 19.4.3 and Definition 19.4.2)

$$\begin{aligned} \mathbb{E}(X|Z) &= \mathbb{E}(X|Z=0)\,\mathbb{1}_{\{Z=0\}} + \mathbb{E}(X|Z=1)\,\mathbb{1}_{\{Z=1\}} \\ &= \frac{\mathbb{E}\left(X\mathbb{1}_{\{Z=0\}}\right)}{\mathbb{P}(Z=0)}\mathbb{1}_{\{Z=0\}} + \frac{\mathbb{E}\left(X\mathbb{1}_{\{Z=1\}}\right)}{\mathbb{P}(Z=1)}\mathbb{1}_{\{Z=1\}} \end{aligned}$$

Recall that $Z = \mathbb{1}_{\{X+Y=0\}}$. It is immediate then that the second term above is equal to 0. For the first term, observe that

$$\mathbb{P}(Z=0) = 1 - \mathbb{P}(Z=1) = 1 - \mathbb{P}(X=0, Y=0) = 1 - (1-p)^2 = p(2-p) \tag{19.11.40}$$

and, additionally, that

$$\mathbb{E}\left(X\mathbb{1}_{\{Z=0\}}\right) = \mathbb{P}(Z=0, X=1) = \mathbb{P}(X=1) = p. \tag{19.11.41}$$

Putting the above into the earlier work, it follows that

$$\mathbb{E}(X|Z) = \frac{\mathbb{1}_{\{Z=0\}}}{2-p}. \tag{19.11.42}$$

19.11.4 Practical problems

Problem 19.11.20 (The Pólya urn model for contagion)**.** We start with an urn which contains one white ball and one black ball. At each second we choose a ball at random from the urn and replace it together with one more ball of the same colour. Is there a tendency to have a large fraction of balls of the same colour in the long run? [Computer simulations are interesting.] Calculate the probability that when n balls are in the urn, i of them are white.

Solution. Let $M_{n,k}$ is the event of having k white balls among n. Obviously, we have $\mathbb{P}(M_{2,1}) = 1$, $\mathbb{P}(M_{n,0}) = 0$ and $\mathbb{P}(M_{n,n}) = 0$. Taking $n \geq 3$ and $0 < k < n$, we have

$$\begin{aligned}\mathbb{P}(M_{n,k}) &= \mathbb{P}(\text{having chosen a white ball from } M_{n-1,k-1}) + \mathbb{P}(\text{having chosen a black ball from } M_{n-1,k}) \\ &= \frac{k-1}{n-1}\mathbb{P}(M_{n-1,k-1}) + \frac{n-1-k}{n-1}\mathbb{P}(M_{n-1,k})\end{aligned} \tag{19.11.43}$$

Thus, it is not difficult to derive that $\mathbb{P}(M_{n,k}) = \frac{1}{n-1}$.

Problem 19.11.21. We want to put n number into n positions. If number i is put in the ith position, we call it a fixed point. What the probability that there is no fixed point[22].

Solution. If we can define M_n the number of no-fixed point situations if we want to put n number into n positions. Thus,

$$M_n = (n-1)(M_{n-1} + M_{n-2}) \tag{19.11.44}$$

We know that there $n!$ possibilities for putting the numbers. Thus, we have define p_n the probability that there is no fixed point. Then

$$p_n = \frac{M_n}{n!} = \frac{n-1}{n!}(M_{n-1} + M_{n-2}) = \frac{n-1}{n} \cdot p_{n-1} + \frac{1}{n} \cdot p_{n-2}. \quad (*) \tag{19.11.45}$$

p_n can also be given by (for position 1, if it takes 1, then there is a fixed point)

$$p_n = \frac{1}{n} \cdot 0 + \frac{n-1}{n} \cdot \left(p_{n-1} + \frac{1}{n-1} \cdot p_{n-2}\right). \tag{19.11.46}$$

From $(*)$, we have

$$\begin{aligned} p_n - p_{n-1} &= \frac{-1}{n}(p_{n-1} - p_{n-2}) \\ &\vdots \\ p_3 - p_2 &= \frac{-1}{3}(p_2 - p_1) \end{aligned}$$

Thus, with $p_1 = 0$ and $p_2 = \frac{1}{2}$,

$$p_n - p_{n-1} = \frac{2 \cdot (-1)^{n-2}}{n!} \cdot (p_2 - p_1) = \frac{2 \cdot (-1)^{n-2}}{n!} \cdot \frac{1}{2} = \frac{(-1)^n}{n!} \tag{19.11.47}$$

Thus,

$$p_n = \sum_{i=2}^{n} \frac{(-1)^i}{i!} \to e^{-1} \quad \text{as } n \to \infty. \tag{19.11.48}$$

[22] this is called fixed point problem, see Grinstead-Snell [9]

Thus, we have

$$p_5 = \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} = \frac{11}{30}. \tag{19.11.49}$$

Problem 19.11.22. John chooses a sequence, such as HHH, and then Mary chooses a sequence, perhaps THH. A fair coin is tossed until on or other sequence occurs, when the coin is awarded to the person whose sequence has been observed. Advise Mary on which sequence she should choose for each (or at least some) of John's eight possible choices.

Solution. Let p be the probability that Mary's choice happens before John's choice when the first toss is H and q be the probability that Mary's choice happens before John's choice when the first toss is T. Thus, in the case that John chooses HHH and Mary chooses THH, we have

$$\begin{cases} p &= \underbrace{\frac{1}{4}0}_{HHH} + \underbrace{\frac{1}{4}q}_{HHT} + \underbrace{\frac{1}{8}1}_{HTHH} + \underbrace{\frac{1}{8}q}_{HTHT} + \underbrace{\frac{1}{4}q}_{HTT} = \frac{1}{8} + \frac{5}{8}q \\ q &= \underbrace{\frac{1}{4}1}_{THH} + \underbrace{\frac{1}{4}q}_{THT} + \underbrace{\frac{1}{8}1}_{TTHH} + \underbrace{\frac{1}{8}q}_{TTHT} + \underbrace{\frac{1}{4}q}_{TTT} = \frac{3}{8} + \frac{5}{8}q \end{cases} \quad \Rightarrow \quad \begin{cases} p &= \frac{3}{4} \\ q &= 1 \end{cases} \tag{19.11.50}$$

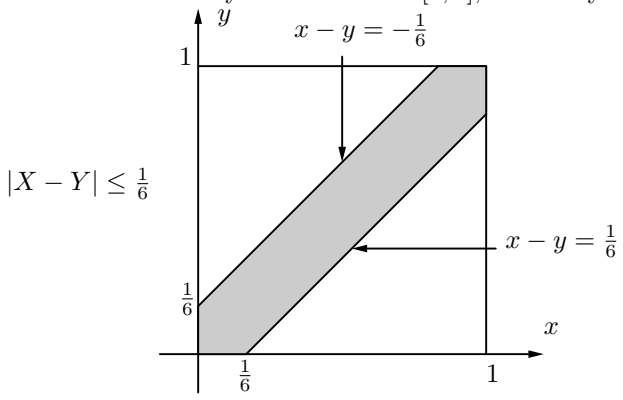
Thus, the probability that John wins the game is $\frac{1}{2}(p+q) = \frac{7}{8}$. Similarly, we have the probabilities of winning for Mary in the following table,

John \ Mary	HHH	HHT	HTH	HTT	THH	THT	TTH	TTT
HHH	-	1/2	3/5	3/5	**7/8**	7/12	7/10	1/2
HHT	1/2	-	1/3	1/3	**3/4**	3/8	1/2	3/10
HTH	2/5	**2/3**	-	1/2	1/2	1/2	5/8	5/12
HTT	2/5	**2/3**	1/2	-	1/2	1/2	1/4	1/8
THH	1/8	1/4	1/2	1/2	-	1/2	**2/3**	2/5
THT	5/12	5/8	1/2	1/2	1/2	-	**2/3**	2/5
TTH	3/10	1/2	3/8	**3/4**	1/3	1/3	-	1/2
TTT	1/2	7/10	7/12	**7/8**	3/5	3/5	1/2	-

where the bold probabilities maximize the value for given sequence chosen by John.

Problem 19.11.23. Alice and Bob agree to meet in the Copper Kettle after their Saturday lectures. They arrive at times that are indepedent and uniformly distributed between 12.00 and 1.00pm. Each is prepared to wait 10 minutes before leaving. Find the probability they meet.

Solution. If the times they arrive are X and Y uniformly distributed on $[0,1]$, then they meet if



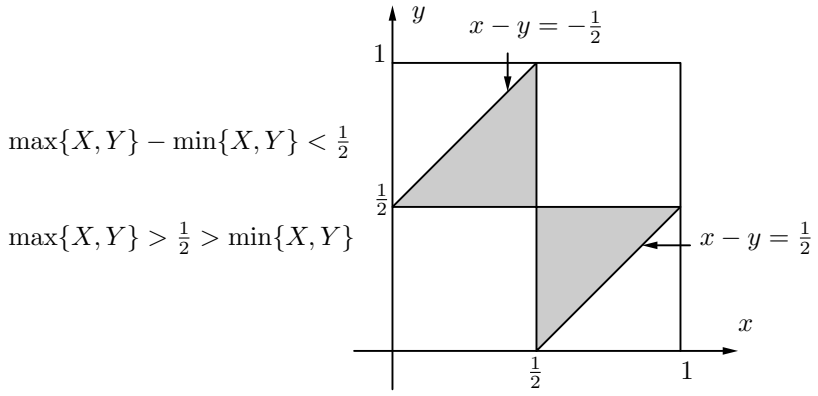
so the probability is the area of the shaded region which is $\frac{11}{36}$.

Problem 19.11.24. A unit stick is broken in two places:

(i) Two breaks are idependently and uniformly distributed along its length. What is the probability that the three pieces will make a triangle?

(ii) The first break is at a $U[0,1]$ point, and the second break is made by breaking the longer part at uniformly chosen position (the two breaks are otherwise independent). What is the probability that the three pieces will make a triangle?

Solution. (i) Let X and Y be independent $U[0,1]$ representing the positions of the breaks along the stick. The pieces are of length $A = \min\{X,Y\}$, $B = \max\{X,Y\} - \min\{X,Y\}$ and $C = 1 - \max\{X,Y\}$ and they form a triangle if $A + B > C$, $B + C > A$ and $C + A > B$. These translate to



and the probability is the area of the shaded region which is $\frac{1}{4}$.

(ii) If we choose the first break and then choose the second break is made by breaking the longer part, X and Y are no longer independent. we can only consider the case that X is in $[\frac{1}{2}, 1]$ due the symmetric property. Thus, Y is choosen in $[0, X]$ uniformly with density function $f(Y|X) = \frac{1}{X}$. Also, to satisfy the triangle conditions, we have

$$\begin{cases} y + (x - y) & > & 1 - x \\ y + (1 - x) & > & x - y \\ (1 - x) + (x - y) & > & y \end{cases} \Rightarrow \begin{cases} x & > & \frac{1}{2} \\ y & > & x - \frac{1}{2} \\ y & < & \frac{1}{2} \end{cases} \tag{19.11.51}$$

Thus, we have the probability

$$2\int_{\frac{1}{2}}^{1}\int_{x-\frac{1}{2}}^{\frac{1}{2}} \frac{1}{x} dy dx = 2\int_{\frac{1}{2}}^{1} \frac{1-x}{x} dx = 2\left(\ln x - x|_{\frac{1}{2}}^{1}\right) = 2\ln 2 - 1 \tag{19.11.52}$$

Problem 19.11.25 (candies in a jar (Zhou [18].P_{79}))**.** You are taking out candies one by one from a jar that has 10 red candies, 20 blue candies, and 30 green candies in it. What is the probability that there are at least 1 blue candy and 1 green candy left in the jar when you have taken out all the red candies?

Solution. Let T_r, T_b and T_g be the number that the last red, blue, and green candies are taken out respectively. To have at least 1 blue candy and 1 green candy left when all the red candies are taken out, we need to have $T_r < T_b$, $T_r < T_g$. In other words, we want to derive $\mathbb{P}(T_r < T_b, T_r < T_g)$. Thus,

$$\mathbb{P}(T_r < T_b, T_r < T_g) = \mathbb{P}(T_r < T_b < T_g) + \mathbb{P}(T_r < T_g < T_b). \tag{19.11.53}$$

$T_r < T_b < T_g$ means that the last candy is green ($T = 60$). Since each of the 60 candies are equally likely to be the last candy among them 30 are green ones, we have $\mathbb{P}(T_g = 60) = \frac{30}{60}$. Conditioned on $T_g = 60$, we need $\mathbb{P}(T_r < T_b | T_g = 60)$. Among the 30 red and blue candies, each candy is again equally likely to be the last candy and there are 20 blue candies, so

$$\mathbb{P}(T_r < T_b | T_g = 60) = \frac{20}{30} \;\Rightarrow\; \mathbb{P}(T_r < T_b < T_g) = \mathbb{P}(T_r < T_b | T_g = 60)\mathbb{P}(T_g = 60) = \frac{20}{30}\frac{30}{60}. \tag{19.11.54}$$

Similarly, we have

$$\mathbb{P}(T_r < T_g < T_b) = \frac{30}{40}\frac{20}{60}. \tag{19.11.55}$$

Therefore,

$$\mathbb{P}(T_r < T_b, T_r < T_g) = \frac{20}{30}\frac{30}{60} + \frac{30}{40}\frac{20}{60} = \frac{7}{12}. \tag{19.11.56}$$

Problem 19.11.26 (Zhou [18].P_{102})**.** 500 ants are randomly put on a 1-foot string (independent uniform distribution for each ant between 0 and 1). Each ant randomly moves toward one end of the string (equal probability to the left or right) at constant speed 1 foot/minute until it falls off at one end of the string. Also assume that the size of the ant is infinitely small. When two ants collide head-on, they both immediately change directions and keep on moving at 1 foot/min. What is the expected time for all ants to fall off the string?

Solution. When two ants collide head-on, both immediately change directions. What does it mean? The following diagram illustrates the key point:

$$\text{before collision: } \overset{A}{\rightarrow}\overset{B}{\leftarrow}, \quad \text{after collision: } \overset{A}{\leftarrow}\overset{B}{\rightarrow}, \quad \text{switch label: } \overset{B}{\leftarrow}\overset{A}{\rightarrow}. \tag{19.11.57}$$

When an ant A collides with another ant B, both switch direction. But if we exchange the ants' labels, it's like that the collision never happens, A continuous to move to the right and B moves to the left. Since the labels are random assigned anyway, collisions make no difference to the result. So we can assume that when two ants meet, each just keeps on going in its original direction. What about the random direction that each ant chooses? Once the collision is removed, we can use symmetry to argue that it makes no difference which direction that an ant goes either.

That means if an ant is put at the x-th foot, the expected value for it to fall off is just x min. If it goes in the other direction, simply set x to $1-x$. So the orginial problem is equivalent to the expected value of the maximum of 500 i.i.d. random variables with uniform distribution between 0 and 1. By Proposition 19.8.5, the answer is $\frac{500}{501}$ min.

Problem 19.11.27 (Zhou [18].P_{79})**.** Suppose 3 points are independently uniformly distributed on a circle. What's the probability that there exists a diameter such that all these 3 points are on the same side of that diameter? What about more general case for n points?

Solution. Suppose that these n points have the angles $\theta_1, \ldots, \theta_n$ with $\theta_i \sim \mathcal{U}(0, 2\pi)$ and let $\widehat{\theta}_n$ be size of the smallest interval containing all the points. Thus, for any $x \in [0, \pi]$,

$$\mathbb{P}\left(\widehat{\theta}_n \le x\right) = \mathbb{P}\left(\widehat{\theta}_{n-1} \le x, 0 \le \theta_n \le \widehat{\theta}_{n-1}\right) + 2\mathbb{P}\left(\theta_n \le x, \theta_n \ge \widehat{\theta}_{n-1}\right) \tag{19.11.58}$$

since θ_n could be at either side of the interval $[0, \widehat{\theta}_{n-1}]$. Thus, ($f_{\widehat{\theta}_{n-1}}$ is the density function of $\widehat{\theta}_{n-1}$)

$$\mathbb{P}\left(\widehat{\theta}_n \le x\right) = \int_0^x f_{\widehat{\theta}_{n-1}}(y) \int_0^y f_{\theta_n}(z) dz dy + 2\int_0^x f_{\theta_n}(z) \int_0^z f_{\widehat{\theta}_{n-1}}(y) dy dz. \tag{19.11.59}$$

We know that $\widehat{\theta}_{n-1}$ is independent of θ_n and thus $f_{\theta_n} = \frac{1}{2\pi}$. Thus,

$$\mathbb{P}\left(\widehat{\theta}_n \le x\right) = \frac{1}{2\pi}\int_0^x f_{\widehat{\theta}_{n-1}}(y) y dy + \frac{1}{\pi}\int_0^x \mathbb{P}\left(\widehat{\theta}_{n-1} \le z\right) dz \tag{19.11.60}$$

If $n = 3$, then $f_{\widehat{\theta}_2} = \frac{1}{\pi}$. Thus,

$$\mathbb{P}\left(\widehat{\theta}_2 \le x\right) = \frac{x}{\pi}, \qquad \mathbb{P}\left(\widehat{\theta}_3 \le x\right) = \frac{1}{2\pi}\int_0^x \frac{1}{\pi} y dy + \frac{1}{\pi}\int_0^x \frac{z}{\pi} dz = \frac{x^2}{4\pi^2} + \frac{x^2}{2\pi^2} = \frac{3x^2}{4\pi^2}. \tag{19.11.61}$$

Thus, by induction we assume $\mathbb{P}\left(\widehat{\theta}_n \le x\right) = n\left(\frac{x}{2\pi}\right)^{n-1}$ with $f_{\widehat{\theta}_n}(x) = n(n-1)\frac{x^{n-2}}{(2\pi)^{n-1}}$. Then

$$\begin{aligned}
\mathbb{P}\left(\widehat{\theta}_{n+1} \le x\right) &= \frac{1}{2\pi}\int_0^x f_{\widehat{\theta}_n}(y) y dy + \frac{1}{\pi}\int_0^x \mathbb{P}\left(\widehat{\theta}_n \le z\right) dz = \frac{1}{2\pi}\int_0^x \frac{n(n-1)y^{n-1}}{(2\pi)^{n-1}} dy + \frac{1}{\pi}\int_0^x n\left(\frac{z}{2\pi}\right)^{n-1} dz \\
&= \frac{1}{(2\pi)^n}(n-1)x^n + \frac{2}{(2\pi)^n}x^n = (n+1)\frac{x^n}{(2\pi)^n}.
\end{aligned}$$

Thus, let $x = \pi$, we have the probability is $\frac{n}{2^{n-1}}$.

Alternative Solution. Let's start at one point and clockwise label the point as $1, 2, \ldots, n$. The probability that all the remaining $N-1$ points from 2 to n are in the clockwise semicircle starting at point 1 (That is, if point 1 is at 12:00, point 2 to n) are all between 12:00 and 6:00) is $1/2^{n-1}$. Similarly the probability that a clockwise semicircle starting at any point i, where $i \in \{2, \ldots, n\}$ contains all the other $n-1$ points is also $1/2^{n-1}$. Thus, the total probability is $n/2^{n-1}$.

Chapter 20

Stochastic Processes and Martingale Theory

20.1 Discrete-time Processes

20.1.1 Stochastic processes and filtrations

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $(E, \mathcal{E})$ be a measurable space. (We will mostly consider $E = \mathbb{R}, \mathbb{R}^d, \mathbb{C}$).

Definition 20.1.1 (stochastic process, discrete)**.** A (discrete) stochastic process in E, $X = (X_n)_{n\geq 0}$ is a sequence of random variables in E.

Remark. stochastic process is also called random process.

Definition 20.1.2. If X_n is $\mathbb{R}$-valued, X is integrable if $X_n \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ for every $n \geq 0$, i.e. $\mathbb{E}\,|X_n| < \infty$.

Definition 20.1.3 (filtration, discrete)**.** A filtration is an increasing family of sub-σ-algebras of $\mathcal{F}$, i.e., $\mathcal{F}_n \subseteq \mathcal{F}_{n+1}$, for all n.

Remark. We think of $\mathcal{F}_n$ as 'the information available at and before time n.'

Definition 20.1.4. We define

$$\mathcal{F}_\infty = \bigvee_{n\geq 0} \mathcal{F}_n = \sigma\left(\bigcup_{n\geq 0} \mathcal{F}_n\right). \tag{20.1.1}$$

Definition 20.1.5 (filtered probability space, discrete)**.** If $(\mathcal{F}_n)_{n\geq 0}$ is a filtration, we say that $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ is a filtered probability space (or f.p.s.).

Definition 20.1.6 (adapted process, discrete)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. A stochastic process $X = (X_n)_{n\geq 0}$ is adapted to the filtration $(\mathcal{F}_n)_{n\geq 0}$ if X_n is $\mathcal{F}_n$-measurable for all $n \geq 0$. $(X_n)_{n\geq 0}$ is called adapted process (or non-anticipating process).

Remark. An adapted process is one that cannot 'see into the future'.

Definition 20.1.7 (natural filtration, discrete)**.** Let $(X_n)_{n\geq 0}$ be a stochastic process, and let $\mathcal{F}_n^X = \sigma\,(X_k, k \leq n)$. Then $\mathcal{F}_n^X$ is the natural filtration of X. It is the smallest filtration with respect to which X is adapted.

20.1.2 Stopping times

Definition 20.1.8 (Doob's stopping time, discrete)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. A stopping time with respect to the filtration $(\mathcal{F}_n)_{n\geq 0}$ is a random variable $T : \Omega \to \mathbb{Z}^+ \cup \{+\infty\}$ such that $\{T \leq n\} \in \mathcal{F}_n$ for all n.

Proposition 20.1.1. T is a stopping time if $\{T = n\} \in \mathcal{F}_n$ for all n.

Proof. Indeed, if $\{T \leq n\} \in \mathcal{F}_n$ for all n, $\{T = n\} = \{T \leq n\} \setminus \{T \leq n-1\} \in \mathcal{F}_n$.
Conversely, if $\{T = n\} \in \mathcal{F}_n$ for all n. $\{T \leq n\} = \bigcup_{k\leq n} \{T = k\} \in \mathcal{F}_n$. □

Example 20.1.2. (i) Constant times are trivial stopping times.

(ii) Let $X = (X_n)_{n\geq 0}$ be an adapted process taking values in $\mathbb{R}$. Let $A \in \mathcal{B}(\mathbb{R})$. The first entrance time to A is

$$T_A = \inf\{n \geq 0 : X_n(\omega) \in A\} \tag{20.1.2}$$

with the convention that $\inf(\emptyset) = \infty$, so that $T_A = \infty$, if X never enters A. This is a stopping time, since

$$\{T_A \leq n\} = \bigcup_{k\leq n} \{X_k \in A\} \in \mathcal{F}_n. \tag{20.1.3}$$

(iii) The last exit time though, $L_A = \sup\{n \leq N : X_n \in A\}$ for some $N \in \mathbb{R}$, is not a stopping time in general.

Proposition 20.1.3. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. Let S, T, and $(T_n)_{n\geq 0}$ all be stopping times. Then the following are stopping times

(i) $S \wedge T$, (ii) $S \vee T$, (iii) $\inf_{n\geq 0} T_n$, (iv) $\sup_{n\geq 0} T_n$, (v) $\liminf_n T_n$, (vi) $\limsup_n T_n$.

Remark. $S - T$ is not. $S + T$?[1]

Proof. [10].P_{193}[2] □

Definition 20.1.9. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. Let T be stopping time with respect to $(\mathcal{F}_n)_{n\geq 0}$, and

$$\mathcal{F}_T = \{A \in \mathcal{F} : A \cap \{T \leq n\} \in \mathcal{F}_n \text{ for all } n\}. \tag{20.1.4}$$

This defines a σ-algebra $\mathcal{F}_T$, called the σ-algebra of measurable events before T.

Proof. (i) Since $\{\emptyset \cap \{T \leq n\}\} = \{\emptyset\} \in \mathcal{F}_n$, $\emptyset \in \mathcal{F}_T$.

(ii) If $A \in \mathcal{F}_T$, $A \cap \{T \leq n\} \in \mathcal{F}_n$. Since T is stopping time, $\{T \leq n\} \in \mathcal{F}_n$. Thus, since $\mathcal{F}_n$ is σ-algebra

$$A^c \cap \{T \leq n\} = \{T \leq n\} \setminus (A \cap \{T \leq n\}) \in \mathcal{F}_n. \tag{20.1.5}$$

(iii) For a sequence $A_m \in \mathcal{F}_T$, we have $A_m \cap \{T \leq n\} \in \mathcal{F}_n$ for all n. Thus, since $\mathcal{F}_n$ is σ-algebra

$$\left(\bigcup_m A_m\right) \cap \{T \leq n\} = \bigcup_m (A_m \cap \{T \leq n\}) \in \mathcal{F}_n \;\Rightarrow\; \bigcup_m A_m \in \mathcal{F}_T. \tag{20.1.6}$$

Thus, $\mathcal{F}_T$ is a σ-algebra. □

Remark. Intuitively $\mathcal{F}_T$ is the information available at time T.

It is easy to check that if $T = n$, then T is a stopping time and $\mathcal{F}_T = \mathcal{F}_n$.

Definition 20.1.10 (stopped process)**.** For a process X, we set $X_T(\omega) = X_{T(\omega)}(\omega)$, whenever $T(\omega) < \infty$.

We also define the stopped process X^T by $X_n^T = X_{T\wedge n}$.

Proposition 20.1.4. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. If S and T are stopping times such that $S \leq T$ then $\mathcal{F}_S \subseteq \mathcal{F}_T$.

Proof. Since S and T are stopping times, then $\{S \leq n\} \in \mathcal{F}_n$, $\{T \leq n\} \in \mathcal{F}_n$ with $\{T \leq n\} \subseteq \{S \leq n\}$ for all n. $\forall A \in \mathcal{F}_S$, we have for all n, $A \cap \{S \leq n\} \in \mathcal{F}_n$. Then

$$A \cap \{T \leq n\} = A \cap (\{S \leq n\} \cap \{T \leq n\}) = \underbrace{(A \cap \{S \leq n\})}_{\in \mathcal{F}_n} \cap \underbrace{\{T \leq n\}}_{\in \mathcal{F}_n} \in \mathcal{F}_n. \tag{20.1.7}$$

Thus, $A \in \mathcal{F}_T$. □

[1] need details

[2] need proof. Note that in discrete time everything follows straight from the definitions. But when one considers continuous time processes, then right continuity of the filtration is needed to ensure that the limits are indeed stopping times.

Proposition 20.1.5. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. Let S be stopping time and let $X = (X_n)_{n\geq 0}$ be an adapted process. $(X : \Omega \to E)$

(i) $X_T \mathbb{1}_{\{T<\infty\}}$ is an $\mathcal{F}_T$-measurable random variable.

(ii) X^T is adapted.

(iii) If X is integrable, then X^T is integrable.

Proof. (i) $\forall A \in \mathcal{E}$. Then since X is adapted ($\{X_n \in A\} \in \mathcal{F}_n$) and $\{T = m\} = \{T \leq m\} \setminus \bigcup_{k\leq m} \{T \leq k\} \in \mathcal{F}_m$.

$$\left\{X_T \mathbb{1}_{\{T<\infty\}} \in A\right\} \cap \{T \leq n\} = \bigcup_{m=1}^{n} \{X_m(\omega) \in A\} \cap \{T(\omega) = m\} \in \mathcal{F}_n \tag{20.1.8}$$

(ii) For every n we have that $X_{T\wedge n}$ is $\mathcal{F}_{T\wedge n}$-measurable since X is adapted. Hence, $X_{T\wedge n}$ is $\mathcal{F}_n$-measurable since $T \wedge n \leq n$ by Proposition 20.1.3 and Proposition 20.1.4 (constant n is also a stopping time).

(iii) We have $X_n^T = X_n \mathbb{1}_{\{T>n\}} + \sum_{m\leq n} X_m \mathbb{1}_{\{T=m\}}$. Thus, since X is integrable, for every n,

$$\mathbb{E}\left|X_n^T\right| = \mathbb{E}\left|X_n^T\right| \leq \mathbb{E}\left|X_n \mathbb{1}_{\{T>n\}}\right| + \sum_{m\leq n} |X_m| \, \mathbb{1}_{\{T=m\}} \leq \mathbb{E}\,|X_n| + \sum_{m\leq n} |X_m| < \infty. \tag{20.1.9}$$

□

20.1.3 Branching process

20.1.4 Random walks

20.2 Discrete-time Martingales

20.2.1 Definitions

Definition 20.2.1. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. Let $X = (X_n)_{n\geq 0}$ be an adpated real-valued integrable process (see Definition 20.1.6 and Definition 20.1.2). Then

(i) X is a martingale with respect to $((\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ if $\mathbb{E}\,(X_n|\mathcal{F}_m) = X_m$ a.s. for all $n \geq m$.

(ii) X is a supermartingale with respect to $((\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ if $\mathbb{E}\,(X_n|\mathcal{F}_m) \leq X_m$ a.s. for all $n \geq m$.

(iii) X is a submartingale with respect to $((\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ if $\mathbb{E}\,(X_n|\mathcal{F}_m) \geq X_m$ a.s. for all $n \geq m$.

In particular, if X is a

(i) martingale, then $\mathbb{E}\,(X_n) = \mathbb{E}\,(X_m)$ for all $m, n \geq 0$.

(ii) supermartingale, then $\mathbb{E}\,(X_n) \leq \mathbb{E}\,(X_m)$ for all $n \geq m$.

(iii) submartingale, then $\mathbb{E}\,(X_n) \geq \mathbb{E}\,(X_m)$ for all $n \geq m$.

Remark. If a process is both supermartingale and submartingale, then it is a martingale.

Example 20.2.1. Let $I = \mathbb{Z}^+$ and $X_1, X_2, \ldots$ be i.i.d. integrable random variables. Take $\mathcal{F}_0 = \{\emptyset, \Omega\}$ and $\mathcal{F}_n = \sigma(X_m, m \leq n)$. Let $S_n = X_1 + \cdots + X_n$. Then S is a martingale if and only if $\mathbb{E}X_1 = 0$, since for all n, S_n is $\mathcal{F}_n$-measurable,

$$\mathbb{E}\,(S_{n+1}|\mathcal{F}_n) = S_n + \mathbb{E}\,(X_{n+1}) = S_n + \mathbb{E}X_1. \tag{20.2.1}$$

Similarily, it is a supermartingale if $\mathbb{E}X_1 \leq 0$ or a submartingale if $\mathbb{E}X_1 \geq 0$.

Example 20.2.2. Let $(\xi_i)_{i\geq 1}$ be a sequence of i.i.d. random variables with $\mathbb{E}(\xi_1) = 1$. Then the product $X_n = \prod_{i=1}^n \xi_i$ is a martingale.

20.2.2 Previsible process and construction of a martingale

Definition 20.2.2 (previsible process, discrete-time)**.** We say that $C = (C_n)_{n\geq 1}$ is previsible if C_n is $\mathcal{F}_{n-1}$-measurable for all $n \geq 1$.

Definition 20.2.3 (discrete stochastic integral)**.** Let $(C_n)_{n\geq 1}$ and $(X_n)_{n\geq 0}$ be processes taking values in $\mathbb{R}$. If $(X_n)_{n\geq 0}$ is adapted and $(C_n)_{n\geq 1}$ is previsible, define

$$(C \cdot X)_n := \sum_{k=1}^{n} C_k(X_k - X_{k-1}) \tag{20.2.2}$$

for $n \geq 1$, and $(C \cdot X)_0 = 0$. Then $C \cdot X$ is called a discrete stochastic integral.

Remark. We can interpret this new process as follows: if X_n is a certain amount of money at time n and if C_n is the bet of a player at time n then $(C \cdot X)_n$ is the total winning of the player at time n.

Proposition 20.2.3. Let $(X_n)_{n\geq 0}$ be a martingale and let $(C_n)_{n\geq 1}$ be a bounded, previsible process. Then the process $((C \cdot X)_n)_{n\geq 0}$ is a martingale.

Remark. (i) The boundedness condition on C may be replaced by the condition $C_n \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, $\forall n$, provided we also insist that $X_n \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, $\forall n$. Williams [16].P_{97}[3]

(ii) Discrete stochastic integral is also called 'martingale transform'.

Proof. $C \cdot X$ is adapted since $\sum_{k=1}^{n} C_k(X_k - X_{k-1})$ is $\mathcal{F}_n$-measurable for every n. Therefore it is integrable since the C_k's are uniformly bounded and the X_k's are integrable.

$$\mathbb{E}\left((C \cdot X)_{n+1}|\mathcal{F}_n\right) = \mathbb{E}\left((C \cdot X)_n + C_{n+1}(X_{n+1} - X_n)|\mathcal{F}_n\right) = (C \cdot X)_n + C_{n+1}\mathbb{E}\left(X_{n+1} - X_n|\mathcal{F}_n\right) = (C \cdot X)_n \quad \text{a.s.} \tag{20.2.3}$$

by the martingale property. □

Proposition 20.2.4. Let $(X_n)_{n\geq 0}$ be a supermartingale (submartingale) and let $(C_n)_{n\geq 1}$ be a bounded, previsible, non-negative process. Then the process $((C \cdot X)_n, n \geq 0)$ is a supermartingale (submartingale).

Remark. (i) The boundedness condition on C may be replaced by the condition $C_n \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, $\forall n$, provided we also insist that $X_n \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, $\forall n$. Williams [16].P_{97}[4]

(ii) The above result shows that there is no way to make money out of supermartingales.

Proof. $C \cdot X$ is adapted since $\sum_{k=1}^{n} C_k(X_k - X_{k-1})$ is $\mathcal{F}_n$-measurable for every n. Therefore it is integrable since the C_k's are uniformly bounded and the X_k's are integrable.

$$\mathbb{E}[(C \cdot X)_{n+1}|\mathcal{F}_n] = \mathbb{E}[(C \cdot X)_n + C_{n+1}(X_{n+1} - X_n)|\mathcal{F}_n] = (C \cdot X)_n + C_{n+1}\mathbb{E}[X_{n+1} - X_n|\mathcal{F}_n] \begin{matrix} \leq \\ \geq \end{matrix} (C \cdot X)_n \quad \text{a.s.} \tag{20.2.4}$$

by the supermartingale (submartingale) property. □

Lemma 20.2.5. Let $(M_n)_{n\geq 0}$ and $(N_n)_{n\geq 0}$ be two martingales in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. For $\Delta M_k = M_k - M_{k-1}$, $\Delta N_k = N_k - N_{k-1}$, we define

$$[M, N]_n := \sum_{k=1}^{n} \Delta M_k \Delta N_k, \qquad [M_n] := \sum_{k=1}^{n} (\Delta M_k)^2. \tag{20.2.5}$$

Then $M_n N_n - M_0 N_0 - [M, N]_n$ is a martingale. In particular, $M_n^2 - M_0^2 - [M]_n$ is also a martingale.

Proof. First, we have

$$M_n N_n - M_0 N_0 = \sum_{k=1}^{n} M_{k-1}\left(N_k - N_{k-1}\right) + \sum_{k=1}^{n} N_{k-1}\left(M_k - M_{k-1}\right) + \sum_{k=1}^{n} \Delta M_k \Delta N_k. \tag{20.2.6}$$

[3] need details
[4] need details

From Proposition 20.2.3, we can have that

$$\sum_{k=1}^{n} M_{k-1}\left(N_k - N_{k-1}\right) \quad \text{and} \quad \sum_{k=1}^{n} N_{k-1}\left(M_k - M_{k-1}\right) \quad \text{martingales.} \tag{20.2.7}$$

Thus, it is obvious that $M_n N_n - M_0 N_0 - [M,N]_n$ is a martingale. □

20.2.3 Optional stopping theorem for bounded stopping time

Theorem 20.2.6 (stopped martingale theorem, discrete-time)**.** Let T be a stopping time and let $(X_n)_{n\geq 0}$ be a martingale (resp. supermartingale, submartingale). Then X^T is also a martingale (resp. supermartingale, submartingale).

Proof. Let $C_n = \mathbb{1}_{\{n\leq T\}}$ for $n \geq 0$. Then $(C_n, n \geq 1)$ is previsible since $\{n \leq T\} = \{T \leq n-1\}^c \in \mathcal{F}_{n-1}$. It is also bounded, integrable, and non-negative, so by the previous proposition $C \cdot X$ is a martingale (resp. supermartingale, submartingale).

$$(C \cdot X)_n = \sum_{k=1}^{n} \mathbb{1}_{\{k\leq T\}}(X_k - X_{k-1}) = \sum_{k=1}^{n\wedge T}(X_k - X_{k-1}) = X_{n\wedge T} - X_0 = X_n^T - X_0, \tag{20.2.8}$$

so X^T is a martingale (resp. supermartingale, submartingale). □

Theorem 20.2.7 (optional stopping theorem, discrete)**.** Let $(X_n, n \geq 0)$ be a martingale.

(i) If S and T be bounded stopping times such that $S \leq T \leq K$, where K is a fixed constant. Then $\mathbb{E}\left(X_T|\mathcal{F}_S\right) = X_S$ a.s. In particular, $\mathbb{E}X_T = \mathbb{E}X_S$.

(ii) If there exists an integrable random variable Y such that $|X_n| \leq Y$ for all n, and T is a stopping time which is finite a.s., then $\mathbb{E}(X_T) = \mathbb{E}(X_0)$.

(iii) If X has bounded increments, i.e., $\exists M > 0 : \forall n \geq 0$, $|X_{n+1} - X_n| \leq M$ a.s., and T is a stopping time with $\mathbb{E}(T) < \infty$, then $\mathbb{E}(X_T) = \mathbb{E}(X_0)$.

Proof. (i) Let $A \in \mathcal{F}_S \subseteq \mathcal{F}_T$, and consider $C_n = \mathbb{1}_A \mathbb{1}_{\{S<n\leq T\}}$. C is previsible since

$$C_n = \mathbb{1}_A \mathbb{1}_{\{S\leq n-1\}} \mathbb{1}_{\{n\leq T\}} = \underbrace{\mathbb{1}_{A\cap\{S\leq n-1\}}}_{\in\mathcal{F}_{n-1}} \underbrace{\mathbb{1}_{\{n\leq T\}}}_{=\mathbb{1}_{\{T\leq n-1\}}\in\mathcal{F}_{n-1}} \tag{20.2.9}$$

is $\mathcal{F}_{n-1}$-measurable. Then $((C \cdot X)_n, n \geq 0)$ is a martingale, and we have

$$(C \cdot X)_K = \sum_{k=S+1}^{T} \mathbb{1}_A(X_k - X_{k-1}) = \mathbb{1}_A(X_T - X_S). \tag{20.2.10}$$

Since $(C \cdot X)$ is a martingale, $\mathbb{E}\left((C \cdot X)_K\right) = \mathbb{E}\left((C \cdot X)_0\right) = 0$. This says that $\mathbb{E}\left(\mathbb{1}_A X_T\right) = \mathbb{E}\left(\mathbb{1}_A X_S\right)$ for all $A \in \mathcal{F}_S$, which is the definition of $\mathbb{E}\left(X_T|\mathcal{F}_S\right) = \mathbb{E}X_S$ a.s. Then take the expectation again, we have $\mathbb{E}X_T = \mathbb{E}X_S$.

(ii) we have $\mathbb{E}(X_{T\wedge n}) = \mathbb{E}(X_n^T) = \mathbb{E}(X_0)$ by stopped martingale theorem (Theorem 20.2.6). With $T < \infty$ a.s., we have $X_{T\wedge n} \to X_T$ a.s. as $n \to \infty$. Thus, by dominated convergence theorem (Theorem 19.3.8),

$$\mathbb{E}(X_0) = \mathbb{E}(X_{T\wedge n}) \to \mathbb{E}(X_T). \tag{20.2.11}$$

(iii) First $\mathbb{E}(T) < \infty \;\Rightarrow\; \mathbb{P}(T < \infty) = 1$ by Markov's inequality (Theorem 19.3.20). Thus, $X_n^T = X_{T\wedge n} \to X_T$ a.s. as $n \to \infty$. We have $X_n^T = X_0 + \sum_{m=0}^{T\wedge n-1}(X_{m+1} - X_m)$ and then

$$\left|X_n^T\right| \leq |X_0| + \sum_{m=0}^{T\wedge n-1} |X_{m+1} - X_m| := M. \tag{20.2.12}$$

Thus, we have

$$\mathbb{E}\left(M\right) = \mathbb{E}\left|X_0\right| + \mathbb{E}\left(\sum_{m=0}^{T\wedge n-1} |X_{m+1} - X_m|\right) \leq \mathbb{E}\left|X_0\right| + M \cdot \mathbb{E}(T-1) < \infty. \tag{20.2.13}$$

Then we apply dominated convergence theorem (Theorem 19.3.8), $\mathbb{E}(X_0) = \mathbb{E}(X_{T\wedge n}) \to \mathbb{E}(X_T)$.

□

Remark. We can summarize with the following table

	T	X
(i)	bounded	$\times$
(iii)	$\mathbb{E}(T) < \infty$	bounded increments
(ii)	$\mathbb{P}(T < \infty)$	bounded by a integrable r.v.

Remark. This is not true in general (for unbounded stopping times). Consider i.i.d. random variables $X_1, \dots, X_n$ such that

$$\mathbb{P}(X_n = 1) = \frac{1}{2} = \mathbb{P}(X_n = -1), \tag{20.2.14}$$

and let $S_n = X_1 + \cdots + X_n$, which we have seen to be a martingale. Let $T = \inf\{n \geq 1 : S_n = 1\}$, a stopping time. It holds that $\mathbb{P}(T < \infty) = 1$, but $\mathbb{E}S_T = 1 > 0 = \mathbb{E}S_0$.

Remark. Note that optional stopping theorem (Theorem 20.2.7) is true[5] if X is a supermartingale or submartingale with the respective inequalities in the statements.

Theorem 20.2.8. Let $(X_n, n \geq 0)$ be a supermartingale and S and T be bounded stopping times such that $S \leq T \leq K$, where K is a fixed constant. Then $\mathbb{E}(X_T|\mathcal{F}_S) \leq X_S$ a.s. In particular, $\mathbb{E}X_T \leq \mathbb{E}X_S$.

Proof. With similar argument to Theorem 20.2.7, we use definition of supermartingale and Proposition 20.2.4 and get

$$\mathbb{E}((C \cdot X)_K) \leq \mathbb{E}((C \cdot X)_0) = 0 \quad \Rightarrow \quad \mathbb{E}(\mathbb{1}_A(X_T - X_S)) \leq 0 \quad \Rightarrow \quad \mathbb{E}(\mathbb{1}_A X_T) \leq \mathbb{E}(\mathbb{1}_A X_S) \text{ for all } A \in \mathcal{F}_S. \quad (*) \tag{20.2.15}$$

We know that X_T is integrable thus by Theorem 19.4.18, there exists $\mathcal{F}_S$-measurable random variable $Y = \mathbb{E}(X_T|\mathcal{F}_S)$ such that $\mathbb{E}(\mathbb{1}_A X_T) = \mathbb{E}(\mathbb{1}_A Y)$ for all $A \in \mathcal{F}_S$.

If $\mathbb{P}(Y > X_S) > 0$, there exist some n such that $A = \left\{Y > X_S + \frac{1}{n}\right\} \in \mathcal{F}_S$ and $\mathbb{P}(A) > 0$, we have $\mathbb{1}_A Y \geq \mathbb{1}_A X_S + \frac{1}{n}\mathbb{1}_A$,

$$\mathbb{E}(\mathbb{1}_A X_T) = \mathbb{E}(\mathbb{1}_A Y) \geq \mathbb{E}(\mathbb{1}_A X_S) + \frac{1}{n}\mathbb{P}(A) \tag{20.2.16}$$

which is contradiction to $(*)$. Hence, $Y \leq X_S$ a.s., that is $\mathbb{E}(X_T|\mathcal{F}_S) \leq \mathbb{E}X_S$ a.s.. Then we can take the expectation to get the require result. □

Proposition 20.2.9. Suppose that X is a non-negative supermartingale. Then for any stopping time T which is finite a.s. we have $\mathbb{E}X_T \leq \mathbb{E}X_0$.

Proof. With $T < \infty$ a.s., we have $X_{T\wedge n} \to X_T$ a.s. as $n \to \infty$. That is

$$\liminf_n X_{T\wedge n} = \lim_{n\to\infty} X_{T\wedge n} = X_T \text{ a.s..} \tag{20.2.17}$$

Since X_n is a supermartingale, we have $\mathbb{E}(X_{T\wedge n}) \leq \mathbb{E}X_0)$. Therefore, by Fatou's lemma (Lemma 19.3.7) as X is non-negative,

$$\mathbb{E}X_T = \mathbb{E}\left(\lim_{n\to\infty} X_{T\wedge n}\right) = \mathbb{E}\left(\liminf_n X_{T\wedge n}\right) \leq \liminf_n \mathbb{E}(X_{T\wedge n}) \leq \liminf_n \mathbb{E}X_0 = \mathbb{E}X_0, \tag{20.2.18}$$

as required. □

Remark. Accordingly, we can not have $\mathbb{E}X_T \geq \mathbb{E}X_0$ for a non-negative submartingale by inverse Fatou's lemma (Lemma 19.3.7) as we can not get a non-negative integrable Y such that $X_n < Y$ for all n.

Example 20.2.10 (symmetric random walk)**.** Let $(\xi_i)_{i\geq 1}$ be an i.i.d. sequence of random variables taking values ± 1 with probabilities $\mathbb{P}(\xi_1 = +1) = \mathbb{P}(\xi_1 = -1) = 1/2$. Define $X_n = \sum_{i=1}^n \xi_i$, for $n \geq 1$, and $X_0 = 0$. This is called the simple symmetric random walk in $\mathbb{Z}$. For $c \in \mathbb{Z}$ we write

$$T_c = \inf\{n \geq 0 : X_n = c\}, \tag{20.2.19}$$

[5] need details

i.e. T_c is the first hitting time of the state c, and hence is a stopping time (by Example 20.1.2.(ii)). Let $a, b > 0$. We will calculate the probability that the random walk hits $-a$ before b, i.e. $\mathbb{P}(T_{-a} < T_b)$.

As mentioned earlier in this section X is a martingale. Also, $|X_{n+1} - X_n| \leq 1$ for all n. We now write $T = T_{-a} \wedge T_b$. We will first show that $\mathbb{E}T < \infty$[6].

It is easy to see that T is bounded from above by the first time that there are $a+b$ consecutive $+1$'s. The probability that the first $\xi_1, \ldots, \xi_{a+b}$ are all equal to $+1$ is $2^{-(a+b)}$. If the first block of $a+b$ variables ξ fail to be all $+1$'s, then we look at the next block of $a+b$, i.e. $\xi_{a+b+1}, \ldots, \xi_{2(a+b)}$. The probability that this block consists only of $+1$'s is again $2^{-(a+b)}$ and this event is independent of the previous one. Hence T can be bounded from above by a geometric random variable of success probability $2^{-(a+b)}$ times $a+b$. Therefore we get

$$\begin{aligned}
\mathbb{E}(T) &\leq (a+b)2^{-(a+b)} + 2(a+b)2^{-(a+b)}\left(1 - 2^{-(a+b)}\right) + 3(a+b)2^{-(a+b)}\left(1 - 2^{-(a+b)}\right)^2 + \ldots \\
&= (a+b)2^{-(a+b)} \sum_{n=1}^{\infty} n\left(1 - 2^{-(a+b)}\right)^{n-1} = (a+b)2^{-(a+b)}\left(\sum_{n=1}^{\infty} \rho^n\right)' \quad (\rho := 1 - 2^{-(a+b)}) \\
&= (a+b)2^{-(a+b)}\left(\frac{\rho}{1-\rho}\right)' = (a+b)2^{-(a+b)}\frac{1}{(1-\rho)^2} = (a+b)2^{-(a+b)}2^{2(a+b)} = (a+b)2^{a+b}.
\end{aligned}$$

We thus have a martingale with bounded increments and a stopping time with finite expectation. Hence, from the optional stopping theorem (Theorem 20.2.7.(iii)), we deduce that

$$\mathbb{E}X_T = \mathbb{E}X_0 = 0. \tag{20.2.20}$$

We also have

$$\mathbb{E}X_T = -a\mathbb{P}(T_{-a} < T_b) + b\mathbb{P}(T_b < T_{-a}), \quad \mathbb{P}(T_{-a} < T_b) + \mathbb{P}(T_b < T_{-a}) = 1, \tag{20.2.21}$$

and hence we deduce that

$$\mathbb{P}(T_{-a} < T_b) = \frac{b}{a+b}. \tag{20.2.22}$$

For similar result, see also Theorem 22.1.21.

20.2.4 Martingale Convergence Theorem

Usually when we want to prove convergence of a sequence, we have an idea of what the limit should be. In the case of the martingale convergence theorem though, we do not know the limit. And, indeed in most cases, we just know the existence of the limit. In order to show the convergence in the theorem, we will employ a beautiful trick due to Doob, which counts the number of upcrossings of every interval with rational endpoints.

Let $x = (x_n)_n$ be a sequence of real numbers. Let $a < b$ be two real numbers. We define $T_0(x) = 0$ and inductively for $k \geq 0$

$$S_{k+1}(x) = \inf\{n \geq T_k(x) : x_n \leq a\}, \qquad T_{k+1}(x) = \inf\{n \geq S_{k+1}(x) : x_n \geq b\} \tag{20.2.23}$$

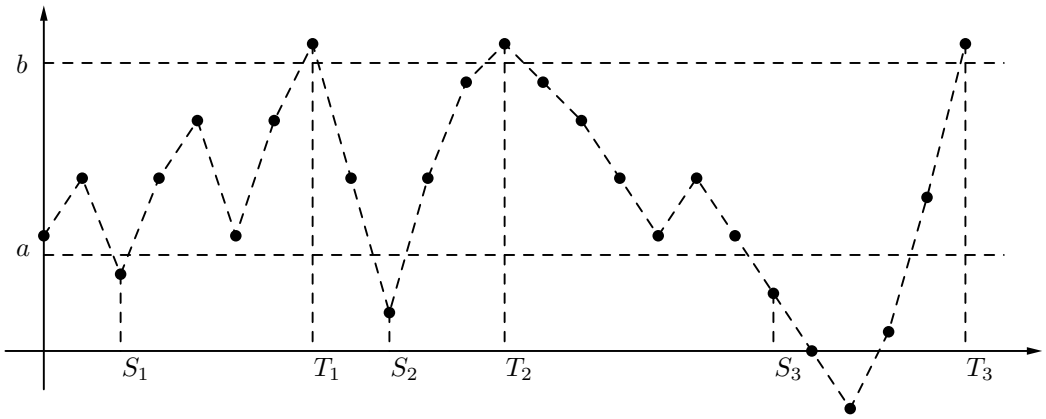
with the usual convention that $\inf \emptyset = \infty$.

We also define $N_n(x, [a,b]) = \sup\{k \geq 0 : T_k(x) \leq n\}$, i.e., the number of upcrossings of the interval $[a,b]$ by the sequence x by time n. As $n \to \infty$ we have

$$N_n(x, [a,b]) \uparrow N(x, [a,b]) = \sup\{k \geq 0 : T_k(x) \leq \infty\}, \tag{20.2.24}$$

i.e., the total number of upcrossings of the interval $[a,b]$. Observe that if $(X_n)_{n\geq 0}$ is an adapted process then $S_k(X)$ and $T_k(X)$ $(k \geq 1)$ are all stopping times.

[6] we can also use probability generating function



Lemma 20.2.11. A real sequence $x = (x_n)_{n\geq 0}$ converges in $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$ if and only if $N(x,[a,b]) < \infty$ for every $a < b \in \mathbb{Q}$.

Proof. Suppose that x converges. Then if for some $a < b$ we had that $N(x,[a,b]) = \infty$, that would imply that

$$\liminf_n x_n \leq a < b \leq \limsup_n x_n, \qquad \text{(by Definition 3.5.2)} \tag{20.2.25}$$

which is a contradiction.

Next suppose that x does not converge. Then $\liminf_n x_n < \limsup_n x_n$ and so taking $a < b$ rationals between these two numbers gives that $N(x,[a,b]) = \infty$ (by Definition 3.5.2). □

Lemma 20.2.12 (Doob's up-crossing inequality)**.** Let $(X_n, n \geq 0)$ be a supermartingale. Then for all $a < b$ and all $n \geq 0$,

$$(b-a)\mathbb{E}\left(N_n(X,[a,b])\right) \leq \mathbb{E}\left((X_n - a)^-\right). \tag{20.2.26}$$

Proof. For this proof we write S_k, T_k, and N_n for the random variables $S_k(X)$, $T_k(X)$, and $N_n(X,[a,b])$, respectively. Let $C_n = \sum_{k\geq 1} \mathbb{1}_{\{S_k < n \leq T_k\}}$. Since $S_1 < T_1 < S_2 < T_2 < \ldots$, C_n takes values in $\{0,1\}$. Note that the process $(C_n, n \geq 1)$ is previsible (we have already seen that $\mathbb{1}_{\{S<n\leq T\}} = \mathbb{1}_{\{S\leq n-1\}}\mathbb{1}_{\{T\leq n-1\}^c}$ is previsible ($\mathcal{F}_{n-1}$-measurable) when $S \leq T$ are stopping times). Therefore $((C\cdot X)_n)_{n\geq 0}$ is a supermartingale. Now from the definition of $N_n(x,[a,b])$, we have $T_{N_n+1} \geq n+1$ and $S_{N_n+2} \geq n+2$,

$$\begin{aligned}
(C\cdot X)_n &= \sum_{m=1}^n C_m(X_m - X_{m-1}) = \sum_{m=1}^n \sum_{k\geq 1} \mathbb{1}_{\{S_k < m \leq T_k\}}(X_m - X_{m-1}) \\
&= \sum_{m=1}^n \sum_{k=1}^{N_n} \mathbb{1}_{\{S_k < m \leq T_k\}}(X_m - X_{m-1}) + \sum_{m=1}^n \mathbb{1}_{\{S_{N_n+1} < m \leq T_{N_n+1}\}}(X_m - X_{m-1}) \\
&= \sum_{k=1}^{N_n} \sum_{m=1}^n \mathbb{1}_{\{S_k < m \leq T_k\}}(X_m - X_{m-1}) + \sum_{m=1}^n \mathbb{1}_{\{S_{N_n+1} < m\}}(X_m - X_{m-1}) \\
&= \sum_{k=1}^{N_n}(X_{T_k} - X_{S_k}) + \mathbb{1}_{\{S_{N_n+1} < n\}}(X_n - X_{S_{N_n+1}}) = \sum_{k=1}^{N_n}(X_{T_k} - X_{S_k}) + \mathbb{1}_{\{S_{N_n+1} \leq n\}}(X_n - X_{S_{N_n+1}}) \\
&\geq (b-a)N_n + \mathbb{1}_{\{S_{N_n+1}\leq n\}}(X_n - a)
\end{aligned}$$

Now either $X_n \geq a$, in which case $\mathbb{1}_{\{S_{N_n+1}\leq n\}}(X_n - a) \geq 0$, or $X_n < a$, in which case $S_{N_n+1} \leq n$, so $\mathbb{1}_{\{S_{N_n+1}\leq n\}}(X_n - a) = (X_n - a)\mathbb{1}_{\{X_n < a\}} = -(X_n - a)^-$. Hence

$$(C\cdot X)_n \geq (b-a)N_n - (X_n - a)^-, \tag{20.2.27}$$

but by Proposition 20.2.4, $0 = \mathbb{E}\left((C\cdot X)_0\right) \geq \mathbb{E}\left((C\cdot X)_n\right) \geq (b-a)\mathbb{E}\left(N_n\right) - \mathbb{E}\left((X_n - a)^-\right)$. □

Alternative proof in Steele [14].P_{25}**.** [7] □

[7] need details

Theorem 20.2.13 (martingale convergence theorem, discrete-time)**.** Let $(X_n)_{n\geq 0}$ be a supermartingale such that $\sup_n \mathbb{E}\,|X_n| < \infty$, i.e., X is bounded in $\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$ (Definition 19.3.5). Then $X_n \to X_\infty$ a.s. as $n\to\infty$ for some $X_\infty \in \mathcal{L}^1(\Omega,\mathcal{F}_\infty{}^{8},\mathbb{P})$[9].

Proof. Let $a<b\in\mathbb{Q}$. By the up-crossing inequality (Lemma 20.2.12)

$$\mathbb{E}\left(N_n(X,[a,b])\right) \leq (b-a)^{-1}\mathbb{E}\left((X_n-a)^-\right) \leq (b-a)^{-1}\left(\mathbb{E}\,|X_n|+a\right) < \infty \tag{20.2.28}$$

for all n. By the monotone convergence theorem (Theorem 19.3.6) since $N_n(X,[a,b]) \uparrow N(X,[a,b])$ as $n\to\infty$, we get

$$\mathbb{E}\left(N_n(X,[a,b])\right) \uparrow \mathbb{E}\left(N(X,[a,b])\right) \leq (b-a)^{-1}\left(\sup_n \mathbb{E}\,|X_n|+a\right) < \infty, \tag{20.2.29}$$

by the assumption on X being bounded in $\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$. Therefore, we get that $N(X,[a,b])<\infty$ a.s. for every $a<b\in\mathbb{Q}$. Hence,

$$\begin{aligned}\mathbb{P}\left(\bigcap_{a<b\in\mathbb{Q}}\{N(X,[a,b])<\infty\}\right) &= 1-\mathbb{P}\left(\bigcup_{a<b\in\mathbb{Q}}\{N(X,[a,b])=\infty\}\right)\\ &\geq 1-\sum_{a<b\in\mathbb{Q}}\mathbb{P}\left(\{N(X,[a,b])=\infty\}\right) = 1-0=1.\end{aligned}$$

Write $\Omega_0=\bigcap_{a<b\in\mathbb{Q}}\{N(X,[a,b])<\infty\}$, we have $\mathbb{P}(\omega_0)=1$ and by Lemma 20.2.11 on Ω_0 we have that X converges to a possible infinite limit X_∞. So we can define

$$X_\infty = \begin{cases}\lim_{n\to\infty} X_n & \text{on } \Omega_0\\ 0 & \text{on } \Omega\backslash\Omega_0\end{cases} \tag{20.2.30}$$

Then X_∞ is $\mathcal{F}_\infty$-measurable (since $X_\infty=\lim_{n\to\infty}X_n\mathbb{1}_{\Omega_0}$, X_n is $\mathcal{F}_\infty$-measurable for all n and $\Omega_0\in\mathcal{F}_\infty$[10]) and by Fatou's lemma (Lemma 15.3.11) and the assumption on X being in $\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$ we get

$$\mathbb{E}\,|X_\infty| = \mathbb{E}\left(\liminf_n |X|\right) \leq \liminf_n \mathbb{E}\,|X_n| \leq \sup_n \mathbb{E}\,|X_n| < \infty. \tag{20.2.31}$$

Hence X_∞ is integrable, i.e., $X\in\mathcal{L}^1(\Omega,\mathcal{F}_\infty,\mathbb{P})$. □

Corollary 20.2.14. If $X=(X_n)_{n\geq 0}$ is a non-negative supermartingale then X_n converges a.s. to a finite limit X_∞ as $n\to\infty$.

Proof. $\mathbb{E}\,|X_n| = \mathbb{E}\,(X_n) = \mathbb{E}\,(X_0) < \infty$ for all n, so $(X_n)_{n\geq 0}$ is bounded in $\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$. □

Corollary 20.2.15. Let $(X_n)_{n\geq 0}$ be a non-negative supermartingale and let T be a stopping time. Then $\mathbb{E}\,(X_T)\leq\mathbb{E}\,(X_0)$ (where $X_T=X_\infty$ on the event $\{T=\infty\}$).

Remark. We can't turn the '$\leq$' into an '$=$' even if X is a martingale.

Proof. $T\wedge n\uparrow T$ and $\mathbb{E}[X_{T\wedge n}]\leq\mathbb{E}[X_0]$ since $T\wedge n$ is bounded (by n) by optional stopping theorem (Theorem 20.2.7). Apply Fatou's lemma (Lemma 15.3.11) and monotone convergence theorem (Theorem 19.3.6) to get

$$E\,(X_0) \geq \liminf_{n\to\infty}\mathbb{E}\,(X_{T\wedge n}) \geq \mathbb{E}\left(\liminf_{n\to\infty} X_{T\wedge n}\right) \uparrow \mathbb{E}\,(X_T)\,. \tag{20.2.32}$$

□

20.2.5 Doob's inequalities and Kolmogorov's inequality

Theorem 20.2.16 (Doob's maximal inequality, discrete-time)**.** Let $(X_n)_{n\geq 0}$ be a non-negative submartingale, and define $X_n^*=\max_{0\leq k\leq n}X_k$. Then we have

$$\lambda\mathbb{P}\,(X_n^*\geq\lambda) \leq \mathbb{E}\left(X_n\mathbb{1}_{\{X_n^*\geq\lambda\}}\right) \leq \mathbb{E}X_n. \tag{20.2.33}$$

[8] see Definition 20.1.4
[9] X_∞ can also be a finite limit
[10] need details

Remark. If $(X_n)_{n\geq 0}$ is a martingale, then $(|X_n|)_{n\geq 0}$ is a non-negative submartingale. Thus, we have

$$\lambda \mathbb{P}\left(\max |X_n| \geq \lambda\right) \leq \mathbb{E}\left(|X_n| \mathbb{1}_{\{\max |X_n| \geq \lambda\}}\right) \leq \mathbb{E}\,|X_n|\,. \tag{20.2.34}$$

Proof. Let $T = \inf\{n \geq 0 : X_n \geq \lambda\}$. Then $T \wedge n$ is a bounded stopping time. Hence by the optional stopping theorem (Theorem 20.2.7), we have (by submartingale property)

$$\mathbb{E}(X_n) \geq \mathbb{E}(X_{T\wedge n}) = \mathbb{E}\left(X_T \mathbb{1}_{\{T\leq n\}}\right) + \mathbb{E}\left(X_n \mathbb{1}_{\{T>n\}}\right) \geq \lambda \mathbb{P}(T \leq n) + \mathbb{E}\left(X_n \mathbb{1}_{\{T>n\}}\right). \tag{20.2.35}$$

It is clear that $\{T \leq n\} = \{X_n^* \geq \lambda\}$. Hence we get

$$\lambda \mathbb{P}(X_n^* \geq \lambda) \leq \mathbb{E}\left(X_n \mathbb{1}_{\{T\leq n\}}\right) = \mathbb{E}\left(X_n \mathbb{1}_{\{X_n^* \geq \lambda\}}\right) \leq \mathbb{E}(X_n). \tag{20.2.36}$$

□

Remark. Compare this theorem with Markov inequality (Theorem 19.3.20). The above conclusion is stronger as it is based on the fact that X is martingale.

Theorem 20.2.17 (Doob's $\mathcal{L}^p$-inequality, discrete-time)**.** Let $p \in (1, \infty]$ and $(X_n)_{n\geq 0}$ be a martingale or a non-negative submartingale. Define $X_n^* = \max_{0\leq k\leq n} |X_k|$. Then

$$\|X_n^*\|_p \leq \frac{p}{p-1} \|X_n\|_p\,. \tag{20.2.37}$$

Proof. For $p = \infty$, it is obvious. Then we only assume $p \in (1, \infty)$.

If X is a martingale, then by Jensen's inequality (Theorem 19.3.22, $f(x) = |x|$ is convex)

$$\mathbb{E}(|X_n|) \geq |\mathbb{E}(X_n)| = |\mathbb{E}X_0|\,. \tag{20.2.38}$$

Thus, $|X|$ is a non-negative submartingale. So it suffices to consider the case where X is a non-negative submartingale. Fix $k < \infty$ and $q = \frac{p}{p-1}$we have

$$\begin{aligned}
\|X_n^* \wedge k\|_p^p &= \mathbb{E}\left((X_n^* \wedge k)^p\right) = \mathbb{E}\left(\int_0^{X_n^*\wedge k} p x^{p-1} dx\right) = \mathbb{E}\left(\int_0^k p x^{p-1} \mathbb{1}_{\{X_n^* \geq x\}} dx\right) \\
&= \int_0^k p x^{p-1} \mathbb{P}(X_n^* \geq x) dx \qquad \text{(Fubini theorem (Theorem 15.3.33))} \\
&\leq p \int_0^k x^{p-2} \mathbb{E}\left(X_n \mathbb{1}_{\{X_n^* \geq x\}}\right) dx \qquad \text{(Doob's maximal inequality (Theorem 20.2.16))} \\
&\leq \frac{p}{p-1} \mathbb{E}\left(|X_n| \int_0^k (p-1) x^{p-2} \mathbb{1}_{\{X_n^* \geq x\}} dx\right) \qquad \text{(Fubini theorem (Theorem 15.3.33))} \\
&= \frac{p}{p-1} \mathbb{E}\left(|X_n| \int_0^{X_n^*\wedge k} (p-1) x^{p-2} dx\right) = \frac{p}{p-1} \mathbb{E}\left(|X_n| \left(X_n^* \wedge k\right)^{p-1}\right) \\
&\leq \frac{p}{p-1} \mathbb{E}\left(|X_n|^p\right)^{1/p} \mathbb{E}\left(\left(X_n^* \wedge k\right)^{(p-1)q}\right)^{1/q} \qquad \text{(Hölder's inequality (Theorem 19.3.24))} \\
&= \frac{p}{p-1} \|X_n\|_p \|X_n^* \wedge k\|_p^{p-1}\,.
\end{aligned}$$

Then we have

$$\|X_n^* \wedge k\|_p \leq \frac{p}{p-1} \|X_n\|_p\,. \tag{20.2.39}$$

Letting $k \to \infty$ and using monotone convergence theorem (Theorem 19.3.6) completes the proof. □

Theorem 20.2.18 (Kolmogorov's inequality)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space based on which $(X_n)_{n\geq 0}$ is a submartingale. Then for any constant $\lambda > 0$,

$$\mathbb{P}\left(\max_{0\leq k\leq n} X_k \geq \lambda\right) \leq \frac{\mathbb{E}X_n^+}{\lambda}. \tag{20.2.40}$$

Remark. (i) Notice the analogy with Markov's inequality. Of course, the conclusion is much stronger than Markov's inequality, as the probabilistic bound applies to an uncountable number of random variables.

(ii) Note that Doob's maximal inequality is a special case of Kolmogorov's inequality.

Proof. Let $B = \{\max_{1\leq k\leq n} X_k \geq \lambda\}$ and split B into disjoint parts B_k, defined by

$$B_k = \{X_m < \lambda \text{ for all } m < k, \text{ but } X_k \geq \lambda\}. \tag{20.2.41}$$

Then

$$\begin{aligned}
\mathbb{P}(B) &= \sum_{k=1}^{n} \mathbb{E}(\mathbb{1}_{B_k}) \leq \sum_{k=1}^{n} \mathbb{E}\left(\frac{1}{\lambda} X_k \mathbb{1}_{B_k}\right) \leq \frac{1}{\lambda} \sum_{k=1}^{n} \mathbb{E}(\mathbb{E}(X_n|\mathcal{F}_k)\, \mathbb{1}_{B_k}) \qquad X \text{ is a submartingale} \\
&= \frac{1}{\lambda} \sum_{k=1}^{n} \mathbb{E}(\mathbb{E}(X_n \mathbb{1}_{B_k}|\mathcal{F}_k)) \qquad B_k \text{ is } \mathcal{F}_k\text{-measurable} \\
&= \frac{1}{\lambda} \sum_{k=1}^{n} \mathbb{E}(X_n \mathbb{1}_{B_k}) = \frac{1}{\lambda} \mathbb{E}(X_n \mathbb{1}_B) \leq \frac{1}{\lambda} \mathbb{E}\left(X_n^+ \mathbb{1}_B\right) \leq \frac{1}{\lambda} \mathbb{E}\left(X_n^+\right),
\end{aligned}$$

as required. □

Corollary 20.2.19. Let $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$ be a filtered probability space. $(X_n)_{n\geq 0}$ is a square-integrable martingale whose unconditional mean is $m = \mathbb{E}X_0$. Then for any constant $\lambda > 0$,

$$\mathbb{P}\left(\max_{0\leq k\leq n} |X_k - m| \geq \lambda\right) \leq \frac{\mathrm{Var}(X_n)}{\lambda^2}. \tag{20.2.42}$$

Remark. Notice the analogy with Chebyshev inequality (Theorem 19.3.21). Of course, the conclusion is much stronger than Chebyshev inequality.

Proof. Apply Kolmogorov's inequality (Theorem 20.2.18) to $(X_n - m)^2$, which is a submartingale by Jensen's inequality. □

20.2.6 Convergence in $\mathcal{L}^p$ for $p \in (1, \infty)$

We have seen that $X_n \to X_\infty$ a.s. if X is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. When can we upgrade this to convergence in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$?

Definition 20.2.4. When $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ a.s. for all $n \geq 0$ for some random variable $Z \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ then $(X_n)_{n\geq 0}$ is a martingale (by Proposition 19.4.28 (tower property)), and if $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ then we say that X is closed in $\mathcal{L}^p$.

Theorem 20.2.20. Let $(X_n)_{n\geq 0}$ be a martingale and $p \in (1, \infty]$. Then the following statements are equivalent:

(i) $X = (X_n)_{n\geq 0}$ is bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, i.e., $\sup_n \|X_n\|_p < \infty$ (Definition 19.3.5).

(ii) $X_n \to X_\infty$ a.s. and in $\mathcal{L}^p$.

(iii) $X = (X_n)_{n\geq 0}$ is closed in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, i.e., there exists a random variable $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ such that

$$X_n = \mathbb{E}(Z|\mathcal{F}_n) \quad \text{a.s. for all } n. \tag{20.2.43}$$

Proof. (i) ⇒ (ii). $X_n \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ for all n since X is bounded in $\mathcal{L}^p$. Consider the convex function $f(x) = |x|^p$. By Jensen inequality (Theorem 19.3.22) we have

$$f(\mathbb{E}(X_n)) \leq \mathbb{E}(f(X_n)) \;\Rightarrow\; (\mathbb{E}|X_n|)^p \leq \mathbb{E}(|X_n|^p) \;\Rightarrow\; \|X_n\|_1 \leq \|X_n\|_p \tag{20.2.44}$$

for $p \in (1, \infty)$. For $p = \infty$, we have the same result by Definition 15.4.2 and Theorem 15.3.7. Thus, bounded in $\mathcal{L}^p$ implies bounded in $\mathcal{L}^1$, so by the martingale convergence theorem (Theorem 20.2.13), X_n converges a.s. to a random variable

$X_\infty \in \mathcal{L}^1(\Omega, \mathcal{F}_\infty, \mathbb{P})$. Then if $p \in (1,\infty)$, $|X_n| \to |X_\infty|$ a.s. and $|X_n|^p \to |X_\infty|^p$ a.s.. So $|X_\infty|^p = \lim_{n\to\infty} |X_n|^p$ a.s.. Then

$$\begin{aligned}
\mathbb{E}\left(|X_\infty|^p\right) &= \mathbb{E}\left(\liminf_n |X_n|^p\right) \qquad \text{(Theorem 15.3.7)} \\
&\le \liminf_n \mathbb{E}\left(|X_n|^p\right) \qquad \text{(Fatou's lemma (Lemma 15.3.11))} \\
&\le \sup_{n\ge 0} \|X_n\|_p^p < \infty.
\end{aligned}$$

If $p = \infty$, $\|X_\infty\|_p = \inf\{\lambda : |X_\infty| \le \lambda \text{ a.s.}\} < \infty$ since $X_\infty \in \mathcal{L}^1(\Omega, \mathcal{F}_\infty, \mathbb{P})$ is integrable. Thus, $X_\infty \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$.

By Doob's $\mathcal{L}^p$-inequality (Theorem 20.2.17),

$$\|X_n^*\|_p \le \frac{p}{p-1}\|X_n\|_p \le \frac{p}{p-1}\sup_{n\ge 0}\|X_n\|_p. \tag{20.2.45}$$

Recalling that $X_n^* = \sup_{0\le k\le n}|X_k|$, we have $X_n^* \uparrow X_\infty^*$. Then by monotone convergence theorem (Theorem 19.3.6),

$$\|X_\infty^*\|_p \le \frac{p}{p-1}\sup_{n\ge 0}\|X_n\|_p < \infty. \qquad \text{(also holds for } p=\infty) \tag{20.2.46}$$

Thus, we have $X_\infty^* \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. Thus,

$$|X_n - X_\infty| \le |X_n| + |X_\infty| \le 2X_\infty^* \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}) \tag{20.2.47}$$

If $p \in (1,\infty)$, we have $|X_n - X_\infty|^p \le 2^p (X_\infty^*)^p \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Also, $|X_n - X_\infty|^p \to 0$ a.s.. Then by dominated convergence theorem (Theorem 19.3.8),

$$\mathbb{E}\left(|X_n - X_\infty|^p\right) \to 0 \;\Rightarrow\; X_n \overset{\mathcal{L}^p}{\to} X_\infty. \tag{20.2.48}$$

If $p = \infty$, we have

$$\|X_n - X_\infty\|_\infty = \inf\{\lambda : |X_n - X_\infty| \le \lambda, \text{a.s.}\} \to 0 \text{ as } n \to \infty. \tag{20.2.49}$$

since $X_n \to X_\infty$ a.s. Thus, $X_n \overset{\mathcal{L}^p}{\to} X_\infty$ for $p \in (1,\infty]$.

(ii) $\Rightarrow$ (iii). We set $Z = X_\infty$. Clearly, $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. We will now show that $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ a.s..

If $m \ge n$, then by martingale property we can have the following. If $p \in (1,\infty)$ and

$$\|X_n - \mathbb{E}(X_\infty|\mathcal{F}_n)\|_p = \|\mathbb{E}(X_m - X_\infty|\mathcal{F}_n)\|_p \le \|X_m - X_\infty\|_p \to 0 \text{ as } m \to \infty \tag{20.2.50}$$

by conditional Jensen's inequality (Theorem 19.4.26) and Proposition 19.4.28 (tower property). Thus, $X_n = \mathbb{E}(X_\infty|\mathcal{F}_n)$ a.s. by Theorem 15.3.10.

If $p = \infty$,

$$\begin{aligned}
\|X_n - \mathbb{E}(X_\infty|\mathcal{F}_n)\|_\infty &= \inf\left(\lambda : |X_n - \mathbb{E}(X_\infty|\mathcal{F}_n)| \le \lambda \text{ a.s.}\right) = \inf\left(\lambda : |\mathbb{E}(X_m - X_\infty|\mathcal{F}_n)| \le \lambda \text{ a.s.}\right) \\
&\le \inf\left(\lambda : \mathbb{E}(|X_m - X_\infty|\,|\mathcal{F}_n) \le \lambda \text{ a.s.}\right) \quad \text{(conditional Jensen's inequality (Theorem 19.4.26))} \\
&\to 0 \text{ as } m \to \infty.
\end{aligned}$$

Thus, $\|X_n - \mathbb{E}(X_\infty|\mathcal{F}_n)\|_\infty = 0$ and thus $X_n = \mathbb{E}(X_\infty|\mathcal{F}_n)$ a.s.

(iii) $\Rightarrow$ (i): Suppose $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ a.s. for some $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. If $p \in (1,\infty)$, by conditional Jensen inequality (Theorem 19.4.26),

$$|X_n|^p = \left(\mathbb{E}(|Z|\,|\mathcal{F}_n)\right)^p \le \mathbb{E}(|Z|^p\,|\mathcal{F}_n) \;\Rightarrow\; \mathbb{E}(|X_n|^p) \le \mathbb{E}(|Z|^p) \;\Rightarrow\; \sup_{n\ge 0}\mathbb{E}(|X_n|^p) \le \mathbb{E}(|Z|^p) < \infty. \tag{20.2.51}$$

If $p = \infty$, by conditional Jensen inequality (Theorem 19.4.26) again, since $\lambda_Z := \|Z\|_\infty = \inf\{\lambda : |Z| \le \lambda \text{ a.s.}\} < \infty$

$$\|X_n\|_\infty = \inf\{\lambda : |\mathbb{E}(Z|\mathcal{F}_n)| \le \lambda \text{ a.s.}\} \le \inf\{\lambda : \mathbb{E}(|Z|\,|\mathcal{F}_n) \le \lambda, \text{ a.s.}\} \tag{20.2.52}$$

Note that we can have that $\mathbb{E}(|Z||\mathcal{F}_n) \leq \lambda_Z$, thus,

$$\|X_n\|_\infty \leq \lambda_Z = \|Z\|_\infty < \infty. \tag{20.2.53}$$

Thus, in both cases, X_n is bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. □

Corollary 20.2.21. Let $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ and $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ a martingale closed in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. Then we have

$$X_n \to X_\infty \text{ as } n \to \infty \text{ a.s. and in } \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P}) \quad \text{with} \quad X_\infty = \mathbb{E}(Z|\mathcal{F}_\infty) \text{ a.s.} \tag{20.2.54}$$

Proof. By Theorem 20.2.20 we have that $X_n \to X_\infty$ as $n \to \infty$ a.s. and in $\mathcal{L}^p$. It only remains to show that $X_\infty = \mathbb{E}(Z|\mathcal{F}_\infty)$ a.s. Clearly X_∞ is $\mathcal{F}_\infty$-measurable.

Let $A \in \bigcup_{n\geq 0} \mathcal{F}_n$. Then $A \in \mathcal{F}_N$ for some N and by dominated convergence theorem (Theorem 19.3.8)

$$\mathbb{E}[Z\mathbb{1}_A] = \mathbb{E}(\mathbb{E}(Z|\mathcal{F}_N)\mathbb{1}_A) = \mathbb{E}(X_N\mathbb{1}_A) \to \mathbb{E}(X_\infty\mathbb{1}_A) \text{ as } N \to \infty. \tag{20.2.55}$$

So this shows that for all $A \in \bigcup_{n\geq 0} \mathcal{F}_n$ we have

$$\mathbb{E}(X_\infty\mathbb{1}_A) = \mathbb{E}(\mathbb{E}(Z|\mathcal{F}_\infty)\mathbb{1}_A). \tag{20.2.56}$$

But $\bigcup_{n\geq 0} \mathcal{F}_n$ is a π-system generating $\mathcal{F}_\infty$, and hence we get the equality for all $A \in \mathcal{F}_\infty$ by Theorem 19.4.18. □

Remark. In particular, if $\mathcal{F} = \mathcal{F}_\infty$ then X_∞ is the only possible Z ($X_\infty = \mathbb{E}(Z|\mathcal{F}_\infty) = \mathbb{E}(Z|\mathcal{F}) = Z$ a.s. since Z is $\mathcal{F}$-measurable) for which $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ for all n. Yet otherwise said,

$$\mathcal{L}^p(\Omega, \mathcal{F}_\infty, \mathbb{P}) \;\to\; \{\mathcal{L}^p\text{-bounded martingales}\} : Z \to (\mathbb{E}(Z|\mathcal{F}_n))_{n\geq 0} \text{ is a bijection.} \tag{20.2.57}$$

20.2.7 UI martingale and convergence in $\mathcal{L}^1$

Recall Definition 19.3.6,

Definition 20.2.5 (UI martingale)**.** A martingale $(X_n)_{n\geq 0}$ is called a UI martingale if it is a martingale and the collection of random variables $(X_n)_{n\geq 0}$ is a UI familty, i.e.,

$$\sup_{n\geq 0} \mathbb{E}\left(|X_n|\mathbb{1}_{\{|X_n|>K\}}\right) \to 0 \text{ as } K \to \infty. \tag{20.2.58}$$

Theorem 20.2.22 (UI martingale convergence theorem, discrete-time)**.** Let $(X_n)_{n\geq 0}$ be a martingale. The following are equivalent:

(i) $(X_n)_{n\geq 0}$ is uniformly integrable.

(ii) $X_n \to X_\infty$ a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$.

(iii) $(X_n)_{n\geq 0}$ is closed in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, i.e., there exists a random variable $Z \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ such that

$$X_n = \mathbb{E}(Z|\mathcal{F}_n) \quad \text{a.s. for all } n. \tag{20.2.59}$$

Proof. (i) ⇒ (ii). Since X is UI, it follows that it is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ (Definition 19.3.6), so $X_n \to X_\infty$ a.s. by the martingale convergence theorem (Theorem 20.2.13). Then Theorem 19.3.36 implies that $X_n \to X_\infty$ in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ since X is UI.

(ii) ⇒ (iii). We set $Z = X_\infty$. Clearly, $Z \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. We will now show that $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ a.s..

If $m \geq n$, then by martingale property we can have the following.

$$\mathbb{E}|X_n - \mathbb{E}(X_\infty|\mathcal{F}_n)| = \mathbb{E}|\mathbb{E}(X_m - X_\infty|\mathcal{F}_n)| \leq \mathbb{E}|X_m - X_\infty| \to 0 \text{ as } m \to \infty \tag{20.2.60}$$

by conditional Jensen's inequality (Theorem 19.4.26) and Proposition 19.4.28.(i) (tower property). Thus, $X_n = \mathbb{E}(X_\infty|\mathcal{F}_n)$ a.s. by Theorem 15.3.10.

(iii) ⇒ (i). Theorem 19.4.30 implies that $(\mathbb{E}[Z|\mathcal{F}_n])_{n\geq 0}$ is UI for any $Z \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. □

Remark. As before (Corollary 20.2.21), $Z = X_\infty$ is the only $\mathcal{F}_\infty$-measurable r.v. for which $X_n = \mathbb{E}(Z|\mathcal{F}_n)$ for all n. Similarly,

$$\mathcal{L}^1(\Omega, \mathcal{F}_\infty, \mathbb{P}) \ \to \ \{\text{UI martingales}\} : Z \to (\mathbb{E}(Z|\mathcal{F}_n))_{n\geq 0} \quad \text{is a bijection.} \tag{20.2.61}$$

Proposition 20.2.23. If X is a UI supermartingale (resp. submartingale), then X_n converges a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ to a limit X_∞, so that $\mathbb{E}(X_\infty|\mathcal{F}_n) \leq X_n$ (resp. $\geq$) for every n.

Proof. [11] □

Example 20.2.24. Let $(X_n)_{n\geq 0}$ be i.i.d. random variables with $\mathbb{P}(X_1 = 0) = \mathbb{P}(X_1 = 2) = 1/2$. Then $Y_n = X_1 \dots X_n$ is a martingale bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and it converges to 0 as $n \to \infty$ a.s. But $\mathbb{E}(Y_n) = 1$ for all n, and hence it does not converge in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$.

If X is a UI martingale and T is a stopping time, which could also take the value ∞, then we can unambiguously define

$$X_T = \sum_{n=0}^{\infty} X_n \mathbb{1}_{\{T=n\}} + X_\infty \mathbb{1}_{\{T=\infty\}}. \tag{20.2.62}$$

Recall Theorem 20.2.7: $\mathbb{E}[X_T|\mathcal{F}_S] = X_S$ when $S \leq T$ are bounded stopping times. It turns out that we may eliminate the boundedness of the stopping times when the martingale is UI.

Theorem 20.2.25 (optional stopping theoerem, UI martingale, discrete-time)**.** Let $(X_n)_{n\geq 0}$ be a uniformly integrable martingale and let S and T be stopping times with $S \leq T$. Then $\mathbb{E}(X_T|\mathcal{F}_S) = X_S$, where we take $X_T = X_T \mathbb{1}_{\{T<\infty\}} + X_\infty \mathbb{1}_{\{T=\infty\}}$. In particular, in this case $\mathbb{E}(X_T) = \mathbb{E}(X_0)$.

Proof. We will first show that $\mathbb{E}(X_\infty|\mathcal{F}_T) = X_T$ a.s. for any stopping time T.

We will now check that $X_T \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Since $(X_n)_{n\geq 0}$ is UI, there exists X_∞ such that $X_n = \mathbb{E}(X_\infty|\mathcal{F}_n)$ by Theorem 20.2.22. Thus,

$$|X_n| = |\mathbb{E}(X_\infty|\mathcal{F}_n)| \leq \mathbb{E}(|X_\infty||\mathcal{F}_n), \tag{20.2.63}$$

by conditional Jensen's inequality (Theorem 19.4.26). We have

$$X_T = X_\infty \mathbb{1}_{\{T=\infty\}} + \sum_{n\geq 0} X_n \mathbb{1}_{\{T=n\}} = X_\infty \mathbb{1}_{\{T=\infty\}} + \sum_{n\geq 0} \mathbb{E}(X_\infty|\mathcal{F}_n) \mathbb{1}_{\{T=n\}} \tag{20.2.64}$$

by uniform integrability. Therefore

$$|X_T| \leq |X_\infty| \mathbb{1}_{\{T=\infty\}} + \sum_{n\geq 0} \mathbb{E}\left(|X_\infty| \mathbb{1}_{\{T=n\}}|\mathcal{F}_n\right) \ \Rightarrow \ \mathbb{E}|X_T| \leq \sum_{n\in\mathbb{Z}^+\cup\{\infty\}} \mathbb{E}\left(|X_\infty| \mathbb{1}_{\{T=n\}}\right) = \mathbb{E}|X_\infty| < \infty. \tag{20.2.65}$$

Thus, X_T is integrable ($X_T \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$). Let $A \in \mathcal{F}_T$. Then since $X_n = \mathbb{E}(X_\infty|\mathcal{F}_n)$

$$\begin{aligned} \mathbb{E}(X_T \mathbb{1}_A) &= \sum_{n\in\mathbb{Z}^+\cup\{\infty\}} \mathbb{E}\left(X_n \mathbb{1}_{\{T=n\}} \mathbb{1}_A\right) = \sum_{n\in\mathbb{Z}^+\cup\{\infty\}} \mathbb{E}\left(\mathbb{E}(X_\infty|\mathcal{F}_n) \mathbb{1}_{\{T=n\}} \mathbb{1}_A\right) \\ &= \sum_{n\in\mathbb{Z}^+\cup\{\infty\}} \mathbb{E}\left(X_\infty \mathbb{1}_{\{T=n\}} \mathbb{1}_A\right) = \mathbb{E}(X_\infty \mathbb{1}_A). \end{aligned}$$

Also, clearly X_T is $\mathcal{F}_T$-measurable, and hence

$$\mathbb{E}(X_\infty|\mathcal{F}_T) = X_T \text{ a.s.} \tag{20.2.66}$$

Now using the tower property of conditional expectation (Proposition 19.4.28.(i)), we get for stopping times $S \leq T$, since $\mathcal{F}_S \subseteq \mathcal{F}_T$,

$$\mathbb{E}(X_T|\mathcal{F}_S) = \mathbb{E}(\mathbb{E}(X_\infty|\mathcal{F}_T)|\mathcal{F}_S) = \mathbb{E}(X_\infty|\mathcal{F}_S) = X_S \text{ a.s.} \tag{20.2.67}$$

The first equality is by Theorem 15.3.10. □

[11] need proof

20.2.8 Backward martingales

Definition 20.2.6 (backward martingale, discrete)**.** Let $\cdots \subseteq \mathcal{F}_2 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_0$ be a sequence of sub-σ-algebras indexed by $\mathbb{Z}^- = \{\ldots, -2, -1, 0\}$. Given such a filtration, a process $(X_n)_{n\leq 0}$ is called a backwards martingale, if it is adapted to the filtration, $X_0 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and for all $n \leq -1$ we have

$$\mathbb{E}\left(X_{n+1}|\mathcal{F}_n\right) = X_n \text{ a.s.} \tag{20.2.68}$$

Remark. By the tower property of conditional expectation (Proposition 19.4.28.(i)) we get that for all $n \leq 0$

$$\mathbb{E}\left(X_0|\mathcal{F}_n\right) = \mathbb{E}\left(\mathbb{E}\left(X_n|\mathcal{F}_0\right)|\mathcal{F}_n\right) = X_n \text{ a.s..} \tag{20.2.69}$$

Since $X_0 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, by Theorem 19.4.30 we get that X is uniformly integrable (then by Theorem 20.2.22, X is closed in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$). This is a nice property that backwards martingales have: they are automatically UI.

Theorem 20.2.26 (backwards martingale convergence theorem, discrete)**.** Let X be a backwards martingale, with $X_0 \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ for some $p \in [1, \infty)$. Then X_n converges a.s. and in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ as $n \to -\infty$ to the random variable $X_{-\infty} = \mathbb{E}\left(X_0|\mathcal{F}_{-\infty}\right)$, where $\mathcal{F}_{-\infty} = \bigcap_{n\leq 0} \mathcal{F}_n$ is a σ-algebra (see measure theorey (Chapter 15)).

Proof. We will first adapt Doob's up-crossing inequality (Lemma 20.2.12), in this setting. Let $a < b$ be real numbers and $N_{-n}(X, [a, b])$ be the number of up-crossings of the interval $[a, b]$ by X between times $-n$ and 0.

If we write $\mathcal{G}_k = \mathcal{F}_{-n+k}$, for $0 \leq k \leq n$, then $\mathcal{G}_k$ is an increasing filtration and the process $(Y_k = X_{-n+k})_{0\leq k\leq n}$ is an $\mathcal{G}_\infty$-martingale. Then $N_{-n}(X, [a, b]) = N_n(Y, [a, b])$ is the number of up-crossings of the interval $[a, b]$ by Y_k between times 0 and n. Thus applying Doob's up-crossing inequality (Lemma 20.2.12) to Y_k we get that

$$(b-a)\mathbb{E}\left(N_{-n}(X, [a, b])\right) = (b-a)\mathbb{E}\left(N_n(Y, [a, b])\right) \leq \mathbb{E}\left((Y_n - a)^-\right) = \mathbb{E}\left((X_0 - a)^-\right). \tag{20.2.70}$$

Letting $n \to \infty$ we have that $N_{-n}(X, [a, b])$ increases to the total number of up-crossings of X from a to b and thus

$$(b-a)\mathbb{E}\left(N_{-n}(X, [a, b])\right) \uparrow (b-a)\mathbb{E}\left(N(X, [a, b])\right) \leq \mathbb{E}|X_0| + a < \infty \tag{20.2.71}$$

since $X_0 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Therefore, forall $a < b \in \mathbb{Q}$, $N(X, [a, b]) < \infty$ a.s. so by the similar argument in proof of martingale convergence theorem (Theorem 20.2.13))

$$X_m \to X_{-\infty} \text{ a.s. as } m \to -\infty. \tag{20.2.72}$$

for some random variable $X_{-\infty}$, which is $\mathcal{F}_{-\infty}$-measurable, since the σ-algebras $\mathcal{F}_n$ are decreasing ($X_{-\infty}$ is $\mathcal{F}_n$-measurable for all n).

By conditional Jensen's inequality (Theorem 19.4.26),

$$|\mathbb{E}\left(X_0|\mathcal{F}_n\right)|^p \leq \mathbb{E}\left(|X_0|^p|\mathcal{F}_n\right) \text{ a.s..} \tag{20.2.73}$$

It follows that by Theorem 15.3.10 and the tower property of conditional expectation (Proposition 19.4.28.(i))

$$\mathbb{E}\left(|X_n|^p\right) = \mathbb{E}\left(|\mathbb{E}\left(X_0|\mathcal{F}_n\right)|^p\right) \leq \mathbb{E}\left(\mathbb{E}\left(|X_0|^p|\mathcal{F}_n\right)\right) = \mathbb{E}\left(|X_0|^p\right) < \infty \tag{20.2.74}$$

since $X_0 \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. Thus, $X_n \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, for all $n \leq 0$. Also, by Fatou's lemma (Lemma 15.3.11), we get that

$$\mathbb{E}|X_{-\infty}|^p = \mathbb{E}\left(\liminf_n |X_n|^p\right) \leq \liminf_n \mathbb{E}\left(|X_n|^p\right) < \infty. \tag{20.2.75}$$

So $X_{-\infty} \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$. Now by conditional Jensen's inequality (Theorem 19.4.26) we obtain (since $X_{-\infty}$ is $\mathcal{F}_n$-measurable for all n)

$$|X_n - X_{-\infty}|^p = |\mathbb{E}\left(X_0|\mathcal{F}_n\right) - X_{-\infty}|^p = |\mathbb{E}\left(X_0 - X_{-\infty}|\mathcal{F}_n\right)|^p \leq \mathbb{E}\left(|X_0 - X_{-\infty}|^p|\mathcal{F}_n\right) \tag{20.2.76}$$

Since $(Z_n)_{n\leq 0} = \left(\mathbb{E}\left(|X_0 - X_{-\infty}|^p|\mathcal{F}_n\right)\right)_{n\leq 0}$ is a family of random variables, it is UI by Theorem 19.4.30. Then by Theorem 15.4.21

$$\sup_{n\leq 0} \mathbb{E}\left(|X_n - X_{-\infty}|^p \mathbb{1}_{\{|X_n - X_{-\infty}|^p > K\}}\right) \leq \sup_{n\leq 0} \mathbb{E}\left(|Z_n| \mathbb{1}_{\{|Z_n| > K\}}\right) \to 0 \text{ as } K \to \infty. \tag{20.2.77}$$

Thus, $(\mathbb{E}(|X_0 - X_{-\infty}|^p|\mathcal{F}_n))_{n\leq 0}$ is UI and $|X_0 - X_{-\infty}|^p \to 0$ a.s.. Then by Theorem 19.3.36 and Theorem 20.2.22 (Or we can use Theorem 19.3.38 directly), we have $X_n \to X$ in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ as $n \to -\infty$.

Now $\forall A \in \mathcal{F}_{-\infty}$. Since $A \in \mathcal{F}_n$, for all $n \leq 0$, we have by the martingale property that and the tower property of conditional expectation (Proposition 19.4.28.(i))

$$\mathbb{E}(X_n \mathbb{1}_A) = \mathbb{E}(\mathbb{E}(X_0|\mathcal{F}_n)\mathbb{1}_A) = \mathbb{E}(\mathbb{E}(X_0\mathbb{1}_A|\mathcal{F}_n)) = \mathbb{E}(X_0\mathbb{1}_A) \tag{20.2.78}$$

Letting $n \to -\infty$ in the above equality and using the $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ convergence of X_n to $X_{-\infty}$,

$$\mathbb{E}(X_0\mathbb{1}_A) = \mathbb{E}(X_n\mathbb{1}_A) \to \mathbb{E}(X_{-\infty}\mathbb{1}_A). \tag{20.2.79}$$

Thus, $X_{-\infty} = \mathbb{E}(X_0|\mathcal{F}_{-\infty})$ a.s.. □

Remark. Sometimes backwards martingales are defined as a forwards process $(Y_n, n \geq 0)$ with respect to a backwards filtration $\mathcal{G}_0 \supseteq \mathcal{G}_1 \supseteq \mathcal{G}_2 \supseteq \dots$ such that Y_n is adapted and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, and $\mathbb{E}(Y_n|\mathcal{G}_{n+1}) = Y_{n+1}$. This is equivalent to our definition by taking $Y_n = X_{-n}$ and $\mathcal{G}_n = \mathcal{F}_{-n}$ for all $n \geq 0$.

20.3 Applications of Discrete Time Martingales

20.3.1 Strong law of large numbers

Now we give the alternative proof of the strong law of large numbers (Comparing with Theorem 19.9.9).

Theorem 20.3.1 (strong law of large numbers)**.** Let $X_1, X_2, \dots$ be i.i.d. random variables in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ with $\mu = \mathbb{E}(X_1)$. Let $S_n = X_1 + \cdots + X_n$, for $n \geq 1$ and $S_0 = 0$. Then $S_n/n \to \mu$ a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ as $n \to \infty$.

Proof. Let

$$\mathcal{G}_n = \sigma(S_n, S_{n+1}, \dots) = \sigma(S_n, X_{n+1}, X_{n+2}, \dots). \tag{20.3.1}$$

Let $(\mathcal{F}_n)_{n\leq -1} = (\mathcal{G}_{-n})_{n\leq -1}$. Thus, $\mathcal{F}_{-\infty} \subseteq \cdots \subseteq \mathcal{F}_{-1}$ We will now show that $(M_n)_{n\leq -1} = \left(\frac{S_{-n}}{-n}\right)_{n\leq -1}$ is a backwards martingale with respect to $(\mathcal{F}_n)_{n\leq -1}$. We have for $m \leq -1$ (M_n is integrable so $\mathbb{E}(M_{m+1}|\mathcal{F}_m)$ is well-defined),

$$\mathbb{E}(M_{m+1}|\mathcal{F}_m) = \mathbb{E}\left(\frac{S_{-m-1}}{-m-1}\middle|\mathcal{G}_{-m}\right). \tag{20.3.2}$$

Setting $n = -m$, since X_n is independent of $X_{n+1}, X_{n+2}, \dots$, we obtain (by Proposition 19.4.20.(ii))

$$\mathbb{E}\left(\frac{S_{n-1}}{n-1}\middle|\mathcal{G}_n\right) = \mathbb{E}\left(\frac{S_n - X_n}{n-1}\middle|\mathcal{G}_n\right) = \frac{S_n}{n-1} - \mathbb{E}\left(\frac{X_n}{n-1}\middle|\mathcal{G}_n\right) \text{ a.s.} \tag{20.3.3}$$

By symmetry, notice that $\mathbb{E}(X_k|\mathcal{G}_n) = \mathbb{E}(X_1|\mathcal{G}_n)$ for all $k \in \{1, 2, \dots, n\}$. Indeed, for any $A \in \mathcal{B}(\mathbb{R})$ we have that $\mathbb{E}\left(X_k\mathbb{1}_{\{S_n\in A\}}\right)$ does not depend on k. Clearly,

$$\mathbb{E}(X_1|\mathcal{G}_n) + \cdots + \mathbb{E}(X_n|\mathcal{G}_n) = \mathbb{E}(S_n|\mathcal{G}_n) = S_n \text{ a.s. } \Rightarrow \mathbb{E}(X_n|\mathcal{G}_n) = S_n/n \text{ a.s.} \tag{20.3.4}$$

Finally putting everything together we get

$$\mathbb{E}(M_{-n+1}|\mathcal{F}_{-n}) = \mathbb{E}\left(\frac{S_{n-1}}{n-1}\middle|\mathcal{G}_n\right) = \frac{S_n}{n-1} - \frac{S_n}{n(n-1)} = \frac{S_n}{n} = M_{-n} \text{ a.s.} \tag{20.3.5}$$

Also $M_{-1} = X_1$ is integrable, so M is a backwards martingale. Then by backwards martingale convergence theorem (Theorem 20.2.26, $X_1 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$), $M_{-n} = \frac{S_n}{n}$ converges a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ to a random variable, $M_{-\infty} \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Obviously, martingale property and dominated convergence theorem (Theorem 19.3.8) give that

$$\mu = \mathbb{E}(X_1) = \mathbb{E}\left(\frac{X_1}{1}\right) = \mathbb{E}(M_{-1}) = \mathbb{E}(M_{-n}) \to \mathbb{E}(M_{-\infty}), \quad (*) \tag{20.3.6}$$

Obviously, for all k,

$$M_{-\infty} = \lim \frac{S_n}{n} = \lim \frac{S_n - S_k}{n} = \lim \frac{X_{k+1} + \dots X_n}{n}. \tag{20.3.7}$$

Thus, $M_{-\infty}$ is $\mathcal{T}_k = \sigma(X_{k+1}, \dots)$-measurable, for all k, hence it is $\mathcal{T}_\infty = \bigcap_k \mathcal{T}_k$-measurable. Then by Kolmogorov's 0-1 law (Theorem 19.2.12), we conclude that there exists a constant $c \in \mathbb{R}$ such that $\mathbb{P}(M_{-\infty} = c) = 1$. But by $(*)$

$$c = \mathbb{E}(M_{-\infty}) = \mu. \tag{20.3.8}$$

Thus, $M_{-n} = S_n/n \to c = \mu$ a.s.. □

20.3.2 Kakutani's theorem for product martingales

Definition 20.3.1 (product martingale)**.** A product martingale is a martingale of the form $X_n = \prod_{i=1}^n Y_i$, where the Y_i are independent, non-negative random variables such that $\mathbb{E}(Y_i) = 1$ for all $i = 1, \dots, n$.

Remark. A product martingale is indeed a martingale, since $\mathbb{E}(X_n) = \prod_{i=1}^n \mathbb{E}(Y_i) = 1$ by independence (Theorem 19.5.4), and

$$\mathbb{E}(X_{n+1}|\mathcal{F}_n) = \mathbb{E}(Y_{n+1}X_n|\mathcal{F}_n) = X_n\mathbb{E}(Y_{n+1}|\mathcal{F}_n) = X_n\mathbb{E}(Y_{n+1}) = X_n, \tag{20.3.9}$$

since Y_{n+1} is independent of $\mathcal{F}_n$, where $\mathcal{F}_n := \mathcal{F}_n^X = \sigma(X_1, \dots, X_n) = \sigma(Y_1, \dots, Y_n)$.

Now $X_n \geq 0$, so $X_n \to X_\infty \geq 0$ finite a.s. as $n \to \infty$ by martingale convergence theorem (Theorem 20.2.13).

Theorem 20.3.2 (Kakutani's product martingale theorem)**.** With the notation in Definition 20.3.1, $X_n \to X_\infty \geq 0$ finite a.s.. Let $a_n = \mathbb{E}\left(\sqrt{Y_n}\right)$. The following are equivalent.

(i) $(X_n)_{n\geq 0}$ is a UI martingale.

(ii) $\mathbb{E}(X_\infty) = 1$.

(iii) $\mathbb{P}(X_\infty > 0) > 0$.

(iv) $\prod_{n\geq 1} a_n > 0$.

Proof. (iii) $\Rightarrow$ (iv): Suppose that $\prod_{n\geq 0} a_n = 0$. Let $M_n = \prod_{i=1}^n \frac{\sqrt{Y_i}}{a_i}$, so that M_n is also a (non-negative) product martingale (M is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$). By the martingale convergence theorem, $M_n \to M_\infty \geq 0$ a.s. where M_∞ is finite a.s.. We have $M_n = \frac{1}{\prod_{i=1}^n a_i}\sqrt{X_n}$, so $X_n = M_n^2 \prod_{i=1}^n a_i^2 \to 0$ a.s. as $n \to \infty$ since M_∞ is finite valued a.s. and $\prod_{n\geq 0} a_n = 0$. Thus $X_\infty \equiv 0$ a.s. and the contrapositive is proved.

(iv) $\Rightarrow$ (i): Assume that $\prod_{n\geq 0} a_n > 0$. Then since $a_n \in [0, 1]$,

$$\mathbb{E}\left(M_n^2\right) = \mathbb{E}\left(\frac{X_n}{\prod_{i=1}^n a_i^2}\right) = \frac{1}{\prod_{i=1}^n a_i^2} \leq \frac{1}{\prod_{i\geq 0} a_i^2} < \infty. \tag{20.3.10}$$

Therefore M is bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. Doob's inequality (Theorem 20.2.17) gives that

$$\mathbb{E}\left((M_n^*)^2\right) \leq \left(\frac{2}{2-1}\right)^2 \mathbb{E}\left(M_n^2\right) \leq \frac{4}{\prod_{i\geq 1} a_i^2} < \infty, \tag{20.3.11}$$

where $M_n^* = \sup_{1\leq i\leq n} M_i$. Also we have $|X_n| = |M_n|^2 \left(\prod_{i=1}^n a_i\right)^2 \leq |M_n|^2$ and M_n is non-negative,

$$\mathbb{E}\left(\sup_{1\leq i\leq n} |X_i|\right) \leq \mathbb{E}\left(\sup_{1\leq i\leq n} |M_n|^2\right) = \mathbb{E}\left(\left(\sup_{1\leq i\leq n} |M_n|\right)^2\right) = \mathbb{E}\left((M_n^*)^2\right) < \infty. \tag{20.3.12}$$

Then $\sup_{1\leq i\leq n} |X_i| \uparrow \sup_{n\geq 0} |X_n| := X^*$, by monotone convergence theomem (Theorem 19.3.6), $\mathbb{E}(X^*) < \infty$. We see that X_n is dominated by the integrable random variable X^*. Then $(X_n)_{n\geq 0}$ is UI (Theorem 15.4.19).

(i) $\Rightarrow$ (ii): If X is UI then $X_n \to X_\infty$ (finite limit) a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ as $n \to \infty$. We have

$$1 = \mathbb{E}(X_n) \to \mathbb{E}(X_\infty) \tag{20.3.13}$$

by dominated convergence theorem (Theorem 19.3.8).

(ii) $\Rightarrow$ (iii): If $\mathbb{P}(X_\infty > 0) = 0$, $X_\infty = 0$ a.s.. Thus, $\mathbb{E}(X_\infty) = 0$ by Theorem 15.3.10. Contradiction. □

Remark. $\prod_n a_n = 0 \Leftrightarrow X_\infty = 0$ a.s..

By the Cauchy-Schwartz inequality, $\mathbb{E}\left(\sqrt{Y_n}\right)^2 \leq \mathbb{E}(Y_n) = 1$, so $a_n \leq 1$ for all n. Recall that $\prod_{n\geq 1} a_n \in [0,1]$, and $\prod_{n\geq 1} a_n > 0$ if and only if $\sum_{n\geq 1}(1-a_n) < \infty$ (this is seen by taking logarithms since $\ln(1-z) = -z - \frac{z^2}{2} - \frac{z^3}{3} - \dots$).

Remark. In the case that every Y_n is positive a.s. for every n, we are assured that $X_n > 0$ for all n as well. Therefore $\{X_\infty = 0\}$ does not depend on the first few Y_i's, so it is a tail event. By Kolmogorov's 0-1 law (Theorem 19.2.12), $\mathbb{P}(X_\infty = 0) \in \{0,1\}$. In this case, $\mathbb{P}(X_\infty > 0) > 0$ if and only if $\mathbb{P}(X_\infty > 0) = 1$.

20.3.3 Radon-Nikodym theorem

Recall Proposition 15.3.22,

Definition 20.3.2 (Radon-Nikodym derivative)**.** Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Let $\mathbb{Q}$ be a non-negative, finite measure on $(\Omega, \mathcal{F})$. If there exists some non-negative random variable X such that $\mathbb{Q} = X \cdot \mathbb{P}$, in the sense that $\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X \mathbb{1}_A)$ for all $A \in \mathcal{F}$, then X is called a density or Radon-Nikodym derivative of $\mathbb{Q}$ with respect to $\mathbb{P}$ (we can say $\mathbb{Q}$ admits a density X with repect to $\mathbb{P}$), and we write $X = \frac{d\mathbb{Q}}{d\mathbb{P}}$.

Now we would like to find conditions under which $\mathbb{Q}$ admits a density X with repect to $\mathbb{P}$.

Lemma 20.3.3. Let $(\mathcal{F}_n)_{n\geq 0}$ be a filtration on $(\Omega, \mathcal{F})$, with $\mathcal{F}_\infty = \mathcal{F}$[12]. Assume that $\mathbb{Q}|_{\mathcal{F}_n} = X_n \cdot \mathbb{P}|_{\mathcal{F}_n}$ (equivalently, $\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X_n \mathbb{1}_A)$ for all $A \in \mathcal{F}_n$) for some non-negative $\mathcal{F}_n$-measurable random variable X_n, for every n. Then $(X_n)_{n\geq 0}$ is a $(\mathcal{F}_n)_{n\geq 0}$-martingale.

Moreover, $\mathbb{Q}$ admits a density X with respect to $\mathbb{P}$ if and only if the martingale $(X_n)_{n\geq 0}$, defined above, is UI. In this case $X = X_\infty$.

Proof. Let $A \in \mathcal{F}_n$. Then $\mathbb{E}^{\mathbb{P}}(X_{n+1}\mathbb{1}_A) = \mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X_n \mathbb{1}_A)$ since $A \in \mathcal{F}_n \subseteq \mathcal{F}_{n+1}$. Therefore $X_n = \mathbb{E}(X_{n+1}|\mathcal{F}_n)$ a.s.. by Theorem 19.4.18. Adaptedness and Integrability are easily obtained by the definition of X ($\mathbb{E}(X_n) = \mathbb{Q}(\Omega) < \infty$) and X_n (X_n is $\mathcal{F}_n$-measurable random variable).

Assume that $(X_n)_{n\geq 0}$ is UI. Then $X_n \to X_\infty$ a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Hence if $A \in \mathcal{F}_m$ then for $n \geq m$, by martingale property,

$$\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X_m \mathbb{1}_A) = \mathbb{E}^{\mathbb{P}}(X_n \mathbb{1}_A) \to \mathbb{E}^{\mathbb{P}}(X_\infty \mathbb{1}_A) \tag{20.3.14}$$

by $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ convergence (Lemma 19.3.11). Therefore, for all $A \in \bigcup_{n\geq 0} \mathcal{F}_n$ which is a π-system, $\mathbb{E}(X_\infty \mathbb{1}_A) = \mathbb{Q}(A)$, and uniqueness of extension (Theorem 15.1.18) this also holds for every $A \in \mathcal{F}_\infty = \sigma(\bigcup_{n\geq 0} \mathcal{F}_n)$, so X_∞ is a density of $\mathbb{Q}$ with respect to $\mathbb{P}$.

Conversely, assume that $\mathbb{Q} = X \cdot \mathbb{P}$ for some $X \geq 0$. Then for all $A \in \mathcal{F}_n$,

$$\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X \mathbb{1}_A) = \mathbb{E}^{\mathbb{P}}\left(\mathbb{E}^{\mathbb{P}}(X|\mathcal{F}_n)\, \mathbb{1}_A\right) \tag{20.3.15}$$

Thus $\mathbb{Q}|_{\mathcal{F}_n} = \mathbb{E}^{\mathbb{P}}(X|\mathcal{F}_n) \cdot \mathbb{P}|_{\mathcal{F}_n}$. By uniqueness of the density (Theorem 15.3.23), $X_n := \frac{d\mathbb{Q}_n}{d\mathbb{P}_n} = \mathbb{E}^{\mathbb{P}}(X|\mathcal{F}_n)$ a.s.. Also, $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ since $\mathbb{E}^{\mathbb{P}}(X) = \mathbb{Q}(\Omega) < \infty$. Hence, $(X_n)_{n\geq 0}$ is closed in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, it is UI (by Theorem 20.2.22). □

Theorem 20.3.4 (Radon-Nikodym theorem[13])**.** Assume that $\mathcal{F}$ is separable (Definition 15.1.4 i.e., there are countable many events $F_1, F_2, \dots$ such that $\mathcal{F} = \sigma(F_1, F_2, \dots)$). Let $\mathbb{Q}$ be a non-negative finite measure on $(\Omega, \mathcal{F})$ and $\mathbb{P}$ be a probability on $(\Omega, \mathcal{F})$. Then the following are equivalent:

(i) $\mathbb{P}(A) = 0$ implies $\mathbb{Q}(A) = 0$ for all $A \in \mathcal{F}$ (in this case $\mathbb{Q}$ is absolutely continuous[14] with respect to $\mathbb{P}$, and write $\mathbb{Q} \ll \mathbb{P}$).

(ii) For all $\varepsilon > 0$ there is $\delta > 0$ such that for all $A \in \mathcal{F}$, $\mathbb{P}(A) < \delta$ implies $\mathbb{Q}(A) < \varepsilon$.

(iii) There exists a non-negative random variable X such that $\mathbb{Q} = X \cdot \mathbb{P}$ (i.e. $\mathbb{Q}$ admits a density with respect to $\mathbb{P}$), for all $A \in \mathcal{F}$, $\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X \mathbb{1}_A)$.

[12] why we need $\mathcal{F}_\infty = \mathcal{F}$ here?
[13] this should also hold for finite measure, need checking
[14] need definition

Proof. (iii) $\Rightarrow$ (i): Trivial, since if $\mathbb{Q}(A) = \mathbb{E}^{\mathbb{P}}(X\mathbb{1}_A)$ for some X then $\mathbb{P}(A) = 0$ implies $\mathbb{1}_A = 0$ a.s. under $\mathbb{P}$, so $\mathbb{Q}(A) = 0$.

(i) $\Rightarrow$ (ii): Assume that (ii) does not hold. Then there is $\varepsilon > 0$ such that for every $\delta > 0$ there is $B \in \mathcal{F}$ such that $\mathbb{P}(B) < \delta$ and $\mathbb{Q}(B) \geq \varepsilon$. By taking $\delta = \frac{1}{2^n}$, we can find $(B_n)_{n\geq 0} \in \mathcal{F}$ such that $\mathbb{P}(B_n) < \frac{1}{2^n}$, but $\mathbb{Q}(B_n) \geq \varepsilon > 0$. Therefore $\sum_n \mathbb{P}(B_n) < \infty$, so by the first Borel-Cantelli Lemma (Lemma 15.1.13), $\mathbb{P}(B_n \text{ i.o.}) = 0$. On the other hand, by Fatou's lemma (Lemma 15.1.14 since $\mathbb{Q}$ is finite),

$$\mathbb{Q}(B_n \text{ i.o.}) = \mathbb{Q}(\limsup B_n) \geq \limsup \mathbb{Q}(B_n) \geq \varepsilon > 0. \tag{20.3.16}$$

and thus (i) does not hold.

(ii) $\Rightarrow$ (iii): Let $\mathcal{F}_n = \sigma(F_1, \ldots, F_n)$. If we write $\mathcal{A}_n = \{H_1 \cap \cdots \cap H_n : H_i = F_i \text{ or } F_i^c\}$, then it is easy to see that $\mathcal{F}_n = \sigma(\mathcal{A}_n)$. Note that the sets in $\mathcal{A}_n$ are disjoint.

We now let $X_n : \Omega \to [0, \infty)$ be the random variable defined as follows

$$X_n(\omega) = \sum_{A\in\mathcal{A}_n} \frac{\mathbb{Q}(A)}{\mathbb{P}(A)} \mathbb{1}_A. \tag{20.3.17}$$

with the convention that $\frac{0}{0} = 0$. Since the sets in $\mathcal{A}_n$ are disjoint, we get that for all $A \in \mathcal{F}_n$,

$$\mathbb{Q}(A) = \left(\frac{\mathbb{Q}(A)}{\mathbb{P}(A)}\right)\mathbb{P}(A) = \mathbb{E}^{\mathbb{P}}\left(\frac{\mathbb{Q}(A)}{\mathbb{P}(A)}\mathbb{1}_A\right) = \mathbb{E}^{\mathbb{P}}\left(\mathbb{1}_A \sum_{B\in\mathcal{A}_n} \frac{\mathbb{Q}(B)}{\mathbb{P}(B)}\mathbb{1}_B\right) \tag{20.3.18}$$

Therefore $\mathbb{Q}(A) = \mathbb{E}(X_n\mathbb{1}_A)$ for all $A \in \mathcal{F}_n$ $(*)$.

By Lemma 20.3.3, $(X_n)_{n\geq 0}$ is a non-negative martingale with respect to the filtered probability space $(\Omega, \mathcal{F}, (\mathcal{F}_n)_{n\geq 0}, \mathbb{P})$. Now it suffices to show that $(X_n)_{n\geq 0}$ is UI by Lemma 20.3.3. We must check that

$$\sup_{n\geq 0} \mathbb{E}^{\mathbb{P}}\left(X_n \mathbb{1}_{\{X_n>\lambda\}}\right) \to 0 \text{ as } \lambda \to \infty. \tag{20.3.19}$$

But $\mathbb{E}^{\mathbb{P}}\left(X_n\mathbb{1}_{\{X_n>\lambda\}}\right) = \mathbb{Q}(X_n > \lambda)$ since $\{X_n > \lambda\} \in \mathcal{F}_n$ by $(*)$. By (ii), we have that for any $\varepsilon > 0$, $\exists\delta > 0$ such that for all $A \in \mathcal{F}$,

$$\mathbb{P}(A) \leq \delta \;\Rightarrow\; \mathbb{Q}(A) < \varepsilon. \tag{20.3.20}$$

Now we set $\lambda = \mathbb{Q}(\Omega)/\delta$, $A = \{X_n > \lambda\} \in \mathcal{F}$. By Markov's inequality (Theorem 19.3.20)

$$\mathbb{P}(X_n > \lambda) \leq \frac{\mathbb{E}(X_n)}{\lambda} = \frac{\mathbb{Q}(\Omega)}{\lambda} = \delta \;\Rightarrow\; \mathbb{Q}(X_n > \lambda) = \mathbb{E}^{\mathbb{P}}\left(X_n\mathbb{1}_{\{X_n>\lambda\}}\right) < \varepsilon. \tag{20.3.21}$$

Therefore for all $\varepsilon > 0$ there is $\delta > 0$ such that $\sup_{n\geq 0} \mathbb{E}[X_n\mathbb{1}_{X_n>\lambda}] \leq \varepsilon$. Hence $(X_n)_{n\geq 0}$ is UI, and $\mathbb{Q} = X_\infty \cdot \mathbb{P}$. □

20.4 Continuous-time Processes

Now we typically take $I \subseteq \mathbb{R}$ to be an interval, and most of the time we take I to be the non-negative reals, $I = \mathbb{R}^{++} \cup \{0\} = [0, \infty)$ (0 plus the whole positive real line). Also, we consider a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ and $t \in \mathbb{R}^{++}$.

20.4.1 Definition

Definition 20.4.1 (stochastic process, continuous)**.** A (continuous) stochastic process in E, $X = (X_t)_{t\geq 0}$ is a collection of random variables in E where $t \in [0, \infty)$.

Remark. stochastic process is also called random process.

Note that Definition 20.4.1 has no extra constraint.

Definition 20.4.2 (sample continuous process)**.** A stochastic process X is said to be sample continuous if for fixed $\omega \in \Omega$, the sample path $X_t(\omega)$ is continuous in all t a.s.

Definition 20.4.3. If X_t is $\mathbb{R}$-valued, X is integrable if $X_t \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ for every $t \in \mathbb{R}^{++}$, i.e. $\mathbb{E}|X_t| < \infty$.

Definition 20.4.4 (filtration, continuous)**.** A filtration is an increasing family of sub-σ-algebras of $\mathcal{F}$, i.e., if $s \leq t$ then $\mathcal{F}_s \subseteq \mathcal{F}_t$.

Remark. We think of $\mathcal{F}_t$ as 'the information available at and before time t.'

Definition 20.4.5. Let $(\mathcal{F}_t)_{t\geq 0}$ be a filtration. For each t we define

$$\mathcal{F}_{t^+} = \bigcap_{s>t} \mathcal{F}_s. \tag{20.4.1}$$

If $\mathcal{F}_{t^+} = \mathcal{F}_t$ for all t, then we call the filtration $(\mathcal{F}_t)$ right-continuous.

Definition 20.4.6 (filtered probability space, continuous)**.** If $(\mathcal{F}_t)_{t\geq 0}$ is a filtration, we say that $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ is a filtered probability space (or f.p.s.).

Definition 20.4.7 (adapted process, continuous)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. A stochastic process $X = (X_t)_{t\geq 0}$ is adapted to the filtration $(\mathcal{F}_t)_{t\geq 0}$ if X_t is $\mathcal{F}_t$-measurable for all $t \in \mathbb{R}^{++}$. $(X_t)_{t\geq 0}$ is called adapted process (or non-anticipating process).

Definition 20.4.8 (natural filtration, discrete)**.** Let $(X_t)_{t\geq 0}$ be a stochastic process, and let $\mathcal{F}_t^X = \sigma(X_s : s \leq t)$. Then $\mathcal{F}_t^X$ is the natural filtration of X. It is the smallest filtration with respect to which X is adapted.

Definition 20.4.9 (indenpendence of processes)**.** Let $(X_t)_{t\geq 0}$, $(Y_t)_{t\geq 0}$ be two stochastic processes. We say X and Y are independent if $\sigma(X_s : s \geq 0)$ and $\sigma(Y_s : s \geq 0)$ are independent.

Definition 20.4.10 (independent and stationary increments)**.** We say that a process $(X_t)_{t\geq 0}$ has independent and stationary increments if for all $t_1, \ldots, t_n$ the random variables $X_{t_{i+1}} - X_{t_i}$ are mutually independent and their law depends only on $t_{i+1} - t_i$.

Definition 20.4.11 (stopping time, continuous)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. A stopping time with respect to the filtration $(\mathcal{F}_t)_{t\geq 0}$ is a random variable $T : \Omega \to \overline{\mathbb{R}} = \mathbb{R}^{++} \cup \{+\infty\}$ such that $\{T \leq t\} \in \mathcal{F}_t$ for all t.

Proposition 20.4.1. If I is countable (for example, if $I = \mathbb{Z}^+$) then T is a stopping time with respect to $\mathcal{F}_t$ if and only if $\{T = t\} \in \mathcal{F}_t$ for all $t \in I$.

Remark. This is not true in general (if I is not countable [15]).

Proof. '$\Leftarrow$'. If $\{T = t\} \in \mathcal{F}_t$ for all $t \in I$. We have $\{T \leq t\} = \bigcup_{s\leq t} \{T = s\} \in \mathcal{F}_t$ since the union of countable sets.

'$\Rightarrow$'. If $\{T \leq t\} \in \mathcal{F}_t$ for all t, then $\left\{T \leq t - \frac{1}{n}\right\} \in \mathcal{F}_t$, then

$$\{T = t\} = \{T \leq t\} \setminus \{T < t\} = \{T \leq t\} \setminus \left(\bigcup_n \left\{T \leq t - \frac{1}{n}\right\}\right) \in \mathcal{F}_t. \tag{20.4.2}$$

□

Definition 20.4.12. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. Let T be stopping time with respect to $(\mathcal{F}_t)_{t\geq 0}$, and

$$\mathcal{F}_T = \{A \in \mathcal{F} : A \cap \{T \leq t\} \in \mathcal{F}_t \text{ for all } t\}. \tag{20.4.3}$$

This defines a σ-algebra $\mathcal{F}_T$, called the σ-algebra of measurable events before T.

Proof. (i) Since $\{\emptyset \cap \{T \leq t\}\} = \{\emptyset\} \in \mathcal{F}_t$, $\emptyset \in \mathcal{F}_T$.

(ii) If $A \in \mathcal{F}_T$, $A \cap \{T \leq t\} \in \mathcal{F}_t$. Since T is stopping time, $\{T \leq t\} \in \mathcal{F}_t$. Thus, since $\mathcal{F}_t$ is σ-algebra

$$A^c \cap \{T \leq t\} = \{T \leq t\} \setminus (A \cap \{T \leq t\}) \in \mathcal{F}_t. \tag{20.4.4}$$

[15] give an example

(iii) For a sequence $A_m \in \mathcal{F}_T$, we have $A_m \cap \{T \le t\} \in \mathcal{F}_t$ for all n. Thus, since $\mathcal{F}_t$ is σ-algebra

$$\left(\bigcup_m A_m\right) \cap \{T \le t\} = \bigcup_m (A_m \cap \{T \le t\}) \in \mathcal{F}_t \;\Rightarrow\; \bigcup_m A_m \in \mathcal{F}_T. \tag{20.4.5}$$

Thus, $\mathcal{F}_T$ is a σ-algebra. □

Proposition 20.4.2. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\ge 0}, \mathbb{P})$ be a filtered probability space. Let S, T be stopping times. Then

(i) $S \wedge T$ is a stopping times.

(ii) If $S \le T$, $\mathcal{F}_S \subseteq \mathcal{F}_T$.

Proof. (i) Since S, T are stopping times, we have $\{S \le t\} \in \mathcal{F}_t$, $\{T \le t\} \in \mathcal{F}_t$ for all t. Thus,

$$\{S \wedge T \le t\} = \{S \le t\} \cup \{T \le t\} \in \mathcal{F}_t \;\Rightarrow\; S \wedge T \text{ is a stopping time.} \tag{20.4.6}$$

(ii) Since S and T are stopping times, then $\{S \le t\} \in \mathcal{F}_t$, $\{T \le t\} \in \mathcal{F}_t$ with $\{T \le t\} \subseteq \{S \le t\}$ for all t. $\forall A \in \mathcal{F}_S$, we have for all t, $A \cap \{S \le t\} \in \mathcal{F}_t$. Then

$$A \cap \{T \le t\} = A \cap (\{S \le t\} \cap \{T \le t\}) = \underbrace{(A \cap \{S \le t\})}_{\in \mathcal{F}_t} \cap \underbrace{\{T \le t\}}_{\in \mathcal{F}_t} \in \mathcal{F}_t \;\Rightarrow\; A \in \mathcal{F}_T. \tag{20.4.7}$$

□

Proposition 20.4.3. A random variable X is $\mathcal{F}_T$-measurable if and only if $X\mathbb{1}_{\{T\le t\}}$ is $\mathcal{F}_t$-measurable for all t.

Proof. Let $X = \mathbb{1}_A$, $A \in \mathcal{F}$. Then if X is $\mathcal{F}_T$-measurable, $A \in \mathcal{F}_T$, by Definition 20.4.12,

$$A \cap \{T \le t\} \in \mathcal{F}_t \;\Leftrightarrow\; X\mathbb{1}_{\{T\le t\}} = \mathbb{1}_A \mathbb{1}_{\{T\le t\}} = \mathbb{1}_{A\cap\{T\le t\}} \text{ is } \mathcal{F}_t\text{-measurable} \tag{20.4.8}$$

by Proposition 15.2.5 and Definition 15.2.1. Similarly, this holds for $X = c\mathbb{1}_A$, $c \in [0, \infty]$ (including two extreme cases $c = 0, \infty$).

If X is a simple function (finite linear combination of indicators), then we can write X as a linear combination of indicators of disjoint sets (by Proposition 15.3.3), say, $X = \sum_{i=1}^n c_i \mathbb{1}_{A_i}$, where the constants $c_i \in [0, \infty]$, $c_i \ne c_j$ for $i \ne j$ and $A_i \in \mathcal{F}$.

$\forall c \in [0, \infty]$, $B = \{X \le c\} \in \mathcal{B}(\overline{\mathbb{R}})$ (this forms a π-system so we can apply Proposition 15.2.1), then since A_i are disjoint,

$$\begin{aligned}
X \text{ is } \mathcal{F}_T\text{-measurable} &\Leftrightarrow \bigcup_{i=1}^n \{A_i : c_i \le c\} = X^{-1}(B) \in \mathcal{F}_T \\
&\Leftrightarrow \left(\bigcup_{i=1}^n \{A_i : c_i \le c\}\right) \cap \{T \le t\} \in \mathcal{F}_t. \\
&\Leftrightarrow \left\{X\mathbb{1}_{\{T\le t\}} \le c\right\} = \left\{\sum_{i=1}^n c_i \mathbb{1}_{A_i\cap\{T\le t\}} \le c\right\} = \left\{\left(\bigcup_{i=1}^n \{A_i : c_i \le c\}\right) \cap \{T \le t\}\right\} \in \mathcal{F}_t \\
&\Leftrightarrow X\mathbb{1}_{\{T\le t\}} \text{ is } \mathcal{F}_t\text{-measurable.}
\end{aligned}$$

For any non-negative random variable X, we can approximate it by $X_n = 2^{-n}\lfloor 2^n X \rfloor \wedge n \uparrow X$ as $n \to \infty$. Then the claim follows for each X_n, since X_n are simple functions. So, by Theorem 15.2.8,

$$\begin{aligned}
X\mathbb{1}_{\{T\le t\}} \text{ is } \mathcal{F}_t\text{-measurable, for all } t &\Leftrightarrow X_n\mathbb{1}_{\{T\le t\}} \text{ is } \mathcal{F}_t\text{-measurable, for all } t \\
&\Leftrightarrow X_n \text{ is } \mathcal{F}_T\text{-measurable} \Leftrightarrow X \text{ is } \mathcal{F}_T\text{-measurable.}
\end{aligned}$$

For any random variable X, we have $X = X^+ - X^-$, X^+, X^- are non-negative random variable ($X^+ = X \vee 0$, $X^- = (-X) \vee 0$). Thus, by Theorem 15.2.7, we have that for any random variable X, X is $\mathcal{F}_T$-measurable if and only if $X\mathbb{1}_{\{T\le t\}}$ is $\mathcal{F}_t$-measurable for all t. □

Definition 20.4.13 (usual conditions)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\in I}, \mathbb{P})$ be a filtered probability space. Let $\mathcal{N}$ be the collection of $\mathbb{P}$-null sets, i.e., sets in $\mathcal{F}$ of measure 0. Then the filtered probability space is said to satisfy the usual conditions or usual hypotheses if the following conditions are met:

(i) The probability space $(\Omega, \mathcal{F}, \mathbb{P})$ is complete (see Definition 15.1.19).

(ii) The σ-algebras $\mathcal{F}_t$ contain all $\mathbb{P}$-null sets in $\mathcal{F}$, i.e., $\mathcal{N} \subseteq \mathcal{F}_t$ for all t. (Equivalently, $\mathcal{N} \subseteq \mathcal{F}_0$.)

(iii) The filtration $\{\mathcal{F}_t\}$ is right-continuous. That is, for every non-maximal $t \in I$,

$$\mathcal{F}_t = \mathcal{F}_{t^+} := \bigcap_{s>t} \mathcal{F}_s. \tag{20.4.9}$$

Given any filtered probability space, it can always be enlarged by passing to the completion of the probability space, adding zero probability sets to $\mathcal{F}_t$, and by replacing $\mathcal{F}_t$ by $\mathcal{F}_{t^+}$. This will then satisfy the usual conditions.

Another way to express it is:

Definition 20.4.14 (completion of the filtered probability space)**.** With the same setup as above, we write $\widetilde{\mathcal{F}}_t := \sigma(\mathcal{F}_{t^+}, \mathcal{N})$ for all t. We say that the filtered probability space $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ satisfies the usual conditions if $\mathcal{F}_t = \widetilde{\mathcal{F}}_t$ for all t.

20.4.2 Stopping time properties

Recalling the discrete case (Definition 20.1.10),

Definition 20.4.15 (stopped process)**.** For a process X, we set $X_T(\omega) = X_{T(\omega)}(\omega)$, whenever $T(\omega) < \infty$. We define the stopped process X^T by $X^T_t = X_{T\wedge t}$.

Proposition 20.4.4. Let T be stopping time and X a càdlàg adapted process. Then

(i) $X_T \mathbb{1}_{\{T<\infty\}}$ is an $\mathcal{F}_T$ -measurable random variable.

(ii) X^T is adapted.

(iii) If X is integrable, then X^T is integrable.

(iv) X^T is càdlàg.

Remark. Similarly, if X is a sample-continunous process, X^T is also sample-continunous.

Proof. (i) By Proposition 20.4.3, in order to prove that $X_T \mathbb{1}_{\{T<\infty\}}$ is $\mathcal{F}_T$-measurable, we will show that

$$X_T \mathbb{1}_{\{T<\infty\}} \mathbb{1}_{\{T\leq t\}} = X_T \mathbb{1}_{\{T\leq t\}} \text{ is } \mathcal{F}_t\text{-measurable for all } t. \tag{20.4.10}$$

We can write $X_T \mathbb{1}_{\{T\leq t\}} = X_T \mathbb{1}_{\{T<t\}} + X_t \mathbb{1}_{\{T=t\}}$. Clearly, the random variable

$$X_t \mathbb{1}_{\{T=t\}} = \underbrace{X_t}_{\mathcal{F}_t\text{-measurable}} \left(\mathbb{1}\left\{ \underbrace{T \leq t}_{\in \mathcal{F}_t} \right\} - \mathbb{1}\left\{ \bigcup_n \underbrace{\left\{ T \leq t - \frac{1}{n} \right\}}_{\in \mathcal{F}_{t-\frac{1}{n}} \subseteq \mathcal{F}_t} \right\} \right) \;\Rightarrow\; X_t \mathbb{1}_{\{T=t\}} \text{ is } \mathcal{F}_t\text{-measurable} \tag{20.4.11}$$

It only remains to show that $X_T \mathbb{1}_{\{T<t\}}$ is $\mathcal{F}_t$-measurable. If we let $T_n = 2^{-n} \lceil 2^n T \rceil$, then it is easy to see that T_n is a stopping time that takes values in the set $\mathcal{D}_n = \{k2^{-n} : k \in \mathbb{N}\}$. Indeed

$$\{T_n \leq t\} = \{\lceil 2^n T \rceil \leq 2^n t\} = \left\{ T \leq 2^{-n} \lfloor 2^n t \rfloor \right\} \in \mathcal{F}_{2^{-n}\lfloor 2^n t \rfloor} \subseteq \mathcal{F}_t. \tag{20.4.12}$$

By the cadlag property of X and the convergence $T_n \downarrow T$ ($T_n \wedge t \downarrow T \wedge t$) we get that

$$X_{T\wedge t} = \lim_{n\to\infty} X_{T_n \wedge t} \;\Rightarrow\; X_T \mathbb{1}_{\{T<t\}} = \lim_{n\to\infty} X_{T_n\wedge t} \mathbb{1}_{\{T<t\}}. \quad (*) \tag{20.4.13}$$

Since T_n takes only countably many values, we have

$$\begin{aligned} X_{T_n\wedge t}\mathbb{1}_{\{T<t\}} &= \sum_{d\in\mathcal{D}_n, d\le t} X_d \mathbb{1}_{\{T_n=d\}} + X_t \mathbb{1}_{\{T_n>t\}}\mathbb{1}_{\{T<t\}} \\ &= \sum_{d\in\mathcal{D}_n, d\le t} X_d \big(\underbrace{\mathbb{1}_{\{T_n\le d\}}}_{\in\mathcal{F}_d\subseteq\mathcal{F}_t} - \underbrace{\mathbb{1}_{\{T_n\le d-2^{-n}\}}}_{\in\mathcal{F}_{d-2^{-n}}\subseteq\mathcal{F}_t}\big) + X_t \underbrace{\mathbb{1}_{\{T_n\le t\}^c}}_{\in\mathcal{F}_t}\mathbb{1}_{\{T<t\}} \\ &\Rightarrow \quad X_{T_n\wedge t}\mathbb{1}_{\{T<t\}} \text{ is } \mathcal{F}_t\text{-measurable for all } n \end{aligned}$$

since T_n is a stopping time wrt the filtration $(\mathcal{F}_t)_{t\ge 0}$. Then we have $X_T\mathbb{1}_{\{T<t\}}$ is $\mathcal{F}_t$-measurable by $(*)$ and Theorem 15.2.8.

(ii) Since $X_{T\wedge t}$ is $\mathcal{F}_{T\wedge t}$-measurable (by (i)), and hence $\mathcal{F}_t$-measurable, since by Proposition 20.4.2, $\mathcal{F}_{T\wedge t}\subseteq\mathcal{F}_t$. Hence, X_t^T is $\mathcal{F}_t$-measurable and thus X^T is adapted.

(iii) We have $X_t^T = X_t\mathbb{1}_{\{T>t\}} + X_T\mathbb{1}_{\{T\le t\}}$,

$$\mathbb{E}\left|X_t^T\right| \le \mathbb{E}\left|X_t\mathbb{1}_{\{T>t\}}\right| + \mathbb{E}\left|X_T\mathbb{1}_{\{T\le t\}}\right| \le \mathbb{E}\left|X_t\right| + \sup_{s\in[0,t]}\mathbb{E}\left|X_s\right| < \infty. \tag{20.4.14}$$

(iv) for any t, we have can find $s\downarrow t$, $r\uparrow t$ such that $s\wedge T\downarrow t\wedge T$ and $r\wedge T\uparrow t\wedge T$. Since X is càdlàg,

$$\lim_{s\downarrow t} X_s^T = \lim_{s\wedge T\downarrow t\wedge T} X_{T\wedge s} = X_{T\wedge t} = X_t^T, \qquad \lim_{r\uparrow t} X_s^T = \lim_{r\wedge T\uparrow t\wedge T} X_{T\wedge r} \text{ exists} \quad\Rightarrow\quad X^T \text{ is càdlàg.} \tag{20.4.15}$$

□

Example 20.4.5. When the time index set is $\mathbb{R}^{++}$, then entry (début) times are not always stopping times. Let J be a random variable that takes values +1 or -1 each with probability 1/2. Consider now the following process

$$X_t = \begin{cases} t & t\in[0,1] \\ 1+J(t-1) & t>1 \end{cases}. \tag{20.4.16}$$

Let $\mathcal{F}_t = \sigma(X_s : s\le t)$ be the natural filtration of X ($\mathcal{F}_t = \mathcal{F}_t^X$). Then if $A=(1,2)$ and we consider

$$T_A = \inf\{t\ge 0 : X_t\in A\}, \tag{20.4.17}$$

then clearly $\{T_A\le 1\}\notin\mathcal{F}_1$ (since T_A depends on the information of $t>1$).

If we impose some regularity conditions on the process or the filtration though, then we get stopping times like in the next two propositions.

Proposition 20.4.6. Let (E,d) be a metric space. The filtered space satisfies the usual conditions. Let $A\subseteq E$ be a closed set and X a (sample) continuous adapted process. Then the entry (début) time[16] of A,

$$T_A = \inf\{t\ge 0 : X_t\in A\}, \tag{20.4.18}$$

is a stopping time with respect to $(\mathcal{F}_t)$.

Proof. Let $d(x,A)$ stand for the distance of x from the set A. Let $\Omega' = \{\omega : X(\omega) \text{ is continuous}\}$ with $\mathbb{P}(\Omega')=1$. We pick any $\omega\in\Omega'$.

If $T_A(\omega) = s\le t$, then there exists a sequence s_n of times such that $X_{s_n}(\omega)\in A$ and $s_n\downarrow s$ as $n\to\infty$ (by definition of début time). By continuity of X, we then deduce that $X_{s_n}(\omega)\to X_s(\omega)$ as $n\to\infty$. Since A is closed, we must have that $X_s(\omega)\in A$. Thus we showed that $X_{T_A}(\omega)\in A$.

We can now find a sequence of rationals $q_n\in\mathbb{Q}$ such that $q_n\uparrow T_A$ as $n\to\infty$ and since $d(X_{T_A}(\omega),A)=0$ we get that $d(X_{q_n}(\omega),A)\to 0$ as $n\to\infty$ by continuity of $X(\omega)$ and $d(\cdot,A)$. Thus, $\{T_A(\omega)\le t\}\subseteq\{\inf_{s\in\mathbb{Q},s\le t} d(X_s(\omega),A)=0\}$.

Suppose now that $\inf_{s\in\mathbb{Q},s\le t} d(X_s(\omega),A)=0$. Then there exists a sequence $s_n\in\mathbb{Q}$, $s_n\le t$ (since rational set is dense), for all n such that

$$d(X_{s_n}(\omega),A)\to 0 \text{ as } n\to\infty. \tag{20.4.19}$$

[16] need definition of entry time and hitting time (see Rogers-Williams [11])

We can find a converging subsequence of s_{n_k} and $s \le t$ such that $s_{n_k} \to s$ (by Bolzano-Weierstrass Theorem[17] since $s_n \in [0,t]$ is bounded) as $k \to \infty$. By continuity of X we get that $X_{s_{n_k}}(\omega) \to X_s(\omega)$ as $n \to \infty$. So $d(X_{s_{n_k}}(\omega), A) \to d(X_s(\omega), A)$ as $n \to \infty$ which implies that $d(X_s(\omega), A) = 0$. Since $d(X_s, A) = 0$ and A is a closed set, we conclude that $X_s(\omega) \in A$ (We can find s_n such that $X_{s_n}(\omega) \in A$ and $d(X_{s_n}, A) = 0$, so $d(X_{s_n}(\omega), A) \to d(X_s(\omega), A)$. If $X_s \notin A$, then A is open (contradiction), so we must have $X_s(\omega) \in A$). Hence $T_A(\omega) \le s \le t$.

Thus, $\{T_A(\omega) \le t\} \supseteq \{\inf_{s\in\mathbb{Q}, s\le t} d(X_s(\omega), A) = 0\}$.

Hence, we have that

$$\{\omega \in \Omega' : T_A(\omega) \le t\} = \left\{\omega \in \Omega' : \inf_{s\in\mathbb{Q}, s\le t} d(X_s(\omega), A) = 0\right\}. \tag{20.4.20}$$

Thus,

$$\begin{aligned}
\{T_A \le t\} &= \{\omega \in \Omega' : T_A(\omega) \le t\} \cup \{\omega \in \Omega'^c : T_A(\omega) \le t\} \\
&= \left\{\omega \in \Omega' : \inf_{s\in\mathbb{Q}, s\le t} d(X_s(\omega), A) = 0\right\} \cup \{\omega \in \Omega'^c : T_A(\omega) \le t\} \\
&= \left\{\left\{\omega \in \Omega : \inf_{s\in\mathbb{Q}, s\le q} d(X_s(\omega), A) = 0\right\} \cap \left\{\omega \in \Omega'^c : \inf_{s\in\mathbb{Q}, s\le q} d(X_s(\omega), A) = 0\right\}^c\right\} \cup \{\omega \in \Omega'^c : T_A(\omega) \le t\} \\
&= (B \cap C) \cap D.
\end{aligned}$$

where C and D ($\mathbb{P}(C^c) \le \mathbb{P}(\Omega'^c) = 0$, $\mathbb{P}(D) \le \mathbb{P}(\Omega'^c) = 0$) are $\mathcal{F}_t$-measurable since $(\mathcal{F}_t)_{t\ge 0}$ satisfies the usual condition. Also, X_s is $\mathcal{F}_s$-measurable and thus $\mathcal{F}_t$-measurable, $d(X_s, A)$ and $\inf_{s\in\mathbb{Q}, s\le t} d(X_s, A)$ are $\mathcal{F}_t$-measurable (since $x \mapsto d(x, A)$ is continuous and then $\mathcal{F}_t$-measurable by Proposition 15.2.3). Thus, B is $\mathcal{F}_t$-measurable. Thus, $\{T_A \le t\}$ is $\mathcal{F}_t$-measurable and T_A is a stopping time. □

Proposition 20.4.7. Let (E, d) be a metric space. The filtered space satisfies the usual conditions. Let A be an open set and X a (sample) right-continuous adapted process. Then

$$T_A = \inf\{t \ge 0 : X_t \in A\} \tag{20.4.21}$$

is a stopping time with respect to the filtration $(\mathcal{F}_t)$.

Remark. If we ignore the usual condition for the filtered space and consider a pathwise right-continuous adapted process, we can have that T_A is a stopping time with respect to the filtration $(\mathcal{F}_{t^+})$.

Proof. First we show that for all t, the event $\{T_A < t\} \in \mathcal{F}_t$.

Indeed, for any $\omega \in \Omega' = \{X(\omega) \text{ is right-continuous}\}$ ($\mathbb{P}(\Omega') = 1$), $\forall s < t, s \in \mathbb{Q}$, $X_s(\omega) \in A \Rightarrow T_A(\omega) \le s < t$, thus $\{T_A(\omega) < t\} \supseteq \{X_s(\omega) \in A\}$ and then $\{T_A(\omega) < t\} \supseteq \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}$.

Now consider $\{T_A(\omega) < t\}$, we have that

$$\{T_A(\omega) < t\} \subseteq \bigcup_{s\le t} \{X_s(\omega) \in A\}. \tag{20.4.22}$$

$\forall \varepsilon > 0$, if $X_s(\omega) \in A$, by the right-continuity of paths, there exists $\delta > 0$, for all $s' < \delta$, $d(X_{s+s'}(\omega), X_s(\omega)) < \varepsilon$. Since A is open, we have that for all $t \in [s, s+\delta)$, $X_t(\omega) \in A$. Thus,

$$\bigcup_{s\le t} \{X_s(\omega) \in A\} \subseteq \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\} \tag{20.4.23}$$

since we can cover the whole set with rational s ($\mathbb{Q}$ is dense). Then we have $\{T_A(\omega) < t\} \subseteq \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}$.

Hence we have

$$\{T_A(\omega) < t\} = \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}. \tag{20.4.24}$$

[17] need link

Thus,

$$\begin{aligned}\{T_A < t\} &= \{\omega \in \Omega' : T_A(\omega) < t\} \cup \{\omega \in \Omega'^c : T_A < t\} = \left\{\omega \in \Omega' : \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}\right\} \cup \{\omega \in \Omega'^c : T_A < t\} \\ &= \left\{\left\{\omega \in \Omega : \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}\right\} \cap \left\{\omega \in \Omega'^c : \bigcup_{s\in\mathbb{Q}, s<t} \{X_s(\omega) \in A\}\right\}^c\right\} \cup \{\omega \in \Omega'^c : T_A < t\} \\ &= (B \cap C) \cup D.\end{aligned}$$

where C and D ($\mathbb{P}(C^c) \leq \mathbb{P}(\Omega'^c) = 0$, $\mathbb{P}(D) \leq \mathbb{P}(\Omega'^c) = 0$) are $\mathcal{F}_t$-measurable since $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual condition. For fixed $s < t$, X_s is $\mathcal{F}_s$-measurable and $x \mapsto d(x, A)$ is continuous (thus $d(X_s, A)$ is $\mathcal{F}_s$-measurable by Proposition 15.2.3) thus $\mathcal{F}_t$-measurable. Then we have $\{X_s \in A\} = \{d(X_s, A) = 0\} \in \mathcal{F}_t$. Thus, $\{T_A < t\} \in \mathcal{F}_t$ since it is a countable union. Since we can write

$$\{T_A \leq t\} = \bigcap_n \{T < t + 1/n\} \tag{20.4.25}$$

we get that $\{T_A \leq t\} \in \mathcal{F}_{t^+}$. Since the filtered space satisfies the usual conditions, we have $\mathcal{F}_t = \mathcal{F}_{t^+}$. Thus, T_A is a stopping time with respect to $(\mathcal{F}_t)$. □

[18]

20.4.3 Technical issues in dealing with continuous-time

When we consider processes in discrete time, if we equip $\mathbb{N}$ with the σ-algebra $\mathcal{P}(\mathbb{N})$ that contains all the subsets of $\mathbb{N}$, then the process

$$X : \Omega \times \mathbb{N} \to \overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\} : (\omega, n) \mapsto X_n(\omega) \tag{20.4.26}$$

is measurable with respect to the product σ-algebra $\mathcal{F} \otimes \mathcal{P}(\mathbb{N})$. This can be proved by the following argument.

If we fix n, then $w \mapsto X_n(\omega)$ is a random variable and thus $\mathcal{F}$-measurable (i.e., $\forall y \in \overline{\mathbb{R}}$, $A_n = \{\omega : X_n(\omega) \leq y, n \text{ fixed}\} \in \mathcal{F}$). Thus $A_n \in \mathcal{F}$ and $\{n\} \in \mathcal{P}(\mathbb{N})$, we have $A_n \times \{n\}$ is $\mathcal{F} \otimes \mathcal{P}(\mathbb{N})$-measurable ($A_n \times \{n\} \in \mathcal{F} \otimes \mathcal{P}(\mathbb{N})$, see Definition 15.3.8).

$$A := \{(\omega, n) : X_n(\omega) \leq y\} = \bigcup_{n\geq 0} \{A_n \times \{n\}\} \in \mathcal{F} \otimes \mathcal{P}(\mathbb{N}) \tag{20.4.27}$$

since A is a union of countably many subsets. Thus, X is $\mathcal{F} \otimes \mathcal{P}(\mathbb{N})$-measurable.

Back to continuous time, if we fix $t \in \mathbb{R}^{++}$, then $\omega \mapsto X_t(\omega)$ is a random variable. But, the mapping $(\omega, t) \mapsto X_t(\omega)$ has no reason to be measurable with respect to $\mathcal{F} \otimes \mathcal{B}(\mathbb{R})$ ($\mathcal{B}(\mathbb{R})$ is the Borel σ-algebra) unless some regularity conditions are imposed on X (We can not apply the above argument for the discrete case.).

Also, if $A \subseteq \mathbb{R}$, then the first hitting time of A, $T_A = \inf\{t : X_t \in A\}$ is not in general a stopping time as the set

$$\{T_A \leq t\} = \bigcup_{0\leq s\leq t} \{T = s\} \notin \mathcal{F}_t \text{ in general, since this is an uncountable union.} \tag{20.4.28}$$

A quite natural requirement is that for a fixed ω the mapping $t \mapsto X_t(\omega)$ is continuous in t. Then, indeed the mapping $(\omega, t) \mapsto X_t(\omega)$ is measurable. More generally we will consider the following process.

Definition 20.4.16 (càdlàg process)**.** A process $X = X_t(\omega)$ is càdlàg (from the french continu à droite limité à gauche) is all its sample paths are càdlàg function (Definition 10.3.7, right-continuous and admitting left limits everywhere) a.s., i.e., for fixed ω,

$$X_t(\omega) = X_{t^+}(\omega) = \lim_{s\downarrow t} X_s(\omega), \qquad X_{t^-}(\omega) = \lim_{s\uparrow t} X_s(\omega) \text{ exists} \quad \text{with probability one..} \tag{20.4.29}$$

Remark. Continuous and càdlàg processes are determined by their values in a countable dense subset of $\mathbb{R}^{++}$, for instance $\mathbb{Q}^+$.

Proposition 20.4.8. If a process $X = (X_t)_{t\in[0,1)}$ is càdlàg, then the mapping $(\omega, t) \mapsto X_t(\omega)$ is measurable with respect to $\mathcal{F} \otimes \mathcal{B}([0, 1))$.

[18] add example here see [11].P_{184}

Proof. We can write (by right-continuity)

$$X_t(\omega) = \lim_{n\to\infty} \sum_{k=1}^{2^n} \mathbb{1}_{\{t\in[(k-1)2^{-n},k2^{-n})\}} X_{k2^{-n}}(\omega). \tag{20.4.30}$$

For each n it is easy to see that

$$(\omega, t) \mapsto \sum_{k=1}^{2^n} \mathbb{1}_{\{t\in[(k-1)2^{-n},k2^{-n})\}} X_{k2^{-n}}(\omega). \tag{20.4.31}$$

$X_{k2^{-n}}(\omega)$ is $\mathcal{F}$-measurable and thus $\mathcal{F}\otimes\mathcal{B}([0,1))$-measurable (since $\{k2^{-n}\} \in \mathcal{B}([0,1))$). Also, $\mathbb{1}_{\{t\in[(k-1)2^{-n},k2^{-n})\}}$ is $\mathcal{B}([0,1))$-measurable and thus $\mathcal{F}\otimes\mathcal{B}([0,1))$-measurable. Hence $X_t(\omega)$ is $\mathcal{F}\otimes\mathcal{B}([0,1))$-measurable, as a limit of measurable functions. □

Remark. Similarly, we can prove that X is measurable with respect to $\mathcal{F}\otimes\mathcal{B}(\mathbb{R})$.

Also, we can have that continuous or làdcàg (left-continuous and right limit exists) function also implies that the mapping $(\omega, t) \mapsto X_t(\omega)$ is measurable with respect to $\mathcal{F}\otimes\mathcal{B}([0,1))$.

20.4.4 Càdlàg processes, finite variation processes

Recalling definition of càdlàg process (Definition 20.4.16) and total variation of càdlàg function (Definition 10.3.8), we definie total variation process.

Definition 20.4.17 (total variation process, finite variation process)**.** Let A be a càdlàg adapted process. Its total variation process V is defined pathwise (for each $\omega\in\Omega$) as the total variation (Definition 10.3.8) of $A(\omega,\cdot)$.

We say that A is of finite variation if A is of finite variation a.s., i.e., for fixed ω, $A(\omega,\cdot)$ (the sample path) is (a càdlàg function and) of finite variation with probability one. Then A is called finite variation process.

Lemma 20.4.9. Let A be a càdlàg adapted process with finite total variation process V. Then V is càdlàg process, non-decreasing a.s..

Furthermore, if the filtration is right-continuous (i.e., $\mathcal{F}_t = \mathcal{F}_{t^+}$), then V is adapted.

Remark. If A is a sample-continuous adapted process, V is also sample-continuous (by replacing the following proof with sample-continuous condition).

Proof. Using the same definition in Lemma 10.3.11, we get for each ω, $t_n^- = 2^{-n}\left(\lceil 2^n t\rceil - 1\right)$,

$$\begin{aligned} V_t^n(\omega) &= \sum_{k=0}^{\lceil 2^n t\rceil -1} \left|A_{(k+1)2^{-n}}(\omega) - A_{k2^{-n}}(\omega)\right| \\ &= \sum_{k=0}^{2^n t_n^- -1} \left|A_{(k+1)2^{-n}}(\omega) - A_{k2^{-n}}(\omega)\right| + \left|A_{2^{-n}\lceil 2^n t\rceil}(\omega) - A_{2^{-n}(\lceil 2^n t\rceil -1)}(\omega)\right| \end{aligned}$$

Thus,

$$\begin{aligned} V_t &= \lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- -1} \left|A_{(k+1)2^{-n}} - A_{k2^{-n}}\right| + \lim_{n\to\infty} \left|A_{2^{-n}\lceil 2^n t\rceil} - A_{2^{-n}(\lceil 2^n t\rceil -1)}\right| \\ &= \lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- -1} \left|A_{(k+1)2^{-n}} - A_{k2^{-n}}\right| + |A_{t^+} - A_{t^-}| \qquad (*). \end{aligned}$$

If the sample path $A(\omega)$ is càdlàg, we have

$$\begin{aligned} V_t(\omega) &= \lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- -1} \left|A_{(k+1)2^{-n}}(\omega) - A_{k2^{-n}}(\omega)\right| + |A_{t^+}(\omega) - A_{t^-}(\omega)| \\ &= \lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- -1} \left|A_{(k+1)2^{-n}}(\omega) - A_{k2^{-n}}(\omega)\right| + |\Delta A_t(\omega)| \end{aligned}$$

and $V_t(\omega)$ is non-decreasing (by Lemma 10.3.11) and càdlàg (by Proposition 10.3.12). Thus, V is non-decreasing a.s. and V is a càdlàg process (by Definition 20.4.16).

We know that $A_{k2^{-n}}$ is $\mathcal{F}_t$-measurable for $k \le 2^n t_n^-$ since $2^n t_n^- < t$. Thus,

$$\lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- - 1} \left|A_{(k+1)2^{-n}} - A_{k2^{-n}}\right| \quad \text{is } \mathcal{F}_t\text{-measurable.} \tag{20.4.32}$$

Thus, the process $U(t) := \lim_{n\to\infty} \sum_{k=0}^{2^n t_n^- - 1} \left|A_{(k+1)2^{-n}} - A_{k2^{-n}}\right|$ is adapted.

Also, $|A_{t^+} - A_{t^-}|$ in $(*)$ is $\mathcal{F}_{t^+}$-measurable. If the filtration is right-continuous ($\mathcal{F}_t = \mathcal{F}_{t^+}$), then $|A_{t^+} - A_{t^-}|$ is $\mathcal{F}_t$-measurable. Therefore, V_t is $\mathcal{F}_t$-measurable and thus V is adapted. □

20.4.5 Finite dimensional marginal distributions

Definition 20.4.18 (law of process)**.** Recalling the law of random variable $X : \Omega \to S$ (Definition 19.2.2)[19],

$$\mu_X((-\infty, x]) = \mathbb{P}(X \le x) = \mathbb{P}\left(\{\omega : X(\omega) \le x\}\right) \;\Rightarrow\; \mu_X(A) = \mathbb{P}\left(\{\omega : X(\omega) \in A\}\right), \quad A \in \mathcal{B}(S). \tag{20.4.33}$$

Now we can view a stochastic process X indexed by $\mathbb{R}^{++}$ as a random variable with values in the space of functions $S = \{f : \mathbb{R}^{++} \to T\}$[20] endowed with the σ-algebra $\mathcal{E}$ on S that makes the projections $f \mapsto f(t)$ measurable for every $t \in \mathbb{R}^{++}$. The law of the process X is the measure μ that is defined as

$$\mu(A) = \mathbb{P}(X \in A), \quad A \in \mathcal{E}. \tag{20.4.34}$$

Or we can denote it as

$$\mu(A) = \mathbb{P}(X \in A), \quad A \in \mathcal{B}(S) \otimes \mathcal{T} \tag{20.4.35}$$

where $\mathcal{T}$ is a compact-open topology (wrt t).

However the measure μ is not easy to work with. Instead we consider simpler objects that we define below.

Definition 20.4.19 (finite dimensional distributions)**.** Let X be the stochastic process definited on probability space $(\Omega, \mathcal{F}, \mathbb{P})$ having the state space $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$. Then we consider the probability measure μ_J, where $J \subseteq \mathbb{R}^{++}$ is a finite set, defined as the law of $(X_t)_{t\in J}$ i.e., $|J| = n$, and $J = \{t_1, t_2, \ldots, t_n\}$ ($t_i < \infty$ since $J \subseteq \mathbb{R}^{++}$),

$$\mu_J = \mathbb{P}\left((X_{t_1}, \ldots, X_{t_n}) \in A\right), \quad A \in \mathcal{B}(\mathbb{R}^{nd}) \tag{20.4.36}$$

The probability measures (μ_J) are called the finite dimensional distributions of stochastic process X.

Definition 20.4.20. Let X, Y be the stochastic processes definited on probability space $(\Omega, \mathcal{F}, \mathbb{P})$ and $(\widetilde{\Omega}, \widetilde{\mathcal{F}}, \widetilde{\mathbb{P}})$, respectively, and having the same state space $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$.

Then X and Y have the same finite dimensional distributions if, for any integer $n \ge 1$, real numbers $0 \le t_1 < t_2 < \ldots t_n < \infty$, and $A \in \mathcal{B}(\mathbb{R}^{nd})$, we have

$$\mathbb{P}\left((X_{t_1}, \ldots, X_{t_n}) \in A\right) = \widetilde{\mathbb{P}}\left((Y_{t_1}, \ldots, Y_{t_n}) \in A\right). \tag{20.4.37}$$

Proposition 20.4.10. Let μ be the law of process X. Then μ is uniquely determined by its finite dimensional marginal distributions.

Proof. By a π-system uniqueness argument, μ is uniquely determined by its finite dimensional marginal distributions (by Theorem 15.1.18 since $\mathbb{P}$ is probability measure (and thus finite)).

Indeed the set

$$\left\{\bigcap_{s\in J} \{X_s \in A_s\} : J \text{ is finite, } A_s \in \mathcal{B}(\mathbb{R})\right\} \tag{20.4.38}$$

is a π-system generating σ-algebra $\mathcal{B}(S)$ (by checking Definition 15.1.5). □

[19] usually $S = \mathbb{R}$
[20] usually $T = \mathbb{R}$

Therefore, when we want to specify the law of a càdlàg process (or just a right-continuous process), it suffices to describe its finite dimensional distributions. Of course we have no a priori reason to believe there exists a càdlàg process whose finite dimensional distributions coincide with a given family of measures $(\mu_J : J \subseteq \mathbb{R}^{++}, J \text{ finite})$.

20.4.6 Versions and indistinguishability

Even if we know the law of a process, this does not give us much information about the sample path properties of the process. Namely, there could be different processes with the same finite marginal distributions. This motivates the following definition:

Definition 20.4.21 (version)**.** Let X and X' be two processes defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. We say that X' is a version (or modification) of X if $X_t = X'_t$ a.s. (i.e., $\mathbb{P}(X_t(\omega) = X'_t(\omega)) = 1$) for every (fixed) t.

Remark. Note that two versions of the same process have the same finite marginal distributions. But they do not share the same sample path properties (there doesn't necessarily exist an ω such that $X_t(\omega) = X'_t(\omega)$ for every t).

Example 20.4.11. Let $X = (X_t)_{t\in[0,1]}$ be the process that is identical to 0 for all t. Then obviously the finite marginal distributions will be Dirac measures at 0. Now let U be a uniform random variable on $[0, 1]$. We define $X'_t = \mathbb{1}_{\{U=t\}}$. Then clearly the finite marginal distributions of X' are Dirac measures at 0, and hence it is a version of X. However it is not continuous and furthermore

$$\mathbb{P}\left(X'_t = 0,\ \forall t \in [0, 1]\right) = 0. \tag{20.4.39}$$

However, we can define a stronger version,

Definition 20.4.22 (indistinguishable version)**.** If X and X' are two processes defined on some common probability space $(\Omega, \mathcal{F}, \mathbb{P})$, we say that X' is an indistinguishable version of X, if $\mathbb{P}(X_t(\omega) = X'_t(\omega) \text{ for all } t) = 1$ i.e., X and X' have the same sample paths a.s.. We say that X and X' are indistinguishable.

Proposition 20.4.12. If X and X' are càdlàg (or sample continuous) and X' is a version of X, then X' is also a indistinguishable version of X.

Remark. Actually, we can release the condition to all (sample) right-continuous (or left-continuous) process.

Proof. Since sample continous process is càdlàg(by Definition 20.4.2, 20.4.16), we only check càdlàg case. First we have for any $t \in [0, \infty)$, $\mathbb{P}\left(X_t(\omega) \neq X_t(\omega)\right) = 0$. Then by Proposition 19.1.6,

$$\mathbb{P}(X_t(\omega) = X_t(\omega), \forall t \in \mathbb{Q}) = 1 - \mathbb{P}\left(X_t(\omega) \neq X_t(\omega), \exists t \in \mathbb{Q}\right) \geq 1 - \underbrace{\sum_{t\in\mathbb{Q}} \mathbb{P}\left(X_t(\omega) \neq X_t(\omega)\right)}_{\text{sum of countably many 0}} = 1 - 0 = 1. \tag{20.4.40}$$

However for any $t \in \mathbb{R}^{++}$, since X and X' are càdlàg, we can find non-negative rational sequence $t_n \downarrow t$, $X_{t_n}(\omega) = X'_{t_n}(\omega)$ for any t_n and

$$X_t(\omega) = \lim_{t_n\downarrow t} X_{t_n}(\omega) = \lim_{t_n\downarrow t} X'_{t_n}(\omega) = X'_t(\omega). \tag{20.4.41}$$

Thus, $\{X_t(\omega) = X'_t(\omega), \forall t \in \mathbb{Q}^+\} = \{X_t(\omega) = X'_t(\omega), \forall t \in \mathbb{R}^{++}\}$. This imples that

$$\mathbb{P}(X_t(\omega) = X'_t(\omega), \forall t \in \mathbb{R}^{++}) = \mathbb{P}(X_t(\omega) = X'_t(\omega), \forall t \in \mathbb{Q}^+) = 1. \tag{20.4.42}$$

This means that X and X' are indistinguishable. □

Note that, up to indistinguishability, there exists at most one continuous version of a given process $(X_t)_{t\geq 0}$ by. Kolmogorov's criterion is a fundamental result which guarantees the existence of a continuous version (but not necessarily indistinguishable version).

Theorem 20.4.13 (Kolmogorov's continuity criterion)**.** Let $(X_t)_{0\leq t\leq 1}$ be a stochastic process with real values. Suppose there exist $p > 0$, $c > 0$, $\varepsilon > 0$ so that for every $s, t \geq 0$,

$$\mathbb{E}[|X_t - X_s|^p] \leq c\,|t - s|^{1+\varepsilon}. \tag{20.4.43}$$

Then, there exists a version $\widetilde{X}$ of X which is (pathwise or sample) continuous, and even α-Hölder continuous for any $\alpha \in (0, \varepsilon/p)$, i.e., for all $s, t \in [0,1]$, there exists K_α such that

$$\left|\widetilde{X}_t - \widetilde{X}_s\right| \leq K_\alpha \left|s-t\right|^\alpha \quad \text{a.s..} \tag{20.4.44}$$

Proof. Let $\mathcal{D}_n = \{k2^{-n} : 0 \leq k \leq 2^n\}$ denote the dyadic numbers of $[0,1]$ with level n.

Then letting $\alpha \in (0, \varepsilon/p)$, Markov's inequality (Theorem 19.3.20) gives for $0 \leq k < 2^n$,

$$\begin{aligned}
\mathbb{P}\left(\left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right| \geq 2^{-n\alpha}\right) &= \mathbb{P}\left(\left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right|^p \geq 2^{-np\alpha}\right) \leq \frac{\mathbb{E}\left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right|^p}{2^{-np\alpha}} \\
&= \mathbb{E}\left[\left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right|^p\right] 2^{np\alpha} \leq c 2^{-n(1+\varepsilon)} 2^{np\alpha} \leq c 2^{-n} 2^{-(\varepsilon - p\alpha)n}.
\end{aligned}$$

Summing over $\mathcal{D}_n$ we obtain

$$\mathbb{P}\left(\max_{0 \leq k < 2^n} \left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right| \geq 2^{-n\alpha}\right) \leq c 2^{-n(\varepsilon - p\alpha)}, \tag{20.4.45}$$

which is summable. Therefore, the Borel-Cantelli lemma (Lemma 19.1.24) shows that for sufficiently large n,

$$\max_{0 \leq k < 2^n} \left|X_{k2^{-n}} - X_{(k+1)2^{-n}}\right| < 2^{-n\alpha} \quad \text{a.s.} \tag{20.4.46}$$

Suppose the set satisfying this condition is Ω' with $\mathbb{P}(\Omega') = 1$. Then for any $\omega \in \Omega'$, we can find $M(\omega)$ (where M is a random variable) such that

$$\sup_{n \geq 0} \max_{0 \leq k < 2^n} \frac{\left|X_{k2^{-n}}(\omega) - X_{(k+1)2^{-n}}(\omega)\right|}{2^{-n\alpha}} \leq M(\omega) < \infty. \tag{20.4.47}$$

We claim that this implies that for every $s, t \in \mathcal{D} = \bigcup_{n \geq 0} \mathcal{D}_n$, $|X_s - X_t| \leq M'(\omega) |t-s|^\alpha$, for some $M'(\omega) < \infty$.

Indeed, if $s, t \in \mathcal{D}$, $s < t$, and let r be the unique integer such that

$$2^{-r-1} < t - s \leq 2^{-r}. \qquad (*) \tag{20.4.48}$$

Then there exists $0 \leq k \leq 2^r$ such that $s < k2^{-r-1} < t$ since the gap between s and t is bigger than 2^{-r-1}. Thus, the gap between t and $k2^{-r-1}$ smaller than 2^{-r}. Similarly, we have the gap between s and $k2^{-r-1}$ smaller than 2^{-r}.

$$\begin{aligned}
s &= k2^{-r-1} - \varepsilon_1 2^{-r-1} - \varepsilon_2' 2^{-r-2} - \dots \\
t &= k2^{-r-1} + \varepsilon_1' 2^{-r-1} + \varepsilon_2' 2^{-r-2} + \dots
\end{aligned}$$

with ε_i, $\varepsilon_i' \in \{0,1\}$, $i \geq 0$. For $i, j \geq 1$, we let

$$\begin{aligned}
s_i &= k2^{-r-1} - \varepsilon_1 2^{-r-1} - \dots - \varepsilon_i 2^{-r-i} \\
t_j &= k2^{-r-1} - \varepsilon_1' 2^{-r-1} - \dots - \varepsilon_i' 2^{-r-j}.
\end{aligned}$$

By the triangular inequality, with assumption and $(*)$,

$$\begin{aligned}
|X_t - X_s| &\leq |X_{t_0} - X_{s_0}| + \sum_{i=1}^{\infty} \left|X_{t_i} - X_{t_{i-1}}\right| + \sum_{j=1}^{\infty} \left|X_{s_j} - X_{s_{j-1}}\right| \\
&\leq \sum_{i=1}^{\infty} M(\omega) 2^{-(r+i)\alpha} + \sum_{j=1}^{\infty} M(\omega) 2^{-(r+j)\alpha} = \frac{2M(\omega) 2^{-(r+1)\alpha}}{1 - 2^{-\alpha}} \leq M'(\omega) |t-s|^\alpha \qquad (\dagger)
\end{aligned}$$

where $M'(\omega) = 2M(\omega)/(1 - 2^{-\alpha})$.

Therefore, the process $(X_t)_{t \in \mathcal{D}}(\omega)$ is uniformly continuous (and even α-Hölder continuous) for $\omega \in \Omega'$. Since $\mathcal{D}$ is an everywhere dense set in $[0,1]$, for any $t \in [0,1]$, we can find a sequence $t_n \in \mathcal{D}$ such that $t_n \to t$. Since t_n is a Cauchy sequence in $[0,1]$, with $(\dagger)$ we have $X_{t_n}(\omega)$ is also a Cauchy sequence. Thus, we have that $X_{t_n}(\omega)$ converges by Theorem 10.2.40 and $\lim_{n \to \infty} X_{t_n}(\omega)$ is well-defined.

Now defined by $\widetilde{X}_t(\omega) = \lim_n X_{t_n}(\omega)$, where $(t_n)_{n \geq 0}$ is any $\mathcal{D}$-valued sequence converging to $t \in [0,1]$). Obviously, $\widetilde{X}(\omega)$

is continous by definition. For the exceptional set where $(X_d)_{d\in\mathcal{D}}$ is not uniformly continuous ($\omega \in \Omega'^c$), we let $\widetilde{X_t}(\omega) = 0$, $t \in [0,1]$, so $\widetilde{X}$ is pathwise continuous. Note that if we don't consider the exceptional set, $\widetilde{X}$ is still a sample continuous process, i.e., the sample path is continuous a.s..

It remains to show that $\widetilde{X}$ is a version of X. If $t_n \to t$ for $t_n \in \mathcal{D}$, then $\liminf_n X_{t_n} = \lim_{n\to\infty} X_{t_n}$. We estimate by Fatou's lemma (Lemma 19.3.7),

$$\mathbb{E}\left|X_t - \widetilde{X}_t\right|^p = \mathbb{E}\left|X_t - \liminf_n X_{t_n}\right|^p = \mathbb{E}\left(\liminf_n |X_t - X_{t_n}|^p\right) \le \liminf_n \mathbb{E}[|X_t - X_{t_n}|^p], \tag{20.4.49}$$

Since $\mathbb{E}\,|X_t - X_{t_n}|^p \le c\,|t - t_n|^{1+\varepsilon}$, this converges to 0 as $n \to \infty$. Therefore, for every t, by Theorem 15.3.7.(iii),

$$\mathbb{E}\left|X_t - \widetilde{X}_t\right|^p = 0 \;\Rightarrow\; \left|X_t - \widetilde{X}_t\right|^p = 0 \text{ a.s. } \Rightarrow\; X_t = \widetilde{X}_t \text{ a.s.} \tag{20.4.50}$$

Thus, $\widetilde{X}$ is a (pathwise or sample) continuous version of X. □

20.4.7 Canonical Processes

Definition 20.4.23 (function space)**.** A function space $F(T,E) = E^T$ with time index is the collection of function f such that

$$f : T \to E,\ t \mapsto f(t). \tag{20.4.51}$$

Definition 20.4.24 (coordinate mapping)**.** Let E^T be a function space with time index. The functions

$$Y_t : E^T \to E,\ \phi \mapsto \phi(t) = Y_t(\phi) \tag{20.4.52}$$

for any $t \in T$ are called coordinate mappings.

Definition 20.4.25 (canonical process)**.** Let $(X_t)_{t\in T}$, be a process defined on $(\Omega, \mathcal{F}, \mathbb{P})$ with state space $(E, \mathcal{E})$. The mapping $\phi : \Omega \to E^T,\ \omega \mapsto \phi(\omega)$ is defined by

$$\phi(\omega) = X(\omega). \qquad (\phi(\omega)(t) = X_t(\omega)) \tag{20.4.53}$$

Then the coordinate mapping are

$$Y_t : E^T \to E,\ \phi(\omega) \mapsto (\phi(\omega))(t) = Y_t(\phi(\omega)) = Y_t \circ \phi(\omega) \tag{20.4.54}$$

with probability one (i.e., a.s.).

They are random variables, hence form a process indexed by T, if E^T is endowed with the product σ-algebra $\mathcal{E}^T$. This σ-algebra is the smallest for which all the functions Y_t are measurable and it is the union of the σ-algebras generated by the countable sub-families of funcitons Y_t, $t \in T$. It is also the smallest σ-algebra containing the measurable rectangles $\prod_{t\in T} A_t$ where $A_t \in \mathcal{E}$ for each t and $A_t = E$ but for a finite sub-family $(t_1, \ldots, t_n)$ of T.

Thus, we have for any finite subset $(t_1, \ldots, t_n)$ of T and sets $A_i \in \mathcal{E}$,

$$\begin{aligned}
\mathbb{P}\left(X_{t_1} \in A_1, \ldots X_{t_n} \in A_n\right) &= \mathbb{P}\left(\omega : X_{t_1}(\omega) \in A_1, \ldots, X_{t_n}(\omega) \in A_n\right) \\
&= \mathbb{P}\left(\omega : \phi(\omega)\,(t_1) \in A_1, \ldots, \phi(\omega)\,(t_n) \in A_n\right) \\
&= \mathbb{P}\left(\omega : Y_{t_1} \circ \phi(\omega) \in A_1, \ldots, Y_{t_n} \circ \phi(\omega) \in A_n\right) \\
&= \mathbb{P} \circ \phi^{-1}\left(Y_{t_1} \in A_1, \ldots, Y_{t_n} \in A_n\right). \qquad (*)
\end{aligned}$$

Thus, by Definition 20.4.20, X and Y have the same finite dimensional distributions.

We call Y the canonical process of the process X.

20.4.8 Previsible processes and finite variation integrals

Definition 20.4.26 (previsible σ-algebra)**.** The previsible σ-algebra $\mathcal{P}$ on $\Omega \times (0,\infty)$ is the σ-algebra generated by sets of the form $E \times (s,t]$ where $E \in \mathcal{F}_s$ and $s < t$.

Definition 20.4.27 (previsible process, continuous-time)**.** A previsible process H is a $\mathcal{P}$-measurable map $H : \Omega \times (0,\infty) \to \mathbb{R}$.

Proposition 20.4.14. Let $(\mathcal{F}_t)_{t\geq 0}$ be the filtration satisfying the usual conditions and X be càdlàg adapted and $H_t = X_{t^-}$ for càdlàg paths, $t > 0$. Then H is previsible.

Proof. For $\Omega' = \{\omega : H(\omega) \text{ has càdlàg path}\}$, we have $\mathbb{P}(\Omega') = 1$. Then for any $\omega \in \Omega'$,

$$\lim_{s\uparrow t} H_s(\omega) = \lim_{s\uparrow t} X_{s^-}(\omega) = X_{(t^-)^-}(\omega) = X_{t^-}(\omega) = H_t(\omega). \tag{20.4.55}$$

For $\omega \in \Omega'^c$, we have $H_s(\omega) = Y_s(\omega)$ for any random variable Y_s (which might not be adapted). Since the filtration satisfies the usual conditions,

$$H_t = X_{t^-}(\omega)\mathbb{1}_{\{\omega\in\Omega'\}} + Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}} \tag{20.4.56}$$

is $\mathcal{F}_t$-measurable ($X_{t^-}(\omega)\mathbb{1}_{\{\omega\in\Omega'\}}$ is $\mathcal{F}_{t^-}$-measurable and thus $\mathcal{F}_t$-measurable. Meanwhile, for any $c \in \mathbb{R}$,

$$\mathbb{P}\left(\omega : Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}} \leq c\right) = 0 \text{ or } 1 \;\Rightarrow \left\{\omega : Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}} \leq c\right\} \text{ is } \mathcal{F}_t\text{-measurable}). \tag{20.4.57}$$

Thus, H is (sample) left-continuous and adapted.

Set $t_n^- = k2^{-n}$ when $k2^{-n} < t \leq (k+1)2^{-n}$ and

$$H_t^n = H_{t_n^-} = \sum_{k=0}^{\infty} X_{k2^{-n}}(t)\mathbb{1}_{\{(k2^{-n},(k+1)2^{-n}]\}}(t). \tag{20.4.58}$$

where

$$X_{k2^{-n}}(t)(\omega) = \begin{cases} H_{k2^{-n}}(\omega) & \omega \in \Omega' \\ Y_t(\omega) & \omega \in \Omega'^c \end{cases} \tag{20.4.59}$$

So $X_{k2^{-n}}(t)$ is $\mathcal{F}_{t_n^-}$-measurable. H is also previsible as it is a pointwise limit of measurable functions. □

Proposition 20.4.15. Let H be a previsible process. Then H_t is $\mathcal{F}_{t^-}$-measurable for all $t > 0$, where $\mathcal{F}_{t^-} = \sigma(F_s : s < t) = \sigma\left(\bigcup_{s<t}\mathcal{F}_s\right)$.

Proof. The previsible σ-algebra $\mathcal{P}$ is generated by π-system

$$\Pi = \{A \times (s,u] : s < u, A \in \mathcal{F}_s\}. \tag{20.4.60}$$

If $H = \mathbb{1}_{\{A\times(s,u]\}}$, then since $\{1\}$ is measurable in $\mathbb{R}$

$$H_t^{-1}(\{1\}) = \begin{cases} A & s < t \leq u \\ \emptyset & \text{otherwise} \end{cases} \tag{20.4.61}$$

Since $A \in \mathcal{F}_s$, we have $H_t^{-1}(\{1\}) \in \mathcal{F}_s \subseteq \mathcal{F}_{t^-}$. Thus, $\mathbb{1}_{\{A\times(s,u]\}}$ is $\mathcal{F}_{t^-}$-measurable.

Now we define

$$\mathcal{A} = \{B \in \mathcal{P} : \mathbb{1}_B(\cdot,t) \text{ is } \mathcal{F}_{t^-}\text{-measurable}\} \subseteq \mathcal{P}. \tag{20.4.62}$$

Clearly, $\Pi \subseteq \mathcal{A}$ since every set $A \times (s,u]$ in Π satisfies $\mathbb{1}_{\{A\times(s,u]\}}$ is $\mathcal{F}_{t^-}$-measurable. Also, we have $\sigma(\Pi) = \mathcal{P}$. Now we show that $\mathcal{A}$ is a d-system. Recall definition of d-system (Definition 15.1.6),

(i) $\Omega \times (0,\infty) \in \mathcal{A}$ as 1 is $\mathcal{F}_{t^-}$-measurable.

(ii) If $C \subset D \in \mathcal{A}$, then $\mathbb{1}_{D\setminus C} = \mathbb{1}_D - \mathbb{1}_C$ is $\mathcal{F}_{t^-}$-measurable since $\mathbb{1}_D, \mathbb{1}_C$ are $\mathcal{F}_{t^-}$-measurable.

(iii) If $C_n \in \mathcal{A}$ with $C_1 \subseteq C_2 \subseteq \ldots$, $\mathbb{1}_{C_n} \uparrow \mathbb{1}_{\bigcup_n C_n}$. Thus $\mathbb{1}_{\bigcup_n C_n}$ is $\mathcal{F}_{t^-}$-measurable as a limit of $\mathcal{F}_{t^-}$-measurable functions.

Thus, $\mathcal{A}$ is a d-system, then by Dynkin's lemma (Lemma 15.1.3), we have $\mathcal{P} \subseteq \mathcal{A}$. So $\mathcal{A} = \mathcal{P}$ and $\forall B \in \mathcal{P}$, we have $\mathbb{1}_B(\cdot,t)$ is $\mathcal{F}_{t^-}$-measurable.

Thus, for $\mathcal{P}$-measurable function H, we define

$$H_t^n := 2^{-n}\lfloor 2^n H_t\rfloor = \sum_{k=1}^{\infty} 2^{-n}k \overbrace{\mathbb{1}_{\underbrace{\left\{H_t \in [2^{-n}k, 2^{-n}(k+1))\right\}}_{\in\mathcal{P}}}}^{\mathcal{F}_{t^-}\text{-measurable}} \tag{20.4.63}$$

Then H_t^n is $\mathcal{F}_{t^-}$-measurable since it is a linear combination of $\mathcal{F}_{t^-}$-measurable functions. Then since $H_t^n \uparrow H_t$, we have H_t is $\mathcal{F}_{t^-}$-measurable as a limit of measurable functions. □

Proposition 20.4.16. Suppose that S and T are stopping times with $S \leq T \leq \infty$. Let Z be a bounded and $\mathcal{F}_S$-measurable. Then $H = Z\mathbb{1}_{(S,T]}$ is $\mathcal{P}$-measurable.

Proof. [21]. □

Theorem 20.4.17. $\mathcal{P}$ is the smallest σ-algebra such that all adapted (sample) left-continuous processes (on $(0,\infty)$) are $\mathcal{P}$-measurable.

Remark. Actually, $\mathcal{P}$ is the smallest σ-algebra such that all bounded adapted left-continuous processes are $\mathcal{P}$-measurable (see Rogers-Williams [11].IV.6).

Proof. For $\Omega' = \{\omega : H(\omega) \text{ has left-continuous path}\}$, we have $\mathbb{P}(\Omega') = 1$. For any bounded adapted(sample) left-continuous process H is the pointwise limit of the processes,

$$H_t^n = H_0\mathbb{1}_{\{0\}}(t) + \sum_{k=0}^{\infty} X_{k/n}(t)\mathbb{1}_{(k/n,(k+1)/n]}(t). \tag{20.4.64}$$

where

$$X_{k/n}(t) = H_{k/n}(\omega)\mathbb{1}_{\{\omega\in\Omega'\}} + Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}}. \tag{20.4.65}$$

Obviously, we have for any $c \in \mathbb{R}$, $\mathbb{P}\left(Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}} \leq c\right) = 0$ or 1. Thus, $\left\{\omega : Y_t(\omega)\mathbb{1}_{\{\omega\in\Omega'^c\}} \leq c\right\}$ is $\mathcal{F}_{k/n}$-measurable (by usual condition of filtered probability space). Therefore, $X_{k/n}(t)$ is $\mathcal{F}_{k/n}$-measurable and H^n is $\mathcal{P}$-measurable. Furthermore, we have $H^n \uparrow H$ which implies that H is $\mathcal{P}$-measurable.

Then for any (sample) left-continuous process H, let $H^m = m \wedge H \vee (-m)$. Since H^m is $\mathcal{P}$-measurable and H is the limit of H^m, we have H is $\mathcal{P}$-measurable as well. Therefore, we have that any (sample) left-continuous process is $\mathcal{P}$-measurable and

$$\sigma\left(\text{all bounded adapted (sample) left-continuous processes}\right) \subseteq \sigma\left(\text{all adapted (sample) left-continuous processes}\right) \subseteq \mathcal{P}.$$

Now we prove the other direction. Define

$$\mathcal{A} := \{A \in \mathcal{P} : \mathbb{1}_A \text{ is (sample) left-continuous}\} = \{A \in \mathcal{P} : \mathbb{1}_A(t) \text{ is (sample) left-continuous for any } t\}. \tag{20.4.66}$$

Obviously, π-system generating $\mathcal{P}$, $\Pi \subseteq \mathcal{A}$. ($\Pi = \{B \times (s,t] : s < t, B \in \mathcal{F}_s\}$). That is, $\mathbb{1}_{B\times(s,t]} = \mathbb{1}_{\omega\in B}\mathbb{1}_{(s,t]}(t)$ is left-continuous for fixed ω.

Now we check that $\mathcal{A}$ is actually a d-system:

(i) $\mathbb{1}_{\Omega\times(0,\infty)}$ is constant 1 a.s. for fixed ω. So it is (sample) continuous and then $\mathbb{1}_{\Omega\times(0,\infty)} \in \mathcal{A}$.

(ii) If $C \subseteq D \in \mathcal{A}$, we have for fixed $\omega \in \Omega$,

$$\mathbb{1}_C, \mathbb{1}_D \text{ are (sample) left-continuous } \Rightarrow \mathbb{1}_{D\setminus C} = \mathbb{1}_D - \mathbb{1}_C \text{ is (sample) left-continuous } \Rightarrow D\setminus C \in \mathcal{A}. \tag{20.4.67}$$

(iii) If $C_n \in \mathcal{A}$ and $C_n \uparrow C$, we have $\mathbb{1}_{C_n}$ is (sample) left-continuous for all n for fixed ω. Then for fixed $\omega \in \Omega$, and $C_0 = \emptyset$,

$$\lim_{t_m\uparrow t} \mathbb{1}_C(t_m) = \lim_{t_m\uparrow t} \lim_{n\to\infty} \mathbb{1}_{C_n}(t_m) = \lim_{t_m\uparrow t} \sum_{n=1}^{\infty} \left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t_m) \quad \text{a.s..} \tag{20.4.68}$$

We can consider $\sum_{n=1}^{\infty}$ as a σ-finite measure. Threrefore, since $\left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t_m) \uparrow \left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t)$ a.s.. Then by monotone convergence theorem (Theorem 15.3.5), we can have (by (sample) left-continuity of C_n and C_{n-1})

$$\lim_{t_m\uparrow t} \sum_{n=1}^{\infty} \left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t_m) = \sum_{n=1}^{\infty} \lim_{t_m\uparrow t} \left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t_m) = \sum_{n=1}^{\infty} \left(\mathbb{1}_{C_n} - \mathbb{1}_{C_{n-1}}\right)(t) = \mathbb{1}_C(t) \quad \text{a.s..} \tag{20.4.69}$$

Thus, $\mathbb{1}_C$ is (sample) left-continuous and $C \in \mathcal{A}$.

[21] see Rogers-Williams [11].IV.6

Therefore, by Dynkin's lemma (Lemma 15.1.3), we have $\mathcal{P} \subseteq \mathcal{A}$. Hence, $\mathcal{A} = \mathcal{P}$, i.e., $\mathcal{P}$ is the smallest σ-algebra such that all adapted (sample) left-continuous processes are $\mathcal{P}$-measurable. □

Proposition 20.4.18. The σ-algebra generated on $\Omega \times (0, \infty)$ by

(i) the space of $E \times (s, t]$ where $E \in \mathcal{F}_s$ and $s < t$,

(ii) the space of all adapted (sample) left-continuous processes on $(0, \infty)$,

(iii) the space of all adapted (sample) continuous processes on $(0, \infty)$

are equal.

Remark. The smallest σ-algebra such that all adapted (sample) continuous processes are $\mathcal{P}$-measurable is the same as the smallest σ-algebra such that all adapted (sample) left-continuous processes are $\mathcal{P}$-measurable!

Proof. Obviously, $\sigma_3 \subseteq \sigma_2$. Also, from Theorem 20.4.17, we have $\sigma_1 = \sigma_2$. So it suffices to prove that $\sigma_1 \subseteq \sigma_3$.

We can see that $\mathbb{1}_{(s,t]}$ is the limit of continuous function f_n with compact support contained in $(s, t + 1/n)$. If $H_s \in \mathcal{F}_s$, the process Hf_n is continuous and adapted which implies that $\sigma_1 \subseteq \sigma_3$. □

Definition 20.4.28 (locally bounded stochastic process)**.** I say that the stochastic process H is locally bounded if there exist stopping times $S_n \uparrow \infty$ a.s. such that $H\mathbb{1}_{(0,S_n]}$ is bounded for all $n \in \mathbb{N}$ a.s., i.e. there exist $C_n < \infty$ non-random such that $\sup_{t \geq 0} \left| H_t \mathbb{1}_{(0,S_n]}(t) \right| \leq C_n$ a.s.. We say $(S_n)_{n \in \mathbb{N}}$ reduce H.

Proposition 20.4.19. Any (sample) continuous adapted process X is locally bounded and previsible.

Proof. Local boundedness is the direct result from Proposition 20.4.6 by taking $T_n = \inf \{t : |X_t| \geq n\}$.

From Proposition 20.4.18, we know that all left-continuous processes are previsible. □

Proposition 20.4.20. Assume that the filtered probability space satisfies usual conditions. Then any càdlàg adapted process X is locally bounded.

Proof. Local boundedness is the direct result from Proposition 20.4.7 by taking $T_n = \inf \{t : |X_t| > n\}$ as A is open $(A := \{|X_t| > n\})$. □

[22]

Theorem 20.4.21. Let $(\mathcal{F}_t)_{t \geq 0}$ be a filtration satisfying usual conditions and A be a càdlàg adapted process with finite variation process V, i.e., for all $\omega \in \Omega$, $A(\omega)$ is càdlàg with finite variation $V(\omega)$ a.s..

Let H be previsible such that for all $t \geq 0$ and $\omega \in \Omega$

$$\int_{(0,t]} |H(\omega, s)| \, dV(\omega, s) < \infty \quad \text{a.s..} \tag{20.4.70}$$

Then we pick set $\Omega' \subseteq \Omega$ $(\mathbb{P}(\Omega') = 1)$ such that for all $\omega' \in \Omega'$, $A(\omega')$ is càdlàg with finite variation $V(\omega')$ and

$$\int_{(0,t]} |H(\omega', s)| \, dV(\omega', s) < \infty \tag{20.4.71}$$

Then the process defined by for all $\omega \in \Omega$,

$$(H \cdot A)_t(\omega) = \begin{cases} \int_{(0,t]} H_s(\omega) dA_s(\omega) & \omega \in \Omega' \\ 0 & \omega \in \Omega'^c \end{cases} \tag{20.4.72}$$

is well-defined, càdlàg, adapted and of (sample) finite variation.

[22] need change, see Rogers-Williams [11].IV10. Let H be an adapted left-continuous process for which $\limsup_{t \downarrow 0} |H_t| < \infty$. Then H is locally bounded and previsible.

Proof. First note that

$$\Delta A_t(\omega) = A_t(\omega) - A_{t^-}(\omega). \tag{20.4.73}$$

Since A is a càdlàg process with finite variation process V, by Proposition 10.3.12, we define

$$A^+ = \frac{1}{2}(V + A), \quad A^- = \frac{1}{2}(V - A) \tag{20.4.74}$$

and we have that A^+ and A^- are non-decreasing (a.s.) càdlàg processes. Then for any $\omega \in \Omega'$,

$$|(H \cdot A)_t(\omega)| = \left| \int_{(0,t]} H_s(\omega) dA_s(\omega) \right| = \left| \int_{(0,t]} H_s(\omega) dA_s^+(\omega) - \int_{(0,t]} H_s(\omega) dA_s^-(\omega) \right| \tag{20.4.75}$$

We know that $dA^+(\omega)$ and $dA^-(\omega)$ are Lebesgue-Stieltjes measure on Ω' by Theorem 15.2.11.

Then by Theorem 15.3.7.(i), for $H_s^+ = \max\{H_s, 0\}$ and $H_s^+ = \max\{-H_s, 0\}$,

$$\begin{aligned}
|(H \cdot A)_t(\omega)| &\leq \left| \int_{(0,t]} H_s^+(\omega) dA_s^+(\omega) - \int_{(0,t]} H_s^-(\omega) dA_s^+(\omega) - \left(\int_{(0,t]} H_s^+(\omega) dA_s^-(\omega) - \int_{(0,t]} H_s^-(\omega) dA_s^-(\omega) \right) \right| \quad (*) \\
&\leq \left| \int_{(0,t]} H_s^+(\omega) dA_s^+(\omega) - \int_{(0,t]} H_s^-(\omega) dA_s^+(\omega) \right| + \left| \int_{(0,t]} H_s^+(\omega) dA_s^-(\omega) - \int_{(0,t]} H_s^-(\omega) dA_s^-(\omega) \right| \\
&\leq \left| \int_{(0,t]} H_s^+(\omega) dA_s^+(\omega) \right| + \left| \int_{(0,t]} H_s^-(\omega) dA_s^+(\omega) \right| + \left| \int_{(0,t]} H_s^+(\omega) dA_s^-(\omega) \right| + \left| \int_{(0,t]} H_s^-(\omega) dA_s^-(\omega) \right|.
\end{aligned}$$

Since $H^+(\omega)$ and $H^-(\omega)$ are non-negative, we can get rid of absolute symbols (as $dA^+(\omega)$ and $dA^-(\omega)$ are measures.). Thus, we have

$$\begin{aligned}
|(H \cdot A)_t(\omega)| &\leq \int_{(0,t]} H_s^+(\omega) dA_s^+(\omega) + \int_{(0,t]} H_s^-(\omega) dA_s^+(\omega) + \int_{(0,t]} H_s^+(\omega) dA_s^-(\omega) + \int_{(0,t]} H_s^-(\omega) dA_s^-(\omega) \\
&= \int_{(0,t]} |H_s(\omega)| \, dA_s^+(\omega) + \int_{(0,t]} |H_s(\omega)| \, dA_s^-(\omega) = \int_{(0,t]} |H_s(\omega)| \, dV_s(\omega) < \infty.
\end{aligned}$$

Thus we have $|(H \cdot A)_t(\omega)| < \infty$ for $\omega \in \Omega'$ and $(H \cdot A)_t(\omega) = 0$ for $\omega \in \Omega'^c$. Thus $(H \cdot A)_t$ is well-defined. In particular, we have

$$(H \cdot A)_t = (H \mathbb{1}_{\{\omega \in \Omega'\}} \cdot A)_t. \qquad (\dagger) \tag{20.4.76}$$

By referring to $(*)$ we may assume without loss of generality in the rest of the proof that $H(\omega)$ is non-negative and $A(\omega)$ non-decreasing and càdlàgfor $\omega \in \Omega'$.

We have

$$\begin{aligned}
&\mathbb{1}_{\{(0,s]\}} \to \mathbb{1}_{(0,t]}, \quad H_s(\omega)\mathbb{1}_{(0,s]}(s) \to H_s(\omega)\mathbb{1}_{(0,t]}(s) \quad \text{as } s \downarrow t, \\
&\mathbb{1}_{\{(0,s]\}} \to \mathbb{1}_{(0,t)}, \quad H_s(\omega)\mathbb{1}_{(0,s]}(s) \to H_s(\omega)\mathbb{1}_{(0,t)}(s) \quad \text{as } s \uparrow t.
\end{aligned}$$

Hence, since dA is a measure and by dominated convergence theorem (Theorem 15.3.12), the following limits exist

$$\begin{aligned}
(H \cdot A)_{t^+}(\omega) &= \lim_{s \downarrow t} (H \cdot A)_s(\omega) = \lim_{s \downarrow t} \int_{(0,\infty)} H_s(\omega)\mathbb{1}_{(0,s]}(s) dA_s(\omega) = \int_{(0,\infty)} H_s(\omega)\mathbb{1}_{(0,t]}(s) dA_s(\omega) = (H \cdot A)_t(\omega) \\
(H \cdot A)_{t^-}(\omega) &= \lim_{s \uparrow t} (H \cdot A)_s(\omega) = \lim_{s \uparrow t} \int_{(0,\infty)} H_s(\omega)\mathbb{1}_{(0,s]}(s) dA_s(\omega) = \int_{(0,\infty)} H_s(\omega)\mathbb{1}_{(0,t)}(s) dA_s(\omega).
\end{aligned}$$

Thus, $(H \cdot A)(\omega)$ is pathwise càdlàg on Ω' with probability one. Also,

$$\Delta(H \cdot A)_t(\omega) = \int_{(0,\infty)} H_s(\omega)\mathbb{1}_{\{t\}}(s) dA_s(\omega) = H_t(\omega) \int_{\{t\}} dA_s(\omega) = H_t(\omega)\Delta A_t(\omega). \qquad (**) \tag{20.4.77}$$

where $H_t(\omega)$ can dragged out of the integral since $H_t(\omega)$ is a real number. Thus, $(H \cdot A)(\omega)$ is càdlàg a.s. on Ω and therefore $(H \cdot A)$ is a càdlàg process.

Next, we show that $H \cdot A$ is adapted.

Suppose first $H = \mathbb{1}_{B\times(u,v]}\mathbb{1}_{\{\omega\in\Omega'\}}$ where $B \in \mathcal{F}_u$. Then

$$\begin{aligned}(H\cdot A)_t &= \int_{(0,t]} \mathbb{1}_{B\times(u,v]}(s)\mathbb{1}_{\{\omega\in\Omega'\}}dA_s = \begin{cases} 0 & t\le u \\ \mathbb{1}_B(A_t - A_u)\mathbb{1}_{\{\omega\in\Omega'\}} & u<t\le v \\ \mathbb{1}_B(A_v - A_u)\mathbb{1}_{\{\omega\in\Omega'\}} & t>v \end{cases} \\ &= \mathbb{1}_B\mathbb{1}_{u<t}(A_{t\wedge v} - A_{t\wedge u})\mathbb{1}_{\{\omega\in\Omega'\}}\end{aligned}$$

which is clearly $\mathcal{F}_t$-measurable. This is true because since $\mathbb{P}(\omega\in\Omega'^c) = 0$ and $\{\{\omega\in\Omega'^c\}\} \in \mathcal{F}_t$ by definition of usual conditions (Definition 20.4.13). Also, $\mathbb{1}_B\mathbb{1}_{u<t}$ and $(A_{t\wedge v} - A_{t\wedge u})$ are $\mathcal{F}_t$-measurable. Thus, $\left(\mathbb{1}_{B\times(u,v]}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)_t$ is $\mathcal{F}_t$-measurable. Now let

$$\Pi = \{B\times(u,v] : B\in\mathcal{F}_u, u<v\}, \qquad \mathcal{A} = \left\{C\in\mathcal{P} : (\mathbb{1}_C\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t \text{ is } \mathcal{F}_t\text{-measurable}\right\} \subseteq \mathcal{P} \tag{20.4.78}$$

so that Π is a π-system. Clearly, $\Pi\subseteq\mathcal{A}$ since every set $B\times(u,v]$ in Π satisfies $\left(\mathbb{1}_{\{B\times(u,v]\}}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)_t$ is $\mathcal{F}_t$-measurable. Also, we have $\sigma(\Pi) = \mathcal{P}$. Now we show that $\mathcal{A}$ is a d-system. Recall definition of d-system (Definition 15.1.6),

(i) $(\mathbb{1}_{\Omega\times(0,\infty)}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t = (A_t - A_0)\mathbb{1}_{\{\omega\in\Omega'\}}$ is $\mathcal{F}_t$-measurable since A is adapted and $\{\omega\in\Omega'\}\in\mathcal{F}_t$ by definition of usual conditions. Thus, $\Omega\times(0,\infty)\in\mathcal{A}$.

(ii) If $C\subset D\in\mathcal{A}$, then $(\mathbb{1}_D\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t$ and $(\mathbb{1}_C\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t$ are $\mathcal{F}_t$-measurable. Then

$$\left(\mathbb{1}_{D\setminus C}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)_t = ((\mathbb{1}_D - \mathbb{1}_C)\cdot A)_t\,\mathbb{1}_{\{\omega\in\Omega'\}} = \underbrace{\left((\mathbb{1}_D\cdot A)_t - (\mathbb{1}_C\cdot A)_t\right)}_{\text{by Theorem 15.3.7.(i)}}\mathbb{1}_{\{\omega\in\Omega'\}} \quad \text{is } \mathcal{F}_t\text{-measurable.} \tag{20.4.79}$$

(iii) If $C_n\in\mathcal{A}$ with $C_1\subseteq C_2\subseteq\ldots$, $\mathbb{1}_{C_n}\uparrow\mathbb{1}_{\bigcup_n C_n}$. Thus by monotone convergence theorem (Theorem 15.3.5),

$$\left(\mathbb{1}_{\bigcup_n C_n}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)_t = \int_{(0,t]}\mathbb{1}_{\bigcup_n C_n}(s)\mathbb{1}_{\{\omega\in\Omega'\}}dA_s = \lim_{n\to\infty}\int_{(0,t]}\mathbb{1}_{C_n}(s)dA_s\mathbb{1}_{\{\omega\in\Omega'\}} = \lim_{n\to\infty}(\mathbb{1}_{C_n}\cdot A)_t\,\mathbb{1}_{\{\omega\in\Omega'\}} \tag{20.4.80}$$

which is $\mathcal{F}_{t^-}$-measurable as a limit of $\mathcal{F}_{t^-}$-measurable functions.

Hence, $\mathcal{A}$ is a d-system. Then by Dynkin's lemma, $\sigma(\Pi)\subseteq\mathcal{A}$ since $\Pi\subseteq\mathcal{A}$. But by definition, $\sigma(\Pi) = \mathcal{P}$ and $\mathcal{A}\subseteq\mathcal{P}$. Thus $\mathcal{A} = \mathcal{P}$.

Recall that H is non-negative and $\mathcal{P}$-measurable. For all $n\in\mathbb{N}$, we set

$$H^n\mathbb{1}_{\{\omega\in\Omega'\}} := 2^{-n}\lfloor 2^nH\rfloor\,\mathbb{1}_{\{\omega\in\Omega'\}} = \sum_{k=1}^{\infty}2^{-n}k\;\mathbb{1}_{\underbrace{\left\{H\in\left[2^{-n}k,2^{-n}(k+1)\right)\right\}}_{\in\mathcal{P}}}\mathbb{1}_{\{\omega\in\Omega'\}}, \tag{20.4.81}$$

so that by Theorem 15.3.7.(i) and Fubini theorem (Theorem 15.3.33),

$$\begin{aligned}(H^n\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t &= \int_{(0,t]}\sum_{k=1}^{\infty}2^{-n}k\;\mathbb{1}_{\{H\in[2^{-n}k,2^{-n}(k+1))\}}dA_s\mathbb{1}_{\{\omega\in\Omega'\}} = \sum_{k=1}^{\infty}\int_{(0,t]}2^{-n}k\;\mathbb{1}_{\{H\in[2^{-n}k,2^{-n}(k+1))\}}\mathbb{1}_{\{\omega\in\Omega'\}}dA_s \\ &= \sum_{k=1}^{\infty}\underbrace{\left(\mathbb{1}_{\{H\in[2^{-n}k,2^{-n}(k+1))\}}\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)_t}_{\mathcal{F}_t\text{-measurable}} \quad \text{is } \mathcal{F}_t\text{-measurable as a sum of } \mathcal{F}_t\text{-measurable functions.}\end{aligned}$$

We have $(H^n\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t\uparrow(H\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t$ by monotone convergence theorem (Theorem 15.3.5 for each ω). Hence, $(H\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A)_t$ is $\mathcal{F}_t$-measurable as a limit of $\mathcal{F}_t$-measurable functions. Thus, by (†), $(H\cdot A) = \left(H\mathbb{1}_{\{\omega\in\Omega'\}}\cdot A\right)$ is adapted.

We know that for all $\omega\in\Omega'$,

$$\begin{aligned}(H\cdot A)_t(\omega) &= \int_{(0,t]}H_s^+(\omega)dA_s^+(\omega) - \int_{(0,t]}H_s^-(\omega)dA_s^+(\omega) - \int_{(0,t]}H_s^+(\omega)dA_s^-(\omega) + \int_{(0,t]}H_s^-(\omega)dA_s^-(\omega) \\ &= \underbrace{\left(\int_{(0,t]}H_s^+(\omega)dA_s^+(\omega) + \int_{(0,t]}H_s^-(\omega)dA_s^-(\omega)\right)}_{:=X_1(\omega)} - \underbrace{\left(\int_{(0,t]}H_s^-(\omega)dA_s^+(\omega) + \int_{(0,t]}H_s^+(\omega)dA_s^-(\omega)\right)}_{:=X_2(\omega)}\end{aligned}$$

We have proved that each integral is càdlàg and non-decreasing. Thus, $X_1(\omega)$ and $X_2(\omega)$ are càdlàg and non-decreasing. So by Proposition 10.3.12, $(H \cdot A)_t(\omega)$ is of finite variation and thus $(H \cdot A)_t$ is of finite variation a.s.. □

Example 20.4.22. Suppose that H is a previsible process and $A_s = s$ for all $\omega \in \Omega$ (thus A is pathwise continuous and of finite variation on $(0, t]$ with pathwise $V_s = s$). If

$$\int_{(0,t]} |H_s|(\omega) ds = \int_{(0,t]} |H_s| \, dV_s(\omega) < \infty \quad \text{for all } \omega \in \Omega, \ t \geq 0. \tag{20.4.82}$$

Then for all $\omega \in \Omega$,

$$\int_{(0,t]} H_s(\omega) ds = \int_{(0,t]} H_s(\omega) dA_s(\omega) \tag{20.4.83}$$

is càdlàg, adapted and of finite variation.

Theorem 20.4.23. Let H be a (sample) left-continuous adapted process which is bounded on compact time intervals (i.e., $\sup_{s \leq t} |H_s| < \infty$ and $\sup_{s \leq t} |K_s| < \infty$ for all t) and let A be a càdlàg adapted finite variation process. Then

$$(H \cdot A)_t = \lim_{n \to \infty} \sum_{k=0}^{\infty} H_{k2^{-n}} (A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t}) \ \text{ a.s.} \tag{20.4.84}$$

Remark. (i) If A is (sample) continuous, we have

$$\begin{aligned}
(H \cdot A)_t &= \lim_{n \to \infty} \sum_{k=0}^{\infty} H_{k2^{-n}} (A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t}) \ \text{ a.s.} \\
&= \lim_{n \to \infty} \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} H_{k2^{-n}} (A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t}) + H_{2^{-n} \lfloor 2^n t \rfloor} (A_t - A_{2^{-n} \lfloor 2^n t \rfloor}) \ \text{ a.s.} \\
&= \lim_{n \to \infty} \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} H_{k2^{-n}} (A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t}) \ \text{ a.s.}
\end{aligned}$$

We can ignore the second term since A is continuous.

(ii) We can also extend this to H locally bounded.

Proof. Since H is bounded on compact time intervals, $(H \cdot A)_t$ is well-defined. Let $H^n_t = H_{2^{-n} \lfloor 2^n t \rfloor}$. Then

$$(H^n \cdot A)_t = \sum_{k=0}^{\infty} H_{k2^{-n}} \left(A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t} \right) \tag{20.4.85}$$

Since H is (sample) left-continuous, we have $H^n_t \to H_t$ a.s. as $n \to \infty$. Fix $T \geq 0$. For $0 \leq t \leq T$ we have (we can consider A as the difference between to non-decreasing càdlàg process, i.e. $A = A^+ - A^-$ and dA^+ and dA^- are Lebesgue-Stieltjes measures by Theorem 15.2.11)

$$|(H^n \cdot A)_t - (H \cdot A)_t| = |((H^n - H) \cdot A)_t| \leq \left(|H^n - H| \cdot (A^+ + A^-) \right)_t \leq \left(|H^n - H| \cdot (A^+ + A^-) \right)_T \tag{20.4.86}$$

since $(|H^n - H| \cdot (A^+ + A^-))_t$ is non-decreasing. But we know that $|H^n - H| \leq 2 \sup_{t \leq T} |H_t| < \infty$ since H is bounded on compact time intervals. Then we use bounded convergence theorem (Theorem 19.3.10 as dA^+ and dA^- are Lebesgue-Stieltjes measures), for any $t \geq 0$

$$|(H^n \cdot A)_t - (H \cdot A)_t| \to 0 \ \text{ a.s..} \tag{20.4.87}$$

as required. □

Theorem 20.4.24 (chain rule)**.** Suppose that H and K are previsible processes which are bounded on compact time intervals (i.e., $\sup_{s \leq t} |H_s| < \infty$ and $\sup_{s \leq t} |K_s| < \infty$ for all t). Let A be a càdlàg adapted finite variation process. Then

$$H \cdot (K \cdot A) = (HK) \cdot A. \tag{20.4.88}$$

Remark. That is, by Proposition 15.3.22 as $d\left(\int_{(0,t]} K_s dA_s\right)$ is a Lebesgue-Stieltjes measure,

$$\int_{(0,t]} H_s d\left((K\cdot A)_s\right) = \int_{(0,t]} H_s K_s dA_s \;\Rightarrow\; d\left(\int_{(0,t]} K_s dA_s\right) = K_t dA_t. \tag{20.4.89}$$

Proof. By Theorem 20.4.21, $K\cdot A$ and $(HK)\cdot A$ are well-defined (since H, K are bounded on compact time intervals and thus satisfy the condition). Also, from Theorem 20.4.21, we know that $K\cdot A$ is also càdlàg, adapted and of finite variation. Thus, $H\cdot(K\cdot A)$ is well-defined.

Therefore, we only consider non-negative H and càdlàg adapted non-decreasing (a.s.) A. For $\omega\in\Omega'^c$ (see the assumption of Theorem 20.4.21), we have for any $t\geq 0$,

$$\left(H\cdot(K\cdot A)\right)_t = \left((HK)\cdot A\right)_t = 0. \tag{20.4.90}$$

For $\omega\in\Omega'$ and any $t\geq 0$, we suppose first

$$H_t = \mathbb{1}_{B_H\times(u_H,v_H]}(t), \quad K_t = \mathbb{1}_{B_K\times(u_K,v_K]}(t) \tag{20.4.91}$$

where $B_H\in\mathcal{F}_{u_H}, B_K\in\mathcal{F}_{u_K}$. Then

$$(H\cdot A)_t = \int_{(0,t]} \mathbb{1}_{B_H\times(u_H,v_H]}(s)dA_s = \begin{cases} 0 & t\leq u_H \\ \mathbb{1}_{B_H}(A_t - A_{u_H}) & u_H < t\leq v_H \\ \mathbb{1}_{B_H}(A_{v_H} - A_{u_H}) & t > v_H \end{cases} = \mathbb{1}_{B_H}\left(A_{t\wedge v_H} - A_{t\wedge u_H}\right) \tag{20.4.92}$$

Similarly, we have $(K\cdot A)_t = \mathbb{1}_{B_K}\left(A_{t\wedge v_K} - A_{t\wedge u_K}\right)$, Thus,

$$\begin{aligned} \left(H\cdot(K\cdot A)\right)_t &= \mathbb{1}_{B_H}\left((K\cdot A)_{t\wedge v_K} - (K\cdot A)_{t\wedge u_K}\right) \\ &= \mathbb{1}_{B_H}\mathbb{1}_{B_K}\left(A_{t\wedge v_H\wedge v_K} + A_{t\wedge u_H\wedge u_K} - A_{t\wedge u_H\wedge v_K} - A_{t\wedge u_K\wedge v_H}\right) \end{aligned}$$

Since $A_{p\wedge q} + A_{p\vee q} = A_p + A_q$, we let $A' = A_{t\wedge u_H\wedge u_K} - A_{t\wedge(u_H\vee u_K)}$. Then

$$\begin{aligned} & A_{t\wedge v_H\wedge v_K} + A_{t\wedge u_H\wedge u_K} - A_{t\wedge u_H\wedge v_K} - A_{t\wedge u_K\wedge v_H} \\ = \;& A_{t\wedge v_H\wedge v_K} + A_{t\wedge(u_H\vee u_K)} - A_{t\wedge u_H\wedge v_K} - A_{t\wedge u_K\wedge v_H} + A' \\ = \;& A_{(t\wedge v_H\wedge v_K)\wedge(t\wedge(u_H\vee u_K))} + A_{(t\wedge v_H\wedge v_K)\vee(t\wedge(u_H\vee u_K))} - A_{(t\wedge u_H\wedge v_K)\wedge(t\wedge u_K\wedge v_H)} - A_{(t\wedge u_H\wedge v_K)\vee(t\wedge u_K\wedge v_H)} + A' \\ = \;& A_{((v_H\wedge v_K)\wedge(u_H\vee u_K))\wedge t} + A_{((v_H\wedge v_K)\vee(u_H\vee u_K))\wedge t} - A_{((u_H\wedge v_K)\wedge(u_K\wedge v_H))\wedge t} - A_{((u_H\wedge v_K)\vee(u_K\wedge v_H))\wedge t} + A' \\ = \;& A_{((u_H\wedge v_K)\vee(v_H\wedge u_K))\wedge t} + A_{((v_H\wedge v_K)\vee(u_H\vee u_K))\wedge t} - A_{(u_H\wedge u_K)\wedge t} - A_{((u_H\wedge v_K)\vee(u_K\wedge v_H))\wedge t} + A' \\ = \;& A_{((v_H\wedge v_K)\vee(u_H\vee u_K))\wedge t} - A_{(u_H\wedge u_K)\wedge t} + A' = A_{((v_H\wedge v_K)\vee(u_H\vee u_K))\wedge t} - A_{(u_H\vee u_K)\wedge t}. \qquad (*) \end{aligned}$$

Thus,

$$\begin{aligned} \left(H\cdot(K\cdot A)\right)_t &= \mathbb{1}_{B_H}\mathbb{1}_{B_K}\left(A_{((v_H\wedge v_K)\vee(u_H\vee u_K))\wedge t} - A_{(u_H\vee u_K)\wedge t}\right) \\ &= \left(\mathbb{1}_{B_H}\mathbb{1}_{B_K}\mathbb{1}_{(u_H\vee u_K,(v_H\wedge v_K)\vee(u_H\vee u_K)]}\cdot A\right)_t = \left((HK)\cdot A\right)_t. \end{aligned}$$

Similarly, suppose

$$H = \sum_{i=1}^{m-1} a_i \mathbb{1}_{B_i^H\times(t_i,t_{i+1}]}(t), \quad K = \sum_{j=1}^{n-1} b_j \mathbb{1}_{B_j^K\times(s_j,s_{j+1}]}(t) \tag{20.4.93}$$

where $a_i, b_j \in \mathbb{R}^{++}$ and $B_i^H \in \mathcal{F}_{t_i}, B_j^K \in \mathcal{F}_{s_j}$. Then

$$\begin{aligned}
& (H \cdot (K \cdot A))_t \\
= & \sum_{i=1}^{m-1} a_i \mathbb{1}_{B_i^H \times (t_i, t_{i+1}]} \cdot \left(\sum_{j=1}^{n-1} b_j \mathbb{1}_{B_j^K \times (s_j, s_{j+1}]} \cdot A \right)_t = \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} a_i b_j \mathbb{1}_{B_i^H \times (t_i, t_{i+1}]} \cdot \left(\mathbb{1}_{B_j^K \times (s_j, s_{j+1}]} \cdot A \right)_t \\
= & \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} a_i b_j \left(\left(\mathbb{1}_{B_i^H \times (t_i, t_{i+1}]} \mathbb{1}_{B_j^K \times (s_j, s_{j+1}]} \right) \cdot A \right)_t = \left(\left(\sum_{i=1}^{m-1} \sum_{j=1}^{n-1} a_i b_j \mathbb{1}_{B_i^H \cap B_j^K} \mathbb{1}_{(t_i \vee s_j, (t_i \vee s_j) \vee (t_{i+1} \wedge s_{j+1})]} \right) \cdot A \right)_t \\
= & ((HK) \cdot A)_t .
\end{aligned}$$

Then for any non-negative uniformly bounded previsible processes H, K, we define $H^m = 2^{-m} \lfloor 2^m H \rfloor$, $K^n = 2^{-n} \lfloor 2^n K \rfloor$, we have

$$(H^m \cdot (K^n \cdot A))_t = ((H^m K^n) \cdot A)_t \tag{20.4.94}$$

By monotone convergence theorem (Theorem 19.3.6 as dA, $d(K^n \cdot A)$ and $d(K \cdot A)$ are Lebesgue-Stieltjes measures),

$$(K^n \cdot A)_t \uparrow (K \cdot A)_t, \quad (H^m \cdot (K \cdot A))_t \uparrow (H \cdot (K \cdot A))_t , \quad ((H^m K^n) \cdot A)_t \uparrow ((HK) \cdot A)_t \tag{20.4.95}$$

We can see that there is an indicator function $\mathbb{1}_{C_n} \uparrow 1$ such that $(K^n \cdot A)_t(\cdot) = (K \cdot A)_t (\mathbb{1}_{C_n})$. Then we have by Proposition 15.3.22,

$$H^m \cdot (K^n \cdot A)_t = (K^n \cdot A)_t (H^m) = (K \cdot A)_t (\mathbb{1}_{C_n} H^m) . \tag{20.4.96}$$

Since $\mathbb{1}_{C_n} H^m \uparrow H^m$, by monotone convergence theorem (Theorem 19.3.6 as $d(K \cdot A)$ is Lebesgue-Stieltjes measure),

$$H^m \cdot (K^n \cdot A)_t \uparrow H^m \cdot (K \cdot A)_t . \tag{20.4.97}$$

Combining these, we have

$$(H \cdot (K \cdot A))_t = ((HK) \cdot A)_t . \tag{20.4.98}$$

Since both processes are càdlàg, they are (pathwise) the same, i.e., $H \cdot (K \cdot A) = (HK) \cdot A$. □

Theorem 20.4.25 (chain rule)**.** Suppose that H and K are locally bounded previsible processes (i.e., there exist stopping times $S_n \uparrow \infty$ a.s. and $S_n' \uparrow \infty$ a.s. such that $\sup_{t \geq 0} \left| H_t \mathbb{1}_{(0, S_n]} \right| < \infty$ and $\sup_{t \geq 0} \left| K_t \mathbb{1}_{(0, S_n']} \right| < \infty$ for all t). Let A be a càdlàg adapted finite variation process. Then

$$H \cdot (K \cdot A) = (HK) \cdot A. \tag{20.4.99}$$

Proof. Let V be the finite variation process of A, we can have (since H, K are locally bounded),

$$\int_{(0,t]} |H(\omega, s)| \, dV(\omega, s) < \infty \ \text{ a.s.}. \tag{20.4.100}$$

Thus, we can use Theorem 20.4.21 and see that $H \cdot (K \cdot A)$ and $(HK) \cdot A$ are well-defined. Let $T_n = S_n \wedge S_n'$, we have by Theorem 20.4.24, for all $t \geq 0$,

$$\left(H \mathbb{1}_{(0, T_n]} \cdot (K \mathbb{1}_{(0, T_n]} \cdot A) \right)_t = \left((H \mathbb{1}_{(0, T_n]} K \mathbb{1}_{(0, T_n]}) \cdot A \right)_t \tag{20.4.101}$$

But $\left((H \mathbb{1}_{(0, T_n]} \mathbb{1}_{(0, T_n]}) \cdot A \right)_t \to ((HK) \cdot A)_t$ a.s., as $n \to \infty$. Similarly,

$$\left(H \mathbb{1}_{(0, T_n]} \cdot (K \mathbb{1}_{(0, T_n]} \cdot A) \right)_t = \left(H \mathbb{1}_{(0, T_n]} \cdot (K \cdot A)^{T_n} \right)_t = (H \cdot (K \cdot A))_t^{T_n} \to (H \cdot (K \cdot A))_t \quad \text{a.s.} \tag{20.4.102}$$

Thus, we have

$$(H \cdot (K \cdot A))_t = ((HK) \cdot A)_t \quad \text{a.s.}. \tag{20.4.103}$$

But both processes are càdlàg, we have these two processes are indistinguishable. That is,

$$H \cdot (K \cdot A) = (HK) \cdot A. \tag{20.4.104}$$

□

20.4.9 Convergence of stochastic processes

Recalling uniform convergence on compacts (Definition 13.3.2), we have the following definition for stochastic processes:

Definition 20.4.29 (uniform convergence on compacts almost surely)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. For a sequence of jointly measurable ($\mathcal{F}\otimes\mathcal{B}(\mathbb{R})$-measurable) stochastic processes $(X^n)_{n\in\mathbb{N}}$ we say that X^n uniformly converges on compacts a.s. to the process X if

$$\forall \varepsilon > 0, \forall t \geq 0, \quad \mathbb{P}\left(\sup_{s\leq t} |X_s^n - X_s| \to 0\right) = 1 \quad \text{as } n \to \infty. \tag{20.4.105}$$

X^n is said to converge u.c.a.s. to X and it is denoted by $X^n \xrightarrow{ucas} X$, or $X^n \to X$ u.c.a.s..

Definition 20.4.30 (uniform convergence on compacts in probability)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. For a sequence of jointly measurable ($\mathcal{F} \otimes \mathcal{B}(\mathbb{R})$-measurable) stochastic processes $(X^n)_{n\in\mathbb{N}}$ we say that X^n converge to the process X in the ucp topology (uniform convergence on compacts in probability, u.c.p.) if

$$\forall \varepsilon > 0, \forall t \geq 0, \quad \mathbb{P}\left(\sup_{s\leq t} |X_s^n - X_s| > \varepsilon\right) \to 0 \quad \text{as } n \to \infty. \tag{20.4.106}$$

X^n is said to converge u.c.p. to X and it is denoted by $X^n \xrightarrow{ucp} X$, or $X^n \to X$ u.c.p..

Remark. This mode of convergence occurs frequently in the theory of continuous-time stochastic processes[23].

Note that this definition does not make sense for arbitrary stochastic processes, as the supremum is over the uncountable index set $[0, t]$ and need not be measurable. However, for right or left continuous processes, the supremum can be restricted to the countable set of rational times, which will be measurable. In fact, for jointly measurable processes, it can be shown that the supremum is measurable with respect to the completion of the probability space, so ucp convergence makes sense.

Comparing to Theorem 19.2.16, we have the following theorem:

Theorem 20.4.26. Let $(X^n)_{n\in\mathbb{N}}$ be a sequence of stochastic processes. Then

(i) If $X^n \to 0$ u.c.a.s., then $X_n \to 0$ u.c.p..

(ii) If $X^n \to 0$ u.c.p., then $X^{n_k} \to 0$ u.c.a.s. for some subsequence $(n_k)_{k\in\mathbb{N}}$.

Remark. For some stochastic process X, we can have (by definitions and Theorem 20.4.26)

(i) If $X^n \to X$ u.c.a.s., then $X_n \to X$ u.c.p..

(ii) If $X^n \to X$ u.c.p., then $X^{n_k} \to X$ u.c.a.s. for some subsequence $(n_k)_{k\in\mathbb{N}}$.

Proof. (i) Suppose $X^n \to 0$ u.c.a.s.. That is,

$$\mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \to 0\right) = 1 \quad \text{as } n \to \infty. \tag{20.4.107}$$

Then for each $\varepsilon > 0$ and $t \geq 0$,

$$\mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \leq \varepsilon\right) \geq \underbrace{\mathbb{P}\left(\bigcap_{m\geq n}\left\{\sup_{0\leq s\leq t} |X_s^n| \leq \varepsilon\right\}\right) \uparrow \mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \leq \varepsilon \text{ ev.}\right)}_{\text{Lemma } 15.1.10} \geq \mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \to 0\right), \tag{20.4.108}$$

$$\mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| > \varepsilon\right) = 1 - \mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \leq \varepsilon\right) \leq 1 - \mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| \to 0\right) = 0. \tag{20.4.109}$$

Hence $\mathbb{P}\left(\sup_{0\leq s\leq t} |X_s^n| > \varepsilon\right) \to 0$ and $X^n \to 0$ u.c.a.s..

[23] need some examples

(ii) Suppose $X^n \to 0$ u.c.p., then $\forall \varepsilon > 0$, $\mathbb{P}\left(\sup_{0\le s\le t} |X_s^n| > \varepsilon\right) \to 0$ i.e.

$$\forall \varepsilon > 0,\ \delta > 0,\ \exists N,\ \forall n \ge N, \quad \mathbb{P}\left(\sup_{0\le s\le t} |X_s^n| > \varepsilon\right) < \delta. \tag{20.4.110}$$

so we can find a subsequence (n_k) such that $\varepsilon_k = 1/k$ and $\delta_k = 2^{-k}$,

$$\mathbb{P}\left(\sup_{0\le s\le t} |X_s^{n_k}| > 1/k\right) < 2^{-k} \ \Rightarrow\ \sum_{k=1}^{\infty} \mathbb{P}\left(\sup_{0\le s\le t} |X_s^{n_k}| > 1/k\right) < \sum_k 2^{-k} = 1 < \infty. \tag{20.4.111}$$

So, by the first Borel-Cantelli lemma (Lemma 19.1.24),

$$0 = \mathbb{P}\left(\sup_{0\le s\le t} |X_s^{n_k}| > 1/k \text{ i.o.}\right) = \mathbb{P}\left(\left\{\sup_{0\le s\le t} |X_s^{n_k}| \le 1/k \text{ ev.}\right\}^c\right) = \mathbb{P}\left(\left\{\sup_{0\le s\le t} |X_s^{n_k}| \to 0\right\}^c\right) \ \Rightarrow\ \sup_{0\le s\le t} |X_s^{n_k}| \to 0 \text{ a.s.}$$

which means that $X^{n_k} \to 0$ u.c.a.s.

□

Theorem 20.4.27 (completeness under u.c.p. convergence)**.** Suppose that $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\ge 0}, \mathbb{P})$ is the filtered probability space satisfying usual conditions. The space of càdlàg (respectively, (sample) continuous) adapted process is complete under u.c.p. convergence.

Furthermore, if $X^n \xrightarrow{ucp} X$ then there is a subsequence whose sample paths almost surely converge to those of X uniformly on compacts.

Proof. We only consider càdlàg case. For any càdlàg adapted process X and Y, we can find stopping time sequence $T_n \uparrow \infty$ a.s. such that the following is well-defined a.s.

$$\sup_{0\le s\le t} \left|X_s^{T_n} - Y_s^{T_n}\right| \tag{20.4.112}$$

as they are locally bounded by Proposition 20.4.20. Thus, for t and any $s \in [0, t]$, we can always find $T_n > s$ a.s. such that we can define

$$\sup_{0\le s\le t} |X_s - Y_s| \quad \text{a.s..} \tag{20.4.113}$$

Let X^n be a Cauchy sequence under u.c.p. convergence, so that for any $t \in \mathbb{R}^{++}$ and $\varepsilon > 0$,

$$\mathbb{P}\left(\sup_{0\le s\le t} |X_s^m - X_s^n| > \varepsilon\right) \to 0 \quad \text{as } m, n \to \infty. \tag{20.4.114}$$

This is equal to the statement

$$\forall \varepsilon > 0,\ \delta > 0,\ \exists N,\ \forall n \ge N,\ \forall m \ge 0, \quad \mathbb{P}\left(\sup_{0\le s\le t} \left|X_s^{m+n} - X_s^n\right| > \varepsilon\right) < \delta \tag{20.4.115}$$

which means $X^{n+m} - X^n \to 0$ u.c.p.. Then by Theorem 20.4.26, we have a subsequence $(n_k)_{k\in\mathbb{N}}$ such that $X^{n_k+m} - X^{n_k} \to 0$ u.c.a.s. for any $m \ge 0$. Thus, let $n_k + m = n_{k+1}$, we can see that

$$\mathbb{P}\left(\sup_{0\le s\le t} |X_s^{n_{k+1}} - X_s^{n_k}| \to 0\right) = 1 \tag{20.4.116}$$

which means X^{n_k} is also a Cauchy sequence under uniform convergence on compacts a.s.. Thus, for any $t \in \mathbb{R}^{++}$, we have that

$$\left|X_t^{n_k} - X_t^{n_{k+1}}\right| \to 0 \text{ a.s. } \Rightarrow\ X_t^{n_k} \to X_t \text{ a.s.} \tag{20.4.117}$$

by completeness of $\mathbb{R}$ (Theorem 3.6.1). We know that X^n is adapted (i.e., X_t^n is $\mathcal{F}_t$-measurable for any t), then we have X is also adapted a.s. (as $X_t = \lim X_t^{n_k}$ is still $\mathcal{F}_t$-measurable by Theorem 15.2.8). But we know that the filtered probability space satisfies usual conditions, we have X is adapted by the definition of usual conditions ($\mathcal{F}_t$ containing all null sets).

Since X^{n_k} have left limits a.s., then it is clear that[24]

$$\sup_{0\le s\le t}\left|X^{n_k}_{s^-}-X^{n_{k+1}}_{s^-}\right|\le\sup_{0\le s\le t}|X^{n_k}_s-X^{n_{k+1}}_s| \tag{20.4.118}$$

and therefore, the left limits of X^{n_k} ($X^{n_k}_-$) are also Cauchy sequence under uniform convergence on compacts a.s.. As limits can be commuted with uniform convergence of sequences[25], if the processes are càdlàg then,

$$\begin{aligned}\lim_{s\downarrow t}X_s&\overset{\text{a.s.}}{=}\lim_{s\downarrow t}\lim_{k\to\infty}X^{n_k}_s=\lim_{k\to\infty}\lim_{s\downarrow t}X^{n_k}_s=\lim_{k\to\infty}X^{n_k}_t\overset{\text{a.s.}}{=}X_t\quad\text{a.s.}\\ \lim_{s\uparrow t}X_s&\overset{\text{a.s.}}{=}\lim_{s\uparrow t}\lim_{k\to\infty}X^{n_k}_s=\lim_{k\to\infty}\lim_{s\uparrow t}X^{n_k}_s=\lim_{k\to\infty}X^{n_k}_{t^-}:=X_{t^-}\quad\text{a.s.}\end{aligned}$$

So X is càdlàg and $X^{n_k}_-\to X_-$ under uniform convergence on compacts.

To complete the proof, it just remains to show that the original sequence X^n does indeed converge ucp to X. We already have that X^{n_k} converges to X under uniform convergence on compacts a.s. (i.e. the sample paths of X^{n_k} almost surely converge to those of X uniformly on compacts). Thus, it is obvious that X^{n_k} converges to X u.c.p., i.e., for any $t\in\mathbb{R}^{++}$ and $\varepsilon>0$,

$$\lim_{k\to\infty}\mathbb{P}\left(\sup_{0\le s\le t}|X^{n_k}_s-X_s|>\varepsilon\right)=0\quad(*) \tag{20.4.119}$$

Then by the assumption that X^n is a Cauchy sequence under u.c.p convergence and $(*)$, we have

$$\begin{aligned}\mathbb{P}\left(\sup_{0\le s\le t}|X^n_s-X_s|>\varepsilon\right)&\le\mathbb{P}\left(\sup_{0\le s\le t}|X^n_s-X^{n_k}_s|+\sup_{0\le s\le t}|X^{n_k}_s-X_s|>\varepsilon\right)\\&\le\mathbb{P}\left(\sup_{0\le s\le t}|X^n_s-X^{n_k}_s|>\varepsilon/2\right)+\mathbb{P}\left(\sup_{0\le s\le t}|X^{n_k}_s-X_s|>\varepsilon/2\right)\to0+0=0\end{aligned}$$

which means $X^n\to X$ u.c.p..

We skip the the continuous adpated processes space case as the argument is similar. □

20.5 Continuous-time Martingales

20.5.1 Definitions

Definition 20.5.1. Let $(\Omega,\mathcal{F},(\mathcal{F}_t)_{t\ge0},\mathbb{P})$ be a filtered probability space. Let $X=(X_t)_{t\ge0}$ be an adpated real-valued integrable process (see Definition 20.4.7 and Definition 20.4.3). Then for $s,t\in\mathbb{R}^{++}$,

(i) X is a martingale with respect to $((\mathcal{F}_t)_{t\ge0},\mathbb{P})$ if $\mathbb{E}(X_t|\mathcal{F}_s)=X_s$ a.s. for all $t\ge s$.

(ii) X is a supermartingale with respect to $((\mathcal{F}_t)_{t\ge0},\mathbb{P})$ if $\mathbb{E}(X_t|\mathcal{F}_s)\le X_s$ a.s. for all $t\ge s$.

(iii) X is a submartingale with respect to $((\mathcal{F}_t)_{t\ge0},\mathbb{P})$ if $\mathbb{E}(X_t|\mathcal{F}_s)\ge X_s$ a.s. for all $t\ge s$.

In particular, if X is a

(i) martingale, then $\mathbb{E}(X_t)=\mathbb{E}(X_s)$ for all $t\ge s$.

(ii) supermartingale, then $\mathbb{E}(X_t)\le\mathbb{E}(X_s)$ for all $t\ge s$.

(iii) submartingale, then $\mathbb{E}(X_t)\ge\mathbb{E}(X_s)$ for all $t\ge s$.

Remark. If a process is both supermartingale and submartingale, then it is a martingale.

Remark. The definition of $\mathbb{E}(X|\mathcal{F})$ the conditional expectation for a random variable $X\in\mathcal{L}^1(\mathbb{C})$ is $\mathbb{E}(\Re X|\mathcal{F})+i\mathbb{E}(\Im X|\mathcal{F})$, and we say that an integrable process $(X_t)_{t\ge0}$ with values in $\mathbb{C}$, and adapted to a filtration $(\mathcal{F}_t)$, is a martingale if its real and imaginary parts are.

Proposition 20.5.1. If X is a martingale, then $|X|$, X^+ and X^- are submartingales.

[24] need details
[25] need theorem

Proof. We know that for all $s \leq t$, by Proposition 19.4.20.(iv),

$$|X_s| = |\mathbb{E}(X_t|\mathcal{F}_s)| \leq \mathbb{E}(|X_t||\mathcal{F}_s) \text{ a.s. } \Rightarrow |X| \text{ is a submartingale.} \tag{20.5.1}$$

Also, $X = X^+ - X^-$ and $|X| = X^+ + X^-$, by Proposition 19.4.20.(iii),(iv)

$$\begin{aligned} X_s^+ &= \frac{1}{2}(|X_s| + X_s) \leq \frac{1}{2}(\mathbb{E}(|X_t||\mathcal{F}_s) + \mathbb{E}(X_t|\mathcal{F}_s)) = \mathbb{E}\left(X_t^+|\mathcal{F}_s\right) \text{ a.s..} \\ X_s^- &= \frac{1}{2}(|X_s| - X_s) \leq \frac{1}{2}(\mathbb{E}(|X_t||\mathcal{F}_s) - \mathbb{E}(X_t|\mathcal{F}_s)) = \mathbb{E}\left(X_t^+|\mathcal{F}_s\right) \text{ a.s..} \end{aligned}$$

Thus, X^+ and X^- are submartingales. □

Remark. We can also prove this with Jensen's inequality as $|X|$, X^+ and X^- are convex.

Proposition 20.5.2. If X is a martingale and f is a convex function with $f(X) \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ or $f > 0$, then $f(X)$ is submartingale.

Proof. By conditional Jensen's inequality (Theorem 19.4.26), for $s \leq t$,

$$f(\mathbb{E}(X_t|\mathcal{F}_s)) \leq \mathbb{E}(f(X)|\mathcal{F}_s) \text{ a.s.} \tag{20.5.2}$$

Also, $\mathbb{E}(X_t|\mathcal{F}_s) = X_s$ a.s.. Thus, we have

$$X_s \leq \mathbb{E}(f(X)|\mathcal{F}_s) \text{ a.s.} \tag{20.5.3}$$

which implies that X is submartingale. □

Lemma 20.5.3. Let X be a martingale and such that for some given $s < t$, $\mathbb{E}(X_s^2) < \infty$ and $\mathbb{E}(X_t^2) < \infty$. Then

$$\mathbb{E}\left(X_t^2 - X_s^2 \middle| \mathcal{F}_s\right) = \mathbb{E}\left((X_t - X_s)^2 \middle| \mathcal{F}_s\right), \quad \text{a.s..} \tag{20.5.4}$$

Proof. By expanding the square $(X_t - X_s)^2$, the right-hand side is equal to

$$\mathbb{E}\left((X_t - X_s)^2 \middle| \mathcal{F}_s\right) \overset{\text{a.s.}}{=} \mathbb{E}\left(X_t^2 \middle| \mathcal{F}_s\right) - 2X_s\mathbb{E}(X_t|\mathcal{F}_s) + X_s^2 \overset{\text{a.s.}}{=} \mathbb{E}\left(X_t^2 \middle| \mathcal{F}_s\right) - 2X_s^2 + X_s^2 \overset{\text{a.s.}}{=} \mathbb{E}(X_t^2 - X_s^2|\mathcal{F}_s). \tag{20.5.5}$$

where we use X_sX_t is integrable ($\mathbb{E}|X_sX_t| \leq \sqrt{\mathbb{E}(X_s^2)\mathbb{E}(X_t^2)} < \infty$ by Hölder's inequality (Theorem 19.3.24)) and Proposition 19.4.28 for the first and third equations. For the second equation, we simply use martingale definition. □

Lemma 20.5.4. Let M be a bounded martingale. Suppose that $n \in \mathbb{N}$ and $0 = t_0 < t_1 < \cdots < t_n < \infty$. Then

$$\mathbb{E}\left(\left(\sum_{k=0}^{n-1}(M_{t_{k+1}} - M_{t_k})^2\right)^2\right) \quad \text{is bounded.} \tag{20.5.6}$$

Proof. First note that

$$\mathbb{E}\left(\left(\sum_{k=0}^{n-1}(M_{t_{k+1}} - M_{t_k})^2\right)^2\right) = \sum_{k=0}^{n-1}\mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^4\right) + 2\sum_{k=0}^{n-1}\mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\sum_{j=k+1}^{n-1}(M_{t_{j+1}} - M_{t_j})^2\right). \tag{$*$}$$

For each fixed k we have (by property of martingale and Lemma 20.5.3),

$$\begin{aligned} \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\sum_{j=k+1}^{n-1}(M_{t_{j+1}} - M_{t_j})^2\right) &= \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\mathbb{E}\left(\sum_{j=k+1}^{n-1}(M_{t_{j+1}} - M_{t_j})^2\middle|\mathcal{F}_{t_{k+1}}\right)\right) \\ &= \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\mathbb{E}\left(\sum_{j=k+1}^{n-1}(M_{t_{j+1}}^2 - M_{t_j}^2)\middle|\mathcal{F}_{t_{k+1}}\right)\right) \\ &= \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\mathbb{E}\left(M_{t_n}^2 - M_{t_{k+1}}^2\middle|\mathcal{F}_{t_{k+1}}\right)\right) \\ &= \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\left(M_{t_n}^2 - M_{t_{k+1}}^2\right)\right) \end{aligned}$$

After inserting this in $(*)$ we get the estimate

$$\begin{aligned}\mathbb{E}\left(\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right) &\leq \mathbb{E}\left(\sup_{0\leq j<n}\left|M_{t_{j+1}}-M_{t_j}\right|^2\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2+2\sup_{0\leq j<n}\left|M_{t_l}-M_{t_j}\right|^2\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right)\\ &= \mathbb{E}\left(\left(\sup_{0\leq j<n}\left|M_{t_{j+1}}-M_{t_j}\right|^2+2\sup_{0\leq j<n}\left|M_{t_l}-M_{t_j}\right|^2\right)\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right).\end{aligned}$$

Now, M is uniformly bounded by C, say ($\sup_{0\leq k<n}|M_{t_k}|\leq C$). So using the inequality $(x-y)^2\leq 2(x^2+y^2)$, we obtain

$$\begin{aligned}\mathbb{E}\left(\left(\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right)^2\right) &\leq \mathbb{E}\left(\left(4C^2+2\cdot 4C^2\right)\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right)=12C^2\mathbb{E}\left(\sum_{k=0}^{n-1}(M_{t_{k+1}}-M_{t_k})^2\right)\\ &= 12C^2\mathbb{E}\left((M_{t_n}-M_{t_0})^2\right)\leq 12C^2\cdot 4C^2=48C^4.\end{aligned}$$

□

20.5.2 Martingale regularization theorem

Lemma 20.5.5. Let $f:\mathbb{Q}^+\to\mathbb{R}$ be a function defined on the positive rational numbers. Suppose that for all $a<b$ and $a,b\in\mathbb{Q}$ and all bounded $I\subseteq\mathbb{Q}^+$ the function f is bounded on I and the number of upcrossings of the interval $[a,b]$ during the time intervals I by f is finite, i.e. $N(f,I,[a,b])<\infty$, where $N(f,I,[a,b])$ is defined as

$$\sup\left\{n\geq 0:\exists 0\leq s_1<t_1<\cdots<s_n<t_n,\ s_i,t_i\in I,\ f(s_i)<a, f(t_i)>b,\ 1\leq i\leq n\right\}. \tag{20.5.7}$$

Then for every $t\in\mathbb{R}^{++}$ the right and left limits of f exist and are finite, i.e.

$$\lim_{s\downarrow t}f(s),\ \lim_{s\uparrow t}f(s)\ \text{ exist and are finite.} \tag{20.5.8}$$

Proof. First note that if (s_n) is a sequence of rationals decreasing to t, then by the same argument in Lemma 20.2.11 (with the assumption that $N(f,I,[a,b])<\infty$), we get that the limit $\lim_n f(s_n)$ exists. Similarly if t_n is a sequence increasing to t, then the limit $\lim_n f(t_n)$ exists. So far we showed that for any sequence converging to t from above (or below) the limit exists. It remains to show that the limit is the same along any sequence decreasing to t.

To see this, note that if $(s_n)_{n\geq 0}$ is a sequence decreasing to t and $(t_n)_{n\geq 0}$ is another sequence decreasing to t but $\lim_n f(s_n)\neq\lim_n f(t_n)$. Then we can combine the two sequences and get a decreasing sequence $(a_n)_{n\geq 0}$ (by $a_n=s_n\wedge t_n$ for all n) converging to t such that $\lim_n f(a_n)$ does not exist, which is a contradiction, since we already showed that for every decreasing sequence the limit exists.

Finally the limits from above and below are finite, which follows by the assumption that f is bounded on any bounded subset of $\mathbb{Q}^+$. □

Theorem 20.5.6 (Martingale regularization theorem)**.** Let $(X_t)_{t\geq 0}$ be a martingale with respect to the filtration $(\mathcal{F}_t)_{t\geq 0}$. Then there exists a càdlàg process $\widetilde{X}$ which is a martingale with respect to $(\widetilde{\mathcal{F}}_t)_{t\geq 0}$ (see Definition 20.4.14) and satisfies

$$X_t=\mathbb{E}\left(\widetilde{X}_t|\mathcal{F}_t\right)\ \text{ a.s. for all } t\geq 0. \tag{20.5.9}$$

If the filtration $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions, then $\widetilde{X}$ is a càdlàg version of X.

Remark. In the case when the filtration satisfies the usual conditions, a martingale admits a càdlàg version so there is 'little to lose' to consider that martingale are càdlàg.

Proof. $\forall t\in\mathbb{R}^{++}$, the goal is to define $\widetilde{X}$ as follows:

$$\widetilde{X}_t=\lim_{s\downarrow t,s\in\mathbb{Q}^+}X_s \tag{20.5.10}$$

on a set of measure 1 and 0 elsewhere.

So first we need to check that the limit above exists a.s. and is finite. In order to do so, we are going to use Lemma 20.5.5. Therefore we first show that X is bounded on bounded subsets I of $\mathbb{Q}^+$.

Let I be such a subset. Consider $J = \{j_1, \ldots, j_n\} \subseteq I$, where $j_1 < j_2 < \cdots < j_n$. Then the process $(X_j)_{j\in J}$ is a discrete time martingale. By Doob's maximal inequality (Theorem 20.2.16) we obtain

$$\lambda \mathbb{P}\left(\max_{j\in J} |X_j| \geq \lambda\right) \leq \mathbb{E}\,|X_{j_n}| \leq \mathbb{E}\,|X_K|\,. \tag{20.5.11}$$

where $K > \sup I$. The second inequality holds since $|X|$ is a submartingale. So taking a monotone limit over J finite subsets of I with union the set I ($\mathbb{1}_{\{\max_{j\in J}|X_j|\}} \uparrow \mathbb{1}_{\left\{\sup_{t\in I}|X_t|\right\}}$), then by monotone convergence theorem (Theorem 19.3.6) we get that

$$\lambda \mathbb{P}\left(\sup_{t\in I} |X_t| \geq \lambda\right) = \lambda \mathbb{E}\left(\mathbb{1}_{\left\{\sup_{t\in I}|X_t|\geq\lambda\right\}}\right) = \lambda \lim_{n\to\infty} \mathbb{E}\left(\mathbb{1}_{\{\max_{j\in J}|X_j|\geq\lambda\}}\right) = \lambda \lim_{n\to\infty} \mathbb{P}\left(\max_{j\in J} |X_j| \geq \lambda\right) \leq \mathbb{E}\,|X_K| < \infty. \tag{20.5.12}$$

since X is a martingale with integrability. Therefore by letting $\lambda \to \infty$ this shows that

$$\mathbb{P}\left(\sup_{t\in I} |X_t| < \infty\right) = 1. \tag{20.5.13}$$

Let $a < b$ be rational numbers. Then we have

$$N(X, I, [a, b]) = \sup_{\substack{J\subseteq I \\ J \text{ is finite}}} N(X, J, [a, b]). \tag{20.5.14}$$

Let $J = \{a_1, \ldots, a_n\}$ (in increasing order again) be a finite subset of I. Then $(X_{a_i})_{i\leq n}$ is a martingale and Doob's upcrossing lemma (Lemma 20.2.12)gives that

$$(b-a)\mathbb{E}\,(N(X, J, [a, b])) \leq \mathbb{E}\left((X_{a_n} - a)^-\right) \leq \mathbb{E}\left((X_K - a)^-\right) \qquad (*) \tag{20.5.15}$$

where the second inequality holds since $(X - a)^-$ is a submartingale (by Proposition 20.5.1).

Let $I_M = \mathbb{Q}^+ \cap [0, M]$. Then we consider the above inequality for $J \subseteq I_M$. By monotone convergence theorem (Theorem 19.3.6) again as $N(X, J, [a, b]) \uparrow N(X, I_M, [a, b])$, we will get that for all M,

$$(b-a)\mathbb{E}\,(N(X, I_M, [a, b])) = (b-a) \lim_{n\to\infty} \mathbb{E}\,(N(X, J, [a, b])) \leq \mathbb{E}\left((X_K - a)^-\right) \leq \mathbb{E}\,|X_K - a| \leq \mathbb{E}\,|X_K| + \mathbb{E}\,|a| < \infty. \tag{20.5.16}$$

where $K = \sup I_M$. The last inequality is from the fact that X is a martingale. Thus,

$$\mathbb{E}\,(N(X, I_M, [a, b])) < \infty \;\Rightarrow\; N(X, I_M, [a, b]) < \infty \text{ a.s.} \tag{20.5.17}$$

Thus if we now let

$$\Omega_0 = \bigcap_{M\in\mathbb{N}} \bigcap_{\substack{a<b \\ a,b\in\mathbb{Q}}} \{N(X, I_M, [a, b]) < \infty\} \cap \left\{\sup_{t\in I_M} |X_t| < \infty\right\}, \tag{20.5.18}$$

then we obtain that $\mathbb{P}(\Omega_0) = 1$. For $\omega \in \Omega_0$ by Lemma 20.5.5 the following limits exist and are finite in $\mathbb{R}$:

$$\begin{aligned} X_{t^+}(\omega) &= \lim_{s\downarrow t, s\in\mathbb{Q}} X_s(\omega), \quad t \geq 0 \\ X_{t^-}(\omega) &= \lim_{s\uparrow t, s\in\mathbb{Q}} X_s(\omega), \quad t > 0. \end{aligned}$$

Hence we can now define for $t \geq 0$,

$$\widetilde{X}_t = \begin{cases} X_{t^+}, & \text{on } \Omega_0 \\ 0 & \text{otherwise} \end{cases} \tag{20.5.19}$$

Then clearly $\widetilde{X}_t$ is $(\widetilde{\mathcal{F}}_t)_{t\geq 0}$ adapted, since $(\widetilde{\mathcal{F}}_t)_{t\geq 0}$ contains also the events of 0 probability.

Let t_n be a sequence in $\mathbb{Q}$ such that $t_n \downarrow t$ as $n \to \infty$. Then

$$\widetilde{X}_t = \lim_{n\to\infty} X_{t_n} \quad \text{a.s.} \tag{20.5.20}$$

Therefore, by conditional dominated convergence theorem (Theorem 19.4.25),

$$\mathbb{E}\left(X_{t_n}|\mathcal{F}_t\right) \to \mathbb{E}\left(\widetilde{X}_t|\mathcal{F}_t\right) \quad \text{a.s.} \tag{20.5.21}$$

But $\mathbb{E}\left(X_{t_n}|\mathcal{F}_t\right) = X_t$ since X is a martingale. Therefore,

$$X_t = \mathbb{E}\left(\widetilde{X}_t|\mathcal{F}_t\right) \quad \text{a.s..} \tag{20.5.22}$$

It remains to show the martingale property of $\widetilde{X}$.

Let $s < t$ and s_n a sequence in $\mathbb{Q}$ such that $s_n \downarrow s$ and $s_0 < t$. Then by martingale property,

$$\widetilde{X}_s \overset{\text{a.s.}}{=} \lim X_{s_n} \overset{\text{a.s.}}{=} \lim \mathbb{E}\left(X_t|\mathcal{F}_{s_n}\right). \tag{20.5.23}$$

Now note that $(\mathbb{E}\left(X_t|\mathcal{F}_{s_n}\right))_{n\geq 0}$ is a backward martingale and hence it converges a.s. and in $\mathcal{L}^1(\Omega,\mathcal{F},\mathbb{P})$ to $\mathbb{E}\left(X_t|\mathcal{F}_{s^+}\right)$ (by Theorem 20.2.26). Therefore,

$$\widetilde{X}_s = \mathbb{E}\left(X_t|\mathcal{F}_{s^+}\right) \quad \text{a.s.} \qquad (\dagger) \tag{20.5.24}$$

If s ¡ t, then by the tower property and (†) we get that for any $r \geq t$,

$$\mathbb{E}\left(\widetilde{X}_t|\mathcal{F}_{s^+}\right) = \mathbb{E}\left(\mathbb{E}\left(X_r|\mathcal{F}_{t^+}\right)|\mathcal{F}_{s^+}\right) \overset{\text{a.s.}}{=} \mathbb{E}\left(X_r|\mathcal{F}_{s^+}\right) \overset{\text{a.s.}}{=} \widetilde{X}_s. \tag{20.5.25}$$

Then by Proposition 19.4.28.(vi), we get that

$$\mathbb{E}\left(\widetilde{X}_t\middle|\,\widetilde{\mathcal{F}}_s\right) = \mathbb{E}\left(\widetilde{X}_t\middle|\,\sigma(\mathcal{F}_{s^+},\mathcal{N})\right) = \mathbb{E}\left(\widetilde{X}_t\middle|\,\mathcal{F}_{t^+}\right) \quad \text{a.s..} \tag{20.5.26}$$

Then with (†), we have

$$\mathbb{E}\left(\widetilde{X}_t\middle|\,\widetilde{\mathcal{F}}_s\right) = \widetilde{X}_s \quad \text{a.s.} \tag{20.5.27}$$

which shows that $\widetilde{X}$ is a martingale with respect to the filtration $\left(\widetilde{\mathcal{F}}_t\right)_{t\geq 0}$.

The only thing that remains to prove is the càdlàg property.

Suppose that for some $\omega \in \Omega_0$ we have that $\widetilde{X}$ is not right continuous. Then this means that there exists a sequence (s_n) such that $s_n \downarrow t$ as $n \to \infty$ and

$$\left|\widetilde{X}_{s_n}(\omega) - \widetilde{X}_t\right|(\omega) > \varepsilon, \tag{20.5.28}$$

for some $\varepsilon > 0$. By the definition of $\widetilde{X}$ for $\omega \in \Omega_0$, there exists a sequence of rational numbers (s'_n) such that $X_{s'_n} \to \widetilde{X}_t$ and $s'_n > s_n$, $s'_n \downarrow t$ as $n \to \infty$ and

$$\left|\widetilde{X}_{s_n}(\omega) - \widetilde{X}_{s'_n}(\omega)\right| \leq \frac{\varepsilon}{2} \;\Rightarrow\; \left|X_{s'_n} - \widetilde{X}_t\right| > \frac{\varepsilon}{2}, \tag{20.5.29}$$

which is a contradiction, since $X_{s'_n} \to \widetilde{X}_t$ as $n \to \infty$.

To prove that $\widetilde{X}$ has left limits, we consider $N(\widetilde{X}(\omega), I_M, [a,b]) \leq N(X(\omega), I_{M+1}, [a,b])$ for $\omega \in \Omega_0$,

$$\mathbb{E}\left(N(\widetilde{X}(\omega), I_M, [a,b])\right) \leq \mathbb{E}\left(N(X, I_M, [a,b])\right) < \infty \;\Rightarrow\; N(\widetilde{X}, I_M, [a,b]) < \infty \text{ a.s.} \tag{20.5.30}$$

Also, if $t \in \mathbb{Q}^+$, we have $\widetilde{X}_t(\omega) = \lim_{s\downarrow t, s\in\mathbb{Q}^+} X_s(\omega) = X_t(\omega)$.

$$\mathbb{P}\left(\sup_{t\in I}\left|\widetilde{X}_t\right| < \infty\right) = \mathbb{P}\left(\sup_{t\in I}|X_t| < \infty\right) = 1. \tag{20.5.31}$$

Thus, we can apply Lemma 20.5.5 to $\widetilde{X}$ and then we have $\forall t \in \mathbb{R}^{++}$, the left limit of $\widetilde{X}_t$, $\lim_{s\downarrow t, s\in\mathbb{Q}^+} \widetilde{X}_s$ exists. □

Example 20.5.7. Let ξ, η be independent random variables taking values $+1$ or -1 with equal probability. We now define

$$X_t = \begin{cases} 0 & t < 1 \\ \xi & t = 1 \\ \xi + \eta & t > 1. \end{cases} \tag{20.5.32}$$

We also define $\mathcal{F}_t$ to be the natural filtration, i.e. $\mathcal{F}_t = \sigma(X_s : s \leq t)$. Then clearly, X is a martingale relative to the

filtration $(\mathcal{F}_t)_{t\geq 0}$, but it is not right continuous at 1. Also, it is easy to see that $\mathcal{F}_1 = \sigma(\xi)$ but $\mathcal{F}_{1^+} = \sigma(\xi, \eta)$. We now define

$$\widetilde{X}_t = \begin{cases} 0 & t < 1 \\ \xi + \eta & t \geq 1. \end{cases} \tag{20.5.33}$$

It is easy to check that $X_t = \mathbb{E}\left(\widetilde{X}_t | \mathcal{F}_t\right)$ a.s. for all t and $\widetilde{X}$ is a martingale with respect to the filtration $(\mathcal{F}_{t^+})_{t\geq 0}$. It is obvious that $\widetilde{X}$ is càdlàg. Note though that $\widetilde{X}$ is not a version of X, since $X_1 \neq \widetilde{X}_1$.

From now on when we work with martingales in continuous time, we will always consider their cadlag version, provided that the filtration satisfies the usual conditions.

20.5.3 Martingale convergence theorem and inequalities

Now we will give the continuous time analogues of Doob's inequalities and the convergence theorems for martingales.

Theorem 20.5.8 (Doob's maximal inequality)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and $(X_t)_{t\geq 0}$ be a càdlàg non-negative submartingale and $X_t^* = \sup_{s\leq t} X_s$. Then, for all $\lambda \geq 0$ and $t \geq 0$,

$$\lambda \mathbb{P}\left(X_t^* \geq \lambda\right) \leq \mathbb{E} X_t. \tag{20.5.34}$$

Remark. Note that if X is a martingale, $|X|$ is submartingale by Jensen's inequality (Theorem 19.3.22). Thus, the above theorem is changed to

$$\lambda \mathbb{P}\left(\sup_{0\leq s\leq t} |X_s| \geq \lambda\right) \leq \mathbb{E}\left|X_t\right|. \tag{20.5.35}$$

when X is a martingale. Compare this theorem with Markov inequality (Theorem 19.3.20). The above conclusion is stronger as it is based on the fact that X is martingale.

Proof. We observe that

$$X_t^* = \sup_{s\leq t} |X_s| = \sup_{s\in\{t\}\cup([0,t]\cap\mathbb{Q})} |X_s| \tag{20.5.36}$$

by the càdlàg property (right continuity) as the supremum of irrationals can be approached by real sequence from right hand side. Therefore,

$$X_t^* = \sup_{\substack{J\subseteq\{t\}\cup([0,t]\cap\mathbb{Q}) \\ J \text{ is finite}}} \max_{s\in J} |X_s|. \tag{20.5.37}$$

Apply discrete Doob's maximal inequality (Theorem 20.2.16) to $(X_s)_{s\in J} = (X_{t_i})_{1\leq i\leq k}$, where $J = \{t_1, \ldots, t_k\}$. Hence

$$\lambda \mathbb{P}\left(\max_{s\in J} |X_s| \geq \lambda\right) \leq \mathbb{E}\left|X_{t_k}\right| \leq \mathbb{E}\left|X_t\right|. \tag{20.5.38}$$

whenever $\sup J \leq t$ because $|X|$ is a sub-martingale. Then we can pass the inequality to the supremum over J by monotone convergence theorem (Theorem 19.3.6)

$$\mathbb{1}_{\{\max_{s\in J}|X_s|\geq\lambda\}} \uparrow \mathbb{1}_{\{X_t^*\geq\lambda\}} \;\Rightarrow\; \mathbb{P}\left(\max_{s\in J} |X_s| \geq \lambda\right) \uparrow \mathbb{P}\left(X_t^* \geq \lambda\right) \tag{20.5.39}$$

which gives the required result. □

Theorem 20.5.9 (Doob's $\mathcal{L}^p$-inequality, continuous-time)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and $(X_t)_{t\geq 0}$ be a càdlàg non-negative submartingale. Setting $X_t^* = \sup_{s\leq t} |X_s|$, then for all $p > 1$ and t we have

$$\left\|X_t^*\right\|_p \leq \frac{p}{p-1} \left\|X_t\right\|_p. \tag{20.5.40}$$

Remark. If X is a martingale, $|X|$ is a non-negative martingale by Jensen's inequality (Theorem 19.3.22). Thus, this theorem also holds for martingale.

Proof. As we did in proof of Theorem 20.5.8, we can have finite subset J. Thus, by discrete Doob's $\mathcal{L}^p$-inequality (Theorem 20.2.17), we have

$$\left\|\max_{s\in J}|X_s|\right\|_p \leq \frac{p}{p-1}\left\|X_{t_k}\right\|_p \leq \frac{p}{p-1}\left\|X_t\right\|_p. \tag{20.5.41}$$

The last inequality holds since $\|X\|$ is submartingale as $\mathbb{E}X_{t_k} \leq \mathbb{E}X_t$. Therefore, by monotone convergence theorem (Theorem 19.3.6)

$$\left(\max_{s\in J}|X_s|\right)^p \uparrow (X_t^*)^p \;\Rightarrow\; \mathbb{E}\left|\max_{s\in J}|X_s|\right|^p \uparrow \mathbb{E}\left|X_t^*\right|^p \;\Rightarrow\; \left\|\max_{s\in J}|X_s|\right\|_p = \left(\mathbb{E}\left|\max_{s\in J}|X_s|\right|^p\right)^{1/p} \uparrow \left(\mathbb{E}\left|X_t^*\right|^p\right)^{1/p} = \left\|X_t^*\right\|_p$$

Hence,

$$\left\|X_t^*\right\|_p \leq \frac{p}{p-1}\left\|X_t\right\|_p. \tag{20.5.42}$$

□

Corollary 20.5.10. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and $(X_t)_{t\geq 0}$ be a càdlàg martingale. For all $p > 1$ and t we have

$$\left\|\sup_{t\geq 0}|X_t|\right\|_p \leq \frac{p}{p-1}\left\|X_\infty\right\|_p. \tag{20.5.43}$$

Proof. By Theorem 20.5.9,

$$\left\|\sup_{s\leq t}|X_s|\right\|_p \leq \frac{p}{p-1}\left\|X_t\right\|_p. \tag{20.5.44}$$

Since $\sup_{s\leq t}|X_s| \uparrow \sup_{t\geq 0}|X_t|$ and $|X_t| \to |X_\infty|$ a.s. as $t \to \infty$, by monotone convergence theorem (Theorem 19.3.6) and dominated convergence theorem (Theorem 19.3.8), we have the required result. □

Theorem 20.5.11 (Kolmogorov's inequality)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space based on which X is a submartingale and and $X_t^* = \sup_{0\leq s\leq t} X_s$. Then for any constant $\lambda > 0$,

$$\mathbb{P}\left(X_t^* \geq \lambda\right) \leq \frac{\mathbb{E}X_t^+}{\lambda}. \tag{20.5.45}$$

Remark. (i) Notice the analogy with Markov's inequality. Of course, the conclusion is much stronger than Markov's inequality, as the probabilistic bound applies to an uncountable number of random variables.

(ii) Note that Doob's maximal inequality is a special case of Kolmogorov's inequality.

Proof. As we did in proof of Theorem 20.5.8, we can have finite subset J. Thus, by the proof in discrete Kolmogorov's inequality (Theorem 20.2.18), we have

$$\mathbb{P}\left(\max_{s\in J} X_s \geq \lambda\right) \leq \frac{\mathbb{E}X_{t_k}\mathbb{1}_B}{\lambda}, \qquad B = \left\{\max_{1\leq i\leq k} X_{t_i} \geq \lambda\right\} \tag{20.5.46}$$

and B is $\mathcal{F}_{t_k}$-measurable. Since X is submartingale, we have

$$\mathbb{E}\left(X_t|\mathcal{F}_t\right) \geq X_{t_k} \text{ a.s. } \Rightarrow\; \left(\mathbb{E}\left(X_t|\mathcal{F}_t\right) - X_{t_k}\right)\mathbb{1}_B \geq 0 \text{ a.s. } \Rightarrow\; \mathbb{E}\left(\left(\mathbb{E}\left(X_t|\mathcal{F}_t\right) - X_{t_k}\right)\mathbb{1}_B\right) \geq 0 \tag{20.5.47}$$

which implies that $\mathbb{E}\left(X_t\mathbb{1}_B\right) \geq \mathbb{E}\left(X_{t_k}\mathbb{1}_B\right)$. Thus,

$$\mathbb{P}\left(\max_{s\in J} X_s \geq \lambda\right) \leq \frac{\mathbb{E}X_{t_k}\mathbb{1}_B}{\lambda} \leq \frac{\mathbb{E}X_t\mathbb{1}_B}{\lambda} \leq \frac{\mathbb{E}X_t^+\mathbb{1}_B}{\lambda} \leq \frac{\mathbb{E}X_t^+}{\lambda}. \tag{20.5.48}$$

Therefore, by monotone convergence theorem (Theorem 19.3.6)

$$\mathbb{1}_{\{\max_{s\in J} X_s\}} \uparrow \mathbb{1}_{\{X_t^*\}} \;\Rightarrow\; \mathbb{P}\left(\max_{s\in J} X_s \geq \lambda\right) \uparrow \mathbb{P}\left(X_t^* \geq \lambda\right). \tag{20.5.49}$$

Hence,

$$\mathbb{P}\left(\sup_{s\in[0,t]} X_s \geq \lambda\right) \leq \frac{\mathbb{E}X_t^+}{\lambda}. \tag{20.5.50}$$

□

Corollary 20.5.12. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtered probability space. $(X_t)_{t\geq 0}$ is a square-integrable martingale whose unconditional mean is $m = \mathbb{E}X_0$. Then for any constant $\lambda > 0$,

$$\mathbb{P}\left(\sup_{s\leq t} |X_s - m| \geq \lambda\right) \leq \frac{\operatorname{Var}(X_t)}{\lambda^2}. \tag{20.5.51}$$

Remark. Notice the analogy with Chebyshev inequality (Theorem 19.3.21). Of course, the conclusion is much stronger than Chebyshev inequality.

Proof. Apply Kolmogorov's inequality (Theorem 20.5.11) to $(X_n - m)^2$, which is a submartingale by Jensen's inequality. □

20.5.4 Convergence in continuous time

Theorem 20.5.13 (martingale convergence theorem, continuous-time)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and $(X_t)_{t\geq 0}$ be a càdlàg martingale which is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ (Definition 19.3.5). Then $X_t \to X_\infty$ a.s. as $t \to \infty$, for some $X_\infty \in \mathcal{L}^1(\Omega, \mathcal{F}_\infty, \mathbb{P})$[26].

Proof. If $N(X, I_M, [a, b])$ stands for the number of up-crossings of the interval $[a, b]$ as defined in martingale regularization theorem, then from $(*)$ in the proof of the martingale regularization theorem, we get that

$$(b-a)\mathbb{E}\left(N(X, I_M, [a, b])\right) \leq \mathbb{E}\left((X_{a_n} - a)^-\right) \leq \mathbb{E}\left(|X_K| + a\right) \leq a + \sup_{t\geq 0} \mathbb{E}|X_t| < \infty, \tag{20.5.52}$$

since X is bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Hence, if we take the limit as $M \to \infty$ then we get that

$$N(X, \mathbb{Q}^+, [a, b]) < \infty \text{ a.s.} \tag{20.5.53}$$

Therefore, the set

$$\Omega_0 = \bigcap_{\substack{a<b \\ a,b\in\mathbb{Q}}} \left\{N(X, \mathbb{Q}^+, [a, b]) < \infty\right\} \tag{20.5.54}$$

has probability 1.

On Ω_0 it is easy to see that X_q converges for $\omega \in \Omega_0$ as $q \to \infty$ and $q \in \mathbb{Q}^+$. Indeed, as in the proof of Lemma 20.2.11, if X_q did not converge, then $\limsup X_q < \liminf X_q$, so take $a < b$ rationals between these two numbers gives that $N(X, \mathbb{Q}^+, [a, b]) = \infty$ and this would contradict the finite number of up-crossings of the interval $[a, b]$ for all a, b.

Thus $(X_q)_{q\in\mathbb{Q}^+}$ converges a.s. as $q \to \infty$, $q \in \mathbb{Q}^+$, to X_∞. That is, $\forall \varepsilon > 0$, there exists $q_0 \in \mathbb{Q}^+$ such that

$$|X_q - X_\infty| < \frac{\varepsilon}{2}, \quad \forall q \geq q_0. \tag{20.5.55}$$

By càdlàg property of X (right continuity), we get for any $t > q_0$, $t \in \mathbb{R}^{++}$, there exists a rational q such that $q > t$ and

$$|X_t - X_q| < \frac{\varepsilon}{2}. \tag{20.5.56}$$

Hence we conclude that for such $q \in \mathbb{Q}^+$,

$$|X_t - X_\infty| = |(X_t - X_q) + (X_q - X_\infty)| \leq |X_t - X_q| + |X_q - X_\infty| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \tag{20.5.57}$$

□

Theorem 20.5.14. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and X be a càdlàg martingale and $p > 1$, then the following statements are equivalent:

[26] some books give that X_∞ is finite a.s., but this situation is included in the statement that $X_\infty \in \mathcal{L}^1(\Omega, \mathcal{F}_\infty, \mathbb{P})$

(i) X is bounded in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ i.e., $\sup_{t\geq 0} \|X_t\|_p < \infty$.

(ii) X converges a.s. and in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ to a random variable X_∞.

(iii) X is closed in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, i.e., there exists a random variable $Z \in \mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$ such that for all t,

$$X_t = \mathbb{E}(Z|\mathcal{F}_t) \quad \text{a.s.} \tag{20.5.58}$$

Proof. Use the similar argument in Theorem 20.2.20. □

Theorem 20.5.15 (UI martingale convergence theorem, continuous-time)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and X be a càdlàg martingale. The following are equivalent:

(i) X is uniformly integrable.

(ii) X converges a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ to a random variable X_∞.

(iii) X is closed in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, i.e., there exists a random variable $Z \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ such that for all t,

$$X_t = \mathbb{E}(Z|\mathcal{F}_t) \quad \text{a.s.}. \tag{20.5.59}$$

Proof. Use the similar argument in Theorem 20.2.22. □

20.5.5 Optional stopping theorems

Theorem 20.5.16 (optional stopping theoerem, bouned stopping time, continuous-time)**.** Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and X be a càdlàg adapted integrable process. Then the following are equivalent:

(i) X is a martingale.

(ii) $X^T = (X_{T\wedge t})_{t\geq 0}$ is a (càdlàg) martingale for all stopping times T.

(iii) For all bounded stopping times S, T, $\mathbb{E}(X_T|\mathcal{F}_S) = X_{S\wedge T}$ a.s..

(iv) $\mathbb{E}(X_T) = \mathbb{E}(X_0)$ for all bounded stopping times T.

Remark. If X is a submartingle (supmartingale), then X^T is submartingle (supmartingale).

Note that we can extend (iii) and (iv) to the case that S, T are bounded stopping times a.s..

Proof. (i) $\Rightarrow$ (ii). From X^T is adaped and integrable (by Proposition 20.4.4.(ii),(iii)).

Let $T_n = 2^{-n}\lceil 2^n T\rceil$ and define $Y_{2^n k} = X_k$ where $k \in \{i2^{-n}, i \in \mathbb{Z}^+\}$. Thus, Y is a (discrete) martingale with respect to filtration $(\mathcal{G}_m)_{m\geq 0}$ ($\mathcal{G}_{2^n k} = \mathcal{F}_k$) where $k \in \{i2^{-n}, i \in \mathbb{Z}^+\}$.

$$\{2^n T_n \leq 2^n k\} = \{T_n \leq k\} = \{\lceil 2^n T\rceil \leq 2^n k\} = \left\{T \leq 2^{-n}\lfloor 2^n k\rfloor\right\} \in \mathcal{F}_k = \mathcal{G}_{2^n k} \tag{20.5.60}$$

Thus, $2^n T_n$ is a stopping time of martingale Y. Then apply Theorem 20.2.6, $Y^{2^n T_n}$ is a martingale. That is, for any $t \geq s$ and $t_n = 2^{-n}\lceil 2^n t\rceil$, $s_n = 2^{-n}\lceil 2^n s\rceil$, we have

$$\mathbb{E}\left(X^{T_n}_{t_n}\middle|\mathcal{F}_{s_n}\right) = \mathbb{E}\left(Y^{2^n T_n}_{2^n t_n}\middle|\mathcal{G}_{2^n s_n}\right) \overset{\text{a.s.}}{=} Y^{2^n T_n}_{2^n s_n} = X^{T_n}_{s_n}. \tag{20.5.61}$$

Equivalently, this is

$$E(X_{T_n\wedge t_n}\mathbb{1}_{A_n}) = \mathbb{E}(X_{T_n\wedge s_n}\mathbb{1}_{A_n}) \text{ for any } A_n \in \mathcal{F}_{s_n}. \tag{20.5.62}$$

Since X is càdlàg, we have $X_{T_n\wedge t_n} \to X_{T\wedge t}$ and $X_{T_n\wedge s_n} \to X_{T\wedge s}$ thus

$$X_{T_n\wedge t_n}\mathbb{1}_{A_n} \to X_{T\wedge t}\mathbb{1}_A, \quad X_{T_n\wedge s_n}\mathbb{1}_{A_n} \to X_{T\wedge s}\mathbb{1}_A \quad \text{for } A \in \mathcal{F}_s (= \mathcal{F}_{s^+} \text{since filtration is right-continuous}). \tag{20.5.63}$$

Since X^T is integrable, we apply dominated convergence theorem (Theorem 19.3.8),

$$\begin{cases} \mathbb{E}\left(X_{T_n\wedge t_n}\mathbb{1}_{A_n}\right)\to\mathbb{E}\left(X_{T\wedge t}\mathbb{1}_A\right) \\ \mathbb{E}\left(X_{s_n}\mathbb{1}_{A_n}\right)\to\mathbb{E}\left(X_{T\wedge s}\mathbb{1}_A\right) \end{cases} \Rightarrow\ \mathbb{E}\left(X_{T\wedge t}\mathbb{1}_A\right)=\mathbb{E}\left(X_{T\wedge s}\mathbb{1}_A\right)\ \Rightarrow\ \mathbb{E}\left(X_{T\wedge t}|\mathcal{F}_s\right)=X_{T\wedge s}\ \text{ a.s..} \tag{20.5.64}$$

Thus, X^T is a martingale. Also, by Proposition 20.4.4, X^T is càdlàg.

(ii) $\Rightarrow$ (iii). Wlog we let $S\le T\le K$. Then apply the similar trick as above and Theorem 20.2.7,

$$\mathbb{E}\left(X_{T_n}|\mathcal{F}_{S_n}\right)=X_{S_n}\ \text{ a.s. }\Rightarrow\ \mathbb{E}\left(X_{T_n}\mathbb{1}_{A_n}\right)=\mathbb{E}\left(X_{S_n}\mathbb{1}_{A_n}\right)\quad\text{for } A_n\in\mathcal{F}_{S_n}. \tag{20.5.65}$$

Then since X is càdlàg, $X_{T_n}\to X_T$ and $X_{S_n}\to X_S$. Since X_T, X_S are integrable (since T,S bounded), we apply dominated convergence theorem (Theorem 19.3.8), for $A\in\mathcal{F}_S$ (by the fact the filtration is right-continous again)

$$\begin{cases} \mathbb{E}\left(X_{T_n}\mathbb{1}_{A_n}\right)\to\mathbb{E}\left(X_T\mathbb{1}_A\right) \\ \mathbb{E}\left(X_{S_n}\mathbb{1}_{A_n}\right)\to\mathbb{E}\left(X_S\mathbb{1}_A\right) \end{cases} \Rightarrow\ \mathbb{E}\left(X_T\mathbb{1}_A\right)=\mathbb{E}\left(X_S\mathbb{1}_A\right)\ \Rightarrow\ \mathbb{E}\left(X_T|\mathcal{F}_s\right)=X_S\ \text{ a.s..} \tag{20.5.66}$$

(iii) $\Rightarrow$ (iv). Direct result from (iii) by letting $S=0$ and taking expectation on both sides.

(iv) $\Rightarrow$ (i). Let $s<t$ and fix $u>t$. Let $A\in\mathcal{F}_s$, and define a random time T by saying $T=t$ if A occurs, or $T=u$ otherwise. Similarly, define $S=s$ if A occurs and $S=u$ otherwise. Note that both S and T are stopping times, and are bounded. Thus by (iv).

$$\mathbb{E}(X_T)=\mathbb{E}(X_0)=\mathbb{E}(X_S).\qquad(*) \tag{20.5.67}$$

On the other hand,

$$\mathbb{E}(X_T)=\mathbb{E}(X_t\mathbb{1}_A)+\mathbb{E}(X_u\mathbb{1}_{A^c}),\quad \mathbb{E}(X_S)=\mathbb{E}(X_s\mathbb{1}_A)+\mathbb{E}(X_u\mathbb{1}_{A^c}). \tag{20.5.68}$$

Plugging this into $(*)$ and cancelling the terms $\mathbb{E}(X_u\mathbb{1}_{A^c})$, we find:

$$\mathbb{E}(X_t\mathbb{1}_A)=\mathbb{E}(X_s\mathbb{1}_A) \tag{20.5.69}$$

for all $s<t$ and all $A\in\mathcal{F}_s$. This means (by definition) that

$$\mathbb{E}(X_t|\mathcal{F}_s)=X_s,\quad\text{a.s.} \tag{20.5.70}$$

as required. Hence, since X is adapted and integrable, X is a martingale. □

Also, we have the following stronger version of optional stopping theorem.

Theorem 20.5.17 (optional stopping theoerem, UI martingale, continuous-time)**.** Let $(\Omega,\mathcal{F},(\mathcal{F}_t)_{t\ge0},\mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and X be a càdlàg UI martingale. Then for every stopping times $S\le T$, we have

$$\mathbb{E}\left(X_T|\mathcal{F}_S\right)=X_S\ \text{ a.s.} \tag{20.5.71}$$

where $X_T=X_T\mathbb{1}_{\{T<\infty\}}+X_\infty\mathbb{1}_{\{T=\infty\}}$.

Proof. Let $A\in\mathcal{F}_S$. We need to show that

$$\mathbb{E}\left(X_T\mathbb{1}_A\right)=\mathbb{E}\left(X_S\mathbb{1}_A\right). \tag{20.5.72}$$

by Definition of conditional expectation (Theorem 19.4.18).

Let $T_n=2^{-n}\lceil 2^nT\rceil$ and $S_n=2^{-n}\lceil 2^nS\rceil$. Then $T_n\downarrow T$ and $S_n\downarrow S$ as $n\to\infty$ and by the right continuity of X we get that

$$X_{S_n}\to X_S,\quad X_{T_n}\to X_T\quad\text{as } n\to\infty. \tag{20.5.73}$$

Also, for all t,

$$\{T_n\le t\}=\{\lceil 2^nT\rceil\le 2^nt\}=\{\lceil 2^nT\rceil\le\lfloor 2^nt\rfloor\}=\{2^nT\le\lfloor 2^nt\rfloor\}=\left\{T\le 2^{-n}\lfloor 2^nt\rfloor\right\}\in\mathcal{F}_{2^{-n}\lfloor 2^nt\rfloor}\subseteq\mathcal{F}_t \tag{20.5.74}$$

as T is a stopping time. Thus, T_n and S_n are stopping times. From the proof of discrete time optional stopping theorem (Theorem 20.2.25), we have that $X_{T_n}=\mathbb{E}\left(X_\infty|\mathcal{F}_{T_n}\right)$ a.s. since T_n is a stopping time.

Thus by UI martingale convergence theorem (Theorem 20.5.15) we see that $(X_{T_n})_{n\geq 0}$ is UI. Hence by UI martingale convergence theorem (Theorem 20.5.15) again, $(X_{T_n})_{n\geq 0}$ converges to X_T as $n \to \infty$ also in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$.

By the discrete time optional stopping theorem for UI martingales (Theorem 20.2.25) we have

$$\mathbb{E}\left(X_{T_n}|\mathcal{F}_{S_n}\right) = X_{S_n} \text{ a.s.} \qquad (*) \tag{20.5.75}$$

since S_n and T_n are stopping times. Since $A \in \mathcal{F}_S$ the definition of S_n implies that $A \in \mathcal{F}_{S_n}$. Hence from $(*)$ we obtain that

$$\mathbb{E}\left(X_{T_n}\mathbb{1}_A\right) = \mathbb{E}\left(X_{S_n}\mathbb{1}_A\right) \tag{20.5.76}$$

We have $X_{T_n}\mathbb{1}_A$ is dominated by $X_{T_n} \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ by using the $\mathcal{L}^1$ convergence of X_{T_n} to X_T. Note that even $T_n = \infty$, this still holds since $X_\infty \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ by using X is UI. Thus, we can apply dominated convergence theorem (Theorem 19.3.8),

$$X_{T_n}\mathbb{1}_A \to X_T\mathbb{1}_A \;\Rightarrow\; \mathbb{E}\left(X_{T_n}\mathbb{1}_A\right) \to \mathbb{E}\left(X_T\mathbb{1}_A\right). \tag{20.5.77}$$

Similarly, for X_{S_n} and X_S, we have $\mathbb{E}\left(X_{S_n}\mathbb{1}_A\right) \to \mathbb{E}\left(X_S\mathbb{1}_A\right)$ which implies that

$$\mathbb{E}\left(X_T\mathbb{1}_A\right) = \mathbb{E}\left(X_S\mathbb{1}_A\right). \tag{20.5.78}$$

□

20.5.6 Convergence of martingale sequence

Theorem 20.5.18. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be filtered probability space satisfying usual conditions and X^n be a sequence of càdlàg martingales, and X be a process such that for any $t \in \mathbb{R}^{++}$, $X_t^n \xrightarrow{\mathcal{L}^1} X_t$ as $n \to \infty$. Then X is a martingale and has a càdlàg version which is the u.c.p. limit of X^n.

Proof. $X_t^n \xrightarrow{\mathcal{L}^1} X_t$ means that $X_t^n, X_t \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathbb{E}\left|X_t^n - X_t\right| \to 0$. So to prove X is a martingale, we only need to show that for any $0 \leq s \leq t < \infty$, X_t is $\mathcal{F}_t$-measurable and

$$\mathbb{E}\left(X_t|\mathcal{F}_s\right) = X_s \text{ a.s..} \qquad (*) \tag{20.5.79}$$

We show that X_t is $\mathcal{F}_t$-measurable later. To prove (*), we need to show that for any $A \in \mathcal{F}_s$, $\mathbb{E}\left(X_t\mathbb{1}_A\right) = \mathbb{E}\left(X_s\mathbb{1}_A\right)$. Since X^n are martingales, then we have that $\mathbb{E}\left(X_t^n\mathbb{1}_A\right) = \mathbb{E}\left(X_s^n\mathbb{1}_A\right)$. We have

$$\left|\mathbb{E}\left(X_t^n\mathbb{1}_A\right) - \mathbb{E}\left(X_t\mathbb{1}_A\right)\right| = \left|\mathbb{E}\left((X_t^n - X_t)\mathbb{1}_A\right)\right| \leq \mathbb{E}\left(\left|X_t^n - X_t\right|\mathbb{1}_A\right) \leq \mathbb{E}\left|X_t^n - X_t\right| \to 0 \;\Rightarrow\; \mathbb{E}\left(X_t^n\mathbb{1}_A\right) \to \mathbb{E}\left(X_t\mathbb{1}_A\right). \tag{20.5.80}$$

Similarly, $\mathbb{E}\left(X_s^n\mathbb{1}_A\right) \to \mathbb{E}\left(X_s\mathbb{1}_A\right)$. Thus, $\mathbb{E}\left(X_t\mathbb{1}_A\right) = \mathbb{E}\left(X_s\mathbb{1}_A\right)$ and therefore we have $(*)$.

Furthermore, since for any m, n, $X^n - X^m$ is a martingale, then by Doob's maximal inequality (Theorem 20.5.8)

$$\mathbb{P}\left(\sup_{0\leq s\leq t}\left|X_s^n - X_s^m\right| \geq \varepsilon\right) \leq \frac{1}{\varepsilon}\mathbb{E}\left|X_t^n - X_t^m\right| \leq \frac{1}{\varepsilon}\left(\mathbb{E}\left|X_t^n - X_t\right| + \mathbb{E}\left|X_t^m - X_t\right|\right) \to 0 \tag{20.5.81}$$

as $m, n \to \infty$ for all $t, \varepsilon > 0$. Thus, X^n is a Cauchy sequence under ucp convergence. Since X^n are a càdlàg adapted processes, thus there is a càdlàg adapted limit (process) Y, $X^n \xrightarrow{ucp} Y$ by Completeness of càdlàg adapted process space (Theorem 20.4.27). Thus, we have for any $t \in \mathbb{R}^{++}$ and $\varepsilon > 0$

$$\mathbb{P}\left(\left|X_t^n - Y_t\right| > \varepsilon\right) \leq \mathbb{P}\left(\sup_{0\leq s\leq t}\left|X_s^n - Y_s\right| > \varepsilon\right) \to 0 \quad \text{as } n \to \infty \;\Rightarrow\; X_t^n \xrightarrow{p} Y_t. \tag{20.5.82}$$

Also, since $X_t^n \xrightarrow{\mathcal{L}^1} X_t$, we have $X_t^n \xrightarrow{p} X_t$ by Proposition 19.3.35. By the almost surely uniqueness of the limit of convergence in probability (Proposition 19.2.17), we have $X_t = Y_t$ a.s.. This means Y is a càdlàg version of X.

We know that Y_t is $\mathcal{F}_t$-measurable since Y is adapted. Therefore, we can have that X_t is $\mathcal{F}_t$-measurable and thus X is adapted since the filtered probability space satisfies usual conditions (as it contains null set). Thus, we can say X is a martingale. □

Corollary 20.5.19. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be filtered probability space satisfying usual conditions and X^n be a sequence of continuous martingales such that $t \in \mathbb{R}^{++}$, $X_t^n \xrightarrow{\mathcal{L}^1} X_t$ as $n \to \infty$ for all t and some process X. Then, X is a martingale and has a continuous version.

Proof. Use similar argument in Theorem 20.5.18 and apply Theorem 20.4.27 □

20.6 Local Martingales

We write $\mathcal{M}$ for the set of all càdlàg martingales. It is also the case that $\mathcal{M}$ is stable under stopping (see Theorem 20.5.16). This observation leads us to define a slightly more general class of processes, called local martingales.

20.6.1 Definitions

Definition 20.6.1. An adapted process X is a local martingale if there exists a sequence $(T_n)_{n\in\mathbb{N}}$ of stopping times with $T_n \uparrow \infty$ a.s. such that $(X_t^{T_n})_{t\geq 0}$ is a martingale for all $n \in \mathbb{N}$ with respect to the filtration $(\mathcal{F}_t)_{t\geq 0}$.

We say that the sequence $(T_n)_{n\in\mathbb{N}}$ reduces X.

Proposition 20.6.1. Let X be a local martingale. If the filtration $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions, there exists a càdlàg version of X, $\widetilde{X}$.

Proof. If X is a local martingale, there exists a sequence of stopping time $T_n \uparrow \infty$ a.s. such that X^{T_n} is a martingale. Then by martingale regularization theorem (Theorem 20.5.6), there exists a càdlàg verion of $\widetilde{X}^{T_n}$ which is also a martingale. Thus, we have for any t,

$$\mathbb{P}\left(X_t^{T_n}(\omega) = \widetilde{X}_t^{T_n}(\omega)\right) = 1 \;\Rightarrow\; X_t^{T_n} = \widetilde{X}_t^{T_n} \text{ a.s.} \tag{20.6.1}$$

Thus, since $T_n \uparrow \infty$ a.s., we have

$$\lim_{n\to\infty} X_t^{T_n} = \lim_{n\to\infty} \widetilde{X}_t^{T_n} \text{ a.s.} \;\Rightarrow\; X_t = \widetilde{X}_t \text{ a.s.} \qquad (*) \tag{20.6.2}$$

Since $\widetilde{X}^{T_n}$ is càdlàg, for any t

$$\lim_{s\downarrow t, s\in\mathbb{Q}^+} \widetilde{X}_s^{T_n} = \widetilde{X}_t^{T_n}, \qquad \lim_{s\downarrow t, s\in\mathbb{Q}^+} \widetilde{X}_s^{T_n} \text{ exists} \quad \text{a.s.} \tag{20.6.3}$$

Also, since $T_n \uparrow \infty$ a.s., we can find a sufficently large n such that $T_n > t$ a.s. with $\widetilde{X}_s^{T_n} = \widetilde{X}_s$ and $\widetilde{X}_t^{T_n} = \widetilde{X}_t$ a.s.. Then

$$\lim_{s\downarrow t, s\in\mathbb{Q}^+} \widetilde{X}_s = \widetilde{X}_t, \qquad \lim_{s\downarrow t, s\in\mathbb{Q}^+} \widetilde{X}_s \text{ exists} \quad \text{a.s.} \qquad (\dagger) \tag{20.6.4}$$

Thus, from $(*)$ and $(\dagger)$, $\widetilde{X}$ is a càdlàg version of X. □

Proposition 20.6.2. Let X be a càdlàg local martingale and T be a stopping time. Then X^T is also a càdlàg local martingale.

Remark. If X is (sample) continuous, then X^T is also (sample) continuous.

Proof. By definition of local martingale, there exists a sequence of stopping times $T_n \uparrow \infty$ a.s. such that X^{T_n} is a martingale. Since X is càdlàg, for any t, we can find $s \downarrow t, s \in \mathbb{Q}^+$ and thus $s \wedge T_n \downarrow t \wedge T_n$ such that

$$\lim_{s\downarrow t} X_s^{T_n} = \lim_{s\downarrow t} X_{s\wedge T_n} = \lim_{s\wedge T_n \downarrow t\wedge T_n} X_{s\wedge T_n} = X_{t\wedge T_n} = X_t^{T_n} \;\Rightarrow\; X^{T_n} \text{ is càdlàg.} \tag{20.6.5}$$

Then by optional stopping theorem (Theorem 20.5.16), $X^{T_n\wedge T}$ is a càdlàg martingale. Thus, we have X^T is a local martingale (by definition of local martingale).

Since $X^{T_n\wedge T}$ is càdlàg, for any t

$$\lim_{s\downarrow t, s\in\mathbb{Q}^+} X_s^{T_n\wedge T} = X_t^{T_n\wedge T}, \qquad \lim_{s\downarrow t, s\in\mathbb{Q}^+} X_s^{T_n\wedge T} \text{ exists} \quad \text{a.s.} \tag{20.6.6}$$

Also, since $T_n \uparrow \infty$ a.s., we can find a sufficently large n such that $T_n > t$ a.s. with $X_s^{T_n \wedge T} = X_s^T$ and $X_t^{T_n \wedge T} = X_t^T$ a.s.. Then

$$\lim_{s \downarrow t, s \in \mathbb{Q}^+} X_s^T = X_t^T, \qquad \lim_{s \downarrow t, s \in \mathbb{Q}^+} X_s^T \text{ exists} \quad \text{a.s..} \tag{20.6.7}$$

Thus, X^T is càdlàg. □

Proposition 20.6.3. Every càdlàg martingale is a càdlàg local martingale.

Remark. By martingale regularization theorem (Theorem 20.5.6), we only consider the càdlàg martingale X.

Proof. By Theorem 20.5.16, for any T we have X^T is also a càdlàg martingale. Then we can find a sequence of stopping times $T_n \uparrow \infty$ a.s. for which X^{T_n} is a càdlàg martingale. Thus, X is a càdlàg local martingale. □

Remark. (i) We write $\mathcal{M}_{loc}$ for the set of all càdlàg local martingales. In particular $\mathcal{M} \subseteq \mathcal{M}_{loc}$ since any sequence $(T_n)_{n \in \mathbb{N}}$ of stopping times reduces X by Theorem 20.5.16.(ii).

(ii) The converse is not true.

One may ask what happens in the case of discrete time. This issue is moot in the following sense:

Proposition 20.6.4. Let $(X_n)_{n \geq 0}$ be discrete integrable local martingale. It is also a martingale.

Remark. This means that the martingale and local martingale are equivalent in discrete time frame. This conclusion is first given by Meyer [12].P_{47}, though there is small difference in proof.

Proof. Since X is integrable, all the conditional expectation is well-defined. With Proposition 20.6.3, we only need to prove that local martingale implies martingales and it suffices to that for any $n \geq m$

$$\mathbb{E}\left(X_n \,|\mathcal{F}_m\right) = X_m \text{ a.s..} \tag{20.6.8}$$

For any set $A \in \mathcal{F}_m$, it is suffices to prove that

$$\mathbb{E}\left(X_n \mathbb{1}_A\right) = \mathbb{E}\left(X_m \mathbb{1}_A\right). \qquad (*) \tag{20.6.9}$$

Since X is a local martingale, we can find $T_k \uparrow \infty$ a.s. such that X^{T_k} is a martingale for all k. That is

$$\mathbb{E}\left(X_n^{T_k} \middle| \mathcal{F}_m\right) = X_m^{T_k} \text{ a.s..} \tag{20.6.10}$$

Thus, set $B = \{T_k > m\} \cap A$ (as B is $\mathcal{F}_m$-measurable), we have $\mathbb{E}\left(X_{m+1}^{T_k} \mathbb{1}_B\right) = \mathbb{E}\left(X_m^{T_k} \mathbb{1}_B\right)$ and this implies that

$$\mathbb{E}\left(X_{m+1} \mathbb{1}_A\right) = \mathbb{E}\left(X_{m+1}^{T_k} \mathbb{1}_{\{T_k > m\}} \mathbb{1}_A\right) = \mathbb{E}\left(X_m^{T_k} \mathbb{1}_{\{T_k > m\}} \mathbb{1}_A\right) = \mathbb{E}\left(X_m \mathbb{1}_A\right). \tag{20.6.11}$$

Thus, we have $(*)$ by induction. Note that we can not use this trick in continuous time frame as T_k has uncountably many values. □

Proposition 20.6.5. If $M, N \in \mathcal{M}_{c,loc}$, then $M + N, M - N \in \mathcal{M}_{c,loc}$.

Proof. Since $M, N \in \mathcal{M}_{c,loc}$, there exist two sequences of stopping times S_n and S_n such that $S_n \uparrow \infty$ a.s., $S_n' \uparrow \infty$ a.s. and

$$(M+N)^{S_n} \in \mathcal{M}_c, \quad (M-N)^{S_n'} \in \mathcal{M}_c. \tag{20.6.12}$$

Now define $T_n = S_n \wedge S_n'$, so we have T_n is also a sequence of stopping times and $T_n \uparrow \infty$ a.s. such that

$$(M+N)^{T_n} = \left((M+N)^{S_n}\right)^{S_n'} \in \mathcal{M}_c, \quad (M-N)^{T_n} = \left((M-N)^{S_n'}\right)^{S_n} \in \mathcal{M}_c. \tag{20.6.13}$$

since stopped martingale is still a martingale (Theorem 20.5.16). Thus, $M + N, M - N \in \mathcal{M}_{c,loc}$. □

20.6.2 The relationship between martingales and local martingales

We now give necessary and sufficient conditions for a local martingale to be a martingale.

Proposition 20.6.6. Let $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ be a filtration (not necessarily satisfying usual conditions) and X be a càdlàg process. The following statements are equivalent:

(i) X is a martingale.

(ii) X is a local martingale and for all $t \geq 0$ the set

$$\mathcal{X}_t = \{X_T : \forall T \text{ is a stopping time, } T \leq t\} \quad \text{is UI.} \tag{20.6.14}$$

Proof. By martingale regularization theorem (Theorem 20.5.6) and Proposition 20.6.1, we only consider the càdlàg case.

(i) $\Rightarrow$ (ii). By optional stopping theorem (Theorem 20.5.16.(iii)), if T is a bounded stopping time with $T \leq t$, then $X_T = \mathbb{E}(X_t|\mathcal{F}_T)$ a.s.. Thus by Corollary 19.4.31 X_t is uniformly integrable since

$$\sup_{T\leq t} \mathbb{E}\left(|X_T|\, \mathbb{1}_{|X_T|\geq\lambda}\right) = \sup_{T\leq t} \mathbb{E}\left(|\mathbb{E}(X_t|\mathcal{F}_T)|\, \mathbb{1}_{|\mathbb{E}(X_t|\mathcal{F}_T)|\geq\lambda}\right). \tag{20.6.15}$$

(ii) $\Rightarrow$ (i). Suppose $(T_n)_{n\geq 0}$ reduces X. Let T be any bounded stopping time, $T \leq t$, say. By optional stopping theorem (Theorem 20.5.16.(iv)) applied to the martingale X^{T_n},

$$\mathbb{E}(X_0) = \mathbb{E}(X_0^{T_n}) = \mathbb{E}(X_T^{T_n}) = \mathbb{E}(X_{T\wedge T_n}). \tag{20.6.16}$$

Since $\{X_{T\wedge T_n} : n \in \mathbb{N}\}$ is uniformly integrable by assumption, $X_{T\wedge T_n} \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$. Also, we have $X_{T\wedge T_n} \to X_T$ a.s. (as T is bounded and $T_n \uparrow \infty$ a.s.). So we can apply dominated convergence theorem (Theorem 19.3.8),

$$\mathbb{E}(X_{T\wedge T_n}) \to \mathbb{E}(X_T) \quad \text{as } n \to \infty. \tag{20.6.17}$$

Therefore, $\mathbb{E}(X_T) = \mathbb{E}(X_0)$. Then by optional stopping theorem (Theorem 20.5.16) again, X must be a martingale. □

An extremely useful consequence of the above is the following.

Corollary 20.6.7. Let X be a càdlàg local martingale, and assume that X is bounded. Then X is a martingale.

Proof. If X is bounded by constant M, i.e. $|X| \leq M$, we recall definition of UI (Theorem 19.3.29)

$$\sup_{T\leq t} \mathbb{E}\left(|X_T|\, \mathbb{1}_{\{|X_T|>K\}}\right) \leq \sup_{T\leq t} M\mathbb{E}\left(\mathbb{1}_{\{|X_T|\geq K\}}\right) = M \sup_{T\leq t} \mathbb{P}\left(|X_T| \geq K\right) \to 0 \ \text{ as } K \to \infty. \tag{20.6.18}$$

Thus, $\mathcal{X}_t = \{X_T : T \text{ is a stopping time, } T \leq t\}$ is UI. By Proposition 20.6.6, we have X is a martingale. □

Corollary 20.6.8. More generally, if X is a càdlàg local martingale such that for all $t \geq 0$, $|X_t| \leq Y$ for some $Y \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, then X is a martingale.

Proof. If $|X| \leq Y$ for some $Y \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, we have $\mathcal{X}_t = \{X_T : T \text{ is a stopping time, } T \leq t\}$ is UI by Proposition 19.3.31.

Then By Proposition 20.6.6, we have X is a martingale. □

Theorem 20.6.9. Let X be a càdlàg local martingale. If $(T_n)_{n\geq 0}$ reduce X and $X_t^{T_n} \xrightarrow{\mathcal{L}^1} X_t$ for any t, i.e., $X_t^{T_n}, X_t \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathbb{E}\left|X_t^{T_n} - X_t\right| \to 0$ as $n \to \infty$, then X is a ture martingale.

Proof. Since $X_t^{T_n}, X_t \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, $\mathbb{E}\left(X_t^{T_n}|\mathcal{F}_s\right), \mathbb{E}\left(X_t|\mathcal{F}_s\right)$ is well-defined. Thus, we only need to show that for all $t \leq s$,

$$\mathbb{E}\left(X_t|\mathcal{F}_s\right) = X_s \text{ a.s..} \tag{20.6.19}$$

Then since X^{T_n} is a martingale,

$$\begin{aligned}
0 &\leq \mathbb{E}\left|\mathbb{E}\left(X_t|\mathcal{F}_s\right) - X_s\right| = \mathbb{E}\left|\mathbb{E}\left(X_t|\mathcal{F}_s\right) - X_s - \mathbb{E}\left(X_t^{T_n}\middle|\mathcal{F}_s\right) + X_s^{T_n}\right| \\
&\leq \mathbb{E}\left|\mathbb{E}\left(X_t^{T_n} - X_t\middle|\mathcal{F}_s\right)\right| + \mathbb{E}\left|X_s^{T_n} - X_s\right| \leq \mathbb{E}\left(\mathbb{E}\left(\left|X_t^{T_n} - X_t\right|\middle|\mathcal{F}_s\right)\right) + \mathbb{E}\left|X_s^{T_n} - X_s\right| \\
&= \mathbb{E}\left|X_t^{T_n} - X_t\right| + \mathbb{E}\left|X_s^{T_n} - X_s\right| \to 0 \text{ as } n \to \infty
\end{aligned}$$

by conditional Jensen's inequality (Theorem 19.4.26), tower property (Proposition 19.4.28.(i)) and $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$-convergence. Thus, by Theorem 15.3.7,

$$\mathbb{E}\left|\mathbb{E}\left(X_t|\mathcal{F}_s\right) - X_s\right| = 0 \;\Rightarrow\; \mathbb{E}\left(X_t|\mathcal{F}_s\right) - X_s = 0 \text{ a.s.} \tag{20.6.20}$$

as required. □

Corollary 20.6.10. Let X be a càdlàg local martingale. If $(T_n)_{n\geq 0}$ reduce X and $\mathbb{E}\left(\sup_{n\geq 0}\left|X_t^{T_n}\right|\right) < \infty$ for every t, then X is a ture martingale.

Proof. Since $X_t^{T_n} \to X_t$ a.s., and $\mathbb{E}\left(\sup_{n\geq 0}\left|X_t^{T_n}\right|\right) < \infty$, we can find $Y \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ such that $\left|X_t^{T_n}\right| \leq Y$. Then by dominated convergence theorem (Theorem 19.3.8), X_t is integrable as well. Also, $X_t^{T_n} - X_t \to 0$ a.s., then by dominated convergence theorem (Theorem 19.3.8) again, we have

$$\mathbb{E}\left|X_t^{T_n} - X_t\right| \to 0. \tag{20.6.21}$$

Then we use Theorem 20.6.9[27]. □

Remark. The following to weaker conditions are not sufficient for a local martingale to be a martingale.

(i) $\sup_{s\in[0,t]} \mathbb{E}|M_s| < \infty$ for every t.

(ii) $\sup_{t\in[0,\infty)} \mathbb{E}\left(e^{|M_t|}\right) < \infty$.

Example 20.6.11. [28]

Theorem 20.6.12. A non-negative càdlàg local martingale X is a supermartingale.

Proof. Since X is local martingale, there exists $T_n \uparrow \infty$ a.s. such that X^{T_n} is a martingale. Thus, for any $t \geq s$,

$$\mathbb{E}\left(X_t^{T_n}\middle|\mathcal{F}_s\right) = X_s^{T_n} \text{ a.s..} \qquad (*) \tag{20.6.22}$$

We know that $\liminf_{n\to\infty} X_t^{T_n} = X_t$ a.s., $\liminf_{n\to\infty} X_s^{T_n} = X_s$ a.s.. Thus, for any $A \in \mathcal{F}_s$, we have

$$\mathbb{E}\left(\liminf_{n\to\infty} X_t^{T_n}\mathbb{1}_A\right) = \mathbb{E}\left(X_t\mathbb{1}_A\right) \quad \text{(by Theorem 15.3.7 as } \liminf_{n\to\infty} X_t^{T_n}\mathbb{1}_A = X_t\mathbb{1}_A \text{ a.s.)} \tag{20.6.23}$$

Thus, by Theorem 19.4.18,

$$\mathbb{E}\left(\liminf_{n\to\infty} X_t^{T_n}\middle|\mathcal{F}_s\right) = \mathbb{E}\left(X_t|\mathcal{F}_s\right) \text{ a.s..} \qquad (**) \tag{20.6.24}$$

Also, by Fatou's lemma for conditional expectations (Theorem 19.4.24, $X_t^{T_n} \geq 0$),

$$\mathbb{E}\left(\liminf_{n\to\infty} X_t^{T_n}\middle|\mathcal{F}_s\right) \leq \liminf_{n\to\infty} \mathbb{E}\left(X_t^{T_n}\middle|\mathcal{F}_s\right) \text{ a.s. } (\dagger) \tag{20.6.25}$$

Then substituting $(*)$ and $(**)$ into the equation $(\dagger)$,

$$\begin{aligned} \mathbb{E}\left(\liminf_{n\to\infty} X_t^{T_n}\middle|\mathcal{F}_s\right) &\leq \liminf_{n\to\infty} X_s^{T_n} \text{ a.s.} \\ \mathbb{E}\left(X_t|\,\mathcal{F}_s\right) &\leq X_s \text{ a.s.} \end{aligned}$$

which implies that X is a supermartingale (Definition 20.5.1). □

Remark. A martingale can be interpreted as the fortune of a player in a fair game. A local martingale which is not a true martingale, on the other hand, is the fortune of a player in a game which looks locally fair. unfortunately, this is only because there are going to be times of huge increases of X followed by an eventual ruin. Overall, as the above proposition shows, the expected fortune decreases. A local martingale is thus something akin to a bubble in the market.

[27] Alternative, we can prove it by Theorem 19.4.25 without using Theorem 20.6.9.
[28] see wiki local martingale

20.6.3 Local martingale properties

Proposition 20.6.13. Let X be a (sample) continuous local martingale ($X \in \mathcal{M}_{c,loc}$) starting from 0. Set

$$S_n = \inf\{t \geq 0 : |X_t| \geq n\}. \tag{20.6.26}$$

Then $(S_n)_{n\geq 0}$ reduces X.

Proof. Recall Proposition 20.4.6. So $A_n = (-n, n)^c$ is a closed set. Thus, S_n is a stopping time. (In particular,

$$\{S_n \leq t\} = \left\{\inf_{s\in\mathbb{Q}, s\leq t} d(X_s, A_n) = 0\right\} = \bigcap_{k\in\mathbb{N}} \left\{\bigcup_{s\in\mathbb{Q}, s\leq t} \left\{d(X_s, A_n) < \frac{1}{k}\right\}\right\} = \bigcap_{k\in\mathbb{N}} \left\{\bigcup_{s\in\mathbb{Q}, s\leq t} \underbrace{\left\{|X_s| > n - \frac{1}{k}\right\}}_{\in\mathcal{F}_s}\right\} \in \mathcal{F}_t, \tag{20.6.27}$$

since there are countably many intersections and unions. So S_n is a stopping time.)

For each $\omega \in \Omega$, $X_{S_n(\omega)}(\omega) = n$ (see Proposition 20.4.6). Then since X is (sample) continuous, for any $\omega \in \Omega' = \{X(\omega) \text{ is continuous}\}$ ($\mathbb{P}(\Omega') = 1$), by the intermediate value theorem (Theorem 10.3.6), we have there exists $t \in [0, S_n(\omega)]$ such that $|X_t(\omega)| = n - 1$. This implies that $S_{n-1}(\omega) \leq t \leq S_n(\omega)$. Thus, $S_n(\omega)$ is non-decreasing.

Also, If $\lim_{n\to\infty} S_n(\omega)$ is not infinite, then it must converge to finite $S(\omega)$. Thus, $S_n(\omega) \to S(\omega)$ and continuity of X implies that $X_{S_n(\omega)}(\omega) \to X_{S(\omega)}(\omega)$, then $\forall\varepsilon$, there exists $N \in \mathbb{N}$ such that $\forall n > m \geq N$, $\left|X_{S_n(\omega)}(\omega) - X_{S_m(\omega)}(\omega)\right| < \varepsilon$. However, we know that

$$\left|X_{S_n(\omega)}(\omega) - X_{S_m(\omega)}(\omega)\right| = |\pm n \pm m| \geq 1 \quad \text{(contradiction.)} \tag{20.6.28}$$

Thus, we have $\lim_{n\to\infty} S_n(\omega) = \infty$ and hence $S_n \uparrow \infty$ a.s..

Let $(T_k)_{k\in\mathbb{N}}$ be a reducing sequence for M, i.e., $T_k \uparrow \infty$ a.s. and $X^{T_k} \in \mathcal{M}$. By optional stopping theorem (Theorem 20.5.16.(ii)), $X^{S_n\wedge T_k} \in \mathcal{M}$ and so $X^{S_n} \in \mathcal{M}_{loc}$ for each $n \in \mathbb{N}$ (by definition of local martingales (Definition 20.6.1)).

But X^{S_n} is bounded ($\left|X_t^{S_n}\right| \leq n$ for all t) and so it is also a martingale (by Corollary 20.6.7). □

Theorem 20.6.14. Suppose that the filtration $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions (which is necessary). Let X be a sample-continuous local martingale (see Definition 20.4.2) which is also of finite variation, and such that $X_0 = 0$ a.s. Then X is indistinguishable from 0.

Remark. It is essential to assume that X is continuous in this theorem.

This makes it clear that the theory of finite variation integrals we have developed is useless for integrating with respect to continuous martingales.

Proof. Let V denote the total variation process of X. Then by Lemma 20.4.9, V is sample-continuous adapted and non-decreasing a.s. with $V_0 = 0$ (as the filtration $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions).

Set $S_n = \inf\{t \geq 0 : V_t = n\}$. Then S_n is a stopping time for all $n \in \mathbb{N}$ (by the same argument in Proposition 20.6.13) since V is adapted. Also, $S_n \uparrow \infty$ as $n \to \infty$ a.s. (by the same argument in Proposition 20.6.13) since V_t is non-decreasing and finite for all $t \geq 0$ a.s..

Since X is sample-continuous (thus càdlàg) local martingale ($X \in \mathcal{M}_{loc}$), $X^{S_n} \in \mathcal{M}_{loc}$ by Proposition 20.6.2. Also, since $|X_t| \leq V_t$ for any t (by Lemma 10.3.11),

$$\left|X_t^{S_n}\right| \leq \left|V_t^{S_n}\right| \leq n, \tag{20.6.29}$$

so by Corollary 20.6.7, $X^{S_n} \in \mathcal{M}$.

Define $M := X^{S_n}$ with $|M| \leq n$. By Proposition 20.4.4, we also have M is sample-continuous. Thus, we have that M is a bounded sample-continuous martingale.

Fix $t > 0$ and set $t_k = kt/N$ for $0 \leq k \leq N$. By Lemma 20.5.3,

$$\mathbb{E}\left(M_t^2\right) = \mathbb{E}\left(\sum_{k=0}^{N-1}\left(M_{t_{k+1}}^2 - M_{t_k}^2\right)\right) = \mathbb{E}\left(\sum_{k=0}^{N-1}\left(M_{t_{k+1}} - M_{t_k}\right)^2\right) \leq \mathbb{E}\left(\underbrace{\sup_{k<N}\left|M_{t_{k+1}} - M_{t_k}\right|}_{\leq 2n} \underbrace{\sum_{0\leq k<N}\left|M_{t_{k+1}} - M_{t_k}\right|}_{\leq |V^{S_n}| \leq n}\right).$$

As M is bounded and sample-continuous, we have $\mathbb{P}\left(M(\omega) \text{ is bounded and continuous in } t, \forall t\right) = 1$. We know that if a function is continuous on a closed bounded interval ($[0,t]$) of the real line, it is uniformly continuous on that interval. It is a special case of Heine-Cantor theorem[29]. Then by proposition[30],

$$\sup_{0\le k<N} \left|M_{t_{k+1}}(\omega) - M_{t_k}(\omega)\right| \to 0 \quad \text{a.s.} \qquad \text{as } N \to \infty. \qquad (*) \tag{20.6.30}$$

Thus, by bounded convergence theorem (Theorem 19.3.10),

$$\mathbb{E}\left(\sup_{k<N} \left|M_{t_{k+1}} - M_{t_k}\right| \sum_{k=0}^{N-1} \left|M_{t_{k+1}} - M_{t_k}\right|\right) \to 0 \qquad \text{as } N \to \infty. \tag{20.6.31}$$

Hence, $\mathbb{E}(M_t^2) = 0$ for all $t \ge 0$. Therefore, $M_t = 0$ a.s. for all t. This means that M is a version of 0. Furthermore, since M is continuous, we have that M is indistinguishable from 0 by Proposition 20.4.12. That is, for $M^{(n)} := X^{S_n}$,

$$\mathbb{P}\left(M^{(n)}(\omega) = 0, \forall t\right) = 1. \tag{20.6.32}$$

Thus, since $S_n \uparrow \infty$ a.s.,

$$\begin{aligned}
\mathbb{P}\left(X_t(\omega) = 0, \forall t\right) &= \mathbb{P}\left(\bigcap_{n\in\mathbb{N}} X_t^{S_n}(\omega) = 0, \forall t\right) = 1 - \mathbb{P}\left(\bigcup_{n\in\mathbb{N}} X_t^{S_n}(\omega) \ne 0, \exists t\right) \\
&\ge 1 - \sum_{n\in\mathbb{N}} \mathbb{P}\left(X_t^{S_n}(\omega) \ne 0, \exists t\right) = 1 - \sum_{n\in\mathbb{N}} \mathbb{P}\left(M^{(n)}(\omega) \ne 0, \exists t\right) \\
&= 1 - \left(1 - \sum_{n\in\mathbb{N}} \left(1 - \mathbb{P}\left(M^{(n)}(\omega) = 0, \forall t\right)\right)\right) = 1 - \sum_{n\in\mathbb{N}} 0 = 1 - 0 = 1.
\end{aligned}$$

Here we use the fact that sum of countably many 0 is still 0. Thus, X is indistinguishable from 0. □

20.6.4 Semimartingales

Definition 20.6.2 (semimartingale)**.** A semimartingale X is a càdlàg adapted process having the decomposition

$$X = X_0 + M + A, \quad M_0 = A_0 = 0 \text{ a.s.} \tag{20.6.33}$$

for a local martingale M and a finite variation process A.

Remark. Since local martingale is adapted (by Definition 20.6.1), then the finite variation process (see Lemma 20.4.9) is also adapted.

[29] need link

[30] need uniformly continuous iff sup to 0

Chapter 21

Markov Chains

21.1 Discrete-time Markov Chains

21.1.1 Definition and basic facts

21.2 Continuous-time Markov Chains

21.3 Problems

21.3.1 Discrete-time Markov chains

Problem 21.3.1. Assume you have 50 noodles in a bowl and each noodle has two ends. You can put any two ends (of the same noodle or not) together with equal probability until there does not exist any available end. What's the expected number of circles in the bowl then?

Solution. Assume it is X_n for n noodles. Then

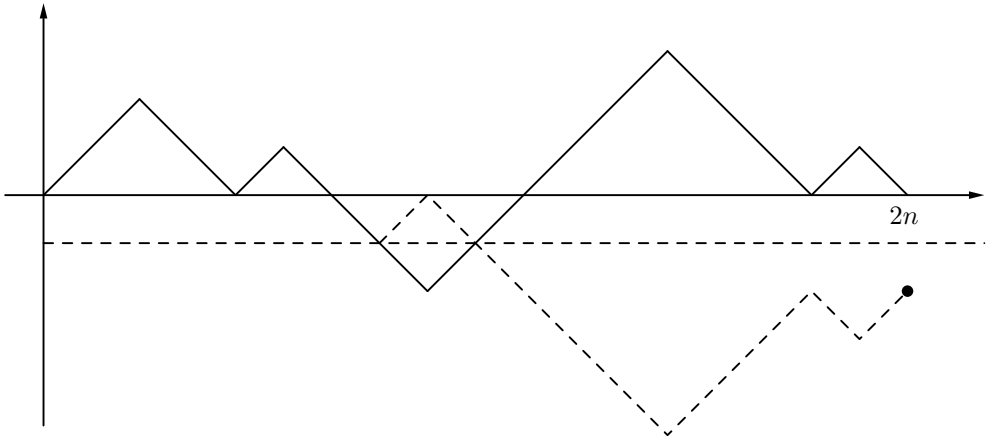
$$X_n = \frac{1}{2n-1}(1 + X_{n-1}) + \frac{2n-2}{2n-1}X_{n-1} = \frac{1}{2n-1} + X_{n-1} \;\Rightarrow\; X_n = \sum_{k=1}^{n} \frac{1}{2k-1}. \tag{21.3.1}$$

In this case, $n = 50$, $X_n = 2.93777$.

Problem 21.3.2 (ticket line, see [18].P_{117})**.** At a theater ticket office, $2n$ people are waiting to buy tickets, n of them have only \$5 bills and the other n people have only \$10 bills. The ticket seller has no change to start with. If each person buys one \$5 ticket, what is the probability that all people will be able to buy their tickets without having to change positions?

Solution. Assign +1 to the n people with \$5 bills and -1 to the n people with \$10 bills. Consider the process as a random walk. Let (a, b) represent that after a steps, the walk ends at b. So we start at $(0, 0)$ and reaches $(2n, 0)$ after $2n$ steps.

For these $2n$ steps, we need to choose n steps as +1, so there are $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ possible paths. We are interested in the paths that have the property $b \geq 0$, $\forall 0 < a < 2n$ steps. It is easier to calculate the number of complement paths that reach $b = -1$, $\exists 0 < a < 2n$.



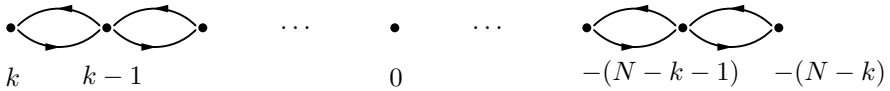
As shown in the figure, if we reflect the path across the line $y=-1$ after a path first reach -1., for every path that reaches $(2n,0)$ at step $2n$, we have one corresponding reflected path that reaches $(2n,-2)$ at step $(2n)$. For a path to reach $(2n,2)$, there are $(n-1)$ steps of $+1$ and $(n+1)$ steps of -1. So there $\binom{2n}{n-1}=\frac{(2n)!}{(n-1)!(n+1)!}$ such paths. The number of paths that have the property $b=-1$, $\exists 0<a<2n$, given that the path reaches $(2n,0)$ is also $\binom{2n}{n-1}$ and the number of paths that have the property $b\geq 0$, $\forall 0<a<2n$ is

$$\binom{2n}{n}-\binom{2n}{n-1}=\binom{2n}{n}-\frac{n}{n+1}\binom{2n}{n}=\frac{1}{n+1}\binom{2n}{n}. \tag{21.3.2}$$

Hence, the probability that all people will be able to buy their tickets without have to change positions is $1/(n+1)$.

Problem 21.3.3 (Cambridge TRIPOS 1/II/19H)**.** The village green is ringed by a fence with N fenceposts, labelled $0,1,\ldots,N-1$. The village idiot is given a pot of paint and a brush, and started at post 0 with instructions, 1 paint all the posts. He paints post 0, and then chooses one of the two nearest neighbours, 1 or $N-1$, with equal probability, moving to the chosen post and painting it. After painting a post, he chooses with equal probability one of the two nearest neighbours, moves there and paints it (regardless of whether it is already painted). Find the distribution of the last post unpainted. What is the expected time to paint all the fence?

Solution. If k is the last painted fence, there are 2 ways to reach it, from $k-1$ and $k+1$. We can find these 2 probabilities separately.



First, from $k-1$, the probability is

$$\mathbb{P}_0(\text{hit } -(N-k-1) \text{ before } k)\,\mathbb{P}_{k-1}(\text{hit } k \text{ before } -(N-k)) \tag{21.3.3}$$

We know

$$\mathbb{P}_i(\text{hit } -(N-k-1) \text{ before } k)=\frac{k-i}{N-1},\quad \mathbb{P}_i(\text{hit } k \text{ before } -(N-k))=\frac{i+N-k}{N} \tag{21.3.4}$$

Thus,

$$\mathbb{P}(\text{painter reach } k \text{ from } k-1)=\frac{k}{N-1}\frac{1}{N}=\frac{k}{N(N-1)}. \tag{21.3.5}$$

Similarly,

$$\mathbb{P}(\text{painter reach } k \text{ from } k+1)=\frac{N-k}{N-1}\frac{1}{N}=\frac{N-k}{N(N-1)}. \tag{21.3.6}$$

Hence

$$\begin{aligned}\mathbb{P}(k \text{ is the last painted fence}) &= \mathbb{P}(\text{painter reach } k \text{ from } k-1)+\mathbb{P}(\text{painter reach } k \text{ from } k+1)\\ &= \frac{k}{N(N-1)}+\frac{N-k}{N(N-1)}=\frac{1}{N-1}.\end{aligned}$$

We define h_i the probability that the painter hits $-(N-k-1)$ before k from i and

$$\begin{aligned}\tilde{p}_{ij} &= \mathbb{P}(X_1=j|X_0=i,\text{hit } -(N-k-1) \text{ before } k)\\ &= \frac{\mathbb{P}(X_1=j,\text{hit } -(N-k-1) \text{ before } k|X_0=i)}{\mathbb{P}(\text{hit } -(N-k-1) \text{ before } k|X_0=i)}\\ &= \frac{\mathbb{P}(\text{hit } -(N-k-1) \text{ before } k|X_1=j,X_0=i)\mathbb{P}(X_1=j|X_0=i)}{h_i}\\ &= \frac{\mathbb{P}(\text{hit } -(N-k-1) \text{ before } k|X_1=j)\mathbb{P}(X_1=j|X_0=i)}{h_i}\\ &= \frac{h_j}{h_i}p_{ij}\end{aligned}$$

Then we calculate

$$\begin{cases}\tilde{p}_{i,i+1}=\frac{k-i-1}{k-i}p_{i,i+1}=\frac{k-i-1}{2(k-i)}\\ \\ \tilde{p}_{i,i-1}=\frac{k-i+1}{k-i}p_{i,i+1}=\frac{k-i+1}{2(k-i)}\end{cases} \tag{21.3.7}$$

The expected time starting at i, T_i is given by

$$\begin{cases} T_{k-1} = 1 + T_{k-2} \\ \vdots \\ T_i = 1 + \frac{k-i+1}{2(k-i)} T_{i-1} + \frac{k-i-1}{2(k-i)} T_{i+1} \\ \vdots \\ T_{-(N-k-2)} = 1 + \frac{N-3}{2(N-2)} T_{-(N-k-3)} \end{cases} \Rightarrow \begin{cases} 2T_{k-1} = 2 + 2T_{k-2} \\ \vdots \\ 2(k-i)T_i = 2(k-i) + (k-i+1)T_{i-1} + (k-i-1)T_{i+1} \\ \vdots \\ 2(N-2)T_{-(N-k-2)} = 2(N-2) + (N-3)T_{-(N-k-3)} \end{cases} \tag{21.3.8}$$

Let $U_i = (k-i)T_i$

$$\begin{cases} 2U_{k-1} = 2 + U_{k-2} \\ \vdots \\ 2U_i = 2(k-i) + U_{i-1} + U_{i+1} \\ \vdots \\ 2U_{-(N-k-2)} = 2(N-2) + U_{-(N-k-3)} \end{cases} \Rightarrow U_{k-1} + U_{-(N-k-2)} = 2\sum_{i=1}^{N-2} i = (N-1)(N-2) \tag{21.3.9}$$

Also, we have

$$\begin{cases} 2U_{k-1} = 2 + U_{k-2} \\ 3U_{k-2} = 10 + 2U_{k-3} \\ 4U_{k-3} = 28 + 3U_{k-4} \\ \vdots \\ (k-i+1)U_i = 2\sum_{j=1}^{k-i} j^2 + (k-i)U_{i-1} \\ \vdots \\ (N-3)U_{-(N-k-4)} = 2\sum_{j=1}^{N-4} j^2 + (N-4)U_{-(N-k-3)} \\ \\ (N-2)U_{-(N-k-3)} = 2\sum_{j=1}^{N-3} j^2 + (N-3)U_{-(N-k-2)} \end{cases} \tag{21.3.10}$$

Thus,

$$\Rightarrow \begin{cases} (N-2)U_{-(N-k-3)} = \frac{(N-3)(N-2)(2N-5)}{3} + (N-3)U_{-(N-k-2)} \\ 2U_{-(N-k-2)} = 2(N-2) + U_{-(N-k-3)} \end{cases} \Rightarrow \begin{cases} U_{-(N-k-2)} = \frac{(N-2)(2N-3)}{3} \\ U_{-(N-k-3)} = \frac{4(N-2)(N-3)}{3} \end{cases} \tag{21.3.11}$$

and $U_{k-1} = \frac{N(N-2)}{3}$. Thus, we have

$$U_i = \frac{k-i}{3}\left[(N-1)^2 - (k-i)^2\right] \Rightarrow T_i = \frac{1}{3}\left[(N-1)^2 - (k-i)^2\right] \Rightarrow T_0 = \frac{1}{3}\left[(N-1)^2 - k^2\right] \tag{21.3.12}$$

Similarly, expected time from $-(N-k-1)$ to k is

$$T'_{-(N-k-1)} = \frac{N^2-1}{3} \tag{21.3.13}$$

Thus, the painter approach k from $k-1$ with probability $\frac{k}{N}$ and expected time

$$\frac{1}{3}\left[(N-1)^2 - k^2\right] + \frac{1}{3}(N^2-1) = \frac{1}{3}\left(2N^2 - 2N - k^2\right) \tag{21.3.14}$$

Similarly, the painter approach k from $k+1$ with probability $\frac{N-k}{N}$ and expected time

$$\frac{1}{3}\left(2N^2 - 2N - (N-k)^2\right) \tag{21.3.15}$$

Thus, the expected time to reach the last fence k is

$$\begin{aligned} & \frac{1}{3N}\left(2kN^2-2kN-k^3+2(N-k)N^2-2(N-k)N-(N-k)^3\right) \\ = & \frac{1}{3N}\left(2N^3-2N^2-k^3-(N-k)^3\right)=\frac{1}{3}\left(2N^2-2N-(N^2-3kN+3k^2)\right) \\ = & \frac{1}{3}\left(N^2-2N+3kN-3k^2\right) \end{aligned} \tag{21.3.16}$$

Since the distribution is uniform, we have the total expected time

$$\frac{1}{3}\left(N^2-2N\right)+\frac{1}{N-1}\left(N\sum_{k=1}^{N-1}k-\sum_{k=1}^{N-1}k^2\right)=\frac{1}{3}\left(N^2-2N\right)+\frac{1}{2}N^2-\frac{1}{6}N(2N-1)=\frac{1}{2}N(N-1). \tag{21.3.17}$$

Alternative approach. Assume the village idiot have already painted k. To get a new fence painted, he need to take expected time k (think about gambler's ruin problem). Thus, the total expected time will be

$$\sum_{k=1}^{N-1}k=\frac{1}{2}N(N-1). \tag{21.3.18}$$

Problem 21.3.4. A box contains n balls of n different colors. Each time, you randomly select a pair of balls, repaint the first to match the second, and put the pair back into the box. What is the expected number of steps until all balls in the box are of the same color?

21.3.2 Continuous-time Markov chains

Problem 21.3.5. You want to sell the ticket of a game. A system generates a uniformly distributed random variable in [0,1] for each round. If the random variable of the current round is bigger than the one of the previous round, the game continues. Otherwise, the game is stopped and the payoff the random variable of previous round (which is maximal of all random variables). What's the ticket value of this game?

Solution. Approach 1. First we have that

$$\begin{aligned} \mathbb{P}\left(X_n\le x, X_1\le\cdots\le X_n, X_{n+1}\le X_n\right) &= \int_0^x\int_0^{x_n}\int_0^{x_n}\int_0^{x_{n-1}}\cdots\int_0^{x_3}\int_0^{x_2}dx_1dx_2\ldots dx_{n-2}dx_{n-1}dx_{n+1}dx_n \\ &= \int_0^x x_n\frac{x_n^{n-1}}{(n-1)!}dx_n=\int_0^x\frac{x_n^n dx_n}{(n-1)!}=\frac{nx^{n+1}}{(n+1)!}. \end{aligned}$$

Thus, taking differentiation, we have

$$f_{X_n\mathbb{1}_{X_1\le\cdots\le X_n,X_{n+1}\le X_n}}(x)=\frac{x^n}{(n-1)!}. \tag{21.3.19}$$

The expected value is that

$$\begin{aligned} \sum_{n=1}^{\infty}\mathbb{E}\left(X_n\mathbb{1}_{X_1\le\cdots\le X_n,X_{n+1}\le X_n}\right) &= \sum_{n=1}^{\infty}\int_0^1\frac{x^{n+1}}{(n-1)!}dx=\sum_{n=1}^{\infty}\frac{n(n+1)}{(n+2)!} \\ &= \sum_{n=1}^{\infty}\frac{(n+2)(n+1)-2(n+2)+2}{(n+2)!}=\sum_{n=1}^{\infty}\frac{1}{n!}-\frac{2}{(n+1)!}+\frac{2}{(n+2)!} \\ &= \sum_{n=1}^{\infty}(e-1)-2\left(e-1-1\right)+2\left(e-1-1-\frac{1}{2}\right)=e-2. \end{aligned}$$

Approach 2. Define the expect value $f(x)$ with current maximal value x, then

$$f(x)=x\int_0^x du+\int_x^1 f(u)du\ \Rightarrow\ f'(x)=2x-f(x) \tag{21.3.20}$$

with boundary condition $f(1) = 1$. Thus, the solution is

$$f(x) = Ae^{-x} + 2(x-1) \;\Rightarrow\; A = e \;\Rightarrow\; f(0) = e - 2. \tag{21.3.21}$$

Chapter 22

Brownian Motion, Poisson Process and Lévy Process

22.1 Brownian Motion

22.1.1 History and definition

Brownian motion earned its name after R. Brown, who observed around 1827 that tiny particles of pollen in water have an extremely erratic motion. It was observed by Physicists that this was due to an important number of random shocks undertaken by the particles from the (much smaller) water molecules in motion in the liquid. A. Einstein established in 1905 the first mathematical basis for Brownian motion, by showing that it must be an isotropic Gaussian process. The first rigorous mathematical construction of Brownian motion is due to N. Wiener in 1923, using Fourier theory. Lévy studied the sample path properties of Brownian motion, and Kakutani and Doob made the link with potential theory. Itô's calculus was developed in 1950.

In order to motivate the introduction of this object, we first begin by a "microscopical" depiction of Brownian motion. Suppose $(X_n)_{n\geq 0}$ is a sequence of $\mathbb{R}^d$ valued random variables with mean 0 and covariance matrix $\sigma^2 I_d$, which is the identity matrix in d dimensions, for some $\sigma^2 > 0$. Namely, if $X_1 = (X_1^1, \dots, X_1^d)$,

$$\mathbb{E}\left(X_1^i\right) = 0, \quad \mathbb{E}\left(X_1^i X_1^j\right) = \sigma^2 \delta_{ij}, \quad 1 \leq i, j \leq d. \tag{22.1.1}$$

We interpret X_n as the spatial displacement resulting from the shocks due to water molecules during the n-th time interval, and the fact that the covariance matrix is scalar stands for an isotropy assumption (no direction of space is privileged).

From this, we let $S_n = X_1 + \cdots + X_n$ and we embed this discrete-time process into continuous time by letting

$$B_t^{(n)} = \frac{1}{\sqrt{n}} S_{\lfloor nt \rfloor}, \quad t \geq 0. \tag{22.1.2}$$

Recall Definition 19.5.3, we have

Definition 22.1.1 (transition density of standard Brownian motion)**.** Let $|\cdot|$ be the Euclidean norm[1] on $\mathbb{R}^d$ and for $t > 0$ and $x \in \mathbb{R}^d$, define

$$p_t(x) = \frac{1}{(2\pi t)^{d/2}} \exp\left(-\frac{|x|^2}{2t}\right), \tag{22.1.3}$$

which is the density of the Gaussian distribution $\mathcal{N}(0, tI_d)$ with mean 0 and covariance matrix tI_d (see Definition 19.5.2). By convention, the Gaussian law $\mathcal{N}(m, 0)$ is the Dirac mass at m.

Proposition 22.1.1. Let $0 = t_1 < t_2 < \cdots < t_k$. Then the finite marginal distributions of $B^{(n)}$ with respect to times $t_1, \dots, t_k$ converge weakly as $n \to \infty$. More precisely, if f is a bounded continuous function, and letting $x_0 = 0$, $t_0 = 0$,

$$\mathbb{E}\left[f\left(B_{t_1}^{(n)}, \dots, B_{t_k}^{(n)}\right)\right] \to \int_{(\mathbb{R}^d)^k} f(x_1, \dots, x_k) \prod_{1 \leq i \leq k} p_{\sigma^2(t_i - t_{i-1})}(x_i - x_{i-1}) dx_i \quad \text{as } n \to \infty. \tag{22.1.4}$$

[1] need definition

Otherwise said, $(B^{(n)}_{t_1}, \dots, B^{(n)}_{t_k})$ converges in distribution to $(G_1, G_2, \dots, G_k)$, which is a random vector whose law is characterized by the fact that $(G_1, G_2 - G_1, \dots, G_k - G_{k-1}) = (N_1, \dots, N_k)$ are independent centered Gaussian random variables with respective covariance matrices $\sigma^2(t_i - t_{i-1})I_d$. $((B^{(n)}_{t_i} - B^{(n)}_{t_{i-1}}, 1 \le i \le k)$ converges in distribution to $(N_i)_{1 \le i \le k}$, where the N_i's are independent and $N_i \sim \mathcal{N}(0, (t_i - t_{i-1})I_d)$. In particular, the law of $B^{(n)}_t$, $\mathcal{L}(B^{(n)}_t) \to \mathcal{N}(0, tI_d)$.)

Remark. This suggests that $B^{(n)}$ should converge to a process B whose increments are independent and Gaussian with covariances dictated by the above formula. This will be set in a rigorous way later with Donsker's invariance theorem[2].

Proof. With the notations of the theorem, we first check that $\left(B^{(n)}_{t_1}, B^{(n)}_{t_2} - B^{(n)}_{t_1}, \dots, B^{(n)}_{t_k} - B^{(n)}_{t_{k-1}}\right)$ is a sequence of independent random variables. Indeed, one has for $1 \le i \le k$

$$B^{(n)}_{t_i} - B^{(n)}_{t_{i-1}} = \frac{1}{\sqrt{n}} \sum_{j=\lfloor nt_{i-1} \rfloor + 1}^{\lfloor nt_i \rfloor} X_j, \tag{22.1.5}$$

and the independence follows by the fact that $(X_j, j \ge 0)$ is an i.i.d. family. Even better, we have the identity in distribution for the i-th increment

$$B^{(n)}_{t_i} - B^{(n)}_{t_{i-1}} \overset{d}{=} \frac{\sqrt{\lfloor nt_i \rfloor - \lfloor nt_{i-1} \rfloor}}{\sqrt{n}} \frac{1}{\sqrt{\lfloor nt_i \rfloor - \lfloor nt_{i-1} \rfloor}} \sum_{j=1}^{\lfloor nt_i \rfloor - \lfloor nt_{i-1} \rfloor} X_j \tag{22.1.6}$$

and the central limit theorem (Theorem 19.9.10) shows that this converges in distribution to $G_j - G_{j-1}$ with a Gaussian law $\mathcal{N}(0, \sigma^2(t_i - t_{i-1})I_d)$.

Summing up our study, and introducing characteristic functions, we have shown that for every $\xi = (\xi_j)_{1 \le j \le k}$, since $B^{(n)}_{t_j} - B^{(n)}_{t_{j-1}}$ are independent,

$$\begin{aligned}
\mathbb{E}\left(\exp\left(i\sum_{j=1}^{k} \xi_j (B^{(n)}_{t_j} - B^{(n)}_{t_{j-1}})\right)\right) &= \prod_{j=1}^{k} \mathbb{E}\left(\exp\left(i\xi_j (B^{(n)}_{t_j} - B^{(n)}_{t_{j-1}})\right)\right) \quad \text{(by Theorem 19.5.4)} \\
&\to \prod_{j=1}^{k} \mathbb{E}\left(\exp(i\xi_j (G_j - G_{j-1}))\right) \quad \text{(by Theorem 19.6.14)} \\
&= \mathbb{E}\left(\exp\left(i\sum_{j=1}^{k} \xi_j (G_j - G_{j-1})\right)\right) \quad \text{(by Theorem 19.5.4).}
\end{aligned}$$

as we assume $G_j - G_{j-1}$ are independent. By Lévy's convergence theorem (Theorem 19.6.13) we deduce that increments of $B^{(n)}$ between times t_i converge to increments of the sequence G_i weakly. That is, by Corollary 19.6.9, for any bounded continuous function F,

$$\mathbb{E}\left(f(B_{t_1}, \dots, B_{t_k})\right) \to \int_{(\mathbb{R}^d)^k} f(x_1, \dots, x_k) \prod_{i=1}^{k} p_{\sigma^2(t_i - t_{i-1})}(x_i - x_{i-1}) dx_1 \dots dx_k \tag{22.1.7}$$

as $n \to \infty$. □

We now start to define and study Brownian motion.

Definition 22.1.2 (standard Brownian motion)**.** An $\mathbb{R}^d$-valued stochastic process $(B_t, t \ge 0)$ is called a standard Brownian motion if it is a (sample) continuous process (has continuous sample path a.s.), that satisfies the following conditions:

(i) $B_0 = 0$ a.s.,

(ii) for every $0 = t_0 \le t_1 \le t_2 \le \dots \le t_k$, the increments $(B_{t_1} - B_{t_0}, B_{t_2} - B_{t_1}, \dots, B_{t_k} - B_{t_{k-1}})$ are independent,

(iii) for every $t, s \ge 0$, the law of $B_{t+s} - B_t$ is Gaussian with mean 0 and covariance sI_d.

Remark. The term "standard" refers to the choice $B_0 = 0$ a.s..

Definition 22.1.3 (Brownian motion)**.** An $\mathbb{R}^d$-valued stochastic process $(B_t, t \ge 0)$ is called a Brownian motion if it is a (sample) continuous process (has continuous sample path a.s.), that satisfies the following conditions:

[2] need theorem

(i) for every $0 = t_0 \le t_1 \le t_2 \le \cdots \le t_k$, the increments $(B_{t_1} - B_{t_0}, B_{t_2} - B_{t_1}, \ldots, B_{t_k} - B_{t_{k-1}})$ are independent,

(ii) for every $t, s \ge 0$, the law of $B_{t+s} - B_t$ is Gaussian with mean 0 and covariance sI_d.

Example 22.1.2. Suppose that $(B_t)_{t\ge 0}$ is a standard Brownian motion and U is an independent random variable uniformly distributed on $[0,1]$. Then the process $(\widetilde{B}_t)_{t\ge 0}$ defined by

$$\widetilde{B}_t = \begin{cases} B_t & t \neq U \\ 0 & t = U \end{cases} \tag{22.1.8}$$

has the same finite dimensional marginal distribution as Brownian motion, but is discontinuous if $B(U) \neq 0$, which happens with probability one, and hence it is not a Brownian motion.

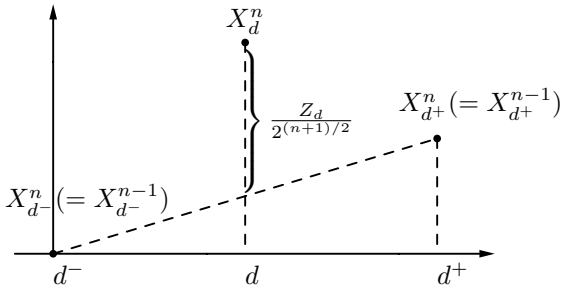
The characteristic properties (i), (ii), (iii) exactly amount to say that the finite dimensional marginals of a Brownian motion are given by the formula of Proposition 22.1.1. Therefore the law of the Brownian motion is uniquely determined by Proposition 20.4.10. We now show Wiener's theorem that Brownian motion exists!

Theorem 22.1.3 (Wiener theorem)**.** There exists a standard Brownian motion on some probability space.

Proof. We will first prove the theorem in dimension $d = 1$ and construct a process $(B_t)_{t\in[0,1]}$ satisfying the properties of a Brownian motion. This proof is essentially due to P. Lévy in 1948. The proof given by Ciesielski [6] is the ultimate refinement of Wiener's original idea of representing Brownian motion as a random Fourier series.

Let $\mathcal{D}_0 = \{0,1\}$, $\mathcal{D}_n = \{k2^{-n}, 0 \le k \le 2^n\}$ for $n \ge 1$, and $\mathcal{D} = \bigcup_{n\ge 0} \mathcal{D}_n$ be the set of dyadic rational numbers in $[0,1]$. On some probability space $(\Omega, \mathcal{F}, \mathbb{P})$, let $(Z_d)_{d\in D}$ be a collection of i.i.d. random variables all having a Gaussian distribution $\mathcal{N}(0,1)$ with mean 0 and variance 1.

It is a well-known and important fact that if the random variables $X_1, X_2, \ldots$ are linear combinations of independent centered Gaussian random variables, then $X_1, X_2, \ldots$ are independent if and only if they are pairwise uncorrelated, namely $\mathrm{Cov}(X_i, X_j) = \mathbb{E}(X_i X_j) = 0$ for every $i \neq j$[3].



We set $X_0^0 = 0$ and $X_1^0 = Z_1$. Inductively, given $(X_d^{n-1})_{d\in\mathcal{D}_{n-1}}$, we build $(X_d^n)_{d\in\mathcal{D}_n}$ in such a way that $(X_d^n)_{d\in\mathcal{D}_n}$ satisfies (i), (ii), (iii) in the definition of the Brownian motion (where the instants under consideration are taken in $\mathcal{D}_n$). To this end, take $d \in \mathcal{D}_n \backslash \mathcal{D}_{n-1}$, and let $d^- = d - 2^{-n}$ and $d^+ = d + 2^{-n}$ so that d^-, d^+ are consecutive dyadic numbers in $\mathcal{D}_{n-1}$. Then define:

$$X_d^n = \frac{X_{d^-}^{n-1} + X_{d^+}^{n-1}}{2} + \frac{Z_d}{2^{(n+1)/2}}. \tag{22.1.9}$$

and put $X_{d^-}^n = X_{d^-}^{n-1}$ and $X_{d^+}^n = X_{d^+}^{n-1}$. Note that with these definitions,

$$X_d^n - X_{d^-}^n = N_d + N'_d, \qquad X_{d^+}^n - X_d^n = N_d - N'_d, \tag{22.1.10}$$

where $N_d := (X_{d^+}^{n-1} - X_{d^-}^{n-1})/2$, $N'_d = Z_d/2^{(n+1)/2}$ are by the induction hypothesis two independent centered Gaussian random variables with variance 2^{-n-1}. From this, one deduces

$$\mathrm{Cov}(N_d + N'_d, N_d - N'_d) = \mathrm{Var}(N_d) - \mathrm{Var}(N'_d) = 0, \tag{22.1.11}$$

so that the increments $X_d^n - X_{d^-}^n$ and $X_{d^+}^n - X_d^n$ are independent with variance 2^{-n}, as should be.

Moreover, these increments are independent of the increments $X_{d'+2^{-n}}^n - X_{d'}^n$ for $d' \in \mathcal{D}_{n-1}$ with $d' \neq d^-$ and of $Z_{d'}$ with $d' \in \mathcal{D}_n \backslash \mathcal{D}_{n-1}$, $d' \neq d$ so they are independent of the increments $X_{d''+2^{-n}} - X_{d''}$ for $d'' \in \mathcal{D}_n$ with $d'' \notin \{d^-, d\}$. This allows the induction argument to proceed one step further.

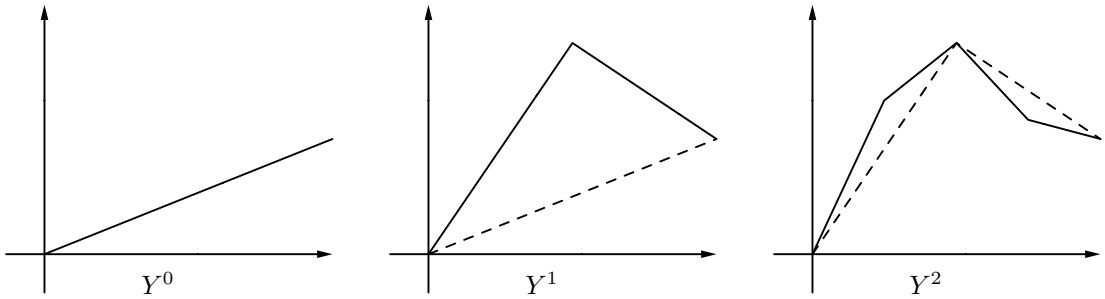
[3] need theorem

We have thus defined a process $(X_d^n)_{d\in\mathcal{D}_n}$ which satisfies properties (i), (ii) and (iii) for all dydadic times $t_1, t_2, \ldots, t_k \in \mathcal{D}_n$. Observe that if $\mathcal{D} \in \mathcal{D}_n$, $X_d^m = X_d^n$ for all $m \geq n$. Hence for all $d \in \mathcal{D}$,

$$X_d = \lim_{n\to\infty} X_d^n \tag{22.1.12}$$

is well-defined and the process $(X_d)_{d\in\mathcal{D}}$ obviously satisfies (i), (ii) and (iii).

To extend this to a process defined on the entire interval $[0,1]$, we proceed as follows. Define, for each $n \geq 0$, a process Y_t^n, $0 \leq t \leq 1$ to be the linear interpolation of the values $(X_d)_{d\in\mathcal{D}_n}$ the dyadic times at level n (with straight line connecting X_d for $d \in \mathcal{D}_n$).



Note that if $d \in \mathcal{D}$, say $d \in \mathcal{D}_m$ with $m \geq 0$, then for any $n \geq m$, $Y_d^n = Y_d^m = B_d$. Furthermore, define an event A_n by

$$A_n = \left\{ \sup_{0\leq t\leq 1} \left|Y_t^n - Y_t^{n-1}\right| > 2^{-n/4} \right\}. \tag{22.1.13}$$

We then have, let Z be a standard gaussian random variable.

$$\begin{aligned}
\mathbb{P}(A_n) &= \mathbb{P}\left(\bigcup_{j=0}^{2^{n-1}-1} \left\{ \sup_{t\in[(2j)2^{-n},(2j+2)2^{-n}]} \left|Y_t^n - Y_t^{n-1}\right| > 2^{-n/4} \right\} \right) \\
&\leq \sum_{j=0}^{2^{n-1}-1} \mathbb{P}\left(\sup_{t\in[(2j)2^{-n},(2j+2)2^{-n}]} \left|Y_t^n - Y_t^{n-1}\right| > 2^{-n/4} \right) \leq \sum_{j=0}^{2^{n-1}-1} \mathbb{P}\left(\frac{\left|Z_{(2j+1)2^{-n}}\right|}{2^{(n+1)/2}} > 2^{-n/4} \right) \\
&\leq \sum_{j=0}^{2^{n-1}-1} \mathbb{P}\left(|Z| > 2^{(n+2)/4} \right) \leq \sum_{j=0}^{2^{n-1}-1} \pi^{-1/2} 2^{-n/4-1} \exp\left(-2^{n/2}\right) \leq \pi^{-1/2} 2^{3n/4} \exp\left(-2^{n/2}\right)
\end{aligned}$$

by Proposition 19.8.16. We conclude that $\sum_{n=0}^{\infty} \mathbb{P}(A_n) < \infty$ and by Borel-Cantelli theorem (Theorem 19.1.24), the events A_n occur only finitely often. We deduce immediately that the sequence of functions Y^n is almost surely Cauchy in $C[0,1]$ equipped with the topology of uniform convergence, and hence Y^n converges toward a (sample) continuous limit function $(B_t)_{0\leq t\leq 1}$ uniformly, almost surely. If ω is in the null set, we simply define $B \equiv 0$.

Since Y_t^n is constantly equal to X_t for $t \in \mathcal{D}$ and for n large enough, it must be that $X_t = B_t$ for all $t \in \mathcal{D}$. Thus B is a continuous extension of X. (The extension of $(X_d, d \in D)$ could have been obtained by appealing to the existence of a continuous modification (version), whose existence is provided by Kolmogorov's criterion below[4].

For $s, t \in \mathcal{D}$, $s < t$, $\mathbb{E}\left(|X_s - X_t|^p\right) = |t-s|^{\frac{p}{2}} \mathbb{E}\left(N^p\right)$ for $p > 2$, where $N \sim \mathcal{N}(0,1)$, since $X_s - X_t \sim \mathcal{N}(0, t-s) \sim \sqrt{t-s}\mathcal{N}(0,1)$. But this latter is $C_p |t-s|^{1+(\frac{p}{2}-1)}$ for some $C_p > 0$. By the Kolmogorov Criterion (Theorem 20.4.13), there exists a.s. a continuous function $(B_t)_{t\in[0,1]}$ that extends $(X_d)_{d\in\mathcal{D}}$.)

We now deduce properties (i), (ii) and (iii) for B by continuity and the fact that Y^n satisfies these properties. Indeed, let $k \geq 1$ and let $0 < t_1 < t_2 \cdots < t_k < \infty$. Fix $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 0$. For every $1 \geq i \geq k$, fix a sequence $(d_i^{(n)})_t$ such that $\lim_{n\to\infty} d_i^{(n)} = t_i$, and assume (since $\mathcal{D}$ is dense in $[0,1]$) that $d_i^{(n)} \in \mathcal{D}$ and $t_{i-1} < d_i^{(n)} \leq t_i$. Thus, $X_{d_i^{(n)}} \to B_{t_i}$ a.s.. Then

[4] need theorem, see unsorted part

by dominated convergence theorem (Theorem 19.3.8),

$$\begin{aligned}
& \mathbb{E}\left(\exp\left(i\alpha_1 B_{t_1} + i\alpha_2(B_{t_2} - B_{t_1}) + \cdots + i\alpha_k(B_{t_k} - B_{t_{k-1}})\right)\right) \\
= & \lim_{n\to\infty} \mathbb{E}\left(\exp\left(i\alpha_1 X_{d_1^{(n)}} + i\alpha_2\left(X_{d_2^{(n)}} - X_{d_1^{(n)}}\right) + \cdots + i\alpha_k\left(X_{d_k^{(n)}} - X_{d_{k-1}^{(n)}}\right)\right)\right) \\
= & \lim_{n\to\infty} \exp\left(-\frac{\alpha_1^2}{2} d_1^{(n)} - \cdots - \frac{\alpha_k^2}{2}\left(d_k^{(n)} - d_{k-1}^{(n)}\right)\right) = \exp\left(-\frac{\alpha_1^2}{2} t_1 - \cdots - -\frac{\alpha_k^2}{2}(t_k - t_{k-1})\right).
\end{aligned}$$

Thus, we can say B is a standard Brownian motion on $[0,1]$ by Lévy convergence theorem (Theorem 19.6.13).

It is now easy to construct a Brownian motion indexed by $\mathbb{R}^+$. Simply take independent standard Brownian motions $(B_t^i)_{t\in[0,1],i\geq 0}$ as we just constructed, and let

$$B_t = \sum_{i=0}^{\lfloor t\rfloor - 1} B_1^i + B_{t-\lfloor t\rfloor}^{\lfloor t\rfloor}, \quad t \geq 0. \tag{22.1.14}$$

It is easy to check that this has the wanted properties[5].

Finally, it is straightforward to build a Brownian motion in $\mathbb{R}^d$, by taking d independent copies $B^1, \ldots, B^d$ of B and checking that $((B_t^1, \ldots, , B_t^d), t \geq 0)$ is a Brownian motion in $\mathbb{R}^d$[6]. □

The uniqueness of Brownian motion is in the distributional sense by Proposition 20.4.10.

Definition 22.1.4 (Wiener's measure)**.** Let $\Omega_W = C(\mathbb{R}^+, \mathbb{R}^d)$ (space of (sample) continuous functions) be the Wiener space, endowed with the product σ-algebra $\mathcal{W}$ (or the Borel σ-algebra associated with the compact-open topology (wrt time)).

Let $(B_t)_{t\geq 0}$ be a Brownian motion, and let $\mathbb{W}$ be the law of B. that is, for any $A \in \mathcal{W}$,

$$\mathbb{W}(A) = \mathbb{P}\left((B_t)_{t\geq 0} \in A\right). \tag{22.1.15}$$

Then $\mathbb{W}$ is called Wiener's measure.

Remark. We must check that this definition makes sense (there is a bijection between Brownian motion and Wiener measure), i.e., that $\mathbb{W}$ does not depend on the construction of B. To see this, note that the finite-dimensional distributions (i.e., the joint law of $(B_{t_1}, \ldots, B_{t_n})$ are entirely specified by the definition of a Brownian motion.

Since the σ-field $\mathcal{W}$ is generated by cylinder events of the form $\{B_{t_1} \in A_1, \ldots, B_{t_n} \in A_n\}$ for $A_i \in \mathcal{B}(\mathbb{R}^d)$, the right-hand side in the above display is indeed uniquely specified by Proposition 20.4.10.

Proposition 22.1.4. Let B be a Brownian motion on $(\Omega, \mathcal{F}, \mathbb{P})$. Then the canonical process Y is a Brownian motion under Wiener's measure.

Proof. Recalling $(*)$ in Definition 20.4.25, we let $(\phi(\omega))(t) = B_t(\omega)$ for $\phi : \Omega \to (\mathbb{R}^d)^{\mathbb{R}^+}$, $\omega \mapsto \phi(\omega)$. Thus, for $A_i \in \mathcal{B}(\mathbb{R}^d)$,

$$\begin{aligned}
\mathbb{W}\left(\phi(\omega) \in \Omega_W : Y_{t_1}(\phi(\omega)) \in A_1, \ldots, Y_{t_n}(\phi(\omega)) \in A_n\right) &= \mathbb{W}\left(\phi(\omega) \in \Omega_W : (\phi(\omega))(t_1) \in A_1, \ldots, (\phi(\omega))(t_n) \in A_n\right) \\
&= \mathbb{W}\left(\phi(\omega) \in \Omega_W : B_{t_1}(\omega) \in A_1, \ldots B_{t_n}(\omega) \in A_n\right) \\
&= \mathbb{P}\left(\omega \in \Omega : B_{t_1}(\omega) \in A_1, \ldots B_{t_n}(\omega) \in A_n\right) \\
&= \mathbb{P}\left(B_{t_1} \in A_1, \ldots B_{t_n} \in A_n\right).
\end{aligned}$$

Thus, two sides have the same distribution since they have the same finite dimensional marginal distribution (by Proposition 20.4.10).

Hence, we can see that the canonical process Y is actually a Brownian motion under Wiener's measure. □

Remark. This is the canonical construction of Brownian motion.

It is rarely the case in probability theory that we put some emphasis on the probability space on which a certain random process is constructed. (In all practical cases, we usually assume that such a random process is given to us). However the full advantage of specifying the probability space and measure will come to light when we deal with Girsanov's change of measure theorem.

[5] need details
[6] need details

Definition 22.1.5. For $x \in \mathbb{R}^d$ we also let $\mathbb{W}_x(dw)$ be the image measure of $\mathbb{W}$ by $(w_t)_{t\geq 0} \mapsto (x + w_t)_{t\geq 0}$.

A (continuous) process with law $\mathbb{W}_x(dw)$ is called a Brownian motion started at x.

We let $(\mathcal{F}_t^B)_{t\geq 0}$ be the natural filtration of $(B_t)_{t\geq 0}$, completed by zero-probability events.

Definition 22.1.6. We say that B is a Brownian motion (started at X) if $(B_t - X)_{t\geq 0}$ is a standard Brownian motion which is independent of X.

Remark. Otherwise said, it is the same as the definition as a standard Brownian motion, except that we do not require that $B_0 = 0$. If we want to express this on the Wiener space with the Wiener measure, we have for every measurable functional $F : \Omega \to \mathbb{R}^+$,

$$\mathbb{E}\left(F(B_t)_{t\geq 0}\right) = \int_{\mathbb{R}^d} \left(\int_\Omega F((x + w(t))_{t\geq 0}) \mathbb{W}(dw) \right) \mathbb{P}(X \in dx) = \int_{\mathbb{R}^d} \mathbb{W}_x(F) \mathbb{P}(X \in dx). \tag{22.1.16}$$

It will be handy to use the notation $W_X(F)$ for the random variable $\omega \mapsto W_{X(\omega)}(F)$, so that the right-hand side can be shortened as $\mathbb{E}(W_X(F))$.

22.1.2 Basic properties

Proposition 22.1.5. Let B be a standard Brownian motion in $\mathbb{R}^d$.

(i) rotational invariance. If $U \in O(d)$ is an orthogonal matrix, then $UB = (UB_t)_{t\geq 0}$ is again a Brownian motion. In particular, $-B$ is a Brownian motion.

(ii) scaling invariance. If $\lambda > 0$ then $(\lambda^{-1/2} B_{\lambda t})_{t\geq 0}$ is a standard Brownian motion.

(iii) time-inversion. $\widetilde{B}_t := (tB_{1/t})_{t\geq 0}$ is also a Brownian motion (at $t = 0$ the process is defined by its value 0 a.s., i.e., $\widetilde{B}_0 = 0$ a.s.).

Proof. (i) Since U is orthogonal matrix, we have $U^T U = UU^T = I$. Then[7] UB has covariance matrix $U^T V U$ where V is the covariance matrix of B, say $\sigma^2 I_d$. Thus the covariance matrix of UB is

$$U^T \sigma^2 I_d U = \sigma^2 U^T I_d U = \sigma^2 U^T U = \sigma^2 I_d \;\Rightarrow\; UB \text{ is a Brownian motion.} \tag{22.1.17}$$

(ii) Obviously, $B_0 = 0$ a.s.. Since

$$\frac{1}{\sqrt{\lambda}} B_{\lambda t} \sim \frac{1}{\sqrt{\lambda}} \mathcal{N}(0, \lambda t) \sim \mathcal{N}(0, t) \tag{22.1.18}$$

we have the increments of $\left(\lambda^{-1/2} B_{\lambda t}\right)_{t\geq 0}$ are independent Gaussian. Thus, $(\lambda^{-1/2} B_{\lambda t})_{t\geq 0}$ is a standard Brownian motion.

(iii) At any time $t > 0$, we have

$$tB_{1/t} \sim t\mathcal{N}\left(0, \frac{1}{t}\right) \sim \mathcal{N}\left(0 \cdot t, t^2 \frac{1}{t}\right) = \mathcal{N}(0, t) \sim B_t. \tag{22.1.19}$$

Thus, the only thing left to prove is that $B_0 = 0$ a.s.. Consider the event $\widetilde{A} = \left\{\omega : \widetilde{B}_t(\omega) \to 0 \text{ as } t \to 0\right\}$ is

$$\widetilde{A} = \bigcap_n \bigcup_m \bigcap_{q\in\mathbb{Q}\cap(0,1/m]} \left\{ \left|\widetilde{B}_q\right| \leq \frac{1}{n} \right\}. \tag{22.1.20}$$

since $\widetilde{B}$ is certainly continuous on $(0, \infty)$. But the processes $(B_t)_{t\geq 0}$ and $(\widetilde{B}_t)_{t\geq 0}$ have the same distribution (they are Gaussian processes with the same covariance), so

$$\mathbb{P}\left(\widetilde{A}\right) = \mathbb{P}(A) = 1 \tag{22.1.21}$$

where A is the event $\bigcap_n \bigcup_m \bigcap_{q\in\mathbb{Q}\cap(0,1/m]} \left\{|B_q| \leq \frac{1}{n}\right\}$ that $B \to 0$ at 0, a.s., which, by definition of B ($B_0 = 0$ a.s.).

□

Corollary 22.1.6. Let B be a standard Brownian motion, then $\lim_{t\to\infty} \frac{B_t}{t} = 0$ a.s.

[7] need theorem

Remark. Of course one can show the above result directly using the strong law of large numbers, i.e., $\lim_{n\to\infty} B_n/n = 0$. The one needs to show that B does not oscillate too much between n and $n+1$.[8]

Proof. Recalling Proposition 22.1.5.(iii), suppose that $B_t = t\widetilde{B}_{1/t}$ where $\widetilde{B}$ is another standard Brownian motion. Thus,

$$\lim_{t\to\infty} \frac{B_t}{t} = \lim_{t\to\infty} \widetilde{B}_{1/t} = \widetilde{B}_0 = 0 \text{ a.s..} \tag{22.1.22}$$

□

Lemma 22.1.7. Let B be a standard Brownian motion and $s, t \geq 0$. Then $\mathrm{Cov}(B_s, B_t) = s \wedge t$.

Proof. Wlog, we assume $t \geq s$, by independent Gaussian increment of Brownian motion, we have

$$\mathrm{Cov}\left(B_s, B_t\right) = \mathbb{E}\left(B_s B_t\right) - \mathbb{E}B_s \mathbb{E}B_t = \mathbb{E}\left(B_s(B_t - B_s + B_s)\right) - 0 = \mathbb{E}\left(B_s(B_t - B_s)\right) + \mathbb{E}\left(B\right)_s^2 = 0 + s = s. \tag{22.1.23}$$

Thus, we have $\mathrm{Cov}(B_s, B_t) = \min\{s, t\} = s \wedge t$. □

Recall Theorem 20.6.14, we have

Proposition 22.1.8. Brownian motion is not of finite variation.

22.1.3 Markov property

We now start to discuss ideas revolving around the Markov property of Brownian motion and its applications to path properties. We begin with the simple Markov property, which takes a particularly nice form in this context.

Theorem 22.1.9 (simple Markov property)**.** Let $(B_t, t \geq 0)$ be a Brownian motion, and let $s > 0$. Then

$$\left(\widetilde{B}_t := B_{t+s} - B_s\right)_{t\geq 0} \tag{22.1.24}$$

is a Brownian motion, independent of the σ-field $\mathcal{F}^B_{s^+} = \bigcap_{t>s} \mathcal{F}^B_t$.

Remark. In $\mathcal{F}^+_s$, we allow an additional infinitesimal glance into the future.

Proof. Since $\widetilde{B}$ is continuous and $\widetilde{B}_0 = 0$, to show that $\widetilde{B}$ is a Brownian motion it suffices to check that the increments have the correct distribution. However if $t \geq u$, $\widetilde{B}_t - \widetilde{B}_u = B_{s+t} - B_{s+u}$ so this follows directly from the fact that B itself is a Brownian motion. It remains to show that $\widetilde{B}$ is independent from $\mathcal{F}_{s^+}$.

We start by checking independence with respect to $\mathcal{F}_s$, for which we can assume $d = 1$. It suffices to check that the finite dimensional marginals are independent. i.e., if $s_1 \leq \ldots s_m \leq s$ and $t_1 \leq \ldots t_n$, we want to show that

$$(B_{s_1}, \ldots, B_{s_m}) \text{ and } (\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_n}) \tag{22.1.25}$$

are independent. However, the $m+n$-coordinate vector $(B_{s_1}, \ldots, B_{s_m}, \widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_n})$ is a Gaussian vector (since it is the image by a linear combination of Gaussian random variables), and it suffices to check that the covariance of two distinct terms is 0. Since each term has zero expectation, we have (by Lemma 22.1.7)

$$\mathrm{Cov}(\widetilde{B}_{t_i}, B_{s_j}) = \mathbb{E}(\widetilde{B}_{t_i} B_{s_j}) = \mathbb{E}(B_{s+t_i} B_{s_j}) - \mathbb{E}(B_s B_{s_j}) = s_j \wedge (s + t_i) - (s_j \wedge s) = s_j - s_j = 0 \tag{22.1.26}$$

which proves the independence with respect to $\mathcal{F}_s$.

To show that $\widetilde{B}$ is independent from $\mathcal{F}_{s^+}$, we wish to show that for every function $f : (\mathbb{R}^d)^k \to \mathbb{R}$ continuous and bounded and $A \in \mathcal{F}_{s^+}$,

$$\mathbb{E}\left(\mathbb{1}_A f(\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_k})\right) = \mathbb{P}(A)\mathbb{E}\left(f(\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_k})\right). \tag{22.1.27}$$

Now, for any $\varepsilon > 0$, $A \in \mathcal{F}_{s^+} \subseteq \mathcal{F}_{s+\varepsilon}$, thus, using the property just proved ($B_{t_i+s+\varepsilon} - B_{s+\varepsilon}$ are independent of $\mathcal{F}_{s+\varepsilon}$)

$$\mathbb{E}(\mathbb{1}_A f(B_{t_1+s+\varepsilon} - B_{s+\varepsilon}, \ldots, B_{t_k+s+\varepsilon} - B_{s+\varepsilon})) = \mathbb{P}(A)\mathbb{E}(f(B_{t_1+s+\varepsilon} - B_{s+\varepsilon}, \ldots, B_{t_k+s+\varepsilon} - B_{s+\varepsilon})) \tag{22.1.28}$$

[8] see example sheet, need details

Letting $\varepsilon \to 0$ in the above identity, since B is continuous and f is bounded and continuous, then by Proposition 19.5.6,

$$f(B_{t_1+s+\varepsilon} - B_{s+\varepsilon}, \ldots, B_{t_k+s+\varepsilon} - B_{s+\varepsilon}) \to f(B_{t_1+s} - B_s, \ldots, B_{t_k+s} - B_s) \tag{22.1.29}$$

we have (by bounded convergence theorem, Theorem 19.3.10),

$$\mathbb{E}\left(\mathbb{1}_A f(\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_k})\right) = \mathbb{P}(A)\mathbb{E}\left(f(\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_k})\right). \tag{22.1.30}$$

Hence, we can say that $\left\{\widetilde{B}_{t_1}, \ldots, \widetilde{B}_{t_k}\right\}$ is independent of the σ-field $\mathcal{F}^B_{s^+}$ by Proposition 19.5.6. Thus, $\widetilde{B}$ is independent of $\mathcal{F}^B_{s^+}$ by Proposition 20.4.10. □

Theorem 22.1.10 (Blumenthal's 0-1 law)**.** Let B be a standard Brownian motion. The σ-algebra $\mathcal{F}^B_{0^+} = \bigcap_{\varepsilon>0} \mathcal{F}^B_\varepsilon$ is trivial, for all $A \in \mathcal{F}^B_{0^+}$, $\mathbb{P}(A) \in \{0, 1\}$.

Proof. Let $A \in \mathcal{F}^B_{0^+}$, then A is independent of $\sigma(B_{t_i}, 1 \le i \le k)$, for all $t_1, \ldots, t_k > 0$ by simple Markov property (Theorem 22.1.9). Therefore A is independent of $\sigma(B_s, s \ge 0) = \mathcal{F}^B_\infty \supseteq \mathcal{F}^B_{0^+}$, so $\mathcal{F}^B_{0^+}$ is independent of itself. Thus for any $A \in \mathcal{F}^B_{0^+}$, $\mathbb{P}(A) = \mathbb{P}(A \cap A) = \mathbb{P}(A)^2$, so $\mathbb{P}(A) \in \{0, 1\}$. □

Proposition 22.1.11. Suppose that $(B_t)_{t\ge0}$ is a standard Brownian motion in 1 dimension. Definie

$$\tau = \inf\{t > 0 : B_t > 0\}, \qquad \sigma = \inf\{t > 0 : B_t = 0\}. \tag{22.1.31}$$

Then $\mathbb{P}(\tau = 0) = \mathbb{P}(\sigma = 0) = 1$.

Proof. For all n we have

$$\{\tau = 0\} = \bigcap_{k\ge n} \{\exists 0 < \varepsilon < 1/k : B_\varepsilon > 0\} \tag{22.1.32}$$

and thus $\{\tau = 0\} \in \mathcal{F}^B_{1/n}$ for all n and hence $\left\{\mathcal{F}^+_0\right\}$. Therefore, $\mathbb{P}(\tau = 0) \in \{0, 1\}$ by Blumental 0-1 law (Theorem 22.1.10). It remains to show that it has positive probability. Clearly, for all $t > 0$ we have

$$\mathbb{P}(\tau > t) \ge \mathbb{P}\left(\sup_{0\le s\le t} B_s \le 0\right) \le \mathbb{P}(B_t \le 0) \;\Rightarrow\; \mathbb{P}(\tau \le t) \ge \mathbb{P}(B_t > 0) = \frac{1}{2}. \tag{22.1.33}$$

Hence by letting $t \downarrow 0$ we get that $\mathbb{P}(\tau = 0) \ge 1/2$ and this finishes the proof.
In exactly the same way we get that (by symmetry)

$$\inf\{t > 0 : B_t < 0\} = 0 \text{ a.s.}. \tag{22.1.34}$$

Since B is a (sample) continuous function, by the intermediate value theorem (Theorem 10.3.6), we have that

$$\mathbb{P}(\sigma = 0) = 1. \tag{22.1.35}$$

□

Proposition 22.1.12. Let $(B_t)_{t\ge0}$ be standard Brownian motion in dimension $d = 1$. Let $S_t = \sup_{0\le s\le t} B_s$ and $I_t = \inf_{0\le s\le t} B_s$. Then

(i) a.s. for all $t > 0$, $S_t > 0$ and $I_t < 0$;

(ii) a.s. $S_\infty = \sup_{t\ge0} B_t = +\infty$ and $I_\infty = \inf_{t\ge0} B_t = -\infty$;

(iii) In dimensions $d \ge 2$, let C be an open cone with origin at 0 and non-empty interior. Let $H_C = \inf\{t > 0 : B_t \in C\}$. Then a.s. $H_C = 0$.

Proof. (i) Let t_k be a positive decreasing sequence with $t_k \to 0$ as $k \to \infty$. Let $A_k = \{B_{t_k} > 0\}$, so $\limsup_k A_k = \{B_{t_k} > 0 \text{ i.o.}\} \in \mathcal{F}^B_t$ for any $t > 0$. Therefore it is in $\mathcal{F}^B_{0^+}$. By Fatou's lemma (Lemma 15.1.14),

$$\mathbb{P}\left(\limsup_k A_k\right) \ge \limsup_k \mathbb{P}(A_k) = \limsup_k \mathbb{P}(B_{t_k} > 0) = \frac{1}{2}. \tag{22.1.36}$$

By Blumenthal's 0-1 law (Theorem 22.1.10), $\mathbb{P}(\limsup_k A_k) \in \{0,1\}$, so it must be one. But

$$\limsup_k A_k = \limsup_k \{B_{t_k} > 0\} = \bigcap_n \bigcup_{m \geq n} \{B_{t_m} > 0\} \subseteq \bigcap_n \{S_{t_n} > 0\} \tag{22.1.37}$$

Thus, $\mathbb{P}(B_t > 0) = 1$ for any $t > 0$. $(-B_t)_{t \geq 0}$ is a Brownian motion, so the result for It follows.

(ii) By scaling invariance of Brownian motion (Proposition 22.1.5.(ii)) we get that for any $\lambda > 0$,

$$S_\infty = \sup_{t \geq 0} B_t = \sup_{t \geq 0} B_{\lambda t} \stackrel{d}{=} \sup_{t \geq 0} \sqrt{\lambda} B_t = \sqrt{\lambda} S_\infty. \tag{22.1.38}$$

Thus for all $x > 0$ the probability $\mathbb{P}(S_\infty \geq x)$ is a constant c, and hence $\mathbb{P}(S_\infty \geq 0) = c$. But we have already showed that $\mathbb{P}(S_\infty \geq 0) = 1$ as $B_0 = 0$ a.s.. Therefore, for all $x > 0$ we have

$$\mathbb{P}(S_\infty \geq x) = 1 \;\Rightarrow\; \mathbb{P}(S_\infty = \infty) = 1. \tag{22.1.39}$$

The same argument for I_∞ gives the required result.

(iii) Since the cone C is invariant under multiplication by a positive scalar, by the scaling invariance property of Brownian motion we get that for any t, $\mathbb{P}(B_t \in C) = \mathbb{P}(B_1 \in C)$. Since C has non-empty interior, we can have that $\mathbb{P}(B_1 \in C) > 0$ and thus $\mathbb{P}(B_t \in C) > 0$ for any t.

Let t_k be a positive decreasing sequence with $t_k \to 0$ as $k \to \infty$. Let $A_k = \{B_{t_k} \in C\}$, so $\limsup_k A_k = \{B_{t_k} \in C \text{ i.o.}\} \in \mathcal{F}_t^B$ for any $t > 0$. Therefore it is in $\mathcal{F}_{0^+}^B$. By Fatou's lemma (Lemma 15.1.14),

$$\mathbb{P}\left(\limsup_k A_k\right) \geq \limsup_k \mathbb{P}(A_k) = \limsup_k \mathbb{P}(B_{t_k} \in C) > 0. \tag{22.1.40}$$

By Blumenthal's 0-1 law (Theorem 22.1.10), $\mathbb{P}(\limsup_k A_k) \in \{0,1\}$, so it must be one. Thus,

$$\mathbb{P}(B_{t_k} \in C \text{ i.o.}) = 1 \;\Rightarrow\; \mathbb{P}(H_C = 0) = 1. \tag{22.1.41}$$

□

We now want to prove an important analog of the simple Markov property, where deterministic times are replaced by stopping times. To begin with, we extend a little the definition of Brownian motion, by allowing it to start from a random location, and by working with filtrations that are (slightly) larger than the natural filtration of a standard Brownian motion.

Definition 22.1.7. Let $(\mathcal{F}_t)_{t \geq 0}$ be a filtration. We say that a Brownian motion B is an $(\mathcal{F}_t)$-Brownian motion if B is adapted to $(\mathcal{F}_t)_{t \geq 0}$, and if $B^{(t)} = (B_{t+s} - B_t)_{s \geq 0}$ is independent of $\mathcal{F}_t$ for every $t \geq 0$.

Remark. For instance, if $(\mathcal{F}_t)$ is the natural filtration of a 2-dimensional Brownian motion $(B_t^1, B_t^2)_{t \geq 0}$, then $(B_t^1)_{t \geq 0}$ is an $(\mathcal{F}_t)$-Brownian motion. If B' is a standard Brownian motion and X is a random variable independent of B', then $B = (X + B'_t)_{t \geq 0}$ is a Brownian motion (started at $B'_0 = X$), and is an $(\mathcal{F}_t^B) = (\sigma(X) \vee \mathcal{F}_t^{B'})$-Brownian motion. A Brownian motion is always an $\mathcal{F}_t^B$)-Brownian motion. If B is a standard Brownian motion, then the completed filtration $\mathcal{F}_t = \mathcal{F}_t^B \vee \mathcal{N}$ ($\mathcal{N}$ being the set of events of probability 0) can be shown to be right-continuous, i.e. $\mathcal{F}_{t^+} = \mathcal{F}_t$ for every $t \geq 0$, and B is an $(\mathcal{F}_t)$-Brownian motion.

Theorem 22.1.13 (Strong Markov property)**.** Let $(B_t)_{t \geq 0}$ be an $(\mathcal{F}_t)$-Brownian motion in $\mathbb{R}^d$ and T be an $(\mathcal{F}_t)$-stopping time. We let

$$B^{(T)} = \begin{cases} (B_{T+t} - B_T)_{t \geq 0} & T < \infty \\ 0 & \text{otherwise} \end{cases} \tag{22.1.42}$$

Conditionally on $\{T < \infty\}$, the process $B^{(T)}$ is a standard Brownian motion, which is independent of $\mathcal{F}_{T^+}$. Otherwise said, conditionally given $\mathcal{F}_T$ and $\{T < \infty\}$, the process $(B_{T+t})_{t \geq 0}$ is an $(\mathcal{F}_{T+t})$-Brownian motion started at B_T.

Proof. Suppose first that $T < \infty$ a.s. We will first prove for the stopping times $T_n = 2^{-n}\lceil 2^n T\rceil$ that discretely approximate T from above. We write $B_t^{(k)} = B_{t+k2^{-n}} - B_{k2^{-n}}$ which is a Brownian motion and B^* for the process defined by

$$B_t^* = B_{t+T_n} - B_{T_n}. \tag{22.1.43}$$

We will first show that B^* is a Brownian motion independent of $\mathcal{F}_{T_n^+}$. Let $A \in \mathcal{F}_{T_n^+}$ and $0 \le t_1 \le \cdots \le t_m$. Then for any bounded continuous function f,

$$\begin{aligned}
\mathbb{E}\left(\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) &= \mathbb{E}\left(\sum_{k=0}^{\infty}\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\mathbb{1}_{\{T_n=k2^{-n}\}}\right) = \mathbb{E}\left(\sum_{k=0}^{\infty}\mathbb{1}_A f\left(B_{t_1}^{(k)},\ldots,B_{t_m}^{(k)}\right)\mathbb{1}_{\{T_n=k2^{-n}\}}\right)\\
&= \sum_{k=0}^{\infty}\mathbb{E}\left(\mathbb{1}_{A\cap\{T_n=k2^{-n}\}} f\left(B_{t_1}^{(k)},\ldots,B_{t_m}^{(k)}\right)\right) \qquad \text{(by Fubini theorem (Theorem 15.3.33))}\\
&= \sum_{k=0}^{\infty}\mathbb{P}\left(A\cap\left\{T_n=k2^{-n}\right\}\right)\mathbb{E}\left(f\left(B_{t_1}^{(k)},\ldots,B_{t_m}^{(k)}\right)\right) \qquad \text{(by Proposition 19.5.6)}\\
&= \mathbb{P}(A)\,\mathbb{E}\left(f\left(B_{t_1}^{(k)},\ldots,B_{t_m}^{(k)}\right)\right).
\end{aligned}$$

By simple Markov property (Theorem 22.1.9), $B^{(k)}$ is Brownian motion. Thus, for standard Brownian motion B, $B^{(k)} \overset{d}{=} B$. Let A be the whole space Ω. Then we have

$$\mathbb{E}\left(f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) = \mathbb{E}\left(f\left(B_{t_1}^{(k)},\ldots,B_{t_m}^{(k)}\right)\right). \tag{22.1.44}$$

Thus, letting $f(x)$ be $\mathbb{1}_{x\in D}$, we have that B^* and B has the same finite dimensional marginal distributions. Thus, we have

$$\mathbb{E}\left(\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) = \mathbb{P}(A)\,\mathbb{E}\left(f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right). \tag{22.1.45}$$

Then by Proposition 19.5.6, $\left\{B_{t_1}^*,\ldots,B_{t_m}^*\right\}$ is independent of $\mathcal{F}_{T_n^+}$. (This can also be proved by checking $\mathbb{P}\left(\{B^*\in D\}\cap A\right) = \mathbb{P}(A)\mathbb{P}\left(B^*\in D\right)$ where $D\in\mathcal{W}$.)

By the continuity of Brownian motion we get that

$$B_{t+s+T} - B_{s+T} = \lim_{n\to\infty}\left(B_{s+t+T_n} - B_{s+T_n}\right). \tag{22.1.46}$$

The increments $(B_{t+s+T_n} - B_{s+T_n})$ are normally distributed with 0 mean variance equal to t. Thus for any $s \ge 0$ the increments $B_{t+s+T} - B_{s+T}$ are also normally distributed with 0 mean and variance t. As the process $(B_{t+T} - B_T)_{t\ge 0}$ is a.s. continuous, it is a Brownian motion. It only remains to show that it is independent of $\mathcal{F}_{T^+}$.

Let $A \in \mathcal{F}_{T^+}$ and $0 \le t_1 \le \cdots \le t_m$. Also, since $T_n > T$, it follows that $A \in \mathcal{F}_{T_n^+}$. Thus, for any bounded continuous function $f : (\mathbb{R}^d)^m \to \mathbb{R}$,

$$\mathbb{E}\left(\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) = \mathbb{P}(A)\,\mathbb{E}\left(f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right). \tag{22.1.47}$$

But we know that since f and B are continuous, as $n\to\infty$, $T_n \to T$,

$$f\left(B_{t_1}^{(T)},\ldots,B_{t_m}^{(T)}\right) = f\left(B_{t_1+T}-B_T,\ldots,B_{t_m+T}-B_T\right) = \lim_{n\to\infty} f\left(B_{t_1+T_n}-B_{T_n},\ldots,B_{t_m+T_n}-B_{T_n}\right) = \lim_{n\to\infty} f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)$$

and $\mathbb{1}_A f\left(B_{t_1}^{(T)},\ldots,B_{t_m}^{(T)}\right) = \lim_{n\to\infty}\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)$. Then by bounded convergence theorem (Theorem 19.3.10),

$$\mathbb{E}\left(\mathbb{1}_A f\left(B_{t_1}^{(T)},\ldots,B_{t_m}^{(T)}\right)\right) = \lim_{n\to\infty}\mathbb{E}\left(\mathbb{1}_A f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) = \mathbb{P}(A)\lim_{n\to\infty}\mathbb{E}\left(f\left(B_{t_1}^*,\ldots,B_{t_m}^*\right)\right) = \mathbb{P}(A)\,\mathbb{E}\left(f\left(B_{t_1}^{(T)},\ldots,B_{t_m}^{(T)}\right)\right).$$

Thus, we have that B is independent of $\mathcal{F}_{T^+}$ by Proposition 20.4.10.

Finally, if $\mathbb{P}(T=\infty) > 0$, check that the above is true when replacing A by $A\cap\{T<\infty\}$, and divide by $\mathbb{P}(T<\infty)$. □

Example 22.1.14. Let $\tau = \inf\{t \ge 0 : B_t = \max_{0\le s\le 1} B_s\}$. It is intuitively clear that τ is not a stopping time. To prove that, first show that $\tau < 1$ a.s. The increment $B_{t+\tau} - B_\tau$ is negative in a small neighbourhood of 0, which contradicts the strong Markov property.

An important example of application of the strong Markov property is the so-called reflection principle.

22.1.4 Reflection principle

Theorem 22.1.15 (reflection principle)**.** Let T be an a.s. finite stopping time and $(B_t)_{t\geq 0}$ a standard Brownian motion. Then the process $(\widetilde{B}_t)_{t\geq 0}$ defined by

$$\widetilde{B}_t = B_t \mathbb{1}_{\{t\leq T\}} + (2B_T - B_t)\mathbb{1}_{\{t>T\}} \tag{22.1.48}$$

is also a standard Brownian motion and we call it Brownian motion reflected at T.

Proof. By the strong Markov property (Theorem 22.1.13), the process $B^{(T)} = (B_{T+t} - B_T)_{t\geq 0}$ is a standard Brownian motion independent of $(B_t)_{0\leq t\leq T}$. Also the process $-B^{(T)} = (B_T - B_{t+T})_{t\geq 0}$ is a standard Brownian motion independent of $(B_t)_{0\leq t\leq T}$. Therefore, the pair $((B_t)_{0\leq t\leq T}, B^{(T)})$ has the same law as $((B_t)_{0\leq t\leq T}, -B^{(T)})$.

We now define the concatenation operation at time T between two continuous paths X and Y by

$$\Psi(X,Y)(t) = X_t \mathbb{1}_{\{t\leq T\}} + (X_T + Y_{t-T})\mathbb{1}_{\{t>T\}}. \tag{22.1.49}$$

Applying Ψ_T to B and $B^{(T)}$ gives us the Brownian motion B, while applying it to B and $-B^{(T)}$ gives us the process $\widetilde{B}$.

Let $\mathcal{A}$ be the product σ-algebra on $C[0,\infty)$, the space of continuous functions on $[0,\infty)$. It is easy to see that Ψ_T is a measurable mapping from $(C[0,\infty)\times C[0,\infty), \mathcal{A}\otimes\mathcal{A})$ to $(C[0,\infty),\mathcal{A})$ (by approximating T by discrete stopping times).

Hence, B and $\widetilde{B}$ have the same law. □

Theorem 22.1.16 (Reflection principle)**.** Let $(B_t)_{t\geq 0}$ be a standard Brownian motion and $a>0$ and $b\leq a$, then for every $t\geq 0$,

$$\mathbb{P}(S_t \geq a, B_t \leq b) = \mathbb{P}(B_t \geq 2a-b) \qquad \text{where } S_t = \sup_{0\leq s\leq t} B_s. \tag{22.1.50}$$

Proof. Let $T_a = \inf\{t\geq 0 : B_t \geq a\}$ be the entry time[9] of B_t in $[a,\infty)$ for $a>0$. Then T_a is an $(\mathcal{F}_t^B)$-stopping time for every a and $T_a<\infty$ a.s. since $S_\infty = \sup_{t\geq 0} B_t = \infty$ a.s. where $S_\infty = \lim_{t\to\infty} S_t$ (Note that $\{S_t\geq a\} = \{T_a \leq t\}$).

Now by continuity of B, $B_{T_a} = a$ for every a. We thus have $B_t - B_{T_a} = B^{(T_a)}_{t-T_a}$ and thus

$$\begin{aligned}\mathbb{P}(S_t\geq a, B_t\leq b) &= \mathbb{P}(T_a\leq t, B_t\leq b) = \mathbb{P}(T_a\leq t, B_t - B_{T_a}\leq b-a)\\ &= \mathbb{P}\left(T_a\leq t, B^{(T_a)}_{t-T_a}\leq b-a\right) = \mathbb{P}\left(T_a\leq t, -B^{(T_a)}_{t-T_a}\geq a-b\right).\end{aligned}$$

By the strong Markov property (Theorem 22.1.13) at time T_a, B^{T_a} is a Brownian motion independent of $\mathcal{F}_{T_a}$ and thus of T_a. In particular, we deduce that the joint law of $(T_a, B^{(T_a)})$ is identical to the joint law of $(T_a, -B^{(T_a)})$, by symmetry of Brownian motion. It follows that

$$\begin{aligned}\mathbb{P}(S_t\geq a, B_t\leq b) &= \mathbb{P}\left(T_a\leq t, -B^{(T_a)}_{t-T_a}\geq a-b\right) = \mathbb{P}\left(T_a\leq t, B^{(T_a)}_{t-T_a}\geq a-b\right)\\ &= \mathbb{P}\left(T_a\leq t, B_{T_a} + B^{(T_a)}_{t-T_a}\geq 2a-b\right) = \mathbb{P}(T_a\leq t, B_t\geq 2a-b) = \mathbb{P}(B_t\geq 2a-b)\end{aligned}$$

since $\{B_t\geq 2a-b\}$ implies that $\{S_t\geq a\} = \{T_a\leq t\}$. □

Remark. We can prove the above by Theorem 22.1.15.

Corollary 22.1.17. Let B be a standard Brownian motion and $S_t = \sup_{0\leq s\leq t} B_s$. We have the following identities in distribution. for all $t\geq 0$,

$$S_t \sim |B_t| \sim |\mathcal{N}(0,t)|. \tag{22.1.51}$$

Proof. We write, for all $t\geq 0$ and all $a\geq 0$,

$$\begin{aligned}\mathbb{P}(S_t\geq a) &= \mathbb{P}(S_t\geq a, B_t\leq a) + \mathbb{P}(S_t\geq a, B_t\geq a)\\ &= \mathbb{P}(B_t\geq 2a-a) + \mathbb{P}(B_t\geq a) = 2\mathbb{P}(B_t\geq a) = \mathbb{P}(|B_t|\geq a)\end{aligned}$$

since when $B_t\geq a$, $S_t\geq a$ automatically as well. □

Proposition 22.1.18. For every $x>0$, the random time $T_x := \inf\{t\geq 0 : B_t = x\}$ has same law as $(x/B_1)^2$.

Also, T_x has independent and stationary increments.

[9] need definition

Proof. Let $x > 0$. We know that $T_x < \infty$ a.s. because B is continuous and $\sup_{t\geq 0} B_t = \infty$ a.s. Then for $x > 0$, the reflection principle and Brownian scaling property (Proposition 22.1.5.(ii)) give that

$$\mathbb{P}(T_x \leq t) = \mathbb{P}(S_t \geq x) = \mathbb{P}(|B_t| \geq x) = \mathbb{P}\left(\sqrt{t}\,|B_1| \geq x\right) = \mathbb{P}\left(\left(\frac{x}{B_1}\right)^2 \leq t\right). \tag{22.1.52}$$

So T_x has same law as $(x/B_1)^2$.

By the strong Markov property at T_x, we have that $B^{(T_x)} = (B_{T_x+t} - B_{T_x})_{t\geq 0} = (B_{T_x+t} - x)_{t\geq 0}$ is a Brownian motion independent of $\mathcal{F}_{T_x}$. Therefore,

$$T_y - T_x := \inf\{t \geq 0 : B_{T_x+t} = y\} = \inf\{t \geq 0 : B_{T_x+t} - x = y - x\} = \inf\left\{t \geq 0 : B^{(T_x)} = y - x\right\} \tag{22.1.53}$$

has the same law as T_{y-x} and is independent of $\mathcal{F}_{T_x}$. Hence we can see that $(T_x)_{x\geq 0}$ has independent and stationary increments (see Definition 20.4.10). □

Proposition 22.1.19. Let $T_x = \inf\{t \geq 0 : B_t = x\}$ for $x > 0$. Then

$$f_{T_x}(t) = \frac{xe^{-\frac{x^2}{2t}}}{\sqrt{2\pi t^3}}. \tag{22.1.54}$$

Proof. By Corollary 22.1.17, we have

$$\mathbb{P}(T_x \leq t) = \mathbb{P}(S_t \geq x) = \mathbb{P}(|B_t| \geq x) = 2\int_x^\infty \frac{1}{\sqrt{2\pi t}} e^{-\frac{x^2}{2t}}\,dx = 2\int_{x/\sqrt{t}}^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\,dx. \tag{22.1.55}$$

Then we take the differentiation,

$$f_{T_x}(t) = -\frac{2}{\sqrt{2\pi}} e^{-\frac{x^2}{2t}} \left(-\frac{1}{2}\frac{x}{\sqrt{t^3}}\right) = \frac{xe^{-\frac{x^2}{2t}}}{\sqrt{2\pi t^3}}. \tag{22.1.56}$$

□

22.1.5 Martingales for Brownian Motion

Theorem 22.1.20. Let $(B_t)_{t\geq 0}$ be an $(\mathcal{F}_t)$-Brownian motion in $d \geq 1$ dimensions.

(i) If $d = 1$ and $B_0 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$, the process $(B_t)_{t\geq 0}$ is a $(\mathcal{F}_{t^+})$-martingale.

(ii) If $d \geq 1$ and $B_0 \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, the process $(|B_t|^2 - dt)_{t\geq 0}$ is a $(\mathcal{F}_{t^+})$-martingale.

(iii) Let $d \geq 1$ and $u = (u_1, \ldots, u_d) \in \mathbb{C}^d$[10]. Assume that $\mathbb{E}\,|\exp(\langle u, B_0\rangle)| < \infty$, the process defined by

$$M_t = \exp\left(\langle u, B_t\rangle - t\,|u|^2/2\right) \tag{22.1.57}$$

is also a $(\mathcal{F}_{t^+})$-martingale for every $u \in \mathbb{C}^d$, where $|u|^2$ is a notation for $\sum_{i=1}^d u_i\overline{u_i}$.

Remark. All the above martingales are also $(\mathcal{F}_t)$-martingales (as $B_t = B_{t^+}$ a.s. and $\mathcal{F}_t \subseteq \mathcal{F}_{t^+}$).

Notice that in (iii), we are dealing with $\mathbb{C}$-valued processes. Also, the hypothesis on B_0 in (iii) is automatically satisfied whenever $u = iv$ is purely imaginary, i.e., $v \in \mathbb{R}$.

Note that the alternative proof by using Itô formula is given later (see Theorem 23.2.2).

Proof. The adaptedness of these three process is obvious, Thus, we only check the integrability and conditional expectation.

(i) If $s \leq t$, then since B is continuous a.s.,

$$\mathbb{E}(B_t - B_{s^+}|\mathcal{F}_{s^+}) = \mathbb{E}(B_t - B_s|\mathcal{F}_{s^+}) = \mathbb{E}\left(B^{(s)}_{t-s}|\mathcal{F}_{s^+}\right) \tag{22.1.58}$$

[10] If $x, y \in \mathbb{C}^d$, we note $\langle x, y\rangle = \sum_{i=1}^d x_i\overline{y}_i$ their complex scalar product.

where $B_u^{(s)} = B_{u+s} - B_s$ has mean 0 and is independent of $\mathcal{F}_{s^+}$, by the simple Markov property (Theorem 22.1.9). Thus, $\mathbb{E}(B_t - B_s|\mathcal{F}_{s^+}) = \mathbb{E}\left(B_{t-s}^{(s)}|\mathcal{F}_{s^+}\right) = \mathbb{E}\left(B_{t-s}^{(s)}\right) = 0$ a.s. by Proposition 19.4.28.(v).

The integrability of the process is obvious by assumption on $B_0 \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ as

$$\mathbb{E}|B_t| \leq \mathbb{E}|B_t - B_0| + \mathbb{E}|B_0| \leq \|B_t - B_0\|_2 + \mathbb{E}|B_0| < \infty. \tag{22.1.59}$$

(ii) Since $B_0 \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ and $B_t - B_0$ is a normal random variable, we have for any $t \geq 0$

$$\mathbb{E}\left||B_t|^2 - dt\right| \leq \mathbb{E}|B_t - B_0 + B_0|^2 + dt = \|B_t - B_0 + B_0\|_2^2 + dt \leq (\|B_t - B_0\|_2 + \|B_0\|_2)^2 + dt < \infty. \tag{22.1.60}$$

by Minkowski inequality (Theorem 19.3.26). Thus, for $s \leq t$, as $B_{u+s} - B_s$ has mean 0 and is independent of $\mathcal{F}_{s^+}$ (by the simple Markov property (Theorem 22.1.9)), ($B_s = B_{s^+}$ a.s., $B_{s^+}, B_t - B_s \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$)

$$\begin{aligned}
\mathbb{E}\left(|B_t|^2 \middle| \mathcal{F}_{s^+}\right) &= \mathbb{E}\left(|B_t - B_s|^2 + 2B_{s^+} \cdot (B_t - B_s) + |B_{s^+}|^2 \middle| \mathcal{F}_{s^+}\right) \\
&= \mathbb{E}\left(|B_t - B_s|^2 \middle| \mathcal{F}_{s^+}\right) + 2\mathbb{E}(B_{s^+} \cdot (B_t - B_s)|\mathcal{F}_{s^+}) + \mathbb{E}\left(|B_{s^+}|^2 \middle| \mathcal{F}_{s^+}\right) \\
&\overset{\text{a.s.}}{=} \mathbb{E}\left(|B_t - B_s|^2 \middle| \mathcal{F}_{s^+}\right) + 2B_{s^+} \cdot \mathbb{E}(B_t - B_s|\mathcal{F}_{s^+}) + \mathbb{E}\left(|B_{s^+}|^2 \middle| \mathcal{F}_{s^+}\right) \quad \text{(Proposition 19.4.28.(iii))} \\
&\overset{\text{a.s.}}{=} \mathbb{E}|B_t - B_s|^2 + 2B_{s^+} \cdot \mathbb{E}(B_t - B_s) + |B_{s^+}|^2 \quad \text{(Proposition 19.4.28.(v) and Proposition 19.4.20.(ii))} \\
&\overset{\text{a.s.}}{=} d(t-s) + 2B_{s^+} \cdot 0 + |B_{s^+}|^2 = d(t-s) + |B_{s^+}|^2 = d(t-s) + |B_s|^2
\end{aligned}$$

since B is continuous a.s. Thus, the process $(|B_t|^2 - dt)_{t \geq 0}$ is a $(\mathcal{F}_{t^+})$-martingale.

(iii) To check integrability, note that by Proposition 19.8.14.(iv),

$$\mathbb{E}(\exp(\lambda B_t)) = \exp\left(t\lambda^2/2\right) \tag{22.1.61}$$

whenever B is a standard Brownian motion, and since $|e^z| = e^{\Re z}$, then we have

$$\begin{aligned}
\mathbb{E}|\exp\langle u, B_t\rangle| &= \mathbb{E}|\exp\langle u, (B_t - B_0 + B_0)\rangle| = \mathbb{E}|\exp\langle u, B_t - B_0\rangle \exp\langle u, B_0\rangle| \\
&= \mathbb{E}|\exp\langle u, B_t - B_0\rangle| \, \mathbb{E}|\exp\langle u, B_0\rangle| \quad \text{(Proposition 19.3.12)} \\
&= \exp\left(t\sum_{i=1}^d (\Re u_i)^2/2\right) \mathbb{E}|\exp\langle u, B_0\rangle| < \infty.
\end{aligned}$$

Then, for $s \leq t$,

$$\begin{aligned}
\mathbb{E}(M_t|\mathcal{F}_{s^+}) &= e^{-|u|^2 t/2}\mathbb{E}(\exp\langle u, B_t\rangle|\mathcal{F}_{s^+}) = e^{-|u|^2 t/2}\mathbb{E}(\exp\langle u, B_t - B_{s^+}\rangle \exp\langle u, B_{s^+}\rangle|\mathcal{F}_{s^+}) \\
&\overset{\text{a.s.}}{=} e^{-|u|^2 t/2} \exp\langle u, B_{s^+}\rangle \mathbb{E}(\exp\langle u, B_t - B_{s^+}\rangle|\mathcal{F}_{s^+}) \quad \text{(Proposition 19.4.28.(iv))} \\
&\overset{\text{a.s.}}{=} e^{-|u|^2 t/2} \exp\langle u, B_{s^+}\rangle \mathbb{E}(\exp\langle u, B_t - B_{s^+}\rangle) \quad \text{(Proposition 19.4.28.(v))} \\
&\overset{\text{a.s.}}{=} e^{-|u|^2 t/2} \exp\langle u, B_{s^+}\rangle \exp\left((t - s^+)\sum_{i=1}^d u_i^2/2\right) \\
&= e^{-|u|^2 t/2} e^{|u|^2(t-s^+)/2} \exp\langle u, B_{s^+}\rangle \overset{\text{a.s.}}{=} e^{-|u|^2 s^+/2} \exp\langle u, B_s\rangle = M_s.
\end{aligned}$$

Therefore, M is a $(\mathcal{F}_{t^+})$-martingale.

□

A classical application of these martingales is to show the following result, often referred to as the gambler's ruin[11] estimates.

Theorem 22.1.21. Let $(B_t)_{t \geq 0}$ be a standard Brownian motion and $T_x = \inf\{t \geq 0 : B_t = x\}$. Then for $x, y > 0$, one has

$$\mathbb{P}(T_{-y} < T_x) = \frac{x}{x+y}, \qquad \mathbb{E}(T_x \wedge T_{-y}) = xy. \tag{22.1.62}$$

[11] need definition

Proof. Let $T = T_{-y} \wedge T_x$ (by Proposition 20.4.6), which is a stopping time.

Since B is a martingale, the stopped martingale B^T is still a martingale (by Theorem 20.5.16.(ii)). Moreover, B^T is bounded (by $\max(x, y)$) so it is UI martingale. Then we may apply the optional stopping theorem (Theorem 20.5.17) to find that $\mathbb{E}(B_T) = \mathbb{E}(B_0) = 0$ a.s.. On the other hand,

$$\mathbb{E}(B_T) = -yp + x(1-p), \tag{22.1.63}$$

where $p = \mathbb{P}(T_{-y} < T_x)$ is the probability of interest to us. Thus $py = (1-p)x \ \Rightarrow \ p = \frac{x}{x+y}$.

For the second statement, we can observe that $B_t^2 - t$ is a martingale and thus $B_{t\wedge T}^2 - (t \wedge T)$ is a martingale (by Theorem 20.5.16.(ii)). Therefore,

$$\mathbb{E}(B_{t\wedge T}^2) = \mathbb{E}(t \wedge T). \tag{22.1.64}$$

We may let $t \to \infty$ since the left-hand side is bounded (we use bounded convergence theorem (Theorem 19.3.10)) and the right-hand side is monotone (we use monotone convergence theorem (Theorem 19.3.6)), and deduce that

$$\mathbb{E}(B_T^2) = \mathbb{E}(T). \tag{22.1.65}$$

Using the first statement,

$$\mathbb{E}(B_T^2) = \frac{x}{x+y}y^2 + \frac{y}{y+x}x^2 = xy \ \Rightarrow \ \mathbb{E}T = \mathbb{E}\left(T_x \wedge T_{-y}\right) = xy. \tag{22.1.66}$$

□

Theorem 22.1.22. Let B be a standard Brownian motion. The Laplace transform of $T_x = \inf\{t \geq 0 : B_t = x\}$ for $x \in \mathbb{R}$ is given by $\mathbb{E}(e^{-qT_x}) = e^{-|x|\sqrt{2q}}$. Moreover, for $x, y > 0$, the random variable $T = T_x \wedge T_{-y}$ has a Laplace transform given by

$$\mathbb{E}\left(e^{-qT}\right) = \frac{\sinh(\sqrt{2q}x) + \sinh(\sqrt{2q}y)}{\sinh(\sqrt{2q}(x+y))} \tag{22.1.67}$$

and when $y = x$, T is independent from the event $\{T_{-x} < T_x\}$.

Proof. Let $x \geq 0$ and $\lambda \geq 0$. We know the fact that $\left(\exp\left(\lambda B_t - \lambda^2 t/2\right)\right)_{t\geq 0}$ is a martingale by Theorem 22.1.20. Therefore,

$$\left(\exp\left(\lambda B_t^{T_x} - \frac{\lambda^2}{2}(t \wedge T_x)\right)\right)_{t\geq 0} \tag{22.1.68}$$

is also a martingale by Theorem 20.5.16.(ii). Since it is bounded, it is UI and thus by optional stopping theorem (Theorem 20.5.17), we have that

$$\mathbb{E}\left(\exp\left(\lambda x - \frac{\lambda^2}{2}T_x\right)\right) = \mathbb{E}\left(\exp\left(\lambda B_{T_x} - \frac{\lambda^2}{2}T_x\right)\right) = 1 \ \Rightarrow \ \exp\left(-\lambda x\right) = \mathbb{E}\left(\exp\left(-\lambda^2 T_x/2\right)\right). \tag{22.1.69}$$

Letting $\lambda = \sqrt{2q}$, we can have the required result. Similarly, for $x \geq 0$, we will let $\lambda \leq 0$ to guarantee the boundedness of the martingale (and then let $\lambda = -\sqrt{2q}$).

The second statement is a bit more involved. Let

$$M_t = e^{-\lambda^2 t/2}\sinh(\lambda(B_t + y)) \tag{22.1.70}$$

is also a martingale since it can be written as

$$\frac{1}{2}e^{-\lambda^2 t/2}e^{\lambda(B_t+y)} - \frac{1}{2}e^{-\lambda^2 t/2}e^{-\lambda(B_t+y)} \tag{22.1.71}$$

which is the sum of two martingales. Now, stopping at $T = T_{-y} \wedge T_x$, M^T is bounded and thus UI, so we can use the optional stopping theorem (Theorem 20.5.17) to obtain:

$$\sinh(\lambda y) = M_0 = M_T = \mathbb{E}(\sinh(\lambda(B_T + y))e^{-\lambda^2 T/2} = \mathbb{E}\left(\sinh(\lambda(x+y)e^{-\lambda^2 T/2}\mathbb{1}_{\{T_x > T_{-y}\}}\right). \tag{22.1.72}$$

Thus,

$$\mathbb{E}\left(e^{-\lambda^2 T/2}\mathbb{1}_{\{T_x>T_{-y}\}}\right)=\frac{\sinh(\lambda y)}{\sinh(\lambda(x+y))}\ \Rightarrow\ \mathbb{E}\left(e^{-\lambda^2 T/2}\mathbb{1}_{\{T_{-y}>T_x\}}\right)=\frac{\sinh(\lambda x)}{\sinh(\lambda(x+y))} \tag{22.1.73}$$

by symmetry. Adding up the two terms,

$$\mathbb{E}(e^{-\lambda^2 T/2})=\frac{\sinh(\lambda x)+\sinh(\lambda y)}{\sinh(\lambda(x+y))} \tag{22.1.74}$$

Again, letting $\lambda=\sqrt{2q}$, we can have the required result. When $x=y$,

$$\mathbb{E}\left(e^{-\lambda^2 T/2}\mathbb{1}_{\{T_{-x}>T_x\}}\right)=\frac{\sinh(\lambda x)}{\sinh(2\lambda x)}=\frac{1}{2}\frac{2\sinh(\lambda x)}{\sinh(2\lambda x)}=\frac{1}{2}\mathbb{E}(e^{-\lambda^2 T/2})=\mathbb{E}\left(e^{-\lambda^2 T/2}\right)\mathbb{P}(T_{-x}<T_x) \tag{22.1.75}$$

Hence, T is independent from the event $\{T_{-x}<T_x\}$ by Corollary 19.5.12. □

Theorem 22.1.23. Let $f:\mathbb{R}^+\times\mathbb{R}^d\to\mathbb{R},\ (t,x)\mapsto f(t,x)$ be $C^{1,2}$ (i.e., continuously differentiable in the first coordinate (time) and twice continuously differentiable in the second coordinate (space)) and $(B_t)_{t\geq 0}$ is a standard Brownian motion with respect to $(\mathcal{F}_t)_{t\geq 0}$. If there exists a constant K such that, for all $t\geq 0$, $x\in\mathbb{R}^d$,

$$|f(t,x)|+\left|\frac{\partial f(t,x)}{\partial t}\right|+\sum_{i=1}^d\left|\frac{\partial f(t,x)}{\partial x_i}\right|+\sum_{i=1}^d\sum_{i=1}^d\left|\frac{\partial f(t,x)}{\partial x_i}\right|\leq Ke^{K(t+|x|)}\qquad(*), \tag{22.1.76}$$

then

$$M_t:=f(t,B_t)-f(0,B_0)-\int_0^t\mathcal{L}f(s,B_s)ds \tag{22.1.77}$$

is an $(\mathcal{F}_{t^+})$-martingale, where (for the Laplaceian Δ)

$$\mathcal{L}f(t,B_t):=\frac{\partial f(t,x)}{\partial t}+\frac{1}{2}\Delta f(t,x)=\frac{\partial f(t,x)}{\partial t}+\frac{1}{2}\sum_{i=1}^d\frac{\partial^2 f(t,x)}{\partial x_i^2}. \tag{22.1.78}$$

Remark. We can extend this to the Brownian motions with start point x a.s., i.e. $\widetilde{B}_t=x+B_t$ where B_t is standard Brownian motions.

If we assume that f and its derivatives up to second order are bounded, they will satisfy $(*)$ automatically and the conclusion will hold for any Brownian motion (see Definition 22.1.3).

Example 22.1.24. (i) Let $f(t,x)=x$, then $M_t=B_t-B_0-\int_0^t 0\ ds=B_t$ which is Theorem 22.1.20.(i).

(ii) Let $f(t,x)=x^2$, then $M_t=B_t^2-B_0^2-\frac{1}{2}\int_0^t 2d\ ds=B_t^2-dt$ which is Theorem 22.1.20.(ii).

Proof. First we prove that $Ke^{K(t+|B_t|)}$ is integrable for any $t\geq 0$.

$$\mathbb{E}\left|Ke^{K(t+|B_t|)}\right|=Ke^{Kt}\mathbb{E}\left(e^{K|B_t|}\right)\leq 2Ke^{Kt}\mathbb{E}\left(e^{K(B_t-B_0}+KB_0\right)=2Ke^{2Kt}\mathbb{E}\left(e^{KB_0}\right)<\infty \tag{22.1.79}$$

as $B_0=0$ a.s.. Then for any $t\geq 0$, by $(*)$,

$$\mathbb{E}\,|M_t|=\mathbb{E}\left|f(t,B_t)-f(0,B_0)-\int_0^t\mathcal{L}f(s,B_s)ds\right|\leq\mathbb{E}\left|Ke^{K(t+|B_t|)}\right|+1+\mathbb{E}\left|\int_0^t Ke^{K(s+|B_s|)}ds\right| \tag{22.1.80}$$

Since $|B_t|$ has the same distribution as $S_t=\sup_{0\leq s\leq t}B_s$ (Corollary 22.1.17),

$$\begin{aligned}\mathbb{E}\,|M_t| &\leq \mathbb{E}\left|Ke^{K(t+|B_t|)}\right|+1+\mathbb{E}\left|\int_0^t Ke^{K(s+S_s)}ds\right|\leq\mathbb{E}\left|Ke^{K(t+|B_t|)}\right|+1+\mathbb{E}\left|\int_0^t Ke^{K(s+S_t)}ds\right|\\ &= \mathbb{E}\left|Ke^{K(t+|B_t|)}\right|+1+\mathbb{E}\left|e^{K|B_t|}\int_0^t Ke^{Ks}ds\right|=\mathbb{E}\left|Ke^{K(t+|B_t|)}\right|+1+\mathbb{E}\left|e^{K|B_t|}\left(e^{Kt}-1\right)\right| \qquad (\dagger)\\ &\leq \mathbb{E}\left|(K+1)e^{K(t+|B_t|)}\right|+1<\infty\end{aligned}$$

as $Ke^{K(t+|B_t|)}$ is integrable for any $t\geq 0$. Therefore, M_t is integrable.

From the assumption, $f(t,x)$ is continuous with respect to x. We know that

$$\mathcal{L}f(t,B_t) = \frac{\partial f(t,x)}{\partial t} + \frac{1}{2}\sum_{i=1}^{d}\frac{\partial^2 f(t,x)}{\partial x_i^2} \tag{22.1.81}$$

is dominated by $Ke^{K(t+|B_t|)}$ which is integrable. Furthermore, we have $\mathcal{L}f(t,B_t+\varepsilon) \to \mathcal{L}f(t,B_t)$ as $\varepsilon \to 0$ since $f(t,x)$ is twice continuously differentiable with respect to x. Then by dominated convergence theorem (Theorem 19.3.8),

$$\int_0^t \mathcal{L}f(s,B_s+\varepsilon)ds \to \int_0^t \mathcal{L}f(s,B_s)ds, \qquad \text{as } \varepsilon \to 0. \tag{22.1.82}$$

Thus, $\int_0^t \mathcal{L}f(s,B_s)ds$ is continuous and therefore M_t is $\mathcal{F}_t$-measurable (and $\mathcal{F}_{t^+}$-measurable) by Proposition 15.2.3.

We will now show the martingale property. Let $t \geq 0$. Then

$$\begin{aligned} M_{t+s} - M_s &= f(t+s,B_{t+s}) - f(s,B_s) - \int_s^{s+t}\left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r,B_r)dr \\ &= f(t+s,B_{t+s}) - f(s,B_s) - \int_0^{t}\left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr. \end{aligned}$$

Thus, by Proposition 19.4.20.(iii),

$$\mathbb{E}\left(M_{t+s} - M_s \middle| \mathcal{F}_{s^+}\right) = \mathbb{E}\left(f(t+s,B_{t+s}) \middle| \mathcal{F}_{s^+}\right) - f(s,B_s) - \mathbb{E}\left(\int_0^t \left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr \middle| \mathcal{F}_{s^+}\right) \tag{22.1.83}$$

Since $B_{t+s} - B_s$ is independent of $\mathcal{F}_{s^+}$ by Theorem 22.1.9 and B_s is $\mathcal{F}_{s^+}$-measurable, by Proposition 19.3.16 and Proposition 19.4.28.(v),

$$\mathbb{E}\left(f(t+s,B_{t+s}) \middle| \mathcal{F}_{s^+}\right) = \mathbb{E}\left(f(t+s,B_{t+s}-B_s+B_s) \middle| \mathcal{F}_{s^+}\right) \overset{\text{a.s.}}{=} \int_{\mathbb{R}^d} \left(f(t+s,x+B_s)\right) p_t(x)dx \qquad (\dagger\dagger) \tag{22.1.84}$$

where

$$p_t(x) = \frac{1}{(2\pi t)^{d/2}} \exp\left(-\frac{|x|^2}{2t}\right) \tag{22.1.85}$$

is defined in Definition 22.1.1 and satisfies (by Proposition[12])

$$\left(\frac{\partial}{\partial t} - \frac{1}{2}\Delta\right) p_t(x) = 0 \qquad (\dagger\dagger\dagger). \tag{22.1.86}$$

Let

$$Y = \mathbb{E}\left(\int_0^t \left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr \middle| \mathcal{F}_{s^+}\right), \qquad Z = \mathbb{E}\left(\left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s}) \middle| \mathcal{F}_{s^+}\right). \tag{22.1.87}$$

Then for any $A \in \mathcal{F}_{s^+}$, by definition of conditional expectation and Fubini theorem (Theorem 15.3.33 as $\int_0^t \left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr$ is integrable[13])

$$\begin{aligned} \mathbb{E}\left(Y\mathbb{1}_A\right) &= \mathbb{E}\left(\int_0^t \left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr\mathbb{1}_A\right) = \int_0^t \mathbb{E}\left(\left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})\mathbb{1}_A\right)dr \\ &= \int_0^t \mathbb{E}(Z\mathbb{1}_A)dr = \mathbb{E}\left(\int_0^t Zdr\mathbb{1}_A\right) \Rightarrow Y = \int_0^t Zdr \text{ a.s.} \end{aligned}$$

That is,

$$\mathbb{E}\left(\int_0^t \left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s})dr \middle| \mathcal{F}_{s^+}\right) = \int_0^t \mathbb{E}\left(\left(\frac{\partial}{\partial r} + \frac{1}{2}\Delta\right) f(r+s,B_{r+s}) \middle| \mathcal{F}_{s^+}\right)dr \text{ a.s.} \tag{22.1.88}$$

[12] need proposition

[13] it dominated by $e^{K|B_t|}\left(e^{Kt}-1\right)$, see (†) which is integrable.

Also, by the same argument in (††), we have

$$\mathbb{E}\left(\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,B_{r+s})\middle|\mathcal{F}_{s^+}\right)\overset{\text{a.s.}}{=}\int_{\mathbb{R}^d}\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,x+B_s)p_r(x)dx. \tag{22.1.89}$$

Then

$$\begin{aligned}\mathbb{E}\left(\int_0^t\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,B_{r+s})dr\middle|\mathcal{F}_{s^+}\right) &\overset{\text{a.s.}}{=} \int_0^t\int_{\mathbb{R}^d}\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,x+B_s)p_r(x)dxdr\\ &= \lim_{\varepsilon\to 0}\int_\varepsilon^t\int_{\mathbb{R}^d}\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,x+B_s)p_r(x)dxdr\end{aligned}$$

by dominated convergence theorem (Theorem 19.3.8). Furthermore, using integral by parts, we have

$$\begin{aligned}&\int_\varepsilon^t\int_{\mathbb{R}^d}\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,x+B_s)p_r(x)dxdr\\ =\;&\int_{\mathbb{R}^d}\int_\varepsilon^t\frac{\partial}{\partial r}f(r+s,x+B_s)p_r(x)drdx+\int_\varepsilon^t\int_{\mathbb{R}^d}\frac{1}{2}\Delta f(r+s,x+B_s)p_r(x)dxdr\\ =\;&\int_{\mathbb{R}^d}\left(f(t+s,x+B_s)p_t(x)-f(\varepsilon+s,x+B_s)p_\varepsilon(x)-\int_\varepsilon^t f(r+s,x+B_s)\frac{\partial}{\partial r}p_r(x)dr\right)dx\\ &+\frac{1}{2}\int_\varepsilon^t\left(\sum_{i=1}^d\frac{\partial f(r+s,x+B_s)}{\partial x_i}p_r(x)\middle|_{\mathbb{R}^d}-f(r+s,x+B_s)\sum_{j=1}^d\frac{\partial p_r(x)}{\partial x_j}\middle|_{\mathbb{R}^d}+\int_{\mathbb{R}^d}f(r+s,x+B_s)\Delta p_r(x)dx\right)dr\\ =\;&\int_{\mathbb{R}^d}\left(f(t+s,x+B_s)p_t(x)-f(\varepsilon+s,x+B_s)p_\varepsilon(x)\right)dx-\int_{\mathbb{R}^d}f(r+s,x+B_s)\left(\frac{\partial}{\partial r}-\frac{1}{2}\Delta\right)p_r(x)dxdr\end{aligned}$$

by Fubini theorem (Theorem 15.3.33 by assumption $(*)$). Then by (†††), we have

$$\mathbb{E}\left(\int_0^t\left(\frac{\partial}{\partial r}+\frac{1}{2}\Delta\right)f(r+s,B_{r+s})dr\middle|\mathcal{F}_{s^+}\right)\overset{\text{a.s.}}{=}\lim_{\varepsilon\to 0}\int_{\mathbb{R}^d}\left(f(t+s,x+B_s)p_t(x)-f(\varepsilon+s,x+B_s)p_\varepsilon(x)\right)dx \tag{††††}$$

Then combining (††) and (††††), we have that

$$\begin{aligned}\mathbb{E}\left(M_{t+s}-M_s|\,\mathcal{F}_{s^+}\right) &\overset{\text{a.s.}}{=} \lim_{\varepsilon\to 0}\int_{\mathbb{R}^d}f(\varepsilon+s,x+B_s)p_\varepsilon(x)dx-f(s,B_s)\\ &\overset{\text{a.s.}}{=} \lim_{\varepsilon\to 0}\mathbb{E}\left(f(\varepsilon+s,B_{s+\varepsilon})|\mathcal{F}_{s^+}\right)-f(s,B_s)=0\end{aligned}$$

by the continuity of Brownian motion and of f and by the conditional dominated convergence theorem (Theorem 19.4.25).

Furthermore, we know that M_t is continuous with respect to t as f is continuous and the integral is also continuous by dominated convergence theorem (Theorem 19.3.8) as the integrand is dominated by $Ke^{K(t+|B_t|)}$ (which is integrable).

Therefore, $M_s=M_{s^+}$ and hence $(M_t)_{t\geq 0}$ is an $(\mathcal{F}_{t^+})$-martingale. □

22.1.6 Recurrence and Transience

We will write $\mathbb{P}_x$ to indicate that the Brownian motion starts from x, i.e., under $\mathbb{P}_x$ the process $(B_t-x)_{t\geq 0}$ is a standard Brownian motion.

Theorem 22.1.25. Let $(B_t)_{t\geq 0}$ be a Brownian motion starting from particular point in $d\geq 1$ dimensions.

(i) In $d=1$, B is point-recurrent, i.e., under $\mathbb{P}_0$ (or any $\mathbb{P}_y$, $y\in\mathbb{R}$),

$$\{t:B_t=x\}\text{ are unbounded for every }x\in\mathbb{R}\text{ a.s..} \tag{22.1.90}$$

(ii) In $d=2$, B is neighbourhood-recurrent, i.e., under $\mathbb{P}_x$,

$$\{t:|B_t-z|\leq r\}\text{ is unbounded for every }x,z\in\mathbb{R}^d,\ r>0\text{ a.s.} \tag{22.1.91}$$

However, points are polar, i.e., for every $x \in \mathbb{R}^d$,

$$\mathbb{P}_0(H_x = \infty) = 1, \qquad \text{where } H_x = \inf\{t > 0 : B_t = x\} \text{ is the hitting time of } x. \tag{22.1.92}$$

(iii) In $d \geq 3$, B is transient, i.e., $|B_t| \to \infty$ as $t \to \infty$ $\mathbb{P}_0$-a.s.. Also, for $0 < r < |x|$,

$$\mathbb{P}_x(H_r < \infty) = \left(\frac{r}{|x|}\right)^{d-2}. \tag{22.1.93}$$

Remark. For 2-dimensional Brownian motion, since $\{t | B_t \in B(x, r)\}$ is unbounded for every $x \in \mathbb{R}^2$ and $r > 0$ and $\mathbb{R}^2$ may be covered by a countable union of balls of a fixed radius, the trajectory of Brownian motion is dense in $\mathbb{R}^2$. On the other hand, a.s. for all $t > 0$, $B_t \notin \mathbb{Q}^2$.

Proof. (i) We already know that $\sup_{t\geq 0} B_t = -\inf_{t\geq 0} B_t = \infty$ by Proposition 22.1.12, so we have point recurrence by continuity of B.

(ii) Note that it suffices to show the claim for $z = 0$. That is, $\{t : |B_t| \leq r\}$ is unbounded for every $x \in \mathbb{R}^d$, $r > 0$ $\mathbb{P}_x$-a.s..

Let $r > 0$, $R > r$, and $D_{r,R} = \left\{x \in \mathbb{R}^2 : r \leq |x| \leq R\right\}$. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be such that $f : x \to \log|x|$ on $D_{r,R}$, so f is bounded, is C^∞, and has bounded derivatives. Also, we have that $\Delta \log|x| = 0$ on $r \leq |x| \leq R$. That is,

$$\Delta \log|x| = \frac{\partial}{\partial x_1}\left(\frac{x_1}{x_1^2 + x_2^2}\right) + \frac{\partial}{\partial x_2}\left(\frac{x_2}{x_1^2 + x_2^2}\right) = \frac{x_1^2 + x_2^2 - 2x_1^2}{(x_1^2 + x_2^2)^2} + \frac{x_1^2 + x_2^2 - 2x_2^2}{(x_1^2 + x_2^2)^2} = 0.$$

Then by Theorem 22.1.23,

$$M_t = f(B_t) - f(x) - \int_0^t \frac{1}{2}\Delta f(B_s) ds = \log|B_t| - \log|x| \tag{22.1.94}$$

is a martingale. Let $T_r = \inf\{t \geq 0 : |B_t| \leq r\}$ and $T_R = \inf\{t \geq 0 : |B_t| \geq R\}$. Therefore let $T = T_r \wedge T_R$, then $T < T_R < \infty$ a.s. since Brownian motion is unbounded a.s. (by Proposition 22.1.12).

By optional stopping theorem (Theorem 20.5.16.(iii)),

$$\mathbb{E}(M_T) = M_0 \;\Rightarrow\; \log|x| = \mathbb{E}_x(\log|B_T|) = \log r \mathbb{P}_x(T_r < T_R) + \log R \mathbb{P}_x(T_R < T_r). \tag{22.1.95}$$

Thus,

$$\mathbb{P}_x(T_r < T_R) = \frac{\log R - \log|x|}{\log R - \log r}, \quad \mathbb{P}_x(T_R < T_r) = \frac{\log|x| - \log r}{\log R - \log r}. \qquad (*) \tag{22.1.96}$$

Applying Proposition 22.1.19, we have that $\mathbb{P}(T_n < \infty) = 1$ for all $n > \lfloor x \rfloor$, $n \in \mathbb{N}$ (this is for one dimensional case, but this implies higher dimensional case as $|B_t| \geq R$ if any dimension exceeds R). We know that

$$\{T_r < \infty\} = \bigcup_{n > \lfloor x \rfloor} \{T_r \leq T_n\} \cap \{T_n < \infty\} \;\Rightarrow\; \mathbb{1}_{\{T_r \leq T_n\}} \uparrow \mathbb{1}_{\{T_r < \infty\}} \text{ a.s.} \tag{22.1.97}$$

Then by dominated convergence theorem (Theorem 19.3.8), we have

$$\mathbb{P}(T_r < T_R) \to \mathbb{P}(T_r < \infty) \;\Rightarrow\; \mathbb{P}(T_r < \infty) = \lim_{R\uparrow\infty} \frac{\log R - \log|x|}{\log R - \log r} = 1. \tag{22.1.98}$$

which shows that

$$\mathbb{P}_x(|B_t| \leq r, \text{ for some } t > 0) = 1. \tag{22.1.99}$$

for any $x \in \mathbb{R}^2$. But

$$\begin{aligned}
\mathbb{P}_x(|B_t| \le r, \text{ for some } t > n) &= \mathbb{P}_x(|B_t - B_n + B_n| \le r, \text{ for some } t > n) = \mathbb{P}_x\left(\left|B_t^{(n)} + B_n\right| \le r, \text{ for some } t > n\right) \\
&= \int_{\mathbb{R}^2} \mathbb{P}_0\left(|B_t + y| \le r, \text{ for some } t > 0\right) \mathbb{P}_x(B_n \in dy) \qquad \text{(by Simple Markov Property)} \\
&= \int_{\mathbb{R}^2} \mathbb{P}_y\left(|B_t| \le r, \text{ for some } t > 0\right) \mathbb{P}_x(B_n \in dy) \\
&= \int_{\mathbb{R}^2} 1 \cdot \mathbb{P}_x(B_n \in dy) = \mathbb{P}\left(B_n \in \mathbb{R}^2\right) = 1,
\end{aligned}$$

so $\{t : |B_t| \le r\}$ is unbounded $\mathbb{P}_x$-a.s..

On the other hand, we know that

$$\{T_0 < \infty\} = \bigcup_{n > \lfloor x \rfloor} \{T_0 \le T_n\} \cap \{T_n < \infty\} = \bigcup_{n > \lfloor x \rfloor} \left\{ \left\{ \bigcap_{m > 1/|x|} \left\{T_{1/m} \le T_n\right\} \right\} \cap \{T_n < \infty\} \right\} \tag{22.1.100}$$

which gives that

$$\mathbb{1}_{\bigcup_{n>\lfloor x \rfloor} \bigcap_{m > 1/|x|} \left\{T_{1/m} \le T_n\right\}} \to \mathbb{1}_{\{T_0 < \infty\}} \text{ a.s. as } m, n \to \infty. \tag{22.1.101}$$

Then by dominated convergence theorem (Theorem 19.3.8), we have

$$\mathbb{P}\left(T_0 < \infty\right) = \lim_{n\to\infty} \lim_{m\to\infty} \mathbb{P}\left(T_{1/m} \le T_n\right) = \lim_{n\to\infty} \lim_{m\to\infty} \frac{\log n - \log |x|}{\log n + \log m} = \lim_{n\to\infty} 0 = 0. \tag{22.1.102}$$

for all $x \neq 0$. That is, for all $x \neq 0$,

$$\mathbb{P}_x\left(B_t = 0, \text{ for some } t > 0\right) = 0. \tag{22.1.103}$$

Now we only need to show that

$$\mathbb{P}_0\left(B_t = 0, \text{ for some } t > 0\right) = 0. \tag{22.1.104}$$

Again, by simple Markov property at $a > 0$ we get

$$\begin{aligned}
\mathbb{P}_0\left(B_t = 0, \text{ for some } t \ge a\right) &= \int_{\mathbb{R}^2} \mathbb{P}_0\left(B_{t+a} - B_a + y\right) \mathbb{P}_0(B_a \in dy) \\
&= \int_{\mathbb{R}^2} \mathbb{P}_y\left(B_t = 0, \text{ for some } t > 0\right) \frac{1}{(2\pi a)^{d/2}} e^{-|y|^2/2a} dy = 0
\end{aligned}$$

since for all $y \neq 0$ we have already proved that $\mathbb{P}_y\left(B_t = 0, \text{ for some } t > 0\right) = 0$. Thus, this holds for all $a > 0$, letting $a \to 0$, we have that $\mathbb{P}_0\left(B_t = 0, \text{ for some } t > 0\right) = 0$. Hence, for all x, we have

$$\mathbb{P}_x\left(B_t = 0, \text{ for some } t > 0\right) = 0 \tag{22.1.105}$$

which means that the Brownian motion can not touch 0 from x a.s..

(iii) Let f be a bounded C^∞ functions with all derivatives bounded such that $f(x) = \frac{1}{|x|^{d-2}}$ on $D_{r,R}$. Again, $\Delta f = 0$ on $D_{r,R}$, that is,

$$\begin{aligned}
\Delta f &= \sum_{i=1}^d \frac{\partial^2}{\partial x_i^2} \left(\frac{1}{\left(x_1^2 + \cdots + x_d^2\right)^{d/2-1}} \right) = \sum_{i=1}^d \frac{\partial}{\partial x_i} \left(\frac{(2-d)x_i}{\left(x_1^2 + \cdots + x_d^2\right)^{d/2}} \right) \\
&= (2-d) \sum_{i=1}^d \frac{\partial}{\partial x_i} \left(\frac{\left(x_1^2 + \cdots + x_d^2\right)^{d/2} - d x_i^2 \left(x_1^2 + \cdots + x_d^2\right)^{d/2-1}}{\left(x_1^2 + \cdots + x_d^2\right)^d} \right) = 0.
\end{aligned}$$

Then by Theorem 22.1.23,

$$M_t = f(B_t) - f(x) - \int_0^t \frac{1}{2} \Delta f(B_s) ds = \frac{1}{|B_t|^{d-2}} - \frac{1}{|x|^{d-2}} \tag{22.1.106}$$

is a martingale. Furthermore, let $T_r = \inf\{t \geq 0 : |B_t| \leq r\}$ and $T_R = \inf\{t \geq 0 : |B_t| \geq R\}$. Therefore let $T = T_r \wedge T_R$. Then the stopped martingale $M_{t\wedge T} = \frac{1}{|B_{t\wedge T}|^{d-2}} - \frac{1}{|x|^{d-2}}$ is also a martingale (Theorem 20.5.16), so $(M_{t\wedge T})_{t\geq 0}$ is a bounded martingale and therefore a UI martingale. Applying optional stopping theorem (Theorem 20.5.17), we have

$$\frac{1}{|x|^{d-2}} = \mathbb{E}\left(\frac{1}{|B_T|^{d-2}}\right) = \left(\frac{1}{r}\right)^{d-2}\mathbb{P}_x(T_r < T_R) + \left(\frac{1}{R}\right)^{d-2}\mathbb{P}_x(T_r > T_R) \tag{22.1.107}$$

which implies

$$\mathbb{P}_x(T_r < T_R) = \frac{\left(\frac{1}{R}\right)^{d-2} - \left(\frac{1}{|x|}\right)^{d-2}}{\left(\frac{1}{R}\right)^{d-2} - \left(\frac{1}{r}\right)^{d-2}}, \quad \mathbb{P}_x(T_R < T_r) = \frac{\left(\frac{1}{|x|}\right)^{d-2} - \left(\frac{1}{r}\right)^{d-2}}{\left(\frac{1}{R}\right)^{d-2} - \left(\frac{1}{r}\right)^{d-2}} \qquad (\dagger) \tag{22.1.108}$$

for $x \in D_{r,R}$. We know that

$$\{T_r < \infty\} = \bigcup_{n > \lfloor x \rfloor} \{T_r \leq T_n\} \cap \{T_n < \infty\} \;\Rightarrow\; \mathbb{1}_{\{T_r \leq T_n\}} \uparrow \mathbb{1}_{\{T_r < \infty\}} \text{ a.s.} \tag{22.1.109}$$

Then by dominated convergence theorem (Theorem 19.3.8), we have

$$\mathbb{P}(T_r < T_R) \to \mathbb{P}(T_r < \infty) \;\Rightarrow\; \mathbb{P}(T_r < \infty) = \lim_{R\uparrow\infty} \frac{\left(\frac{1}{R}\right)^{d-2} - \left(\frac{1}{|x|}\right)^{d-2}}{\left(\frac{1}{R}\right)^{d-2} - \left(\frac{1}{r}\right)^{d-2}} = \left(\frac{r}{|x|}\right)^{d-2}. \qquad (\dagger\dagger) \tag{22.1.110}$$

which is the probability of ever visiting the ball centred at 0 and of radius r when starting from $|x| \geq r$.

Now we will show that

$$\mathbb{P}_0(|B_t| \to \infty \text{ as } t \to \infty) = 1. \tag{22.1.111}$$

Since the first three components of Brownian motion in $\mathbb{R}^d$ are a Brownian motion in $\mathbb{R}^3$, it suffices to prove the result for $d = 3$. For fix $r > 0$, we define $S_r = \inf\{t > 0 : |B_t| = r\}$ and

$$A_n = \{|B_t| > n \text{ for all } t \geq S_{n^3}\}. \tag{22.1.112}$$

By the unboundedness of Brownian motion (Proposition 22.1.12), it is clear that

$$\mathbb{P}_0(S_{n^3} < \infty) = 1. \tag{22.1.113}$$

Applying the strong Markov property (Theorem 22.1.13) at time T_{n^3} we obtain

$$\begin{aligned}
\mathbb{P}_0(A_n^c) &= \mathbb{P}_0(|B_t| \leq n \text{ for some } t \geq S_{n^3}) = \mathbb{P}_0\left(\left|B_{t+S_{n^3}} - B_{S_{n^3}} + B_{S_{n^3}}\right| \leq n \text{ for some } t \geq 0\right) \\
&= \int_{\mathbb{R}^3} \mathbb{P}_0\left(\left|B_t^{(S_{n^3})} + y\right| \leq n \text{ for some } t \geq 0\right) \mathbb{P}_0\left(B_{S_{n^3}} \in dy\right) \\
&= \int_{\mathbb{R}^3} \mathbb{P}_y(|B_t| \leq n \text{ for some } t \geq 0)\, \mathbb{P}_0\left(B_{S_{n^3}} \in dy\right) = \int_{\mathbb{R}^3} \mathbb{P}_{n^3}(|B_t| \leq n \text{ for some } t \geq 0)\, \mathbb{P}_0\left(B_{S_{n^3}} \in dy\right) \\
&= \mathbb{P}_{n^3}(|B_t| \leq n \text{ for some } t \geq 0) \int_{\mathbb{R}^3} \mathbb{P}_0\left(B_{S_{n^3}} \in dy\right) = \mathbb{P}_{n^3}(|B_t| \leq n \text{ for some } t \geq 0) \\
&= \mathbb{P}_{n^3}(T_n < \infty) = \frac{n}{n^3} = \frac{1}{n^2}
\end{aligned}$$

by (††). Since the $\mathbb{P}_0(A_n^c)$ is summable, by first Borel-Cantelli lemma (Lemma 19.1.24) we get that A_n happens eventually $\mathbb{P}_0$-a.s., which implies that $|B_t| \to \infty$ as $t \to \infty$ $\mathbb{P}_0$-a.s..

□

22.1.7 Conditioned Brownian motion and Brownian bridge

Now let B be a standard Brownian motion (with $B_0 = 0$ a.s.) and let $0 < s < t$. What's the conditional distribution of B_s given B_t. The next result gives a nice way of working with the relevant normal distributions.

Lemma 22.1.26. let B be a standard Brownian motion and $0 < s < t$. Then $B_s - sB_t/t$ is independent of B_t.

Proof. First we know that $B_s - sB_t/t$ and B_t are Gaussian random variables. Also for any $\theta_1, \theta_2 \in \mathbb{R}$, we have

$$\theta_1 (B_s - sB_t/t) + \theta_2 B_t = (\theta_1 + \theta_2 - s\theta_1/t) B_s + (\theta_2 - s\theta_1/t)(B_t - B_s) \tag{22.1.114}$$

is still Gaussian as B_s and $B_t - B_s$ are independent. Thus, $B_s - sB_t/t$ and B_t are multivariate Gaussian random variables. So it suffices to show that $\operatorname{Cov}(B_s - sB_t/t, B_t) = 0$ by Theorem 19.8.20.(v).

To verify this, just note that

$$\operatorname{Cov}(B_s - sB_t/t, B_t) = \operatorname{Cov}(B_s, B_t) - \frac{s}{t}\operatorname{Cov}(B_t, B_t) = s \wedge t - \frac{s}{t} t = 0. \tag{22.1.115}$$

□

Proposition 22.1.27 (conditioned Brownian motion)**.** let B be a standard Brownian motion and $0 \le s < t$. Then

$$B_s|_{B_t} \sim \mathcal{N}\left(\frac{sB_t}{t}, \frac{s(t-s)}{t}\right). \tag{22.1.116}$$

Proof. To check the moment generating function of the conditioned Brownian motion $B_s|_{B_t}$. For any $\theta \in \mathbb{R}$,

$$\begin{aligned}
\mathbb{E}\left(e^{\theta B_s} \middle| B_t\right) &= \mathbb{E}\left(e^{\theta(B_s - sB_t/t)} e^{\theta s B_t/t} \middle| B_t\right) \overset{\text{a.s.}}{=} e^{\theta s B_t/t} \mathbb{E}\left(e^{\theta(B_s - sB_t/t)} \middle| B_t\right) \quad \text{by Proposition 19.4.28.(ii)} \\
&\overset{\text{a.s.}}{=} e^{\theta s B_t/t} \mathbb{E}\left(e^{\theta(B_s - sB_t/t)}\right) \quad \text{by Lemma 22.1.26 and Proposition 19.4.28.(v)} \\
&= e^{\theta s B_t/t} \mathbb{E}\left(e^{\theta\left(\frac{t-s}{t} B_s - \frac{s}{t} B_{t-s}\right)}\right) = e^{\theta s B_t/t} \mathbb{E}\left(e^{\frac{t-s}{t}\theta B_s}\right) \mathbb{E}\left(e^{-\frac{s}{t}\theta B_{t-s}}\right) \quad \text{by Proposition 19.5.13} \\
&= e^{\theta s B_t/t} e^{\frac{\theta^2 (t-s)^2 s}{2t^2}} e^{\frac{\theta^2 s^2 (t-s)}{2t^2}} = e^{\theta s B_t/t} e^{\frac{\theta^2 s(t-s)}{2t}}.
\end{aligned}$$

Thus, we have the required result. □

A more general proposition is given by

Proposition 22.1.28 (conditioned Brownian motion)**.** let B be a standard Brownian motion and $0 \le s < t < u$. Then

$$B_t|_{B_s, B_u} \sim \mathcal{N}\left(B_s + \frac{t-s}{u-s}(B_u - B_s), \frac{(t-s)(u-t)}{u-s}\right). \tag{22.1.117}$$

Proof. Let $\widetilde{B}_v := B_{s+v} - B_s$ for $v \ge 0$. Then by simple Markov property (Theorem 22.1.9), we have $\widetilde{B}_v$ is still a standard Brownian motion. Thus,

$$B_t|_{B_s, B_u} = \widetilde{B}_v + B_s|_{\widetilde{B}_w + B_s, B_s} = \underbrace{\widetilde{B}_v|_{\widetilde{B}_w, B_s} + B_s \sim \widetilde{B}_v|_{\widetilde{B}_w} + B_s}_{\text{by Proposition 19.4.28.(ii)}}. \tag{22.1.118}$$

Then, by Proposition 22.1.27 ($t = s + v$, $u = s + w$),

$$\widetilde{B}_v|_{\widetilde{B}_w} \sim \mathcal{N}\left(\frac{v\widetilde{B}_w}{w}, \frac{v(w-v)}{w}\right) = \mathcal{N}\left(\frac{(t-s)(B_u - B_s)}{u-s}, \frac{(t-s)(u-t)}{u-s}\right). \tag{22.1.119}$$

Therefore, the conditional distribution $B_t|_{B_s, B_u}$ is as required. □

Example 22.1.29. Given $B_s = a$, $B_u = b$, the conditional distribution of $B_t|_{B_s = a, B_u = b}$ is

$$\mathcal{N}\left(a + \frac{t-s}{u-s}(b-a), \frac{(t-s)(u-t)}{u-s}\right). \tag{22.1.120}$$

Note that the variance is maximized at time $t = (s+u)/2$ with value $(u-s)/4$.

Now we define Brownian bridge:

Definition 22.1.8 (Brownian bridge)**.** A Brownian bridge X is a centered Gaussian process[14] defined on $[0, T]$ and with covariance $\operatorname{Cov}(X_s, X_t) = s(T-t)/T$ for $s \le t \le T$.

[14] need definition

Remark. The easiest way to find a Brownian bridge is use $X_t = B_t - tB_T/T$ where B is a standard Brownian motion. We can easily calculate that for $s \leq t \leq T$,

$$\begin{aligned}
\operatorname{Cov}(X_s X_t) &= \operatorname{Cov}(B_s - sB_T/T, B_t - tB_T/T) \\
&= \mathbb{E}(B_s - sB_T/T, B_t - tB_T/T) - \mathbb{E}(B_s - sB_T/T)\,\mathbb{E}(B_t - tB_T/T) \\
&= s \wedge t - \frac{t}{T} s \wedge T - \frac{s}{T} t \wedge T + \frac{st}{T^2} T = s - ts/T = s(T-t)/T.
\end{aligned}$$

Thus, X_t is a continuous version of the Brownian bridge.

Note that $X_T = 0$ a.s. when Brownian bridge is between 0 and 0 and we can denote it as X_t^0. If the Brownian bridge is between 0 and x, we can use

$$X_t^x = B_t - t(B_T - x)/T = X_t^0 + tx/T. \tag{22.1.121}$$

However, these differences do not change the covariance, so X_t^x is also a Brownian bridge.

Proposition 22.1.30. let B be a standard Brownian motion ($B_0 = 0$ a.s.) and $0 \leq s < t$. Then $B_s|_{B_t}$ is a Brownian bridge on $[0, t]$.

Proof. Direct result from Definition 22.1.8 and Proposition 22.1.27. □

22.1.8 Quadratic variation

Lemma 22.1.31. Let B be a standard Brownian motion and let $t \geq 0$ be fixed. For $n \geq 1$, let

$$\Delta_n := \{0 = t_0(n) < t_1(n) < \ldots t_{m_n}(n) = t\} \tag{22.1.122}$$

be a subdivision of $[0, t]$, such that $\eta_n := \max_{1 \leq i \leq m_n} \{t_i(n) - t_{i-1}(n)\}$. Then

$$\lim_{n \to \infty} \sum_{i=1}^{m_n} \left(B_{t_i} - B_{t_{i-1}}\right)^2 = t \qquad \text{in } \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P}). \tag{22.1.123}$$

Proof. To show the result, we must show that ($\sum_{i=1}^{m_n} \left(B_{t_i} - B_{t_{i-1}}\right)^2 \in \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ is obvious)

$$\mathbb{E}\left(\left(\sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - t\right)^2\right) \to 0 \tag{22.1.124}$$

as $n \to \infty$. But we have (by Proposition 19.8.12)

$$\begin{aligned}
\mathbb{E}\left(\left(\sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - t\right)^2\right) &= \mathbb{E}\left(\left(\sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2\right)^2 - 2t \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 + t^2\right) \\
&= \mathbb{E}\left(\sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^4 + \sum_{i \neq j}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 (B_{t_j} - B_{t_{j-1}})^2 - 2t \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 + t^2\right) \\
&= 3 \sum_{i=1}^{m_n} (t_i - t_{i-1})^2 + \sum_{i \neq j}^{m_n} (t_i - t_{i-1})(t_j - t_{j-1}) - 2t \sum_{i=1}^{m_n} (t_i - t_{i-1}) + t^2 \\
&= 2 \sum_{i=1}^{m_n} (t_i - t_{i-1})^2 + \left(\sum_{i=1}^{m_n} (t_i - t_{i-1})\right)^2 - 2t^2 + t^2 \\
&= 2 \sum_{i=1}^{m_n} (t_i - t_{i-1})^2 \leq 2\eta_n \sum_{i=1}^{m_n} (t_i - t_{i-1}) = 2t\eta_n \to 0
\end{aligned}$$

as $n \to \infty$. □

Definition 22.1.9 (quadratic variation)**.** Let B be a standard Brownian motion and let $t \geq 0$ be fixed. For $n \geq 1$, let

$$[B]_t^n := \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} \left(B_{(k+1)2^{-n}} - B_{k2^{-n}} \right)^2 \tag{22.1.125}$$

for dyadic subdivision. $[B]_t^n$ is called quadratic variation of B with respect to n-dyadic subdivision.

Lemma 22.1.32. Let B be a standard Brownian motion and let $t \geq 0$ be fixed. For $n \geq 1$,

$$[B]_t^n \to t \quad \text{a.s..} \tag{22.1.126}$$

Proof. If the subdivision is dyadic, we can take $t_{m_n}(n) = \lfloor 2^n t \rfloor 2^{-n}$ and have that (by Markov inequality (Theorem 19.3.20))

$$\mathbb{P}\left(\left| [B]_t^n - \lfloor 2^n t \rfloor 2^{-n} \right| \geq \varepsilon \right) = \mathbb{P}\left(\left| \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - \lfloor 2^n t \rfloor 2^{-n} \right| \geq \varepsilon \right) \leq \frac{1}{\varepsilon^2} \mathbb{E}\left(\left(\sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - \lfloor 2^n t \rfloor 2^{-n} \right)^2 \right)$$

by calculations in Lemma 22.1.31, it is equal to

$$\frac{2}{\varepsilon^2} \sum_{i=1}^{m_n} (t_i - t_{i-1})^2 = \frac{2}{\varepsilon^2} \frac{1}{2^{2n}} \left(\lfloor 2^n t \rfloor 2^{-n} \right) 2^n = \frac{2 \lfloor 2^n t \rfloor}{\varepsilon^2} \frac{1}{2^{2n}} \leq \frac{2t}{\varepsilon^2 2^n}. \tag{22.1.127}$$

Thus,

$$\sum_{n=1}^{\infty} \mathbb{P}\left(\left| \sum_{i=1}^{m_n} \left(B_{t_i} - B_{t_{i-1}} \right)^2 - \lfloor 2^n t \rfloor 2^{-n} \right| \geq \varepsilon \right) < \infty, \tag{22.1.128}$$

hence we deduce by first Borel-Cantelli lemma (Lemma 19.1.24) that

$$\mathbb{P}\left(\left| \sum_{i=1}^{m_n} \left(B_{t_i} - B_{t_{i-1}} \right)^2 - \lfloor 2^n t \rfloor 2^{-n} \right| < \varepsilon \text{ ev.} \right) = 1. \tag{22.1.129}$$

Hence, $\forall \varepsilon > 0$, for all $n = n(\omega)$ sufficiently large we have that

$$\left| \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - \lfloor 2^n t \rfloor 2^{-n} \right| < \varepsilon \text{ a.s.} \tag{22.1.130}$$

But we also have

$$\left| \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - t \right| \leq \left| \sum_{i=1}^{m_n} (B_{t_i} - B_{t_{i-1}})^2 - \lfloor 2^n t \rfloor 2^{-n} \right| + \left| \lfloor 2^n t \rfloor 2^{-n} - t \right| < \varepsilon/2 + \varepsilon/2 = \varepsilon \quad \text{a.s..} \tag{22.1.131}$$

Thus, we have $[B]_t^n \to t$ a.s.. □

Since Brownian motion B is a special stochastic process, we can give the stronger version of its quadratic variation.

Theorem 22.1.33. Let B be a standard Brownian motion ($B_0 = 0$ a.s.) and let $t \geq 0$ be fixed. For $n \geq 1$, $([B]_t^n)_{t \geq 0}$ converges to $(t)_{t \geq 0}$ uniformly on compacts almost surely (u.c.a.s.), i.e.,

$$\sup_{0 \leq s \leq t} |[B]_s^n - s| \to 0 \quad \text{a.s..,} \qquad \text{or} \qquad \mathbb{P}\left(\lim_{n \to \infty} \sup_{0 \leq s \leq t} |[B]_s^n - s| = 0 \right) = 1. \tag{22.1.132}$$

Proof. Clearly, $[B]_t^n - \lfloor 2^n t \rfloor 2^{-n}$ is adapted and integrable. From Lemma 20.2.5, we know that

$$B^2_{\lfloor 2^n t \rfloor 2^{-n}} - [B]_t^n \quad \text{is a martingale.} \tag{22.1.133}$$

But we know that $\left(B^2_{\lfloor 2^n t \rfloor 2^{-n}} - \lfloor 2^n t \rfloor 2^{-n} \right)_{t \geq 0}$ is martingale as $B_t^2 - t$ is a martingale (by Theorem 22.1.20.(ii)). Thus,

we have that $[B]_t^n - \lfloor 2^n t \rfloor 2^{-n}$ is actually a martingale. Then by Doob's maximal inequality (Theorem 20.5.8), we have

$$\mathbb{P}\left(\sup_{0\le s\le t}\left|[B]_s^n - \lfloor 2^n s\rfloor 2^{-n}\right| \ge \varepsilon\right) \le \frac{1}{\varepsilon^2}\mathbb{E}\left(\left([B]_t^n - \lfloor 2^n t\rfloor 2^{-n}\right)^2\right). \tag{22.1.134}$$

Then with the same argument in Lemma 22.1.32, we have $\forall \varepsilon > 0$, for all $n = n(\omega)$ sufficiently large we have that

$$\sup_{0\le s\le t}\left|[B]_s^n - \lfloor 2^n s\rfloor 2^{-n}\right| < \varepsilon \text{ a.s.} \tag{22.1.135}$$

But we also have

$$\sup_{0\le s\le t}|[B]_s^n - s| \le \sup_{0\le s\le t}\left|[B]_s^n - \lfloor 2^n s\rfloor 2^{-n}\right| + \sup_{0\le s\le t}\left|\lfloor 2^n s\rfloor 2^{-n} - s\right| < \varepsilon/2 + \varepsilon/2 = \varepsilon \quad \text{a.s..} \tag{22.1.136}$$

Thus, we have $\left([B]_t^n\right)_{t\ge 0} \to (t)_{t\ge 0}$ u.c.a.s.. □

22.2 Problems

22.2.1 Brownian motion

Problem 22.2.1 (Zhou [18].P_{130})**.** Let $(B_t)_{t\ge 0}$ be a Brownian motion with $B_t \sim \mathcal{N}(0, \sigma^2 t)$. For $t_1 < t_2$, what's the probability that $B_{t_1} > 0$ and $B_{t_2} < 0$?

In particular, what's the probability that $B_1 > 0$ and $B_2 < 0$?

Solution. Since $B_{t_2} - B_{t_1}$ is independent of B_{t_1},

$$\begin{aligned}
\mathbb{P}(B_{t_1} > 0, B_{t_2} < 0) &= \mathbb{P}(B_{t_1} > 0, B_{t_2} - B_{t_1} < -B_{t_1}) = \mathbb{P}(B_{t_1} > 0)\,\mathbb{P}(B_{t_2-t_1} < -B_{t_1}|B_{t_1}) \\
&= \int_0^\infty \frac{1}{\sqrt{2\pi t_1}\sigma} e^{-\frac{x^2}{2t_1\sigma^2}} \int_{-\infty}^{-x} \frac{1}{\sqrt{2\pi(t_2-t_1)}\sigma} e^{-\frac{y^2}{2(t_2-t_1)\sigma^2}}\, dydx \\
&= \int_0^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \int_{-\infty}^{(-x\sigma\sqrt{t_1})/\sigma\sqrt{t_2-t_1}} \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}}\, dydx
\end{aligned}$$

Thus, we converse it to polar coordinate

$$\mathbb{P}(B_{t_1} > 0, B_{t_2} < 0) = \frac{1}{2\pi}\int_{-\frac{\pi}{2}}^{-\arctan\sqrt{\frac{t_1}{t_2-t_1}}} d\theta = \frac{1}{2\pi}\arctan\sqrt{\frac{t_2-t_1}{t_1}}. \quad (*) \tag{22.2.1}$$

If $t_1 = 1$ and $t_2 = 2$, we have $B_1 \sim (B_2 - B_1)$. Therefore,

$$\begin{aligned}
\mathbb{P}(B_1 > 0, B_2 < 0) &= \mathbb{P}(B_1 > 0, B_2 - B_1 < -B_1) = \mathbb{P}(B_1 > 0, |B_2 - B_1| > |B_1|, B_2 - B_1 < 0) \\
&= \mathbb{P}(B_1 > 0)\,\mathbb{P}(|B_2 - B_1| > |B_1|, B_2 - B_1 < 0|B_1 > 0) \\
&= \mathbb{P}(B_1 > 0)\,\mathbb{P}(B_2 - B_1 < 0)\,\mathbb{P}(|B_2 - B_1| > |B_1|\,|B_1 > 0, B_2 - B_1 < 0) = \frac{1}{2}\frac{1}{2}\frac{1}{2} = \frac{1}{8}.
\end{aligned}$$

which is consistent with $(*)$.

Problem 22.2.2. Define $R = \inf\{t \ge 1 : B_t = 0\}$ and let $L = \sup\{t \le 1 : B_t = 0\}$.

(a) Show that L is not a stopping time. Is R a stopping time?

(b) Show that

$$\mathbb{P}(R > 1 + u) = 1 - \frac{2}{\pi}\arctan(\sqrt{u}). \tag{22.2.2}$$

(c) Deduce that L has the arcsince law[15]:

$$\mathbb{P}(L < t) = \int_0^t \frac{dx}{\pi\sqrt{x(1-x)}} = \frac{2}{\pi}\arcsin\sqrt{t}. \tag{22.2.3}$$

[15] need citation of P.Levy, see Ito & McKean P_28

Solution. (a) L is not a stopping time, because the event $\{L > t\}$ depends only on $(B_{s+t})_{s\geq 0}$ so it not in $\mathcal{F}_t^B$.

R is a stopping time, because for $t < 1$, $\{R \leq t\} = \emptyset \in \mathcal{F}_t^B$. For $t \geq 1$, we have

$$\{R \leq t\} = \left\{B_1 > 0, \inf_{1\leq s\leq t} B_s < 0\right\} \cup \left\{B_1 < 0, \sup_{1\leq s\leq t} B_s > 0\right\} \cup \{B_1 = 0\} \in \mathcal{F}_t^B. \tag{22.2.4}$$

(b) We have $R = \inf\{t \geq 1 : B_t = 0\} = 1 + \inf\{t \geq 0 : B_{t+1} = 0\} = 1 + \inf\{t \geq 0 : B_{t+1} - B_1 = -B_1\}$.

Thus, $R-1 = \inf\{t \geq 0 : B_{t+1} - B_1 = -B_1\} = \inf\{t \geq 0 : B'_t = -B_1\}$. Then by the simple Markov property (Theorem 22.1.9), we have that $(B'_t = B_{t+1} - B_1)_{t\geq 0}$ is a standard Brownian motion independent of B_1. If we know B_1 then $R-1$ is the first hitting time of $-B_1$, which we know that $R-1$ has the same distribution as $\left(\frac{B_1}{B'_1}\right)^2$ by Proposition 22.1.18. Thus, by tower property (Proposition 19.4.28),

$$\mathbb{P}(R-1 > u) = \mathbb{E}(\mathbb{P}(R-1 > u)|\, B_1) = \mathbb{E}\left(\mathbb{P}\left(\left(\frac{B_1}{B'_1}\right)^2 > u\right)\middle|\, B_1\right) = \mathbb{P}\left(\left(\frac{B_1}{B'_1}\right)^2 > u\right) \tag{22.2.5}$$

where B_1 and B'_1 are two independent Gaussian with zero mean and variance 1. Thus, B_1/B'_1 is Cauchy distributed, $\mathbb{P}(B_1/B'_1 \leq k) = \frac{1}{2} + \frac{1}{\pi}\arctan k$ (Proposition 19.8.26),

$$\begin{aligned}\mathbb{P}(R-1 > u) &= \mathbb{P}\left(\left|\frac{B_1}{B'_1}\right| > \sqrt{u}\right) = \mathbb{P}\left(\frac{B_1}{B'_1} > \sqrt{u}\right) + \mathbb{P}\left(\frac{B_1}{B'_1} < -\sqrt{u}\right)\\ &= 1 - \left(\frac{1}{2} + \frac{1}{\pi}\arctan k\right) + \frac{1}{2} + \frac{1}{\pi}\arctan\left(-\sqrt{u}\right) = 1 - \frac{2}{\pi}\arctan\sqrt{u}.\end{aligned}$$

(c) We have that

$$R^{-1} = \sup\left\{\frac{1}{t} : t \geq 1, B_t = 0\right\} = \sup\left\{u \leq 1 : B_{1/u} = 0\right\} = \sup\left\{u \leq 1 : uB_{1/u} = 0\right\}. \tag{22.2.6}$$

But we know that $\left(uB_{1/u}\right)_{u\geq 0}$ has the same law as $(B_u)_{u\geq 0}$, so $R^{-1} \sim L$. Thus,

$$\mathbb{P}(L < t) = \mathbb{P}\left(R > \frac{1}{t}\right) = \mathbb{P}\left(R > 1 + \frac{1-t}{t}\right) = 1 - \frac{2}{\pi}\arctan\sqrt{\frac{1-t}{t}} \tag{22.2.7}$$

Taking differentiation wrt t we have

$$\left(1 - \frac{2}{\pi}\arctan\sqrt{\frac{1-t}{t}}\right)' = -\frac{1}{1+\frac{1-t}{t}}\left(\left(\frac{1-t}{t}\right)^{1/2}\right)' = -t\left(\frac{1-t}{t}\right)^{-1/2}\frac{-t-(1-t)}{t^2} = \frac{1}{\pi\sqrt{t(1-t)}} \tag{22.2.8}$$

as required.

Chapter 23

Stochastic Calculus

In this chapter, we work with a filtered probability space satisfying the usual condition (see Definition 20.4.13).

23.1 Itô Stochastic Integral

In this section we establish the stochastic integral with respect to continuous semimartingales. In places, we develop parts of the theory also for càdlàg semimartingales, where this involves no extra work. However, parts of the construction will use crucially the assumption of continuity.

Write $\mathcal{M}^2$ for the set of all càdlàg $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$-bounded (see Definition 19.3.5) martingales, and $\mathcal{M}_c^2$ for the set of sample-continuous (sample path is continuous a.s.) martingales bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$.

Similar to the construction to the Lebesgue integral in measure theory, we start by constructing the stochastic integral when the the integrand is very simple.

23.1.1 Simple integrands and $\mathcal{M}^2$ properties

Definition 23.1.1 (simple process)**.** A simple process is any map $H : \Omega \times (0, \infty) \to \mathbb{R}$ of the form

$$H(\omega, t) = \sum_{k=0}^{n-1} Z_k(\omega) \mathbb{1}_{(t_k, t_{k+1}]}(t) \tag{23.1.1}$$

where $n \in \mathbb{N}$, $0 = t_0 < \cdots < t_n < \infty$ and Z_k is a bounded $\mathcal{F}_{t_k}$-measurable random variable for all k. We denote the set of simple processes by $\mathcal{S}$.

Proposition 23.1.1. $\mathcal{S}$ is a vector space over $\mathbb{R}$. Indeed, $\mathcal{S}$ is an algebra (see Definition 8.1.3).

Proof. Check the definition of vector space (Definition 8.1.1). Define

$$H_1(\omega, t) = \sum_{i=0}^{m-1} X_i(\omega) \mathbb{1}_{(t_i, t_{i+1}]}(t), \; H_2 = \sum_{j=0}^{n-1} Y_j(\omega) \mathbb{1}_{(s_j, s_{j+1}]}(t) \; \in \mathcal{S} \tag{23.1.2}$$

with $0 = t_0 < \cdots < t_m < \infty$ and $0 = s_0 < \cdots < s_n < \infty$, X_i and Y_j are bounded $\mathcal{F}_{t_i}, \mathcal{F}_{s_j}$-measurable, respectively. Then we resort t_i and s_j with increasing order and form a new sequence $0 = r_0 < \ldots r_l < \infty$. Then,

$$\begin{aligned}
(H_1 + H_2)(\omega, t) &= \sum_{i=0}^{m-1} X_i(\omega) \sum_{k=0}^{l-1} \mathbb{1}_{(r_k, r_{k+1}] \subseteq (t_i, t_{i+1}]}(t) + \sum_{j=0}^{n-1} Y_j(\omega) \sum_{k=0}^{l-1} \mathbb{1}_{(r_k, r_{k+1}] \subseteq (s_j, s_{j+1}]}(t) \\
&= \sum_{k=0}^{l-1} \left(\sum_{i=0}^{m-1} X_i(\omega) \mathbb{1}_{\{t_i \le r_k, t_{i+1} \ge r_{k+1}\}} + \sum_{j=0}^{n-1} Y_j(\omega) \mathbb{1}_{\{s_j \le r_k, s_{j+1} \ge r_{k+1}\}} \right) \mathbb{1}_{(r_k, r_{k+1}]}(t) \\
&= \sum_{k=0}^{l-1} \left(\sum_{i=0}^{m-1} \underbrace{X_i(\omega) \mathbb{1}_{\{t_i \le r_k\}}}_{\mathcal{F}_{r_k}\text{-measurable}} \mathbb{1}_{\{t_{i+1} \ge r_{k+1}\}} + \sum_{j=0}^{n-1} \underbrace{Y_j(\omega) \mathbb{1}_{\{s_j \le r_k\}}}_{\mathcal{F}_{r_k}\text{-measurable}} \mathbb{1}_{\{s_{j+1} \ge r_{k+1}\}} \right) \mathbb{1}_{(r_k, r_{k+1}]}(t)
\end{aligned}$$

Thus, $(H_1+H_2)(\omega,t)\in\mathcal{S}$. For any $\lambda\in\mathbb{R}$,

$$\lambda H_1=\lambda\sum_{i=0}^{m-1}X_i(\omega)\mathbb{1}_{(t_i,t_{i+1}]}(t)=\sum_{i=0}^{m-1}\underbrace{\lambda X_i(\omega)}_{\mathcal{F}_{t_i}\text{-measurable}}\mathbb{1}_{(t_i,t_{i+1}]}(t)\ \Rightarrow\ \lambda H_1\in\mathcal{S}. \tag{23.1.3}$$

Thus, $\mathcal{S}$ is a vector space over $\mathbb{R}$.

To see $\mathcal{S}$ is a ring, we only need an extra condition that $H_1H_2\in\mathcal{S}$.

$$\begin{aligned}H_1(\omega,t)H_2(\omega,t) &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}X_i(\omega)Y_j(\omega)\mathbb{1}_{(t_i,t_{i+1}]}(t)\mathbb{1}_{(s_j,s_{j+1}]}(t)\\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}X_i(\omega)Y_j(\omega)\mathbb{1}_{(t_i\vee s_j,(s_j\vee t_i)\vee(t_{i+1}\wedge s_{j+1})]}(t).\end{aligned}$$

where $X_i(\omega)Y_j(\omega)$ is $\mathcal{F}_{t_i\vee s_j}$-measurable. Thus, $H_1(\omega,t)H_2(\omega,t)\in\mathcal{S}$. Therefore, $\mathcal{S}$ is also an algebra (Definition 8.1.3). □

Proposition 23.1.2. Every simple process is previsible.

Proof. For any simpel process $H(\omega,t)=\sum_{k=0}^{n-1}Z_k(\omega)\mathbb{1}_{(t_k,t_{k+1}]}(t)\in\mathcal{S}$ with Z_k is bounded $\mathcal{F}_{t_k}$-measurable.

If $Z_k=\mathbb{1}_A$ where $A\in\mathcal{F}_{t_k}$, then $Z_k(\omega)\mathbb{1}_{(t_k,t_{k+1}]}(t)=\mathbb{1}_{A\times(t_k,t_{k+1}]}(\omega,t)$ is in the π-system $\mathcal{A}$ which generates $\mathcal{P}$ ($\mathcal{P}=\sigma(\mathcal{A})$). Thus, $\mathbb{1}_{A\times(t_k,t_{k+1}]}(\omega,t)$ is $\mathcal{P}$-measurable. Thus,

$$\sum_{k=0}^{n-1}a_k\mathbb{1}_{A_k}\mathbb{1}_{(t_k,t_{k+1}]}(\omega,t)=\sum_{k=0}^{n-1}a_k\mathbb{1}_{A_k\times(t_k,t_{k+1}]}(\omega,t)\ \text{ is }\mathcal{P}\text{-measurable} \tag{23.1.4}$$

where A_k is $\mathcal{F}_{t_k}$-measurable and a_k are bounded.

Now for any $H\in\mathcal{S}$, we can write

$$H(\omega,t)=\sum_{k=0}^{n-1}Z_k(\omega)\mathbb{1}_{(t_k,t_{k+1}]}(t)=\sum_{k=0}^{n-1}Z_k^+(\omega)\mathbb{1}_{(t_k,t_{k+1}]}(t)-\sum_{k=0}^{n-1}Z_k^-(\omega)\mathbb{1}_{(t_k,t_{k+1}]}(t) \tag{23.1.5}$$

Since H is bounded, we can consider non-negative H instead and define define

$$\begin{aligned}H^m=2^{-m}\lfloor 2^mH\rfloor &= \sum_{k=0}^{n-1}2^{-m}\lfloor 2^mZ_k(\omega)\rfloor\mathbb{1}_{(t_k,t_{k+1}]}(t)=\sum_{k=0}^{n-1}2^{-m}\sum_{r=0}^{\infty}\mathbb{1}_{\{2^mZ_k(\omega)\geq r\}}\mathbb{1}_{(t_k,t_{k+1}]}(t)\\ &= \sum_{k=0}^{n-1}2^{-m}\sum_{r=0}^{\infty}\mathbb{1}_{\{Z_k(\omega)\geq r2^{-m}\}}\mathbb{1}_{(t_k,t_{k+1}]}(t)=\underbrace{\sum_{r=0}^{\infty}\sum_{k=0}^{n-1}2^{-m}\overbrace{\mathbb{1}_{\{Z_k(\omega)\geq r2^{-m}\}}}^{\mathcal{F}_{t_k}\text{-measurable}}\mathbb{1}_{(t_k,t_{k+1}]}(t)}_{\mathcal{P}\text{-measurable}}.\end{aligned}$$

Thus, H^m is $\mathcal{P}$-measurable. Since $H^m\uparrow H$, we have non-negative H is $\mathcal{P}$-measurable. Then for any $H\in\mathcal{S}$, we can write $H=H^+-H^-$ which is the difference between two $\mathcal{P}$-measurable functions. Thus, H is also $\mathcal{P}$-measurable. □

Definition 23.1.2 (essential supremum)**.** Given a stochastic process $(X_t)_{t\geq0}$, we denote $\|X\|_\infty=\operatorname{esssup}(X)$ the essential supremum of X (see essential supremum of function, Definition 15.4.2). It is the smallest $\lambda>0$ such that $\sup_{t\geq0}|X(t,\omega)|\leq\lambda$ almost surely, i.e.,

$$\|X\|_\infty:=\operatorname{esssup}(X)=\inf\left\{\lambda:\sup_{t\geq0}|X(t,\omega)|\leq\lambda\text{ a.s.}\right\}. \tag{23.1.6}$$

We now define the stochastic integral for simple processes.

Definition 23.1.3. For $H=\sum_{k=0}^{n-1}Z_k\mathbb{1}_{(t_k,t_{k+1}]}\in\mathcal{S}$ and $M\in\mathcal{M}^2$ set

$$(H\cdot M)_t=\sum_{k=0}^{n-1}Z_k\left(M_{t_{k+1}\wedge t}-M_{t_k\wedge t}\right).\qquad((H\cdot M)_0) \tag{23.1.7}$$

Proposition 23.1.3. Let $H\in\mathcal{S}$ and $M\in\mathcal{M}^2$. Let T be a stopping time. Then

(i) $H \cdot M^T = (H \cdot M)^T$.

(ii) $H \cdot M \in \mathcal{M}^2$. (If $M \in \mathcal{M}_c^2$, then $H \cdot M \in \mathcal{M}_c^2$.)

(iii) $\mathbb{E}\left((H \cdot M)_\infty^2\right) \leq \|H\|_\infty^2 \, \mathbb{E}\left((M_\infty - M_0)^2\right)$.

Proof. (i) For all $t \geq 0$ we have

$$\left(H \cdot M^T\right)_t = \sum_{k=0}^{n-1} Z_k \left(M^T_{t_{k+1}\wedge t} - M^T_{t_k \wedge t}\right) = \sum_{k=0}^{n-1} Z_k \left(M_{t_{k+1}\wedge t \wedge T} - M_{t_k \wedge t \wedge T}\right) = (H \cdot M)_{t\wedge T} = (H \cdot M)^T_t. \tag{23.1.8}$$

(ii) For $t_k \leq s \leq t < t_{k+1}$, $(H \cdot M)_t - (H \cdot M)_s = Z_k(M_t - M_s)$, so that (by Proposition 19.4.28.(iv) since Z_k is $\mathcal{F}_s$-measurable)

$$\mathbb{E}\left((H \cdot M)_t - (H \cdot M)_s | \mathcal{F}_s\right) \overset{\text{a.s.}}{=} Z_k \mathbb{E}(M_t - M_s | \mathcal{F}_s) \overset{\text{a.s.}}{=} 0. \tag{23.1.9}$$

This extends easily to general $s \leq t$ and hence $H \cdot M$ is a martingale.

To show it is bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, note that if $j < k$ we have the following "orthogonality relation" (by Proposition 19.4.20.(i) and Proposition 19.4.28.(iv)).

$$\mathbb{E}\left(Z_j(M_{t_j+1} - M_{t_j}) Z_k (M_{t_{k+1}} - M_{t_k})\right) = \mathbb{E}\left(\underbrace{Z_j(M_{t_j+1} - M_{t_j}) Z_k}_{\mathcal{F}_{t_k}\text{-measurable}} \mathbb{E}\left(M_{t_{k+1}} - M_{t_k} | \mathcal{F}_{t_k}\right)\right) = 0. \tag{23.1.10}$$

Thus let $t \geq 0$ and assume that $t_n \leq t$ for simplicity. To compute $\mathbb{E}((H \cdot M)_t^2)$, we expand the square and use the above orthogonality relation.

$$\begin{aligned} \mathbb{E}\left((H \cdot M)_t^2\right) &= \mathbb{E}\left(\left(\sum_{k=0}^{n-1} Z_k (M_{t_{k+1}} - M_{t_k})\right)^2\right) = \sum_{k=0}^{n-1} \mathbb{E}\left(Z_k^2 (M_{t_{k+1}} - M_{t_k})^2\right) \qquad (*) \\ &\leq \|H\|_\infty^2 \sum_{k=0}^{n-1} \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2\right) = \|H\|_\infty^2 \, \mathbb{E}\left((M_{t_n} - M_0)^2\right). \end{aligned}$$

(On two occasions, we used the trick (Lemma 20.5.3)).

Similarly, if $t_j \leq t < t_{j+1}$ then the same calculation gives:

$$\mathbb{E}\left((H \cdot M)_t^2\right) \leq \|H\|_\infty^2 \, \mathbb{E}\left((M_t - M_0)^2\right). \tag{23.1.11}$$

But note that since $M \in \mathcal{M}$, then $(M - M_0)^2$ is a submartingale (by Proposition 20.5.2). So if $s \geq t$ then

$$\mathbb{E}((M_t - M_0)^2) \leq \mathbb{E}((M_s - M_0)^2). \tag{23.1.12}$$

Therefore, for either case ($t_n \leq t$ or $t_j \leq t < t_{j+1}$), we have,

$$\mathbb{E}\left((H \cdot M)_t^2\right) \leq \|H\|_\infty^2 \, \mathbb{E}\left((M_t - M_0)^2\right). \tag{23.1.13}$$

Since $M \in \mathcal{M}^2$, then the convergence of M_s to M_∞ holds in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ and a.s. as $s \to \infty$ (by Theorem 20.5.14), hence we deduce $E((M_t - M_0)^2) \leq \mathbb{E}((M_\infty - M_0)^2)$ by letting $s \to \infty$. Thus for all $t \geq 0$,

$$\mathbb{E}\left((H \cdot M)_t^2\right) \leq \|H\|_\infty^2 \, \mathbb{E}\left((M_\infty - M_0)^2\right) \qquad (*) \tag{23.1.14}$$

and

$$\sup_{t\geq 0} \|(H \cdot M)_t\|_2 = \sup_{t \geq 0} \left(\mathbb{E}\left((H \cdot M)_t^2\right)\right)^{1/2} \leq \underbrace{\|H\|_\infty}_{\text{bounded}} \underbrace{\left(\mathbb{E}\left((M_\infty - M_0)^2\right)\right)^{1/2}}_{M_\infty \in \mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})} < \infty. \tag{23.1.15}$$

Thus, by Definition 19.3.5, $(H \cdot M)$ is bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$.

Now we show that $H \cdot M$ is càdlàg. For any $t \geq 0$, if $r_n \downarrow t$ and $s_n \uparrow t$, we have $r_n \wedge t_k \downarrow t \wedge t_k$ and $s_n \wedge t_k \uparrow t \wedge t_k$ and $M_{t\wedge t_k} = \lim_{r_n \wedge t_k \downarrow t \wedge t_k} M_{r_n \wedge t_k}$ a.s. and $M_{(t\wedge t_k)^-} = \lim_{s_n \wedge t_k \uparrow t \wedge t_k} M_{s_n \wedge t_k}$. a.s.. Thus, $(H \cdot M)_t$ is just linear combination of càdlàg process and so it is also a càdlàg process.

Thus $H \cdot M \in \mathcal{M}^2$.

(iii) Since $(H \cdot M) \in \mathcal{M}^2$ from (ii), we have $(H \cdot M)_t \to (H \cdot M)_\infty$ a.s. and in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$. Thus, by $(*)$

$$\|H\|_\infty^2 \, \mathbb{E}\left((M_\infty - M_0)^2\right) \geq \lim_{t\to\infty} \mathbb{E}\left((H \cdot M)_t^2\right) = \mathbb{E}\left((H \cdot M)_\infty^2\right). \tag{23.1.16}$$

□

To extend the simple integral defined in the last section, we will need some Hilbert space properties of the set of integrators we are considering. As before, we work on a filtered probability space $(\Omega, \mathcal{F}, (\mathcal{F}_t)_{t\geq 0}, \mathbb{P})$ where $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions.

Definition 23.1.4. For all càdlàg adapted processes X define the triple norm[1]

$$|||X||| := \left\| \sup_{t\geq 0} |X_t| \right\|_2. \tag{23.1.17}$$

We write $\mathcal{C}^2$ for the set of all càdlàg adapted processes X such that $|||X||| < \infty$.

Definition 23.1.5. Let $X \in \mathcal{M}^2$, we define the norm $\|X\| := \|X_\infty\|_2$.

Remark. It is well-defined since X_∞ exists by Theorem 20.5.14.

Note that the function $\|\cdot\|$ on $\mathcal{M}^2$ defines indeed a norm. The only point which demands justification is the requirement that if $\|M\| = 0$, then M is indistinguishable from 0.

If $\|M\| = 0$, then $\mathbb{E}\left(M_\infty^2\right) = 0$ so $M_\infty = 0$ a.s. by Theorem 15.3.7. By the martingale convergence theorem (Theorem 20.5.13),

$$M_t = \mathbb{E}\left(M_\infty | \mathcal{F}_t\right) \quad \text{a.s.} \tag{23.1.18}$$

so $M_t = 0$ a.s. for all t. Since M is càdlàg, it is indistinguishable from 0 by Proposition 20.4.12.

We may now state some $\mathcal{L}^2$ properties which show that the space of square-integrable martingales can be seen as a Hilbert space. As we will see later, this underlying Hilbert structure is the basis of the formal definition of the stochastic integral in the general case. (Formally, it is defined as an isometry between Hilbert spaces).

Proposition 23.1.4. Let $(\mathcal{F}_t)_{t\geq 0}$ be the filtration satisfying usual conditions. Then

(i) $(\mathcal{C}^2, |||\cdot|||)$ is complete.

(ii) $\mathcal{M}^2 = \mathcal{M} \cap \mathcal{C}^2$.

(iii) $(\mathcal{M}^2, \|\cdot\|)$ is a Hilbert space[2] with $\mathcal{M}_c^2 = \mathcal{M}_c \cap \mathcal{M}^2$ as a closed subspace.

(iv) $X \mapsto X_\infty : \mathcal{M}^2 \to \mathcal{L}^2(\Omega, \mathcal{F}_\infty, \mathbb{P})$ is an isometry $\left(\left(\mathcal{M}^2, \|\cdot\|\right) \to \left(\mathcal{L}^2(\Omega, \mathcal{F}_\infty, \mathbb{P}), \|\cdot\|_2\right)\right)$.

Remark. $\mathcal{L}^2(\Omega, \mathcal{F}_\infty, \mathbb{P})$ is not a Hilbert space, but $L^2(\Omega, \mathcal{F}_\infty, \mathbb{P})$ ($\mathcal{L}^2(\Omega, \mathcal{F}_\infty, \mathbb{P})$ quotiented out almost surely equivalent set) is a Hilbert space.

Proof. (i) Suppose $(X^n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $(\mathcal{C}^2, |||\cdot|||)$. Then we can find a subsequence $(n_k)_{k\in\mathbb{N}}$ such that

$$\sum_{k=1}^{\infty} |||X^{n_{k+1}} - X^{n_k}||| < \infty. \tag{23.1.19}$$

Then by the Hölder inequality (Theorem 19.3.24),

$$\left\| \sum_{k=1}^{\infty} \sup_{t\geq 0} \left|X_t^{n_{k+1}} - X_t^{n_k}\right| \right\|_2 \leq \sum_{k=1}^{\infty} \left\| \sup_{t\geq 0} \left|X_t^{n_{k+1}} - X_t^{n_k}\right| \right\|_2 = \sum_{k=1}^{\infty} |||X^{n_{k+1}} - X^{n_k}||| < \infty \tag{23.1.20}$$

[1] Usual conventions about versions apply, dealing with equivalence classes analogous to $\mathcal{L}^p$-spaces

[2] need definition

Thus, $\sum_{k=1}^{\infty} \sup_{t\geq 0} \left|X_t^{n_{k+1}}(\omega) - X_t^{n_k}(\omega)\right| < \infty$ a.s.. Then by Lemma 10.2.9,

$$\sup_{t\geq 0} \left|X_t^{n_{k+1}}(\omega) - X_t^{n_k}(\omega)\right| \to 0 \text{ a.s. as } k \to \infty. \tag{23.1.21}$$

By Definition 23.1.2,

$$\left\|X^{n_{k+1}}(\omega) - X^{n_k}(\omega)\right\|_\infty = \inf\left\{\lambda : \sup_{t\geq 0} \left|X_t^{n_{k+1}}(\omega) - X_t^{n_k}(\omega)\right| \leq \lambda \text{ a.s.}\right\}$$

Thus, $\forall \varepsilon > 0$, we can find $k \in \mathbb{N}$ such that $\sup_{t\geq 0} \left|X_t^{n_{k+1}}(\omega) - X_t^{n_k}(\omega)\right| < \varepsilon$ a.s., then

$$\left\|X^{n_{k+1}}(\omega) - X^{n_k}(\omega)\right\|_\infty < \varepsilon \;\Rightarrow\; \left(X^{n_k}\right)_{k\in\mathbb{N}} \text{ is Cauchy sequence on } \left(\mathcal{C}^2, \|\cdot\|_\infty\right) \tag{23.1.22}$$

Since the space of càdlàg adapted process equipped with the $\|\cdot\|_\infty$ norm is complete (by Theorem 15.4.9), there exists a càdlàg process X such that

$$\left\|X^{n_k}(\omega) - X(\omega)\right\|_\infty \to 0 \;\Rightarrow\; \sup_{t\geq 0} \left|X_t^{n_k}(\omega) - X_t(\omega)\right| \to 0 \text{ a.s.} \tag{23.1.23}$$

as $k \to \infty$. That is, $X_t^{n_k}(\omega) \to X_t(\omega)$ uniformly[3]. Now we prove that X is indeed a càdlàg adapted process. Assume for any $\omega \in \Omega'$, $\sup_{t\geq 0} \left|X_t^{n_k}(\omega) - X_t(\omega)\right| \to 0$. Then $\forall t \geq 0, \varepsilon > 0$, $\exists N \in \mathbb{N}$ such that $\forall k \geq N$,

$$\left|X_t^{n_k}(\omega) - X_t(\omega)\right| < \frac{\varepsilon}{3}. \qquad (*) \tag{23.1.24}$$

Thus, if $s \downarrow t$, we have

$$\left|X_s(\omega) - X_t(\omega)\right| \leq \left|X_s^{n_k}(\omega) - X_s(\omega)\right| + \left|X_t^{n_k}(\omega) - X_t(\omega)\right| + \left|X_s^{n_k}(\omega) - X_t^{n_k}(\omega)\right| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \underbrace{\frac{\varepsilon}{3}}_{X^n \text{ is càdlàg}} = \varepsilon.$$

Thus, $X_t(\omega)$ is right-continuous for all $\omega \in \Omega'$. Also, since X^{n_k} is a convergent sequence, $\lim_{k\to\infty} X_t^{n_k}(\omega)$ for all $t \geq 0$. Thus, if $s \uparrow t$, we have

$$\begin{aligned}\left|X_s(\omega) - \lim_{k\to\infty} X_{t^-}^{n_k}(\omega)\right| &\leq \left|X_s^{n_k}(\omega) - X_s(\omega)\right| + \left|X_{t-}^{n_k}(\omega) - X_{t^-}(\omega)\right| + \left|X_{t^-}^{n_k}(\omega) - \lim_{k\to\infty} X_{t^-}^{n_k}(\omega)\right| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \underbrace{\frac{\varepsilon}{3}}_{X^n \text{ is càdlàg}} = \varepsilon.\end{aligned}$$

Thus, the left limit of $X_t(\omega)$ exists for all $t \geq 0$. So $X(\omega)$ is càdlàg for $\omega \in \Omega'$. Since $\mathbb{P}(\Omega') = 1$, we have that X is a càdlàg process. To construct an adapted X, we let for fix $t \geq 0$

$$X_t(\omega) = \begin{cases} \lim_{k\to\infty} X_t^{n_k}(\omega) & \omega \in \Omega' \\ 0 & \omega \in \Omega'^c \end{cases} = X_t^{n_k}(\omega)\mathbb{1}_{\{\omega\in\Omega'\}}. \tag{23.1.25}$$

We know $X_t^{n_k}$ is adapted and $\mathbb{1}_{\{\omega\in\Omega'\}}$ is $\mathcal{F}_t$-measurable (since $(\mathcal{F}_t)_{t\geq 0}$ satisfies the usual conditions and $\mathbb{P}(\Omega') = 1$).

[3]need definition

Thus, X_t is $\mathcal{F}_t$-measurable and X is adapted. Now we have

$$\begin{aligned}
|||X^n - X|||^2 &= \left\| \sup_{t\geq 0} |X_t^n - X_t| \right\|_2^2 = \mathbb{E}\left(\left(\sup_{t\geq 0} |X_t^n - X_t| \right)^2 \right) = \mathbb{E}\left(\sup_{t\geq 0} |X_t^n - X_t|^2 \right) \\
&\leq \mathbb{E}\left(\lim_{k\to\infty} \sup_{t\geq 0} \left\{ |X_t^n - X_t^{n_k}|^2 + |X_t - X_t^{n_k}|^2 + 2\,|X_t^n - X_t^{n_k}|\,|X_t - X_t^{n_k}| \right\} \right) \\
&\leq \mathbb{E}\left(\lim_{k\to\infty} \sup_{t\geq 0} |X_t^n - X_t^{n_k}|^2 + \lim_{k\to\infty} \sup_{t\geq 0} |X_t - X_t^{n_k}|^2 + 2 \lim_{k\to\infty} \sup_{t\geq 0} |X_t^n - X_t^{n_k}| \sup_{t\geq 0} |X_t - X_t^{n_k}| \right) \\
&= \mathbb{E}\left(\lim_{k\to\infty} \sup_{t\geq 0} |X_t^n - X_t^{n_k}|^2 + 0 + 0 \right) = \mathbb{E}\left(\liminf_{k\to\infty} \left\{ \sup_{t\geq 0} |X_t^n - X_t^{n_k}|^2 \right\} \right) \\
&\leq \liminf_{k\to\infty} \mathbb{E}\left(\left(\sup_{t\geq 0} |X_t^n - X_t^{n_k}| \right)^2 \right) \qquad \text{(by Fatou's lemma, Theorem 19.3.7)} \\
&= \liminf_{k\to\infty} |||X^n - X^{n_k}|||^2 \to 0 \quad \text{as } n \to \infty
\end{aligned}$$

since $(X^n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\left(\mathcal{C}^2, |||\cdot|||\right)$. Hence, $X^n \to X$ in $|||\cdot|||$ and thus $(\mathcal{C}^2, |||\cdot|||)$ is complete.

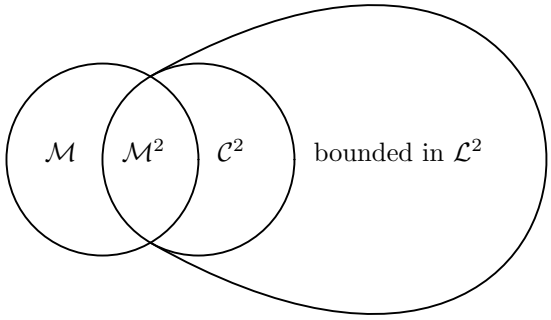
(ii) For $X \in \mathcal{C}^2 \cap \mathcal{M}$ we have

$$\sup_{t\geq 0} \|X_t\|_2 = \sup_{t\geq 0} \left(\mathbb{E}\left|X_t^2\right|\right)^{1/2} \leq \left(\mathbb{E}\left(\sup_{t\geq 0} |X_t|^2 \right) \right)^{1/2} = \left\| \sup_{t\geq 0} |X_t| \right\|_2 = |||X||| < \infty \tag{23.1.26}$$

and so X is bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ and thus $X \in \mathcal{M}^2$.

On the other hand, if $X \in \mathcal{M}^2$, by Corollary 20.5.10 Doob's inequality,

$$|||X||| = \left\| \sup_{t\geq 0} |X_t| \right\|_2 \leq \underbrace{2\,\|X_\infty\|_2}_{=2\|X\|} < \infty \;\Rightarrow\; X \in \mathcal{C}^2 \;\Rightarrow\; X \in \mathcal{C}^2 \cap \mathcal{M}. \tag{23.1.27}$$



(iii) $(X, Y) \to \mathbb{E}(X_\infty Y_\infty)$ defines an inner product[4] on $\mathcal{M}^2$ whose associated norm is precisely the double norm $\|\cdot\|$. Moreover, for $X \in \mathcal{M}^2$, we have

$$\|X\| = \|X_\infty\|_2 \leq \sup_{t\geq 0} \|X_t\|_2 \leq \left\| \sup_{t\geq 0} X_t \right\|_2 = \underbrace{|||X||| \leq 2\,\|X\|}_{\text{shown in (ii)}}, \qquad (\dagger) \tag{23.1.28}$$

that is, $\|\cdot\|$ and $|||\cdot|||$ are (Lipschitz) equivalent (see Definition 12.0.9) on $\mathcal{M}^2$. Thus $\mathcal{M}^2$ is complete for $\|\cdot\|$ if and only if it is complete for $|||\cdot|||$[5]. Since closed set of complete space is also complete[6], it is thus sufficient to show that $\mathcal{M}^2$ is closed in $(\mathcal{C}^2, |||\cdot|||)$.

If $X^n \in \mathcal{M}^2$ and $|||X^n - X||| \to 0$ as $n \to \infty$ for some X, then X is a càdlàg adapted process (with similar argument in (i)) and $\mathcal{L}^2$-bounded (since $X \in \mathcal{C}^2$ (by (ii))). So we only need the martingale property of X.

Since X is bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$, we have X is UI and thus bounded in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ (by Proposition 19.3.32). So X_t

[4] need definition
[5] need theorem
[6] need theorem

is integrable for any $t \geq 0$. By Minkowski inequality (Theorem 19.3.26) and Corollary 19.4.27, ($\mathbb{E}(X_t|\mathcal{F}_s) = X_s$ a.s.)

$$\begin{aligned}\|\mathbb{E}(X_t|\mathcal{F}_s) - X_s\|_2 &= \|\mathbb{E}(X_t|\mathcal{F}_s) - X_s - (\mathbb{E}(X_t^n|\mathcal{F}_s) - X_s^n)\|_2 \leq \|\mathbb{E}(X_t^n - X_t|\mathcal{F}_s)\|_2 + \|X_s^n - X_s\|_2 \\ &\leq \|X_t^n - X_t\|_2 + \|X_s^n - X_s\|_2 \leq 2\sup_{t\geq 0}\|X_t^n - X_t\|_2 \leq 2\,|||X^n - X||| \to 0\end{aligned}$$

as $n \to \infty$ and so $\mathbb{E}(X_t|\mathcal{F}_s) - X_s = 0$ a.s. and X is a martingale. Thus, $X \in \mathcal{M}^2$. By the similar argument $\mathcal{M}_c^2$ is closed in $(\mathcal{M}^2, \|\cdot\|)$.

(iv) For $X, Y \in \mathcal{M}^2$, $\|X - Y\| = \|X_\infty - Y_\infty\|_2$ by definition[7].

□

Lemma 23.1.5. Let $M^n \to M$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$ and T be a stopping time. Then $(M^n)^T \to M^T$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$.

Proof. If $M^n \to M$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$, we have $M^n, M \in \mathcal{M}_c^2$ and

$$\|M^n - M\| \to 0 \;\Leftrightarrow\; \|M_\infty^n - M_\infty\|_2 \to 0. \tag{23.1.29}$$

Thus, $(M^n)^T, M^T \in \mathcal{M}_c^2$ by Theorem 20.5.16 and

$$\begin{aligned}\left\|(M^n)^T - M^T\right\| &= \left\|(M^n - M)^T\right\| = \left\|(M_\infty^n - M_\infty)^T\right\|_2 = \|M_T^n - M_T\|_2 \leq \left\|\sup_{0\leq t\leq T}|M_t^n - M_t|\right\|_2 \\ &\leq \left\|\sup_{t\geq 0}|(M^n - M)_t|\right\|_2 \leq 2\,\|(M^n - M)_\infty\|_2 = 2\,\|M_\infty^n - M_\infty\|_2 \to 0.\end{aligned}$$

by Corollary 20.5.10. Thus, $(M^n)^T \to M^T$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$. □

23.1.2 Quadratic variation

We now introduce the quadratic variation. Recalling the definition of u.c.p. convergence of processes (Definition 20.4.30), we have

Proposition 23.1.6. Let X^n be a sequence of càdlàg processes and let T_k a sequence of random times, with $T_k \uparrow \infty$ a.s. as $k \to \infty$. Suppose $|||(X^n)^{T_k}||| \to 0$ as $n \to \infty$ for all k, then $X^n \to 0$ u.c.p..

Proof. First we have by definition

$$\left|\left|\left|(X^n)^{T_k}\right|\right|\right| \to 0 \;\text{ as } n \to \infty,\ \forall k \;\Rightarrow\; \mathbb{E}\left(\sup_{0\leq t\leq T_k}|X_t^n|^2\right) \to 0 \;\text{ as } n \to \infty,\ \forall k. \tag{23.1.30}$$

Now fix $T < \infty$, detetministic. Then given $\varepsilon > 0$, by Chebyshev inequality (Theomem 19.3.21)

$$\begin{aligned}\mathbb{P}\left(\sup_{0\leq t\leq T}|X_t^n| > \varepsilon\right) &\leq \mathbb{P}\left(\sup_{0\leq t\leq T_k}|X_t^n| > \varepsilon\right) + \mathbb{P}\left(T_k \leq T\right) \\ &\leq \mathbb{E}\left(\sup_{0\leq t\leq T_k}|X_t^n|^2\right)\Big/\varepsilon^2 + \mathbb{P}\left(T_k \leq T\right) \to \mathbb{P}\left(T_k \leq T\right) \quad \text{as } n \to \infty.\end{aligned}$$

But $T_k \uparrow \infty$ a.s. and $\mathbb{P}\left(T_k \leq T\right) \to 0$ as $k \to \infty$. Hence,

$$\mathbb{P}\left(\sup_{0\leq t\leq T}|X_t^n| > \varepsilon\right) \quad \text{as } n \to \infty, \tag{23.1.31}$$

for any $T < \infty$ and any $\varepsilon > 0$, i.e., $X^n \to 0$ u.c.p. by Definition 20.4.30. □

Theorem 23.1.7 (quadratic variation process)**.** For each $M \in \mathcal{M}_{c,loc}$ there exists a unique (up to indistinguishability) (pathwise) continuous adapted (pathwise) non-decreasing process $[M]$ such that $M^2 - [M] \in \mathcal{M}_{c,loc}$ and such that $[M]_0 = 0$ a.s.. Moreover, for

$$[M]_t^n := \sum_{k=0}^{\lfloor 2^n t\rfloor - 1}\left(M_{(k+1)2^{-n}} - M_{k2^{-n}}\right)^2, \quad [M]_0^n = 0, \qquad (*) \tag{23.1.32}$$

[7] need definition of isometry

we have $[M]_n \to [M]$ u.c.p. as $n \to \infty$. We call $[M]$ the quadratic variation process of M.

Remark. (i) It is essential to assume that M is continuous in this theorem.

(ii) The idea of the proof itself is based on Itô's formula. Indeed, as we will soon prove, if $M \in \mathcal{M}_{c,loc}$, then

$$M^2 = 2M \cdot M + [M]. \tag{23.1.33}$$

(iii) Some textbooks use the notation $\langle M \rangle$ rather than $[M]$ for the quadratic variation. In general (i.e., in the discontinuous case), $\langle M \rangle$ should be previsible and means something slightly different, but it coincides with $[M]$ when M is continuous.

(iv) If $M \in \mathcal{M}_{loc}$, there exists (pathwise) càdlàg adapted non-decreasing process $[M]$ such that $M^2 - [M] \in \mathcal{M}_{loc}$ and $[M]_0 = 0$ a.s.. However, we cannot guarantee the uniqueness and won't have $[M]^n \to [M]$ u.c.p.[8].

(v) Note that $[M]^n_t$ is a càdlàg adapted process, then we can have that if $[M]_n \to [M]$ u.c.p., $[M]$ must be càdlàg adapted process as well by Theorem 20.4.27. But this is just a weaker conclusion comparing to the statement in current theorem ($[M]$ is (pathwise) continuous adapted process).

(vi) Sometimes $[M]^n_t$ is defined by (e.g., Rogers-William [11].I11)

$$[M]^n_t := \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} \left(M_{(k+1)2^{-n}} - M_{k2^{-n}}\right)^2 + \left(M_t - M_{\lfloor 2^n t \rfloor 2^{-n}}\right)^2 \tag{23.1.34}$$

which is a (sample) continuous adapted process. Then we can have that if $[M]_n \to [M]$ u.c.p., $[M]$ must be (sample) continuous adapted process as well by Theorem 20.4.27. Again, this a weaker conclusion comparing to the current theorem.

(v) For standard Brownian motion, we have a stronger version. By Theorem 22.1.33, we know that $[B]^n_t \to t$ u.c.a.s. which implies that $[B]^n_t \to t$ u.c.p.. Since the quadratic variation is unique, we can have that $(t)_{t\geq 0}$ is the quadratic variation of $(B_t)_{t\geq 0}$.

Proof. Wlog we will consider the case $M_0 = 0$.

Uniqueness. if A and A' are two pathwise continuous increasing processes satisfying the conditions for $[M]$ ($A, A' \in \mathcal{M}_{c,loc}$) then

$$A_t - A'_t = (M_t^2 - A'_t) - (M_t^2 - A_t) \in \mathcal{M}_{c,loc} \tag{23.1.35}$$

Then since $A_t - A'_t$ is càdlàg, we have it has finite variation process by Proposition 10.3.12. Thus since $A - A'$ is indistinguishable from 0 then A is distinguishable from A' by Theorem 20.6.14.

Existence. First we assume that M is bounded, which implies $M \in \mathcal{M}^2_c$ by Corollary 20.6.7. Fix $T > 0$ deterministic. Let

$$H^n_t = \sum_{k=0}^{\lfloor 2^n T \rfloor - 1} M_{k2^{-n}} \mathbb{1}_{(k2^{-n},(k+1)2^{-n}]}(t). \tag{23.1.36}$$

Then $H^n \in \mathcal{S}$ for all $n \in \mathbb{N}$ since $M_{k2^{-n}}$ is $\mathcal{F}_{k2^{-n}}$-measurable. Hence X^n defined by

$$X^n_t = (H^n \cdot M)_t = \sum_{k=0}^{\lfloor 2^n T \rfloor - 1} M_{k2^{-n}} \left(M_{(k+1)2^{-n}\wedge t} - M_{k2^{-n}\wedge t}\right). \tag{23.1.37}$$

Then $X^n \in \mathcal{M}^2_c$ by Proposition 23.1.3.(ii) and the continuity of M.

[8] need checking

Wlog we assume $m \geq n$. Therefore, computing this as in Proposition 23.1.3 and letting $t \to \infty$,

$$\begin{aligned}
& X^n - X^m \\
= & \sum_{k=0}^{\lfloor 2^m T \rfloor - 1} M_{k2^{-m}} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) - \sum_{k=0}^{\lfloor 2^n T \rfloor - 1} M_{k2^{-n}} \left(M_{(k+1)2^{-n}} - M_{k2^{-n}} \right) \\
= & \sum_{k=0}^{\lfloor 2^m T \rfloor - 1} M_{k2^{-m}} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) - \sum_{k=0,\ \text{step}=2^{m-n}}^{2^{m-n}(\lfloor 2^n T \rfloor - 1)} M_{k2^{-m}} \left(M_{(k+2^{m-n})2^{-m}} - M_{k2^{-m}} \right) \\
= & \sum_{k=0}^{2^{m-n}(\lfloor 2^n T \rfloor - 1)} \underbrace{\left(M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \right)}_{\mathcal{F}_{k2^{-m}}\text{-measurable}} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) + \sum_{k=2^{m-n}(\lfloor 2^n T \rfloor - 1)+1}^{\lfloor 2^m T \rfloor - 1} M_{k2^{-m}} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right).
\end{aligned}$$

Thus, we can find $N \in \mathbb{N}$ such that $\forall m, n \geq N$, $2^{m-n}(\lfloor 2^n T \rfloor - 1) = \lfloor 2^m T \rfloor - 1$ since $2^{-n}(\lfloor 2^n T \rfloor - 1) \uparrow 2^{-m}(\lfloor 2^m T \rfloor - 1)$. So if m, n are sufficiently large, we can ignore the second summation. Thus, we have

$$\begin{aligned}
\|X^n - X^m\|^2 &= \left\| \sum_{k=0}^{\lfloor 2^m T \rfloor - 1} \left(M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \right) \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) \right\|_2^2 \\
&= \mathbb{E} \left(\sum_{k=0}^{\lfloor 2^m T \rfloor - 1} \left(M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \right) \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) \right)^2 \\
&\leq \mathbb{E} \left(\sup_{0 \leq k < \lfloor 2^m T \rfloor} \left| M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \right|^2 \left(\sum_{k=0}^{\lfloor 2^m T \rfloor - 1} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) \right)^2 \right) \\
&\leq \left(\mathbb{E} \left(\sup_{0 \leq k < \lfloor 2^m T \rfloor} \left| M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \right|^2 \right) \right)^{1/2} \left(\mathbb{E} \left(\sum_{k=0}^{\lfloor 2^m T \rfloor - 1} \left(M_{(k+1)2^{-m}} - M_{k2^{-m}} \right) \right)^2 \right)^{1/2}
\end{aligned}$$

by Cauchy-Schwarz inequality (Theorem 19.3.25). The first term tends to 0 since $M_{k2^{-m}} - M_{2^{-n}\lfloor k2^{-m+n} \rfloor} \to 0$ as $m, n \to \infty$. The second term is bounded by Lemma 20.5.4 since M is bounded. Thus, $\|X^n - X^m\| \to 0$, i.e., X^n is a Cauchy sequence in $(\mathcal{M}_c^2, \|\cdot\|)$. Thus, by Proposition 23.1.4.(iii), X^n converges to a limit $Y = (Y_t)_{t \geq 0} \in \mathcal{M}_c^2$.

Now, for any n and $1 \leq k \leq \lfloor 2^n T \rfloor$, by definition of X_t^n,

$$\begin{aligned}
(M_{k2^{-n}})^2 - 2X_{k2^{-n}}^n &= \sum_{j=0}^{k-1} \left(M_{(j+1)2^{-n}}^2 - M_{j2^{-n}}^2 \right) - 2 \sum_{j=0}^{k-1} M_{j2^{-n}} (M_{(j+1)2^{-n}} - M_{j2^{-n}}) \\
&= \sum_{j=0}^{k-1} (M_{(j+1)2^{-n}} - M_{j2^{-n}})^2 = [M]_{k2^{-n}}^n. \qquad (\dagger)
\end{aligned}$$

Hence, $M_t^2 - 2X_t^n$ is increasing along the sequence of times $(k2^{-n}, 1 \leq k \leq \lfloor 2^n T \rfloor)$. Passing to the limit $n \to \infty$, since $M_t, X_t^n \in \mathcal{M}_c^2$, by right-continuuos of M_t and X_t^n, $M_t^2 - 2X_t^n$ must be a.s. increasing. Define

$$\Omega' = \left\{ \omega : M^2(\omega) - 2Y(\omega) \text{ is increasing} \right\} = \left\{ \omega : M^2(\omega) - 2X^n(\omega) \text{ is increasing} \right\} \bigcap \{ \omega : Y(\omega) \text{ exists} \} \tag{23.1.38}$$

Obviously, we have $\mathbb{P}(\Omega') = 1$. Thus, for $t \in [0, T]$, set

$$[M]_t := \begin{cases} M_t^2 - 2Y_t & \omega \in \Omega', \\ 0 & \omega \in \Omega'^c \end{cases} = \left(M_t^2 - 2Y_t \right) \mathbb{1}_{\{\omega \in \Omega'\}}. \tag{23.1.39}$$

Therefore, $[M]$ is pathwise continuous increasing (even on the set Ω'^c which gives $[M] = 0$). For integrability, for any $t \in [0, T]$,

$$\mathbb{E} \left| M^2 - [M]_t \right| = 2\mathbb{E} |Y_t| < \infty \quad \text{as } Y_t \in \mathcal{M}_c^2. \tag{23.1.40}$$

Since the filtration satisfies the usual conditions, $\left(M_t^2 - 2Y_t \right) \mathbb{1}_{\{\omega \in \Omega'\}}$ is $\mathcal{F}_t$-measurable and thus $[M]$ is adapted. Note

that $Y \in \mathcal{M}_c^2$ implies the adaptedness. Also, for any $s \le t$ and $\forall A \in \mathcal{F}_s$, ($M_t^2 - [M]_t = 2Y_t$ a.s. for any t),

$$\mathbb{E}\left(\left(M_t^2 - [M]_t\right)\mathbb{1}_A\right) = \mathbb{E}\left(2Y_t\mathbb{1}_A\right) = \mathbb{E}\left(\mathbb{1}_A\mathbb{E}\left(2Y_t|\mathcal{F}_s\right)\right) = \mathbb{E}\left(\mathbb{1}A2Y_s\right) = \mathbb{E}\left(\left(M_s^2 - [M]_s\right)\mathbb{1}_A\right). \tag{23.1.41}$$

since $Y \in \mathcal{M}_c^2$. Thus, we have $\mathbb{E}\left(M_t^2 - [M]_t|\mathcal{F}_s\right) = M_s^2 - [M]_s$ a.s.. Hence, $[M]$ is a pathwise continuous increasing process and $M^2 - [M]$ is a martingale on $[0,T]$.

We now extend the definition of $[M]_t$ to $t \in [0,\infty)$ by applying the foregoing for all $T \in \mathbb{N}$. Note that the process $[M]$ obtained with T is the restriction to $[0,T]$ of $[M]$ defined with $T+1$.

By $(*)$ and $(\dagger)$, we have

$$[M]_t^n = [M]_{2^{-n}\lfloor 2^n t\rfloor}^n = M_{2^{-n}\lfloor 2^n t\rfloor}^2 - 2X_{2^{-n}\lfloor 2^n t\rfloor}^n, \qquad [M]_t = M_t^2 - 2Y_t. \tag{23.1.42}$$

Thus, $\forall t \ge 0$, since $X^n, M \in \mathcal{M}_c^2$, we have X^n and M^2 are uniformly continuous on $[0,t]$[9] a.s., i.e.,

$$\begin{cases} \sup_{0\le s\le t}\left|X_{2^{-n}\lfloor 2^n s\rfloor}^n - X_s^n\right| \to 0 \ \text{ a.s.} \\ \sup_{0\le s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - M_s^2\right| \to 0 \ \text{ a.s.} \end{cases} \Rightarrow \begin{cases} \left\|\sup_{0\le s\le t}\left|X_{2^{-n}\lfloor 2^n s\rfloor}^n - X_s^n\right|\right\|_2 \to 0 \\ \left\|\sup_{0\le s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - M_s^2\right|\right\|_2 \to 0 \end{cases} \tag{23.1.43}$$

by Theorem 20.5.14.,

Note that $X^n \to Y$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$, equivalently, $X^n \to Y$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$, i.e.,

$$\left\|\sup_{0\le s\le t}|X_s^n - Y_s|\right\|_2 = |||X^n - Y||| \to 0. \tag{23.1.44}$$

By Markov inequality (Theorem 19.3.20), Proposition 15.4.5 and Hölder's inequality (Theorem 19.3.24),

$$\begin{aligned} \mathbb{P}\left(\sup_{s\le t}|[M]_s^n - [M]_s| > \varepsilon\right) &\le \frac{\mathbb{E}\left(\sup_{s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - 2X_{2^{-n}\lfloor 2^n s\rfloor}^n - \left(M_s^2 - 2Y_s\right)\right|\right)}{\varepsilon} \\ &\le \frac{\left\|\sup_{s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - 2X_{2^{-n}\lfloor 2^n s\rfloor}^n - \left(M_s^2 - 2Y_s\right)\right|\right\|_2}{\varepsilon} \\ &\le \frac{\left\|\sup_{s\le t}\left|X_{2^{-n}\lfloor 2^n s\rfloor}^n - X_s^n\right| + \sup_{s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - M_s^2\right| + \sup_{s\le t}|X_s^n - Y_s|\right\|_2}{\varepsilon} \\ &\le \frac{\left\|\sup_{s\le t}\left|X_{2^{-n}\lfloor 2^n s\rfloor}^n - X_s^n\right|\right\|_2 + \left\|\sup_{s\le t}\left|M_{2^{-n}\lfloor 2^n s\rfloor}^2 - M_s^2\right|\right\|_2 + \left\|\sup_{s\le t}|X_s^n - Y_s|\right\|_2}{\varepsilon} \to 0. \end{aligned}$$

Thus $[M]^n \xrightarrow{ucp} [M]$. For $[M]_0$, let $t = 0$, for any $\varepsilon > 0$,

$$\mathbb{P}\left(|[M]_0| > \varepsilon\right) = \mathbb{P}\left(|[M]_0^n - [M]_0| > \varepsilon\right) = \mathbb{P}\left(\sup_{0\le s\le 0}|[M]_s^n - [M]_s| > \varepsilon\right) \to 0 \ \text{ as } n \to \infty. \tag{23.1.45}$$

Thus, $\mathbb{P}\left(|[M]_0| > \varepsilon\right) = 0$ and thus

$$\mathbb{P}\left([M]_0 \ne 0\right) = \mathbb{P}\left(|[M]_0| > 0\right) = \mathbb{P}\left(\bigcup_{n\in\mathbb{N}}\left\{|[M]_0| > \frac{1}{n}\right\}\right) \le \sum_{n\in\mathbb{N}}\mathbb{P}\left(|[M]_0| > \frac{1}{n}\right) = \sum_{n\in\mathbb{N}} 0 = 0. \tag{23.1.46}$$

So we have $[M_0] = 0$ a.s. and the theorem is proved when M is bounded.

Now we turn to the general case $M \in \mathcal{M}_{c,loc}$. Define[10]

$$T_n := \inf\left\{t \ge 0 : |M_t| \ge n\right\}. \tag{23.1.47}$$

By Proposition 20.6.13, $(T_n)_{n\in\mathbb{N}}$ reduces M and we can apply the bounded case to M^{T_n}, writing $A^n = \left[M^{T_n}\right]$.

By uniqueness, $A_{t\wedge T_n}^{n+1} = \left[M^{T_{n+1}}\right]_{t\wedge T_n} = \left[M^{T_{n+1}}\right]_t^{T_n}$ and $A_t^n = \left[M^{T_n}\right]_t$ are indistinguishable. Thus there exists a

[9] need theorem here

[10] should say $M_0 = 0$ a.s.

continuous increasing process A such that for all $n \in \mathbb{N}$, ($A_t = [M^{T_n}]_t$ for all $n \in \mathbb{N}$)

$$A_{t\wedge T_n} = A_t^{T_n} = \left[M^{T_{n+1}}\right]_t^{T_n} \quad \text{and} \quad A_t^n = \left[M^{T_n}\right]_t \text{ are indistinguishable.} \tag{23.1.48}$$

Define $[M]_t = A_t$. By construction, for any $t \geq 0$,

$$\left(M_t^2 - [M]_t\right)^{T_n} = M_{t\wedge T_n}^2 - [M]_t^{T_n} = \left(M_t^{T_n}\right)^2 - A_{t\wedge T_n} = \left(M_t^{T_n}\right)^2 - [M^{T_n}]_t \in \mathcal{M}_c \tag{23.1.49}$$

since M^{T_n} is bounded martingale. Thus, we know that T_n also reduces $\left(M_t^2 - [M]_t\right)_{t\geq 0}$ and it is a local martingale. that is $\left(M_t^2 - A_t\right)_{t\geq 0} \in \mathcal{M}_{c,loc}$, as required.

It remains to show that $[M]$ is the u.c.p. limit of its dyadic approximations. Let $[M]^m$ be the dyadic approximation at stage m. Note that for fixed $n \geq 0$, we have $\left[M^{T_n}\right]^m \to \left[M^{T_n}\right]$ u.c.p. as $m \to \infty$ by the bounded case. Since for all fixed $t \geq 0$, $\mathbb{P}(T_n \leq t) \to 0$ as $n \to \infty$, we obtain that $\forall \varepsilon > 0, \forall t \geq 0$,

$$\begin{aligned}
\mathbb{P}\left(\sup_{s\leq t} |[M]_s^m - [M]_s| > \varepsilon\right) &= \mathbb{P}\left(\left\{\sup_{s\leq t} |[M]_s^m - [M]_s| > \varepsilon,\ T_n \leq t\right\} \bigcup \left\{\sup_{s\leq t} |[M]_s^m - [M]_s| > \varepsilon,\ T_n > t\right\}\right) \\
&= \mathbb{P}\left(\left\{\sup_{s\leq t} |[M]_s^m - [M]_s| > \varepsilon,\ T_n \leq t\right\} \bigcup \left\{\sup_{s\leq t} \left|\left[M^{T_n}\right]_s^m - \left[M^{T_n}\right]_s\right| > \varepsilon,\ T_n > t\right\}\right) \\
&\leq \mathbb{P}\left(T_n \leq t\right) + \mathbb{P}\left(\sup_{s\leq t} \left|\left[M^{T_n}\right]_s^m - \left[M^{T_n}\right]_s\right| > \varepsilon\right) \to 0 + 0 = 0.
\end{aligned}$$

Thus, $[M]^m \xrightarrow{ucp} [M]$ as $m \to \infty$. □

Proposition 23.1.8. Let T be a stopping time and $M \in \mathcal{M}_{c,loc}$. Then $\left[M^T\right] = [M]^T$ (up to indistinguishability).

Proof. By Proposition 20.6.2, $M^T \in \mathcal{M}_{c,loc}$. Thus, by Theorem 23.1.7,

$$M^2 - [M],\ \left(M^T\right)^2 - \left[M^T\right] \in \mathcal{M}_{c,loc} \ \Rightarrow\ \left(M^2 - [M]\right)^T = \left(M^T\right)^2 - [M]^T \in \mathcal{M}_{c,loc} \tag{23.1.50}$$

For $M^T \in \mathcal{M}_{c,loc}$, there exists unique continuous non-decreasing process A such that $\left(M^T\right)^2 - A \in \mathcal{M}_{c,loc}$. Thus,

$$A = \left[M^T\right] = [M]^T \tag{23.1.51}$$

in the sence of indistinguishability. □

Since the quadratic variation is unchanged by the addition of a constant to M, we may assume wlog that $M_0 = 0$ a.s..

Theorem 23.1.9. If $M \in \mathcal{M}_c^2$ and $M_0 = 0$ a.s.. Then $\mathbb{E}([M]_\infty) = \mathbb{E}(M_\infty^2)$ and $M^2 - [M]$ is a uniformly integrable martingale.

Proof. First we have $M \in \mathcal{M}_{c,loc}$ and let $S_n = \inf\{t \geq 0 : |M|_t \geq n\}$. Then by Proposition 20.4.6, S_n is a stopping time and $[M]_{t\wedge S_n} \leq n$. Also, with the similar argument in Proposition 20.6.13, we have $S_n \uparrow \infty$ a.s. and $(S_n)_{n\geq 0}$ reduces M. Thus, M^{S_n} is bounded martingale and thus $M_{t\wedge S_n}^2 - [M^{S_n}]_t \in \mathcal{M}_c$ by Theorem 23.1.7. Thus as $M_0 = 0$ a.s. and $[M]_0 = 0$ a.s., for all $t \geq 0$,

$$0 = \mathbb{E}\left(M_0^2 - [M]_0\right) = \mathbb{E}\left(M_{S_n\wedge 0}^2 - [M]_{0\wedge S_n}\right) \underbrace{= \mathbb{E}\left(\left(M^{S_n}\right)_0^2 - \left[M^{S_n}\right]_0\right)}_{\text{Proposition 23.1.8}} = \mathbb{E}\left(\left(M^{S_n}\right)_t^2 - \left[M^{S_n}\right]_t\right) = \mathbb{E}\left(M_{S_n\wedge t}^2 - [M]_{t\wedge S_n}\right)$$

which gives that

$$\mathbb{E}\left([M]_{t\wedge S_n}\right) = \mathbb{E}(M_{t\wedge S_n}^2) \quad \text{for all } t \geq 0. \qquad (*) \tag{23.1.52}$$

Since $M \in \mathcal{M}_c^2$, M_∞ exists and $M_t \to M_\infty$ a.s. by Theorem 20.5.14. We take the limit $t \to \infty$ ($t \wedge S_n \uparrow \infty$ a.s.) using monotone convergence theorem (Theorem 19.3.6) on the left and dominated convergence theorem (Theorem 19.3.8) on the right, and then $n \to \infty$ by the same arguments to get

$$\mathbb{E}\left([M]_\infty\right) = \mathbb{E}\left(M_\infty^2\right) < \infty. \qquad (\dagger) \tag{23.1.53}$$

Hence, $\left|M_t^2-[M]_t\right|$ is dominated by $\sup_{t\geq 0}M_t^2+[M]_\infty$ which is integrable. Thus by Corollary 20.6.8, $M^2-[M]$ is a true martingale. Also,

$$\begin{aligned}\mathbb{E}\left(\sup_{t\geq 0}\left|M_t^2-[M]_t\right|\right) &\leq \mathbb{E}\left(\sup_{t\geq 0}M_t^2+\sup_{t\geq 0}[M]_t\right)\leq \mathbb{E}\left(\sup_{t\geq 0}M_t^2\right)+\mathbb{E}\left([M]_\infty\right)\\ &\leq 4\mathbb{E}\left(M_\infty^2\right)+\mathbb{E}\left(M_\infty^2\right)=5\mathbb{E}\left(M_\infty^2\right)<\infty.\end{aligned}$$

by Corollary 20.5.10. Then $M_t^2-[M]_t$ is uniformly integrable by Definition 19.3.6. □

Theorem 23.1.10. If $M\in\mathcal{M}_{c,loc}$ with $M_0=0$ a.s.. Then $M\in\mathcal{M}_c^2$ if and only if $\mathbb{E}\left([M]_\infty\right)<\infty$.

Proof. ($\Rightarrow$). It is proved by (†) in Theorem 23.1.9.

($\Leftarrow$). With the same argument, we have ($*$) in Theorem 23.1.9. By Fatou lemma (Lemma 19.3.7),

$$\mathbb{E}(M_t^2)=\mathbb{E}\left(\lim_{n\to\infty}M_{t\wedge S_n}^2\right)=\mathbb{E}\left(\liminf_n M_{t\wedge S_n}^2\right)\leq\liminf_n\mathbb{E}\left(M_{t\wedge S_n}^2\right)=\liminf_n\mathbb{E}\left([M]_{t\wedge S_n}\right)\leq\mathbb{E}\left([M]_t\right). \tag{23.1.54}$$

Thus, since $[M]$ is non-decreasing,

$$\sup_{0\leq s\leq t}\mathbb{E}(M_s^2)\leq\mathbb{E}\left([M]_t\right)\leq\mathbb{E}\left([M]_\infty\right)<\infty. \tag{23.1.55}$$

Thus, for any stopping time $S\leq t$, the stopped local martingale M^S, $\forall t\geq 0$,

$$\left\|M_{S\wedge t}^2\right\|_2\leq\left(\sup_{0\leq s\leq t}\mathbb{E}\left(M_s^2\right)\right)^{1/2}<\infty. \tag{23.1.56}$$

Thus, M_t^S is bounded in $\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$ and thus UI (by Proposition 19.3.32). Thus, M is, in fact, a true martingale (by Proposition 20.6.6). Also, $\sup_{0\leq s\leq t}\mathbb{E}(M_s^2)\leq\mathbb{E}\left([M]_\infty\right)$ implies that

$$\sup_{t\geq 0}\mathbb{E}(M_t^2)\leq\mathbb{E}\left([M]_\infty\right)<\infty. \tag{23.1.57}$$

Thus, M is bounded in $\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$ and $M\in\mathcal{M}_c^2$. □

Corollary 23.1.11. Let H be a non-negative locally bounded previsible process and $M\in\mathcal{M}_{c,loc}$. Then $H\cdot[M]$ is adapted, (pathwise) continuous (càdlàg) and (pathwise) non-decreasing.

Proof. This is direct result from Theorem 20.4.21 for the case that H is non-negative and A is non-decreasing. The (pathwise) continuity is from ($**$) in proof of Theorem 20.4.21. □

23.1.3 Itô stochastic integrals for $\mathcal{L}^2(M)$ with $M\in\mathcal{M}_c^2$

Proposition 23.1.12. Let μ be a finite measure on the previsible σ-algebra $\mathcal{P}$. Then the simple process space $\mathcal{S}$ is a dense[11] subspace of $\mathcal{L}^2(\Omega\times(0,\infty),\mathcal{P},\mu)$.

Proof. If $H\in\mathcal{S}$ then H is bounded so $H\in\mathcal{L}^2(\Omega\times(0,\infty),\mathcal{P},\mu)$ an thus $S\subseteq\mathcal{L}^2(\Omega\times(0,\infty),\mathcal{P},\mu)$. Denote by $\overline{\mathcal{S}}$ the closure of $\mathcal{S}$ in $\mathcal{L}^2(\Omega\times(0,\infty),\mathcal{P},\mu)$. Since linear combinations of indicator functions of the form 1_A for $A\in\mathcal{P}$ are dense in $\mathcal{L}^2(\mathcal{P},\mu)$ by measure theory (for any measurable function f, $2^{-n}\lfloor 2^n f\rfloor$ is simple function), it suffices to prove that if $A\in\mathcal{P}$, then $\mathbb{1}_A\in\overline{\mathcal{S}}$. Set

$$\mathcal{A}=\left\{A\in\mathcal{P}:\mathbb{1}_A\in\overline{\mathcal{S}}\right\}. \tag{23.1.58}$$

Then $\mathcal{A}$ is d-system. To see this,

(i) $\mathbb{1}_{\Omega\times(0,n)}\in\mathcal{S}\ \Rightarrow\ \mathbb{1}_{\Omega\times(0,\infty)}\in\overline{\mathcal{S}}$. Thus, $\Omega\times(0,\infty)\in\mathcal{A}$.

(ii) If $C\subseteq D\in\mathcal{A}$, then $\mathbb{1}_C\in\overline{\mathcal{S}}$ and $\mathbb{1}_D\in\overline{\mathcal{S}}$. Thus, there are $C_n\subseteq D_n\in\mathcal{A}$ such that $\mathbb{1}_{C_n}\downarrow\mathbb{1}_C$ and $\mathbb{1}_{D_n}\uparrow\mathbb{1}_D$. Therefore, $\mathbb{1}_{D_n}-\mathbb{1}_{C_n}\uparrow\mathbb{1}_D-\mathbb{1}_C=\mathbb{1}_{D\setminus C}$. Since $\mathcal{S}$ is vector space, then $\mathbb{1}_{D_n}-\mathbb{1}_{C_n}\in\mathcal{S}$. Thus, $\mathbb{1}_{D\setminus C}\in\overline{\mathcal{S}}$.

[11] need definition

(iii) If $C_n \in \mathcal{A}$ and $C_n \uparrow C$, we have $\mathbb{1}_{C_n} \in \overline{\mathcal{S}}$. Since $\mathcal{S}$ is vector space, there exist $D_m^n \in \mathcal{S}$ such that $\mathbb{1}_{D_m^n} \uparrow \mathbb{1}_{C_n}$ as $m \to \infty$. Thus, let $B_k = D_k^k \in \mathcal{S}$ such that $\mathbb{1}_{B_k} \uparrow \mathbb{1}_C$. Therefore, $\mathbb{1}_C \in \overline{\mathcal{S}}$.

Moreover $\mathcal{A}$ contains the π-system $\{B \times (s,t] : B \in \mathcal{F}_s, s \leq t\}$, which generates $\mathcal{P}$. Hence, by Dynkin's lemma, $\mathcal{P} \subseteq \mathcal{A}$. Thus, $\mathcal{A} = \mathcal{P}$. □

Definition 23.1.6. Given $M \in \mathcal{M}_c^2$, define a measure μ on $\mathcal{P}$ by

$$\mu\left(A \times (s,t]\right) = \mathbb{E}\left(\mathbb{1}_A\left([M]_t - [M]_s\right)\right) \quad \text{for all } s < t, A \in \mathcal{F}_s. \tag{23.1.59}$$

Since $\mathcal{P}$ is generated by the π-system of events of this form, this uniquely specifies μ. Alternatively, write

$$\mu\left(d\omega \otimes dt\right) = d[M](\omega, dt)\mathbb{P}(d\omega), \tag{23.1.60}$$

where for a fixed ω, $d[M](\omega,\cdot)$ is the Lebesgue-Stieltjes measure associated to the non-decreasing function $[M](\omega)$ (by Theorem 23.1.7 and Theorem 15.2.11). Thus, for a previsible process $H \geq 0$,

$$\int_{\Omega\times(0,\infty)} H d\mu = \mathbb{E}\left(\int_0^\infty H_s d[M]_s\right). \tag{23.1.61}$$

Definition 23.1.7. Given $M \in \mathcal{M}_c^2$, we set $\mathcal{L}^2(M) = \mathcal{L}^2\left(\Omega \times (0,\infty), \mathcal{P}, \mu\right)$ and write

$$\|H\|_M^2 = \|H\|_{\mathcal{L}^2(M)}^2 = \mathbb{E}\left(\int_0^\infty H_s^2 d[M]_s\right) = \mu(H^2), \tag{23.1.62}$$

so that $\mathcal{L}^2(M)$ is the space of previsible processes H such that $\|H\|_M^2 < \infty$.

Remark. (i) Note that the simple processes $\mathcal{S} \subseteq \mathcal{L}^2(M)$ for all $M \in \mathcal{M}_c^2$. Now, recall that if $M \in \mathcal{M}_c^2$ we defined $\|M\|^2 = \mathbb{E}(M_\infty^2)$.

(ii) Thus, the measure $\mu\left(\Omega \times (0,\infty)\right) = \|1\|_M^2 < \infty$ since $1 \in \mathcal{S} \subseteq \mathcal{L}^2(M)$.

Theorem 23.1.13 (Itô isometry)**.** For every $M \in \mathcal{M}_c^2$ there exists a unique isometry $I : (\mathcal{L}^2(M), \|\cdot\|_M) \to (\mathcal{M}_c^2, \|\cdot\|)$ such that $I(H) = H \cdot M$ for all $H \in \mathcal{S}$. Also, $I(H) \in \mathcal{M}_c^2$ for all $H \in \mathcal{L}^2(M)$ and $I(H)_0 = 0$ a.s..

Proof. Let $H = \sum_{k=0}^{n-1} Z_k \mathbb{1}_{(t_k, t_{k+1}]} \in \mathcal{S}$. By Proposition 23.1.3, $H \cdot M \in \mathcal{M}_c^2$ with

$$\|H \cdot M\|^2 = \|(H \cdot M)_\infty\|_2^2 = \sum_{k=0}^{n-1} \mathbb{E}\left(Z_k^2 (M_{t_{k+1}} - M_{t_k})^2\right) \qquad \text{(by } (*) \text{ in Proposition 23.1.3)} \tag{23.1.63}$$

But $M^2 - [M]$ is a martingale since $M \in \mathcal{M}_c^2$ by Theorem 23.1.9. Thus,

$$\mathbb{E}\left(Z_k^2 (M_{t_{k+1}} - M_{t_k})^2\right) = \mathbb{E}\left(Z_k^2 \mathbb{E}\left((M_{t_{k+1}} - M_{t_k})^2 | \mathcal{F}_{t_k}\right)\right) = \mathbb{E}\left(Z_k^2 \mathbb{E}\left(M_{t_{k+1}}^2 - M_{t_k}^2 | \mathcal{F}_{t_k}\right)\right) = \mathbb{E}\left(Z_k^2 ([M]_{t_{k+1}} - [M]_{t_k})\right),$$

and so by Theorem 15.3.10.(i) (or Fubini theorem (Theorem 15.3.33) if we consider summatio as a σ-finite integral),

$$\begin{aligned} \|H \cdot M\|^2 &= \sum_{k=0}^{n-1} \mathbb{E}\left(Z_k^2 ([M]_{t_{k+1}} - [M]_{t_k})\right) = \sum_{k=0}^{n-1} \mathbb{E}\left(\int_0^\infty Z_k^2 \mathbb{1}_{(t_k, t_{k+1}]} d[M]_s\right) \\ &= \mathbb{E}\left(\int_0^\infty \sum_{k=0}^{n-1} Z_k^2 \mathbb{1}_{(t_k, t_{k+1}]} d[M]_s\right) = \mathbb{E}\left(\int_0^\infty H_s^2 d[M]_s\right) = \|H\|_M^2. \end{aligned}$$

Now let $H \in \mathcal{L}^2(M)$. We have thus defined a function I from $\mathcal{S}$ to $\mathcal{M}_c^2$, which is an isometry, say $I(H) = H \cdot M$.

However, $\mathcal{S}$ is dense in $\mathcal{L}^2(M) = \mathcal{L}^2(\Omega \times (0,\infty), \mathcal{P}, \mu)$ by Proposition 23.1.12. This implies that there is a unique way to extend I to $\mathcal{L}^2(M)$ which makes I into an isometry.

Indeed, let $H \in \mathcal{L}^2(M)$. Then there exists a sequence of simple processes $H^n \in \mathcal{S}$ such that $H^n \to H$ in $\mathcal{L}^2(M)$. Then by linearity and $H^n - H^m \in \mathcal{S}$,

$$\|I(H^n) - I(H^m)\| = \|I(H^n - H^m)\| = \|H^n - H^m\|_M. \tag{23.1.64}$$

Thus $I(H^n)$ is a Cauchy sequence in $(\mathcal{M}_c^2, \|\cdot\|)$, which is complete (by Theorem 23.1.4.(iii)). Therefore, $I(H^n)$ converges to some limit which we may denote by $I(H) \in \mathcal{M}_c^2$.

It is easy to check that $I(H)$ does not depend on the sequence H^n chosen to approximate H. if $H^n \to H$ and $K^n \to H$ in $\mathcal{L}^2(M)$ ($H^n, K^n \in \mathcal{S}$), then by linearity of $\mathcal{S}$ and Minkowski's inequality (Theorem 15.4.8 as $\|H\|_M = \left(\mu\left(H^2\right)\right)^{1/2}$),

$$\|I(H^n) - I(K^n)\| = \|I(H^n - K^n)\| = \|H^n - K^n\|_M \leq \|H^n - H\|_M + \|K^n - H\|_M + \|H - H\|_M \to 0 \tag{23.1.65}$$

as $n \to \infty$, so for the limits of $I(H^n)$ and $I(K^n)$, say $I(H')$ and $I(H'')$,

$$\|I(H') - I(H'')\| = 0 \;\Rightarrow\; I(H') - I(H'') \text{ is indistinguishable from } 0 \tag{23.1.66}$$

by the fact that $(\mathcal{M}_c^2, \|\cdot\|)$ is a Hilbert space. Thus, the two limits must be indistinguishable. $I(H)$ is then, indeed, an isometry on $\mathcal{L}^2(M)$. For $H \in \mathcal{S}$ we have consistently $I(H) = H \cdot M$ by choosing $H^n \equiv H$.

In particular, by the argument above, for $H^n \to H$ with $H^n \in \mathcal{S}$, the fact $\|H^n \cdot M - I(H)\| \to 0$ implies that

$$\left\||H^n \cdot M - I(H)|_0\right\|_2 \leq \left\|\sup_{t\geq 0} |H^n \cdot M - I(H)|_t\right\|_2 = \left\|\left|H^n \cdot M - I(H)\right|\right\| \leq 2\|H^n \cdot M - I(H)\| \to 0 \tag{23.1.67}$$

But $(H^n \cdot M)_0 = 0$ by Definition 23.1.3. Thus, $\|I(H)_0\|_2 = 0$, then $I(H)_0 = 0$ a.s. □

Definition 23.1.8 (Itô's stochastic integral)**.** We write

$$I(H)_t = (H \cdot M)_t = \int_0^t H_s dM_s \tag{23.1.68}$$

for all $H \in \mathcal{L}^2(M)$ with $(H \cdot M)_0 = 0$ a.s. The process $H \cdot M$ is Itô's stochastic integral of H with respect to M. Note that from Theorem 23.1.13, $(H \cdot M)_t \in \mathcal{M}_c^2$.

Remark. By Theorem 23.1.13, this is consistent with our previous definition of $H \cdot M$ for $H \in \mathcal{S}$.

Proposition 23.1.14. Let $M \in \mathcal{M}_c^2$ and $H \in \mathcal{L}^2(M)$. Let T be a stopping time. Then $H\mathbb{1}_{(0,T]} \in \mathcal{L}^2(M)$ and $H \in \mathcal{L}^2(M^T)$, and we have

$$(H \cdot M)^T = (H\mathbb{1}_{(0,T]}) \cdot M = H \cdot (M^T). \tag{23.1.69}$$

Proof. Let $H \in \mathcal{L}^2(M)$ and H is previsible.

We see that $\mathbb{1}_{(0,T]}(t)$ is left-continuous and hence previsible (Theorem 20.4.17) and thus $H\mathbb{1}_{(0,T]}$ is previsible. Also,

$$\left\|H\mathbb{1}_{(0,T]}\right\|_M = \mu\left(H^2\mathbb{1}_{(0,T]}\right) \leq \mu\left(H^2\right) = \|H\|_M < \infty. \tag{23.1.70}$$

Thus, $H\mathbb{1}_{(0,T]} \in \mathcal{L}^2(M)$.

By Proposition 23.1.8, $\left[M^T\right] = [M]^T$ (in the sense of distinguishability),

$$\mathbb{E}\left(\int_0^\infty H_s^2 d\left[M^T\right]_s\right) = \mathbb{E}\left(\int_0^\infty H_s^2 d[M]_s^T\right) = \mathbb{E}\left(\int_0^T H_s^2 d[M]_s\right) = \mu\left(H\mathbb{1}_{(0,T]}\right) \leq \mu(H) = \mathbb{E}\int_0^\infty H_s^2 d[M]_s < \infty.$$

Thus, $H \in \mathcal{L}^2(M^T)$.

Step 1. Take $M \in \mathcal{M}_c^2$ and suppose first that $H = \sum_{k=0}^{n-1} Z_k \mathbb{1}_{(t_k, t_{k+1}]} \in \mathcal{S}$. If T takes only finitely many values, $H\mathbb{1}_{(0,T]} \in \mathcal{S}$ and

$$(H \cdot M)_t^T = \sum_{k=0}^{n-1} Z_k \left(M_{t_{k+1}\wedge t\wedge T} - M_{t_k \wedge t \wedge T}\right) = \sum_{k=0}^{n-1} Z_k \mathbb{1}_{(0,T]}\left(M_{t_{k+1}\wedge t} - M_{t_k \wedge t}\right) = (H\mathbb{1}_{(0,T]}) \cdot M. \tag{23.1.71}$$

For general T, set $T_n = \left(2^{-n}\lfloor 2^n T\rfloor\right) \wedge n$ which is a stopping time (see proof of Proposition 20.4.4) that takes only finitely many values

$$(H \cdot M)_t^{T_n} = \left(H\mathbb{1}_{(0,T_n]}\right) \cdot M. \qquad (*) \tag{23.1.72}$$

Then $T_n \uparrow T$ as $n \to \infty$, this gives that $\mathbb{1}_{(0,T_n]} \uparrow \mathbb{1}_{(0,T]}$ and

$$\left\|H\mathbb{1}_{(0,T_n]} - H\mathbb{1}_{(0,T]}\right\|_M^2 = \mathbb{E}\left(\int_0^\infty H_t^2 (\mathbb{1}_{(0,T_n]} - \mathbb{1}_{(0,T]})^2(t) d[M]_t\right) = \mu\left(H^2\mathbb{1}_{(T_n,T]}\right) = \mu\left(H^2\mathbb{1}_{(0,T]}\right) - \mu\left(H^2\mathbb{1}_{(0,T_n]}\right) \to 0$$

as $n \to \infty$, by dominated convergence theorem (Theorem 19.3.8), and so

$$H\mathbb{1}_{(0,T_n]} \cdot M \to H\mathbb{1}_{(0,T]} \cdot M \text{ in } \mathcal{M}_c^2 \text{ by Theorem 23.1.13} \Leftrightarrow \left\|\left(H\mathbb{1}_{(0,T_n]}\right) \cdot M - \left(H\mathbb{1}_{(0,T]}\right) \cdot M\right\| \to 0. \quad (\dagger) \tag{23.1.73}$$

By Proposition 23.1.3, $H \cdot M \in \mathcal{M}_c^2$, thus $(H \cdot M)_t^{T_n} \to (H \cdot M)_t^T$ a.s. for any $t \geq 0$ by continuity. Thus,

$$\left((H \cdot M)_t^{T_n} - (H \cdot M)_t^T\right)^2 \to 0 \text{ a.s. } \Rightarrow \mathbb{E}\left(\left((H \cdot M)_t^{T_n} - (H \cdot M)_t^T\right)^2\right) \to 0 \Rightarrow \left\|(H \cdot M)_t^{T_n} - (H \cdot M)_t^T\right\|_2 \to 0$$

by dominated convergence theorem (Theorem 19.3.8). Then for any $t \geq 0$,

$$\left\|(H \cdot M)^{T_n} - (H \cdot M)^T\right\| = \left\|(H \cdot M)_\infty^{T_n} - (H \cdot M)_\infty^T\right\|_2 \leq \sup_{t \geq 0}\left\|(H \cdot M)_t^{T_n} - (H \cdot M)_t^T\right\|_2 \to 0. \tag{23.1.74}$$

Hence, as $H \cdot M \in \mathcal{M}_c^2$ and $(H \cdot M)^T \in \mathcal{M}_c^2$,

$$\begin{aligned}
\left\|(H \cdot M)^T - (H\mathbb{1}_{(0,T]}) \cdot M\right\| &\leq \left\|(H \cdot M)^{T_n} - (H \cdot M)^T\right\| + \left\|(H \cdot M)^{T_n} - \left(H\mathbb{1}_{(0,T]} \cdot M\right)\right\| \\
&= \left\|(H \cdot M)^{T_n} - (H \cdot M)^T\right\| + \left\|\left(H\mathbb{1}_{(0,T_n]}\right) \cdot M - \left(H\mathbb{1}_{(0,T]}\right) \cdot M\right\| \qquad \text{(by } (*)\text{)} \\
&\to 0 + 0 = 0. \qquad \text{(by } (\dagger)\text{)}
\end{aligned}$$

Hence, $(H \cdot M)^T = (H\mathbb{1}_{(0,T]}) \cdot M$. On the other hand we already know $(H \cdot M)^T = H \cdot (M^T)$ by Proposition 23.1.4.

Step 2. Now for $H \in \mathcal{L}^2(M)$, we can choose a sequence of processes $H^n \in \mathcal{S}$ such that $H^n \to H$ in $\mathcal{L}^2(M)$. Then $H^n \cdot M \to H \cdot M$ in $\mathcal{M}_c^2$ by Theorem 23.1.13, so $(H^n \cdot M)^T \to (H \cdot M)^T$ in $\mathcal{M}_c^2$ by Lemma 23.1.5. That is,

$$\left\|(H^n \cdot M)^T - (H \cdot M)^T\right\| \to 0. \qquad (\dagger\dagger) \tag{23.1.75}$$

Also,

$$\left\|H^n\mathbb{1}_{(0,T]} - H\mathbb{1}_{(0,T]}\right\|_M^2 = \mathbb{E}\left(\int_0^T (H^n - H)_s^2 d[M]_s\right) \leq \mathbb{E}\left(\int_0^\infty (H^n - H)_s^2 d[M]_s\right) = \|H^n - H\|_M^2 \to 0 \tag{23.1.76}$$

as $n \to \infty$, so $\left(H^n\mathbb{1}_{(0,T]}\right) \cdot M \to \left(H\mathbb{1}_{(0,T]}\right) \cdot M$ in $\mathcal{M}_c^2$ by the isometry property of Theorem 23.1.13. That is,

$$\left\|(H^n\mathbb{1}_{(0,T]}) \cdot M - (H\mathbb{1}_{(0,T]}) \cdot M\right\| \to 0. \tag{23.1.77}$$

Then since $(H^n \cdot M)^T = (H^n\mathbb{1}_{(0,T]}) \cdot M$,

$$\left\|(H \cdot M)^T - (H\mathbb{1}_{(0,T]}) \cdot M\right\| \leq \left\|(H^n\mathbb{1}_{(0,T]}) \cdot M - (H\mathbb{1}_{(0,T]}) \cdot M\right\| + \left\|(H^n \cdot M)^T - (H \cdot M)^T\right\| \to 0 \tag{23.1.78}$$

So we get $(H \cdot M)^T = \left(H\mathbb{1}_{(0,T]}\right) \cdot M$. Moreover, by Proposition 23.1.8,

$$\|H^n - H\|_{M^T}^2 = \mathbb{E}\left(\int_0^\infty (H^n - H)_s^2 \, d\left[M^T\right]_s\right) = \mathbb{E}\left(\int_0^T (H^n - H)_s^2 d[M]_s\right) \leq \|H^n - H\|_M \to 0, \tag{23.1.79}$$

so $H^n \cdot (M^T) \to H \cdot (M^T)$ in $\mathcal{M}_c^2$. That is,

$$\left\|H^n \cdot (M^T) \to H \cdot (M^T)\right\| \to 0. \tag{23.1.80}$$

Then by $(H^n \cdot M)^T = H^n \cdot (M^T)$ and $(\dagger\dagger)$, we have

$$\begin{aligned}
\left\|(H \cdot M)^T - H \cdot (M^T)\right\| &\leq \left\|H^n \cdot (M^T) - H \cdot (M^T)\right\| + \left\|(H \cdot M)^T - (H^n \cdot M)^T\right\| + \left\|(H^n \cdot M)^T - H^n \cdot (M^T)\right\| \\
&\to 0 + 0 + 0 = 0.
\end{aligned}$$

Hence, $(H \cdot M)^T = H \cdot (M^T)$. □

Proposition 23.1.14 allows us to make a final extension of Itô's integral to locally bounded, previsible integrands.

23.1.4 Stochastic integrals for locally bounded previsible processes with $M \in \mathcal{M}^2_{c,loc}$

Definition 23.1.9 (Itô integral for locally bounded previsible processes)**.** Let H be a locally bounded previsible process reduced by $(S_n)_{n\in\mathbb{N}}$ and $M \in \mathcal{M}_{c,loc}$. Choose stopping times $S'_n = \inf\{t \geq 0 : |M_t| \geq n\} \uparrow \infty$ (see Proposition 20.6.13), and note that $M^{S'_n} \in \mathcal{M}^2_c$ for all $n \in \mathbb{N}$ (since $M^{S'_n}$ is bounded). Set $T_n = S_n \wedge S'_n$ and define

$$(H \cdot M)_t \quad \text{s.t.} \quad (H \cdot M)^{T_n}_t = \left(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}\right)_t \quad \text{for all } t. \tag{23.1.81}$$

with $(H \cdot M)_0 = 0$ a.s. by Definition 23.1.8.

By Theorem 23.1.13, we have $\left(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}\right) \in \mathcal{M}^2_c$. Thus, we have $H \cdot M \in \mathcal{M}_{c,loc}$ by definition of local martingale. The (sample) continuity is given by let $T_n \uparrow \infty$, as $(H \cdot M)^{T_n}_t = (H \cdot M)_t$ for all $t \leq T_n$.

Remark. (i) The stochastic integral in the right-hand side of definition 23.1.9 is well-defined. indeed, every bounded previsible process is in $\mathcal{L}^2(M)$ whenever $M \in \mathcal{M}^2_c$. That is, if $\sup_{t\geq 0} |H| \leq K$ where K is non-random,

$$\|H\|_M = \mathbb{E}\left(\int_0^\infty H_s^2 d[M]_s\right) \leq K^2\mathbb{E}\left(\int_0^\infty d[M]_s\right) = \mathbb{E}\left([M]_\infty\right) < \infty \tag{23.1.82}$$

by Theorem 23.1.10.

(ii) Moreover, $H\mathbb{1}_{(0,T_n]}$ is bounded and $M^{T_n} = (M^{S'_n})^{T_n} \in \mathcal{M}^2_c$, so $H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}$ makes sense (it falls within the category of processes covered by Theorem 23.1.13).

(iii) Proposition 23.1.14 ensures that the right-hand side does not depend on n for all n large enough that $T_n \geq t$.

(iv) It is furthermore consistent with our previous definitions of stochastic integral when $M \in \mathcal{M}^2_c$ and $H \in \mathcal{L}^2(M)$.

Proposition 23.1.15. If H is locally bounded previsible and $M \in \mathcal{M}_{c,loc}$, then for all stopping times T we have

$$(H \cdot M)^T = (H\mathbb{1}_{(0,T]}) \cdot M = H \cdot (M^T). \tag{23.1.83}$$

Proof. By Proposition 23.1.14, we know that

$$(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n})^T = H\mathbb{1}_{(0,T]}\mathbb{1}_{(0,T_n]} \cdot M^{T_n} \tag{23.1.84}$$

As $n \to \infty$, the left-hand side is $(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n})^T = (H \cdot M)^{T_n \wedge T}$. Thus, for any t, we have

$$(H \cdot M)^{T_n \wedge T}_t \to (H \cdot M)^T_t \quad \text{a.s.} \tag{23.1.85}$$

by (sample) continuity of $(H \cdot M)^T$ (by Proposition 20.6.2). For the right-hand side, since the sequence (T_n) also reduce M and imply that $H\mathbb{1}_{(0,T]}\mathbb{1}_{(0,T_n]}$ is bounded. Thus, $H\mathbb{1}_{(0,T]} \cdot M$ is also a (sample) continuous local martingale such that

$$\left(H\mathbb{1}_{(0,T]} \cdot M\right)^{T_n} = H\mathbb{1}_{(0,T]}\mathbb{1}_{(0,T_n]} \cdot M^{T_n} \tag{23.1.86}$$

Thus, for any t, we have by continuity of $H\mathbb{1}_{(0,T]} \cdot M$,

$$\left(H\mathbb{1}_{(0,T]} \cdot M\right)^{T_n}_t \to \left(H\mathbb{1}_{(0,T]} \cdot M\right)_t \quad \text{a.s.} \tag{23.1.87}$$

Combining these equation together, we have

$$\left(H\mathbb{1}_{(0,T]} \cdot M\right)_t = (H \cdot M)^T_t \quad \text{a.s..} \tag{23.1.88}$$

Then by Proposition 20.4.12, $H\mathbb{1}_{(0,T]} \cdot M = (H \cdot M)^T$ in the sense of indistinguishability.
By Proposition 23.1.14, we know that

$$(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n})^T = H\mathbb{1}_{(0,T_n]} \cdot \left(M^{T_n \wedge T}\right) = H\mathbb{1}_{(0,T_n]} \cdot \left(M^T\right)^{T_n} \tag{23.1.89}$$

For the right-hand side, since the sequence (T_n) also reduce M^T (which is also a continuous local martingale by Proposition 20.6.2) and imply that $H\mathbb{1}_{(0,T_n]}$ is bounded. Thus, $H \cdot M^T$ is also a (sample) continuous local martingale such that

$$\left(H \cdot M^T\right)^{T_n} = H\mathbb{1}_{(0,T_n]} \cdot \left(M^T\right)^{T_n} \tag{23.1.90}$$

Thus, for any t, we have by continuity of $H \cdot M^T$,

$$\left(H \cdot M^T\right)_t^{T_n} \to \left(H \cdot M^T\right)_t \quad \text{a.s.} \tag{23.1.91}$$

Combining these equation together, we have

$$\left(H\mathbb{1}_{(0,T]} \cdot M\right)_t = \left(H \cdot M^T\right)_t \quad \text{a.s..} \tag{23.1.92}$$

Then by Proposition 20.4.12, $H\mathbb{1}_{(0,T]} \cdot M = H \cdot M^T$ in the sense of indistinguishability. □

Theorem 23.1.16 (quadratic variation of stochastic integral)**.** Let $M \in \mathcal{M}_{c,loc}$ and H be locally bounded previsible. Then $H \cdot M$ is a continuous local martingale, whose quadratic variation is given by

$$[H \cdot M] = H^2 \cdot [M]. \tag{23.1.93}$$

Remark. In practice, we often use this theorem in combination with Theorem 23.1.9 to conclude that $H \cdot M$ is a true martingale. In addition, as already discussed informally at the very beginning of the construction, this is the property which in some sense motivates the entire construction of the stochastic integral.

Proof. Let T_n be a sequence of stopping times (as above) which "reduces" both H and $M : H^{T_n}$ is bounded and $M^{T_n} \in \mathcal{M}_c^2$.

By Propostion 23.1.15,

$$(H \cdot M)^{T_n} = (H\mathbb{1}_{(0,T_n]}) \cdot M^{T_n} \in \mathcal{M}_c^2 \tag{23.1.94}$$

which implies that $H \cdot M$ is a continuous local martingale. To compute the quadratic variation, assume first that $M \in \mathcal{M}_c^2$ and that H is uniformly bounded in time (and thus $\subseteq \mathcal{L}^2(M)$). For any stopping time T, we have by Proposition 23.1.15 and the isometry property of Theorem 23.1.13):

$$\begin{aligned}
\mathbb{E}\left((H \cdot M)_T^2\right) &= \mathbb{E}\left((H \cdot M)_{T\wedge\infty}^2\right) = \mathbb{E}\left((H\mathbb{1}_{(0,T]} \cdot M)_\infty^2\right) = \left\|H\mathbb{1}_{(0,T]} \cdot M\right\|^2 = \left\|H\mathbb{1}_{(0,T]}\right\|_M^2 \\
&= \mathbb{E}\left(\int_0^\infty H_s^2 \mathbb{1}_{(0,T]}(s) d[M]_s\right) = \mathbb{E}\left(\int_0^T H_s^2 d[M]_s\right) = \mathbb{E}\left((H^2 \cdot [M])_T\right).
\end{aligned}$$

By the optional stopping theorem (Theorem 20.5.16), we conclude that $(H \cdot M)^2 - H^2 \cdot [M]$ is a martingale (thus a local martingale). Moreover, since H is uniformly bounded and $[M]$ (pathwise) continuous, we can also show that $H^2 \cdot [M]$ is adapted, (sample) continuous and non-decreasing (by Corollary 23.1.11). Therefore, by Theorem 23.1.7, we have $[H \cdot M] = H^2 \cdot [M]$ in the sense of indistinguishable.

In the general case, for any $t \geq 0$,

$$\begin{aligned}
[H \cdot M]_t &\overset{\text{a.s.}}{=} \lim_{n\to\infty} [H \cdot M]_t^{T_n} \qquad \text{(by continuity of quadratic variation and } T_n \uparrow \infty \text{ a.s.)} \\
&= \lim_{n\to\infty} [(H \cdot M)^{T_n}]_t \qquad \text{(by Proposition 23.1.8)} \\
&= \lim_{n\to\infty} [H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}]_t = \lim_{n\to\infty} \left(H^2\mathbb{1}_{(0,T_n]} \cdot [M]^{T_n}\right)_t \quad \text{(by the case of uniformly bounded } H \text{ and } M \in \mathcal{M}_c^2) \\
&= \lim_{n\to\infty} \int_0^t H_s^2 \mathbb{1}_{T_n}(s) d[M]_s = \int_0^t H_s^2 \lim_{n\to\infty} \mathbb{1}_{T_n}(s) d[M]_s \quad \text{(by monotone convergence theorem, Theorem 19.3.6)} \\
&= \int_0^t H_s^2 d[M]_s = \left(H^2 \cdot [M]\right)_t.
\end{aligned}$$

Thus, $[H \cdot M]$ is a version of $H^2 \cdot [M]$. But we know that both processes are (sample) continuous (Corollary 23.1.11 gives the properties of $H^2 \cdot [M]$. Actually, $[H \cdot M]$ is pathwise continuous by Theorem 23.1.7). Thus, by Proposition 20.4.12, $[H \cdot M] = H^2 \cdot [M]$ in the sense of indistinguishability. □

Theorem 23.1.17 (stochastic chain rule)**.** Let H, K be locally bounded and previsible and $M \in \mathcal{M}_{c,loc}$. Then

$$H \cdot (K \cdot M) = (HK) \cdot M. \tag{23.1.95}$$

Remark. We view this result as a stochastic chain rule, since it is telling us that:

$$d\left(\int_0^t K_s dM_s\right) = K_t dM_t. \tag{23.1.96}$$

This is a rule that is extremely useful in the practice of computing stochastic integrals. e.g.,

$$dY_t = H_t dX_t \;\Rightarrow\; dX_t = (1/H_t) dY_t. \tag{23.1.97}$$

Proof. For $H, K \in \mathcal{S}$ and $M \in \mathcal{M}_c^2$, we have

$$H = \sum_{i=1}^{m-1} X_i \mathbb{1}_{(t_i, t_{i+1}]}(t), \quad K = \sum_{j=1}^{n-1} Y_j \mathbb{1}_{(s_j, s_{j+1}]}(t) \tag{23.1.98}$$

where $t_i < t_{i+1}$, $s_j < s_{j+1}$ and $X_i \in \mathcal{F}_{t_k}, Y_j \in \mathcal{F}_{s_j}$. Then for any $t \geq 0$ (using $(*)$ in proof of Theorem 20.4.24 and linearity)

$$(H \cdot (K \cdot M))_t = (HK \cdot (M))_t \,. \tag{23.1.99}$$

Thus, for any $t \geq 0$, we have $(H \cdot (K \cdot M))_t = (HK \cdot M)_t$. Since both processes is in $\mathcal{M}_c^2$ (by Proposition 23.1.3), we have $H \cdot (K \cdot M) = HK \cdot M$ is the sense of indistinguishability.

For H, K uniformly bounded (and thus in $\mathcal{L}^2(M)$) for $M \in \mathcal{M}_c^2$, there exist $H^n, K^n \in \mathcal{S}$, $n \in \mathbb{N}$ such that $H^n \to H$ and $K^n \to K$ in $\mathcal{L}^2(M)$, i.e.,

$$\|H^n - H\|_{\mathcal{L}^2(M)} \to 0, \quad \|K^n - K\|_{\mathcal{L}^2(M)} \to 0. \tag{23.1.100}$$

Furthermore, we may also assume that $\|H^n\|_\infty$ and $\|K^n\|_\infty$ are uniformly bounded in n. (we can truncate K^n with $n \wedge K^n \vee (-n)$ such that the truncated K^n is uniformly bounded).

By Theorem 20.4.24, we have for any $t \geq 0$,

$$\left(H^2 \cdot (K^2 \cdot [M])\right)_t = \left((HK)^2 \cdot [M]\right)_t. \tag{23.1.101}$$

Note that $H, K \in \mathcal{L}^2(M)$ for $M \in \mathcal{M}_c^2$ thus $(K^2 \cdot M) \in \mathcal{M}_c^2$ by Theorem 23.1.13. Thus, $K^2 \cdot M$ converges to $(K^2 \cdot M)_\infty$ a.s. in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ and therefore $\mathbb{E}\left((K^2 \cdot M)_\infty\right) < \infty$. Then

$$\mathbb{E}\left((H^2 \cdot [K^2 \cdot M])_\infty\right) = \mathbb{E}\left(\int_0^\infty H_s^2 d[K^2 \cdot M]_s\right) \leq \mathbb{E}\left(\sup_{t \geq 0} H_t^2 [K^2 \cdot M]_\infty\right) < \infty \tag{23.1.102}$$

since H is uniformly bounded (i.e., $\sup_{t \geq 0} H_t^2$). Therefore, $(H^2 \cdot [K^2 \cdot M])_\infty$ is finite a.s.. Similarly, $\left((HK)^2 \cdot [M]\right)_\infty$ is well-defined and finite a.s.. Thus, since $\left(H^2 \cdot (K^2 \cdot [M])\right) = \left((HK)^2 \cdot [M]\right)$,

$$\left(H^2 \cdot (K^2 \cdot [M])\right)_\infty = \left((HK)^2 \cdot [M]\right)_\infty \quad \text{a.s..} \qquad (*) \tag{23.1.103}$$

We first prove an upper bound on $\|H\|_{\mathcal{L}^2(K \cdot M)}$:

$$\begin{aligned}
\|H\|^2_{\mathcal{L}^2(K \cdot M)} &= \mathbb{E}\left(\int_0^\infty H_s^2 d[K \cdot M]_s\right) = \mathbb{E}\left((H^2 \cdot [K \cdot M])_\infty\right) \\
&= \mathbb{E}\left((H^2 \cdot (K^2 \cdot [M]))_\infty\right) \qquad \text{(by Theorem 23.1.16)} \\
&\overset{(*)}{=} \mathbb{E}\left(((HK)^2 \cdot [M])_\infty\right) = \mathbb{E}\left(\int_0^\infty (H_s K_s)^2 d[M]_s\right) = \|HK\|^2_{\mathcal{L}^2(M)} \\
&\leq \min\left\{\|H\|_\infty^2 \|K\|^2_{\mathcal{L}^2(M)}, \|H\|^2_{\mathcal{L}^2(M)} \|K\|_\infty^2\right\} < \infty
\end{aligned}$$

where H and K are uniformly bounded ($\|H\|_\infty \leq \sup_{t \geq 0} |H_t| < \infty$).

We have $H^n \cdot (K^n \cdot M) = (H^n K^n) \cdot M$ and using the above equations,

$$\begin{aligned}
\|H^n \cdot (K^n \cdot M) - H \cdot (K \cdot M)\| &\leq \|H^n \cdot (K^n \cdot M) - H \cdot (K^n \cdot M)\| + \|H \cdot (K^n \cdot M) - H \cdot (K \cdot M)\| \\
&\leq \|(H^n - H) \cdot (K^n \cdot M)\| + \|H \cdot ((K^n - K) \cdot M)\| \\
&= \|H^n - H\|_{\mathcal{L}^2(K^n \cdot M)} + \|H\|_{\mathcal{L}^2((K^n - K) \cdot M)} \\
&\leq \|H^n - H\|_{\mathcal{L}^2(M)} \|K^n\|_\infty + \|H\|_\infty \|K^n - K\|_{\mathcal{L}^2(M)} \to 0 \quad \text{as } n \to \infty.
\end{aligned}$$

So $H^n \cdot (K^n \cdot M) \to H \cdot (K \cdot M)$ in $\mathcal{M}_c^2$. Similarly,

$$\begin{aligned}
\|(H^n K^n) \cdot M - (HK) \cdot M\| &\leq \|(H^n K^n - HK^n) \cdot M\| + \|(HK^n - HK) \cdot M\| \\
&= \|(H^n - H)K^n\|_{\mathcal{L}^2(M)} + \|H(K^n - K)\|_{\mathcal{L}^2(M)} \\
&\leq \|K^n\|_\infty \|H^n - H\|_{\mathcal{L}^2(M)} + \|H\|_\infty \|K^n - K\|_{\mathcal{L}^2(M)}.
\end{aligned}$$

So $(H^n K^n) \cdot M \to (HK) \cdot M$ in $\left(\mathcal{M}_c^2, \|\cdot\|\right)$. Thus, $H \cdot (K \cdot M) = (HK) \cdot M$ (†) in the sense of distinguishability.

For more general case, for locally bounded previsible H, K and $M \in \mathcal{M}_{c,loc}$. we can find a sequence of stopping times $(T_n)_{n \in \mathbb{N}}$ such that T_n reduce H, K and M (use the same T_n as before such that M^{T_n} is a bounded martingale). We can see that $(H \cdot (K \cdot M))$ and $(HK) \cdot M$ are both (sample) continuous local martingales. Thus, by Proposition 23.1.15,

$$\begin{aligned}
(H \cdot (K \cdot M))^{T_n} &= (H \cdot (K \cdot M))^{T_n \wedge T_n} = H \mathbb{1}_{(0,T_n]} \cdot (K \cdot M)^{T_n} = H \mathbb{1}_{(0,T_n]} \cdot (K \cdot M)^{T_n \wedge T_n} \\
&= H \mathbb{1}_{(0,T_n]} \cdot \left(K \mathbb{1}_{(0,T_n]} \cdot M^{T_n}\right) \overset{(\dagger)}{=} H \mathbb{1}_{(0,T_n]} K \mathbb{1}_{(0,T_n]} \cdot M^{T_n} = \left(HK \mathbb{1}_{(0,T_n]}\right) \cdot M^{T_n} \\
&= ((HK) \cdot M)^{T_n \wedge T_n} = ((HK) \cdot M)^{T_n}.
\end{aligned}$$

Thus, for any $t \geq 0$, by (sample) continuity of $(H \cdot (K \cdot M))$ and $(HK) \cdot M$,

$$(H \cdot (K \cdot M))_t^{T_n} \to (H \cdot (K \cdot M))_t \quad \text{a.s.}, \quad ((HK) \cdot M)_t^{T_n} \to ((HK) \cdot M)_t \quad \text{a.s.}. \tag{23.1.104}$$

Thus, $(H \cdot (K \cdot M))_t = ((HK) \cdot M)_t$ a.s.. Since both local martingales are continuous, we have $H \cdot (K \cdot M) = (HK) \cdot M$ in the sense of distinguishability. □

23.1.5 Covariation

In practice we do not calculate integrals from first principles, but rather use tools of calculus such as integration by parts or the chain rule. In this section we derive these tools for stochastic integrals, which differ from ordinary calculus in certain correction terms. A useful tool for deriving these rules will be the covariation of two local martingales.

Definition 23.1.10 (covariation)**.** Let $M, N \in \mathcal{M}_{c,loc}$, adapted to a common filtration $(\mathcal{F}_t)_{t \geq 0}$ satisfying the usual conditions, and set

$$[M, N] = \frac{1}{4}([M + N] - [M - N]) \qquad \text{(polarization identity)} \tag{23.1.105}$$

$[M, N]$ is called the covariation of M and N.

Proposition 23.1.18. Let $M, N \in \mathcal{M}_{c,loc}$. Then we have:

(i) $[M, N]$ is the unique (up to indistinguishability) (pathwise) continuous adapted process with finite variation such that $MN - [M, N]$ is a continuous local martingale. Also, $[M, N]_0 = 0$ a.s.

(ii) For $n \geq 1$ and for all $t \geq 0$, let

$$[M, N]_t^n := \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} \left(M_{(k+1)2^{-n}} - M_{k2^{-n}}\right)\left(N_{(k+1)2^{-n}} - N_{k2^{-n}}\right). \tag{23.1.106}$$

Then $[M, N]^n \to [M, N]$ u.c.p. as $n \to \infty$.

(iii) for $M, N \in \mathcal{M}_c^2$, $MN - [M, N]$ is a UI martingale.

(iv) $[M, N]$ is a symmetric bilinear form.

(v) For any stopping time T, $\left[M^T, N^T\right] = [M,N]^T$.

Remark. Of course, $[M,M] = [M]$.

Proof. (i) First, we know that $M+N, M-N \in \mathcal{M}_{c,loc}$ by Proposition 20.6.5. Then exist unique $[M+N]$ and $[M-N]$ such that $(M+N)^2 - [M-N], (M+N)^2 - [M-N] \in \mathcal{M}_{c,loc}$. Therefore, there exist unique $[M+N]-[M-N]$ such that $(M+N)^2 - (M-N)^2 - ([M+N]-[M-N]) \in \mathcal{M}_{c,loc}$.

We know that $MN = \frac{1}{4}\left((M+N)^2 - (M-N)^2\right)$, so

$$MN - [M,N] = \frac{1}{4}\left((M+N)^2 - [M+N]\right) - \frac{1}{4}\left((M-N)^2 - [M-N]\right). \tag{23.1.107}$$

Thus, both terms are continuous local martingales from Theorem 23.1.7. Then $MN - [M,N] \in \mathcal{M}_{c,loc}$ by Proposition 20.6.5. Since such $[M+N]-[M-N]$ is unique, we have that $[M,N]$ is unique.

Also, since $[M+N]$ and $[M-N]$ are (pathwise) continuous adapted processes, we have $[M,N]$ is also (pathwise) continuous adapted. Furthermore, since $[M+N]$ and $[M-N]$ are (pathwise) non-decreasing, we have that $[M,N]$ is (pathwise) continuous process with (pathwise) finite variation process by Proposition 10.3.12.

By definition of $[M,N]$, it is obvious that $[M,N]_0 = \frac{1}{4}\left([M+N]_0 - [M-N]_0\right) = 0$ a.s..

(ii) By Proposition 20.6.5, $M+N, M-N \in \mathcal{M}_{c,loc}$, thus

$$\begin{aligned}
[M,N]^n_t &= \sum_{k=0}^{\lfloor 2^n t\rfloor - 1} \left(M_{(k+1)2^{-n}} - M_{k2^{-n}}\right)\left(N_{(k+1)2^{-n}} - N_{k2^{-n}}\right) \\
&= \sum_{k=0}^{\lfloor 2^n t\rfloor - 1} M_{(k+1)2^{-n}}N_{(k+1)2^{-n}} - M_{(k+1)2^{-n}}N_{k2^{-n}} - M_{k2^{-n}}N_{(k+1)2^{-n}} + M_{k2^{-n}}N_{k2^{-n}} \\
&= \frac{1}{4}\sum_{k=0}^{\lfloor 2^n t\rfloor - 1} \left(M_{(k+1)2^{-n}} + N_{(k+1)2^{-n}} - M_{k2^{-n}} - N_{k2^{-n}}\right)^2 - \left(M_{(k+1)2^{-n}} - N_{(k+1)2^{-n}} - M_{k2^{-n}} + N_{k2^{-n}}\right)^2 \\
&= \frac{1}{4}\left([M+N]^n_t - [M-N]^n_t\right).
\end{aligned}$$

By Theorem 23.1.7, we have $[M+N]^n \xrightarrow{ucp} [M+N]$, $[M-N]^n \xrightarrow{ucp} [M-N]$, i.e., $\forall \varepsilon > 0, \forall t \geq 0$,

$$\mathbb{P}\left(\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| > \varepsilon\right) \to 0, \quad \mathbb{P}\left(\sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon\right) \to 0 \quad \text{as } n \to \infty.$$

Thus, we have $\forall \varepsilon > 0, \forall t \geq 0$,

$$\begin{aligned}
\mathbb{P}\left(\sup_{s\leq t} |[M,N]^n_s - [M,N]_s| > \varepsilon\right) &= \mathbb{P}\left(\sup_{s\leq t} \left|\frac{1}{4}\left([M+N]^n_s - [M-N]^n_s\right) - \frac{1}{4}\left([M+N]_s - [M-N]_s\right)\right| > \varepsilon\right) \\
&= \mathbb{P}\left(\frac{1}{4}\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| + \frac{1}{4}\sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon\right) \\
&\leq \mathbb{P}\left(\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| + \sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon\right)
\end{aligned}$$

However, $\mathbb{P}\left(\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| + \sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon\right)$ is

$$\begin{aligned}
&\mathbb{P}\left(\bigcup_{q\leq\varepsilon, q\in\mathbb{Q}^+} \left\{\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| > q\right\} \cap \left\{\sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon - q\right\}\right) \\
\leq &\sum_{q\leq\varepsilon, q\in\mathbb{Q}^+} \mathbb{P}\left(\left\{\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| > q\right\} \cap \left\{\sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon - q\right\}\right) \\
\leq &\sum_{q\leq\varepsilon, q\in\mathbb{Q}^+} \mathbb{P}\left(\sup_{s\leq t} |[M+N]^n_s - [M+N]_s| > q\right) + \mathbb{P}\left(\sup_{s\leq t} |[M-N]^n_s - [M-N]_s| > \varepsilon - q\right) \to 0
\end{aligned}$$

as countably many sum of zeros. Thus, $[M,N]^n \to [M,N]$ u.c.p. as $n \to \infty$.

(iii) Since $M, N \in \mathcal{M}_c^2$, then $M+N, M-N \in \mathcal{M}_c^2$, $(M+N)^2 - [M+N]$ and $(M-N)^2 - [M-N]$ are UI martingale by Theorem 23.1.9. Then

$$MN - [M,N] = \frac{1}{4}\left((M+N)^2 - [M+N] + (M-N)^2 - [M-N]\right) \quad \text{is also a UI martingale} \tag{23.1.108}$$

since $\left((M+N)^2 - [M+N]\right)_t \to \left((M+N)^2 - [M+N]\right)_\infty$ and $\left((M-N)^2 - [M-N]\right)_t \to \left((M-N)^2 - [M-N]\right)_\infty$ a.s. and in $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ by Theorem 20.5.15. Thus,

$$(MN - [M,N])_t \to \left((M+N)^2 - [M+N]\right)_\infty + \left((M-N)^2 - [M-N]\right)_\infty \quad \text{a.s. and in } \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P}). \tag{23.1.109}$$

Then by Theorem 20.5.15 again, we have $MN - [M,N] \in \mathcal{M}_c^2$.

(iv) Since $MN = NM$ by uniqueness in (i) we have $[M,N] = [N,M]$ (symmetry). Now $M_1, M_2, N_1, N_2 \in \mathcal{M}_{c,loc}$ and $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{R}$. Then

$$(\lambda_1 M_1 + \lambda_2 M_2)(\mu_1 N_1 + \mu_2 N_2) = \lambda_1\mu_1 M_1 N_1 + \lambda_1\mu_2 M_1 N_2 + \lambda_2\mu_1 M_2 N_1 + \lambda_2\mu_2 M_2 N_2 \tag{23.1.110}$$

implies that (by uniqueness in (i)),

$$[\lambda_1 M_1 + \lambda_2 M_2, \mu_1 N_1 + \mu_2 N_2] = \lambda_1\mu_1[M_1, N_1] + \lambda_1\mu_2[M_1, N_2] + \lambda_2\mu_1[M_2, N_1] + \lambda_2\mu_2[M_2, N_2]. \tag{23.1.111}$$

which is the bilinearity.

(v) By definition and Proposition 23.1.8,

$$\left[M^T, N^T\right] = \frac{1}{4}\left(\left[M^T + N^T\right] - \left[M^T - N^T\right]\right) = \frac{1}{4}\left(\left[M+N\right]^T - \left[M-N\right]^T\right) = [M,N]^T. \tag{23.1.112}$$

□

Theorem 23.1.19 (Kunita-Watanabe identity)**.** Let $M, N \in \mathcal{M}_{c,loc}$ and H be a locally bounded previsible process. Then

$$[H \cdot M, N] = H \cdot [M,N]. \tag{23.1.113}$$

Proof. We may assume by localization that $M, N \in \mathcal{M}_c^2$ and that H is uniformly bounded in time.

If H is of the form $Z\mathbb{1}_{(s,t]}$ with Z bounded $\mathcal{F}_s$-measurable ($H \in \mathcal{L}^2(M) \Rightarrow (H \cdot M) \in \mathcal{M}_c^2$), we have $((H \cdot M)_\infty$ and N_∞ are well-defined since $(H \cdot M), N \in \mathcal{M}_c^2$.

Then by tower property (Proposition 19.4.28) we have

$$\begin{aligned}
\mathbb{E}\left((H \cdot M)_\infty N_\infty\right) &= \mathbb{E}\left(Z(M_t - M_s)N_\infty\right) = \mathbb{E}\left(ZM_t\mathbb{E}(N_\infty|\mathcal{F}_t)\right) - \mathbb{E}\left(ZM_s\mathbb{E}(N_\infty|\mathcal{F}_s)\right) \\
&= \mathbb{E}\left(Z\mathbb{E}(M_tN_t - M_sN_s|\mathcal{F}_s)\right) \qquad \text{(by Theorem 20.5.14)} \\
&= \mathbb{E}\left(Z\mathbb{E}([M,N]_t - [M,N]_s|\mathcal{F}_s)\right) \qquad \text{(by Proposition 23.1.18.(iii))} \\
&= \mathbb{E}\left(Z([M,N]_t - [M,N]_s)\right) = \mathbb{E}\left(H \cdot [M,N]_\infty\right) \qquad (*)
\end{aligned}$$

Note that $[M,N]_\infty$ is well-defined since $\mathbb{E}([M+N]_\infty) < \infty$ and $\mathbb{E}([M-N]_\infty) < \infty$ (This is true by Theorem 23.1.10 since $M+N, M-N \in \mathcal{M}_c^2$). Note that $(*)$ also holds for any $H \in \mathcal{S}$ by linearity.

Now suppose H is uniformly bounded, of course $H \in \mathcal{L}(M)$. Then we can find $H^n \to H$ with $H^n \in \mathcal{S}$ for all n. Then

$$H^n \cdot [M,N]_\infty \to H \cdot [M,N]_\infty \tag{23.1.114}$$

by dominated convergence theorem (Theorem) since H^n is bounded and $[M,N]$ is of finite variation. Also,

$$H^n \cdot M \to H \cdot M \ \text{ in } \left(\mathcal{M}_c^2, \|\cdot\|\right) \tag{23.1.115}$$

by isometry theorem (Theorem 23.1.13). Then

$$\|(H^n \cdot M)_\infty - (H \cdot M)_\infty\|_2 = \|H^n \cdot M - H \cdot M\| \to 0 \;\Rightarrow\; (H^n \cdot M)_\infty \to (H \cdot M)_\infty \;\text{ a.s.} \tag{23.1.116}$$

by Theorem 20.2.20. Thus, we have

$$(H \cdot M)_\infty N_\infty = H \cdot [M, N]_\infty \text{ a.s.} \tag{23.1.117}$$

For any bounded stopping time T, we have that H^T is uniformly bounded (and thus $H^T \in \mathcal{L}^2(M)$) and $M^T, N^T \in \mathcal{M}_c^2$, which also satisfy $(*)$. That is, $\mathbb{E}\left((H^T \cdot M^T)_\infty N_\infty^T\right) = \mathbb{E}\left(H^T \cdot [M, N]_\infty^T\right)$ which implies that

$$\mathbb{E}\left((H \cdot M)_T N_T\right) = \mathbb{E}\left((H \cdot [M, N])_T\right) \qquad (\dagger) \tag{23.1.118}$$

But we know that $(H \cdot M)_0 = 0$ a.s. (by Definition 23.1.8) and $[M, N]_0 = 0$ a.s. (by Proposition 23.1.18.(i)). Thus,

$$\mathbb{E}\left((H \cdot M)_T N_T - (H \cdot [M, N])_T\right) = 0 = \mathbb{E}\left((H \cdot M)_0 N_0 - (H \cdot [M, N])_0\right) \tag{23.1.119}$$

Then by optional stopping theorem (Theorem 20.5.16), $(H \cdot M)N - H \cdot [M, N]$ is a martingale. That is,

$$(H \cdot M)N - H \cdot [M, N] \in \mathcal{M}_{c,loc}. \tag{23.1.120}$$

Note that $H \cdot [M, N]$ is adapted and (pathwise) continuous (by Corollary 23.1.11) and of finite variation (by Theorem 20.4.21), and thus by the uniqueness of Proposition 23.1.18.(i), we have

$$(H \cdot M)N = H \cdot [M, N] \tag{23.1.121}$$

in the sense of indistinguishability.

Now Let H be a locally bounded process and $M, N \in \mathcal{M}_{c,loc}$. Let T_n be the sequence of stopping times reducing H, M, N. That is, $T_n \uparrow \infty$ a.s. and $H\mathbb{1}_{(0,T_n]}$ is uniformly bounded a.s. and $M^{T_n}, N^{T_n} \in \mathcal{M}_c^2$. Then for any $t \geq 0$

$$\left(\left(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}\right) N^{T_n}\right)_t = \left(H\mathbb{1}_{(0,T_n]} \cdot \left[M^{T_n}, N^{T_n}\right]\right)_t \;\text{ a.s.} \tag{23.1.122}$$

By Proposition 23.1.15, we have

$$\left(\left(H\mathbb{1}_{(0,T_n]} \cdot M^{T_n}\right) N^{T_n}\right)_t = \left(\left(H \cdot M^{T_n}\right)^{T_n} N^{T_n}\right)_t = \left((H \cdot M)^{T_n \wedge T_n} N^{T_n}\right)_t = \left((H \cdot M)\, N\right)_t^{T_n} \to \left((H \cdot M)\, N\right)_t \;\text{ a.s.}$$

Also,

$$\left(H\mathbb{1}_{(0,T_n]} \cdot \left[M^{T_n}, N^{T_n}\right]\right)_t = \left(H\mathbb{1}_{(0,T_n]} \cdot [M, N]^{T_n}\right)_t = (H \cdot [M, N])_t^{T_n} \to (H \cdot [M, N])_t \;\text{ a.s.} \tag{23.1.123}$$

Thus, we have

$$\left((H \cdot M)\, N\right)_t = (H \cdot [M, N])_t \;\text{ a.s. } \Rightarrow\; (H \cdot M)\, N = H \cdot [M, N] \tag{23.1.124}$$

in the sence of indistinguishability since both process are (sample) continuous. □

Remark. Note that a consequence of this identity is that $[H \cdot M, H \cdot N] = H^2 \cdot [M, N]$. We can derive directly the latter identity by polarization arguments.

Now we give more general property.

Proposition 23.1.20. Let $M, N \in \mathcal{M}_{c,loc}$ and H, K be a locally bounded previsible processes. Then

$$[H \cdot M, K \cdot N] = (HK) \cdot [M, N]. \tag{23.1.125}$$

Proof. First we have $K \cdot N \in \mathcal{M}_{c,loc}$ by Definition 23.1.9. Then by Theorem 23.1.19 and symmetry of covariation (Proposition 23.1.18.(iv)),

$$[H \cdot M, K \cdot N] = H \cdot [M, K \cdot N] = H \cdot [K \cdot N, M] = H \cdot (K \cdot [N, M]) = H \cdot (K \cdot [M, N])\,. \tag{23.1.126}$$

Then by Theorem 20.4.25,

$$H \cdot (K \cdot [M,N]) = (HK) \cdot [M,N]. \tag{23.1.127}$$

as required. □

23.1.6 Stochastic integral for semimartingales

Recall definition of semimartingale (Definition 20.6.2). Now we have the continuous semimartingale.

Definition 23.1.11 (continuous semimartingale)**.** A continuous semimartingale X is an adapted (sample) continuous process which may be written as

$$X = X_0 + M + A, \qquad M_0 = A_0 = 0 \ \text{ a.s.}, \tag{23.1.128}$$

where $M \in \mathcal{M}_{c,loc}$ and A is a continuous finite variation process[12].

We set the quadratic variation of X to be that of its local martingale part, $[X] := [M]$, independently of A.

This definition finds its justification in the fact that

Proposition 23.1.21. Let X be a continuous semimartingale and we define that

$$[X]^n_t := \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} (X_{(k+1)2^{-n}} - X_{k2^{-n}})^2 \quad \text{and } [X]^n \to [X] \text{ u.c.p..} \tag{23.1.129}$$

Proof. By definition, we have for any $t \geq 0$,

$$\begin{aligned} [X]^n_t &= \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} (X_{(k+1)2^{-n}} - X_{k2^{-n}})^2 = \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} (M_{(k+1)2^{-n}} + A_{(k+1)2^{-n}} - M_{k2^{-n}} - A_{k2^{-n}})^2 \\ &= [M]^n_t + [A]^n_t + 2 \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} \left(M_{(k+1)2^{-n}} - M_{k2^{-n}}\right)\left(A_{(k+1)2^{-n}} - A_{k2^{-n}}\right) := [M]^n_t + [A]^n_t + 2W^n_t. \end{aligned}$$

Since M and A are (sample) continuous, then they are uniformly continuous on a compact set $[0,t]$[13] a.s.. Thus, we have

$$\sup_{0\leq s\leq t} \left|M_{2^{-n}\lfloor 2^n s\rfloor} - M_s\right| \to 0 \ \text{ a.s.}, \qquad \sup_{0\leq s\leq t} \left|A_{2^{-n}\lfloor 2^n s\rfloor} - A_s\right| \to 0 \ \text{ a.s.} \tag{23.1.130}$$

as $n \to \infty$. However, we know that

$$\left| \sum_{k=0}^{\lfloor 2^n t \rfloor - 1} \left(A_{(k+1)2^{-n}} - A_{k2^{-n}}\right) \right| = \left|A_{2^{-n}\lfloor 2^n t\rfloor}\right| < \infty \ \text{ a.s.} \tag{23.1.131}$$

since A is (sample) continuous on $[0,t]$ (by Theorem 10.3.8). Then we have

$$\begin{aligned} \sup_{0\leq s\leq t} |[A]^n_s + 2W^n_s| &\leq \left(\sup_{0\leq s\leq t} \left|A_{2^{-n}\lfloor 2^n s\rfloor} - A_s\right| + 2 \sup_{0\leq s\leq t} \left|M_{2^{-n}\lfloor 2^n s\rfloor} - M_s\right|\right) \sup_{0\leq s\leq t} \left| \sum_{k=0}^{\lfloor 2^n s \rfloor - 1} \left(A_{(k+1)2^{-n}} - A_{k2^{-n}}\right) \right| \\ &\leq \left(\sup_{0\leq s\leq t} \left|A_{2^{-n}\lfloor 2^n s\rfloor} - A_s\right| + 2 \sup_{0\leq s\leq t} \left|M_{2^{-n}\lfloor 2^n s\rfloor} - M_s\right|\right) \sup_{0\leq s\leq t} \left|A_{2^{-n}\lfloor 2^n s\rfloor}\right| \to 0 \ \text{ a.s..} \end{aligned}$$

Then by Markov inequality (Theorem 19.3.20), we have $\forall \varepsilon > 0$, $\forall t \geq 0$,

$$\mathbb{P}\left(\sup_{0\leq s\leq t} |[A]^n_s + 2W^n_s| > \varepsilon\right) \leq \mathbb{E}\left(\sup_{0\leq s\leq t} |[A]^n_s + 2W^n_s|\right) \Big/ \varepsilon \to 0. \tag{23.1.132}$$

Thus, we have $[A]^n + 2W^n \to 0$ u.c.p.. By Theorem 23.1.7, we also have $[M]^n \to [M]$ u.c.p.. Thus, can have $[X]^n =$

[12] this is actually canonical decomposition of a continuous semimartingale, see [11].V31

[13] need theorem here

$[M]^n + [A]^n + 2W^n \to [M]$ u.c.p.. since

$$\begin{aligned}\mathbb{P}\left(\sup_{0\le s\le t}|[M^n_s]+[A]^n_s+2W^n_s|>\varepsilon\right) &\le \mathbb{P}\left(\sup_{0\le s\le t}|[M^n_s]|+\sup_{0\le s\le t}|[A]^n_s+2W^n_s|>\varepsilon\right)\\ &\le \mathbb{P}\left(\sup_{0\le s\le t}|[M^n_s]|>\varepsilon/2\right)+\mathbb{P}\left(\sup_{0\le s\le t}|[A]^n_s+2W^n_s|>\varepsilon/2\right)\to 0+0=0.\end{aligned}$$

Since $[X]=[M]$, we have $[X]^n \to [X]$ u.c.p.. □

Proposition 23.1.22. Let M, N be continuous local martingales in a common filtration $(\mathcal{F}_t)_{t\ge 0}$ satisfying the usual conditions, and assume that M and N are independent, i.e., $\sigma(M_s : s \ge 0)$ and $\sigma(N_s : s \ge 0)$ are independent. Then $[M, N] \equiv 0$.

Proof. For any bounded stopping time T and a sequence stopping times $T_n \uparrow \infty$ a.s. which reduce both M and N. We have (since M and N are independent and $M^{T_n}_T$ and $N^{T_n}_T$ are independent) by Proposition 19.3.12

$$\mathbb{E}\left((MN)^{T_n}_T\right)=\mathbb{E}\left(M^{T_n}_T N^{T_n}_T\right)=\mathbb{E}\left(M^{T_n}_T\right)\mathbb{E}\left(N^{T_n}_T\right)\overset{\text{a.s.}}{=}M^{T_n}_0 N^{T_n}_0=(MN)^{T_n}_0. \tag{23.1.133}$$

Thus, $(MN)^{T_n}$ is martingale and therefore MN is a continuous local martingale. But $[M, N]$ is the unique process gives that $MN - [M, N] \in \mathcal{M}_{c,loc}$ by Proposition 23.1.18. Thus, $[M, N]_t = 0$ a.s. for all t. That is, $[M, N] = 0$ in the sence of distinguishability since $[M, N]$ is (pathwise) continuous by Proposition 20.4.12. □

Remark. In particular, if $B = (B^1, \dots, B^2)$ is a 2-dimensional Brownian motion, then $\left[B^1, B^2\right]_t = 0$.

However, the converse does not hold. By polarization,

$$\left[B^T, B - B^T\right] = \frac{1}{2}\left([B_t] - \left[2B^T - B\right]_t\right) = 0 \tag{23.1.134}$$

as the by the reflection principle[14], $2B^T - B$ is another Brownian motion.

Let $X = B^T$ and $Y = B - B^T$. Then $[X]_t = T \wedge t$ and $T = \inf\{t \ge 0 : Y_t \ne 0\}$ and so T is measurable both wrt σ-algebra generated by X and wrt σ-algebra generated by Y. Hence X and Y are not independent.

Definition 23.1.12. Let X, Y be continuous semimartingales. We define their covariation $[X, Y]$ to be the covariation of their respective local martingale parts.

Proposition 23.1.23. Let X, Y be two continuous semimartingales and we define that

$$[X,Y]^n_t := \sum_{k=0}^{\lfloor 2^n t\rfloor -1}(X_{(k+1)2^{-n}} - X_{k2^{-n}})(Y_{(k+1)2^{-n}} - Y_{k2^{-n}}) \quad \text{and } [X,Y]^n \to [X,Y] \text{ u.c.p..} \tag{23.1.135}$$

Proof. By Proposition 20.6.5, $M + N, M - N \in \mathcal{M}_{c,loc}$, thus

$$\begin{aligned}[X,Y]^n_t &= \sum_{k=0}^{\lfloor 2^n t\rfloor -1}\left(X_{(k+1)2^{-n}} - X_{k2^{-n}}\right)\left(Y_{(k+1)2^{-n}} - Y_{k2^{-n}}\right)\\ &= \sum_{k=0}^{\lfloor 2^n t\rfloor -1} X_{(k+1)2^{-n}}Y_{(k+1)2^{-n}} - X_{(k+1)2^{-n}}Y_{k2^{-n}} - X_{k2^{-n}}Y_{(k+1)2^{-n}} + X_{k2^{-n}}Y_{k2^{-n}}\\ &= \frac{1}{4}\sum_{k=0}^{\lfloor 2^n t\rfloor -1}\left(X_{(k+1)2^{-n}} + Y_{(k+1)2^{-n}} - X_{k2^{-n}} - Y_{k2^{-n}}\right)^2 - \left(X_{(k+1)2^{-n}} - Y_{(k+1)2^{-n}} - X_{k2^{-n}} + Y_{k2^{-n}}\right)^2\\ &= \frac{1}{4}\left([X+Y]^n_t - [X-Y]^n_t\right).\end{aligned}$$

Then by Proposition 23.1.21, we have

$$[X+Y]^n \to [X+Y] \text{ u.c.p}, \quad [X-Y]^n \to [X-Y] \text{ u.c.p.} \tag{23.1.136}$$

[14] need theorem

Let M, N be the respective local martingale parts of X, Y. Thus, $[X,Y]^n \to \frac{1}{4}([X+Y]-[X-Y])$ u.c.p. So

$$[X,Y]^n \to \frac{1}{4}([X+Y]-[X-Y]) = \frac{1}{4}([M+N]-[M-N]) = [M,N] = [X,Y] \text{ u.c.p} \tag{23.1.137}$$

by Definition 23.1.10. □

Remark. An important property of the covariation is that two independent semi-martingales have zero covariation. However, just as there exist many pairs of random variables with zero correlation which are not independent, the converse is false. A notable exception is the Lévy characterization of Brownian motion.

Definition 23.1.13 (integral of semimartingale)**.** For a continuous semimartingale $X = X_0 + M + A$ with $M_0 = A_0 = 0$ a.s. and H locally bounded and previsible, we define the stochastic integral (which is also a continuous semimartingale)

$$H \cdot X = H \cdot M + H \cdot A, \qquad \text{writing also} \quad (H \cdot X)_t = \int_0^t H_s dX_s, \tag{23.1.138}$$

where $H \cdot M$ is Itô's integral (which is a local martingale) from Definition 23.1.9 and $H \cdot A$ is the finite variation integral (which is also a continuous finite variation process) defined in Proposition 20.4.21. We agree that

$$dZ_t = H_t dX_t \qquad \text{means} \quad Z_t - Z_0 = \int_0^t H_s dX_s \tag{23.1.139}$$

Proposition 23.1.24 (Kunita Watanabe identity)**.** Let X, Y be (sample) continuous semimartingales and H be a locally bounded previsible process. Then

$$[H \cdot X, Y] = H \cdot [X,Y] = [X, H \cdot Y]. \tag{23.1.140}$$

Remark. This is Kunita Watanabe identity for semimartingale.

In particular, if $B = (B^1, \dots, B^d)$ is a d-dimensional Brownian motion, then $\left[B^i, B^j\right]_t = \delta_{ij} t$.

Proof. Let M, N and A, B be the local martingale parts and finite variation parts of X, Y, respectively. Then by Definition 23.1.13,

$$[H \cdot X, Y] = \Bigg[\underbrace{H \cdot M}_{\text{local martingale}} + \underbrace{H \cdot A}_{\text{finite variation}}, N + B \Bigg] = [H \cdot M, N] = H \cdot [M,N] = H \cdot [X,Y] \tag{23.1.141}$$

by Theorem 23.1.19 and Definition 23.1.12. Then by symmetry of covariance (Proposition 23.1.18), we have $[X,Y] = [Y,X]$ and

$$H \cdot [X,Y] = H \cdot [Y,X] = H \cdot [N,M] = [H \cdot N, M] = [M, H \cdot N] = [X, H \cdot Y]. \tag{23.1.142}$$

□

Under the additional assumption that H is left-continuous, one can show that the Riemann sum approximation to the integral converges.

Proposition 23.1.25. Let X be a (sample) continuous semimartingale and H be a left-continuous, adapted and locally bounded process. Then

$$\sum_{k=0}^{\lfloor 2^n t \rfloor - 1} H_{k2^{-n}} (X_{(k+1)2^{-n}} - X_{k2^{-n}}) \to \int_0^t H_s dX_s \quad \text{u.c.p. as } n \to \infty. \tag{23.1.143}$$

Proof. By Theorem 20.4.17, H is previsible so the integral is well-defined.

We can treat the finite variation part $X_0 + A$ and the local martingale part M separately. The first is proved in Theorem 20.4.23,

$$(H \cdot A)_t = \lim_{n \to \infty} \sum_{k=0}^{\infty} H_{k2^{-n}} (A_{(k+1)2^{-n} \wedge t} - A_{k2^{-n} \wedge t}) \text{ a.s.} \tag{23.1.144}$$

and thus, $(H \cdot A)_t \to \sum_{k=0}^{\infty} H_{k2^{-n}}(A_{(k+1)2^{-n}\wedge t} - A_{k2^{-n}\wedge t})$ u.c.p.. So it suffices to show that

$$\sum_{k=0}^{\lfloor 2^n t\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}}) \to (H \cdot M)_t \quad \text{u.c.p. as } n \to \infty \tag{23.1.145}$$

when $M \in \mathcal{M}_{c,loc}$ with $M_0 = 0$.

First let H bounded uniformly and $H^n_t = H_{2^{-n}\lfloor 2^n t\rfloor}$. Then $H^n_t \to H_t$ a.s. as $n \to \infty$ by left continuity. Now,

$$(H^n \cdot M)_t = \sum_{k=0}^{\lfloor 2^n t\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}}) + H_{2^{-n}\lfloor 2^n t\rfloor}(M_t - M_{2^{-n}\lfloor 2^n t\rfloor}) \tag{23.1.146}$$

where, since M is (sample) continuous (and therefore almost surely uniformly continuous on any compact interval), $M_t - M_{2^{-n}\lfloor 2^n t\rfloor} \to 0$ u.c.p as $n \to \infty$. We can thus ignore the second term on the right. Now

$$\left\|H^n - H^k\right\|_M = \mathbb{E}\left(\int_0^\infty (H^n_t - H_t)^2 d[M]_t\right) \to 0 \quad \text{as } n \to \infty \tag{23.1.147}$$

by bounded convergence theorem (Theorem 19.3.10) and the fact that $H^n_t \to H_t$ for every t as $n \to \infty$. By the isometry property (Theorem 23.1.13), $H^n \cdot M \to H \cdot M$ in $\mathcal{M}^2_c$. Using Doob's inequality (Corollary 20.5.10), it is easy to see that this implies u.c.p. convergence. That is, for any $\varepsilon > 0$ and $t \geq 0$

$$\begin{aligned}
\mathbb{P}\left(\sup_{0\leq s\leq t} |(H^n \cdot M)_s - (H \cdot M)_s| > \varepsilon\right) &\leq \frac{\left\|\sup_{0\leq s\leq t} |(H^n \cdot M)_s - (H \cdot M)_s|\right\|_2}{\varepsilon} \leq \frac{\left\|\sup_{t\geq 0} |(H^n \cdot M)_t - (H \cdot M)_t|\right\|_2}{\varepsilon} \\
&\leq \frac{4\left\|(H^n \cdot M)_\infty - (H \cdot M)_\infty\right\|_2}{\varepsilon} = \frac{4\left\|H^n \cdot M - H \cdot M\right\|}{\varepsilon} \to 0
\end{aligned}$$

Now let H be locally bounded and M be local martingale. Suppose T_m reduce both processes with $T_m \uparrow \infty$. Thus,

$$\sum_{k=0}^{\lfloor 2^n t\rfloor -1} H^{T_m}_{k2^{-n}}(M^{T_m}_{(k+1)2^{-n}} - M^{T_m}_{k2^{-n}}) \to \sum_{k=0}^{\lfloor 2^n t\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}}) \text{ a.s..} \tag{23.1.148}$$

which gives that (since there countably many intervals for fixed n as $k2^{-n} \in \mathbb{Q}^+$)

$$\sup_{0\leq s\leq t}\left|\sum_{k=0}^{\lfloor 2^n s\rfloor -1} H^{T_m}_{k2^{-n}}(M^{T_m}_{(k+1)2^{-n}} - M^{T_m}_{k2^{-n}}) - \sum_{k=0}^{\lfloor 2^n s\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}})\right| \to 0 \text{ a.s..} \tag{23.1.149}$$

as $m \to \infty$. Also, $(H^{T_n} \cdot M^{T_n})_t \to (H \cdot M)_t$ a.s. gives that $\sup_{0\leq s\leq t}\left|(H^{T_m} \cdot M^{T_m})_s - (H \cdot M)_s\right| \to 0$ a.s. as $m \to \infty$. Then

$$\sup_{0\leq s\leq t}\left|\sum_{k=0}^{\lfloor 2^n s\rfloor -1} H^{T_m}_{k2^{-n}}(M^{T_m}_{(k+1)2^{-n}} - M^{T_m}_{k2^{-n}}) - \sum_{k=0}^{\lfloor 2^n s\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}}) + \left((H^{T_m} \cdot M^{T_m})_s - (H \cdot M)_s\right)\right| \to 0 \text{ a.s..} \tag{23.1.150}$$

as $m \to \infty$. Thus, we have

$$\begin{aligned}
&\mathbb{P}\left(\sup_{0\leq s\leq t}\left|\sum_{k=0}^{\lfloor 2^n s\rfloor -1} H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}} - (H \cdot M)_s\right| > \varepsilon\right) \\
\leq\ &\mathbb{P}\left(\sup_{0\leq s\leq t}\left|\sum_{k=0}^{\lfloor 2^n s\rfloor -1} H^{T_m}_{k2^{-n}}(M^{T_m}_{(k+1)2^{-n}} - M^{T_m}_{k2^{-n}}) - \left(H_{k2^{-n}}(M_{(k+1)2^{-n}} - M_{k2^{-n}})\right) + (H^{T_m} \cdot M^{T_m})_s - (H \cdot M)_s\right| > \varepsilon/2\right) \\
&\qquad + \mathbb{P}\left(\sup_{0\leq s\leq t}\left|\sum_{k=0}^{\lfloor 2^n s\rfloor -1} H^{T_m}_{k2^{-n}}(M^{T_m}_{(k+1)2^{-n}} - M^{T_m}_{k2^{-n}}) + (H^{T_m} \cdot M^{T_m})_s\right| > \varepsilon/2\right) \\
\to\ &0 + 0 = 0
\end{aligned}$$

Therefore,

$$\sum_{k=0}^{\lfloor 2^n t\rfloor -1} H_{k2^{-n}}(X_{(k+1)2^{-n}} - X_{k2^{-n}}) \to (H\cdot X)_t = \int_0^t H_s dX_s \quad \text{u.c.p. as } n\to\infty. \tag{23.1.151}$$

□

23.1.7 Itô's formula

Theorem 23.1.26 (integration by parts)**.** Let X, Y be (sample) continuous semimartingales. Then

$$X_tY_t - X_0Y_0 = \int_0^t X_s dY_s + \int_0^t Y_s dX_s + [X,Y]_t \quad \text{a.s..} \tag{23.1.152}$$

Proof. By Proposition 20.4.19, the integrals are well-defined.

Since both sides are (sample) continuous in t, it suffices to consider $t = M2^{-N}$ for $M, N \geq 1$. Note that

$$X_tY_t - X_sY_s = X_s(Y_t - Y_s) + Y_s(X_t - X_s) + (X_t - X_s)(Y_t - Y_s) \tag{23.1.153}$$

so for $n \geq N$,

$$\begin{aligned} X_tY_t - X_0Y_0 &= \sum_{k=0}^{M2^{n-N}-1} X_{k2^{-n}}(Y_{(k+1)2^{-n}} - Y_{k2^{-n}}) + \sum_{k=0}^{M2^{n-N}-1} Y_{k2^{-n}}(X_{(k+1)2^{-n}} - X_{k2^{-n}}) \\ &\quad + \sum_{k=0}^{M2^{n-N}-1} (X_{(k+1)2^{-n}} - X_{k2^{-n}})(Y_{(k+1)2^{-n}} - Y_{k2^{-n}}) \\ &\xrightarrow{\text{u.c.p.}} (X\cdot Y)_t + (Y\cdot X)_t + [X,Y]_t \qquad \text{as } n\to\infty \end{aligned}$$

by Proposition 23.1.25 and Proposition 23.1.18 (ii). □

Proposition 23.1.27. Let $(M_t)_{t\geq 0}$ be a continuous local martingale. Then for all $t \geq 0$,

$$M_t^2 = M_0^2 + 2\int_0^t M_s dM_s + [M]_t \quad \text{a.s..} \tag{23.1.154}$$

Remark. In particular if $(B_t)_{t\geq 0}$ is a one-dimensional standard Brownian motion, then

$$B_t^2 = 2\int_0^t B_s dB_s + t \quad \text{a.s.} \tag{23.1.155}$$

is a semimartingale.

Note the extra covariation term which we do not get in the deterministic case. The next result, Itô's formula, tells us that a smooth function of a continuous semimartingale is again a continuous semimartingale and gives us its precise decomposition in a sort of chain rule.

Theorem 23.1.28 (Itô's formula)**.** The filtered space satisfies the usual conditions. Let $X^1, X^2, \ldots, X^d$ be (sample) continuous semimartingales and set $X = (X^1, \ldots, X^d)$. Let $f : \mathbb{R}^d \to \mathbb{R}, x \mapsto f(x)$ and $f \in C^2(\mathbb{R}^d)$. Then

$$f(X_t) = f(X_0) + \sum_{i=1}^d \int_0^t \frac{\partial f(X_s)}{\partial X^i} dX_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 f(X_s)}{\partial X^i \partial X^j} d[X^i, X^j]_s \quad \text{a.s..} \qquad (*) \tag{23.1.156}$$

Remark. (i) In particular, $f(X)$ is a continuous semimartingale with decomposition

$$f(X_t) = f(X_0) + \underbrace{\sum_{i=1}^d \int_0^t \frac{\partial f(X_s)}{\partial X^i} dM_s^i}_{\in \mathcal{M}_{c,loc}} + \underbrace{\sum_{i=1}^d \int_0^t \frac{\partial f(X_s)}{\partial X^i} dA_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 f(X_s)}{\partial X^i \partial X^j} d[M^i, M^j]_s}_{\text{finite variation}}. \tag{23.1.157}$$

where the covariation of the $\mathbb{R}^d$-valued semimartingale $X = X_0 + A + M$ is $[X^i, X^j] = [M^i, M^j]$ (by Definition 23.1.12), due to quadratic variation and the polarization identity 23.1.10.

(ii) Intuitive proof by Taylor expansion for $d = 1$:

$$\begin{aligned} f(X_t) &= f(X_0) + \sum_{k=0}^{\lfloor 2^n t\rfloor - 1} \left(f(X_{(k+1)2^{-n}}) - f(X_{k2^{-n}})\right) + \left(f(X_t) - f(X_{\lfloor 2^n t\rfloor 2^{-n}}\right) \\ &= f(X_0) + \sum_{k=0}^{\lfloor 2^n t\rfloor - 1} f'(X_{k2^{-n}}) \left(X_{(k+1)2^{-n}} - X_{k2^{-n}}\right) + \frac{1}{2} \sum_{k=0}^{\lfloor 2^n t\rfloor - 1} f''0(X_{k2^{-n}}) \left(X_{(k+1)2^{-n}} - X_{k2^{-n}}\right)^2 + \text{error} \\ &\overset{\text{u.c.p.}}{\to} f(X_0) + \int_0^t f'(X_s) dX_s + \frac{1}{2} \int_0^t f''(X_s) d[X]_s. \end{aligned}$$

We will not follow this method of proof, because the error terms are hard to deal with.

Proof. For $d = 1$. Write $X = X_0 + M + A$, where A has total variation process V (Definition 20.4.17). Let

$$T_r = \inf\{t \geq 0 : Y_t > r\}, \qquad \text{where } Y_t = |X_t| + V_t + [M]_t. \tag{23.1.158}$$

Since Y_t is (sample) continuous, we have that T_r is stopping time by Proposition 20.4.7. If $\lim_{r\to\infty} T_r(\omega)$ is not infinite, it must converge to $T(\omega)$ as it is increasing. Then by (sample) continuity of Y_t, we have that $Y_{T_r(\omega)}(\omega) \to Y_{T(\omega)}(\omega)$ a.s., then $\forall \varepsilon$, there exists $N \in \mathbb{N}$ such that $\forall n > m \geq N$, $\left|Y_{T_n(\omega)}(\omega) - Y_{T_m(\omega)}(\omega)\right| < \varepsilon$. However, we know that

$$\left|Y_{T_n(\omega)}(\omega) - Y_{T_m(\omega)}(\omega)\right| = |\pm n \pm m| \geq 1 \qquad \text{contradiction.} \tag{23.1.159}$$

Then $(T_r)_{r\geq 0}$ is a family of stopping times with $T_r \uparrow \infty$ a.s.. It is sufficient to prove the required result on the time intervals $[0, T_r]$.

Let $\mathcal{A} \subseteq C^2(\mathbb{R})$ denote the subset of functions $f : \mathbb{R} \to \mathbb{R}$ for which the formula holds. Then

(i) $\mathcal{A}$ contains the functions $f(x) \equiv 1$ and $f(x) = x$.

(ii) $\mathcal{A}$ is a vector space over $\mathbb{R}$ (see Definition 8.1.1).

Below we will show that $\mathcal{A}$ is, in fact, an algebra (see Definition 8.1.3 and Definition 8.1.4), i.e. in addition

(iii) $f, g \in \mathcal{A} \;\Rightarrow\; fg \in \mathcal{A}$.

Finally we will show that[15]

(iv) if $f_n \in \mathcal{A}$ and $f_n \to f$ in $C^2(B_r)$ for all $r > 0$ then $f \in \mathcal{A}$, where $f_n \to f$ in $C^2(B_r)$ means that $\Delta_{n,r} \to 0$ as $n \to \infty$ with $B_r = \{x : |x| \leq r\}$ and

$$\Delta_{n,r} := \max\left\{ \sup_{x\in B_r} |f_n(x) - f(x)|, \sup_{x\in B_r} |f_n'(x) - f'(x)|, \sup_{x\in B_r} |f_n''(x) - f''(x)| \right\}. \tag{23.1.160}$$

(i) -(iii) imply that $\mathcal{A}$ contains all polynomials. By Weierstrass' approximation theorem (Corollary 14.0.3), these are dense in $C^2(B_r)$ and so (iv) implies $\mathcal{A} = C^2(B_r)$.

Proof of (i). For $f(x) = 1$, $(*)$ holds obviously as $f(X_t) = 1 = f(X_0)$.

For $f(x) = x$, we have that $\frac{\partial^2 f(x)}{\partial x^2} = 0$ and

$$f(X_t) = X_t = X_0 + X_t - X_0 = X_0 + \int_0^t 1 dX_s = f(X_0) + \int_0^t \frac{\partial f(X_s)}{\partial X_s} dX_s \quad \text{which is } (*). \tag{23.1.161}$$

[15] the proof is similar to the one for monotone class theorem (Theorem 15.2.9)

Proof of (ii). For any $a, b \in \mathbb{R}$ and $f, g \in \mathcal{A}$, we have for f, g $(*)$ holds. Thus, $af + bg \in C^2(\mathbb{R})$ and

$$\begin{aligned}(af+bg)(X_t) = af(X_t) + bg(X_t) &= a\left(f(X_0) + \sum_{i=1}^d \int_0^t \frac{\partial f(X_s)}{\partial X^i} dX_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 f(X_s)}{\partial X^i \partial X^j} d[X^i, X^j]_s\right) \\ &\quad + b\left(g(X_0) + \sum_{i=1}^d \int_0^t \frac{\partial g(X_s)}{\partial X^i} dX_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 g(X_s)}{\partial X^i \partial X^j} d[X^i, X^j]_s\right) \\ &= (af+bg)(X_0) + \sum_{i=1}^d \int_0^t \frac{\partial (af+bg)(X_s)}{\partial X^i} dX_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 (af+bg)(X_s)}{\partial X^i \partial X^j} d[X^i, X^j]_s\end{aligned}$$

as required.

Proof of (iii). Suppose $f, g \in \mathcal{A}$ and set $F_t = f(X_t)$, $G_t = g(X_t)$. Since the formula holds for f and g, F and G are continuous semimartingales by Theorem 20.4.21 and Theorem 23.1.16. Integration by parts (Theorem 23.1.26) yields

$$F_t G_t - F_0 G_0 = \int_0^t F_s dG_s + \int_0^t G_s dF_s + [F, G]_t \quad \text{a.s.} \qquad (\dagger). \tag{23.1.162}$$

By Theorem 23.1.17, we have $F \cdot G = F \cdot (1 \cdot G)$ in the sense of indistinguishability, and using Itô's formula for $(1 \cdot G)_s = g(X_s) - g(X_0)$ we get again by Theorem 23.1.17 as g satisfies $(*)$,

$$\int_0^t F_s dG_s = \int_0^t f(X_s) g'(X_s) dX_s + \frac{1}{2}\int_0^t f(X_s) g''(X_s) d[X]_s. \tag{23.1.163}$$

Similarly, we have

$$\int_0^t G_s dF_s = \int_0^t f'(X_s) g'(X_s) dX_s + \frac{1}{2}\int_0^t f''(X_s) g(X_s) d[X]_s. \tag{23.1.164}$$

Also, we have the covariation of two semimartingale is just the covariation of their local martingale parts,

$$[F, G]_t = [f'(X) \cdot X, g'(X) \cdot X]_t = f'(X) g'(X) [X, X]_t = \int_0^t f'(X_s) g'(X_s) d[X]_s. \tag{23.1.165}$$

by applying Kunita-Watanabe identity (Proposition 23.1.20). Substituting these into $(\dagger)$, we obtain Itô's formula for fg,

$$\begin{aligned}(fg)(X_t) &= (fg)(X_0) + \int_0^t \left(f(X_s) g'(X_s) + f(X_s) g'(X_s)\right) dX_s \\ &\quad + \frac{1}{2}\int_0^t \left(f(X_s) g''(X_s) + 2 f'(X_s) g'(X_s) + f''(X_s) g(X_s)\right) d[X]_s \\ &= (fg)(X_0) + \int_0^t (fg)'(X_s) dX_s + \frac{1}{2}\int_0^t (fg)''(X_s) d[X]_s.\end{aligned}$$

Proof of (iv). Let $f_n \in \mathcal{A}$ such that $f_n \to f$ in $C^2(B_r, \mathbb{R})$. Then by definition of $\Delta_{n,r}$, for an arbitrary finite positive number ε,

$$\begin{aligned}&\left|\int_0^{t\wedge T_r} (f_n'(X_s) - f'(X_s)) dA_s + \frac{1}{2}\int_0^{t\wedge T_r} (f_n''(X_s) - f''(X_s)) d[M]_s\right| \\ \leq\ &\int_0^{t\wedge T_r} |f_n'(X_s) - f'(X_s)| \, dV_s + \frac{1}{2}\int_0^{t\wedge T_r} |f_n''(X_s) - f''(X_s)| \, d[M]_s \\ \leq\ &\Delta_{n,r}\left(V_{t\wedge T_r} + \frac{1}{2}[M]_{t\wedge T_r}\right) \leq r\Delta_{n,r} \to 0 \text{ as } n \to \infty \text{ a.s.} \quad (\text{as } Y_t \text{ is continuous}) \\ \Rightarrow\ &\int_0^{t\wedge T_r} f_n'(X_s) dA_s + \frac{1}{2}\int_0^{t\wedge T_r} f_n''(X_s) d[M]_s \to \int_0^{t\wedge T_r} f'(X_s) dA_s + \frac{1}{2}\int_0^{t\wedge T_r} f''(X_s) d[M]_s \text{ a.s..}\end{aligned}$$

Moreover, by Proposition 23.1.8, $\mathbb{E}\left[M^{T_r}\right]_\infty = \mathbb{E}\,[M]_\infty^{T_r} = \mathbb{E}\,[M]_{T_r}$ is bounded by $(r+\varepsilon)$ and thus $M^{T_r} \in \mathcal{M}_c^2$ by Theorem 23.1.10.

Since $f_n \to f$ in $C^2(B_r)$, we know that $f_n'(X^{T_r})$ and $f'(X^{T_r})$ are bounded by Theorem 10.3.8). Thus, $f_n'(X^{T_r}) \cdot M^{T_r}$ and

$f'(X^{T_r}) \cdot M^{T_r}$ are well-defined and are in $\mathcal{M}_c^2$ by Theorem 23.1.13. Then by Proposition 23.1.15,

$$\begin{aligned}\left\|f_n'(X^{T_r}) \cdot M^{T_r} - f'(X^{T_r}) \cdot M^{T_r}\right\|^2 &= \left\|(f_n'(X) \cdot M)^{T_r} - (f'(X) \cdot M)^{T_r}\right\|^2 = \|f_n'(X_s) - f'(X_s)\|^2_{\mathcal{L}(M^{T_r})} \\ &= \mathbb{E}\left(\int_0^{T_r} \left(f_n'(X_s) - f'(X_s)\right)^2 d[M]_s\right) \leq \Delta_{n,r}^2 \mathbb{E}\left([M]_{T_r}\right) \leq r\Delta_{n,r}^2 \to 0\end{aligned}$$

as $n \to \infty$ and so $(f_n'(X) \cdot M)^{T_r} \to (f'(X) \cdot M)^{T_r}$ in $\mathcal{M}_c^2$ and

$$\int_0^{t\wedge T_r} f_n'(X_s) dM_s \to \int_0^{t\wedge T_r} f'(X_s) dM_s \text{ a.s.} \tag{23.1.166}$$

For $f_n \in \mathcal{A}$, we have

$$f_n(X_{t\wedge T_r}) = f_n(X_0) + \int_0^{t\wedge T_r} f_n'(X_s) dX_s + \frac{1}{2}\int_0^{t\wedge T_r} f_n''(X_s) d[X]_s \quad \text{a.s..} \tag{23.1.167}$$

Thus, if $|X_0(\omega)| > r$, we have $T_r = 0$, then $(*)$ still holds. If $|X_0(\omega)| \leq r$,

$$\begin{aligned}&\left|f(X_{t\wedge T_r}) - f(X_0) + \int_0^{t\wedge T_r} f'(X_s) dX_s + \frac{1}{2}\int_0^{t\wedge T_r} f''(X_s) d[X]_s\right| \\ \leq\ & |f(X_{t\wedge T_r}) - f_n(X_{t\wedge T_r})| + |f(X_0) - f_n(X_0)| + \left|\int_0^{t\wedge T_r} f_n'(X_s) dM_s - \int_0^{t\wedge T_r} f'(X_s) dM_s\right| \\ &+ \left|\int_0^{t\wedge T_r} f_n'(X_s) dA_s + \frac{1}{2}\int_0^{t\wedge T_r} f_n''(X_s) d[M]_s - \int_0^{t\wedge T_r} f'(X_s) dA_s - \frac{1}{2}\int_0^{t\wedge T_r} f''(X_s) d[M]_s\right| \\ \to\ & |f(X_{t\wedge T_r}) - f_n(X_{t\wedge T_r})| + |f(X_0) - f_n(X_0)| + 0 + 0 \text{ a.s.} \leq 2\Delta_{n,r} \to 0 \text{ a.s.}\end{aligned}$$

as $n \to \infty$ by definition of $\Delta_{n,r}$. Thus,

$$f(X_{t\wedge T_r}) = f(X_0) + \int_0^{t\wedge T_r} f'(X_s) dX_s + \frac{1}{2}\int_0^{t\wedge T_r} f''(X_s) d[X]_s \text{ a.s..} \tag{23.1.168}$$

For $d > 1$, (i) becomes '$\mathcal{A}$ contains the constant 1 and the coordinate functions $f_1(x) = x_1, \ldots, f_d(x) = x_d$.'
We can then follow the same argument, dealing with all the different components X^i, M^i, $[M^i, M^j]$ etc[16]. □

Corollary 23.1.29. Let $X^1, X^2, \ldots, X^d$ be continuous semimartingales and set $X = (X^1, \ldots, X^d)$. Let $f \in C^2(\mathbb{R}^{++} \times \mathbb{R}^d, \mathbb{R})$. Then

$$f(t, X_t) = f(0, X_0) + \int_0^t \frac{\partial f}{\partial t}(s, X_s) ds + \sum_{i=1}^d \int_0^t \frac{\partial f}{\partial x^i}(X_s) dX_s^i + \frac{1}{2}\sum_{i,j=1}^d \int_0^t \frac{\partial^2 f}{\partial x^i \partial x^j}(X_s) d[X^i, X^j]_s. \tag{23.1.169}$$

Proof. This is an immediate consequence of $(*)$ in Theorem 23.1.28. Indeed, the process $t \mapsto t$ is non-decreasing and so of finite variation, so $(t, X_t^1, \ldots, X_t^d)$ is a $(d+1)$-dimensional semi-martingale. The result follows by applying Itô's formula to this $d+1$-dimensional process, and observing that since $t \to t$ is of finite variation, it does not contribute to any of the covariation terms. □

23.2 Applications to Brownian Motion and Martingales

23.2.1 Brownian martingales

As we will see in a few moments, martingales are very useful to understand (and ultimately prove results about) the behaviour of random processes. We start with the following very useful observation.

Theorem 23.2.1 (exponential martingale)**.** Let $M \in \mathcal{M}_{c,loc}$ with $M_0 = 0$ a.s.. Then $Z_t = \exp\left(M_t - \frac{1}{2}[M]_t\right)$ defines a continuous local martingale. We call Z the exponential (local) martingale of M.

[16] need details

Proof. The function $f(x,y) = \exp(x - y/2)$ is $C^2(\mathbb{R}^2)$ and M_t and $[M]_t$ are both semimartingales. By Itô's formula (Theorem 23.1.28),

$$\begin{aligned} dZ_t &= df(M_t,[M]_t) = \frac{\partial f(M_t,[M]_t)}{\partial M_t}dM_t + \frac{\partial f(M_t,[M]_t)}{\partial [M]_t}d[M]_t + \frac{1}{2}\frac{\partial^2 f(M_t,[M]_t)}{\partial M_t^2}d[M]_t \\ &= Z_t\left(dM_t - \frac{1}{2}d[M]_t\right) + \frac{1}{2}Z_t d[M]_t = Z_t dM_t. \end{aligned}$$

We know that Z_t is locally bounded and previsible since Z_t is continuous by Proposition 20.4.19. Thus, $(Z \cdot M)$ is a local martingale by Definition 23.1.9. That is, $Z_t = Z_0 + \int_0^t Z_s dM_s$ is a local martingale. □

Applying this to Brownian motion, we find the following martingales, which are the basis of a finer study of Brownian motion.

Theorem 23.2.2. Let $(B_t)_{t\geq 0}$ be an $(\mathcal{F}_t)$-Brownian motion in $d \geq 1$ dimensions.

(i) If $d \geq 1$ and $B_0 \in \mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$, the process $(|B_t|^2 - dt)_{t\geq 0}$ is a $(\mathcal{F}_t)$-martingale.

(ii) Let $d \geq 1$ and $u = (u_1,\ldots,u_d) \in \mathbb{C}^d$. Assume that $\mathbb{E}\left|\exp(\langle u, B_0\rangle)\right| < \infty$, the process defined by

$$M_t = \exp\left(\langle u, B_t\rangle - t\left|u\right|^2/2\right) \tag{23.2.1}$$

is also a $(\mathcal{F}_t)$-martingale for every $u \in \mathbb{C}^d$, where $|u|^2$ is a notation for $\sum_{i=1}^d u_i\overline{u_i}$.

Remark. This is another version of Theorem 22.1.20.

Proof. We skip the integrability and adaptedness since we can find those in the proof of Theorem 22.1.20.

(i) By Itô's formula (Theorem 23.1.28), we have for $f(x) = x^2$,

$$\begin{aligned} B_t^2 &= f(B_t) = f(B_0) + \int_0^t \frac{\partial f(B_s)}{\partial B_s}dB_s + \frac{1}{2}\int_0^t \frac{\partial^2 f(B_s)}{\partial B_s^2}d[B_s,B_s] \\ &= B_0^2 + 2\int_0^t B_s dB_s + \frac{1}{2}\int_0^t 2ds = B_0^2 + 2\int_0^t B_s dB_s + t. \end{aligned}$$

Thus, $M_t = B_t^2 - t = B_0^2 + 2\int_0^t B_s dB_s$[17] is an $\mathcal{F}$-local martingale as B is semimartingale by Definition 23.1.9.

It thus suffices to show that it is a true martingale, which can be proved for instance by observing that the quadratic variation is (by Theorem 23.1.16),

$$[M]_t = [2B\cdot B]_t = \left(4B^2\cdot[B]\right)_t = 4\int_0^t B_s^2 ds \tag{23.2.2}$$

which has finite expectation for all $t > 0$ by Fubini's theorem (Theorem 15.3.33) as two measures are finite. By Theorem 23.1.10, $(M_{s\wedge t})_{s\geq 0}$ is a martingale bounded in $\mathcal{L}^2(\Omega,\mathcal{F},\mathbb{P})$ and thus it is UI martingale by Proposition 19.3.32.

Hence M is a true martingale by Proposition 20.6.6 with

$$M_T = \begin{cases} M_t & s \geq t \\ M_0 = B_0 & s < t \end{cases} \quad \text{is UI} \tag{23.2.3}$$

as constant t is also a stopping time for $s \geq t$ and 0 is also a stopping time for $s < t$.

(ii) To show that M is a martingale, consider $X^{d+1} = t$ which is a continuous semi-martingale. Let $f : \mathbb{R}^{d+1} \to \mathbb{C}$,

$$f(x_1,\ldots,x_d,x_{d+1}) = \exp\left(\sum_{i=1}^d u_i x_i - u^2 x_{d+1}/2\right). \tag{23.2.4}$$

[17] Note that here $\int_0^t B_s dB_s$ is actually $\int_0^t (B_s - B_0)dB_s$ i.e., the integrand is standard Brownian motion

So $f \in C^2(\mathbb{R}^{d+1})$ and we may apply Itô's formula (Theorem 23.1.28) and obtain:

$$\begin{aligned} M_t &= M_0 + \int_0^t \sum_{i=1}^d u_i \exp\left(\langle u, B_s\rangle - su^2/2\right) dB_s^i - \int_0^t \frac{1}{2} u^2 \exp\left(\langle u, B_s\rangle - su^2/2\right) dt \\ &\quad + \int_0^t \sum_{i=1}^d \sum_{j=1}^d u_i u_j \exp\left(\langle u, B_s\rangle - su^2/2\right) d[B^i, B^j]_s \\ &= M_0 + \int_0^t \sum_{i=1}^d u_i \exp\left(\langle u, B_s\rangle - su^2/2\right) dB_s^i \end{aligned}$$

since $d[B^i, B^j]_t = \delta_{i,j} dt$ and $[B^i, t] = 0$ for all $1 \leq i, j \leq d$ (by Proposition 23.1.22), so that the finite variations term cancel. It thus suffices to show that $\int_0^t u_i \exp\left(\langle u, B_s\rangle - su^2/2\right) dB_s^i$ is a true martingale [18].

Obviously, the stochastic integral is a local martingale as $u_i \exp\left(\langle u, B_s\rangle - su^2/2\right)$ is continuous (thus locally bounded and previsible). Let $u_i = a_i + b_i i$, then we have

$$\begin{aligned} \int_0^t u_i \exp\left(\langle u, B_s\rangle - su^2/2\right) dB_s^i &= \int_0^t (a_i + b_i i) \exp\left(\sum_{j=1}^d (a_j + b_j i) B_s^j - \frac{s}{2} \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) dB_s^i \\ &= \underbrace{\int_0^t \left(a_i \cos(b_i B_s^i) - b_i \sin(b_i B_s^i)\right) \exp\left(\sum_{j=1}^d (a_j B_s^j - \frac{s}{2} \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) dB_s^i}_{=\Re M} \\ &\quad + i \underbrace{\int_0^t \left(a_i \sin(b_i B_s^i) + b_i \cos(b_i B_s^i)\right) \exp\left(\sum_{j=1}^d (a_j B_s^j - \frac{s}{2} \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) dB_s^i}_{=\Im M} \end{aligned}$$

We take the quadratic variation of the real and imaginary parts,

$$[\Re M]_t = \int_0^t \left(a_i \cos(b_i B_s^i) - b_i \sin(b_i B_s^i)\right)^2 \exp\left(\sum_{j=1}^d 2a_j B_s^j - s \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) ds \tag{23.2.5}$$

$$[\Im M]_t = \int_0^t \left(a_i \sin(b_i B_s^i) + b_i \cos(b_i B_s^i)\right)^2 \exp\left(\sum_{j=1}^d 2a_j B_s^j - s \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) ds \tag{23.2.6}$$

Thus,

$$[\Re M]_t + [\Im M]_t = \left(a_i^2 + b_i^2\right) \exp\left(-s \sum_{j=1}^d \left(a_j^2 + b_j^2\right)\right) \int_0^t \exp\left(\sum_{j=1}^d 2a_j B_s^j\right) ds \tag{23.2.7}$$

so by Fubini's theorem (Theorem 15.3.33) and Proposition 19.8.11

$$\int_0^t \mathbb{E}\left(\exp\left(\sum_{j=1}^d 2a_j B_s^j\right)\right) ds = \int_0^t \exp\left(s \sum_{j=1}^d 2a_j^2\right) ds < \infty \tag{23.2.8}$$

where $a = (a^1, \ldots, a^d)^T$. Then use the same trick as in (i), we have that M is a true martingale.

□

Another family of martingales is provided by the result below. This is the first hint of a deep connection between Brownian motion and second-order elliptic partial differential operators, a theme which we will explore in greater detail later on in the course. (This also connects to the theory of martingale problems developed by Stroock and Varadhan, which has proved to be one of the most successful tools in probability theory).

[18] Note B in the integrand is a standard Brownian motion.

Theorem 23.2.3. Let $(B_t)_{t\geq 0}$ be a $(\mathcal{F}_t)$-Brownian motion. Let $f(t,x) : \mathbb{R}^{++} \times \mathbb{R}^d \to \mathbb{C}$ be continuously differentiable in the variable t and twice continuously differentiable in x. Then,

$$M_t = f(t, B_t) - f(0, B_0) - \int_0^t \left(\frac{\partial}{\partial t} + \frac{1}{2}\Delta\right) f(s, B_s)ds, \qquad t \geq 0 \tag{23.2.9}$$

is a $(\mathcal{F}_t)$-local martingale, where $\Delta = \sum_{i=1}^d \frac{\partial^2}{\partial x_i^2}$ is the Laplacian operator acting on the spatial coordinate of f. If moreover, the first derivatives are uniformly bounded on every compact interval, i.e., for all $T > 0$,

$$\sup_{t\in[0,T]} \sup_{x\in\mathbb{R}^d} \left|\frac{\partial f}{\partial x_i}(t,x)\right| < \infty \quad \text{for all } 1 \leq i \leq d, \tag{23.2.10}$$

then M is a true martingale.

Remark. This is another verision of Theorem 22.1.23

Proof. By Itô's formula (Corollary 23.1.29),

$$M_t = \int_0^t \sum_{i=1}^d \frac{\partial f}{\partial x_i}(s, B_s)dB_s^i \tag{23.2.11}$$

is indeed a local martingale. The fact it is a true martingale when the first partial derivatives are uniformly bounded on every compact time interval, follows from the fact that the quadratic variation of M^f is bounded on on every compact time interval, and hence it is a true martingale (even bounded in $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$) on every compact time interval. □

23.2.2 Dubins-Schwarz theorem

Theorem 23.2.4 (Lévy's characterization of Brownian motion)**.** Let $X^1, \ldots, X^d \in \mathcal{M}_{c,loc}$. The two following statements are equivalent:

(i) For all $t \geq 0$, $[X^i, X^j]_t = \delta_{ij}t$.

(ii) $X = (X^1, \ldots, X^d)$ is a standard Brownian motion in $\mathbb{R}^d$ (i.e., $X^1, \ldots, X^d$ are independent standard Brownian motions).

Proof. It is easy to show that (ii) implies (i).

For the inverse, it suffices to show that, for $0 \leq s \leq t$, $X_t - X_s \sim \mathcal{N}(0, (t-s)I)$ and the increment is independent of $\mathcal{F}_s$. By uniqueness of characteristic functions and Theorem 19.5.8, this is equivalent to showing that for all $s \leq t$ and for all $\theta \in \mathbb{R}^d$,

$$\mathbb{E}\left(\exp(i\left\langle\theta, X_t - X_s\right\rangle)|\mathcal{F}_s\right) = \exp\left(-\frac{1}{2}\left\|\theta\right\|^2(t-s)\right). \quad (*) \tag{23.2.12}$$

Here $\langle\cdot,\cdot\rangle$ is the usual scalar product on $\mathbb{R}^d$ and $\|\theta\|$ is the Euclidean norm[19]). Fix $\theta \in \mathbb{R}^d$ and set

$$Y_t = \langle\theta, X_t\rangle = \theta_1 X_t^1 + \cdots + \theta_d X_t^d. \tag{23.2.13}$$

Then Y is a local martingale, and by the assumptions and the bilinearity of the covariation, $[Y] = \sum_{i=1}^d \theta_i^2 t = t\left\|\theta\right\|^2$. Define also

$$Z_t = \exp\left(iY_t + \frac{1}{2}[Y]_t\right) = \exp\left(i\left\langle\theta, X_t\right\rangle + \frac{1}{2}\left\|\theta\right\|^2 t\right). \tag{23.2.14}$$

Z is is the exponential martingale associated with iY_t which is a local martingale, so $Z \in \mathcal{M}_{c,loc}$ by Theorem 23.2.1. Moreover, Z is bounded on $[0,t]$ for all $t \geq 0$ (since $[Y]_t = \left\|\theta\right\|^2 t$) and so is a true martingale by Proposition 20.6.6. Hence, $\mathbb{E}(Z_t|\mathcal{F}_s) = Z_s$, or equivalently.

$$\mathbb{E}\left(\frac{Z_t}{Z_s}\middle|\mathcal{F}_s\right) = 1, \quad \text{a.s.} \tag{23.2.15}$$

Then $(*)$ follows directly. □

[19] need definition

23.3 Stochastic Differential Equations

23.4 Problem

Problem 23.4.1. Let $(B_t)_{t\geq 0}$ be a standard Brownian motion. Show that the following two stochastic integrals are Gaussian random variables:

$$\int_0^T tdB_t, \qquad \int_0^T B_t dt \tag{23.4.1}$$

Also, calculate their means, variances and covariance.

Solution First, from definition of stochastic integral (Definition 23.1.3), we have that if the integrand is simple process $H^n = \sum_{i=1}^n \lfloor iT/n \rfloor \mathbb{1}_{(\lfloor (i-1)T/n \rfloor, \lfloor iT/n \rfloor]}$, then the integral at finite time T is Gaussian random variable with mean 0 as it is a weighted sum of independent Brownian motion increments. Note that the means of $(H^n \cdot B)_T$ are all zeros and the variances are bounded by T^2.

Clearly, $B_t^T \in \mathcal{M}_c^2$. Then we can find a sequence of Gaussian random variables $(H^n \cdot B^T) := X^n$ such that $X^n \to \left(\int_0^t sdB_s^T\right)_{t\geq 0}$ in $(\mathcal{M}^2, \|\cdot\|)$. Recall Definition 23.1.5 and Definition 23.1.4 and Proposition 23.1.4, we see that $\|\cdot\|$ and $|||\cdot|||$ are (Lipschitz) equivalent (see Definition 12.0.9) on $\mathcal{M}^2$. Thus, we can see that for time T,

$$X^n \to \int_0^T tdB_t \ \text{ in } \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P}). \tag{23.4.2}$$

Thus, by Proposition 19.3.35, we have $X_T^n \xrightarrow{d} \int_0^T tdB_t$. Since the sequence of Gaussian random variables with bounded means (which are zeros) and variances converges to $\int_0^T tdB_t := Y_T$, we can say $\int_0^T tdB_t$ is also Gaussian by Proposition 19.8.17.

Thus, the means in sequence are all zeros, thus $\mathbb{E}\left(\int_0^T tdB_t\right) = 0$. Furthermore, since $B_t^T \in \mathcal{M}_c^2$, $Y_T = \int_0^T tdB_t \in \mathcal{M}_c^2$ by Definition 23.1.8. Then by Theorem 23.1.9 ($(Y^T)^2 - [Y^T]$ is UI martingale) and Theorem 23.1.16, we have

$$\mathrm{Var}(Y_T) = \mathrm{Var}\left(\int_0^T tdB_t\right) = \mathbb{E}\left(\int_0^T tdB_t\right)^2 = \left[\int_0^T tdB_t\right] = \int_0^T t^2 d[B_t] = \int_0^T t^2 dt = \frac{T^3}{3}. \tag{23.4.3}$$

By Theorem 23.1.26, we have

$$Z_T := \int_0^T B_t dt = TB_T - \int_0^T tdB_t = \int_0^T (T-t)dB_t. \tag{23.4.4}$$

Clearly, Z_T is again a Gaussian with mean zero and $(Z^T)^2 - [Z^T]$ is a UI martingale. Similarly,

$$\mathrm{Var}(Z_T) = \mathbb{E}\left(\int_0^T (T-t)dB_t\right)^2 = \left[\int_0^T (T-t)dB_t\right] = \int_0^T (T-t)^2 d[B_t] = \int_0^T (T-t)^2 dt = \frac{T^3}{3}. \tag{23.4.5}$$

We can see that $TB_T = Y_T + Z_T$. Thus, by Proposition 19.3.43.(ix), we have

$$T^3 = \mathrm{Var}\left(TB_T\right) = \mathrm{Var}(Y_T + Z_T) = \mathrm{Var}(Y_T) + \mathrm{Var}(Z_T) + 2\,\mathrm{Cov}(Y_T, Z_T) = \frac{2T^3}{3} + 2\,\mathrm{Cov}(Y_T, Z_T) \ \Rightarrow \ \rho = \frac{1}{2}, \tag{23.4.6}$$

where ρ is the correlation of Y_T and Z_T.

Part VII

Statistics

Chapter 24

Distributions

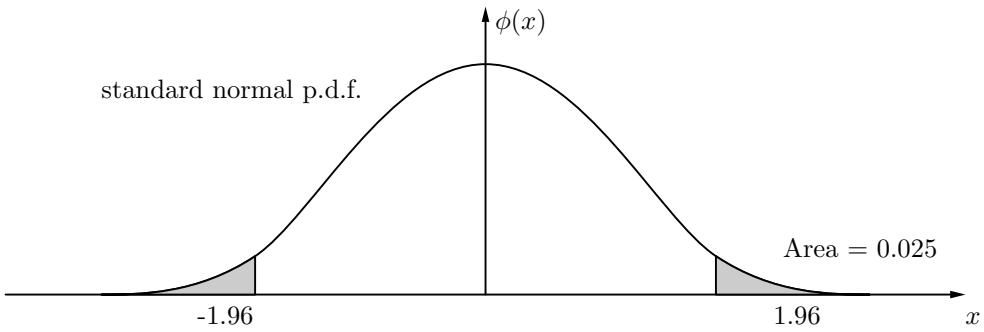
24.0.1 Gaussian distribution

Recall Definition 19.8.6, we see that the important points of the standard normal distribution function are

x	1.28	1.64	1.96	2.33
$\Phi(x)$	0.90	0.95	0.975	0.99

The third of these points leads to an important observation: for $X \sim \mathcal{N}\left(\mu, \sigma^2\right)$,

$$\mathbb{P}\left(\mu - 2\sigma \leq X \leq \mu + 2\sigma\right) = \mathbb{P}\left(\left|\frac{X-\mu}{\sigma}\right| \leq 2\right) \geq \mathbb{P}\left(\left|\frac{X-\mu}{\sigma}\right| \leq 1.96\right) = 0.95, \tag{24.0.1}$$



which is usually summed up in the statement "more than 95% of the normal distribution is within two standard deviations of the mean".

24.0.2 Chi-squared random variables

Definition 24.0.1 (chi-squared random variable)**.** If $Z_1, \ldots, Z_k$ are independent, standard normal random variables, then the sum of their squares,

$$X = \sum_{i=1}^{k} Z_i^2, \tag{24.0.2}$$

is called chi-squared distributed with $k \in \mathbb{N}$ degrees of freedom. Its density function is

$$f_X(x) = \frac{1}{\Gamma\left(k/2\right)} 2^{-k/2} x^{k/2-1} e^{-x/2}, \qquad x \in [0, \infty) \tag{24.0.3}$$

We write $X \sim \chi_k^2$.

Proposition 24.0.2. Suppose that $X \sim \chi_k^2$. Then its density function is the form in Definition 24.0.1.

Proof. We start from the case $k = 1$,

$$\mathbb{P}\left(X \leq x\right) = \mathbb{P}\left(Z^2 \leq x\right) = \mathbb{P}\left(-\sqrt{x} \leq Z \leq \sqrt{x}\right) = \frac{1}{\sqrt{2\pi}} \int_{-\sqrt{x}}^{\sqrt{x}} e^{-y^2/2} dy. \tag{24.0.4}$$

Then taking the differentiation, we have ($\Gamma(1/2) = \sqrt{\pi}$ from Proposition 4.5.2)

$$f_X(x) = \frac{1}{\sqrt{2\pi}} 2 \left(\frac{1}{2} x^{-1/2} e^{-x/2} \right) = \frac{1}{\sqrt{2\pi}} x^{-1/2} e^{-x/2} = \frac{1}{\Gamma(1/2)} 2^{-1/2} x^{1/2-1} e^{-x/2}. \tag{24.0.5}$$

Now assume the formula is true for $k-1$ degree. With the convolution of density functions, we have

$$\begin{aligned} f_X^k(x) &= \int_0^x f_X^{k-1}(y) f_X^1(x-y) dy = \int_0^x \frac{1}{\Gamma\left((k-1)/2\right)} 2^{-(k-1)/2} y^{(k-1)/2-1} e^{-y/2} \frac{1}{\sqrt{2\pi}} (x-y)^{-1/2} e^{-(x-y)/2} dy \\ &= 2^{-k/2} e^{-x/2} \int_0^x \frac{1}{\Gamma(1/2)\,\Gamma\left((k-1)/2\right)} y^{(k-1)/2-1} (x-y)^{-1/2} dy \\ &= \frac{1}{\Gamma(k/2)} 2^{-k/2} x^{k/2-1} e^{-x/2} \int_0^1 \frac{1}{B(1/2,(k-1)/2)} z^{(k-1)/2-1} (1-z)^{-1/2} dz = \frac{1}{\Gamma(k/2)} 2^{-k/2} x^{k/2-1} e^{-x/2}. \end{aligned}$$

by Beta distribution. □

Proposition 24.0.3. Suppose $X \sim \chi_k^2$. Then for $\theta < \frac{1}{2}$ and $t \in \mathbb{R}$,

$$M_X(\theta) = \left(\frac{1}{1-2\theta} \right)^{k/2}, \qquad \phi_X(t) = \left(\frac{1}{1-2it} \right)^{k/2}. \tag{24.0.6}$$

Proof. From Definition 19.5.4,

$$\begin{aligned} M_X(\theta) &= \mathbb{E}\left(e^{\theta X}\right) = \int_0^\infty e^{\theta x} \frac{1}{\Gamma\left(k/2\right)} 2^{-k/2} x^{k/2-1} e^{-x/2} dx \\ &= \left(\frac{1/2}{1/2-\theta} \right)^{k/2} \int_0^\infty \frac{1}{\Gamma\left(k/2\right)} 2^{-k/2} \left(\frac{(1/2-\theta)}{1/2} x \right)^{k/2-1} e^{-(\frac{(1/2-\theta)}{1/2})x/2} d\frac{(1/2-\theta)}{1/2} x \\ &= \left(\frac{1}{1-2\theta} \right)^{k/2} \int_0^\infty \frac{1}{\Gamma\left(k/2\right)} 2^{-k/2} y^{k/2-1} e^{-y/2} dy = \left(\frac{1}{1-2\theta} \right)^{k/2}. \end{aligned}$$

Similarly for $\phi_X(t)$. □

Proposition 24.0.4. Suppose $X \sim \chi_k^2$. Then

$$\text{(i) } \mathbb{E}X = k, \quad \text{(ii) } \operatorname{Var} X = 2k, \quad \text{(iii) } \operatorname{Skew}(X) = \sqrt{8/k}, \quad \text{(iv) } \operatorname{Kurt}(X) = 12/k.$$

Proof. With Propositions 24.0.3, 19.5.10,

$$\mathbb{E}X = \left. \frac{dM_X(\theta)}{d\theta} \right|_{\theta=0} = \left. k(1-2\theta)^{-k/2-1} \right|_{\theta=0} = k, \qquad \mathbb{E}X^2 = \left. \frac{d^2 M_X(\theta)}{d\theta^2} \right|_{\theta=0} = \left. k(k+2)(1-2\theta)^{-k/2-2} \right|_{\theta=0} = k^2 + 2k.$$

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = k^2 + 2k - k^2 = 2k$. Also,

$$\mathbb{E}X^3 = \left. \frac{d^3 M_X(\theta)}{d\theta^3} \right|_{\theta=0} = \left. k(k+2)(k+4)(1-2\theta)^{-k/2-3} \right|_{\theta=0} = k(k+2)(k+4). \tag{24.0.7}$$

Thus,

$$\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = k(k+2)(k+4) - 3k(k^2+2k) + 2k^3 = 8k. \tag{24.0.8}$$

By Definition 19.5.5, $\operatorname{Skew}(X) = \frac{8k}{(2k)^{3/2}} = \sqrt{8/k}$. Furthermore,

$$\mathbb{E}X^4 = \left. \frac{d^4 M_X(\theta)}{d\theta^4} \right|_{\theta=0} = \left. k(k+2)(k+4)(k+6)(1-2\theta)^{-k/2-4} \right|_{\theta=0} = k(k+2)(k+4)(k+6). \tag{24.0.9}$$

Thus,

$$\begin{aligned} \mathbb{E}\left(X-\mu\right)^4 &= \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 \\ &= k(k+2)(k+4)(k+6) - 4k k(k+2)(k+4) + 6k^3(k+2) - 3k^4 = 12k^2 + 48k. \end{aligned}$$

By Definition 19.5.6, we have $\text{Kurt}(X) = \frac{12k^2+48k}{4k^2} - 3 = 12/k$. □

We can extend to more general case.

Definition 24.0.2 (non-central chi-squared random variable)**.** Let Z_i be k independent, normally distributed random variables with means μ_i and variances σ_i^2. Then the random variable

$$X = \sum_{i=1}^{k} \left(\frac{Z_i}{\sigma_i}\right)^2 \tag{24.0.10}$$

is distributed according to the noncentral chi-squared distribution. It has two parameters: k which specifies the number of degrees of freedom (i.e. the number of Z_i), and λ which is related to the mean of the random variables Z_i by:

$$\lambda = \sum_{i=1}^{k} \left(\frac{\mu_i}{\sigma_i}\right)^2. \tag{24.0.11}$$

λ is called the noncentrality parameter. It density function is

$$f_X(x) = \frac{1}{2} e^{-(x+\lambda)/2} \left(\frac{x}{\lambda}\right)^{k/4-1/2} I_{k/2-1}\left(\sqrt{\lambda x}\right) \tag{24.0.12}$$

where $I_\nu(z)$ is modified Bessel function of the first kind. We write $X \sim \chi_k^2(\mu_i, \sigma_i^2)$.

Remark. If $\lambda \to 0$, from Proposition 16.2.3 (if $z \to 0$, $I_\nu(z) \sim \left(\frac{1}{2}z\right)^\nu / \Gamma(\nu+1)$) we have

$$f_X(x) \sim \frac{1}{2} e^{-(x+\lambda)/2} \left(\frac{x}{\lambda}\right)^{k/4-1/2} \left(\frac{1}{2}\sqrt{\lambda x}\right)^{k/2-1} \Big/ \Gamma(k/2) = \frac{1}{\Gamma(k/2)} 2^{-k/2} x^{k/2-1} e^{-x/2} \tag{24.0.13}$$

which is consistent with Definition 24.0.1

Proposition 24.0.5. Suppose that $X \sim \chi_k^2(\mu_i, \sigma_i^2)$. Then its density function is the form in Definition 24.0.2.

Proof. We start from the case $k = 1$,

$$\mathbb{P}(X \le x) = \mathbb{P}\left(Z^2 \le \sigma^2 x\right) = \mathbb{P}\left(-\sigma\sqrt{x} \le Z \le \sigma\sqrt{x}\right) = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\sigma\sqrt{x}}^{\sigma\sqrt{x}} e^{-(y-\mu)^2/2\sigma^2} dy. \tag{24.0.14}$$

Then taking the differentiation, we have ($\Gamma(1/2+n) = \frac{(2n)!}{4^n n!}\sqrt{\pi}$ from Proposition 4.5.2)

$$\begin{aligned}
f_X(x) &= \frac{\sigma}{\sqrt{2\pi}\sigma}\left(\frac{1}{2}x^{-1/2}e^{-(\sigma\sqrt{x}-\mu)^2/2\sigma^2} + \frac{1}{2}x^{-1/2}e^{-(\sigma\sqrt{x}+\mu)^2/2\sigma^2}\right) = \frac{1}{2}e^{-(x+\lambda)/2}x^{-1/2}\frac{1}{\sqrt{2\pi}}\left(e^{\frac{\mu}{\sigma}\sqrt{x}} + e^{-\frac{\mu}{\sigma}\sqrt{x}}\right) \\
&= \frac{1}{2}e^{-(x+\lambda)/2}x^{-1/2}\frac{1}{\sqrt{2\pi}}\left(2\sum_{n=0}^{\infty}\frac{(\sqrt{\lambda x})^{2n}}{(2n)!}\right) = \frac{1}{2}e^{-(x+\lambda)/2}x^{-1/2}\left(\sqrt{2}\sum_{n=0}^{\infty}\frac{(\lambda x)^n}{(2n)!\sqrt{\pi}}\right) \\
&= \frac{1}{2}e^{-(x+\lambda)/2}x^{-1/2}\left(\sqrt{2}\sum_{n=0}^{\infty}\frac{(\lambda x)^n}{\Gamma\left(\frac{1}{2}+n\right)4^n n!}\right) = \frac{1}{2}e^{-(x+\lambda)/2}x^{-1/2}\sqrt{2}\left(\frac{2}{\sqrt{\lambda x}}\right)^{-\frac{1}{2}} I_{-1/2}(\sqrt{\lambda x}).
\end{aligned}$$

by Proposition 16.2.1 ($I_\nu(z) = \left(\frac{1}{2}z\right)^\nu \sum_{k=0}^{\infty} \frac{\left(\frac{1}{4}z^2\right)^k}{k!\Gamma(\nu+k+1)}$). This result is consistent with Definition 24.0.2.

Now assume the formula is true for $k-1$ degree. With the convolution of density functions, we have $\lambda = \sum_{i=0}^{k-1}\left(\frac{\mu_i}{\sigma_i}\right)^2$ and $\lambda' = \left(\frac{\mu_k}{\sigma_k}\right)^2$, the density function $f_X^k(x)$ is

$$\begin{aligned}
\int_0^x f_X^{k-1}(y) f_X^1(x-y)dy &= \int_0^x \frac{1}{2}e^{-(y+\lambda)/2}\left(\frac{y}{\lambda}\right)^{k/4-3/4} I_{k/2-3/2}\left(\sqrt{\lambda y}\right)\frac{1}{2}e^{-(x-y+\lambda')/2}\left(\frac{x-y}{\lambda'}\right)^{-1/4} I_{-1/2}\left(\sqrt{\lambda'(x-y)}\right)dy \\
&= \frac{1}{2}e^{-(x+\lambda+\lambda')/2}\int_0^x \frac{1}{2}\left(\frac{y}{\lambda}\right)^{k/4-3/4} I_{k/2-3/2}\left(\sqrt{\lambda y}\right)\left(\frac{x-y}{\lambda'}\right)^{-1/4} I_{-1/2}\left(\sqrt{\lambda'(x-y)}\right)dy
\end{aligned}$$

Thus,

$$\begin{aligned}
I &:= \int_0^x \frac{1}{2}\left(\frac{y}{\lambda}\right)^{k/4-3/4}\left(\frac{x-y}{\lambda'}\right)^{-1/4} I_{k/2-3/2}\left(\sqrt{\lambda y}\right) I_{-1/2}\left(\sqrt{\lambda'(x-y)}\right) dy \\
&= \int_0^x \frac{1}{2}\left(\frac{y}{\lambda}\right)^{k/4-3/4}\left(\frac{x-y}{\lambda'}\right)^{-1/4}\left(\frac{1}{2}\sqrt{\lambda y}\right)^{k/2-3/2}\left(\frac{1}{2}\sqrt{\lambda'(x-y)}\right)^{-1/2}\sum_{n=0}^{\infty}\frac{\left(\frac{1}{4}\lambda y\right)^n}{n!\Gamma((k-1)/2+n)}\sum_{m=0}^{\infty}\frac{\left(\frac{1}{4}\lambda'(x-y)\right)^m}{m!\Gamma(1/2+m)}dy \\
&= \int_0^x \left(\frac{1}{2}\right)^{k/2-1} y^{k/2-3/2}(x-y)^{-1/2}\sum_{n=0}^{\infty}\frac{\left(\frac{1}{4}\lambda y\right)^n}{n!\Gamma((k-1)/2+n)}\sum_{m=0}^{\infty}\frac{\left(\frac{1}{4}\lambda'(x-y)\right)^m}{m!\Gamma(1/2+m)}dy.
\end{aligned}$$

Then by Proposition 16.2.1,

$$\begin{aligned}
I &= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left(\frac{1}{2}\right)^{k/2-1}\frac{\left(\frac{1}{4}\lambda\right)^n\left(\frac{1}{4}\lambda'\right)^m}{n!m!}\int_0^x \frac{(y)^{n+k/2-3/2}(x-y)^{m-1/2}}{\Gamma((k-1)/2+n)\Gamma(1/2+m)}dy \\
&= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left(\frac{1}{2}\right)^{k/2-1}\frac{\left(\frac{1}{4}\lambda\right)^n\left(\frac{1}{4}\lambda'\right)^m x^{k/2+n+m-1}}{n!m!\Gamma(k/2+n+m)} = \left(\frac{1}{2}\right)^{k/2-1}\sum_{l=0}^{\infty}\frac{x^{k/2+l-1}}{\Gamma(k/2+l)}\sum_{n=0}^{l}\frac{\left(\frac{1}{4}\lambda\right)^n\left(\frac{1}{4}\lambda'\right)^{l-n}}{n!(l-n)!} \\
&= \left(\frac{x}{2}\right)^{k/2-1}\sum_{l=0}^{\infty}\frac{\left(\frac{1}{4}(\lambda+\lambda')x\right)^l}{l!\Gamma(k/2+l)} = \left(\frac{x}{2}\right)^{k/2-1}\left(\frac{2}{\sqrt{(\lambda+\lambda')x}}\right)^{k/2-1} I_{k/2-1}\left(\sqrt{(\lambda+\lambda')x}\right)
\end{aligned}$$

as required. Note that the density function can also be achieved by the product of moment generating function. □

Proposition 24.0.6. Suppose $X \sim \chi^2_k(\mu_i, \sigma_i^2)$. Then for $\theta < \frac{1}{2}$ and $t \in \mathbb{R}$,

$$M_X(\theta) = \frac{\exp\left(\frac{\lambda\theta}{1-2\theta}\right)}{(1-2\theta)^{k/2}}, \qquad \phi_X(t) = \frac{\exp\left(\frac{i\lambda t}{1-2it}\right)}{(1-2it)^{k/2}}. \tag{24.0.15}$$

Proof. From Definition 19.5.4,

$$\begin{aligned}
M_X(\theta) &= \mathbb{E}\left(e^{\theta X}\right) = \int_0^{\infty} e^{\theta x}\frac{1}{2}e^{-(x+\lambda)/2}\left(\frac{x}{\lambda}\right)^{k/4-1/2} I_{k/2-1}\left(\sqrt{\lambda x}\right)dx \\
&= \left(\frac{1}{1-2\theta}\right)^{k/4-1/2}\int_0^{\infty}\frac{1}{2}e^{-(x(1-2\theta)+\lambda)/2}\left(\frac{x(1-2\theta)}{\lambda}\right)^{k/4-1/2} I_{k/2-1}\left(\sqrt{\frac{\lambda}{(1-2\theta)}x(1-2\theta)}\right)dx \\
&= \left(\frac{1}{1-2\theta}\right)^{k/4+1/2}\int_0^{\infty}\frac{1}{2}e^{-(x+\frac{\lambda}{1-2\theta})/2}\left(\frac{x}{\lambda}\right)^{k/4-1/2} I_{k/2-1}\left(\sqrt{\frac{\lambda}{(1-2\theta)}x}\right)dx \\
&= \left(\frac{1}{1-2\theta}\right)^{k/2}\int_0^{\infty}\frac{1}{2}e^{-(x+\frac{\lambda}{1-2\theta})/2}e^{-\lambda\left(1-\frac{1}{1-2\theta}\right)/2}\left(\frac{x(1-2\theta)}{\lambda}\right)^{k/4-1/2} I_{k/2-1}\left(\sqrt{\frac{\lambda}{(1-2\theta)}x}\right)dx \\
&= \frac{\exp\left(\frac{\lambda\theta}{1-2\theta}\right)}{(1-2\theta)^{k/2}}.
\end{aligned}$$

Similarly for $\phi_X(t)$. □

Proposition 24.0.7. Suppose $X \sim \chi^2_k(\mu_i, \sigma_i^2)$. Then

$$\text{(i) } \mathbb{E}X = k+\lambda, \quad \text{(ii) } \operatorname{Var}X = 2(k+2\lambda), \quad \text{(iii) } \operatorname{Skew}(X) = \frac{2^{3/2}(k+3\lambda)}{(k+2\lambda)^{3/2}}, \quad \text{(iv) } \operatorname{Kurt}(X) = \frac{12(k+4\lambda)}{(k+2\lambda)^2}.$$

Proof. With Propositions 24.0.6, 19.5.10,

$$\begin{aligned}
\mathbb{E}X &= \left.\frac{dM_X(\theta)}{d\theta}\right|_{\theta=0} = \left.k(1-2\theta)^{-k/2-1}\exp\left(\frac{\lambda\theta}{1-2\theta}\right) + \lambda(1-2\theta)^{-k/2-2}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)\right|_{\theta=0} \\
&= \left.(1-2\theta)^{-k/2-2}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)(k(1-2\theta)+\lambda)\right|_{\theta=0} = k+\lambda.
\end{aligned}$$

$$\begin{aligned}\mathbb{E}X^2 &= \left.\frac{d^2M_X(\theta)}{d\theta^2}\right|_{\theta=0} = (1-2\theta)^{-k/2-4}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)\left(((k+4)(1-2\theta)+\lambda)\left(k(1-2\theta)+\lambda\right)-2k(1-2\theta)^2\right)\Big|_{\theta=0}\\ &= (1-2\theta)^{-k/2-4}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)\left(k(k+2)(1-2\theta)^2+2\lambda(k+2)(1-2\theta)+\lambda^2\right)\Big|_{\theta=0} = k(k+2)+2\lambda(k+2)+\lambda^2.\end{aligned}$$

Thus, $\operatorname{Var}X = \mathbb{E}X^2-(\mathbb{E}X)^2 = k(k+2)+2\lambda(k+2)+\lambda^2-(k+\lambda)^2 = 2(k+2\lambda)$. Also,

$$\begin{aligned}&\mathbb{E}X^3 = \left.\frac{d^3M_X(\theta)}{d\theta^3}\right|_{\theta=0}\\ =\;& (1-2\theta)^{-k/2-6}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)((k+8)(1-2\theta)+\lambda)\left(k(k+2)(1-2\theta)^2+2\lambda(k+2)(1-2\theta)+\lambda^2\right)\Big|_{\theta=0}\\ &+(1-2\theta)^{-k/2-6}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)(1-2\theta)^2\left(-4k(k+2)(1-2\theta)-4\lambda(k+2)\right)\Big|_{\theta=0}\\ =\;& (1-2\theta)^{-k/2-6}\exp\left(\frac{\lambda\theta}{1-2\theta}\right)\left(k(k+2)(k+4)(1-2\theta)^3+3\lambda(k+2)(k+4)(1-2\theta)^2+3\lambda^2(k+4)(1-2\theta)+\lambda^3\right)\Big|_{\theta=0}\\ =\;& k(k+2)(k+4)+3\lambda(k+2)(k+4)+3\lambda^2(k+4)+\lambda^3.\end{aligned}$$

Thus,

$$\begin{aligned}&\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3-3\mu\mathbb{E}X^2+3\mu^2\mathbb{E}X-\mu^3\\ =\;& k(k+2)(k+4)+3\lambda(k+2)(k+4)+3\lambda^2(k+4)+\lambda^3-3(k+\lambda)\left(k(k+2)+2\lambda(k+2)+\lambda^2\right)+2(k+\lambda)^3\\ =\;& 8k+24\lambda.\end{aligned}$$

By Definition 19.5.5, $\operatorname{Skew}(X) = \frac{8k+24\lambda}{2^{3/2}(k+2\lambda)^{3/2}} = \frac{2^{3/2}(k+3\lambda)}{(k+2\lambda)^{3/2}}$. Furthermore,

$$\begin{aligned}&\mathbb{E}X^4 = \left.\frac{d^4M_X(\theta)}{d\theta^4}\right|_{\theta=0}\\ =\;& \frac{(k+12)(1-2\theta)+\lambda}{(1-2\theta)^{k/2+8}}e^{\frac{\lambda\theta}{1-2\theta}}\left(k(k+2)(k+4)(1-2\theta)^3+3\lambda(k+2)(k+4)(1-2\theta)^2+3\lambda^2(k+4)(1-2\theta)+\lambda^3\right)\Big|_{\theta=0}\\ &+\frac{(1-2\theta)^2}{(1-2\theta)^{k/2+8}}e^{\frac{\lambda\theta}{1-2\theta}}\left(-6k(k+2)(k+4)(1-2\theta)^2-12\lambda(k+2)(k+4)(1-2\theta)-6\lambda^2(k+4)\right)\Big|_{\theta=0}\\ =\;& e^{\frac{\lambda\theta}{1-2\theta}}\frac{(k+6)\left(k(k+2)(k+4)(1-2\theta)^4+4\lambda(k+2)(k+4)(1-2\theta)^3+6\lambda^2(k+4)(1-2\theta)^2+4\lambda^3(1-2\theta)\right)+\lambda^4}{(1-2\theta)^{k/2+8}}\Big|_{\theta=0}\\ =\;& (k+6)\left(k(k+2)(k+4)+4\lambda(k+2)(k+4)+6\lambda^2(k+4)+4\lambda^3\right)+\lambda^4\end{aligned}$$

Thus,

$$\begin{aligned}&\mathbb{E}\left(X-\mu\right)^4 = \mathbb{E}X^4-4\mu\mathbb{E}X^3+6\mu^2\mathbb{E}X^2-4\mu^3\mathbb{E}X+\mu^4\\ =\;& (k+6)\left(k(k+2)(k+4)+4\lambda(k+2)(k+4)+6\lambda^2(k+4)+4\lambda^3\right)+\lambda^4-3(k+\lambda)^4\\ &-4(k+\lambda)\left(k(k+2)(k+4)+3\lambda(k+2)(k+4)+3\lambda^2(k+4)+\lambda^3\right)+6(k+\lambda)^2\left(k(k+2)+2\lambda(k+2)+\lambda^2\right)\\ =\;& 12k(k+4)+48\lambda(k+4)+48\lambda^2.\end{aligned}$$

By Definition 19.5.6, we have $\operatorname{Kurt}(X) = \frac{12k(k+4)+48\lambda(k+4)+48\lambda^2}{4(k+2\lambda)^2}-3 = \frac{12(k+4\lambda)}{(k+2\lambda)^2}$. □

24.0.3 Student-t random variables

Definition 24.0.3 (Student-t random variable)**.** A random variable X in $(-\infty,\infty)$ is called Student-t distributed if, for some $\nu>0$, its density function is

$$f_X(x) = \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} = \frac{1}{\sqrt{\nu}\,B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} \tag{24.0.16}$$

where ν is the degree of freedom and $\Gamma(x)$ is Gamma function. We write $X\sim T(\nu)$.

Remark. We need to guarantee the integral of the density function is 1. Take the substitution $x = \sqrt{\nu}\tan\theta$ with $\theta \in [-\pi/2, \pi/2]$.

$$\begin{aligned}
&\int_{-\pi/2}^{\pi/2} \frac{1}{\sqrt{\nu}\, B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(1 + \frac{\nu \tan^2\theta}{\nu}\right)^{-\frac{\nu+1}{2}} \sqrt{\nu}\sec^2\theta d\theta \\
= &\int_{-\pi/2}^{\pi/2} \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(\sec^2\theta\right)^{-\frac{\nu-1}{2}} d\theta = 2\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(\cos^2\theta\right)^{\frac{\nu-1}{2}} \frac{-1}{2\cos\theta\sin\theta} d\cos^2\theta \\
= &-\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(\cos^2\theta\right)^{\frac{\nu}{2}-1} \left(\sin^2\theta\right)^{\frac{1}{2}-1} d\cos^2\theta = \int_0^1 \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} x^{\frac{\nu}{2}-1}(1-x)^{\frac{1}{2}-1} dx = 1
\end{aligned}$$

by beta distribution.

Proposition 24.0.8. Suppose $X \sim T(\nu)$. Then for $t \in \mathbb{R}$,

$$M_X(\theta) \text{ is undefined}, \qquad \phi_X(t) = \frac{K_{\nu/2}\left(\sqrt{\nu}|t|\right)\left(\sqrt{\nu}|t|\right)^{\nu/2}}{\Gamma(\nu/2)2^{\nu/2-1}}. \tag{24.0.17}$$

where $K_\nu(x)$ is modified Bessel function of the second kind.

Proof. By Proposition 16.2.8,

$$\begin{aligned}
\phi_X(t) &= \mathbb{E}\left(e^{itX}\right) = \int_{-\infty}^{\infty} e^{itx} \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})} \left(1 + \frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} dx = 2\frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})} \nu^{\frac{\nu+1}{2}} \int_0^{\infty} \cos\left(|t|\,x\right)\left(\nu + x^2\right)^{-\frac{\nu+1}{2}} dx \\
&= 2^{1-\frac{\nu}{2}} \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\pi}\,\Gamma(\frac{\nu}{2})} (2\nu)^{\frac{\nu}{2}} \int_0^{\infty} \cos\left(|t|\,x\right)\left(\nu + x^2\right)^{-\frac{\nu+1}{2}} dx = \frac{K_{\nu/2}\left(\sqrt{\nu}|t|\right)\left(\sqrt{\nu}|t|\right)^{\nu/2}}{\Gamma(\nu/2)2^{\nu/2-1}}
\end{aligned}$$

as required. □

Proposition 24.0.9. Suppose $X \sim T(\nu)$. Then

$$\text{(i) } \mathbb{E}X = \begin{cases} 0 & \nu > 1 \\ \text{undefined} & \text{otherwise} \end{cases}, \qquad \text{(ii) } \operatorname{Var} X = \begin{cases} \frac{\nu}{\nu-2} & \nu > 2 \\ \infty & 1 < \nu \le 2 \\ \text{undefined} & \text{otherwise} \end{cases},$$

$$\text{(iii) } \operatorname{Skew}(X) = \begin{cases} 0 & \nu > 3 \\ \text{undefined} & \text{otherwise} \end{cases}, \qquad \text{(iv) } \operatorname{Kurt}(X) = \begin{cases} \frac{6}{\nu-4} & \nu > 4 \\ \infty & 2 < \nu \le 4 \\ \text{undefined} & \text{otherwise} \end{cases}.$$

Proof.

$$\begin{aligned}
\mathbb{E}X &= \int_{-\infty}^{\infty} x \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})} \left(1 + \frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} dx = \int_{-\pi/2}^{\pi/2} \frac{\sqrt{\nu}\tan\theta}{\sqrt{\nu}\, B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(1 + \frac{\nu\tan^2\theta}{\nu}\right)^{-\frac{\nu+1}{2}} \sqrt{\nu}\sec^2\theta d\theta \\
&= \int_{-\pi/2}^{\pi/2} \frac{\sqrt{\nu}}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(\sec^2\theta\right)^{-\frac{\nu-1}{2}} \tan\theta d\theta = (1-1)\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} \left(\cos^2\theta\right)^{\frac{\nu-1}{2}} \frac{-1}{2\cos^2\theta} d\cos^2\theta \\
&= (1-1)\int_0^1 \frac{1}{B\left(\frac{1}{2}, \frac{\nu}{2}\right)} x^{\frac{\nu-1}{2}-1}(1-x)^{1-1} dx = 0
\end{aligned}$$

when $\nu - 1 > 0$ since the integral is well-defined by Definition 4.6.1.

$$\begin{aligned}\mathbb{E}X^2 &= \int_{-\infty}^{\infty} x^2 \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} dx = \int_{-\pi/2}^{\pi/2} \frac{\nu\tan^2\theta}{\sqrt{\nu}\,B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(1+\frac{\nu\tan^2\theta}{\nu}\right)^{-\frac{\nu+1}{2}} \sqrt{\nu}\sec^2\theta d\theta \\ &= \int_{-\pi/2}^{\pi/2} \frac{\nu}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(\sec^2\theta\right)^{-\frac{\nu-1}{2}}\tan^2\theta d\theta = 2\nu\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(\cos^2\theta\right)^{\frac{\nu-1}{2}} \frac{-\sin\theta}{2\cos^3\theta} d\cos^2\theta \\ &= \nu\frac{B\left(\frac{3}{2},\frac{\nu}{2}-1\right)}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\int_0^1 \frac{1}{B\left(\frac{3}{2},\frac{\nu}{2}-1\right)} x^{\frac{\nu}{2}-2}(1-x)^{\frac{3}{2}-1}dx.\end{aligned}$$

Thus, if $\nu > 2$, $B\left(\frac{3}{2},\frac{\nu}{2}-1\right)$ is well-defined. Thus,

$$\mathbb{E}X^2 = \frac{\nu B\left(\frac{3}{2},\frac{\nu}{2}-1\right)}{B\left(\frac{1}{2},\frac{\nu}{2}\right)} = \frac{\nu\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{\nu}{2}-1\right)}{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{\nu}{2}\right)} = \frac{\nu\frac{1}{2}}{\frac{\nu}{2}-1} = \frac{\nu}{\nu-2}. \tag{24.0.18}$$

Meanwhile, it is easy to see that if $\nu \leq 2$ the integral is infinity. Thus, we have the required result (since $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2$).

$$\begin{aligned}\mathbb{E}X^3 &= \int_{-\infty}^{\infty} x^3 \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} dx = (1-1)\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(\cos^2\theta\right)^{\frac{\nu-1}{2}} \frac{-\sin^2\theta}{2\cos^4\theta} d\cos^2\theta \\ &= (1-1)\int_0^1 \frac{1}{B\left(\frac{1}{2},\frac{\nu}{2}\right)} x^{\frac{\nu-1}{2}-2}(1-x)^{2-1}dx = 0\end{aligned}$$

when $\frac{\nu-1}{2} - 1 > 0 \;\Rightarrow\; \nu > 3$ since the integral is well-defined by Definition 4.6.1.

By Definition 19.5.5, $\operatorname{Skew}(X) = 0$ for $\nu > 3$. Furthermore,

$$\begin{aligned}\mathbb{E}X^4 &= \int_{-\infty}^{\infty} x^4 \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\,\Gamma(\frac{\nu}{2})}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} dx = 2\nu^2\int_0^{\pi/2} \frac{1}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\left(\cos^2\theta\right)^{\frac{\nu-1}{2}} \frac{-\sin^3\theta}{2\cos^5\theta} d\cos^2\theta \\ &= \nu^2\frac{B\left(\frac{5}{2},\frac{\nu}{2}-2\right)}{B\left(\frac{1}{2},\frac{\nu}{2}\right)}\int_0^1 \frac{1}{B\left(\frac{5}{2},\frac{\nu}{2}-2\right)} x^{\frac{\nu}{2}-3}(1-x)^{\frac{5}{2}-1}dx.\end{aligned}$$

Thus, if $\nu > 2$, $B\left(\frac{3}{2},\frac{\nu}{2}-1\right)$ is well-defined. Thus,

$$\mathbb{E}X^4 = \frac{\nu^2 B\left(\frac{5}{2},\frac{\nu}{2}-2\right)}{B\left(\frac{1}{2},\frac{\nu}{2}\right)} = \frac{\nu^2\Gamma\left(\frac{5}{2}\right)\Gamma\left(\frac{\nu}{2}-2\right)}{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{\nu}{2}\right)} = \frac{\nu^2\frac{3}{2}\frac{1}{2}}{\left(\frac{\nu}{2}-1\right)\left(\frac{\nu}{2}-2\right)} = \frac{3\nu^2}{(\nu-2)(\nu-4)}. \tag{24.0.19}$$

In this case, by Definition 19.5.6, we have

$$\operatorname{Kurt}(X) = \frac{\frac{3\nu^2}{(\nu-2)(\nu-4)}}{\frac{\nu^2}{(\nu-2)^2}} - 3 = \frac{3(\nu-2)}{(\nu-4)} - 3 = \frac{6}{\nu-4}. \tag{24.0.20}$$

Meanwhile, it is easy to see that if $\nu \leq 4$ the integral is infinity. Thus, we have the required result. □

Proposition 24.0.10. Let $X \sim T(\nu)$. The raw moments of X are

$$\mathbb{E}X^k = \begin{cases} 0 & k \text{ odd}, \quad 0 < k < \nu \\ \frac{1}{\sqrt{\pi}\Gamma\left(\frac{\nu}{2}\right)}\left(\Gamma\left(\frac{k+1}{2}\right)\Gamma\left(\frac{\nu-k}{2}\right)\nu^{\frac{k}{2}}\right) & k \text{ even}, \quad 0 < k < \nu \\ \text{undefined} & k \text{ odd}, \quad 0 < \nu \leq k \\ \infty & k \text{ even}, \quad 0 < \nu \leq k \end{cases} \tag{24.0.21}$$

Proposition 24.0.11. Student's t-distribution with ν degrees of freedom can be defined as the distribution of the random variable X with

$$X = \frac{Z}{\sqrt{V/\nu}} = Z\sqrt{\frac{\nu}{V}}, \tag{24.0.22}$$

where Z is normally distributed with expected value 0 and variance 1, V has a chi-squared distribution with ν degree of

freedom; Z and V are independent.

Proof. For standard normal Z and standard chi-squared distributed V with drgree of freedom ν, we have

$$f_Z(z) = \frac{1}{\sqrt{2\pi}} e^{-z^2/2}, \qquad f_V(u) = \frac{1}{\Gamma(\nu/2)} 2^{-\nu/2} u^{\nu/2-1} e^{-u/2}. \tag{24.0.23}$$

Then

$$\mathbb{P}(X \le x) \;=\; \mathbb{P}\left(Z\sqrt{\frac{\nu}{V}} \le x\right) = \int_0^\infty \int_{-\infty}^{x\sqrt{u}/\sqrt{\nu}} \frac{1}{\sqrt{2\pi}} e^{-z^2/2} \frac{1}{\Gamma(\nu/2)} 2^{-\nu/2} u^{\nu/2-1} e^{-u/2} dz du$$

Taking the differentiation wrt x under the integral sign, we have (by Theorem 15.3.29)

$$\begin{aligned} f_X(x) &= \int_0^\infty \frac{\sqrt{u}}{\sqrt{\nu}} \frac{1}{\sqrt{2\pi}} e^{-\frac{ux^2}{2\nu}} \frac{1}{\Gamma(\nu/2)} 2^{-\nu/2} u^{\nu/2-1} e^{-u/2} du = \frac{1}{\sqrt{2\pi\nu}} \int_0^\infty \frac{1}{\Gamma(\nu/2)} 2^{-\nu/2} u^{\nu/2-1/2} e^{-u\left(1+\frac{x^2}{\nu}\right)/2} du \\ &= \frac{1}{\sqrt{\pi\nu}} \left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} \frac{\Gamma((\nu+1)/2)}{\Gamma(\nu/2)} \int_0^\infty \frac{1}{\Gamma((\nu+1)/2)} 2^{-(\nu+1)/2} x^{(\nu+1)/2-1} e^{-x/2} dx \\ &= \frac{\Gamma((\nu+1)/2)}{\sqrt{\pi\nu}\Gamma(\nu/2)} \left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} \end{aligned}$$

which is the density function of t-distribution. □

24.0.4 Inverse Gaussian random variables

Definition 24.0.4 (inverse Gaussian random variable)**.** A random variable X in $(0,\infty)$ is called inverse Gaussian distributed if, for some $\mu > 0$ and $\lambda > 0$, its density function is

$$f_X(x) = \left(\frac{\lambda}{2\pi x^3}\right)^{1/2} \exp\left(-\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right) \tag{24.0.24}$$

where μ is the mean and λ is the shape parameter. We write $X \sim IG(\mu, \lambda)$.

Remark. As λ tends to infinity, the inverse Gaussian distribution becomes more like a normal (Gaussian) distribution. The inverse Gaussian distribution has several properties analogous to a Gaussian distribution. The name can be misleading: it is an "inverse" only in that, while the Gaussian describes a Brownian Motion's level at a fixed time, the inverse Gaussian describes the distribution of the time a Brownian Motion with positive drift takes to reach a fixed positive level.

Its cumulant generating function (logarithm of the characteristic function) is the inverse of the cumulant generating function of a Gaussian random variable.

First we need to guarantee that the integral of the density function is 1.

Proposition 24.0.12.

$$I = \int_0^\infty \left(\frac{\lambda}{2\pi x^3}\right)^{1/2} \exp\left(-\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right) dx = 1. \tag{24.0.25}$$

Proof. First, we have

$$I = \int_0^\infty \left(\frac{\lambda}{2\pi x^3}\right)^{1/2} \exp\left(-\frac{\lambda\left(\sqrt{\frac{x}{\mu}} - \sqrt{\frac{\mu}{x}}\right)^2}{2\mu}\right) dx = \left(\frac{\lambda}{2\pi\mu}\right)^{1/2} \int_0^\infty x^{-3/2} \exp\left(-\frac{\lambda\left(\sqrt{x} - \frac{1}{\sqrt{x}}\right)^2}{2\mu}\right) dx \tag{24.0.26}$$

Taking the substitution $y = 1/x$, we have that

$$I = \left(\frac{\lambda}{2\pi\mu}\right)^{1/2} \int_\infty^0 y^{3/2} \exp\left(-\frac{\lambda\left(\sqrt{y} - \frac{1}{\sqrt{y}}\right)^2}{2\mu}\right)\left(-\frac{1}{y^2}\right) dy = \left(\frac{\lambda}{2\pi\mu}\right)^{1/2} \int_0^\infty x^{-1/2} \exp\left(-\frac{\lambda\left(\sqrt{x} - \frac{1}{\sqrt{x}}\right)^2}{2\mu}\right) dx. \tag{24.0.27}$$

Therefore,

$$\begin{aligned} I &= \frac{1}{2}\left(\frac{\lambda}{2\pi\mu}\right)^{1/2}\left(\int_0^\infty \left(x^{-3/2}+x^{-1/2}\right)\exp\left(-\frac{\lambda\left(\sqrt{x}-\frac{1}{\sqrt{x}}\right)^2}{2\mu}\right)dx\right) \\ &= \left(\frac{\lambda}{2\pi\mu}\right)^{1/2}\left(\int_0^\infty \exp\left(-\frac{\lambda\left(\sqrt{x}-\frac{1}{\sqrt{x}}\right)^2}{2\mu}\right)d\left(x^{1/2}-x^{-1/2}\right)\right) = \left(\frac{\lambda}{2\pi\mu}\right)^{1/2}\int_{-\infty}^\infty \exp\left(-\frac{\lambda x^2}{2\mu}\right)dx \\ &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty e^{-x^2/2}dx = 1 \end{aligned}$$

by normal distribution. □

Proposition 24.0.13. Suppose $X \sim IG(\mu,\lambda)$. Then for $t \in \mathbb{R}$,

$$M_X(\theta) = \exp\left(\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)\right), \qquad \phi_X(t) = \exp\left(\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2i\mu^2 t}{\lambda}}\right)\right). \tag{24.0.28}$$

Proof.

$$\begin{aligned} M_X(\theta) &= \int_0^\infty \exp(\theta x)\left(\frac{\lambda}{2\pi x^3}\right)^{1/2}\exp\left(-\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right)dx \\ &= \exp\left(\frac{2\lambda\mu}{2\mu^2}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)\right)\int_0^\infty \left(\frac{\lambda}{2\pi x^3}\right)^{1/2}\exp\left(-\frac{\lambda\left(x\sqrt{1-\frac{2\mu^2\theta}{\lambda}}-\mu\right)^2}{2\mu^2 x}\right)dx \\ &= \exp\left(\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)\right). \end{aligned}$$

Similarly for $\phi_X(t)$. □

Proposition 24.0.14. Suppose $X \sim IG(\mu,\lambda)$. Then

$$\text{(i) } \mathbb{E}X = \mu, \quad \text{(ii) } \operatorname{Var} X = \frac{\mu^3}{\lambda}, \quad \text{(iii) } \operatorname{Skew}(X) = 3\left(\frac{\mu}{\lambda}\right)^{1/2}, \quad \text{(iv) } \operatorname{Kurt}(X) = \frac{15\mu}{\lambda}.$$

Proof. With Propositions 24.0.13, 19.5.10,

$$\mathbb{E}X = \left.\frac{dM_X(\theta)}{d\theta}\right|_{\theta=0} = \mu\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-1/2}\exp\left(\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)\right)\Bigg|_{\theta=0} = \mu. \tag{24.0.29}$$

$$\mathbb{E}X^2 = \left.\frac{d^2M_X(\theta)}{d\theta^2}\right|_{\theta=0} = \left(\mu^2\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-1}+\frac{\mu^3}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-3/2}\right)\exp\left(\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)\right)\Bigg|_{\theta=0} = \mu^2+\frac{\mu^3}{\lambda}.$$

Thus, $\operatorname{Var} X = \mathbb{E}X^2 - (\mathbb{E}X)^2 = \mu^2 + \frac{\mu^3}{\lambda} - \mu^2 = \frac{\mu^3}{\lambda}$. Also,

$$\begin{aligned} \mathbb{E}X^3 = \left.\frac{d^3M_X(\theta)}{d\theta^3}\right|_{\theta=0} &= \left(\mu^3\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-3/2}+\frac{\mu^4}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-2}\right)e^{\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)}\Bigg|_{\theta=0} \\ &\quad + \left(\frac{2\mu^4}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-2}+\frac{3\mu^5}{\lambda^2}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-5/2}\right)e^{\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)}\Bigg|_{\theta=0} \\ &= \left(\mu^3\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-3/2}+\frac{3\mu^4}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-2}+\frac{3\mu^5}{\lambda^2}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-5/2}\right)e^{\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)}\Bigg|_{\theta=0} \\ &= \mu^3+\frac{3\mu^4}{\lambda}+\frac{3\mu^5}{\lambda^2}. \end{aligned}$$

Thus,

$$\mathbb{E}\left(X-\mu\right)^3 = \mathbb{E}X^3 - 3\mu\mathbb{E}X^2 + 3\mu^2\mathbb{E}X - \mu^3 = \mu^3 + \frac{3\mu^4}{\lambda} + \frac{3\mu^5}{\lambda^2} - 3\mu\left(\mu^2 + \frac{\mu^3}{\lambda}\right) + 2\mu^3 = \frac{3\mu^5}{\lambda^2}. \tag{24.0.30}$$

By Definition 19.5.5, $\text{Skew}(X) = \frac{3\mu^5/\lambda^2}{\mu^{9/2}/\lambda^{3/2}} = 3\left(\frac{\mu}{\lambda}\right)^{1/2}$. Furthermore,

$$\begin{aligned}
\mathbb{E}X^4 = \left.\frac{d^4 M_X(\theta)}{d\theta^4}\right|_{\theta=0} &= \left.\left(\mu^4\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-2} + \frac{3\mu^5}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-5/2} + \frac{3\mu^6}{\lambda^2}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-3}\right) e^{\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)}\right|_{\theta=0} \\
&\quad + \left.\left(\frac{3\mu^5}{\lambda}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-5/2} + \frac{12\mu^6}{\lambda^2}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-3} + \frac{15\mu^7}{\lambda^3}\left(1-\frac{2\mu^2\theta}{\lambda}\right)^{-7/2}\right) e^{\frac{\lambda}{\mu}\left(1-\sqrt{1-\frac{2\mu^2\theta}{\lambda}}\right)}\right|_{\theta=0} \\
&= \mu^4 + \frac{6\mu^5}{\lambda} + \frac{15\mu^6}{\lambda^2} + \frac{15\mu^7}{\lambda^3}.
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathbb{E}\left(X-\mu\right)^4 &= \mathbb{E}X^4 - 4\mu\mathbb{E}X^3 + 6\mu^2\mathbb{E}X^2 - 4\mu^3\mathbb{E}X + \mu^4 \\
&= \mu^4 + \frac{6\mu^5}{\lambda} + \frac{15\mu^6}{\lambda^2} + \frac{15\mu^7}{\lambda^3} - 4\mu\left(\mu^3 + \frac{3\mu^4}{\lambda} + \frac{3\mu^5}{\lambda^2}\right) + 6\mu^2\left(\mu^2 + \frac{\mu^3}{\lambda}\right) - 3\mu^4 = \frac{3\mu^6}{\lambda^2} + \frac{15\mu^7}{\lambda^3}.
\end{aligned}$$

By Definition 19.5.6, we have

$$\text{Kurt}(X) = \frac{\frac{3\mu^6}{\lambda^2} + \frac{15\mu^7}{\lambda^3}}{\frac{\mu^6}{\lambda^2}} - 3 = \frac{15\mu}{\lambda}. \tag{24.0.31}$$

□

24.0.5 Generalized inverse Gaussian random variables

Definition 24.0.5 (generalized inverse Gaussian random variable)**.** A random variable X in $(0,\infty)$ is called generalized inverse Gaussian distributed if, for some $a>0, b>0, p\in\mathbb{R}$, its density function is

$$f_X(x) = \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} e^{-(ax+b/x)/2} \tag{24.0.32}$$

where $K_\nu(z)$ is a modified Bessel function of the second kind. We write $X \sim GIG(a,b,p)$.

Remark. The inverse Gaussian and gamma distributions are special cases of the generalized inverse Gaussian distribution for $p=-1/2$ and $b=0$, respectively. Specifically, an inverse Gaussian distribution of the form

$$f_X(x) = \left(\frac{\lambda}{2\pi x^3}\right)^{1/2} \exp\left(-\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right) \tag{24.0.33}$$

is a GIG with $a=\lambda/\mu^2$, $b=\lambda$, and $p=-1/2$.

A Gamma distribution of the form

$$f_X(x) = \frac{1}{\Gamma(k)}\lambda^k x^{k-1} e^{-\lambda x} \tag{24.0.34}$$

is a GIG with $a=2\lambda$, $b=0$, and $p=k$.

First we need to guarantee that the integral of the density function is 1.

Proposition 24.0.15.

$$I = \int_0^\infty \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} e^{-(ax+b/x)/2} dx = 1. \tag{24.0.35}$$

Proof. First, we have

$$\begin{aligned} I &= \int_0^\infty \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} e^{-(ax+b/x)/2} dx = \int_0^\infty \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} \exp\left(-\frac{\sqrt{ab}}{2}\left(\sqrt{\frac{a}{b}}x + \sqrt{\frac{b}{a}}\frac{1}{x}\right)\right) dx \\ &= \frac{1}{2K_p(\sqrt{ab})} \int_0^\infty t^{(p-1)} \exp\left(-\frac{\sqrt{ab}}{2}\left(t + \frac{1}{t}\right)\right) dt. \end{aligned}$$

Taking the substitution $t = e^x$, we have that

$$\begin{aligned} I &= \frac{1}{2K_p(\sqrt{ab})} \int_{-\infty}^\infty e^{(p-1)x} \exp\left(-\sqrt{ab}\cosh x\right) de^x = \frac{1}{2K_p(\sqrt{ab})} \int_{-\infty}^\infty e^{px} \exp\left(-\sqrt{ab}\cosh x\right) dx \\ &= \frac{1}{K_p(\sqrt{ab})} \int_0^\infty \cosh(px) \exp\left(-\sqrt{ab}\cosh x\right) dx = \frac{1}{K_p(\sqrt{ab})} K_p(\sqrt{ab}) = 1 \end{aligned}$$

by Proposition 16.2.7. □

Proposition 24.0.16. Suppose $X \sim GIG(a, b, p)$. Then for $t \in \mathbb{R}$,

$$M_X(\theta) = \left(\frac{a}{a-2\theta}\right)^{\frac{p}{2}} \frac{K_p(\sqrt{b(a-2\theta)})}{K_p(\sqrt{ab})}, \qquad \phi_X(t) = \left(\frac{a}{a-2it}\right)^{\frac{p}{2}} \frac{K_p(\sqrt{b(a-2it)})}{K_p(\sqrt{ab})}. \tag{24.0.36}$$

Remark. If we let $a = \lambda/\mu^2$, $b = \lambda$, and $p = -1/2$, then by Proposition 16.2.11,

$$M_X(\theta) = \left(\frac{a}{a-2\theta}\right)^{-1/4} \frac{(b(a-2\theta))^{-1/4} e^{-\sqrt{b(a-2\theta)}}}{(ab)^{-1/4} e^{-\sqrt{ab}}} = e^{\sqrt{ab}\left(1-\sqrt{1-\frac{2\theta}{a}}\right)} = \exp\left(\frac{\lambda}{\mu}\left(1 - \sqrt{1 - \frac{2\mu^2\theta}{\lambda}}\right)\right) \tag{24.0.37}$$

which is pdf of inverse gaussian distribution.

If we let $a = 2\lambda$, $b = 0$, and $p = k$, then by Proposition 16.2.5, $z \to 0$, $K_\nu(z) \sim \frac{1}{2}\Gamma(\nu)\left(\frac{1}{2}z\right)^{-\nu}$

$$M_X(\theta) = \left(\frac{a}{a-2\theta}\right)^{k/2} \frac{\frac{1}{2}\Gamma(k)\left(\frac{1}{2}\sqrt{b(a-2\theta)}\right)^{-k}}{\frac{1}{2}\Gamma(k)\left(\frac{1}{2}\sqrt{ba}\right)^{-k}} = \left(\frac{a}{a-2\theta}\right)^{k} = \left(\frac{\lambda}{\lambda-\theta}\right)^{k} \tag{24.0.38}$$

which is pdf of Gamma distribution.

Proof. For moment generating function,

$$\begin{aligned} M_X(\theta) &= \int_0^\infty e^{\theta x} \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{p-1} e^{-(ax+b/x)/2} dx \\ &= \int_0^\infty \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} \exp\left(-\frac{\sqrt{(a-2\theta)b}}{2}\left(\sqrt{\frac{a-2\theta}{b}}x + \sqrt{\frac{b}{a-2\theta}}\frac{1}{x}\right)\right) dx \\ &= \frac{1}{2K_p(\sqrt{ab})} \left(\frac{a}{a-2\theta}\right)^{p/2} \int_0^\infty t^{(p-1)} \exp\left(-\frac{\sqrt{(a-2\theta)b}}{2}\left(t + \frac{1}{t}\right)\right) dt. \end{aligned}$$

Taking the substitution $t = e^x$, we have that

$$\begin{aligned} M_X(\theta) &= \frac{1}{2K_p(\sqrt{ab})} \left(\frac{a}{a-2\theta}\right)^{p/2} \int_{-\infty}^\infty e^{(p-1)x} \exp\left(-\sqrt{(a-2\theta)b}\cosh x\right) dx \\ &= \frac{1}{K_p(\sqrt{ab})} \left(\frac{a}{a-2\theta}\right)^{p/2} \int_0^\infty \cosh(px) \exp\left(-\sqrt{(a-2\theta)b}\cosh x\right) dx = \left(\frac{a}{a-2\theta}\right)^{\frac{p}{2}} \frac{K_p(\sqrt{b(a-2\theta)})}{K_p(\sqrt{ab})} \end{aligned}$$

by Proposition 16.2.7. Similarly for $\phi_X(t)$. □

Proposition 24.0.17. Suppose $X \sim GIG(a,b,p)$. Then

$$\text{(i) } \mathbb{E}X = \frac{\sqrt{b}\ K_{p+1}(\sqrt{ab})}{\sqrt{a}\ K_p(\sqrt{ab})}, \qquad \text{(ii) } \operatorname{Var} X = \left(\frac{b}{a}\right)\left(\frac{K_{p+2}(\sqrt{ab})}{K_p(\sqrt{ab})} - \left(\frac{K_{p+1}(\sqrt{ab})}{K_p(\sqrt{ab})}\right)^2\right), \qquad \text{(iii) } \mathbb{E}X^n = \left(\frac{b}{a}\right)^{n/2} \frac{K_{p+n}(\sqrt{ab})}{K_p(\sqrt{ab})}.$$

Proof. With Propositions 24.0.16, 19.5.10,

$$\mathbb{E}X^n = \int_0^\infty \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{p+n-1} e^{-(ax+b/x)/2} dx = \left(\frac{b}{a}\right)^{n/2} \int_0^\infty \frac{(a/b)^{p+n/2}}{2K_p(\sqrt{ab})} x^{p+n-1} e^{-(ax+b/x)/2} dx = \left(\frac{b}{a}\right)^{n/2} \frac{K_{p+n}(\sqrt{ab})}{K_p(\sqrt{ab})}.$$

Therefore,

$$\mathbb{E}X = \frac{\sqrt{b}\ K_{p+1}(\sqrt{ab})}{\sqrt{a}\ K_p(\sqrt{ab})}, \qquad \operatorname{Var} X = \left(\frac{b}{a}\right)\left(\frac{K_{p+2}(\sqrt{ab})}{K_p(\sqrt{ab})} - \left(\frac{K_{p+1}(\sqrt{ab})}{K_p(\sqrt{ab})}\right)^2\right). \tag{24.0.39}$$

□

24.0.6 Weibull random variables

24.0.7 Hyperbolic random variables

Definition 24.0.6 (hyperbolic random variable)**.** A random variable X in $(-\infty,\infty)$ is called hyperbolic distributed if, for some $\mu,\alpha,\beta,\delta \in \mathbb{R}$ and $\gamma = \sqrt{\alpha^2-\beta^2}$ its density function is

$$f_X(x) = \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2} + \beta(x-\mu)\right) \tag{24.0.40}$$

where $K_\nu(z)$ is a modified Bessel function of the second kind. μ is location parameter, β asymmetry parameter and δ is scale parameter. We write $X \sim H(\mu,\alpha,\beta,\delta)$.

Proposition 24.0.18.

$$\frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2} + \beta(x-\mu)\right) dx = 1. \tag{24.0.41}$$

Proof. Taking the substitutions, we have (by Proposition 4.3.1)

$$\begin{aligned} I &= \int_{-\infty}^{\infty} \exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2} + \beta(x-\mu)\right) dx = \int_{-\infty}^{\infty} \exp\left(-\alpha\sqrt{\delta^2+x^2} + \beta x\right) dx \\ &= \delta\int_{-\infty}^{\infty} \exp\left(-\alpha\delta\cosh t + \beta\delta\sinh t\right) d\sinh t = \delta\int_{-\infty}^{\infty} \exp\left(-\gamma\delta\cosh(t-a)\right)\cosh t dt \\ &= \delta\int_{-\infty}^{\infty} \exp\left(-\gamma\delta\cosh t\right)\cosh(t+a) dt = 2\cosh a\delta\int_0^{\infty} \exp\left(-\gamma\delta\cosh t\right)\cosh t dt \end{aligned}$$

where $\cosh a = \frac{\alpha}{\gamma}$ and $\sinh a = \frac{\beta}{\gamma}$. Thus,

$$I = 2\delta\frac{\alpha}{\gamma}\int_0^{\infty} \exp\left(-\gamma\delta\cosh t\right)\cosh t dt = 2\delta\frac{\alpha}{\gamma}K_1\left(\gamma\delta\right) \tag{24.0.42}$$

by Proposition 16.2.7. Thus, we have the required result. □

Proposition 24.0.19. Suppose $X \sim H(\mu,\alpha,\beta,\delta)$. Then for $\theta,t \in \mathbb{R}$,

$$M_X(\theta) = \frac{e^{\mu\theta}\gamma K_1\left(\delta\sqrt{\alpha^2-(\beta+\theta)^2}\right)}{\sqrt{\alpha^2-(\beta+\theta)^2}K_1(\delta\gamma)}, \qquad \phi_X(t) = \frac{e^{i\mu t}\gamma K_1\left(\delta\sqrt{\alpha^2-(\beta+it)^2}\right)}{\sqrt{\alpha^2-(\beta+it)^2}K_1(\delta\gamma)}. \tag{24.0.43}$$

where $K_\nu(z)$ is modified Bessel function of the second kind.

Proof. We have

$$\begin{aligned} M_X(\theta) &= \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(\theta x) \exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2}+\beta(x-\mu)\right) dx \\ &= \frac{e^{\mu\theta}\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2}+(\beta+\theta)(x-\mu)\right) dx \\ &= \frac{e^{\mu\theta}\gamma}{2\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(-\alpha\delta\cosh t+(\beta+\theta)\delta\sinh t)\cosh t dt = \frac{e^{\mu\theta}\gamma}{2\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(-\delta\gamma'\cosh(t-b))\cosh t dt \\ &= \frac{e^{\mu\theta}\gamma}{2\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(-\delta\gamma'\cosh t)\cosh(t+b) dt = \frac{e^{\mu\theta}\gamma}{\alpha K_1(\delta\gamma)} \int_{0}^{\infty} \exp(-\delta\gamma'\cosh t)\cosh t dt \end{aligned}$$

where $\gamma' = \sqrt{\alpha^2-(\beta+\theta)^2}$, $\cosh b = \frac{\alpha}{\gamma'}$ and $\sinh b = \frac{\beta+\theta}{\gamma'}$.

Thus, by Proposition 16.2.7, we have

$$M_X(\theta) = \frac{e^{\mu\theta}\gamma K_1\left(\delta\sqrt{\alpha^2-(\beta+\theta)^2}\right)}{\sqrt{\alpha^2-(\beta+\theta)^2}K_1(\delta\gamma)}. \tag{24.0.44}$$

□

Proposition 24.0.20. Suppose $X \sim H(\mu,\alpha,\beta,\delta)$. Then

$$\text{(i) } \mathbb{E}X = \mu + \frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}, \qquad \text{(ii) } \operatorname{Var} X = \frac{\delta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)} + \frac{\beta^2\delta^2}{\gamma^2}\left(\frac{K_3(\delta\gamma)}{K_1(\delta\gamma)} - \frac{K_2^2(\delta\gamma)}{K_1^2(\delta\gamma)}\right).$$

Proof. With Propositions 24.0.16, 19.5.10,

$$\begin{aligned} \mathbb{E}X &= \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} x\exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2}+\beta(x-\mu)\right) dx = \mu + \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} x\exp\left(-\alpha\sqrt{\delta^2+x^2}+\beta x\right) dx \\ &= \mu + \frac{\gamma\delta}{2\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \sinh t\exp(-\delta\gamma\cosh(t-a))\cosh t dt = \mu + \frac{\gamma\delta}{4\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(-\delta\gamma\cosh(t-a))\sinh 2t dt \\ &= \mu + \frac{\gamma\delta}{4\alpha K_1(\delta\gamma)} \int_{-\infty}^{\infty} \exp(-\delta\gamma\cosh t)\sinh 2(t+a) dt = \mu + \frac{\gamma\delta\sinh(2a)}{2\alpha K_1(\delta\gamma)} \int_{0}^{\infty} \exp(-\delta\gamma\cosh t)\cosh 2t dt. \end{aligned}$$

Therefore,

$$\mathbb{E}X = \mu + \frac{\gamma\delta\sinh(2a)}{2\alpha K_1(\delta\gamma)}K_2(\delta\gamma) = \mu + \frac{\gamma\delta\sinh a\cosh a}{\alpha K_1(\delta\gamma)}K_2(\delta\gamma) = \mu + \frac{\gamma\delta\frac{\beta}{\gamma}\frac{\alpha}{\gamma}K_2(\delta\gamma)}{\alpha K_1(\delta\gamma)} = \mu + \frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}. \tag{24.0.45}$$

$$\begin{aligned} \mathbb{E}X^2 &= \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} x^2\exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2}+\beta(x-\mu)\right) dx \\ &= \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} (x-\mu)^2\exp\left(-\alpha\sqrt{\delta^2+(x-\mu)^2}+\beta(x-\mu)\right) dx + 2\mu\left(\mu + \frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right) - \mu^2 \\ &= \frac{\gamma}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} x^2\exp\left(-\alpha\sqrt{\delta^2+x^2}+\beta x\right) dx + \mu\left(\mu + 2\frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right). \end{aligned}$$

Then make the substitution, (also $4\cosh^3 t = \cosh(3t) + 3\cosh t$)

$$\begin{aligned}
& \frac{\gamma\delta^3}{2\alpha\delta K_1(\delta\gamma)} \int_{-\infty}^{\infty} \left(\cosh^3(t+a) - \cosh(t+a)\right) \exp\left(-\gamma\delta\cosh t\right) dt \\
= & \frac{\gamma\delta^2}{4\alpha K_1(\gamma)} \int_0^{\infty} \left(\cosh 3(t+a) - \cosh(t+a)\right) \exp\left(-\gamma\delta\cosh t\right) dt \\
= & \frac{\gamma\delta^2}{4\alpha K_1(\gamma)} \int_0^{\infty} \left(\cosh(3t)\cosh(3a) - \cosh t\cosh a\right) \exp\left(-\gamma\delta\cosh t\right) dt \\
= & \frac{\gamma\delta^2}{4\alpha K_1(\gamma)} \left(K_3(\delta\gamma)\cosh(3a) - K_1(\delta\gamma)\cosh a\right) = \frac{\gamma\delta^2}{4\alpha K_1(\gamma)} \left(K_3(\delta\gamma)\left(4\cosh^3 a - 3\cosh a\right) - K_1(\delta\gamma)\cosh a\right) \\
= & \frac{\delta^2\beta^2 K_3(\delta\gamma)}{\gamma^2 K_1(\delta\gamma)} + \frac{\delta^2}{4K_1(\delta\gamma)} \left(K_3(\delta\gamma) - K_1(\delta\gamma)\right)
\end{aligned}$$

By Proposition 16.2.9, $K_3(z) - K_1(z) = \frac{4}{z} K_2(z)$ ($e^{(\nu-1)\pi i} K_{\nu-1}(z) - e^{(\nu+1)\pi i} K_{\nu+1}(z) = \frac{2\nu}{z} e^{\nu\pi i} K_\nu(z)$). Thus,

$$\begin{aligned}
\mathbb{E}X^2 &= \frac{\delta^2\beta^2 K_3(\delta\gamma)}{\gamma^2 K_1(\delta\gamma)} + \frac{\delta^2}{4K_1(\delta\gamma)} \left(K_3(\delta\gamma) - K_1(\delta\gamma)\right) + \mu\left(\mu + 2\frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right) \\
&= \frac{\delta^2\beta^2 K_3(\delta\gamma)}{\gamma^2 K_1(\delta\gamma)} + \frac{\delta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)} + \mu\left(\mu + 2\frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
\operatorname{Var} X &= \frac{\delta^2\beta^2 K_3(\delta\gamma)}{\gamma^2 K_1(\delta\gamma)} + \frac{\delta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)} + \mu\left(\mu + 2\frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right) - \left(\mu + \frac{\delta\beta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)}\right)^2 \\
&= \frac{\delta K_2(\delta\gamma)}{\gamma K_1(\delta\gamma)} + \frac{\beta^2\delta^2}{\gamma^2}\left(\frac{K_3(\delta\gamma)}{K_1(\delta\gamma)} - \frac{K_2^2(\delta\gamma)}{K_1^2(\delta\gamma)}\right).
\end{aligned}$$

□

24.0.8 Generalized hyperbolic random variables

Chapter 25

Statistics

25.0.9 Linear model

Part VIII

Optimization

Chapter 26

Optimization

26.1 Problems

Problem 26.1.1 (the locker puzzle [7])**.** Suppose there are $2n$ person indexed from 1 to $2n$. Also, there is a room having $2n$ doors in order and behind each of the doors there is a corresponding number to each person with random distribution without repeat. Now $2n$ person are allowed to get into the room one by one, open at most n doors and leave without communication with other person. If one of the doors the person checked has his corresponding number, we say that this person is successful.

All the person could have a chat to make a particular stategy to open the doors. What's the optimal strategy to maximize the probability that all the persons are successful?

Solution. We can have the following strategy. The ith person checks the ith door. If the number behind the door is i then the person stops and leaves the room. If the number is $j \neq i$, then the person checks the jth door.

Note that any permutation of a finite set can be written as a product of disjoint cycles (Theorem 6.1.18). Thus, this strategy will let the persons forming cycles (by the numbers behind the doors) follow the overlapping paths. Thus, it will be different from the strategy that pick the doors independent for each person (which gives the probability 2^{-2n}). Thus, we need to count the number of situations in which n-cycle is the biggest one. Or we can count the number of situations that the size of maximal cycle is equal to or more than $n+1$. If the maximal cycle is k-cycle for $2n \geq k \geq n+1$, we have

$$C_{2n}^{k}(k-1)!(2n-k)! = \frac{(2n)!}{(2n-k)!k!}(k-1)!(2n-k)! = \frac{(2n)!}{k} \text{ possible ways.} \tag{26.1.1}$$

Here we have $(k-1)!$ for all the possible ways of k-cycle. Thus, the totally unsuccessful probability is

$$\frac{1}{(2n)!}\sum_{k=n+1}^{2n}\frac{(2n)!}{k} = \sum_{k=n+1}^{2n}\frac{1}{k}. \tag{26.1.2}$$

Then successful probability is

$$1-\sum_{k=n+1}^{2n}\frac{1}{k}, \qquad \text{e.g., for } n=2, \text{ it is } 1-\frac{1}{3}-\frac{1}{4}=\frac{5}{12}. \tag{26.1.3}$$

If $n \to \infty$, we can have that (by Corollary[1])

$$1-\sum_{k=n+1}^{2n}\frac{1}{k} \to 1-\ln 2 = 0.306853. \tag{26.1.4}$$

However, we still need to show that this strategy is optimal[2].

[1] need corollary
[2] need details

Bibliography

[1]

[2] Milton Abramowitz and Irene A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1972.

[3] Alan F. Beardon. *Algebra and Geometry*. Cambridge University Press, 2005.

[4] Patrick Billingsley. *Probability and Measure, 3rd Edition*. Wiley-Blackwell, 1995.

[5] Kai Lai Chung. *A Course in Probability Theory, 3rd Edition*. Academic Press, 2000.

[6] Z. Ciesielski. Hölder conditions for realizations of gaussian processes. *Transactions of the American Mathematical Society*, 99:403–413, 1961.

[7] Eugene Curtin and Max Warshauer. The locker puzzle. *The Mathematical Intelligencer*, 28(1):28–31, 2006.

[8] Richard Durrett. *Probability: Theory and Examples, 3rd*. Brooks/Cole, 2004.

[9] Charles M. Grinstead and J. Laurie Snell. *Introduction to Probability*. American Mathematical Society, 1997.

[10] Achim Klenke. *Probability Theory: A Comprehensive Course, 1st Edition*. Springer, 2008.

[11] L.C.G.Rogers and David Williams. *Diffusions, Markov Processes, and Martingales, 2nd Edition*. Cambridge University Press, 1994.

[12] Paul-André Meyer. *Martingales and Stochastic Integrals I, Lecture Notes in Mathematics*. Springer-Verlag, 1972.

[13] S. Rolewicz. *Functional Analysis and Control Theory: Linear Systems*. Springer, 1987.

[14] J.Michael Steele. *Stochastic Calculus and Financial Applications*. Springer, 2001.

[15] Terence Tao. *Analysis I*. Hindustan Book Agency, 2006.

[16] David Williams. *Probability with Martingales*. Cambridge University Press, 1991.

[17] Kosaku Yoshida. *Functional Analysis*. Springer-Verlag, 1980.

[18] Xinfeng Zhou. *A Practical Guide To Quantitative Finance Interviews, 1 Edition*. Lulu.com, 2008.

Index

abelian, 29
absolute value
    rational numbers, 14
absolutely continuous
    measure, 392
ACC
    ring, 87
adapted process, 375
    continuous, 394
addition
    natural number, 9
additive, 200
adjoint matrix, 127
adjugate matrix, 134
algebra, 110, 197
algebraic integer, 96
almost everywhere
    set, 215
almost surely
    set, 274
alternating group, 36
alternating series test, 148
anti-symmetric
    matrix, 127
arithmetic-geometric mean inequality, 195
Ascending chain condition
    ring, 87
associates
    element of ring, 81
associativity
    Groups, 29
atom
    distribution function, 281
automorphism
    groups, 34
    vector space, 114
automorphism group, 34
Axiom of Archimedes, 145

backward martingale
    discrete, 389
backwards martingale convergence theorem
    discrete, 389
Bakers' map, 258
Banach space, 195
basis
    vector space, 111
Bayes' Theorem, 302
Bernoulli, 284
Bernoulli random variable
    $\mathbb{R}$, 330
beta function, 22
beta-distributed random variable, 352
bijective, 20
Binomial random variable
    $\mathbb{R}$, 331
binomial series, 22
Birkhoff's almost everywhere ergodic theorem, 256
block diagonal matrix, 132
Blumenthal's 0-1 law, 446
Bolzano-Weierstrass theorem, 151
Bonferroni's inequalities, 275
Borel σ-algebra, 199
Borel function, 211
Borel measurable space, 199
Borel measure, 208
Borel's Normal Number Theorem, 17
Borel-Cantelli Lemma
    measure, 204
    probability, 280
bounded convergence theorem
    $\mathcal{L}^p$ finite measure, 246
    finite measure, 225
    measurable function, 225
    probability, 290
bounded in $\mathcal{L}^p$
    measurable function, 244
    random variable family, 294
Brownian bridge, 459
Brownian motion, 440
    standard, 440

càdlàg function, 156
càdlàg process, 399
cancellation law
    addition of natural number, 10
    integers, 12
    multiplication of natural number, 11
canonical probability space
    random variable sequence, 355

canonical process, 404
Carathéodory's Extension Theorem, 205
Cauchy random variable
  standard, 350
Cauchy sequence
  real numbers, 152
Cauchy's condensation test, 148
Cauchy's mean value theorem, 164
Cauchy's residue theorem, 187
Cauchy-Schwarz inequality
  measure, 240
  probability, 294
Cayley Theorem, 54
central limit theorem, 358
centraliser, 50
centre
  group, 51
chain rule
  càdlàg adapted finite variation process with integrands bounded on compact time intervals, 410
  càdlàg adapted finite variation process with locally bounded integrands, 412
  differentiable real functions, 161
  matrix, 117
  stochastic integrals, 482
characteristic
  ring, 79
characteristic function, 314
Chebyshev's inequality, 293
chi squared-distributed random variable, 501
closed
  $\mathcal{L}^2(E, \mathcal{E}, \mu)$ space, 243
  $\mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P})$ space, 294
closed in $\mathcal{L}^p$, 385
closure
  Groups, 29
cofactor matrix, 134
column space
  matrix, 124
commutative
  ring, 73
commute
  matrices, 128
compact support, 8
comparison test, 146
complement, 274
complete, 243
  measure space, 202
Completeness of $\mathcal{L}^p$, 241
completion, 202
composition
  function, 19
composition factor, 47
concatenation operation, 449
conditional expectation
  elementary for σ-algebra, 303
  elementary for set, 303
conditional probability, 299
conjugacy class
  group, 50
conjugate indices, 239
conjugation action, 50
constant polynomial, 74
content
  polynomial, 90
continuous
  topological space, 193
convergence
  almost everywhere, 215
  almost surely, 287
  as distribution function, 321
  in $\mathbb{R}$, 143
  in $\mathcal{L}^p(\Omega, \mathcal{F}, \mathbb{P})$, 296
  in $\mathcal{L}^p(E, \mathcal{E}, \mu)$, 246
  in distribution, 322
  in measure, 215
  in probability
    metric space, 287
    real space, 287
  sum, 145
  vaguely, 251
  weakly
    finite measure, 251
    probability measure, 323
convergence on compact, 193
convex, 238
coordinate mapping, 404
coprime
  elements of ring, 90
correlation, 299
countable additivity, 200
countably generated
  σ-algebra, 197
countably subadditive, 200
covariance, 298
covariation
  stochastic processes, 483
cycle, 33
cycle type, 52
cyclic group, 31

d-system, 197
De Morgan laws, 7
decreasing
  real function, 156

sequence, 16
set function, 200
degree
polynomial, 74
density function
conditional, 313
conditional probability, 313
measure, 227
probability, 291
Radon-Nikodym derivative, 392
determinant
linear endomorphism, 118
matrix, 128
determinant function, 128
diagonal matrix, 131
positive, non-negative, 131
differentiable
real function, 159
differentiation under integral sign, 231
dihedral group, 33
dimension
vector space, 111
direct product
group, 40
direct sum
matrices, 132
vector space, 113
disjoint, 200
cycle, 33
distance
rational number, 14
distribution, 280
Cauchy, 350
distribution function, 281
distribution function of random variable, 280
distributive law
natural number, 11
divergence
sum, 145
division
rational numbers, 14
domain, 19
dominated convergence theorem
conditional expectation, 309
measure, 223
probability, 290
Doob's $\mathcal{L}^p$-inequality
continous, 420
discrete, 384
Doob's maximal inequality
continuous-time, 420
discrete, 383
Dynkin's Lemma, 198

ED
Euclidean domain, 84
Eisenstein's criterion, 94
element
set, 5
elementary matrix, 125
empty set, 5
endomorphism
groups, 34
vector space, 114
equality
functions, 19
ordered pair, 7
sets, 5
equivalence relation
Groups, 38
equivalent
matrix, 123
ergodic
measure preserving transformation, 254
essential supremum, 237
stochastic process, 466
Euclidean algorithm
natural numbers, 11
polynomials, 77
Euclidean domain, 84
Euclidean function, 84
Eula's constant, 181
Euler's formula, 301
Euler's totient function, 39
event, 273
eventually, 203
expectation, 287
exponent
group, 38
exponential random variable
$\mathbb{R}$, 343
exponentiation
natural number, 15
negative integer, 15

faithful
group action, 49
Fatou's Lemma
conditional expectation, 308
function, 222
set, 204
Fatou's lemma
probability, 290
field, 73
field of fractions, 81

filtered probability space
continuous, 394
discrete, 375
filtration
continuous, 394
discrete, 375
finite dimensional distributions
stochastic process, 401
finite measure, 201
finite variation, 157
finite variation process, 400
Fubini's Theorem, 233
function, 19
function space
with time index, 404
Fundamental Axiom of Analysis, 143
fundamental property of measure, 203
fundamental theorem of calculus
measure theory, 229

gamma function, 22
Gamma-distributed random variable, 351
Gauss' lemma
polynomial, 91
Gaussian integer, 94
Gaussian random variable
$\mathbb{R}$, 345
standard, 314
Gaussian random variables
bivariate, 348
multivariate, 348
general principle of convergence, 152
generalized inverse Gaussian distributed random variable, 510
generated σ-algebra, 198
generator
Groups, 31
geometric random variable
$\mathbb{R}$, 332
group, 29
group action, 48

Hölder's inequality
expectation, 294
measure, 239
heat kernal, 315
Hermitian matrix, 127
highest common factor
rings, 89
Hilbert space, 243
Hilbert's basis theorem, 87
homomorphism
groups, 34
linear map, 114
rings, 74
hyperbolic distributed random variable, 512

i.i.d.
random variables, 358
ideal, 75
left ideal, 75
right ideal, 75
identity element, 29
identity matrix, 122
image
homomorphism, 35
set, 7
image measure, 214
inclusion, 274
inclusion-exclusion formula
measure theory, 202
probability, 274
increasing
real function, 156
sequence, 16
set function, 200
set sequence, 197
independent
σ-algebra, 279
set, 278
independent and stationary increments, 394
index
Groups, 38
indicator function, 212
indicator random variable, 280
indistinguishable version
stochastic process, 402
infimum, 8
infinitely often, 203
injective, 19
inner product, 184
inner regular measure, 208
integer, 11
integer part
rational number, 16
integrable
Lebesgue, 221
Riemann, 173, 228
stochastic process, 375, 393
integral
measurable function, 219
non-negative measurable function, 219
integral domain, 80
integration by parts
stochastic calculus, 491
intermediate value theorem, 154
intersection, 274

pairwise, 6
intrinsic metric, 189
invariant
measurable function, 253
set, 253
inverse
Groups, 29
matrix, 123
inverse Gaussian distributed random variable, 508
inverse image
measure, 211
set, 7
inverse theorem
real function, 164
invertible
function, 20
matrix, 123
irreducible
element of ring, 81
isomorphism
groups, 34
rings, 75
vector space, 114
Isomorphism Theorem
Group, 46
isomorphism theorem
group, 44, 45
ring, 78, 79
Itô's formula, 491
Itô's stochastic integral, 478

Jensen's Inequality
conditional expectation, 309
Jensen's inequality
expectation, 293
measure, 238
joint density function
probability, 292
joint distribution function, 292

Kakutani's product martingale theorem, 391
kernel
group action, 49
group homomorphism, 35
ring homomorphism, 75
Kolmogorov's 0-1 law, 285
Kolmogorov's continuity criterion, 402
Kolmogorov's inequality
continuous-time martingale, 421
discrete time martingale, 384
Kronecker delta, 20
Kunita Watanabe identity
semimartingale, 489
Kunita-Watanabe identity, 485
kurtosis, 321

Laurent polynomials, 74
Laurent series, 74
law, 280
process, 401
law of total probability, 301
Lebesgue measure, 208
Lebesgue-Stieltjes measure, 214
left coset, 37
left inverse
matrix, 123
left regular action, 54
limit
real number, 143
linear map
vector space, 114
linearly dependent
vectors, 111
linearly independent
subvector space, 111
vectors, 111
Lipschitz constant, 191
Lipschitz continuous, 191
Lipschitz equivalent metrics, 190
locally bounded
stochastic process, 407
locally finite
measure, 208
locally uniform convergence
real-valued function, 184
$\mathcal{L}^p$-norm, 237

marginal density function
probability, 292
Markov's inequality, 293
martingale
continuous, 415
discrete, 377
martingale convergence theorem
continuous, 422
martingale transform, 378
mass function, 204
matrix, 121
maximal ergodic lemma, 255
maximal ideal, 83
mean value theorem, 162
measurable function, 211
measurable set, 197
measurable space, 197
measure, 201
measure space, 201

measure-preserving transformation, 253
median
    random variable, 337
memoryless property
    exponential distribution, 344
metric, 189
metric space, 189
minimal polynomial, 83
minimal polynomial of algebraic integer, 96
Minkowski's inequality
    expectation, 294
    measure, 240
minor
    matrix, 133
mode
    random variable, 337
modification
    stochastic process, 402
moment generating function, 320
monic
    polynomial, 74
monotone class Theorem, 213
monotone convergence theorem
    almost everywhere, 221
    conditional expectation, 308
    pointwise, 219
    probability, 290
monotonic
    sequence, 16
multiplication
    natural number, 11
mutually exclusive, 274

natural filtration
    continuous, 394
    discrete, 375
natural numbers, 9
negative
    rational numbers, 14
negative binomial random variable
    $\mathbb{R}$, 333
Noetherian
    ring, 87
non-singular
    matrix, 123
norm, 184
    element of ring, 81
normal
    subgroup, 43
normal representation, 217
normaliser
    group action, 58
null set
    measure, 202
nullity, 115
nullspace, 115

observation, 273
occur, 273
Odd Order Theorem, 59
one-to-one, 19
onto, 20
open set
    topological space, 193
optional stopping theoerem
    bounded stopping time, continuous, 423
    UI martingale, continuous, 424
    UI martingale, discrete, 388
optional stopping theorem
    discrete, bounded, 379
orbit
    group action, 48
order
    group, 30
    group element, 38
ordered pair, 7
orthogonal
    general inner product space, 243
orthogonal matrix, 127
orthogonal projection
    measure, 243
    probability, 294
Orthogonal Projection Theorem
    measure, 243
    probability, 294
outer measure, 205
outer regular measure, 208

p-group, 54
pair set, 5
pairwise independent, 278
parallelogram law, 243
partition, 301
Peano axioms, 9
permutation, 31
permutation group, 32
permutation representation, 48
π-system, 197
PID
    principal ideal domain, 82
Poisson random variable
    $\mathbb{R}$, 335
polynomial, 74
polynomial functions, 74
polynomial ring, 74
Portemanteau Theorem, 251

positive
natural number, 10
rational numbers, 14
previsible sigma-algebra, 404
previsible process
continuous-time, 404
discrete-time, 378
prime
element of ring, 81
prime ideal, 83
prime subring, 79
primitive
polynomial, 90
principal ideal, 76
principal ideal domain, 82
probability distribution
discrete, 328
probability generating function, 328
probability mass function, 328
probability space, 273
process, 284
product σ-algebra, 232
product martingale
discrete, 391
product measure, 233
proper ideal, 83
pseudometric, 189
Pythagoras' rule, 243

quadratic variation process, 471
quasimetric, 189
quotient
rational numbers, 14
quotient group, 44
quotient ring, 76

Rademacher functions, 284
Radon measure, 208
Radon-Nikodym derivative, 392
Radon-Nikodym theorem
discrete, 392
random process
continuous, 393
discrete, 375
random variable, 280
discrete, 328
random walk
symmetric, 380
range, 19
rank
column, matrix, 124
linear map, 115
row, matrix, 124
ratio test, 147
rational numbers, 13
reciprocal
rational numbers, 13
record
probability, 284
reflection principle, 449
regular measure, 208
Riemann-Lebesgue lemma, 250
right coset, 37
right inverse
matrix, 123
right-continuous
filtration, 394
ring
group, 73
set, 199
ring of formal power series, 74
Rolle's Theorem, 162
root test, 147
row space
matrix, 124

sample space, 273
sampling
probability, 275
scalar matrix, 131
Scheffé's Lemma
measure, 225
probability, 290
second-countable space, 193
semidirect product
groups, 68
semigroup, 29
semimartingale, 431
continuous, 487
semimetric, 190
separable
σ-algebra, 197
set, 5
set function, 200
shift map, 356
σ-algebra, 197
σ-algebra of measurable events before stopping time
continuous, 394
discrete, 376
σ-finite measure, 202
sign
permutation, 36
similar
matrix, 139
simple
group, 46

simple function, 216
simple process, 465
simple symmetric random walk, 380
singleton set, 5
skew-Hermitian matrix, 127
skewness, 321
Skorokhod representation theorem, 322
soluble
    group, 47
spaces of measures, 208
sporadic group, 47
stabiliser
    group action, 48
stationary
    sequence of random variables, 356
stepfunction, 249
Stirling's formula, 183
stochastic integral
    discrete, 378
stochastic process
    continuous, 393
    discrete, 375
Stone-Weierstrass theorem, 195
stopped martingale theorem
    discrete, 379
stopped process
    continuous, 396
    discrete, 376
stopping time
    continuous, 394
    discrete, 375
strictly decreasing
    real function, 156
    sequence, 16
strictly increasing
    real function, 156
    sequence, 16
strong closure property
    ring, 75
strong law of large numbers
    4th moment, 354
    ergodic theorem approach, 358
    martingale approach, 390
structure theorem for finite abelian groups, 56
Student-t distributed random variable, 505
subalgebra, 110
subgroup, 30
submartingale
    continuous, 415
    discrete, 377
subring
    group, 73
subsapce
    continuous real functions, 110
    differential real functions, 110
    polynimial real functions, 110
subset, 5
subspace
    vector space, 110
supermartingale
    continuous, 415
    discrete, 377
support, 8
surjective, 20
Sylow p-subgroup, 56
Sylow's theorem, 56
symmetric
    matrix, 126
symmetric difference, 7
symmetric group, 32

tail σ-algebra, 285
tight
    measure family, 253
topological space, 193
topology, 193
total variation, 157
total variation process, 400
tower property, 310
trace
    linear endomorphism, 119
    matrix, 127
transition density
    Brownian motion, 439
transitive
    group action, 48
translation invariant
    metric, 189
transpose
    matrix, 122
transposition
    groups, 34
triangular matrix, 132

UFD
    Unique factorisation domain, 88
UI (uniformly integrable)
    measurable function family, 245
    random variable family, 295
UI martingale, 387
UI martingale convergence theorem
    continuous, 423
    discrete, 387
ultrametric, 189
uniform convergence

real-valued function, 184
uniform convergence on compacts, 194
stochastic process, almost surely, 413
stochastic process, in probability, 413
uniform random variable
$\mathbb{R}$, 337
uniformly integrable
measurable function family, 245
random variable family, 295
union, 274
pairwise, 6
Unique factorisation domain, 88
uniqueness of extension
measure, 207
unit
element of ring, 73, 81
unitary matrix, 127
up-crossing inequality, 382
usual conditions
filtered probability space, 395

variance, 297
vector space, 109
version
stochastic process, 402
Vitali Convergence Theorem, 247
volume form, 128
von Neumann's $\mathcal{L}^p$ ergodic theorem, 259

weak law of large numbers
finite absolute moment, 354
finite variance, 353
Weierstrass' approximation theorem, 195
Wiener's measure, 443

zero divisor, 79