# Introduction to Number Theory

Zexiang Chen

January 12, 2015

## PREFACE

This is a collection of topics in Number Theory and some of the materials were lectured in Cambridge in PartII Number Theory, PartII Number Field, PartIII Algebraic Number Theory, PartIII Local Fields and PartIII Elliptic Curves. Exercises (together with solutions) are given at the end of each chapter. This is intended to be a supplementary material for students to have better general understanding in Number Theory. I will keep updating exercises and course notes if there are anything new. All comments and corrections are welcome zc231@cam.ac.uk

### Notation

We will introduce and use the following notations throughout the book:

$$f(x) \sim g(x) \text{ if } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

$$f(x) = O(g(x)) \text{ if } \lim_{x\to\infty} \frac{|f(x)|}{g(x)} \text{ is bounded.}$$

$$f(x) = o(g(x)) \text{ if } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Sometimes we write *card* of a set to mean the cardinality (or size) of a set.

**Prerequisites** Basic knowledge of group theory and Linear Algebra is needed. We provide some basic revision of PartIB Groups, Rings and Modules. Some calculus and real analysis is assumed, and very basic complex analysis is used. I do intend to cover some basic materials in Galois theory which will be needed for some of the topics.
We shall use the following facts:

(i) The Vandermonde determinant. If $x_1, \ldots, x_n$ are complex numbers then

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \ldots & \ldots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{1\le i<j\le n} (x_j - x_i)$$

(ii) Euler's integral theorem with the Euler constant $\gamma$ such that if $x \ge 1$

$$\sum_{n=1}^{x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

(iii) The series

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

This will be proved in chapter 6

**Acknowledgement**

I want to thank many of my undergraduate supervisors who give me advises to some of the exercises.

**To Readers**

If you are interested in contributing to this handbook or if you have any better idea for collections of topics in Number Theory, please contact me.

# Contents


**1 Introduction and divisibility** **8**
- 1.1 Introduction and examples . . . 8
- 1.2 Divisibility . . . 8
- 1.3 Fundamental theorem . . . 9
- 1.4 Exercises . . . 9
- 1.5 Hint and Solutions . . . 10

**2 Arithmetical functions** **12**
- 2.1 Multiplicative functions . . . 12
- 2.2 Perfect number . . . 13
- 2.3 Inverse formula . . . 13
- 2.4 Euler's totient function $\phi$(n) . . . 15
- 2.5 Liouville function $\lambda$ . . . 15
- 2.6 Average order . . . 16
- 2.7 Exercises . . . 17
- 2.8 Hints and Solutions . . . 18

**3 Prime numbers and congruence** **21**
- 3.1 Prime numbers . . . 21
- 3.2 Congruence . . . 21
- 3.3 Fermat's little theorem and Euler's theorem . . . 22
- 3.4 Wilson's theorem . . . 23
- 3.5 Chinese remainder theorem . . . 23
- 3.6 Polynomial and polynomial congruence . . . 24
- 3.7 Chevalley's theorem . . . 25
- 3.8 Primitive root and non-linear congruence . . . 26
- 3.9 Exercises . . . 29
- 3.10 Hint and Solutions . . . 30

**4 Quadratic residue** **35**
- 4.1 Legendre symbol . . . 35
- 4.2 Euler's criterion . . . 35
- 4.3 Gauss's lemma . . . 36
- 4.4 Law of quadratic reciprocity . . . 36
- 4.5 Jacobi symbol . . . 38
- 4.6 Kronecker symbol . . . 39
- 4.7 Pseudo prime . . . 41
- 4.8 Exercises . . . 44
- 4.9 Hint and Solutions . . . 46

**5 Continued fraction** **52**
- 5.1 Basic properties . . . 52
- 5.2 Pell's equation . . . 58
- 5.3 A set of real numbers modulo 1 . . . 62
- 5.4 Exercises . . . 64
- 5.5 Hint and Solutions . . . 66

**6 Distribution of prime numbers and Riemannn zeta function** **73**
6.1 Basic properties . . . 73
6.2 Legendre formulae . . . 74
6.3 The result of Chebyshev . . . 76
6.4 Bertrand's postulate and some other results . . . 79
6.5 Riemann zeta function . . . 82
6.6 Bernoulli numbers . . . 87
6.7 Exercises . . . 89
6.8 Hint and Solutions . . . 92

**7 Algebraic background-Integral domain** **99**
7.1 Basic properties . . . 99
7.2 Irreducible and Primes . . . 101
7.3 Ideals . . . 102
7.4 Principal Ideal Domains . . . 103
7.5 Maximal ideals and prime ideals . . . 104
7.6 Sum and products of ideals . . . 105
7.7 Exercises . . . 106
7.8 Hint and Solutions . . . 107

**8 Algebraic background-Euclidean domain** **110**
8.1 Euclidean Domains . . . 110
8.2 Almost Euclidean domains . . . 111
8.3 Exercises . . . 112
8.4 Hint and Solutions . . . 113

**9 Algebraic background-Noetherian domain** **115**
9.1 Noetherian domains . . . 115
9.2 Factorisation domain and unique factorisation domains . . . 116

**10 Algebraic background-Modules** **120**
10.1 Modules . . . 120
10.2 Direct Sum, Free Modules . . . 122
10.3 Matrices Over Euclidean Domain, Smith Normal Form . . . 123

**11 Field extension** **126**
11.1 Basic properties . . . 126
11.2 K-Homomorphism . . . 127
11.3 Algebraic extension . . . 127
11.4 Automorphism group . . . 129
11.5 Splitting field and separability . . . 130
11.6 Exercises . . . 132
11.7 Hint and Solutions . . . 133

**12 Algebraic Number field** **137**
12.1 Basic concepts . . . 137
12.2 Cayley-Hamilton Theorem . . . 137
12.3 Ring of integers . . . 138
12.4 Integral elements and integral closure . . . 139
12.5 Trace and norm . . . 141
12.6 Conjugates . . . 143
12.7 Complex embeddings . . . 144

12.8 $\mathcal{O}_K$ as finitely generated $\mathbb{Z}$-module . . . 145
12.9 Exercises . . . 146
12.10Hint and Solutions . . . 147

**13 Dedekind Domain** **150**
13.1 Dedekind domains . . . 150
13.2 Ideals in a Dedekind domain . . . 151
13.3 Factorisation into prime ideals . . . 153
13.4 Order of an ideal . . . 156
13.5 Chinese Remainder Theorem . . . 159
13.6 Exercises . . . 160
13.7 Hint and Solutions . . . 161

**14 Discriminant and norm** **165**
14.1 Discriminant . . . 165
14.2 Discriminant of a polynomial . . . 167
14.3 Norm of an ideal . . . 169
14.4 Norm of a product of ideals . . . 170
14.5 Norm of an element . . . 173
14.6 Norm of fractional ideal . . . 174
14.7 Exercises . . . 175
14.8 Hint and Solutions . . . 178

**15 Factorisation of prime numbers** **188**
15.1 Basic property . . . 188
15.2 Ramification . . . 190
15.3 Application in a quadratic field . . . 191
15.4 Kummer-Dedekind theorem . . . 195
15.5 Generalisation of Kummer-Dedekind theorem . . . 197
15.6 Exercise . . . 198
15.7 Hint and Solutions . . . 200

**16 The ideal class group** **206**
16.1 Basic concept . . . 206
16.2 Minkowski's convex body theorem . . . 206
16.3 Finiteness of the ideal class group . . . 210
16.4 Further properties . . . 213
16.5 Algorithm to determine the ideal class group . . . 214
16.6 Exercises . . . 217
16.7 Hint and Solutions . . . 219

**17 Units in the ring of integers** **233**
17.1 Units in a quadratic field . . . 233
17.2 Dirichlet's unit theorem . . . 237
17.3 Independent units . . . 240
17.4 The Diophantine equation: $x(x+1)(x+2) = y(y+1)$ . . . 243
17.5 Exercise . . . 247
17.6 Hint and Solutions . . . 250

**18 Gauss and Jacobi sums** **262**
18.1 Representation and character . . . 262
18.2 Sum of squares . . . 268
18.3 Gauss and Jacobi sums . . . 273
18.4 Number of solutions to $x^n + y^n \equiv 1 \pmod{p}$ . . . 279
18.5 The sign of quadratic Gauss sum . . . 281
18.6 Exercise . . . 283
18.7 Hint and Solutions . . . 287

**19 Algebraic Number Theory** **294**
19.1 Summary of Results of General Number Field Extensions . . . 294
19.2 Decomposition of Primes . . . 298
19.3 Counting Primes . . . 301
19.4 Representations . . . 304
19.5 Exercises . . . 307
19.6 Hint and Solutions . . . 309

**20 $L$-series** **317**
20.1 Dirichlet's Theorem of Primes in Arithmetic Progression . . . 317
20.2 Artin $L$-function . . . 323
20.3 Applications . . . 328
20.4 Induction Theorems . . . 329
20.5 Chebotarev's Density Theorem . . . 331
20.6 Exercises . . . 333
20.7 Hint and Solutions . . . 334

**21 p-adic number** **338**
21.1 Absolute value . . . 338
21.2 Valuation . . . 346
21.3 The Techmüller map . . . 351
21.4 Exercises . . . 352
21.5 Hint and Solutions . . . 353

**22 Dedekind Domain** **360**
22.1 Exercises . . . 365
22.2 Hint and Solutions . . . 366

**23 Extension of Complete Fields** **368**
23.1 Unique Extension . . . 368
23.2 Extension of Number Fields . . . 369
23.3 Application of Techmuller Map . . . 373
23.4 Exercises . . . 376
23.5 Hint and Solutions . . . 377

**24 Inverse Limit And Local Fields** **382**
24.1 Inverse Limit . . . 382
24.2 Local Fields . . . 383
24.3 Exercises . . . 385
24.4 Hint and Solutions . . . 385

**25 Ramification Theory** **387**
25.1 Unramified Extensions . . . 387
25.2 Totally Ramified Extension And Eisenstein Polynomial . . . 388
25.3 The Norm Map . . . 389
25.4 Different And Inverse Different . . . 390
25.5 Krasner's Lemma And Application . . . 395
25.6 Ramification Group . . . 397
25.7 Exercises . . . 398
25.8 Hint and Solutions . . . 400

**26 Introduction to Elliptic Curves** **405**
26.1 Basic Properties . . . 405
26.2 Elliptic Curves over $\mathbb{C}$ . . . 406
26.3 Height . . . 411
26.4 Exercises . . . 418
26.5 Hint and Solutions . . . 419

**27 Modell-Weil Theorem and Rank of Elliptic Curves** **422**
27.1 Rank of Elliptic Curves . . . 422
27.2 Modell-Weil Theorem . . . 424
27.3 Elliptic Curve Over $p$-adic field . . . 428
27.4 Decent . . . 435
27.5 Exercises . . . 442
27.6 Hint and Solutions . . . 444

**28 Introduction To Class Field Theory** **450**
28.1 Cyclotomic Extensions . . . 450
28.2 Class Field . . . 455
28.3 Main Theorem of Class Field Theory . . . 457
28.4 Ray Class Field . . . 458
28.5 Principal Ideal Theorem . . . 460
28.6 Exercises . . . 462
28.7 Hint and Solutions . . . 463

**29 Isogeny and The Weil Pairing** **468**
29.1 Isogeny . . . 468
29.2 Invariant Differential . . . 472
29.3 The Dual Isogeny . . . 474
29.4 The Tate Module . . . 477
29.5 The Weil Pairing . . . 480
29.6 Exercises . . . 485
29.7 Hint and Solutions . . . 487

**30 Computation of Mordell-Weil Group** **493**
30.1 Cohomology Group . . . 493
30.2 Revisit of Two Descent . . . 496
30.3 Twisting . . . 500

# 1 Introduction and divisibility

## 1.1 Introduction and examples

We first look at some examples of conjectures:

1. Let $N$ be any integer $\geq 1$ of the form $8n+5, 8n+6, 8n+7$. Then there always exists a right angle triangle of area $N$, all of whose size has rational length.

2. If $x$ is a rational number, $x \geq 2$, write $\pi(x)$ = number of primes $\leq x, li(x) = \int_2^x \frac{dt}{\log t}$. Then $\forall x \geq 3, |\pi(x) - li(x)| \leq \sqrt{(x)} \log x$.

3. There are infinitely many primes $p$ such that $p+2$ is also a prime.

A famous example which has only been solved in the last twenty years is Fermat's Last theorem, by Andrew Wiles, which says that $\forall n \geq 3, x^n + y^n = z^n$ has no non-obvious integer solutions. i.e. one of $x, y, z$ must be 0.

These are all examples of number theory which may or may not require a large amount of knowledge from other area of mathematics, e.g. Elliptic Curve, Modular Form, etc.

Now for the first few Chapters, we will concentrate more on analytic number theory and basic background of group theory is needed. Details will be explained later.

## 1.2 Divisibility

**Theorem 1.1.** *Let $a, b \in \mathbb{Z}, a > 0$, then $\exists q, r \in \mathbb{Z}$ such that $b = aq + r$, where $0 \leq r < a$.*

*Proof.* Let $S = \{b - na : n \in \mathbb{Z}\}$. S contains a least non-zero integer, say $r$, and let $r = b - qa$. Then $r < a$ because if $r \geq a$ then $r - a = b - (q+1)a \in S$, which contradicts $r$ being least in $S$. This is a special case of Euclidean algorithm in group theory, which we will discuss later. □

**Corollary 1.2.** *Given integers $a_1, a_2 \dots a_n$, not all 0. Let $I = \{a_1x_1 + \dots + a_nx_n : x_i \in \mathbb{Z}\}$. Then there exists $d > 0$, such that $I = d\mathbb{Z}$.*

*Proof.* It is easy to see that $I$ is an ideal. $I$ contains integer $> 0$. Let $d$ be the least integer $> 0$ in $I$, and claim that $I = d\mathbb{Z}$. Take any $c$ in $I$, we have $c = qd + r, 0 \leq r < d$ by Euclidean algorithm. Then $r = c - qd \in I$, and hence $r = 0$ by definition of $d$. Hence $I = d\mathbb{Z}$. □

**Definition 1.3.** *We call such $d$ above the greatest common divisor of $a_1, a_2 \dots a_n$, and write $d = (a_1, \dots a_n)$.*

The efficient way of calculating $d = (a, b), b > a > 0$ is as follows:
$b = aq_1 + r_1, 0 \leq r_1 < a$.
$a = r_1q_2 + r_2, 0 \leq r_2 < r_1$.
$\vdots$
Until $\exists n$, $r_{n-1} = r_nq_{n+1}$.
Then it is easy to check that $r_n = (a, b) = d$. Such algorithm is called **Euclidean algorithm**.

**Example 1.4.** *Find the greatest common divisor of 45 and 36. we have $45 = 36 + 9$, $36 = 9 \cdot 4$. And hence the greatest common divisor is 9.*

Hence we may use Euclidean algorithm to find solutions of equations of the form:
$a \cdot x + b \cdot y = c$.
In the example above, $a = 45, b = 36$. Let $c = 9$ then we have $x = 1, y = -1$. In fact:

**Theorem 1.5.** *Suppose $n \neq 0$, then the equation $ax + by = n$ is soluble if and only if $(a, b)|n$. Moreover, if $(a, b)|n$. The general solution of the equation $ax + by = n$ has the form $\{x_0 + \frac{tb}{(a,b)}, y_0 - \frac{ta}{(a,b)}\}$, where $t \in \mathbb{Z}$ and $\{x_0, y_0\}$ is one solution of the equation above.*

*Proof.* Suppose $(a, b) \nmid n$, then we have no solutions. Suppose now $(a, b)|n$, as by Euclid's algorithm we can find integers $x, y$ such that $ax_1 + by_1 = (a, b)$. Then let $x = x_1\frac{n}{(a,b)}, y = y_1\frac{n}{(a,b)}$, and so we have a solution.

Now it is clear that integers in the above set are indeed solutions of the equation. Now suppose $\{x_1, y_1\}, \{x_1 + u, y_1 - v\}$ are both solutions of the equations. Then $au = bv$, and so $\frac{a}{(a,b)}u = \frac{b}{(a,b)}v$. Hence $\frac{b}{(a,b)}|u$. Thus $u \geq \frac{b}{(a,b)}$. And hence the result. □

**Lemma 1.6.** *Let $p$ be a prime. If $p|ab$, then $p|a$ or $p|b$.*

*Proof.* Suppose $p \nmid a$. Then $(a, p) = 1$, and so $\exists x, y$ such that $ax + py = 1$. Then $abx + pby = b$. And so as $p|ab$ and $p|aby$. Therefore, $p$ divides RHS i.e. $p|b$. □

## 1.3 Fundamental theorem

**Theorem 1.7.** [**Fundamental Theorem**] *Every integer $N > 1$ can be written as a product of primes, and this computation is unique up to reordering.*

For example, we have $24 = 2 \cdot 2 \cdot 2 \cdot 3, 34 = 2 \cdot 17$.

*Proof.* We need to prove both existence and uniqueness of the theorem.

1. Existence: Let $p_1 \dots p_k$ be the list of primes less than or equal to $\sqrt{N}$. $p_i < p_{i+1}$. To find a factorisation, start with $p_1$ and for each $p_i$, if $p_i$ divides $N$, then it is a factor of $N$ and then consider the new $N$ to be $\frac{N}{p_i}$, and continue again from $p_i$. If $p_i$ does not divide $N$, then move on to $p_{i+1}$. Continue this until we have run though every $p_i$.

2. Uniqueness: Suppose $N = p_1p_2 \dots p_r = q_1q_2 \dots q_s$, where $p_i, q_j$ are primes. Now use the lemma above, start from $p_1$, as $p_1|q_1(q_2 \cdots q_s)$, so $p_1|q_1$ or $p_1|q_2 \cdots q_s$.
   Continue this and so we have $p_1|q_j$ for some $j$. WLOG, we reorder so that $p_1|q_1$. But $q_1$ is prime, and so we must have $p_1 = q_1$. Now remove $p_1, q_1$ in the above equation and continue this. Hence we conclude that $r = s$ and $p_i = q_i$ after suitable reordering.

□

The fundamental theorem gives a trivial way of finding the factorisation of $N$, but it is not efficient. **Elementary Operation** is add or multiply any two elements of the set $\{0, 1 \dots 9\}$, carrying a remainder if necessary. For example, for any integer $M$ of $m$ digits, $R$ of $r$ digits, the multiplication $MR$ requires $2mr$ elementary operations. The algorithm is polynomial if the number of operations required is at most $a(\log N)^b, a, b > 0$. And it is still unknown whether there is algorithm which factorsises $N$ in polynomial time.

## 1.4 Exercises

1. Find integers $x, y$ such that $25x + 42y = 1$.

2. Find integers $x, y, z$ such that $6x + 10y + 15z = 1$.

3. Let $n > 1$ and $S_n = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, show that $S_n$ cannot be an integer.

4. Let $n$ be a positive integer, prove that $n$ can be written as a sum of (at least two) consecutive positive integers if and only if $n \neq 2^k$ for some $k$.

5. Let $a, b$ be positive integer such that $(a, b) = 1$. Then show that $ax + by = n$ is soluble in non-negative integer $x$ and $y$ whenever $n \geq (a-1)(b-1)$.

6. Show that if $m > n$, then $2^{2^n} + 1$ divides $2^{2^m} - 1$ and so $(2^{2^m} + 1, 2^{2^n} + 1) = 1$.

7. Given $a \geq b \geq 1$, let $\lambda(a, b)$ be the number of steps of finding $(a, b)$ by Eulcidean algorithm (excluding the last step where the remainder is 0). Show that

$$\lambda(a, b) \leq 2 \left\lfloor \frac{\log b}{\log 2} \right\rfloor.$$

8. Improve the result of the previous question by showing that the least number $b$ for which $\lambda(a, b) = n$ is $F_{n+1}$ where $F_n$ is the $n^{\text{th}}$ Fibonacci number.

## 1.5 Hint and Solutions

1. $x = -5, y = 3$.

2. To find the greatest common divisor of three integers say $(a, b, c)$, we can find the greatest common divisor of two of them, say $d = (a, b)$ and then find $(c, d)$. So we have $15 - 6 \cdot 2 = 3$ and then we have $10 - 3 \cdot 3 = 1$. Hence we conclude $10 - (15 - 6 \cdot 2) \cdot 3 = 1$, and so $x = 6, y = 1, z = -3$.

3. Let $2^k \leq n < 2^{k+1}$ for some $k$, and consider $S = S_n \cdot 2^{k-1} \cdot 3 \cdot 5 \ldots$ (we multiply every odd number less than or equal to $n$). Then suppose $S_n$ is an integer, then $S$ is also an integer. But consider each term of $S$, all of them are integers except a $\frac{1}{2}$ from $2^{k-1} \cdot \frac{1}{2^k}$, and so $S$ is not an integer, which is a contradiction.

4. Let $n = 2^k$ for some $k$ and suppose we have $a, a+1 \ldots a+l, l \geq 1$ such that the sum of these integers equals $n$. Then we have $\frac{(2a+l)(l+1)}{2} = 2^k$, i.e. $(2a + l)(l + 1)$ is a power of 2. Then as $l \neq 0$, and we must have $l$ is $2^t - 1$ for some $t$ but then $2a+l$ cannot be a power of 2. Conversely, if $n$ is not a power of 2, then let $n = 2^k t$ where $t$ is odd. Then if we want $\frac{(2a+l)(l+1)}{2} = n$, i.e. $(2a + l)(l + 1) = 2n = 2^{k+1}t$. Then we simply let $l = 2^{k+1} - 1$ and $2a + l = t$. This is always possible as $t$ is odd and in particular, $t \geq 3$.

5. Use Theorem 1.5 for the general solution so we can write $(x, y) = (x_0 + tb, y_0 - ta)$ and so WLOG, we let $(x, y)$ be the solution such that $0 \leq y < a$. So $y \leq a-1$ and so $ax+by = n \leq ax+b(a-1)$. Now $n \geq (a-1)(b-1)$, so we have $(a-1)(b-1) \leq ax+b(a-1)$ and hence we rearrange the inequality, we get $1 \leq a(x+1)$. Therefore, we must have $x \geq 0$ and so both $x, y$ are non-negative.

6. When $m > n$, $2^{2^m} = (((2^{2^n})^2)^2)^{\cdots}$ and so clearly $2^{2^n}$ divides $2^{2^m}$. The later follows from an obvious fact that any two consecutive odd number is coprime, and use $2^{2^n}$ divides $2^{2^m}$.

7. Let $\lambda(a,b) = n$. Observe that $\lambda(ac,bc) = \lambda(a,b)$ for any $c \geq 1$. To see this, simply multiply $c$ in each step of finding $(a,b)$ and hence it gives an algorithm of finding $(ac,bc)$. Therefore, we may assume $(a,b) = 1$.

   At any stage $t$, say $r_{t-2} = q_t r_{t-1} + r_t$, observe that $q_t \geq 1$ and $r_{t-1} \geq r_t$. Hence

   $$r_{t-2} \geq 2r_t.$$

   This shows that $r_{n-2} \geq 2$ (as we assume that $r_n = (a,b) = 1$) and $r_{n-4} \geq 4$ etc. Therefore, $b \geq 2^{\frac{n}{2}}$ and so the result follows by taking logarithm.

8. Observe further that the number of steps of finding $(a,b)$ is the same as finding $(b + r_1, b)$. In other words, we can replace $q_1$ by 1. For the same reason, we can replace $q_i$ by 1 for each $i$. This gives the Fibonacci number (with the assumption $(a,b) = 1 = r_n$, $r_{n-1} \geq 2 = F_2$) and so $b \geq F_{n+1}$. It is easy to check that $F_{n+1} \geq \phi^{n-1}$ where $\phi = \frac{\sqrt{5}+1}{2}$. Therefore,

   $$b \geq \phi^{n-1} \Rightarrow n \geq 1 + \log_\phi b.$$

# 2 Arithmetical functions

## 2.1 Multiplicative functions

We begin the section with some basic definitions

**Definition 2.1.** *A function that maps the positive integers into an integral domain or field is called a* **number theoretic** *function.*

**Definition 2.2.** *A number theoretic function $f$ is said to be* **multiplicative** *if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.*

**Definition 2.3.** *A number theoretic function $g$ is said to be* **completely multiplicative** *if $g(mn) = g(m)g(n)$ without restriction.*

We will see several examples of multiplicative functions later.

**Theorem 2.4.** *If $f$ is a multiplicative function and*

$$g(n) = \sum_{d|n} f(d)$$

*,then $g$ is also multiplicative.*

*Proof.* Let $(m, n) = 1$. A divisor of $mn$ can be uniquely written as $d = d_1 d_2$, where $d_1|m, d_2|n$ and also $(d_1, d_2) = 1$ as $(m, n) = 1$. Then we have:

$$\begin{aligned} g(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= g(m)g(n) \end{aligned}$$

□

**Definition 2.5.** *The function $\tau$ and $\sigma$ are given by:*

$$\tau(n) = \text{the number of positive divisors of } n.$$
$$\sigma(n) = \text{the sum of the positive divisors of } n.$$

**Lemma 2.6.** *$\tau$ and $\sigma$ are both multiplicative.*

*Proof.* Consider that

$$\tau(n) = \sum_{d|n} 1$$

and as the constant function 1 is multiplicative, and hence by Theorem 1.1 we have $\tau$ multiplicative. Similarly, as the identity function is multiplicative, and

$$\sigma(n) = \sum_{d|n} d$$

so $\sigma$ is also multiplicative. □

One of the advantages of multiplicative functions is that we can use the property of it to give a general formula for the function itself. For example, let $p$ be a prime, and let $\alpha \geq 0$, we have:

$$\tau(p^\alpha) = 1 + \alpha \text{ and } \sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$$

Hence for any $n$, we have $n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, and use the lemma above, we have:

$$\tau(n) = \prod_{i=1}^{k}(1 + \alpha_i) \text{ and } \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

**Example 2.7.** *As an example, we calculate $\tau(30)$ and $\sigma(30)$.*
*Apply the formula above, we have $30 = 2 \cdot 3 \cdot 5$. Hence $\tau(30) = 2 \cdot 2 \cdot 2 = 8$, and $\sigma(30) = 3 \cdot 4 \cdot 6 = 72$.*

## 2.2 Perfect number

**Definition 2.8.** *A natural number $n$ is said to be a perfect number if $\sigma(n) = 2n$*

Let's list the first several perfect numbers: 6, 28, 496, 8128. We will see the result below which characterises the even prefect numbers, yet it is still unknown whether there are infinitely many perfect numbers or if any odd perfect numbers exists.

**Lemma 2.9.** *Let $n$ be an even integer. Then $n$ is a perfect number if and only if $2^{p-1}(2^p - 1)$ where both $p$ and $2^p - 1$ are prime.*

*Proof.* If $n = 2^{p-1}(2^p - 1)$ such that both $p$ and $2^p - 1$ are primes, then we have $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = n$. So $n$ is a perfect number.

Conversely, suppose $n$ is even and is a perfect number, WLOG, let $n = 2^{k-1}m$, where $m$ is odd and $k \geq 2$. Now

$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1})\sigma(m) \\ &= (2^k - 1)\sigma(m) \end{aligned}$$

But by definition,

$$\begin{aligned} \sigma(n) &= 2n \\ &= 2^k m \end{aligned}$$

So we have $(2^k - 1)\sigma(m) = 2^k m$ and so as $2^k - 1$ is odd, we have $2^k - 1$ divides $m$. Write $m = (2^k - 1)t$ and so we have $\sigma(m) = 2^k t$. But as $m = (2^k - 1)t$, if $t \neq 1$, we have $\sigma(m) \geq 1 + t + 2^k - 1 + m > 2^k t$, which is a contradiction. Hence we have $t = 1$ and so $m = 2^k - 1$ and $\sigma(m) = 2^k t$. So $m$ must be a prime. And $m = 2^k - 1$ prime implies that $k$ must be a prime. □

## 2.3 Inverse formula

**Definition 2.10.** *The Möbius function $\mu$ is the number theoretic function given by:*

$\mu(1) = 1$
$\mu(n) = 0$ *if $n$ has a squared factor*
$\mu(p_1 p_2 \dots p_n) = (-1)^k$, *where $p_1 \cdots p_k$ are distinct primes.*

**Lemma 2.11.** *$\mu$ is multiplicative and moreover:*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

*Proof.* $\mu$ is clearly multiplicative by considering $m, n$ as a product of primes and consider them separately. Now let

$$s(n) = \sum_{d|n} \mu(n)$$

And if consider $s(p^\alpha)$. If $\alpha = 0$, then $s(1) = 1$. If $\alpha > 0$, then $s(p^\alpha) = 1 - 1 + 0 + 0 \cdots = 0$. Now we know by previous theorem that $s$ is multiplicative, as $\mu$ is, and so the result follows. □

The function $\mu$ is extremely useful when we prove the inverse formula below:

**Theorem 2.12. The Inversion Formula** *If $f$ is a number theoretic function and $g$ is defined by*

$$g(n) = \sum_{d|n} f(d)$$

*Then*

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$$

*Proof.* Consider:

$$\begin{aligned} \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) &= \sum_{d_1 d_2 = n} g(d_1)\mu(d_2) \\ &= \sum_{d_1 d_2 = n} [\mu(d_2) \sum_{d|d_1} f(d)] \\ &= \sum_{d_1 d|n} \mu(d_2) f(d) \\ &= \sum_{d|n} f(d) \sum_{d_2|\frac{n}{d}} \mu(d_2) \\ &= f(n) \end{aligned}$$

Using that

$$\sum_{d_2|\frac{n}{d}} \mu(d_1) \text{ is only non-zero when } n = d \text{ by previous Lemma}$$

Thus we have

$$f(n) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$$

And the second equality is obvious, as summing over $d|n$ is the same as over $\frac{n}{d}|n$ □

**Theorem 2.13.** *If $g$ is a multiplicative function and it satisfies*

$$g(n) = \sum_{d|n} f(d)$$

*for some number theoretic function $f$, then $f$ is also multiplicative.*

*Proof.* We use the above theorem, and so

$$f(mn) = \sum_{d_1|m, d_2|n} g(mn)\mu\left(\frac{mn}{d_1 d_2}\right)$$

Now use $g$ is multiplicative and $\mu$ is multiplicative and so we have the result. □

## 2.4 Euler's totient function $\phi$(n)

**Definition 2.14.** *The Euler's totient function $\phi(n)$ is the number of integers less than or equal to $n$ which are coprime to $n$.*

For example $\phi(1) = \phi(2) = 1, \phi(10) = 4$. In particular, $\phi(p) = p - 1$ whenever $p$ is a prime.

**Lemma 2.15.**

$$\sum_{d|n} \phi(d) = n$$

*Proof.* For each divisor $d$ of $n$, let $X_d = \{m : m \leq d, (m, d) = 1\}$, and so $|X_d| = \phi(d)$. Let $Y_d = \{\frac{nm}{d} : m \leq d, (m, d) = 1\}$. Clearly, $|Y_d| = |X_d| = \phi(d)$. Now we claim that each $Y_d$ are disjoint and the union of them is $\{1, 2, \ldots, n\}$. Let $d_1, d_2|n$, and suppose $\frac{nm_1}{d_1} = \frac{nm_2}{d_2}$, where $m_1 \leq d_1, (m_1, d_1) = 1$ and $m_2 \leq d_2, (m_2, d_2) = 1$. Then we have $d_1 m_2 = d_2 m_1$. But $(d_1, m_1) = 1$ so $d_1|d_2$ and $(d_2, m_2) = 1$ so $d_2|d_1$. Therefore, $d_1 = d_2$, and so if $d_1 \neq d_2$ then $Y_{d_1}$ is disjoint from $Y_{d_2}$. Now for any $k \in \{1, 2, \ldots n\}$. Let $t = (k, n)$, and so $(\frac{k}{t}, \frac{n}{t}) = 1$. As $\frac{n}{t}$ is a divisor of $n$, so we have $k = \frac{n}{\frac{n}{t}} \cdot \frac{k}{t}$, where $\frac{k}{t} \leq \frac{n}{t}$ and they are coprime. Therefore, we have that the union of $Y_d$'s is $\{1, 2, \ldots n\}$ and hence the result. □

**Theorem 2.16.** *The function $\phi$ is multiplicative, and moreover, if $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, then*

$$\phi(n) = \prod_{p_i|n} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = n \prod_{p_i|n} (1 - \frac{1}{p_i})$$

*Proof.* Use Theorem 2.13 and Lemma 2.15 and the fact that identity function is multiplicative. Then observe that, if $p$ is a prime, then for $\alpha \geq 1$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Then use that $\phi$ is multiplicative □

**Lemma 2.17.**

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

*Proof.* Apply inverse formula □

## 2.5 Liouville function $\lambda$

**Definition 2.18.** *Let $\nu$ denote the number of (not necessarily distinct) prime factors of $n$.*

For example, $\nu(10) = 2, \nu(24) = 4$.

**Definition 2.19.** *The number theoretic function $\lambda$ is defined to be $\lambda(n) = (-1)^{\nu(n)}$.*

Note that $\nu(mn) = \nu(m) + \nu(n)$, for every $m, n > 0$. And hence that the function $\lambda$ is *completely* multiplicative.

**Lemma 2.20.**

$$\sum_{d|n} \lambda = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$$

*Proof.* Let $s(n) = \sum_{d|n} \lambda(d)$, and so by earlier result, $s(n)$ is multiplicative. Now let $p$ be a prime, and $\alpha \geq 0$, then

$$s(p^\alpha) = 1 - 1 + 1 - 1 \cdots = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases}$$

Then use the fact that $s$ is multiplicative. □

## 2.6 Average order

We begin with the definition of Riemann Zeta function.

**Definition 2.21.** *The Riemann Zeta function $\zeta(s)$ is defined to be:*

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s}$$

Deed discussion of the function will be in later chapters.

It is often in interest to determine the magnitude on average of arithmetic functions $f$, that is, to find estimates for sums of the form $\sum f(n)$ with $n \leq x$, where $x$ is a largest real number. Firstly, we consider the function $\tau$.

$$\sum_{n\leq x} \tau(n) = \sum_{n\leq x} \sum_{d|n} 1 = \sum_{d\leq x} \sum_{m\leq \frac{x}{d}} 1 = \sum_{d\leq x} \left(\frac{x}{d}\right)$$

We shall use the fact that

$$\sum_{d\leq x} \frac{1}{d} = \log x + O(1)$$

and hence we have

$$\sum_{n\leq x} \tau(n) = x \log x + O(x)$$

and so we see that asymptotically

$$\frac{1}{x} \sum_{n\leq x} \tau(n) \sim \log x \text{ as } x \to \infty$$

Now, for $\sigma(n)$, we have:

$$\sum_{n\leq x} \sigma(n) = \sum_{n\leq x} \sum_{d|n} \left(\frac{n}{d}\right) = \sum_{d\leq x} \sum_{m\leq \frac{x}{d}} m$$

which gives

$$\frac{1}{2} \left[\frac{x}{d}\right] \left(\left[\frac{x}{d}\right] + 1\right) = \frac{1}{2} \left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)$$

Now we shall use the fact that

$$\sum_{d\leq x} \frac{1}{d^2} = \sum_{d=1}^{\infty} \frac{1}{d^2} + O\left(\frac{1}{x}\right) \text{ and } \sum_{d=1}^{\infty} \frac{1}{d^2} = \frac{\pi^2}{6}$$

Thus we conclude that

$$\sum_{n\leq x} \sigma(n) = \frac{1}{12}\pi^2 x^2 + O\left(x \log x\right)$$

Finally, we shall consider the estimate for $\phi$. We have

$$\sum_{n\leq x} \phi(n) = \sum_{n\leq x} \sum_{d|n} \mu(d) \left(\frac{n}{d}\right) = \sum_{d\leq x} \mu(d) \sum_{m\leq \frac{x}{d}} m$$

Now consider that, as

$$\sum_{m\leq \frac{x}{d}} m = \frac{1}{2} \left(\frac{x}{d}\right) + O\left(\frac{x}{d}\right)$$

we have,

$$\sum_{d\leq x} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(\frac{1}{x}\right)$$

and then we require the following lemma:

**Lemma 2.22.**

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$$

*Proof.* We use the fact that $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, and so we will check that $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$, whenever $s > 1$.
We shall assume for now (which will be explained in later chapters) that the series converges absolutely when $s > 1$, and so we have:

$$\sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{d=1}^{\infty} \left( \frac{1}{d^s} \sum_{k|d} \mu(k) \right) = 1$$

using Lemma 2.11 □

Hence we conclude that:

$$\sum_{n \leq x} \phi(n) = \left( \frac{3}{\pi^2} \right) x^2 + O(x \log x)$$

To finish the chapter, we have the following surprising result:

**Corollary 2.23.** *The probability that any two positive integers are coprime is* $\frac{6}{\pi^2}$.

*Proof.* Consider that the number of pairs $\{r, s\}$ satisfying $1 \leq r \leq s \leq n$ is $\frac{n(n+1)}{2}$, and $\sum_{d \leq n} \phi(d)$ counts the number of such pairs which are also coprime. Therefore, let $n$ runs through every natural number, and so the probability of any two positive integers being coprime is:

$$\lim_{n \to \infty} \frac{\sum_{d \leq n} \phi(d)}{\frac{n(n+1)}{2}} = \frac{6}{\pi^2}$$

by previous result. □

## 2.7 Exercises

1. Show that $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$

2. Show that the number of ordered pairs of positive integers whose least common multiple is $n$ equals $\tau(n^2)$.

3. Show that $\sum_{d^2|n} \mu(d) = |\mu(n)|$

4. Show that if $\sigma(n)$ is odd then $n$ is a square or twice a square.

5⋆. Let $det(i, j)$ be the determinant of $n \times n$ matrix whose i,j entry is (i,j). Prove that

$$det(i, j) = \prod_{k=1}^{n} \phi(k)$$

6. Let
$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of prime } p \\ 0 & \text{otherwise} \end{cases}$$
Evaluate $\sum_{d|n} \Lambda(d)$. Express $\sum_{n=0}^{\infty} \frac{\Lambda(n)}{n^s}$ in terms of $\zeta(s)$.
(You may use $\prod_{p \text{ prime}}(1-p^{-s})^{-1} = \zeta(s)$).

7. Let $a$ run through the integers with $1 \leq a \leq n$ and $(a,n) = 1$. Show that $f(n) = \frac{1}{n}\sum a$ satisfies $\sum_{d|n} f(d) = \frac{1}{2}(n+1)$. Hence prove that $f(n) = \frac{1}{2}\phi(n)$ for $n > 1$

8. If $f(s) = \sum a_n n^{-s}$ and $g(s) = \sum b_n n^{-s}$. Show that $g(s) = f(s)\zeta(s)$ if and only if $\sum a_n \left(\frac{x^n}{1-x^n}\right) = \sum b_n x^n$ with $0 \leq x < 1$. Hence show that $\sum_{n=1}^{\infty} \frac{\phi(n)x^n}{1-x^n} = \frac{x}{(1-x)^2}$
(Hint: You may need the identity that $\sum_{n=1}^{\infty} nx^n = \frac{x}{(1-x)^2}$).

9. For which positive integer $n$ does the equation
$$\sigma(n) + \phi(n) = n\tau(n)$$
hold?

10. Prove that if $s = r^2$ is a square, then
$$\sum_{mn=s} |\mu(m)|\mu(n) = \mu(r).$$
What happens when $s$ is not a square?

11. Deduce the identity
$$\left(\frac{\lambda(n)}{n^s}\right)\zeta(s) = \zeta(2s)$$
with $\Re(s) > 1$.

## 2.8 Hints and Solutions

1. Pair $d$ and $\frac{n}{d}$ for each divisor $d$ and so the result follows.

2. If a pair $(x,y)$ has least common multiple $p^\alpha$, for some prime $p$ and $\alpha \geq 1$. Then, we must have, $a = p^\alpha, b = p^\beta$ for some $0 \geq \beta \leq \alpha$ or vice versa. So we have $2\alpha + 1$ such pairs. And $\tau(p^{2\alpha}) = 2\alpha + 1$. Now let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and so we have $\prod_{i=1}^{k}(2\alpha_i + 1)$ such pairs, which is equal to $\tau(n^2)$ as $\tau$ is multiplicative.

3. Suppose $n$ has a squared factor, then $\mu(n) = 0$. Let $n = a^2 b$, where $a > 1$ and $b$ is square free. Then $d^2|n \iff d|a$ and so LHS is $\sum_{d|a} \mu(d) = 0$ by Lemma 2.11.
Suppose now $n$ is square free, then $d^2|n \iff d = 1$ and so we have LHS is just $\mu(1) = 1$, and RHS is also 1.

4. Write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, where $p_i$ are distinct primes. Then suppose $\sigma(n)$ is odd, as $\sigma$ is multiplicative, we have that $\sigma(p_i^{\alpha_i}$ is odd for each $i$. But for $p_i \neq 2$, $\sigma(p_i^{\alpha_i}) = 1 + p_i + \dots + p_i^{\alpha_i}$ is odd if and only if $\alpha_i$ is even. And $\sigma(2^t)$ is odd $\forall k \geq 1$. Therefore, we conclude that $n$ is either a square or twice a square.

5. Let $g(i,j) = 1$ if $j|i$ and 0 otherwise. Then by Lemma 2.15, we have $(i,j) = \sum_{d|(i,j)} \phi(d) = \sum_{d \leq n} g(i,d)g(j,d)\phi(d)$ as $d|i, d|j \iff d|(i,j)$. Now let $A_{i,j} = (i,j)$ and let $B_{i,j} = g(i,j)$, $C_{i,j} = g(j,i)\phi(i)$. Then we have $A = BC$ and so $det(A) = det(B)det(C)$. Clearly, $det(B) = 1$ (It's upper triangular and every diagonal entry is 1). For $det(C)$, $C$ is also upper triangular, and the diagonal entry $C_{i,i} = \phi(i)$. Hence $det(A) = det(C) = \prod_{d=1}^{n} \phi(d)$.

6. Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Then the only contributions of $d$ in the sum are those divisors $d = p_i^{\beta_i}$, where $1 \leq \beta_i \leq \alpha_i$. And we have that $\Lambda(p_i^{\beta_i}) = \log p_i$ for each $i$ and so the total contribution is $\sum \alpha_i \log p_i = \log \prod p_i^{\alpha_i} = \log n$.
   Now by definition of $\Lambda$, we have that

$$\sum_{n=0}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{p \text{ prime}} \sum_{k=1}^{\infty} \frac{\log p}{p^{ks}} = \sum_{p \text{ prime}} \frac{p^{-s} \log p}{1 - p^{-s}}$$

   Now we may check that $\frac{\zeta'(s)}{\zeta(s)} = \frac{d(\log \zeta(s)}{ds}$, which is:

$$\frac{d\ [\log \prod_p (1 - p^{-s})^{-1}]}{ds} = -\sum_p \frac{d(\log 1 - p^{-s})}{ds} = -\sum_{p \text{ prime}} \frac{p^{-s} \log p}{1 - p^{-s}}$$

   Hence we conclude that the sum is $-\frac{\zeta'(s)}{\zeta(s)}$.

7. The first part follows from the proof of Lemma 2.15.
   Consider $\sum_{d|n} n \cdot f(d) = \sum_{d|n} \sum_{(a,d)=1} \frac{na}{d}$, and as in the proof, we know the that the sum runs through every integer in the set $\{1, 2 \dots n\}$ and so is $\frac{n(n+1)}{2}$. Therefore, since we have multiplied it by $n$, so $\sum_{d|n} f(d) = \frac{n+1}{2}$.
   For the second part, apply Theorem 2.12 (The inversion formula) and Lemma 2.17.

8. The series is absolutely convergent for $s > 1$ and so

$$f(s)\zeta(s) = \sum_{m=1}^{\infty} m^{-s} \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} n^{-s} \sum_{d|n} a_d$$

   Hence $f(s)\zeta(s) = g(s)$ if and only if

$$\sum_{d|n} a_d = b_n$$

   And for

$$\sum a_n \left( \frac{x^n}{1 - x^n} \right) = \sum b_n x^n$$

   Now we expand the fraction $\frac{x^n}{1-x^n} = x^n(1 + x^n + x^{2n} + \dots)$ (We can expand as $0 \leq x < 1$), we still have that the above equality holds if and only if

$$\sum_{d|n} a_d = b_n$$

   Thus we have proved the first part. For the second part, use the hint and write RHS as a sum. Then use Lemma 2.15 to write $n$ as a sum. It is then easy to check that $f(s)\zeta(s) = g(s)$, as $a_n = \phi(n), b_n = n$. So as in the proof of the first part, that

$$\sum_{d|n} a_d = b_n$$

9. Use the identities

$$\tau(n_= \sum_{d|n} 1, \sigma(n) = \sum_{d|n} d.$$

The equation can be rearranged as

$$\sum_{d|n} (n-d) = \phi(n).$$

In particular, if $n > 1$, the sum on LHS has a term $n-1$. Now we know that $\phi(n) \leq n-1$ and hence the sum on LHS must be $n-1$, and so $n$ must be a prime. Thus, it is true for all primes and nothing else.

10. We know that

$$\sum_{d^2|m} \mu(d) = |\mu(m)|$$

by question 3. Then

$$\begin{aligned} \sum_{mn=s} |\mu(n)|\mu(m) &= \sum_{nd^2=s} \mu(d)\mu(n) \\ &= \sum_{md^2=r^2} \mu(d)\mu(n) \\ &= \mu(r). \end{aligned}$$

The last lane follows from the fact that if $d|r$ then $n = \frac{r^2}{d^2}$ is a square and $\mu(m) = 0$ unless $m = 1$, in which case $d = r$.

If $s$ is not s square then $s > 1$ and we can write $s$ as $ab^2$ where $a$ is square free and $a > 1$. Then the above gives $d|b$ and $n|a\frac{b^2}{d^2}$, so

$$\begin{aligned} \sum_{nd^2=ab^2} \mu(d)\mu(n) &= \sum_{d|b} \mu(d) \sum_{n|a\frac{b^2}{d^2}} \mu(n) \\ &= \sum_{n|a} \mu(b)\mu(n) \\ &= 0. \end{aligned}$$

11. The quotient $\frac{\zeta(2s)}{\zeta(s)}$ has Euler product $\prod_p \frac{1}{1+p^{-s}}$ valid on $\Re(s) > 1$. Therefore, if we expand that in terms of power series then the result follows by considering the sign of the term $n^{-s}$.

# 3 Prime numbers and congruence

## 3.1 Prime numbers

**Theorem 3.1.** **[Euclid]** *There are infinitely many prime numbers.*

*Proof.* Suppose there are finitely many. Let $p_1, p_2 \dots p_n$ be the list of all primes. Then consider $N = \prod_{i \leq n} p_i + 1$. This is not divisible by any prime $p_i$ and hence it must have a prime factor different from $p_i$, which is a contradiction. □

**Definition 3.2.** *A prime number is called Mersenne Prime if it is a prime of the form $2^n - 1$ for some integer $n$. For example, $7 = 2^3 - 1, 31 = 2^5 - 1$.*

**Remark 3.3.** *Clearly, if $2^n - 1$ is prime, $n$ must be prime, otherwise, let $d|n$, then $2^d - 1$ is a proper factor.*

Here is a big conjecture of prime numbers: The number of primes $q \leq x$ such that $2^q - 1$ is also a prime is asymptotically $\sim c \log x$, where $c = \frac{e^\gamma}{\log 2}, \gamma = \lim_{n\to\infty}(1 + \cdots \frac{1}{n}) - \log n$. $\gamma$ is called Euler constant.

**Proposition 3.4.** *Let $N$ be any integer $\geq 2$, then there is a block of $N + 1$ consecutive composite numbers.*

*Proof.* Pick $p = N+2$, and let $M = p!$, then the integers $M+2, M+3 \dots M+p$ are all composite. □

**Definition 3.5.** *For any $x \geq 2$, write $\pi(x) = card\{p : p \text{ prime}, p \leq x\}$.*

Numerically, $\pi(10^2) = 25, \pi(10^3) = 168, \pi(10^4) = 1229, \pi(10^6) = 78498$.

**Definition 3.6.** *We write $f_S(x)$ to be the number of positive integer $\leq x$, composed of primes in the set $S$.*

**Proposition 3.7.** $\forall x \geq 2, f_S(x) \leq \sqrt{x} \cdot 2^{card(s)}$.

*Proof.* Take any $n \leq x$, composed only of primes in $S$. We can write $n = m^2 r$, where $r$ is square free. Then as $n \leq x$ and so $m \leq \sqrt{x}$. So we have at most $\sqrt{x}$ choices for $m$. Then for $r$, we write $r = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, where $p_i \in S$ and $\epsilon_i \in \{0, 1\}$ because $r$ is square free. And so we have $2^k = 2^{card(s)}$ choices for $r$. Therefore, we conclude that $f_S(x) \leq \sqrt{x} \cdot 2^{card(s)}$. □

**Corollary 3.8.** $\forall x \geq 2, \pi(x) \geq \frac{\log x}{2 \log 2}$.

*Proof.* Take $S$ to be the set of all primes $\leq x$. Then we have, by definition that $f_S(x) = x$, and $card(S) = \pi(x)$. Then by the above proposition, we have that $x \leq \sqrt{x} \cdot 2^{\pi(x)}$, and so $\pi(x) \geq \frac{\log x}{2 \log 2}$. □

## 3.2 Congruence

**Definition 3.9.** *If $a, b \in \mathbb{Z}$, we say $a \equiv b \pmod m$ if $m|a - b$.*

**Remark 3.10.** *We can easily check that this is an equivalence relation, and the equivalence classes are of the form $a + m\mathbb{Z}$. The set of equivalence classes is $\mathbb{Z}/m\mathbb{Z}$ (Quotient ring).*

**Lemma 3.11.** *If we write $[a]_m$ for the equivalence class of $a$ mod $m$, then we have:*

$$[a]_m + [b]_m = [a + b]_m, [a]_m \cdot [b]_m = [ab]_m$$

*Proof.* It is enough to check that, if $a \equiv a' \bmod m$, $b \equiv b' \bmod m$, then:

$$a + b \equiv a' + b' \pmod{m}, ab \equiv a'b' \pmod{m}$$

But, we know that $m|a-a', m|b-b'$, and so $m|(a+b)-(a'+b')$. Also as $ab-a'b' = (a-a')b+a'(b-b')$. Therefore, $m|ab - a'b'$. □

It is also easy to check that if $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$, where $(p, q) = 1$. Then we have $x \equiv a \pmod{pq}$.

We shall now use the notation that $(\mathbb{Z}/m\mathbb{Z})^*$ to mean the multiplicative group of $\mathbb{Z}/m\mathbb{Z}$. Sometimes, we write $(\mathbb{Z}/(m))^*$

**Lemma 3.12.** $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^* \iff (a, m) = 1$.

*Proof.* $a + m\mathbb{Z}$ is in the group if and only if it has an inverse element, say $b + m\mathbb{Z}$. And so we have proved that $[a]_m[b]_m = [ab]_m$. So the inverse element exists if and only if $\exists b, c$ such that $ab + cm = 1$. And this implies that $(a, m) = 1$. □

**Corollary 3.13.** *Let $p$ be a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field with $p$ elements.*

*Proof.* By Lemma 3.12, we have $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - [0]_p$ because every positive integer less than $p$ is prime to $p$. □

**Theorem 3.14.** *Let $a, b$ and $m$ be integers with $m > 0$. The congruence*

$$ax \equiv b \ (mod\ m)$$

*is soluble if and only if $(a, m)|b$. If $x_0$ os a solution, then there are exactly $(a, m)$ solutions given by $\{x_0 + \frac{tm}{(a,m)}\}$ where $t = 0, 1 \ldots (a, m) - 1$.*

*Proof.* This is just a restatement of Theorem 1.5 and use the definition of congruence. □

**Corollary 3.15.** *If $(a, m) = 1$ then the congruence*

$$ax \equiv b \ (mod\ m)$$

*has exactly one solution.*

*Proof.* Use Theorem 3.14. □

## 3.3 Fermat's little theorem and Euler's theorem

Fermat's theorem (Often called Fermat's little theorem) states that if $a$ is any natural number and $p$ is any prime, then $a^p \equiv a \pmod{p}$. The theorem was first announced in 1640 by Fermat but without proof. Euler, however, gave a first demonstration in 1760 and established a more general result:

**Theorem 3.16.** **[Euler's Theorem]** *Let $a, n$ be any positive integers such that $(a, n) = 1$. Then*

$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

*Proof.* Clearly, Fermat's little theorem is a special case of Euler's theorem. One may apply Lagrange theorem in group theory that the order of any element in the group divides the order of the group, and hence the result follows immediately. But here is a proof without Lagrange theorem:

Let $S$ be the set of integers less than $n$ which are prime to $n$, say $S = \{p_1, p_2, \ldots p_{\phi(n)}\}$. Then consider that for each $p_i a = b_i \pmod{n}$, $b_i$ must also be prime to $n$. And if $p_i a = p_j a \pmod{n}$, then $a(p_i - p_j) = 0 \pmod{n}$, and so $n|p_i - p_j$. But $(a, n) = 1$ and $-n < p_i - p_j < n$, so this is only possible when $p_i - p_j = 0$. i.e. $p_i = p_j$.

Use the above fact and by congruence multiplication, we have:

$$p_1 a \cdot p_2 a \cdots p_{\phi(n)} a \equiv b_1 b_2 \cdots b_{\phi(n)} \pmod{n}$$

where $\{b_1, b_2 \dots b_{\phi(n)}\}$ is a rearrangement of $\{p_1 \dots p_{\phi(n)}\}$. Hence we can cancel both sides by $p_1 p_2 \cdots p_{\phi(n)}$, and so

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

□

## 3.4 Wilson's theorem

**Theorem 3.17.** [**Wilson's Theorem**] *Let $p$ be any prime, then*

$$(p-1)! \equiv -1 \ (mod\ p)$$

The theorem was known to Ibn al-Haytham (also known as Alhazen) in Medieval Europe) circa 1000 AD, but it is named after John Wilson, a student of Waring. It is first published by Waring in his Meditationes algebraicae of 1770, but he nor Wilson could prove it. Lagrange gave the first proof in 1773.

*Proof.* It suffices to assume that $p > 2$ as the case when $p = 2$ is trivially true. Now assume $p > 2$, then let $b = 1$ and for each $a < p$, apply Corollary 3.15, we have that each $ax \equiv 1 \pmod{p}$ has only one solution. And we know by Corollary 3.13 and uniqueness of inverse in group, we can pair each $(a, x)$ such that $ax \equiv 1 \pmod{p}$. The inverse of 1 is itself, and the inverse of $p-1$ is also itself, and there are only one element which has order 2, because if $x^2 \equiv 1 \pmod{p}$, we have $p|(x-1)(x+1)$ but as $p$ is prime, so $p|x-1$ or $p|x+1$ and hence $x = 1$ or $x = p-1$. Therefore, other integers are paired up and so the product is 1 mod $p$. Therefore, we have that:

$$(p-1)! \equiv (p-1) \equiv -1 \pmod{p}$$

□

## 3.5 Chinese remainder theorem

The theorem was first stated by Chinese mathematician Sun Tzu in first century AD, and was later republished in a 1247 book by Qin jiushao, the Shushu jiuzhang. It concerns about simultaneous congruences.

For example, how can we solve a simultaneous congruence like:

$$x \equiv 2 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 6 \pmod{7}$$

**Theorem 3.18.** [**Chinese remainder theorem**] *Assume $(m_i, m_j) = 1$ for $i \neq j$, and that $M = m_1 m_2 \dots m_k$, and $a_1, a_2 \dots a_k$ are arbitary integers, then there exists $x$ in $\mathbb{Z}$ satisfying $x \equiv a_1$ (mod $m_1$), ..., $x = a_k$ (mod $m_k$). Moreover, any two solutions are congruent mod $M$.*

*Proof.* Define $M_i = \frac{M}{m_i}$. Then we have $(m_i, M_i) = 1$. Hence $\exists u_i$ such that $u_i M_i \equiv 1 \pmod{m_i}$. Then we set $x = \sum_{j=1}^{k} a_j u_j M_j$. Then we can check that as $M_i \equiv 0 \pmod{m_j}$ for any $i \neq j$. Hence $x \equiv a_i \pmod{m_i}$ and so it is a solution.

Finally, to check that any two solutions are congruent mod $M$, let $x_1, x_2$ be two solutions. Then $x_1 \equiv x_2 \pmod{m_i}$ $\forall i$. And as $(m_i, m_j) = 1$, so $x_1 \equiv x_2 \pmod{\prod m_i}$, i.e. $x_1 \equiv x_2 \pmod{M}$. □

We have another group theoretic of Chinese remainder theorem.

**Definition 3.19.** $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \mathbb{Z}/m_k\mathbb{Z} = \{(r_1, r_2, \ldots r_k) : r_i \in \mathbb{Z}/m_i\mathbb{Z}\}$ *is a ring given by pointwise operation.*

**Theorem 3.20.** *Assume* $(m_i, m_j) = 1, i \neq j$ *and* $M = m_1 m_2 \ldots m_k$. *Then the map:*

$$\theta : \mathbb{Z}/M\mathbb{Z} \longmapsto \mathbb{Z}/m_1\mathbb{Z} \times \ldots \mathbb{Z}/m_k\mathbb{Z}$$

*by* $\theta(a + M\mathbb{Z}) = (a + m_1\mathbb{Z}, \ldots, a + m_k\mathbb{Z})$ *is an isomorphism.*

*Proof.* It is clear that $\theta$ is an homomorphism, by definition of congruence operation. $\theta$ is clearly injective, since if $\theta(a + M\mathbb{Z}) = 0$, so have:

$$a \equiv 0 \pmod{m_i} \forall i$$

As $(m_i, m_j) = 1$, so $a \equiv 0 \pmod{M}$. Now consider cardinality of $\mathbb{Z}/M\mathbb{Z}$ and the cardinality of $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$. They are the same, hence it is bijective. So $\theta$ is isomorphism. □

This has an immediate corollary:

**Corollary 3.21.** $\phi$ *is multiplicative. (This is another proof)*

*Proof.* Use Theorem 3.20 □

## 3.6 Polynomial and polynomial congruence

The polynomial congruence investigates the solutions to the congruence of the form $f(x) \equiv 0 \pmod{m}$, where $f(x) \in \mathbb{Z}[x]$. For example, $f(x) = x^2 - 1, m = 8$ has four solutions, $x = 1, 3, 5, 7$.

**Definition 3.22.** *Let* $R$ *be commutative ring.* $R[x] = \{\sum_{i=1}^{n} a_i x^i : a_i \in R, n \in \mathbb{N}\}$. *We call the* **evaluation** *of* $\alpha \in R$ *if* $f(x) = \sum_{i=0}^{n} a_i x^i, f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in R$.

**Lemma 3.23.** *For each* $f(x)$ *in* $R[x]$ *and each* $\alpha \in R$, *there exists* $h(x)$ *in* $R[x]$ *such that* $f(x) - f(\alpha) = (x - \alpha)h(x)$.

*Proof.* $f(x) - f(\alpha) = a_1(x - \alpha) + \cdots a_n(x^n - \alpha^n)$. Then

$$x^k - \alpha^k = (x - \alpha)(x^{k-1} + \cdots + \alpha^{k-1})$$

So $f(x) - f(\alpha) = (x - \alpha)h(x)$ for some $h(x)$. □

**Corollary 3.24.** *For any* $f(x)$ *in* $R[x]$ *and any* $\alpha \in R$, *we have* $f(\alpha) = 0$ *if and only if* $f(x) = (x - \alpha)h(x)$ *for some* $h(x)$ *in* $R[x]$.

*Proof.* Use Lemma 3.23. □

**Definition 3.25.** $R$ *is an* **integral domain** *if* $R$ *has no zero divisor, i.e.* $\alpha\beta = 0 \Rightarrow \alpha = 0$ *or* $\beta = 0$.

**Proposition 3.26.** *Let* $R$ *be an integral domain. Let* $f(x) \in R[x]$ *have distinct root* $\alpha_1, \ldots, \alpha_k$. *Then we can write:*

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_k)h(x)$$

*for some* $h(x) \in R[x]$.

*Proof.* Induction on $k$. It is true for $k = 1$ by applying Lemma 3.23 with $f(\alpha) = 0$. Assume it is true for $k = s$. Then for $s + 1$, we have:

$$0 = f(\alpha_{s+1}) = (\alpha_{s+1} - \alpha_1) \cdots (\alpha_{s+1} - \alpha_s)h(\alpha_{s+1})$$

by inductive hypothesis, where $\alpha_{s+1} \neq \alpha_i, i = 1, 2 \ldots, s$. Hence $h(\alpha_{s+1}) = 0$ because $R$ is integral domain. And so we apply the case when $k = 1$ to write $h(x) = (x - \alpha_{s+1})h_1(x)$. The result follows □

**Corollary 3.27.** [**Lagrange**] *Let $R$ be an integral domain, let $f$ be a non-zero polynomial in one variable of degree $n$. Then $f$ has at most $n$ distinct roots in $R$.*

*Proof.* The proof is again induction on $n$. When $n = 1$, we have $f(x) = ax + b, a \neq 0$, say. Then $ax + b = 0 \iff ax = -b$. As $a \neq 0$ and so we have an inverse of $a$. Therefore, $x = -a^{-1}b$ is the only solution. □

Here is an immediate application of Lagrange's theorem, which is another proof of Wilson's theorem (Theorem 3.17):

Again the case $p = 2$ is trivial so let $p > 2$. Consider the equation $f(x) = x^{p-1} - 1 - (x - 1)(x - 2)\dots(x - p + 1)$ in the ring $\mathbb{Z}/p\mathbb{Z}$. Then by Fermat's little theorem, any $x \in \{0, 1 \dots p - 1\}$ is a solution, but the term $x^{p-1}$ is canceled and so degree of $f(x)$ is at most $p - 2$. Therefore, by Lagrange's theorem, $f(x)$ must be identically zero in the ring $\mathbb{Z}/p\mathbb{Z}$. Hence, we consider the constant coefficient, we have that

$$-(-1)^{p-1}(p-1)! - 1 \equiv 0 \pmod{p}$$

Hence the result follows.

Surprisingly, the converse is also true and the proof is left as an exercise (see question 6)

## 3.7 Chevalley's theorem

We may briefly discuss the general case in this subsection and congruences in more than more variable will be considered. Throughout the section, let $p$ be a fixed prime, and $f, g$ and $h$ be polynomials defined over $\mathbb{Z}/p\mathbb{Z}$, and let $\deg f$ denote the total degree of $f$. We begin with the following definitions:

**Definition 3.28.** *If $f$ and $g$ are $n$-variable polynomials, we say $f$ is* **equivalent** *to $g$, written $f \equiv g$, if for all sets $\{a_1, \dots a_n\}$ of elements of $\mathbb{Z}/p\mathbb{Z}$ we have*

$$f(a_1, ldots, a_n) \equiv g(a_1, \dots a_n) \ (mod\ p)$$

**Definition 3.29.** *We say $f$ is* **congruent** *to $g$, written as $f \sim g$, if all coefficients of corresponding monomials of $f$ and $g$ are congruent mod $p$. (monomials are of the form $x_1^{\alpha_1} \dots x_n^{\alpha_n}$)*

**Definition 3.30.** *$f$ is called reduced if $f$ has degree less than $p$ in each of its variables.*

**Remark 3.31.** *If $f$ is congruent to $g$, then $f$ is equivalent to $g$, as the coefficient of each monomial is congruent mod $p$. But the converse is not true. For example, $x^p \equiv x$, but $x^p \not\sim x$ as the coefficient of $x$ in $x^p$ is $0$ but is $1$ in $x$. Note that $x^p$ is not reduced.*

**Lemma 3.32.** *Given a polynomial $f$ we can find a reduced polynomial $f'$ such that $\deg f' \leq \deg f$ and $f' \equiv f$.*

*Proof.* Use Fermat's little theorem and so for each term $x^k, k \geq p$ in $f$. Write $k = ap + b$, where $b < p$. Then $x^k \equiv x^{a+b} \pmod{p}$ and $a + b < k$. If $a + b < p$ then we are done with this term, and if not we apply the above to $x^{a+b}$ again until the index is less than $p$. Now apply this to every term $x^k, k > p$ □

**Lemma 3.33.** *If $f$ and $g$ are reduced polynomials and $f \equiv g$, then $f \sim g$.*

*Proof.* It is easy to check from definition that $f \equiv g \iff f - g \equiv 0$ and $f \sim g \iff f - g \sim 0$. So WLOG, we can assume that $g$ is zero polynomial.

Let $f$ be reduced, $f \equiv 0$. If $n = 1$, as $f$ has degree less than $p$ but any $a \in \mathbb{Z}/p\mathbb{Z}$ is a root, so by Lagrange theorem (Corollary 3.27) we must have that $f \sim g$.

If $n \geq 2$, write $f = f(x_1, \dots x_n)$. Then we may fix $a_2, a_3 \dots a_n$ and treat $f$ as a polynomial in one variable $x_1$. Then as $f(a_1, \dots, a_n) \equiv 0$ for any set $\{a_1, a_2 \dots a_n\}$, it is equivalent to say that the

polynomial $f$ in the variable $x_1$ has roots $\{0, 1, 2, \dots p-1\} = \mathbb{Z}/p\mathbb{Z}$. But $f$ has degree less than $p$ in $x_1$, and hence by Lagrange theorem, we have that each coefficient is congruent to 0.

Now each coefficient is a polynomial in n-1-variables, i.e. $x_2, x_3 \dots x_n$. And we can continue this argument inductively, and hence we conclude that $f \sim 0$. □

**Theorem 3.34. [Chevalley's Theorem]** *Suppose $f$ and $g$ are n-variable polynomials with degree less than $n$.*

*(i) If the congreunce*

$$f(x_1, \dots, x_n) \equiv 0 \ (mod\ p)$$

*is soluble, then it has at least two solutions.*

*(ii) Suppose $g$ is a homogeneous polynomial then the congruence*

$$g(x_1, \dots x_n) \equiv 0 \ (mod\ p)$$

*has a non-trivial solution.*

*Proof.* (ii) follows from (i) because clearly that in the homogenous case, $\{0, 0, \dots 0\}$ is always a solution and hence by (i) we have another non-trivial solution.
For (i) assume that $\deg f = r$ and we have only one solution $x_i = a_i \pmod p$, $i = 1, 2 \dots n$. Let $h$ be given by:

$$h(x_1, \dots, x_n) = 1 - f(x_1, \dots, x_n)^{p-1}$$

then by assumption we have $h(x_1, \dots, x_n) \equiv 1 \pmod p$ if $x_1 \equiv a_i \pmod p$ for all $i$, and by Fermat's little theorem, $h(x_1, \dots, x_n) \equiv 0 \pmod p$ for any other $x_i$.

Now by Lemma 3.32 we have some $h'$ which is a reduced polynomial such that $h' \equiv h$. Then we define:

$$h''(x_1, \dots x_n) = \prod_{i=1}^{n} \left(1 - (x_i - a_i)^{p-1}\right)$$

Clearly, $h'' \equiv h$, and hence we have $h'' \equiv h'$. But both $h'$ and $h''$ are reduced, then by Lemma 3.33, $h' \sim h''$. By Lemma 3.32, $\deg h' \leq \deg h = r(p-1)$. But $h''$ has degree $n(p-1)$, and this is impossible as we assume that $r < n$, which is a contradiction. So we have at least two solutions. □

## 3.8 Primitive root and non-linear congruence

In this subsection, we will investigate $\mathbb{Z}/p^\alpha\mathbb{Z}$ for any odd prime $p$ and $\alpha \geq 1$.

**Lemma 3.35.** *Let $G$ be a cyclic group of order $d > 1$, then $G$ has $\phi(d)$ generators.*

*Proof.* Write $G =< g >$. Then each element $g^n$ has order $d$ if and only if $(n, d) = 1$. □

**Lemma 3.36.** *Let $H$ be any finite group of order $n$. Suppose for all divisor of $n$, the set of $x$ in $H$ with $x^d = 1$ has cardinality $\leq d$, then $H$ is cyclic.*

*Proof.* For each $d|n$, let $W_d = \{x \in H : x \text{ has exact order } d\}$. We check that $W_d$ is non-empty for each $d$. Suppose it is, then by construction, we have:

$$n = \sum_{d|n} card(W_d)$$

and if $\exists x, x$ has order $d$, then consider $G =< x >$ and apply Lemma 3.35, we have $\phi(d)$ elements of order $d$. Therefore, we know that $card(W_d) = \phi(d)$ or 0. But by lemma 2.15

$$n = \sum_{d|n} \phi(d)$$

and hence $W_d$ can never be empty.

Now as each $W_d$ is non-empty, take $y \in W_d$, and consider the set:

$$\{1, y, y^2, \ldots, y^{d-1}\}$$

Each element in the set satisfies $x^d = 1$. Now by assumption we have at most $d$ elements satisfying this for each $d$. Hence we conclude these are all solutions. In particular, take $d = n$, then every element in the group satisfies $x^n = 1$ and $W_n$ is non-empty, i.e. we have some element whose exact order is $n$ and so the group is cyclic. □

**Theorem 3.37.** *Let $F$ be any finite field. Then $F^*$ ($F - \{0\}$ as a group under $*$) is cyclic.*

*Proof.* Let $H = F^*$, and as $q = card(F)$. Then $F*$ has $q-1$ elements. If $d|q-1$, then $x^d - 1$ has at most $d$ distinct roots by Lagrange's theorem (3.27) as a field must be an integral domain. Then the set of $x \in H$ with $x^d = 1$ has cardinality $\leq d$, by Lemma 3.36, $F^* = H$ is cyclic. □

The main theorem of the subsection is:

**Theorem 3.38.** *If $p$ is an odd prime, then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic for all $n \geq 1$.*

**Remark 3.39.** *The condition that $p$ is an odd prime is necessary. It does not work for $p = 2$. For example, $(\mathbb{Z}/8\mathbb{Z})^* = C_2 \times C_2$. But in fact, we can prove that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is isomorphic to $C_2 \times C_{2^{n-2}}$.*

To prove the theorem, we need the followings:

**Lemma 3.40.** *There is a primitive root $g$ mod $p$ (i.e. $g$ has exact order $p-1$) such that $g^{p-1} = 1+bp$, where $(b, p) = 1$*

*Proof.* Take any primitive root $g_1$ as we know the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Let $g_1^{p-1} = 1 + b_1 p$. If $(b_1, p) = 1$ then we take $g_1$. Otherwise, we have $p|b$, and we take $g = g_1 + p$. Then $g^p - 1 = (g_1 + p)^{p-1} - 1 = g_1^{p-1} - 1 + (p-1)g_1^{p-2}p + cp^2$.

So we have $g^p - 1 = (b_1 p + cp^2) + (p-1)g_1^{p-2}p = p(b_1 + cp + (p-1)g_1^{p-2})$, and as we have $p|b_1$, so $p|b_1 + cp$ and so $p \nmid b_1 + cp + (p-1)g_1^{p-2}$ and so $g^p = 1 + bp$, where $(b, p) = 1$. □

**Lemma 3.41.** *Let $p$ be an odd prime and $w$ be any integer of the form $w = 1 + bp$, where $(b, p) = 1$. Then $\forall n \geq 0$, we have $w^{p^n} = 1 + b_n p^{n+1}$ with $(b_n, p) = 1$.*

*Proof.* Use induction on n. It is true for $n = 0$ by assumption. Suppose it is true for n, then $w^{p^{n+1}} = (1 + b_n p^{n+1})^p = 1 + b_n p^{n+2} + \sum_{i=2}^{p} \binom{p}{i} {b_n}^i p^{(n+1)i}$ As $p$ is an odd prime, so $p|\binom{p}{i}$ $\forall 1 \leq i \leq p-1$.

So we have $1+b_n p^{n+2}+cp^{2n+3} = 1+b_{n+1}p^{n+2}$, where $b_{n+1} = b_n+cp^{n+1}$. Therefore, $(b_{n+1}, p) = 1$ □

Now we can prove theorem 3.38

*Proof.* Take $g$ to be any primitive root with $(b, p) = 1$, as in Lemma 3.40. Then $g + p^n\mathbb{Z}$ has exact order $p^{n-1}(p-1)$ $\forall n \geq 0$, by using Lemma 3.41. So $g$ is a generator. □

**Remark 3.42.** *This means that, to find the generator of $(\mathbb{Z}/p^n\mathbb{Z})^*$, we just need to check $(\mathbb{Z}/p\mathbb{Z})^*, (\mathbb{Z}/p^2\mathbb{Z})^*$.*

Finally, we briefly discuss some non-linear congruences. Consider $f(x)$, a polynomial in one variable, and we want to find all solutions to

$$f(x) \equiv 0 \pmod{m}$$

Then by Chinese remainder theorem, the problem is reduced to solving $f(x) \equiv 0 \pmod{p^\alpha}$ for some prime $p$ and $\alpha \geq 1$. Consider that, suppose we have a solution $x_0$ of the congruence

$$f(x) \equiv 0 \pmod{p^\alpha}$$

Then we use a version of Taylor's theorem, so that:

$$f(x_0 + tp^\alpha) = f(x_0) + tp^\alpha f'(x_0) + \ldots + \frac{(tp^\alpha)^n}{n!} f^{(n)}(x_0)$$

where $n$ is the degree of $f$ and $t$ is an integer. As $f$ is a polynomial, so that consider the expansion of $f(x_0 + tp^\alpha)$, we have that the $k^{th}$ derivative of $f$ is divisible by $k!$. So that $f(x_0 + tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$ if and only if

$$f(x_0) + tp^\alpha f'(x_0) \equiv 0 \pmod{p^{\alpha+1}}$$

which is equivalent to

$$tf'(x_0) = -f(x_0)/p^\alpha \pmod{p}$$

Now if $p \nmid f'(x_0)$, then it has a unique $t$ and so the solution $x_0$ to $f(x_0) \equiv 0 \pmod{p^\alpha}$ gives rise to a unique solution $x_0 + tp^\alpha$. If $p | f'(x_0)$, then we are in the case

$$f(x_0 + tp^\alpha) \equiv f(x_0) \pmod{p^{\alpha+1}}$$

and so either $x_0 + tp^\alpha$ is a solution to

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}$$

for all $t$, or we have no solution corresponding to $x_0$.

**Example 3.43.** *Consider the congruence $f(x) \equiv 0$ (mod 27) where $f(x) = x^3 - 2x^2 + 3x + 9$.*
*STEP(i): As $27 = 3^3$, we start with 3. Clearly, we have two solutions, $x = 0, 2$.*
*STEP(ii): Congruence mod 9.*

*(a) $x = 0$. We have $f(0) = 9$ and $f'(0) = 3$, so 0 is a solution mod 0, and both 3 and 6 are solutions (mod 9).*

*(b) $x = 2$. We have $f(2) = 15$ and $f'(2) = 7$, and the congruence:*

$$7t \equiv -15/3 \pmod{3}$$

*has a solution $t1$. Hence $2 + 3 = 5$ is another solution (mod 9).*

*STEP(iii): Congruence mod 27.*

*(a) $x = 0$. As $3 | f'(0), 27 \nmid f(0)$, so we have no solution.*

*(b) $x = 3$. As $3 | f'(3), 27 | f(3)$, and so we have solutions $3, 12, 21$.*

*(c) $x = 6$. As $3 | f'(6), 27 \nmid f(6)$, so we have no solution.*

*(d) $x = 5$. $f(5) = 99, f'(5) = 58, 3 \nmid 58$ so the congruence*

$$58t \equiv -11 \pmod{3}$$

*has a solution $t = 1$ and so 14 is a solution.*

*To conclude, we have solutions $3, 12, 14, 21$ (mod 27).*

## 3.9 Exercises

1. If $x$ is an integer $\geq 2$, by considering the fundamental theorem, show that

$$x \leq \left(1 + \frac{logx}{log2}\right)^{\pi(x)}$$

2. Let $p_n$ denote the $n^{th}$ prime. Deduce that $p_{n+1} \leq 2^{2^n} + 1$, whence $\pi(x) \geq \log\log x$ for $x \geq 2$.

3. Let $q$ be an odd prime. Prove that every prime factor of $2^q - 1$ must be congruent to 1 mod $q$.

4. Prove that there exists infinitely many primes of the form $4k + 3$.

5. Prove that if $(a, m) = (a - 1, m) = 1$, then

$$1 + a + a^2 + \ldots + a^{\phi(m)-1} \equiv 0 \pmod{m}$$

and deduce that every prime other than 2 or 5 divides infinitely many of the integers,$1, 11, 111, 1111, \ldots$.

6. Show that if $m > 4$ then $(m - 1)! \equiv -1 \pmod{m}$ if and only if $m$ is prime. (This proves the converse of Wilson's theorem)
Show further that if $p$ is an odd prime and $0 < k < p$, then

$$(p - k)!(k - 1)! \equiv (-1)^k \pmod{p}$$

7. Show that if $(m, n) = 1$, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

8. Show that the congruence $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ has just $p - 1$ solutions $\pmod{p^j}$ for every prime power $p^j$.

9. Solve the simultaneous congruences:

$$x \equiv 5 \pmod{6}$$

$$7x \equiv 5 \pmod{12}$$

$$17x \equiv 19 \pmod{30}$$

10. Show that

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}$$

have a common solution if and only if $(m, n)|b - a$, and the solution is unique modulo the least common multiple of $m$ and $n$.

11. Show that 2 and 3 are both generators of $(\mathbb{Z}/5^n\mathbb{Z})^*$. Prove that, for every natural number $n$, either there is no primitive root (mod $n$) or there are $\phi(\phi(n))$ primitive roots (mod $n$).

12. Prove that, for any prime $p$, the sum of all the distinct primitive roots (mod $p$) is congruent to $\mu(p-1)$ (mod $p$).

13. Solve the congruence if possible:

$$x^3 - 2x + 4 \equiv 0 \pmod{125}$$

14. Suppose $a, n$ are integers $\geq 2$, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^*$ is exactly $n$, and deduce that $n$ divides $\phi(N)$. If $n$ is a prime, deduce that there exists infinitely many primes $q$ such that $q \equiv 1 \pmod{n}$.

15. Let $p$ be an odd prime. By considering the polynomial $x^{p-1} - 1 - (x-1)(x-2)\dots(x-p+1)$, show that if $u_p = 1 + \frac{1}{2} + \dots \frac{1}{p-1}$, then the numerator of $u_p$ is divisible by $p$.$^\star$ Show further that it is also divisible by $p^2$.

16. Compute $(\mathbb{Z}/2^n\mathbb{Z})^*$ for $n \geq 3$ (Hint: you may find it useful to show that $-1, 5$ generate the group).

## 3.10 Hint and Solutions

1. Let $S$ be the set of all primes less than or equal to $x$. By fundamental theorem, we may factorise any integer $n \leq x$ into prime factors in $S$, say $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, where we have $k = \pi(x)$ and as each $p_i \geq 2$, so $\alpha_i \leq \frac{\log x}{\log 2}$. Hence the result follows.

2. Induction on $n$. It is true when $n = 0$, as $p_1 = 2 \leq 3$. Suppose it is true for all $k \leq n$, then consider $p_1 \cdot p_2 \dots p_n + 1$, this number is not divisible by any of the first $n$ primes and hence the $(n+1)^{th}$ prime must be less than or equal to this number. By induction, it is $\leq (2^{2^0} + 1)(2^{2^1} + 1) \dots (2^{2^n} + 1) \leq 2^{2^{n+1}} + 1$. Hence it holds for all $n$. For the second part, replace $n$ with $\pi(n)$ in the result, and by definition $p_{\pi(n)+1}$ is the least prime greater than $n$ and hence $p_{\pi(n)+1} - 1 \geq n$. Then take logarithm on both sides, and use $2 < e$, so that we have $\pi(n) \geq \log\log n$.

3. Let $p$ be a prime factor of $2^q - 1$. Then we have $p | 2^q - 1$ and so

$$2^q \equiv 1 \pmod{p}$$

But $p$ is also prime, and so by Fermat's little theorem

$$2^{p-1} \equiv 1 \pmod{p}$$

Let $d$ be the order of 2 mod $p$. Then $d|q$ and $d|p-1$. But $q$ is prime, so $d = 1$ or $d = q$. But $d = 1$ is impossible and so $d = q$. Hence $q|p-1$.

4. Suppose there are finitely many, say $p_1, p_2 \dots p_n$. Then consider

$$P = 4\prod_{t=1}^{n} p_i - 1$$

This is an integer of the form $4k+3$, but is not divisible by any $p_i$. Now consider the prime factor of $P$. If every prime factor is of the form $4k+1$, then the product $P$ also has the form $4k+3$. Therefore, we have some prime factor, say $p$, which has the form $4k+3$ and is distinct from $p_i$, which is a contradiction.

5. As $(a, m) = 1$ we have the following two congruences

$$a^{\phi(m)} - 1 \equiv 0 \pmod{m} \text{ and } a^{\phi(m)} - 1 \equiv 0 \pmod{a-1}$$

and use Chinese Remainder theorem, as $(a-1, m) = 1$, we have that

$$a^{\phi(m)} - 1 \equiv 0 \pmod{(a-1)m}$$

and so $m|\frac{a^{\phi(m)}-1}{a-1}$. Therefore,

$$1 + a + \dots a^{\phi(m)-1} = \frac{a^{\phi(m)} - 1}{a-1} \equiv 0 \pmod{m}$$

Now use the first part we conclude that for each prime $m$, if $(m, 10) = (m, 9) = 1$. (i.e. $m \neq 2, 3, 5$), then we have $m|\underbrace{11\dots1}_{m-1}$. For example, $7|111111$. Also, we may observe that $3|111$.
So we can conclude that, if $m \neq 2, 5$ then there is at least one integer $n$ of the form $11\dots1$ such that $m|n$.
If $m|n$, let $k$ be an integer such that $10^{k-1} \leq n < 10^k$, then $m|10^k n + n$. Hence we have construct another integer $n' = 10^k n + n$ of the form $11\dots1$ such that $m|n'$. Use this observation, we conclude that there are infinitely many of them.

6. If $m$ is prime, then $(m-1)! \equiv -1 \pmod{m}$ by Wilson's theorem. Conversely, suppose $m$ is not prime, then if $m$ is not a square, we have $m = ab$ with $a, b < m, a \neq b$, and so $(m-1)! \equiv 0 \pmod{m}$. If $m$ is a square, let $m = p^2$, then as $m > 4$, we have $p > 2$ and so $2p < p^2$. So $p \cdot 2p \equiv 0 \pmod{m}$ and hence $(m-1)! \equiv 0 \pmod{m}$.
The second part is an immediate application of Wilson's theorem. As we have

$$(p-1)! = -1 \pmod{p}$$

and observe that $p - k + t \equiv (-1)(k-t) \pmod{p}$ and hence the result follows by applying Wilson's theorem and counting the number of $t, 1 \leq t \leq k-1$.

7. By Euler's theorem, as $(m, n) = 1$, we have

$$m^{\phi(n)} \equiv 1 \pmod{n} \text{ and } n^{\phi(m)} \equiv 1 \pmod{m}$$

and so we have

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m} \text{ and } m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n}$$

To finish the proof, apply Chinese Remainder theorem.

8. If $p = 2$, then it is clear that we have only one solution. If $p > 2$, then we apply Theorem 3.38. Let $g$ be a generator of $(\mathbb{Z}/p^j\mathbb{Z})^*$ and then $g^{kp^{j-1}}, k = 1, 2, \ldots p-1$ are the only solutions.

9. We need to check that the second congruence is consistent with the first one. But indeed if we multiply both sides by $-5$, We have $x \equiv 5 \pmod{12}$. And so we don't need the first congruence anymore. Now solve the third congruence, we have $x \equiv 17 \pmod{30}$. Now use Chinese Remainder theorem, we have $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$. Therefore, we have $x \equiv 17 \pmod{60}$.

10. Let $d = (m, n), k = \frac{m}{d}, l = \frac{n}{d}$. Then it has a solution if and only if

$$x \equiv a \pmod d \text{ and } x \equiv b \pmod d$$

by applying Chinese Remainder theorem. This is consistent if and only if $d|(b-a)$, and so the result follows. Then again by Chinese Remainder theorem, the solution is unique up to modulo $d \cdot k \cdot l$, which is the least common multiple of $m, n$.

11. By Remark 3.42, we can easily check that $2, 3$ are generators of $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/25\mathbb{Z}$, and so they are generators of $\mathbb{Z}/5^n\mathbb{Z}$ for all $n$. Now for a natural number $n$, suppose it has a primitive root, say $g$. The order of the cyclic group is $k = \phi(n)$, and there are $\phi(k)$ integers which are less than $k$ and prime to $k$, say $\{1 = a_1, a_2, \ldots a_{\phi(k)}\}$, and so $g^{a_i}$ gives a list of primitive roots, and so we have $\phi(k) = \phi(\phi(n))$ of them.

12. If $p = 2$, it is obvious. If not, let $f(d)$ be the sum of $d^{th}$ primitive root, where $d$ is a factor of $p-1$. Then consider that

$$1 + 2 + \ldots p - 1 = \sum_{d|p-1} f(d)$$

because each element is some $d^{th}$ primitive root. We want to calculate $f(p-1)$. Let $g(p-1) = \sum_{d|p-1} f(d)$, then we apply Theorem 2.12, the inversion formula, we get $f(p-1) = \sum_{d|p-1} g\left(\frac{p-1}{d}\right)\mu(d)$. Now $g(p-1) \equiv 0 \pmod p$. But $g(1) = 1$, so we apply the inversion formula, we have $f(p-1) \equiv \mu(p-1) \pmod p$.

13. STEP(i): Congruence mod 5, we have solutions $3, 4$.
STEP(ii): Congruence mod 25

(a) $x = 3, f(3) = 20, f'(3) = 25$, we have no solution.

(b) $x = 4, f(4) = 55, f'(4) = 46$, so $t = 4$, and so 24 is a solution.

STEP(iii): Congruence mod 125 $x = 19, f(19) = 13375, f'(19) = 1081$, so $t = 0$ and so 24 is a solution.
Hence the only solution is 24.

14. The first part is clear as $a^n \equiv 1 \pmod N$ and $a^d < N$, if $d < n$. The order of the multiplicative group is $\phi(N)$ and so the order of $a$, which is $n$, divides $\phi(N)$.

Now fix a prime number $n$, suppose there are only finitely many, say $q_1, \ldots q_k$. Let $Q = q_1 q_2 \ldots q_k$ for any $q_i \equiv 1 \pmod n$, and let $N = (nQ)^n - 1$. WLOG, $N = p_1^{e_1} \ldots p_t^{e_t}$, and by

previous part, we know $n|\phi(N) = p_1^{e_1-1} \dots p_t^{e_t-1}(p_1-1)\dots(p_t-1)$. But clearly, $n \nmid N$, and so $n$ cannot be any $p_i$. Thus $n|p_i - 1$ for some $i$. Hence, $p_i \equiv 1 \pmod{n}$, but $q_j \nmid N$ for all $j$, and so $p_i \neq q_j \ \forall i, j$. So we have constructed another prime which is congruent to 1 mod $n$, contradicting the assumption.

15. Observe that the numerator of $u_p$ is the coefficient of the sub-leading term of the given polynomial, possibly with a negative sign, which we don't need to care about. Now, by Lagrange's theorem and Fermat's little theorem, we have that the polynomial must be 0 congruent to $p$, because $1, 2 \dots p-1$ are all solutions but the degree of the polynomial is $p-2$ (at most). Hence the sub-leading term is divisible by $p$. For the second part, we can rearrange the summation, so that

$$1 + \frac{1}{2} + \ldots + \frac{1}{p-1} = (1 + \frac{1}{p-1}) + (\frac{1}{2} + \frac{1}{p-2}) + \ldots + (\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}})$$

which can be simplified as

$$\frac{pA}{(p-1)!}$$

where

$$A = \sum_{a=1}^{\frac{p-1}{2}} \frac{(p-1)!}{a(p-a)}$$

Now we check that, for each $a$

$$\frac{(p-1)!}{a(p-a)} \equiv a^{-2} \pmod{p}$$

Indeed, let $x = \frac{(p-1)!}{a(p-a)}$, then $a(p-a)x = (p-1)!$, which is congruent to $-1$ mod $p$, by Wilson's theorem. And as $(p-a) \equiv -a \pmod{p}$, hence $x \equiv a^{-2} \pmod{p}$. Use this, we conclude that

$$A \equiv (1)^{-2} + (2)^{-2} + \ldots + (\frac{p-1}{2})^{-2} \pmod{p}$$

Therefore,

$$2A \equiv (1)^{-2} + (2)^{-2} + \ldots + (\frac{p-1}{2})^{-2} + (1)^{-2} + (2)^{-2} + \ldots + (\frac{p-1}{2})^{-2} \pmod{p}$$

Writing $a^{-2}$ as $(-a)^{-2}$ in the above summation, we have

$$2A \equiv \sum_{a=1}^{p-1} a^{-2} \pmod{p}$$

But summing over $a^{-1}$ is the same as summing over $a$, hence

$$2A \equiv \sum_{a=1}^{p-1} a^{2} \pmod{p}$$

Now apply

$$\sum_{a=1}^{p-1} a^2 = \frac{(p-1)p(2p-1)}{6}$$

as $p > 3$, so $6 \nmid p$, and so $2A \equiv 0 \pmod{p}$ and hence $A \equiv 0 \pmod{p}$. Therefore, as $(p-1)! \nmid p$, so the numerator $\frac{pA}{(p-1)!}$ is congruent to 0 mod $p$.

16. Check that for $n \geq 3$, we have

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n} \ \forall n.$$

Indeed, it is true for $n = 3$. Suppose it is true for $n - 1$, then

$$5^{2^{n3}} = \left(5^{2^{n-4}}\right)^2 = \left(1 + 2^{n-2} + t(2^{n-1})\right)^2 \equiv 1 + 2^{n-1} \pmod{2^n}.$$

Thus it holds for all $n$. Also, this implies that $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ and so 5 has order $2^{n-2}$.

It is clear that $-1$ has order 2. We check that $-1$ does not lie in $\langle 5 \rangle$. To see this, suppose $5^x \equiv -1 \pmod{2^n}$, and pick $x$ to be the least number which satisfies that, then $2x = 2^{n-2}$ and $x = 2^{n-3}$ but this is impossible as

$$1 + 2^{n-1} \not\equiv -1 \pmod{2^n}.$$

Hence $\langle -1, 5 \rangle = (\mathbb{Z}/2^n\mathbb{Z})^*$ by comparing the order of both sides. Therefore, we conclude that

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

# 4 Quadratic residue

In the end of last chapter, we have seen some simple examples of non-linear congruence. We shall continue the development of congruence theory. In this chapter we shall focus on the quadratic case in detail and prove Gauss's famous law of quadratic reciprocity. A general quadratic congruence is of the form

$$ax^2 + bx + c \equiv 0 \pmod{m} \text{ where } m \nmid a$$

But it can be reduced to the basic form

$$x^2 \equiv a \pmod{\text{m}}$$

Firstly, by using Chinese Remainder theorem, and the last subsection of chapter 3, we may reduce it to the case when $m = p$ is a prime. As $p \nmid a$, we have some $a'$ such that $2aa' \equiv 1 \pmod{p}$. Then we multiply both sides by $2a'$, we have

$$x^2 + 2b'x + c' \equiv 0 \pmod{p}$$

where $b' = a'b, c' = 2a'c$. Completing the square, we have

$$(x + b')^2 \equiv b'^2 - c' \pmod{p}$$

which is of form $x^2 \equiv a \pmod{p}$. Therefore, we shall focus on the congruence $x^2 \equiv a \pmod{p}$

## 4.1 Legendre symbol

**Definition 4.1.** *Let $(a, p) = 1$, we say $a$ is a* **quadratic residue** *mod $p$ if $a + p\mathbb{Z}$ is a square in $\mathbb{Z}/p\mathbb{Z}$. In other words, $\exists x$ such that $x^2 \equiv a$ (mod $p$)*

**Lemma 4.2.** *Let $p$ be an odd prime, then the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ has precisely $\frac{p-1}{2}$ quadratic residues.*

*Proof.* Pick a primitive root $g$ mod $p$. Then each element can be written as $g^i$ for some $i$. If $i$ is even, then $g^i$ is a quadratic residue. Conversely, suppose $g^i$ is a quadratic residue, then we have $g^i = g^{2j}$ for some $j$, and so $2j \equiv i \pmod{p-1}$. As $p - 1$ is even, so $i$ must be even. So $g^i$ is a quadratic residue if and only if $i$ is even, and there are $\frac{p-1}{2}$ of them. □

**Definition 4.3.** *Let $p$ be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } (a,p) = 1, a \text{ is a quadratic residue} \\ -1 & \text{if } (a,p) = 1, a \text{ is not a quadratic residue} \end{cases}$$

## 4.2 Euler's criterion

**Lemma 4.4. [Euler]** $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$ *(mod $p$)*

*Proof.* Write $P = \frac{p-1}{2}$. If $p|a$, then $(\frac{a}{p}) = 0 \equiv a^P \pmod{p}$.

If not, $a^{p-1} - 1 \equiv (a^P - 1)(a^P + 1) \equiv 0 \pmod{p}$. Then $p|a^{p-1} - 1 \Rightarrow p|a^P - 1$ or $p|a^P + 1$. Let $g$ be a primitive root mod $p$. WLOG, $a = g^k \pmod{p}$ for some $k \in \mathbb{Z}$. By Lemma 4.2, $(\frac{a}{p}) = 1$ if and only if $k$ is even.

Now if $k$ is even, then $a^P = g^{kP} = g^{\frac{k}{2}(p-1)} \equiv 1 \pmod{p}$. If $k$ is odd, then $a^P \equiv -1 \pmod{p}$. (This is because, if $x = a^P$, then $x^2 \equiv 1 \pmod{p}$ and as $p$ is prime, we can only have $x \equiv \pm 1 \pmod{p}$ ). Therefore, $(\frac{a}{p}) \equiv a^P \pmod{p}$. □

**Corollary 4.5.** $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

*Proof.* Apply Lemma 4.4 □

## 4.3 Gauss's lemma

It is often interesting in mathematics that an mathematical expression can be written in two different ways. Here is another expression of $(\frac{a}{p})$ by Gauss.

**Lemma 4.6.** **[Gauss]** *Let $p$ be an odd prime, $(a,p)=1$, write $P=\frac{p-1}{2}$. For $j=1,2,\dots P$, define $a_j \equiv j\cdot a \pmod p$ and $-\frac{p}{2}<a_j<\frac{p}{2}$. Let $\nu(a)$ be the number of $a_j$ with $a_j<0$. Then $(\frac{a}{p})=(-1)^{\nu(a)}$.*

*Proof.* Let $S=\{\pm 1,\dots \pm P\}$ and so $a_j \in S$. The subset given by $a_j : j=1,2\dots P$ consists of every integer $1,2\dots P$ with a unique sign.

Indeed, if $a_{j_1}=a_{j_2}$, then $j_1 a \equiv j_2 a \pmod p$, and so $j_1 \equiv j_2 \pmod p$, $j_1=j_2$. If $a_{j_1}=-a_{j_2}$, then $(j_1+j_2)a \equiv 0 \pmod p$ and so $j_1+j_2 \equiv 0 \pmod p$, but $j_1,j_2 \le P=\frac{p-1}{2}$, and so this is impossible. Hence

$$a\cdot 2a\dots Pa \equiv a_1\dots a_P \pmod p$$

is congruent to $1\cdot 2\dots P(-1)^{\nu(a)} \pmod p$. By Euler (Lemma 4.4), and we cancel $1\cdot 2\dots P$ on both sides, we conclude that $(\frac{a}{p} \equiv (-1)^{\nu(a)} \pmod p$, but both of them can only take values $\pm 1$, so we have $(\frac{a}{p})=(-1)^{\nu(a)}$. □

**Example 4.7.** *Let $a=2$, and let $p=8k+r, r=1,3,5,7$. We count the number of integers $x$ such that $\frac{p}{2}<2x<p$, i.e. $\frac{p}{4}<x<\frac{p}{2}$.*

1. *$r=1$. We have $x=2k+1,\dots 4k$, and so $\nu(2)=2k$.*

2. *$r=3$. We have $x=2k+1,\dots 4k+1$, and so $\nu(2)=2k+1$.*

3. *$r=5$. We have $x=2k+2,\dots 4k+2$, and so $\nu(2)=2k+1$.*

4. *$r=7$. We have $x=2k+2,\dots 4k+3$, and so $\nu(2)=2k+2$.*

*Now apply Lemma 4.7, so we conclude that*

$$\left(\frac{2}{p}\right)=\begin{cases} 1 & \text{if } p\equiv \pm 1 \pmod 8 \\ -1 & \text{if } p\equiv \pm 3 \pmod 8 \end{cases}$$

## 4.4 Law of quadratic reciprocity

The main theorem of the subsection is to prove the law of quadratic reciprocity, and we shall begin with the following idea.
Write $p=4am_p+r_p$, where $r_p$ satisfies $0<r_p<4a$, $(a,r_p)=1$.

**Theorem 4.8.** *Let $p_1$ and $p_2$ be any two odd primes with $(p_1,a)=(p_2,a)=1$ then: (i) If $p_1 \equiv p_2 \pmod{4a}$, we have $(\frac{a}{p_1})=(\frac{a}{p_2})$.*
*(ii) If $p_1 \equiv -p_2 \pmod{4a}$, then $(\frac{a}{p_1})=(\frac{a}{p_2})$.*

To prove this, we need:

**Lemma 4.9.** *Assume $\alpha,\beta \in \mathbb{R}, \alpha \le \beta, \alpha \notin \mathbb{Z}$. Then:*
*(i) The number of integers in $[\alpha,\beta]$ is $[\beta]-[\alpha]$.*
*(ii) If $n\in\mathbb{Z}$. $[n+\beta]=n+[\beta]$.*
*(iii) If $n_1,n_2$ are in $\mathbb{Z}$, $n_1\le n_2$, then the number of integers in $[\alpha,\beta]$ and in $[2n_1+\alpha,2n_2+\beta]$ have the same parity.*

*Proof.* (i) Since $\alpha \notin \mathbb{Z}.[\alpha]+1, \ldots [\beta]$ has $[\beta]-[\alpha]$ integers.
(ii) Let $\beta_1 = \beta - [\beta]$. Then $n+\beta = (n+[\beta])+\beta_1$, and so $[n+\beta] = n+[\beta]$.
(iii) The first interval has $[\beta]-[\alpha]$ integers, and the second one has $[\beta+2n_2]-[\alpha+2n_1] = [\beta]+2n_2-[\alpha]-2n_1$, by using the previous parts. Hence they have the same parity. □

Now we can prove Theorem 4.8:

*Proof.* Consider $a, 2a, \ldots Pa$, where $P = \frac{p-1}{2}$. Note that $Pa$ is the largest multiple of $a < \frac{pa}{2}$. The integers in the set $\{a, \ldots, Pa\}$ with a negative $a_j$ are those lying in the interval $[\frac{p}{2}, p], [\frac{3p}{2}, 2p] \ldots [(b-\frac{1}{2})p, bp]$. We write $p = 4m_p a + r_p$ and then $b = \frac{a}{2}$ if $a$ is even, and $b = \frac{a+1}{2}$ if $a$ is odd.

But the number of integers in the above intervals are precisely the number of integers in the interval

$$\left[\frac{p}{2a}, \frac{p}{a}\right], \ldots \left[\frac{(2b-1)p}{2a}, \frac{bp}{a}\right]$$

which is

$$\left[2m_p + \frac{r_p}{2a}, 4m_p + \frac{r_p}{a}\right], \ldots \left[2m_p(2b-1) + \frac{(2b-1)r_p}{2a}, 4m_p b + \frac{br_p}{a}\right]$$

As $(a, r_p) = 1$, so none of the above boundaries is integer. Apply Lemma 4.9, it has the same parity as

$$\left[\frac{r_p}{2a}, \frac{r_p}{a}\right] \ldots \left[\frac{(2b-1)r_p}{2a}, \frac{br_p}{a}\right]$$

Recall from Gauss's lemma, that $(\frac{a}{p}) = (-1)^{\nu(a)}$. So for part (i) of the theorem, if $p_1 \equiv p_2 \pmod{4a}$, i.e. $r_{p_1} = r_{p_2}$, then $(\frac{a}{p_1}) = (\frac{a}{p_2})$.

For (ii), $p_1 \equiv -p_2 \pmod{4a}$, so $r_{p_2} = 4a - r_{p_1}$. Substitute this into the expression, so consider

$$\left[2 - \frac{r_{p_1}}{2a}, 4 - \frac{r_{p_1}}{a}\right] \ldots \left[4b - 2 - \frac{(2b-1)r_{p_1}}{2a}, 4b - \frac{br_{p_1}}{a}\right]$$

If $\alpha \notin \mathbb{Z}$, then $[-\alpha] = -[\alpha] - 1$, so $[4 - \frac{r_{p_1}}{a}] - [2 - \frac{r_{p_1}}{2a}] = 2 - [\frac{r_{p_1}}{a}] + [\frac{r_{p_1}}{2a}]$ etc.

Therefore, $[\frac{p_i}{2a}, \frac{p_i}{a}], \ldots [\frac{(2b-1)p}{2a}, \frac{bp}{a}]$ have the same parity, and so we again have $(\frac{a}{p_1}) = (\frac{a}{p_2})$. □

**Theorem 4.10. [Law of quadratic reciprocity]** *Let $p, q$ be distinct odd primes, then $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. In particular, $(\frac{p}{q}) = (\frac{q}{p})$ when at least one of $p, q \equiv 1$ (mod 4), and $(\frac{p}{q}) = -(\frac{q}{p})$ if both $p, q \equiv 3$ (mod 4).*

*Proof.* We have two cases:

1. $p \equiv q \pmod{4}$. WLOG, let $p > q$. Then $p = q + 4a$ for some $a$, and then we write $p = 4am_p + r_p, q = 4am_q + r_q, r_p, r_q < 4a$, we have $4a(m_q+1) + r_q = 4am_p + r_p$. Hence $r_p = r_q$, and so $p \equiv q \pmod{4a}$. By Theorem 4.8(i), we have $(\frac{a}{p}) = (\frac{a}{q})$. Now

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$$

by Corollary 4.5.

Hence $(\frac{p}{q}) = (-1)^{\frac{p-1}{2}}(\frac{q}{p})$ when $p \equiv q \pmod{4}$, which is the same as $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

2. $p \not\equiv q \pmod 4$, then $p \equiv -q \pmod 4$. So we can write $p + q = 4a$ for some $a$, and so $p \equiv -q \pmod{4a}$, by Theorem 4.8(ii), we again have $(\frac{a}{p}) = (\frac{a}{q})$. Now

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right)$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right)$$

So we have $(\frac{q}{p}) = (\frac{q}{p})$ when $p \equiv -q \pmod 4$, i.e. at least one of them is 1 mod 4 and hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

Now the calculation of the Legendre symbol is much easier.

**Example 4.11.** $(\frac{7411}{9283}) = -(\frac{9283}{7411}) = -(\frac{1872}{7411})$

$1872 = 2^4 3^2$, *so we have* $-(\frac{13}{7411}) = -(\frac{7411}{13}) = -(\frac{1}{13}) = -1$.

## 4.5 Jacobi symbol

Let $n$ be any **odd** integer $> 1$, and write $n = q_1 q_2 \dots q_r$, where $q_i$ are prime but not necessarily distinct.

**Definition 4.12.** *If $a \in \mathbb{Z}$, the Jacobi symbol is defined as*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{q_i}\right)$$

**Remark 4.13.** *1. $(\frac{a}{n})$ only depends on $a + n\mathbb{Z}$ because if $a \equiv b \pmod n$, then $a \equiv b \pmod{p_i}$ $\forall i$.*

*2. $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$ by Corollary 4.5.*

*3. $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$ by definition.*

**Lemma 4.14.** $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}, (\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.

*Proof.* For the first identity, we shall apply Corollary 4.5 and check the fact that for any two odd integers $n_1, n_2$, we have $n_1 n_2 \equiv n_1 + n_2 - 1 \pmod 4$. This is because $(n_1 - 1)(n_2) - 1 \equiv 0 \pmod 4$. So that

$$\left(\frac{-1}{n_1}\right)\left(\frac{-1}{n_2}\right) = (-1)^{\frac{n_1-1}{2}}(-1)^{\frac{n_2-1}{2}} = (-1)^{\frac{n_1 n_2 - 1}{2}}$$

For the second identity, we have $({n_1}^2 - 1)({n_2}^2 - 1) \equiv 0 \pmod{16}$. Then we have ${n_1}^2{n_2}^2 - 1 \equiv {n_1}^2 + {n_2}^2 - 2 \pmod{16}$. Using Example 4.7, we have

$$\left(\frac{2}{n_1}\right)\left(\frac{2}{n_2}\right) = (-1)^{\frac{{n_1}^2-1}{8}}(-1)^{\frac{{n_1}^2-1}{8}} = (-1)^{\frac{{n_1}^2{n_2}^2-1}{8}}$$

□

**Theorem 4.15.** *If $m, n$ are odd positive integers. then*

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

*Proof.* The case when $(m, n) = 1$ is clear, as both sides are 0. So assume now $(m, n) = 1$. Let $m = p_1 \dots p_r, n = q_1 \dots q_s$, where $p_i, q_j$ are prime but not necessarily distinct. Now

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right) \text{ and } \left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)$$

Let $u$ be the number of $p_i$ which is congruent to 3 mod 4, and $v$ be the number of $q_j$ which is congruent to 3 mod 4. We know by Theorem 4.10, $(\frac{p_i}{q_j}) = -(\frac{q_j}{p_i})$ if and only if both $p_i, q_j \equiv 3 \pmod 4$, and we have $uv$ pairs of such $p_i, q_j$.

Therefore, $(\frac{m}{n}) = (\frac{n}{m})(-1)^{uv}$. Finally we check that the parity of $uv$ is the same as $\frac{n-1}{2}\frac{m-1}{2}$. This is because that each odd prime is either 1 or 3 mod 4, and so $u$ is odd if and only if $m \equiv 3 \pmod 4$. Similarly, $v$ is odd if and only if $n \equiv 3 \pmod 4$. Hence, they have the same parity and the result follows. □

**Remark 4.16.** *The definition of Jacobi symbol has nothing to do with quadratic residues. For example, let $n = 15$, then we can check that $x^2 \equiv 2 \pmod{15}$ is not soluble. But $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$.*

## 4.6 Kronecker symbol

**Definition 4.17.** *Let $d$ satisfy: $d \equiv 0$ or $1 \pmod 4$, and $d$ is not square. The Kronecker symbol $(\frac{d}{n})$ is defined when $n > 0$ by:*

*(i)* $(\frac{d}{n}) = 0$ *if* $(d, n) > 1$;

*(ii)* $(\frac{d}{1}) = 1$;

*(iii) If $d$ is odd, $(\frac{d}{2}) = (\frac{2}{|d|})$, a Jacobi symbol, so*

$$\left(\frac{d}{2}\right) = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 8 \\ -1 & \text{if } d \equiv 5 \pmod 8 \end{cases}$$

*(iv) If $n = \prod_{i=1}^{r} p_i$, then $(\frac{d}{n}) = \prod_{i=1}^{r}(\frac{d}{p_i})$*

*So it is a product of Legendre symbols, and the symbol $(\frac{d}{2})$ if $n$ is even.*

Here is an equivalent definition:

**Theorem 4.18.** *Let $n > 0$ and $(d, n) = 1$ with $d$ as above. Then (i) If $d$ is odd, we have $(\frac{d}{n}) = (\frac{n}{|d|})$, a Jacobi symbol.*
*(ii) If $d = 2^s t$, where $t$ is odd and $s > 0$, we have:*

$$(\tfrac{d}{n}) = (\tfrac{2}{n})^s(-1)^{\frac{(t-1)(n-1)}{4}}(\tfrac{n}{|t|})$$

*a product of Jacobi symbols.*

*Proof.* (i)Consider the case $d > 0, n = 2^u v$ where $v$ is odd. As $d$ is odd so $d \equiv 1 \pmod 4$, and so

$$\left(\frac{d}{n}\right) = \left(\frac{d}{2^u v}\right) = \left(\frac{d}{2}\right)^u \left(\frac{d}{v}\right) = \left(\frac{2}{d}\right)^u \left(\frac{v}{d}\right) = \left(\frac{n}{d}\right)$$

For the case $d < 0$, we use the fact that:

1. $(\frac{d}{2}) = (\frac{2}{|d|})$.

2. $(\frac{d}{v}) = (\frac{-1}{v})(\frac{-d}{v}) = (\frac{-1}{v})(\frac{|d|}{v})$.

3. $-d \equiv 3 \pmod 4$ and so $(\frac{-d}{v}) = (\frac{v}{d})(-1)^{\frac{v-1}{2}}$.

(ii) $d = 2^s t$, where $t$ is odd and $s > 0$, if $n$ is even, then $(d, n) > 1$ and so both sides are 0. So assume $n$ is odd and we have $(\frac{d}{n})$ is already a Jacobi symbol and so:

$$\left(\frac{d}{n}\right) = \left(\frac{2^s}{n}\right)\left(\frac{t}{n}\right)$$

By definition, as $n > 0$ and is odd, we have $(\frac{2^s}{n}) = (\frac{n}{2^s}) = (\frac{n}{2})^s = (\frac{2}{n})^s$. Then:
If $t > 0$, we have

$$\left(\frac{t}{n}\right) = (-1)^{\frac{t-1}{2}\frac{n-1}{2}}\left(\frac{n}{t}\right)$$

and so the result follows.
If $t < 0$, we have $t = -|t|$, and so

$$\left(\frac{t}{n}\right) = (-1)^{\frac{n-1}{2}}(-1)^{\frac{|t|-1}{2}\frac{n-1}{2}}\left(\frac{n}{|t|}\right)$$

Hence the result follows. □

**Theorem 4.19.** *If $m \equiv n \pmod{|d|}$, then $(\frac{d}{m}) = (\frac{d}{n})$.*

*Proof.* Assume $(m, n) = 1$, otherwise both sides are 0 and the result is trivial. If $d$ is odd, then use Theorem 4.18, we have

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right) = \left(\frac{n}{|d|}\right) = \left(\frac{d}{n}\right)$$

If $d$ is even, let $d = 2^s t$. Then we have

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^s (-1)^{\frac{x(m-1)}{2}}\left(\frac{m}{|t|}\right)$$

$$\left(\frac{d}{n}\right) = \left(\frac{2}{n}\right)^s (-1)^{\frac{x(n-1)}{2}}\left(\frac{n}{|t|}\right)$$

where $x = \frac{t-1}{2}$. Now we again we $(\frac{m}{|b|}) = (\frac{n}{|b|})$, and as $d \equiv 0 \pmod 4$, we have

$$(-1)^{\frac{x(m-1)}{2}} = (-1)^{\frac{x(n-1)}{2}}$$

and also

$$\left(\frac{2}{m}\right)^s = \left(\frac{2}{n}\right)^s$$

by Lemma 4.14. Note that we must have $s \geq 2$ as $d \equiv 0 \pmod 4$ and if $s \geq 2$, then $m \equiv n \pmod 4$. □

## 4.7 Pseudo prime

With the notion of quadratic residues, we are now able to introduce the concept of pseudo primes. Throughout the subsection, $N$ is odd.

**Definition 4.20.** *We say an integer $b$ is a base for $N$, if $(b, N) = 1$. Usually, we take $b \in \{1, 2, \ldots N-1\}$.*

**Definition 4.21.** *We say $N$ is a* **pseudo prime** *to the base $b$ if $b^{N-1} \equiv 1$ (mod $N$).*

**Remark 4.22.** *By Fermat's little theorem, $b^{p-1} \equiv 1$ (mod $p$) and so $p$ is a pseudo prime for every base.*

But if a number $N$ is a pseudo prime for every base $b$, $N$ needs not be a prime.

**Example 4.23.** *$N = 561 = 3 \cdot 10 \cdot 17$, $N - 1 = 560$, which is divisible by $2, 10, 16$. So let $b$ be a base of $561$, then $b^{560} \equiv 1$ (mod $3, 11, 17$) and so by Chinese Remainder theorem, $b^{561} \equiv 1$ (mod $561$). But clearly $561$ is not a prime.*

**Definition 4.24.** *We say an odd* **composite** *integer $n > 1$ is a* **Carmichael number**, *if $b^{N-1} \equiv 1$ (mod $N$) for every integer $(b, N) = 1$.*

Here is an interesting result of Carmichael number which we do not give the proof in this book.

**Theorem 4.25.** *There are infinitely many Carmichael number. Let $C(x)$ be the number of Carmichael number $< x$, then $c(x) > x^{\frac{2}{7}}$, where $x >> 0$.*

**Theorem 4.26.** *Assume $b$ is any integer $> 1$, then there exists infinitely many composite number $N$, such that $b^{N-1} \equiv 1$ (mod $N$).*

*Proof.* Take any prime $p$ which satisfies: $p > 2$, $(p, b) = 1$ and $(p, b^2 - 1) = 1$. Let $N = \frac{b^{2p}-1}{b^2-1}$. Clearly, $N$ is an positive integer. We firstly check that $N$ is composite. We can write $N$ as:

$$N = \frac{b^p - 1}{b - 1} \frac{b^p + 1}{b + 1}$$

and both are integers greater than 1, and so $N$ is composite. Then we have $b^p \equiv b \pmod{p}$ by Fermat's little theorem, and so $b^{2p} \equiv b^2 \pmod{p}$. As we have chosen $(p, b^2 - 1) = 1$, so that $b^2 - 1 \nmid p$, and so

$$N - 1 = \frac{b^{2p} - b^2}{b^2 - 1} \equiv 0 \pmod{p}$$

and so $p | N - 1$. Now

$$N = \frac{b^{2p} - 1}{b^2 - 1} = b^{2p-2} + \ldots b^2 + 1$$

we have $p$ terms in the summation and as $p - 1$ is even so $b^{2p-2} + \ldots b^2$ must be even. So $N$ is odd and $N - 1$ is even. Let $N - 1 = 2pm$. Then

$$b^{2p} - 1 = (b^2 - 1)N$$

Thus,

$$b^{2p} \equiv 1 \pmod{N} \text{ and so } b^{N-1} \equiv b^{(2p)m} \equiv 1 \pmod{N}$$

Thus, as we have infinitely many $p$ which satisfies the condition at the beginning, so we can construct infinitely many such $N$. □

**Definition 4.27.** *We say $N$ is an* **Euler pseudo prime** *to the base $b$, if*

$$b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \ (mod\ N)$$

**Lemma 4.28.** *Assume $N$ is prime and $b$ is any base, $(b, N) = 1$. Write $N - 1 = 2^s t$, where $s \geq 1, t$ is odd. Then either $b^t \equiv 1$ (mod $N$) or $\exists r$ with $0 \leq r < s$ such that $b^{2^r t} \equiv -1$ (mod $N$).*

*Proof.* If $b^t \equiv 1 \pmod N$, then we have the first case. If not, we have $b^t \not\equiv 1 \pmod N$. But $b^{2^s t} \equiv 1 \pmod N$ by Fermat's little theorem. Then $\exists k$ such that $k$ is the largest integer that $b^{2^k t} \not\equiv 1 \pmod N$. So $b^{2^{k+1} t} \equiv 1 \pmod N$, i.e. $(b^{2^k t})^2 \equiv 1 \pmod N$. As $N$ is prime, so we have at most two solutions, and so we must have $b^{2^k t} \equiv -1 \pmod N$, which is the second case. □

**Definition 4.29.** *Assume $(b, N) = 1$. We say $N$ is a* **strong pseudo prime** *if either $b^t \equiv 1$ (mod $N$) or $\exists r$ with $0 \leq r < s$, such that $b^{2^r t} \equiv -1$ (mod $N$), where $N - 1 = 2^s t$.*

**Definition 4.30.** $S(N) = \{b : 1 \leq b < N, (b, N) = 1, N$ *is a strong pseudo prime to the base* $b\}$

Clearly $card(S(N)) \leq \phi(N)$, and by Lemma 4.28, equality holds when $N$ is a prime.

**Theorem 4.31.** [**Mercer**] *Assume $N$ is an odd integer $> 9$, then*

$$card(S(N)) \leq \frac{1}{4}\phi(N)$$

We shall prove several lemmas before we prove the theorem.

**Definition 4.32.** *Let $u(N)$ denote the largest integer such that $2^{u(N)}$ divides $p - 1$ for* **every** *prime divisor $p$ of $N$. Let $U(N) = \{b : 1 \leq b \leq N, (b, N) = 1$ and $b^{2^{u(N)-1} t} \equiv \pm 1$ mod $N\}$*

**Lemma 4.33.** *$S(N) \subset U(N)$.*

*Proof.* Take $b \in S(N)$. If $b^t \equiv 1 \pmod N$, then clearly

$$b^{2^{u(N)-1} t} \equiv 1 \pmod N$$

and so $b \in U(N)$.

Now assume $b^{2^r t} \equiv -1 \pmod N$, for some $0 \leq r < s$. Take any prime $p|N$. Define $k_p =$ order of $b$ in $(\mathbb{Z}/p\mathbb{Z})^*$. As

$$b^{2^{r+1} t} = (b^{2^r t})^2 \equiv 1 \pmod N\}$$

we have, $b^{2^{r+1} t} \equiv 1 \pmod p$. So $k_p | 2^{r+1} t$, and $k_p \nmid 2^r t$. Hence $k_p$ must take the factor $2^{r+1}$.

Then we can write $k_p = 2^{r+1} k_p'$, by Fermat's little theorem, we have $k_p | p - 1$, and so $2^{r+1} | p - 1$, and so $r + 1 \leq u(N)$. Now we have two cases.

(i) If $r + 1 = u(N)$, then we have $b^{2^{u(N)-1} t} \equiv -1 \pmod N$ because $u(N) - 1 = r$ and so $b \in U(N)$.

(ii) If $r + 1 < u(N)$, and so $u(N) - 1 \geq r + 1$. So $b^{2^{u(N)-1} t} \equiv 1 \pmod N$ and so again $b \in U(N)$.

Hence $S(N) \subset U(N)$. □

**Definition 4.34.** *Let $w(N) =$ number of distinct prime factors of $N$.*

**Theorem 4.35.** $card(U(N)) = 2 \cdot 2^{(u(N)-1)w(N)} \prod_{p\ prime | N} (t, p - 1)$

*Proof.* Define $m = 2^{u(N)-1}t$. We must count the number of $b$ mod $N$ satisfying either $x^m \equiv 1 \pmod N$ or $x^m \equiv -1 \pmod N$. Let $N = {p_1}^{j_1} \dots {p_k}^{j_k}$, where $j_i \geq 1$, and $p_i$ distinct prime. So $w(N) = k$.

For $x^m \equiv 1 \pmod N$. By Chinese Remainder theorem, we count the solutions to $x^m \equiv 1 \pmod{{p_i}^{j_i}}$ for each $i$. We know that $(\mathbb{Z})/p^j\mathbb{Z})^*$ is cyclic. So let $g$ be the generator. Consider that if $(g^i)^m = 1$, and as the order of the group is $p^{j-1}(p-1)$, so $im = kp^{j-1}(p-1)$ for some $k$, then we have exactly $d$ solutions, where $d = (m, p^{j-1}(p-1))$. But $p|N, (2t, N) = 1$ so that $(m, p^{j-1}) = 1$ and so we have $(m, p^{j-1}(p-1) = (m, p-1)$. But $2^{u(N)}|p-1$, so $(m, p-1) = 2^{u(N)-1}(t, p-1)$. Thus for each $p_i$, we have these solutions, and so in total, using Chinese Remainder theorem, we have

$$(2^{u(N)-1})^{w(N)} \prod_{p \text{ prime}|N} (t, p-1)$$

For $x^m \equiv -1 \pmod N$. We consider the solutions to $x^{2m} \equiv 1 \pmod{{p_i}^{j_i}}$ for each $i$, then exclude those solutions which also satisfy $x^m \equiv 1 \pmod{{p_i}^{j_i}}$. This is using $p^j|(x^m-1)(x^m+1) \Rightarrow p^j|x^m-1$ or $p|x^m+1$, because $p$ is prime. Then we run through the same argument as above, we shall get the number of solutions to $x^m \equiv -1 \pmod N$ is also

$$(2^{u(N)-1})^{w(N)} \prod_{p \text{ prime}|N} (t, p-1)$$

Hence the result follows by combining both parts. □

**Corollary 4.36.** *If $N$ is composite and $N \geq 9$, then $card(U(N)) \leq \frac{1}{4}\phi(N)$*

*Proof.* Let $\delta(N) = \frac{\phi(N)}{card(U(N))}$, and we can write

$$\phi(N) = \prod_{p \text{ prime}|N} p^{j-1}(p-1)$$

By Theorem 4.35, we have

$$\delta(N) = \frac{1}{2}\frac{\prod_{p|N} p^{j-1}(p-1)}{\prod_{p|N} 2^{u(N)-1}(t, p-1)} = \frac{1}{2}\prod_{p^j||N} \frac{p^{j-1}(p-1)}{2^{u(N)-1}(t, p-1)}$$

where $p^j||N$ means $p^j$ exactly divides $N$, i.e. $p^{j+1} \nmid N$.

If $w(N) \geq 2$ and $j \geq 2$ for some $p|N$, then $\delta(N) \geq 6$, and so $\delta(N) \geq 4$, because $\frac{p-1}{2^{u(N)-1}} \geq 2$ and $p \geq 3$ as $p$ must be odd prime. So it is $\geq \frac{1}{2}2^2 \cdot 3 = 6$. Similarly, if $w(N) \geq 3$ then $\delta(N) \geq 2 \cdot 2 = 4$. Hence the result follows.

So we only need to deal with some other cases.

1. $w(N) = 2, N = pq$, where $p, q$ distinct prime, and WLOG, assume $p < q$.

$$\delta(N) = \frac{1}{2}\frac{(p-1)(q-1)}{2^{u(N)-1}(t, p-1)2^{u(N)-1}(t, q-1)}$$

where $2^{u(N)}|p-1, q-1$.

If $2^{u(N)+1}|q-1$, then $\frac{q-1}{2^{u(N)-1}(t,q-1)} \geq 4$ and so the result follows. If not, we have $2^{u(N)}||q-1$, but

$$N - 1 = pq - 1 \equiv p - 1 \pmod{q-1}$$

So $2^{u(N)}|N-1$. But $q-1 \nmid N-1$, so there must be some odd factor $r|q-1$ but $r \nmid N-1$. $r \geq 3$, and so $\frac{q-1}{(t,q-1)} \geq r \geq 3$ and again $\delta(N) \geq 6$. Hence the result follows.

2. $N = p^j$ for some $j \geq 2$, because $N$ is composite. Then

$$\delta(N) = \frac{p^{j-1}(p-1)}{2^{u(N)-1}(t, p-1)} \geq p^{j-1}$$

$p$ is odd so $p \geq 3$. Either $p = 3$, then $j \geq 3$ because we assume that $N \geq 9$; Or $p \geq 4$. But in both cases we have $\delta(N) \geq 4$.

Combining all these cases, we have proved the assertion. □

Finally, to prove Theorem 4.31, we simply apply Corollary 4.36 and Lemma 4.33.

## 4.8 Exercises

1. Determine the primes $p$ for which 5 is quadratic residue (mod $p$).

2. Let $p$ be a prime such that $p \equiv 1 \pmod 4$. Show that the sum of quadratic residues in the interval $[1, p-1]$ is equal to the sum of quadratic non-residues in the interval.

3. Show that if $p$ is an odd prime then the product $P$ of all the quadratic residues mod $p$ satisfies

$$P \equiv (-1)^{\frac{1}{2}(p+1)} \text{ (mod p)}$$

4. Show that, for any integer $d$ and any odd prime $p$, then number of solutions of the congruence $x^2 \equiv d \pmod p$ is $1 + (\frac{d}{p})$.

5. Show that if $p$ is an odd prime, then the number of quadratic residues mod $p$ is equal to the quadratic non-residues. Evaluate

$$\sum_{a=1}^{p-2} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)$$

6. Show that if $q$ is a prime, $p > 3$ with $p \equiv 3 \pmod 4$ such that $2p + 1$ is also a prime number, then $2^p - 1$ is composite.

7. Let $N$ be a positive odd integer and assume that $N$ is divisible by a square of a prime number $p$. Prove that there exists an integer $z$ such that $z^p \equiv 1 \pmod N$ but $z \not\equiv 1 \pmod N$. Hence prove that there exists an integer $a$ with $(a, n) = 1$ such that the congruence

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod n$$

does not hold. Show further that this congruence fails to hold for at least half of all relatively prime residue classes modulo $N$.

8. Show that an integer $a$ is a square if and only if the congruence

$$x^2 \equiv a \pmod{p}$$

is soluble for every prime $p$.

9. Let $f(x) = ax^2 + bx + c$, where $a, b, c$ are integers, and let $p$ be an odd prime that does not divide $a$. Further let $d = b^2 - 4ac$. Show that, if $p$ does not divide $d$, then

$$\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) = -\left(\frac{a}{p}\right)$$

Evaluate the sum when $p$ divides $d$.
(Hint: You may use the fact that when $p \nmid d$, the number of solutions to the congruence

$$x^2 - y^2 \equiv d \pmod{p}$$

is $p - 1$. We shall prove this later by Jacobi sum).

10. If $p$ is a prime $> 3$ with $p \equiv 3 \pmod{8}$, prove that

$$\prod_{r=1}^{\frac{p-1}{2}} (\frac{r}{p})$$

is always divisible by 3.

11. Using the Kronecker symbol show that $(\frac{d}{|d|-1}) = sgn(d)$ where $sgn$ is the sign function ($sgn(d) = 1$ if $d > 0$ and $sgn(d) = -1$ if $d < 0$). Deduce that if $m > 0, n > 0$, and $m + n \equiv 0 \pmod{|d|}$ then $(\frac{d}{n}) = (\frac{d}{m})sgn(d)$.

12. Let $p$ be a prime number such that $2p - 1$ is also prime. Show that $N = p(2p - 1)$ is a pseudo prime for precisely half of all bases.

13. (i) Let $p$ be a prime $> 5$. Prove that $N = \frac{4^p+1}{5}$ is always a composite integer. Show further that $N$ is always a strong pseudo prime to the base 2.
(ii) Now Let $M$ be an odd integer greater than 1 such that $M$ is a pseudo prime to the base 2. Prove that $2^M - 1$ is always a strong pseudo prime to the base 2.

⋆14. This is a short, but tricky proof of quadratic reciprocity which uses Chinese Remainder theorem in place of Gauss's Lemma.

(i) Suppose $p$ and $q$ are distinct odd primes. By considering the group $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ and its subgroup $U = \{(1, 1), (p - 1, q - 1)\}$, show that

$$K = \{(i, j) : i = 1, \ldots p - 1; j = 1, \ldots \frac{q-1}{2}\}$$

is a complete system of coset representatives for $U$ in $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, and the product of all elements of $K$ equals

$$\Pi = ((p - 1)!^{\frac{q-1}{2}}, (q - 1)!^{\frac{p-1}{2}}(-1)^{\frac{(p-1)(q-1)}{4}}).$$

(ii) Secondly consider the set

$$L = \{(t_p, t_q) : t = 1, \dots \frac{pq-1}{2} \text{ and } (t, pq) = 1\}$$

where $t_p \equiv t \pmod{p}$ and $0 \leq t_p < p$, and $t_q$ is defined similarly. Using the ring version of Chinese Remainder theorem, show that this is also a complete system of coset representatives for $U$ in $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. Now calculate the product $\Phi$ of all elements of $L$ as follows; show that the first entry of $\Phi$ is:

$$\frac{1 \dots (p-1)(p+1) \dots (2p-1) \dots (\frac{(q-1)p}{2} + 1) \dots (\frac{(q-1)p}{2} + \frac{p-1}{2})}{q \cdot 2q \dots \cdot \frac{(p-1)q}{2}}$$

which is congruent to $\frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \mod p$. Repeat this calculation for the second entry and hence show that

$$\Phi = ((p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right))$$

(iii) Prove law of reciprocity by nothing that $\Pi = \Phi$ in the quotient group of $U$.

## 4.9 Hint and Solutions

1. We want to find $p$ such that $(\frac{5}{p}) = 1$. By law of reciprocity, we have $(\frac{5}{p}) = (\frac{p}{5})$. And so we have $p \equiv 1, 4 \pmod{5}$. In fact we have $p \equiv \pm 1 \pmod{10}$ because $p$ is prime.

2. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$. So we know that $-1$ is a square mod $p$. Hence we have

$$\left(\frac{p-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$$

Hence, we can pair each $a$ with $p - a$, and so the sum of quadratic residues and non-residues are both $\frac{p(p-1)}{4}$.

3. Observe that if $ab \equiv 1 \pmod{p}$, then as

$$1 = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$(a, p), (b, p) = 1$, so we must have $(\frac{a}{p}) = (\frac{b}{p})$. So we can pair each quadratic residue with its inverse. The only elements whose inverse is itself are 1 and $-1$. And use

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

to achieve the result.

4. If $p|d$, then we have $x \equiv 0 \pmod{p}$ and so we have one solution. If $d$ is not a quadratic residue, then we have no solution. Finally, if $d$ is a quadratic residue, then we have at most two solutions by Lagrange's theorem. We need to check it has precisely two solutions. But this is clear as if $x^2 \equiv d \pmod{p}$, so is $(p - x)^2$.

5. Use question 5, we know that each quadratic residues $d$ corresponds to two solutions, and so the number of quadratic residues is $\frac{p-1}{2}$, which is equal to the number of non-residues. Hence we have

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$$

and so

$$\sum_{a=2}^{p-1}\left(\frac{a}{p}\right)=-1$$

Now

$$\sum_{a=1}^{p-2}\left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{a^2(1+a^{-1})}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{1+a^{-1}}{p}\right)$$

as $a^{-1}$ are all different and $p-1$ has itself inverse, so $1+a^{-1}$ runs through $\{2,\dots p-1\}$ as 0 has no inverse. Thus we have

$$\sum_{a=1}^{p-2}\left(\frac{1+a^{-1}}{p}\right)=\sum_{a=2}^{p-1}\left(\frac{a}{p}\right)=-1$$

6. $p\equiv 3 \pmod 4$ and so $2p+1\equiv 7 \pmod 8$. Hence 2 is a quadratic residue mod $2p+1$. So we may write $2\equiv x^2 \pmod{2p+1}$. By Fermat's little theorem, $x^{2p}\equiv 1 \pmod{2p+1}$ because $2p+1$ is prime. Therefore, $2^p\equiv 1 \pmod{2p+1}$, and so $2^p-1$ is divisible by $2p+1$. Now as $p>3$, $2p+1<2^p-1$, so it is a proper factor and so $2^p-1$ is composite.

7. $N$ is odd, so we use Chinese Remainder theorem (ring version) to write

$$(\mathbb{Z}/N\mathbb{Z})^*\cong\prod_i(\mathbb{Z}/{p_i}^{j_i}\mathbb{Z})^*$$

WLOG we can assume that $p=p_1$, and so $j_1\geq 2$ as $p^2|N$. Now pick a primitive root $g$ of $(\mathbb{Z}/{p_1}^{j_1}\mathbb{Z})^*$, and let $h=g^{p^{j-2}(p-1)}$, so $h$ has order $p$ in the group and is non-identity. Then, pick $z$ to be the element corresponding to

$$(h,e,\dots,e)$$

in the ring and so this element $z$ gives $z^p\equiv 1 \pmod N$ but $z\not\equiv 1 \pmod N$.

Now pick $a$ to be the $z$ above. Suppose the congruence holds, then we square both sides, we have

$$a^{N-1}\equiv 1 \pmod N$$

But $(p,N-1)=1$ and so we have $x,y$ such that $px+y(N-1)=1$. Therefore, we have

$$a=a^{px+y(N-1)}\equiv 1 \pmod N$$

which contradicts the way we chose $a$. So the congruence does not hold for this $a$. Finally, observe that $a^{\frac{N-1}{2}}b^{\frac{N-1}{2}}=(ab)^{\frac{N-1}{2}}$, and $(\frac{ab}{N})=(\frac{a}{N})(\frac{b}{N})$. So if we have no element for which the congruence holds, then we are done. If we have one for which the congruence holds, say $b$, then the congruence does not hold for $ab$, and hence the congruence does not hold for at least half of all relatively prime residue classes modulo $N$.

8. One way is clear, if $a$ is a square, then we simply take $x$ to be $\sqrt{a}$ and so the congruence is soluble.

   Conversely, suppose $a$ is not a square, then we got to prove that there exists a prime $p$ such that $(\frac{a}{p}) = -1$ (In fact we can find infinitely many, the proof of this is in a similar manner). To do this, we firstly find some odd integer $n$ such that $(\frac{a}{n}) = -1$.

   We firstly deal with the case when $a$ is positive. Let $a = b^2 r$ where $r$ is square free and let $r = p_1 p_2 \dots p_k$, where $p_i$ are distinct primes. Then $(\frac{a}{n}) = (\frac{r}{n})$. Now pick $n$ which satisfies:

$$n \equiv 1 \pmod 4$$

$$n \equiv 1 \pmod{p_i}$$

$$n \equiv z \pmod{p_1}$$

   where $i \geq 2, (\frac{z}{p_1}) = -1$. Such $n$ exists by Chinese Remainder theorem.

   Then by law of reciprocity $(\frac{r}{n}) = (\frac{n}{r})$ and

$$\left(\frac{n}{r}\right) = \prod_{i=1}^{k} \left(\frac{n}{p_i}\right) = -1$$

   Hence $(\frac{a}{n}) = -1$ and so there must exists a prime factor $p$ of $n$ such that $(\frac{a}{p}) = -1$.

   Now suppose $a$ is negative, and so let $a = -b^2 r$, where $r > 0$ and is square free. Again let $r = p_1 p_2 \dots p_k$, where $p_i$ are distinct primes.Then $(\frac{a}{n}) = (\frac{-r}{n})$, and we pick $n$ satisfying the same condition as above. Use $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$, but $\frac{n-1}{2}$ is even as $n \equiv 1 \pmod 4$. Hence we again have $(\frac{a}{n}) = -1$ and so there must exists a prime factor $p$ of $n$ such that $(\frac{a}{p}) = -1$.

9. Let $p \nmid d$. So we can simplify the sum as

$$\left(\frac{a}{p}\right) \sum_{x=1}^{p} \left(\frac{(x + b(2a)^{-1})^2 - d(4a)^{-1}}{p}\right)$$

   by completing the square, and $b(2a)^{-1}$ is just a linear transformation, and so it is the same as

$$\left(\frac{a}{p}\right) \sum_{y=1}^{p} \left(\frac{y^2 + e}{p}\right)$$

   where $e = -d(4a)^{-1}$ which is not divisible by $p$.

   Now use question 4 that the number of solutions to the congruence

$$x^2 \equiv y^2 + e \pmod p$$

   is $1 + (\frac{y^2+e}{p})$ for each fixed $y$, and so in total we have

$$\sum_{y=1}^{p} \left(1 + \left(\frac{y^2 + e}{p}\right)\right)$$

   solutions. Use the hint, we know this is equal to $p - 1$. So we conclude that

$$\sum_{y=1}^{p} \left(\frac{y^2 + e}{p}\right) = -1$$

and so the result follows.

For the case when $p|d$, the above expression is simplified to

$$\sum_{y=1}^{p}\left(\frac{y^2}{p}\right)=\sum_{y=1}^{p-1}1=p-1$$

and so it is $(p-1)(\frac{a}{p})$.

10. Consider $\sum_{r=1}^{p-1}(\frac{r}{p})r$. There are two ways to sum this.

$$\sum_{r=1}^{p-1}r\left(\frac{r}{p}\right)=\sum_{r=1}^{\frac{p-1}{2}}(2r)\left(\frac{2r}{p}\right)+\sum_{r=1}^{\frac{p-1}{2}}(p-2r)\left(\frac{p-2r}{p}\right)$$

or we have

$$\sum_{r=1}^{p-1}r\left(\frac{r}{p}\right)=\sum_{r=1}^{p-1}r\left(\frac{r}{p}\right)+\sum r=1^{\frac{p-1}{2}}(p-r)\left(\frac{p-r}{p}\right)$$

As $p\equiv 3 \pmod 8$ we have $(\frac{-1}{p})=(\frac{2}{p})=-1$. So we can equate the above two and we have LHS:

$$\sum_{r=1}^{\frac{p-1}{2}}(-2r)\left(\frac{r}{p}\right)+\sum_{r=1}^{\frac{p-1}{2}}\left\{p\left(\frac{r}{p}\right)-2r\left(\frac{r}{p}\right)\right\}$$

RHS:

$$\sum_{r=1}^{\frac{p-1}{2}}r\left(\frac{r}{p}\right)+\sum_{r=1}^{\frac{p-1}{2}}\left\{(-p)\left(\frac{r}{p}\right)+r\left(\frac{r}{p}\right)\right\}$$

And so rearrange the equation we have

$$\sum_{r=1}^{\frac{p-1}{2}}2p\left(\frac{r}{p}\right)=\sum_{r=1}^{\frac{p-1}{2}}6r\left(\frac{r}{p}\right)$$

and so

$$p\sum_{r=1}^{\frac{p-1}{2}}\left(\frac{r}{p}\right)=3\sum_{r=1}^{\frac{p-1}{2}}r\left(\frac{r}{p}\right)$$

As $p>3$, so we have

$$3|\sum_{r=1}^{\frac{p-1}{2}}\left(\frac{r}{p}\right)$$

11. If $d$ is odd then apply Lemma 4.18, we have $(\frac{d}{|d|-1})=(\frac{|d|-1}{|d|})$, and so it gives $(\frac{-1}{|d|})$, if $d>0$, by definition of Kronecker symbol, $d\equiv 1 \pmod 4$, and so it is 1. If $d<0$, then $|d|\equiv 3 \pmod 4$, and so it is $-1$, which gives the result.

Now let $d$ be even, $d=2^st$. Then we have

$$\left(\frac{d}{|d|-1}\right)=\left(\frac{2^s}{2^st-1}\right)\left(\frac{t}{2^st-1}\right)$$

By definition of Kronecker symbol, $d\equiv 0 \pmod 4$, and so $s\geq 2$. If $s=2$ or $s$ is even, then $(\frac{2^s}{2^st-1})=1$. if not $2^st-1\equiv 7 \pmod 8$, and so $(\frac{2^s}{2^st-1})=(\frac{2}{2^st-1})=1$.

Then for $(\frac{t}{2^s t-1})$, then if $d > 0$, i.e. $t > 0$, by law of reciprocity we have, as $2^s t - 1 \equiv 3 \pmod 4$, that

$$\left(\frac{t}{2^s t-1}\right) = (-1)^{\frac{t-1}{2}} \left(\frac{2^s t-1}{t}\right)$$

which is

$$(-1)^{\frac{t-1}{2}}(-1)^{\frac{t-1}{2}} = 1$$

If $d < 0$, i.e. $t < 0$, we have $(\frac{-t}{1-2^s t})$ which is $-1$. So $(\frac{d}{|d|-1}) = sgn(d)$.

For the second part, use Theorem 4.19, so we know that

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m|d|-m}\right)$$

as $n \equiv m|d| - m \pmod{|d|}$. Now

$$\left(\frac{d}{m|d|-m}\right) = \left(\frac{d}{m}\right)\left(\frac{d}{|d|-1}\right)$$

and the result follows by applying the first part.

12. $\phi(N) = \phi(p)\phi(2p-1) = 2(p-1)^2$. We need to check that $N$ is pseudo prime for precisely $(p-1)^2$ bases. We have

$$b^{N-1} \equiv 1 \pmod N \iff b^{N-1} \equiv 1 \pmod{p, 2p-1}$$

$N - 1 = p(2p-1) - 1 = (2p+1)(p-1)$. By Fermat's little theorem:

$$b^{2p-1} \equiv 1 \pmod{2p-1} \text{ and } b^{p-1} \equiv 1 \pmod p$$

Now as $p - 1|N - 1$, so $b^{N-1} \equiv 1 \pmod p$ for every base $b$, and this has $p - 1$ solutions.

For $2p - 1$, $b^{N-1} = b^{p(2p-2)+(p-1)} \equiv b^{p-1} \pmod{2p-1}$, so we want $b^{p-1} \equiv 1 \pmod{2p-1}$. But $b^{2p-2} = (b^{p-1})^2 \equiv 1 \pmod{2p-1}$ and so we have precisely $\frac{\phi(2p-1)}{2} = p - 1$ solutions satisfying this. So use Chinese Remainder theorem, we have in total $(p-1)^2$ bases which satisfy $b^{N-1} \equiv 1 \pmod N$.

13. (i) $4^p + 1 = 2^{2p} + 1 = (2^p+1)^2 - 2^{p+1}$. $p$ is a prime $> 5$ and so is odd, so $2^{p+1} = (2^{\frac{p+1}{2}})^2$ and so

$$4^p + 1 = (2^p+1)^2 - (2^{\frac{p+1}{2}})^2 = (2^p + 1 + 2^{\frac{p+1}{2}})(2^p + 1 - 2^{\frac{p+1}{2}})$$

Clearly as $p > 5$, both factors are greater than 1 and is not 5. Hence $\frac{4^p+1}{5}$ is composite.

Let $N - 1 = 2^s t$. We want to show that

$$\text{Either } 2^t \equiv 1 \pmod N \text{ or } 2^{2^r t} \equiv -1 \pmod N$$

for some $0 \le r < s$. $N - 1 = 4\frac{4^{p-1}}{5}$ and so $s = 2, t = \frac{4^{p-1}}{5}$. But $5N = 4^p + 1 = 2^{2p} + 1$, so we have

$$2^{2p} \equiv -1 \pmod N$$

Also as $p > 5$, so $4^{p-1} - 1 \equiv 0 \pmod p$ and so $p|t$. Let $t = mp$ with $m$ odd. Therefore we have

$$2^{2t} = 2^{2mp} = (2^{2p})^m \equiv (-1)^m \equiv -1 \pmod N$$

And so there exists such $r$, $r = 1$ and $0 \le r < 2$ as required.

(ii) Let $N = 2^M - 1$, and $N - 1 = 2t$, where $t = 2^{M-1} - 1$. So $2^M \equiv 1 \pmod N$. Also as $M$ is a pseudo prime to the base 2, so

$$2^{M-1} \equiv 1 \pmod M$$

So that $M|2^{M-1} - 1$ and so $2^{2^{M-1}-1} = 2^t \equiv 1 \pmod N$. Hence the result follows.

14. (i) Suppose $(a,b)U = (c,d)U$, then $(ac^{-1}, bd^{-1}) \in U$. If $ac^{-1} = 1$ then $bd^{-1} = 1$ and so $a = c, b = d$. If $ac^{-1} = p-1 =$ then $bd^{-1} = p-1$, and so $b+d \equiv 0 \pmod{p}$ which is impossible. Hence we know that these cosets are all different and there are $\frac{(p-1)(q-1)}{2}$ of them, and so they form a complete system of coset representatives for $U$. The product is:

$$\prod_{i=1}^{p-1}\prod_{j=1}^{\frac{p-1}{2}}(i,j) = \left((p-1)!^{\frac{q-1}{2}}, (\frac{q-1}{2})!^{p-1}\right)$$

We can write $(\frac{q-1}{2})!^{p-1}$ as $(\frac{q-1}{2})!^{2\frac{p-1}{2}}$ and for each $k > \frac{q-1}{2}, k \equiv -(p-k) \pmod{p}$. Hence we have

$$\left((\frac{q-1}{2})!^{p-1}\right) = (\frac{q-1}{2})!^{\frac{p-1}{2}}(\frac{q-1}{2})!^{\frac{p-1}{2}} = (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

(ii) As $(p,q) = 1$, so we have, by Chinese Remainder theorem,

$$(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \cong (\mathbb{Z}/pq\mathbb{Z})^*$$

where the isomorphism is sending $t \in (\mathbb{Z}/pq\mathbb{Z})^*$ to $(t_p, t_q)$ in $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, with $t_p, t_q$ defined in the question.

$U$ corresponds to $\{1, pq-1\}$ in $(\mathbb{Z}/pq\mathbb{Z})^*$ because $pq - 1 \equiv p-1 \pmod{p}$ and is $q-1 \pmod{q}$. And so $\{1, 2, \ldots \frac{pq-1}{2}\}$ is a complete system of coset representatives. Now reduce it to $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, it is just $L$.

Then it is clear that the first entry is the product of all these, except those multiples of $p$ and $q$, and so we get the required product.

Now the numerator is congruence to $(p-1)!^{\frac{q-1}{2}}(\frac{p-1}{2})! \bmod p$ (Remember the last term terminates at a multiple of $p$ plus $\frac{p-1}{2}$.

The denominator is congruent to $(\frac{p-1}{2})!q^{\frac{p-1}{2}} \bmod p$, and so together we have $\frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \bmod p$.

Recall from Lemma 4.4 (Euler's criterion) that $(\frac{q}{p}) \equiv q^{\frac{p-1}{2}} \pmod{p}$, and $(\frac{q}{p})^{-1} = (\frac{q}{p})$ so we have shown the first entry is $(p-1)!^{\frac{q-1}{2}}(\frac{q}{p})$. As the product is symmetric in $p$ and $q$, so in the second entry we just swap $p$ and $q$.

(iii)As we proved that both $\Pi$ and $\Phi$ form complete system of coset representatives and so their products must be the same in the quotient group of $U$. This is because, as both are just product of the representatives, so it means that

$$\Phi U = \Pi U$$

Then $\Phi = \pm\Pi$, but in either case we have that the proportion of the first entry is equal to that of the second entry. Therefore, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

which proves the law of reciprocity.

# 5 Continued fraction

## 5.1 Basic properties

We have seen many rational approximations of the irrational $\pi$. For example, $\frac{22}{7}, \frac{355}{113}$, and in fact these are in some sense the best approximations of $\pi$. In this chapter we are going to introduce the concept of continued fraction to construct these magic fractions which are going to make very good approximations of many irrationals. We begin with the following definition:

**Definition 5.1.** *A continued fraction is an expression of the form*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

*with either a finite or infinite number of entries $a_i$,where $a_i$ are positive integers. We shall use the notation $[a_0, a_1, a_2, \ldots]$ for this expression.*

*Formally, to obtain the continued fraction for a real number $\alpha$. let $a_0 = [\alpha]$. If $a_0 = \alpha$ then we stop and $\alpha = [a_0]$. If not, then $\alpha = a_0 + \frac{1}{\alpha_1}, \alpha_1 > 1$ and let $a_1 = [\alpha_1]$. If $a_1 = [\alpha_1]$ then we stop and $\alpha = [a_0, a_1]$, and if not, we continue as in the above procedure. We call these $a_i$ the* **partial quotients** *of $\alpha$.*

**Lemma 5.2.** *The series $a_i$ is finite if and only if $\alpha$ is rational.*

*Proof.* If $a_i$ is finite then clearly $\alpha$ is rational. Conversely, if $\alpha$ is rational, let $\alpha = \frac{a}{b}$, and WLOG, $b > 0$, $(a, b) = 1$.

Let $a = ba_0 + r_1$, and so $\alpha = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\alpha_1}$. Now as $r_1, b > 0$ then we can apply Euclidean algorithm to $b$ and $r_1$, $b = r_1 a_1 + r_2$ etc. and then the partial quotients $a_i$ come from the sequence $r_i$, but as Euclidean algorithm terminates, so the series of partial quotients must be finite. □

It is not of great interest to find the continued fraction of $\alpha$ when it is rational, thus we shall assume from now on that $\alpha$ is irrational.

**Example 5.3.** $\pi = [3, 7, 15, 1, \ldots]$
$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, \ldots]$
$\sqrt[3]{2} = [1, 3, 1, 5, 1, 1, 4, \ldots]$
$\sqrt{41} = [6, 2, 2, 1, 2, 2, 2, 1, \ldots]$

**Definition 5.4.** *The $n^{th}$* **convergent** *of $\alpha$, $\frac{p_n}{q_n}$ is defined as:*
$p_0 = a_0, p_1 = a_1 a_0 + 1$, *and* $p_n = a_n p_{n-1} + p_{n-2}$ $\forall n \geq 2$.
$q_0 = 1, p_1 = a_1$, *and* $q_n = a_n q_{n-1} + q_{n-2}$ $\forall n \geq 2$.

For example, $\alpha = \pi$, we have $p_0 = 3, q_0 = 1$, $p_1 = 22, q_1 = 7$, $p_2 = 333, q_2 = 106$, $p_3 = 355, q_3 = 113$. And we might intuitively guess that these rational approximations come from the convergent.

**Lemma 5.5.** *For each $\beta > 0$, and for each $n \geq 2$, we have that*

$$[a_0, \ldots a_{n-1}, \beta] = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}}$$

*Proof.* We use induction on $n$. By definition of $p_i, q_i$, it is easily checked that

$$[a_0, a_1, \beta] = \frac{\beta p_1 + p_0}{\beta q_1 + q_0}$$

and so it is true for $n = 2$. Suppose it is true for $n \geq 2$, that

$$[a_0, \dots a_{n-1}, \beta] = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}}$$

Then as

$$[a_0, \dots a_n, \beta] = [a_0, \dots a_{n-1}, a_n + \frac{1}{\beta}]$$

by definition, and $\beta > 0$. So we use induction that

$$[a_0, \dots a_n, \beta] = \frac{(a_n + \frac{1}{\beta})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{\beta})q_{n-1} + q_{n-2}} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

as $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$. □

**Corollary 5.6.** *$\forall n \geq 0$, we have*

$$[a_0, \dots a_n] = \frac{p_n}{q_n}$$

*Proof.* Check for the case when $n = 0, 1$, and then put $\beta = a_n$ in Lemma 5.5 □

**Remark 5.7.** *Sometimes in some other book, reader might find that the definition of convergent is given by Corollary 5.6. This is an equivalent definition as we can deduce our definition by Corollary 5.6*

**Lemma 5.8.** *Corollary 5.6 is an equivalent definition of convergent.*

*Proof.* Let $\alpha = [a_0, \dots a_n$ and $\frac{r_k}{s_k} = [a_k, \dots a_n]$. Thus we have

$$\frac{r_k}{s_k} = a_k + \frac{1}{\frac{r_{k+1}}{s_{k+1}}}$$

Equate both sides and let $r_k = a_k r_k + s_{k+1}, s_k = r_{k+1}$. Then

$$\begin{pmatrix} r_k \\ s_k \end{pmatrix} = \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{k+1} \\ s_{k+1} \end{pmatrix}$$

and so

$$\begin{pmatrix} r_0 \\ s_0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n \\ 1 \end{pmatrix}$$

Now by definition $p_n = r_0, q_n = s_0$, so that

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} p_{n+1} \\ q_{n+1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n+1} \\ 1 \end{pmatrix}$$

And so

$$\begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix}$$

which gives

$$\begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix}$$

Compare the first column, and the result follows. □

**Lemma 5.9.** *$\forall n \geq 1$, we have*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

*and in particular, $p_n, q_n$ are coprime.*

*Proof.* We use induction on $n$. The case $n = 1$ follows immediately from the definition. Suppose it is true for $n - 1$, that

$$p_{n-1} q_{n-2} - q_{n-1} p_{n-2} = (-1)^{n-2}$$

then we have

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= q_{n-1}(a_n p_{n-1} + p_{n-2}) - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= (-1)^{n-1} \end{aligned}$$

Hence it holds for all $n \geq 1$. □

**Lemma 5.10.** *$\forall n \geq 2$, we have*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$

*Proof.* Expand $p_n$ and $q_n$ by definition so we have

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= q_{n-2}(a_n p_{n-1} + p_{n-2}) - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= a_n(-1)^n \end{aligned}$$

where we applied Lemma 5.9 and use $(-1)^{n-2} = (-1)^n$. □

**Lemma 5.11.** *The sequence $\frac{p_{2n}}{q_{2n}}$ is strictly increasing for $n \geq 0$ while the sequence $\frac{p_{2n-1}}{q_{2n-1}}$ is strictly decreasing.*

*Proof.* We have, by Lemma 5.10, that

$$\frac{p_{2n}}{q_{2n}} - \frac{p_{2n-2}}{q_{2n-2}} = (-1)^{2n} \frac{a_{2n}}{q_{2n} q_{2n-2}} > 0$$

and similarly for the other one. □

**Theorem 5.12.** *Assume that $\alpha$ is irrational. Then $\forall n \geq 0$, we have*

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

*Proof.* Use Lemma 5.5, we have

$$\alpha = [a_0, \ldots, a_n, \alpha_{n+1}] = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

and so we have

$$\begin{aligned} \alpha - \frac{p_n}{q_n} &= \frac{-p_n q_{n-1} + q_n p_{n-1}}{q_n(\alpha_{n+1} q_n + q_{n-1})} \\ &= \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1})} \end{aligned}$$

and so

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\ &< \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} \\ &\leq \frac{1}{q_n q_{n+1}} \\ &< \frac{1}{q_n^2}\end{aligned}$$

where we used $a_{n+1} \leq \alpha_{n+1}$ and $a_{n+1} \geq 1$. □

**Theorem 5.13.** *Assume $\alpha$ is irrational. Let $p, q$ be any two integers such that $0 < q < q_{n+1}$, $(n \geq 0)$ then*

$$|q\alpha - p| \geq |q_n\alpha - p_n|$$

*Proof.* Since we know that $p_n q_{n+1} - p_{n+1}q_n = \pm 1$ so we can find integers $u, v$ such that

$$p = up_n + vp_{n+1}$$

$$q = uq_n + vq_{n+1}$$

Since $0 < q < q_{n+1}$, we have $u \neq 0$.

Suppose $v = 0$, then $\frac{p}{q} = \frac{p_n}{q_n}$, but $(p_n, q_n) = 1$ and so equality holds in the theorem. Hence we assume $v \neq 0$, as $0 < q < q_{n+1}$, $u$ and $v$ must have opposite sign. By Lemma 5.21 and we know that $\frac{p_n}{q_n} \to \alpha$ by definition, so that $\alpha - \frac{p_n}{q_n}$ and $\alpha - \frac{p_{n+1}}{q_{n+1}}$ must have opposite sign and so combing these two, we have that $u(q_n\alpha - p_n)$ and $v(q_{n+1}\alpha - p_{n+1})$ have the same sign. Therefore,

$$|q\alpha - p| = |u(q_n(\alpha - p_n) + v(q_{n+1} - p_{n+1})|$$

and so

$$|q\alpha - p| \geq |u|\,|q_n\alpha - p_n| \geq |q_n\alpha - p_n|$$

because $u \neq 0$. □

**Corollary 5.14.** *Assume $\alpha$ is irrational. Let $0 < q$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \left|\alpha - \frac{p_n}{q_n}\right|$$

*for some $n$, then $q > q_n$.*

*Proof.* Assume $q \leq q_n < q_{n+1}$, then we have

$$\begin{aligned}q\left|\alpha - \frac{p}{q}\right| &= |q\alpha - p| \\ &\geq |q_n\alpha - p_n| \\ &= q_n\left|\alpha - \frac{p_n}{q_n}\right|\end{aligned}$$

by using Theorem 5.13. So we have

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{q_n}{q}\left|\alpha - \frac{p_n}{q_n}\right| \geq \left|\alpha - \frac{p_n}{q_n}\right|$$

which is a contradiction. □

**Theorem 5.15.** *Assume $\alpha$ is irrational, then at least one of any two successive convergents satisfy*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

*Moreover, if $\frac{p}{q}$ is arbitrary rational number with $q > 0$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

*then we must have $\frac{p}{q} = \frac{p_n}{q_n}$ for some $n$. i.e, this says that the convergents are the best approximation of $\alpha$.*

*Proof.* Take any two $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$. Then by Theorem 5.12 we have

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

and also $\alpha - \frac{p_{n+1}}{q_{n+1}}$, $\alpha - \frac{p_n}{q_n}$ have opposite sign. So we have

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$

Apply AM-GM inequality, this is $< \frac{1}{2{q_n}^2} + \frac{1}{2{q_{n+1}}^2}$ And so one of them must satisfy

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

Moreover, assume now $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$. We choose $n$ such that $q_n \leq q < q_{n+1}$ (Because $q_n$ is unbounded). Apply triangle inequality we have,

$$\left|\frac{pq_n - qp_n}{qq_n}\right| = \left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{p}{q}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q}\left|q\alpha - p\right| + \frac{1}{q_n}\left|q_n\alpha - p_n\right|$$

As $q < q_{n+1}$, by Theorem 5.13, we have $|q\alpha - p| \geq |q_n\alpha - p_n|$. Hence

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left(\frac{1}{q} + \frac{1}{q_n}\right)|q\alpha - p| < \frac{1}{2q^2} + \frac{1}{2qq_n}$$

by assumption.

Since $q \geq q_n$, so

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{1}{2qq_n} + \frac{1}{2qq_n} = \frac{1}{qq_n}$$

Hence we have

$$\left|\frac{pq_n - qp_n}{qq_n}\right| < \frac{1}{qq_n}$$

and so

$$|pq_n - qp_n| < 1$$

But this is an integer and so it must be 0. Therefore, we have

$$\frac{p}{q} = \frac{p_n}{q_n}$$

□

The theorem above also says that there are infinitely many convergents which satisfy

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{2q_n^2}$$

But the fraction $\frac{1}{2}$ is not best possible and we can in fact improve this by:

**Theorem 5.16.** **[Hurwitz]** *There are infinitely many convergents of an irrational $\alpha$ which satisfies*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{b_n^2\sqrt{5}}$$

The proof is similar to Theorem 5.15 and is left an exercise to the reader (see Exercise 4 of this chapter). But the fraction $\sqrt{5}$ in the theorem can not be improved as we have the following theorem:

**Theorem 5.17.** *There exists a real number $\gamma$ with the property: if $\theta > \sqrt{5}$ then the inequality*

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q^2\theta}$$

*has only finitely many rational solutions $\frac{p}{q}$.*

*Proof.* Set $\gamma = \frac{-1+\sqrt{5}}{2}$ and suppose the solutions to the above inequality exist with arbitrarily large $q$. We may rewrite the above as:

$$\frac{-1+\sqrt{5}}{2} = \frac{p}{q} + \frac{\delta}{p^2} \quad \text{where } |\delta| < \frac{1}{\theta} < \frac{1}{\sqrt{5}}$$

That is

$$-\frac{\delta}{q} + \frac{\sqrt{5}}{2}q = \frac{q}{2} + p$$

Squaring both sides we have

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = p^2 + pq - q^2$$

Now, as $-1 < -\frac{\delta}{5} < 1$, we have for sufficiently large $q$,

$$-1 < \frac{\delta^2}{q^2} - \frac{\delta}{\sqrt{5}} < 1$$

and hence $p^2 + pq - q^2 = 0$ as it is an integer between $-1$ and 1. Multiply both sides by 4 and we have $(2p+q)^2 = 5q^2$ which is impossible as LHS is a perfect square, but RHS is not. Therefore, we can only have finitely many such $q$ satisfying the inequality, and for each $q$, it is clear that we only have finitely many such $p$. □

The continued fraction of $\frac{-1+\sqrt{5}}{2}$ is $[0, 1, 1, \ldots]$. In fact, any real number whose continued fraction is **eventually** all ones can be used for $\gamma$ in Theorem 5.17. Further, it can be shown that, for all numbers not of this type, we may replace $\sqrt{5}$ in Theorem 5.16 by $\sqrt{8}$ and this is the best possible when $\gamma = \sqrt{2}$ or is equal to any number whose continued fraction is eventually all twos. An analogue to Theorem 5.17 is the following: it can be shown that there are uncountably many real numbers $\beta$ such that the inequality

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{3b^2}$$

has infinitely many rational solutions $\frac{p}{q}$, but only finitely many solutions if the number 3 is replaced by any large number.

## 5.2 Pell's equation

The Diophantine equation $x^2 - dy^2 = 1$, usually known as Pell's equation, is of considerable importance in number theory. The main applications are in quadratic form theory and in the unit problem. The case when $d$ is a square only have trivial solution and so throughout the subsection we shall assume that $d > 0$ and is not a square.

**Theorem 5.18.** *Any solution to*

$$x^2 - dy^2 = 1$$

*for $x, y > 0$ must have $x = p_n, y = q_n$ for some $n$, where $\frac{p_n}{q_n}$ is convergent of $\sqrt{d}$.*

*Proof.* As $d$ is square free, so $\sqrt{d}$ is irrational, and $d > 1$. Let $x = p, y = q$ be a solution to $x^2 - dy^2 = 1$. We have

$$p^2 - dq^2 = (p - \sqrt{d}q)(p + \sqrt{d}q) = 1$$

and as $p + \sqrt{d}q > 0$, we must have $p - \sqrt{d}q > 0$. So $p > q\sqrt{d}$. Then

$$0 < p - q\sqrt{d} = \frac{1}{p + q\sqrt{d}} < \frac{1}{2q\sqrt{d}}$$

and so

$$\left|\frac{p}{q} - \sqrt{d}\right| < \frac{1}{2q^2\sqrt{d}} < \frac{1}{2q^2}$$

and so $\frac{p}{q} = \frac{p_n}{q_n}$ for some $n$ by Theorem 5.15. □

The converse of the theorem above is the following, which proves the existence of the solution:

**Theorem 5.19.** *The Pell's equation $x^2 - dy^2 = 1$ is soluble in integers $x$ and $y$.*

Before we prove the theorem, we shall introduce a very important concept

**Definition 5.20.** *We say $\alpha$ has a period continued fraction if there exists $\omega > 0$ such that $a_{n+\omega} = a_n$ for all $n \geq b_0$ for some $n_0$.*

For example, $\sqrt{43} = [6, \underbrace{1, 1, 3, 1, 5, , 3, 1, 1, 1, 2}_{\omega=10, n_0=1}, 1, 1 \ldots]$

**Definition 5.21.** *We say an irrational number $\alpha$ is a quadratic irrationality if there exists integers $a, b, c$, not all 0 with $a\alpha^2 + b\alpha + c = 0$*

**Theorem 5.22.** **[Lagrange]** *Assume that $\alpha$ is irrational. Then $\alpha$ is a quadratic irrationality if and only if $\alpha$ has a periodic continued fraction.*

*Proof.* We introduce the notation $[a_0, \ldots a_{n-1}, a_n^*]$ for $[a_0, \ldots a_{n-1}, a_n, a_n \ldots]$ Suppose that $\alpha$ has a periodic continued fraction.

$$\alpha = [a_0, \ldots a_{n-1}, a_n^*, \ldots a_{n+m-1}^*]$$

Then we have, by Lemma 5.5

$$\alpha = [a_0, \ldots a_{n-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + qn - 2}$$

and as $[a_n, \ldots a_{n+m-1}]$ is repeated

$$\alpha_n = [a_n, \ldots a_{n+m-1}, \alpha_n] = \frac{\alpha_n p'_{m-1} + p'_{m-2}}{\alpha_n q'_{m-1} + q'_{m-2}}$$

where $\frac{p'_m}{q'_m}$ is the $m^{th}$ convergent of $\alpha_n$. From the second equality we have a quadratic equation for $\alpha_n$ as $p'_m, q'_m$ are integers. Then from the first equality we can write $\alpha_n$ in the form $\frac{a\alpha+b}{c\alpha+d}$. Substitute this into the quadratic equation of $\alpha_n$ and clear the denominators, and we have a quadratic equation for $\alpha$ after rearrange the equation.

Conversely, suppose $\alpha$ is positive and $\alpha = \alpha_0 = \frac{c_0+\sqrt{d}}{e_0}$, where $c_0, d_0$ and $e_0$ are integers and $d_0$ is not a square, $e_0 \neq 0$. We may rewrite $\alpha_0$ as $\frac{c_0 e_0+\sqrt{de_0{}^2}}{e_0{}^2}$ if necessary so that we have $e_0|d - c_0{}^2$. By definition of continued fraction of $\alpha$, we can define $c_i$ and $e_i$ by:

$$c_{i+1} = a_i e_i - c_i,\ e_{i+1} = \frac{d - c_{i+1}{}^2}{e_i}$$

It is a simple matter to check by induction that $c_i$ and $e_i$ are integers and that $e_i \neq 0$ and $e_i|d - c_i{}^2$, using the equations

$$e_{i+1} = \frac{d - c_{i+1}{}^2}{e_i} = \frac{d - c_i{}^2}{e_i} + 2a_i c_i - a_i{}^2 e_i$$

And so we conclude that

$$\alpha_i = \frac{c_i + \sqrt{d}}{e_i}$$

by induction using the equation $\alpha_i - a_i = \frac{1}{\alpha_{i+1}}$ and above.

Further, let $\alpha'_i = \frac{c_i-\sqrt{d}}{e_i}$. By Lemma 5.5, and rearrange the equation, we have

$$\alpha_i = -\frac{\alpha_0 q_{i-2} - p_{i-2}}{\alpha_0 q_{i-1} - p_{i-1}}$$

and $\alpha'_i$ is the conjugate of $\alpha_i$, so taking conjugate, we have

$$\alpha'_i = -\frac{\alpha'_0 q_{i-2} - p_{i-2}}{\alpha'_0 q_{i-1} - p_{i-1}}$$

which we may rewrite as

$$\alpha'_i = -\frac{q_{i-2}}{q_{i-1}} \left( \frac{\alpha'_0 - \frac{p_{i-2}}{q_{i-2}}}{\alpha'_0 - \frac{p_{i-1}}{q_{i-1}}} \right)$$

As the convergent tends to $\alpha$ as $i$ tends to infinity, and so the term in parentheses tends to 1, and so there is an $n_0$ such that $\alpha'_n < 0$ if $n > n_0$. Hence $\alpha_n - \alpha'_n = \frac{2\sqrt{d}}{e_n} > 0$, and thus $e_n > 0$ if $n > n_0$. Also as $e_n$ is integer, so that

$$e_n \leq e_n e_{m+1} = d - c_{n+1}^2 < d$$

and

$$c_{n+1}^2 < c_{n+1}^2 + e_n e_{n+1} = d$$

Hence if $n > n_0$ there can be only finitely many distinct pairs $\{c_n, e_n\}$ as they are integers bounded by $|d|$, and so there is a $k > 0$, such that if $n > n_0$, $a_{n+k} = a_n$ because each pair $\{c_n, e_n\}$ determines a unique $\alpha_i$, and each $\alpha_i$ determines $a_i$. Then use $\alpha_i - a_i = \frac{1}{\alpha_{i+1}}$, we have $a_{n+t} = a_{n+k+t}$ where $t \geq 0$, and the result follows. □

Now we can prove Theorem 5.19.

*Proof.* Let $\alpha = \sqrt{d}$, by Theorem 5.22 we have $\alpha_n = \frac{c_n+\sqrt{d}}{e_n}$ and so by Lemma 5.5 we have

$$\sqrt{d} = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} = \frac{(c_n + \sqrt{d})p_{n-1} + e_n p_{n-2}}{(c_n + \sqrt{d})q_{n-1} + e_n q_{n-2}}$$

Equating irrational and rational parts, we have

$$q_{n-1}c_n + qn - 2e_n = p_{n-1} \text{ and } p_{n-1}c_n + p_{n-2}e_n = dq_{n-1}$$

and multiplying by $p_{n-1}$ and $q_{n-1}$ respectively, and subtract, we have

$$p_{n-1}^2 - dq_{n-1}^2 = (p_{n-1}q_{n-2} - p_{n-2}q_{n-1})e_n = (-1)^n e_n$$

by Lemma 5.9.

Now let $k$ be the period of the continued fraction of $\sqrt{d}$, and $t$ be any positive integer. Then by Theorem 5.22 we have

$$\frac{c_n + \sqrt{d}}{e_n} = \frac{c_{n+kt} + \sqrt{d}}{e_{n+kt}}$$

. As in the proof of Theorem 5.22, we have $e_n \leq d$ and so will repeat. Then there is a non-zero integer $e$ such that

$$u^2 - dv^2 = e$$

has infinitely many solutions $\{u, v\}$. (This is from the equation $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n e_n$ above as $p_n, q_n$ are monotonically increasing. We may assume that $u$ and $v$ are positive and we partition this set of solutions into classes by: $\{u, v\}$ is in the same set as $\{u', v'\}$ if and only if $u \equiv u'$ and $v \equiv v'$ (mod $|e|$). At least one of these classes has two distinct (in fact infinitely many as the pair $(u, v)$ (mod $|e|$) is finite) members $\{u_1, v_1\}$ and $\{u_2, v_2\}$. Now let $x$ and $y$ be given by:

$$x = \frac{u_1u_2 - dv_1v_2}{e}, y = \frac{u_1v_2 - u_2v_1}{e}$$

We claim that $x$ and $y$ are integers and they are solutions to the original Pell's equation. Indeed, we have

$$u_1u_2 - dv_1v_2 \equiv u_1^2 - d_1^2 \equiv 0 \text{ (mod } |e|)$$

$$0 \neq u_1v_2 - u_2v_1 \equiv 0 \text{ (mod } |e|)$$

and

$$e^2(x^2 - dy^2) = (u_1^2 - dv_1^2)(u_2^2 - dv_2^2) = e^2$$

and so we have

$$x^2 - dy^2 = 1$$

□

**Theorem 5.23.** *Suppose $\{x_0, y_0\}$ is the solution of Pell's equation with $x_0, y_0$ positive and $D = x_0 + y_0\sqrt{d}$ minimal, then $\{x, y\}$ is a solution of the Pell's equation if and only if $x$ and $y$ satisfy*

$$x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$$

*for some integer $n$ which is positive, negative, or zero. We call such solution $\{x_0, y_0\}$ the fundamental solution.*

*Proof.* Suppose that $\{x_1, y_1\}$ and $\{x_2, y_2\}$ are solutions of the Pell's equation and $x_3, y_3$ are given by

$$x_3 + y_3\sqrt{d} = (x_1 + y\sqrt{d})(x_2 + y\sqrt{d})$$

then $\{x_3, y_3\}$ is a solution of Pell's equation because

$$x_3^2 - dy_3^2 = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1$$

Then, note that if $n = 0$ we have $x = 1, y = 0$, the trivial solution.
Also

$$(x_1 + y_1\sqrt{d})^{-1} = \frac{x_1 - y_1\sqrt{d}}{x_1^2 - dy_1^2} = x_1 + (-y_1)\sqrt{d}$$

It follows by considering conjugate that if $\{x_1, y_1\}$ is a solution and $x, y$ are given by

$$x + y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n$$

then $\{x, y\}$ is also a solution for every integer $n$.

Now suppose $\{t, u\}$ is a solution with $t, u > 0$. Choose $m$ to satisfy

$$D^m \leq t + u\sqrt{d} < D^{m+1}$$

that is

$$1 \leq (t + u\sqrt{d})D^{-m} < D$$

By the argument above, if $(t + u\sqrt{d})D^{-m} = X + Y\sqrt{d}$, then $\{X, Y\}$ is a solution with $X, Y$ non-negative, because we have $1 \leq X + Y\sqrt{d} < D$ and $0 < X - Y\sqrt{d} \leq 1$ (as $X^2 - dY^2 = 1$) and so $2X \geq 1$ and $2Y\sqrt{d} \geq 0$. It follows by minimality of $D$ that $X = 1$ and $Y = 0$. Hence $t + u\sqrt{d} = D^m$ and the proof is complete. □

Let's briefly discuss the relation between continued fraction and Pell's equation. If $k$ is the period of continued fraction of $\sqrt{d}$ and $k$ is even, then $\{a_{k-1}, b_{k-1}\}$ is a solution of Pell's equation (See in the proof of Theorem 5.19, we had $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n e_n$); and using a similar argument, it follows that equation $x^2 - dy^2 = -1$ is insoluble. If $k$ is odd the situation is slightly different: $\{p_{k-1}, q_{k-1}\}$ is a solution to the equation $x^2 - dy^2 = -1$, and $\{p_{2k-1}, q_{2k-1}\}$ is a solution of $x^2 - dy^2 = 1$. We shall left these as an exercise (see Exercise 10 of this chapter).

As an example, consider $d = 13$ and $d = 14$. In the first case we have $\sqrt{13} = [3, 1^*, 1, 1, 1, 6^*]$ with period 5. $[3, 1, 1, 1, 1] = \frac{18}{5}$ and we can check that $x = 18, y = 5$ is a solution of $x^2 - 13y^2 = -1$. And as $649 + 180\sqrt{3} = (18 + 5\sqrt{13})^2$, $\{649, 180\}$ is a solution of Pell's equation. Now for the second case $\sqrt{14} = [3, 1^*, 2, 1, 6^*]$ with period 4, and $[3, 1, 2, 1] = \frac{15}{4}$. Hence $\{15, 4\}$ is a solution to the Pell's equation. The equation $x^2 - 14^2 = -1$ is not soluble by considering the equation modulo 7 ($-1$ is not a square mod 7).

**Theorem 5.24.** *If the equation*

$$u^2 - dv^2 = m$$

*has a solution $\{u, v\}$, then it has infinitely many solutions, at least one of which satisfies*

$$0 < u < \sqrt{\frac{(x_0 + 1)|m|}{2}}$$

*where $\{x_0, y_0\}$ is the fundamental solution of Pell's equation in Theorem 5.23.*

*Proof.* Consider the case when $m > 0$; a virtually identical argument can be used if $m < 0$. Assume that the equation is soluble and all solutions $\{u, v\}$ are such that

$$u \geq \sqrt{\frac{(x_0 + 1)m}{2}}$$

Choose $u$ and $v$ so that $\{u, v\}$ is a solution with $u, v > 0$, and $u$ is minimal. Define $u_1$ and $v_1$ by

$$u_1 + v_1\sqrt{d} = (u + v\sqrt{d})(x_0 - y_0\sqrt{d})$$

As above $\{u_1, v_1\}$ is also a solution by considering the conjugate, and use

$$x_0^2 - dy_0^2 = 1 \text{ and } 1 - \frac{m}{u^2} = d\frac{v^2}{u^2}$$

Now $u_1 = ux_0 - dvy_0 > u$ so divide both sides by $u$, we have

$$1 < x_0 - \frac{dvy_0}{u}$$

We write $\frac{dvy_0}{y}$ as $(\sqrt{d}y_0)\frac{\sqrt{d}v}{u}$ and use:

$$\sqrt{d}y_0 = \sqrt{x_0^2 - 1}$$

and

$$\frac{\sqrt{d}v}{u} = \sqrt{1 - \frac{m^2}{u^2}}$$

so we have

$$1 < x_0 - \sqrt{x_0^2 - 1}\sqrt{1 - \frac{m^2}{u^2}}$$

Rearrange and square both sides, we have

$$1 - \frac{m^2}{u^2} < \frac{x_0 - 1}{x_0 + 1} = 1 - \frac{2}{x_0 + 1}$$

by noticing that $x_0 \geq 1$. Rearrange again, we have

$$(x_0 + 1)m^2 > 2u^2$$

and hence the result follows. □

## 5.3 A set of real numbers modulo 1

The last topic of this section is Chebysheve's theorem, which concerns the distribution of $(n\alpha)$ for $n \geq 1$ and $\alpha$ any fixed irrational number, where $(a)$ denotes the fractional part of $a$. We shall prove that the set $\{(n\alpha) : n = 1, 2, \ldots\}$ is dense in $[0, 1]$ and is uniformly distributed.

**Theorem 5.25.** *If $\alpha$ is an irrational number $\beta$ is a real number, then there are infinitely many pairs of integers $x$ and $y$ such that*

$$|x\alpha - y - \beta| < \frac{3}{x}$$

*Proof.* By Theorem 5.16 (Hurwitz), there are infinitely many integers $a$ and $b$ satisfying $(a, b) = 1$ and

$$\alpha = \frac{a}{b} + \frac{\gamma}{b}$$

for some $\gamma$ with $|\gamma| < 1$ (In Theorem 5.16 we took $\gamma$ to be $\frac{1}{\sqrt{5}}$). Also let $c$ be the integer closet to $b\beta$, so

$$\beta = \frac{c}{b} + \frac{\delta}{2b}$$

where $|\delta| \leq 1$. Further, as $(a, b) = 1$, integers $x$ and $y$ can be found to satisfy $ax - by = c$ and $b \leq 2x < 3b$. Using these, we have

$$\begin{aligned} |x\alpha - y - \beta| &= \left|\frac{xa}{b} + \frac{x\gamma}{b^2} - y - \frac{c}{b} - \frac{\delta}{2b}\right| \\ &= \left|\frac{x\gamma}{b^2} - \frac{\delta}{2b}\right| \\ &< \frac{x}{b^2} + \frac{1}{2b} \\ &< \frac{9}{4x} + \frac{3}{4x} = \frac{3}{x} \end{aligned}$$

as $b > \frac{2x}{3}$. The result follows because $x \geq \frac{b}{2}$ and $b$ can be arbitrarily large. □

**Definition 5.26.** *Let $R = \{\alpha_0, \alpha_1, \ldots\}$ be a set of real numbers in the unit interval and let $0 \leq \beta_1 < \beta_2 \leq 1$. Define $T$ by: $T(n, \beta_1, \beta_2)$ equals the number of elements $\alpha_i$ of $R$ satisfying $i \leq n$ and $\beta_1 \leq \alpha_i \leq \beta_2$. $R$ is said to be* **uniformly distributed** *in the unit interval if and only if*

$$\lim_{n\to\infty} \frac{T(n, \beta_1, \beta_2)}{n} = \beta_2 - \beta_1$$

*holds for all $\beta_1$ and $\beta_2$.*

**Theorem 5.27.** *If $\alpha$ is irrational, then the set*

$$S = \{(n\alpha) : n = 1, 2, \ldots\}$$

*is uniformly distributed in the unit interval.*

*Proof.* By Theorem 5.16 we have infinitely many $a$ and $b$ with $b > 0$ such that

$$\alpha = \frac{a}{b} + \frac{\delta}{b^2}, |\delta| < 1, (a, b) = 1$$

For $b$ to be chosen, let $J_j$ be the set $\{jb + k : k = 0, 1, \ldots b - 1\}$ and consider the set $K_j = \{(i\alpha) : i \in J_j\}$. We have

$$\alpha(jb + k) = \left(\frac{a}{b} + \frac{\delta}{b^2}\right)(jb + k) = ja + \frac{ka + j\delta}{b} + \frac{k\delta}{b^2}$$

and so as $k < b$

$$(\alpha(jb + k)) = \left(\frac{ka + [j\delta]}{b} + \frac{\gamma}{b}\right)$$

where $|\gamma| < 2$ (We can write $\gamma$ explicitly as $\frac{\frac{k\delta}{b} + (j\delta)}{b}$). $[j\delta]$ is independent of $k$ and so, as $k$ ranges over a complete system of residues modulo $b$, $ka + [jb]$ ranges over this system. It follows that

$$K_j = \left\{\left(\frac{k + \gamma}{b}\right) : k = 0, 1, \ldots b - 1\right\}$$

Let $[\beta_1, \beta_2]$ be a subinterval of the unit interval and let $b$ be sufficiently large so that we can choose integers $v$ and $w$ to satisfy

$$v - 1 < b\beta_1 \leq v < w \leq b\beta_2 < w + 1$$

Let the number of elements of $K_j$ in the interval $[\beta_1, \beta_2]$ be denoted by $W_j$. The $W_j$ is bounded below by the number of elements of $K_j$ in the interval $(\frac{v}{b}, \frac{w}{b})$; that is, use the above conclusion for $K_j$, $W_j$ is bounded below by the number of integers $k$ which satisfy

$$v \leq k + \gamma \leq w$$

It follows that $W_j \geq w - v - 4$ as $|\gamma| < 2$.
Similarly by considering

$$v - 1 \leq k + \gamma \leq w + 1$$

$W_j \leq w - v + 6$; note that these bounds are independent of $j$.

Let $n = rb + s$ where $0 \leq s < b$ and let $T(n, \beta_1, \beta_2)$ be the number of reals $(x\alpha)$ in the interval $[\beta_1, \beta_2]$ for $x \leq n$. Then by definition of $J_j$, we have

$$\sum_{j=0}^{r-1} W_j \leq T(n, \beta_1, \beta_2) \leq \sum_{j=0}^{r} W_j$$

and use the inequalities above,we have

$$r(w-v-4) \leq T(n,\beta_1,\beta_2) \leq (r+1)(w-v+6)$$

But provided $r > 1$, use $w - v + 2 \geq b(\beta_2 - \beta_1)$ and $s < b$

$$r(w-v-4) = \frac{n-s}{b}(w-v-4) \geq n(\beta_2-\beta_1) - \frac{6n}{b} - (w-v-4)$$

and by $w - v \leq b(\beta_2 - \beta_1)$ and $s \geq 0$,

$$(r+1)(w-v+6) \leq \left(\frac{n}{b}+1\right)(w-v+6) \leq n(\beta_2-\beta_1) + \frac{6n}{b} + (w-v+6)$$

Given $\epsilon > 0$ choose $b$ such that $b > \frac{1}{\epsilon}$, and $n$ such that $\frac{b(\beta_2-\beta_1)}{n} < \epsilon$ (We choose $b$ according to this $\epsilon$, and the previous paragraph is based on any $v, w$ satisfying the condition). This gives that $\frac{w-v}{n} < \epsilon$ and $\frac{1}{n} \leq \frac{w-v}{n} < \epsilon$ and so $1 < n\epsilon$.

Combining the inequalities above we have

$$n(\beta_2-\beta_1) - 7n\epsilon \leq T(n,\beta_1,\beta_2) \leq n(\beta_2-\beta_1) + 13n\epsilon$$

(Note in both inequalities, we use $\frac{6n}{b} < 6n\epsilon$ as $b > \frac{1}{\epsilon}$) Hence

$$\lim_{n\to\infty} \frac{1}{n} T(n,\beta_1,\beta_2) = \beta_2 - \beta_1$$

□

**Remark 5.28.** *The last inequality in the proof might not be the best bounds but is sufficient for the proof.*

## 5.4 Exercises

1. Let $N$ and $M$ be positive integers such that $N$ is not a square and $M \leq \sqrt{N}$. If $x, y$ are positive integers satisfyig

   $$x^2 - Ny^2 = M$$

   Prove that $\frac{x}{y}$ is a convergent of $\sqrt{N}$.

2. Let $\alpha = [a_0, a_1, \ldots]$ and $\frac{p_n}{q_n}$ be convergent. Show that

   $$p_n = det \begin{pmatrix} a_0 & -1 & 0 & \ldots & 0 & 0 \\ 1 & a_1 & -1 & \ldots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \ldots & 1 & a_n \end{pmatrix}$$

   Find a similar expression for $q_n$.
   Show also that $\frac{p_{n+1}}{p_n} = [a_{n+1}, \ldots, a_0]$ and $\frac{b_{n+1}}{b_n} = [a_{n+1}, \ldots, a_1]$

3. Let $u_n$ be the $n^{th}$ term in the Fibonacci sequence. i.e.

   $$u_1 = 1, u_2 = 1 \text{ and } u_{n+2} = u_{n+1} + u_n \ \forall n \geq 0$$

   Let $\alpha = \frac{1+\sqrt{5}}{2}$. Show that:

(i) $\frac{u_{n+2}}{u_{n+1}}$ is the $n^{th}$ convergent of $\alpha$.

(ii) If $p$ is a prime, then $p|u_{p-1}$ if $p \equiv \pm 1 \pmod 5$, and $p|u_{p+1}$ if $p \equiv \pm 2 \pmod 5$, and hence show that every prime divides infinitely many Fibonacci numbers.
Hint: you may consider $2^{p-1}u_p \bmod p$ and use the fact that

$$u_n = \frac{\alpha^n - \alpha'^n}{\sqrt{5}}$$

4. Prove Theorem 5.16. (Hurwitz)
(Hint: Consider any three consecutive convergents. If we write $\beta_n = \frac{q_{n-2}}{q_{n-1}}$, try to prove that

$$\beta_n + \frac{1}{\beta_n} < \sqrt{5}$$

and hence get a contradiction of the fact $a_n \geq 1$)

5. Suppose $\alpha$ is a real number in the interval $(0, 1)$ and $\alpha = [0, a_1, a_2, \ldots]$ Evaluate the probability that $a_1 \geq m$ and $a_1 = m$ Further, show that the probability that $a_2 \geq m$ is

$$\sum_{a_1=1}^{\infty} \frac{1}{a_1(ma_1 + 1)}$$

Hence, find the probability that $a_2 = 1$.

6. Assume that $\alpha$ is a quadratic irrational number which satisfies $\alpha > 1$, and $-1 < \alpha' < 0$ where $\alpha'$ is the conjugate of $\alpha$; that is, $\alpha' = \frac{a-b\sqrt{d}}{c}$, if $\alpha = \frac{a+b\sqrt{d}}{c}$. Show that

(i) $-1 < \alpha'_n < 0$, where $\alpha_n$ satisfies $\alpha = [a_0, a_1, \ldots a_{n-1}, \alpha_n]$.

(ii) $a_n = [\frac{-1}{\alpha'_{n+1}}]$.

(iii) $\alpha$ is purely periodic (that is, the first period of the continued fraction of $\alpha$ begins with $a_0$).

7. Assume that $\alpha > 1$ is irrational and is purely periodic defined in the above question. Let $\frac{p_n}{q_n}$ be convergent. Show that $\alpha$ satisfies the polynomial equation $f(\alpha) = 0$ where

$$f(x) = x^2 q_{n-1} + x(q_{n-2} - p_{n-1}) - p_{n-2}$$

for suitably chosen $n$. Hence show that the second root $\alpha'$ of this equation satisfies $-1 < \alpha' < 0$. Combine question 6 and 7, it follows that the continued fraction of a quadratic irrational number $\alpha$ is purely periodic if and only if $\alpha > 1$ and $-1 < \alpha' < 0$.

8. By writing $x^3 - dy^3$ as a product of two factors, with one of which being $\frac{x}{y} - d^{\frac{1}{3}}$, show that if $\{x_0, y_0\}$ is a solution of the equation $x^3 - dy^3 = n$ then $\frac{x_0}{y_0}$ is a convergent of $d^{\frac{1}{3}}$ provided that $y_0 > \frac{8|n|}{3d^{\frac{2}{3}}}$ and $d$ is positive and not a cube.

9. Suppose $d$ is positive and is not square. Show that the equation

$$v^2 - dw^2 = 4$$

is always soluble and there is a fundamental solution $\{v_0, w_0\}$ from which all other solutions are generated by ($n \in \mathbb{Z}$)

$$\frac{v + w\sqrt{d}}{2} = \pm \left( \frac{v_0 + w_0\sqrt{d}}{2} \right)^n$$

* 10. Let $k$ be the period of continued fraction of $\sqrt{d}$ where $d > 0$ and is not square. Suppose $\alpha = [\sqrt{d}] + \sqrt{d}$, $c_0 = [\sqrt{d}]$, $e_0 = 1$ and $c_i$ and $e_i$, $i = 1, 2, \ldots$ are as defined in Theorem 5.22 (on page 55). Show that:

(i) $e_i = 1$ if and only if $k|i$.

(ii) $e_j \neq -1$ for all $j$.

(iii) $a_i < \sqrt{d}$ for $i = 1, 2, \ldots, k-1$.

Further, Show that the continued fraction of $\sqrt{d}$ has the form

$$[a_0, a_1^*, \ldots, a_{k-1}, 2a_0^*] \text{ where } a_0 = [\sqrt{d}] \text{ and } a_i = a_{k-i}$$

for $i = 1, 2, \ldots k-1$. (You may use question 2 and 6 in this question).

11. Show that there are infinitely many integers $n$ such that the sum

$$1 + 2 + \ldots + n$$

is a square.

## 5.5 Hint and Solutions

1. $(x - \sqrt{N}y)(x + \sqrt{N}y) = M$ and so $x - \sqrt{N}y > 0$. So we have$x > \sqrt{N}y$. Now consider that

$$\frac{x}{y} - \sqrt{N} = \frac{M}{y(x + \sqrt{N}y)} < \frac{M}{2\sqrt{N}y^2}$$

But $M \leq \sqrt{N}$ and hence we have

$$\left| \sqrt{N} - \frac{x}{y} \right| < \frac{1}{2y^2}$$

By Theorem 5.15, $\frac{x}{y}$ is a convergent of $\sqrt{N}$.

2. This is clearly true for $n = 0, 1$. And for $n \geq 2$, we notice that

$$det \begin{pmatrix} a_0 & -1 & 0 & \ldots & 0 & 0 \\ 1 & a_1 & -1 & \ldots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \ldots & 1 & a_n \end{pmatrix}$$

is just

$$a_n det \begin{pmatrix} a_0 & -1 & 0 & \dots & 0 & 0 \\ 1 & a_1 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix} - det \begin{pmatrix} a_0 & -1 & 0 & \dots & 0 & 0 \\ 1 & a_1 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -1 \end{pmatrix}$$

Now use induction, and combine the above expression, we have exactly that the determinant gives $a_n p_{n-1} + p_{n-2}$ because

$$-det \begin{pmatrix} a_0 & -1 & 0 & \dots & 0 & 0 \\ 1 & a_1 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -1 \end{pmatrix} = det \begin{pmatrix} a_0 & -1 & 0 & \dots & 0 & 0 \\ 1 & a_1 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & p_{n-2} \end{pmatrix}$$

Similarly, we have $q_0 = 1$ and

$$q_n = det \begin{pmatrix} a_1 & -1 & 0 & \dots & 0 & 0 \\ 1 & a_2 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 & a_n \end{pmatrix}$$

for $n \geq 1$.

For $\frac{p_{n+1}}{p_n}$, it is easy to check that this holds for $n = 0$. Now use induction on $n$ and notice that $p_{n+1} = a_{n+1} p_n + p_{n-1}$, and hence

$$\frac{p_{n+1}}{p_n} = a_{n+1} + \frac{p_{n-1}}{p_n}$$

But assume $\frac{p_n}{p_{n-1}} = [a_n, \dots, a_0]$ by induction, then we have

$$a_{n+1} + \frac{1}{[a_n, \dots, a_0]} = [a_{n+1}, a_n, \dots, a_0]$$

Use a similar argument for $\frac{q_{n+1}}{q_n}$.

3. (i) Observe that

$$\frac{1+\sqrt{5}}{2} = \frac{1}{\frac{\sqrt{5}-1}{2}}$$

Hence by induction that $\alpha_n = \frac{\sqrt{5}+1}{2}$ for all $n$ and so $\frac{\sqrt{5}+1}{2} = [1, 1, 1, \dots]$. Therefore, as we can easily check that $p_0 = u_2, p_1 = u_1$, and $p_n = a_n p_{n-1} + p_{n-2} = p_{n-1} + p_{n-2}$. Thus $p_n = u_{n+2}$ and similarly $q_n = u_{n+1}$.

(ii) If $p < 5$, we can check directly for the first few cases. Let $p > 5$, expand $\alpha^n - \alpha'^n$ for $n$ odd, we have

$$2^{n-1} u_n = \left( n + \binom{n}{3} 5 + \dots + 5^{\frac{n-1}{2}} \right)$$

As $p$ is a prime, and so $2^{p-1} \equiv 1 \pmod{p}$, and $p | \binom{p}{k}$ for $1 \leq k \leq p-1$. Hence we have

$$u_p \equiv 5^{\frac{p-1}{2}} \equiv \left( \frac{5}{p} \right) \pmod{p}$$

by Euler's criterion (Lemma 4.4). By Lemma 5.9, we have

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

Use (i), and $p$ odd, we have

$$u_p^2 - u_{p+1}u_{p-1} = 1$$

By above, $u_p^2 \equiv 1 \pmod{p}$ and hence $p|u_{p-1}u_{p+1}$ and so

$$p|u_{p-1} \text{ or } p|u_{p+1}$$

Now consider when $n$ is even, we have

$$2^{n-1}u_n = n + \binom{n}{3} + \ldots + n5^{\frac{n-2}{2}}$$

Let $n = p+1$, and we have $2^p u_{p+1} \equiv 1 + (\frac{5}{p}) \pmod{p}$. Therefore, if $(\frac{5}{p}) = -1$, we have $p|u_{p+1}$. Otherwise, we have $p|u_{p-1}$.
But $5 \equiv 1 \pmod{4}$ and so

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 \iff p \equiv \pm 2 \pmod{p}$$

The result follows by combining the above arguments.

4. As in the proof of Theorem 5.12, we have

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

and we set $\beta_{n+1} = \frac{q_{n-1}}{q_n}$, and we aim to show that

$$\alpha_n + \beta_n \leq \sqrt{5}$$

cannot hold for three consecutive convergents if $n > 1$.

Suppose the above holds for $n-1$ and $n$, then Use $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$, and

$$\frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \beta_{n-1}$$

we have

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1}$$

As we assume $\alpha_n + \beta_n \leq \sqrt{5}$, and use the above we have

$$1 = \frac{\alpha_n}{\alpha_n} \leq \left(\frac{-1}{\beta_n} + \sqrt{5}\right)\left(-\beta_n + \sqrt{5}\right)$$

Rearrange the inequality we have

$$\beta_n + \frac{1}{\beta_n} < \sqrt{5} \text{ and so } \beta_n > \frac{\sqrt{5}-1}{2}$$

as $0 < \beta_n < 1$.

If now we assume

$$\alpha_n + \beta_n \leq \sqrt{5}$$

holds for $n$ and $n+1$, then the above holds if we replace $\beta_n$ by $\beta_{n+1}$. That is, the inequality holds for $n-1, n, n+1/$ Then

$$a_n = \frac{q_n - qn - 2}{q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < (-\beta_{n+1} + \sqrt{5}) - \beta_n$$

Then use $-\beta_n, -\beta_{n+1} < -\frac{-1+\sqrt{5}}{2}$, we have

$$a_n < \sqrt{5} - (-1 + \sqrt{5}) = 1$$

which contradicts $\alpha$ being irrational (as then $a_n \geq 1$).

5. $a_0 = 0$ and so $\alpha_1 = \frac{1}{\alpha}, a_1 = [\frac{1}{\alpha}]$. So the probability that $a_1 \geq m$ is the probability that $\alpha \leq \frac{1}{m}$, which is $\frac{1}{m}$. Now the probability that $a_1 = m$ is the same as $a_1 \geq m$ but not $a_1 \geq m+1$ as $a_1$ is an integer. Hence it is $\frac{1}{m} - \frac{1}{m+1} = \frac{1}{m(m+1)}$.

   Now

$$\alpha_2 = \frac{1}{\frac{1}{\alpha} - a_1}$$

   So the probability of $a_2 \geq m$ is the same as $\alpha_2 \leq \frac{1}{m}$. i.e. we have

$$\frac{1}{a_1} \leq \alpha \leq \frac{1}{a_1 + m}$$

   for each $a_1$ and so we have

$$\sum_{a_1=1}^{\infty} \frac{1}{a_1(ma_1 + 1)}$$

   Put $m = 2$ we have

$$\sum_{a_1=1}^{\infty} \frac{1}{a_1(2a_1 + 1)} = 2\sum_{n=1}^{\infty} \left( \frac{1}{2n} - \frac{1}{2n+1} \right)$$

   Now expand $\log 2 = \log 1 + 1$, we have

$$\log 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} \ldots$$

   and hence the summation above is equal to $2(1 - \log 2)$. Therefore, the probability is

$$2 \log 2 - 1$$

   as the probability that $a_2 \geq 1$ is 1.

6. (i) We have $\frac{1}{\alpha_{n+1}} = \alpha_n - a_n$, and so we can check directly by algebra that the conjugates satisfies

$$\frac{1}{\alpha'_{n+1}} = \alpha'_n - a_n$$

   Then use $-1 < \alpha'_0 < 0$ and the above, and apply induction on $n$, we deduce that $-1 < \alpha'_n < 0$ for all $n$.

   (ii) We have $\frac{1}{\alpha'_{n+1}} = \alpha'_n - a_n$ and so $[\frac{-1}{\alpha'_{n+1}}] = [-\alpha'_n] + a_n$. Use (i), $0 < -\alpha'_n < 1$ and so $[-\alpha'_n] = 0$. Therefore, we have $a_n = [\frac{-1}{\alpha'_{n+1}}]$.

   (iii) By Theorem 5.22, we know $a_n$ is periodic and we have $\alpha_j = \alpha_k$ for some $j, k$. We also have that

$$\alpha_{j-1} = \frac{1}{\alpha_j} + a_{j-1} = \frac{1}{\alpha_j} + \left[ \frac{1}{\alpha'_j} \right]$$

   by (ii). Also if $\alpha_j = \alpha_k$, then we take conjugates on both sides, we would have $\alpha'_j = \alpha'_k$. Therefore, use the equation above, we conclude that if $\alpha_j = \alpha_k$, then $\alpha_{j-1} = \alpha_{k-1}$ and hence the period starts from $a_0$.

7. By Lemma 5.5, we have

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

Now as $\alpha$ is purely periodic, and so we have $\alpha = \alpha_n$ for some $n$. Pick that $n$, and we rearrange the above equation, we have

$$\alpha^2 q_{n-1} + \alpha(q_{n-2} - p_{n-1}) - p_{n-2}$$

as required.

Now consider that $f(0) = -p_{n-2} < 0$, $f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0$ and $f(1) = q_{n-1} + q_{n-2} - p_{n-1} - p_{n-2} < 0$ and so we conclude that: One of the roots is greater than 1 and the other one is between 0 and $-1$. Hence the result follows.

8. We have

$$n = x^3 - dy^3 = y^3 \left( \left( \frac{x}{y} \right) - d^{\frac{1}{3}} \right) \left[ \left( \frac{x}{y} + \frac{d^{\frac{1}{3}}}{2} \right)^2 + \frac{3}{4} d^{\frac{2}{3}} \right]$$

Hence we have

$$\left| \frac{x}{y} - d^{\frac{1}{3}} \right| = \frac{|n|}{y \cdot y^2 \left[ \left( \frac{x}{y} + \frac{d^{\frac{1}{3}}}{2} \right)^2 + \frac{3}{4} d^{\frac{2}{3}} \right]} < \frac{|n|}{y \cdot y^2 \frac{3}{4} d^{\frac{2}{3}}}$$

Now, since $y_0 > \frac{8|n|}{3} d^{\frac{2}{3}}$, we have that

$$\left| \frac{x_0}{y_0} - d^{\frac{1}{3}} \right| < \frac{1}{2d^{\frac{2}{3}}}$$

and hence $\frac{x_0}{y_0}$ is a convergent by Theorem 5.15.

9. This is always soluble as we have solutions to $x^2 - dy^2 = 1$ and let $v = 2x, w = 2y$. Now let $D = \frac{v + w\sqrt{d}}{2}$, and let $v_0, w_0$ be a positive solution such that $D$ is minimal. It is easy to check that if $\{a, b\}, \{v, w\}$ are solutions, then $\{x, y\}$ defined as

$$\frac{x + y\sqrt{d}}{2} = \left( \frac{a + b\sqrt{d}}{2} \right) \left( \frac{v + w\sqrt{d}}{2} \right)$$

is also a solution.

Further, let $\{t, u\}$ be a solution and we choose $m$ so that

$$D^m \leq \frac{t + u\sqrt{d}}{2} < D^{m+1}$$

and so we have

$$1 \leq \left( t + u\sqrt{d} \right) D^{-m} < D$$

Write $\frac{(t+u\sqrt{d})}{2} D^{-m} = \frac{X + Y\sqrt{d}}{2}$, then $\{X, Y\}$ is a solution with $X, Y$ non-negative because we have $1 \leq \frac{X+Y\sqrt{d}}{2} < D$ and so $0 < \frac{X - Y\sqrt{d}}{2} \leq 1$ and hence $X \geq 1$ and $Y\sqrt{d} \geq 0$. Then it follows by the minimality of $D$ that $X = 2$ and $Y = 0$. Hence $\frac{t+u\sqrt{d}}{2} = D^m$ for some $m$. The proof is just an analogue of Theorem 5.23.

10. (i) $\alpha > 1$, and $\alpha' = [\sqrt{d}] - \sqrt{d}$ and so $-1 < \alpha' < 0$. Use question 6, we know that $\alpha$ is purely periodic. As $k$ is the period, so we have $\alpha = \alpha_{nk}$, and $\alpha \neq \alpha_i$ for $k \nmid i$.

$$\frac{c_{nk} + \sqrt{d}}{e_{nk}} = \frac{c_0 + \sqrt{d}}{e_0} = [\sqrt{d}] + \sqrt{d}$$

Compare both sides for the irrational parts, we have $e_{nk} = 1$.
Conversely, if $e_i = 1$, then we have $\alpha_i = c_i + \sqrt{d}$ and $\alpha_i' = c_i - \sqrt{d}$. By question 6, we know that $-1 < \alpha_i' < 0$ and $c_i$ is integer. Hence we have $c_i = [\sqrt{d}]$. Therefore, $\alpha_i = \alpha$ and so $k|i$.

(ii) As $\alpha_i > 0$, suppose $e_i = -1$, then we have $c_i < -\sqrt{d}$. Then $\alpha_i' = -c_i + \sqrt{d} > 0$, contradicts what we had in question 6.

(iii) In fact $e_i \geq 0$ for all $i$ in (ii), using a similar argument. Then we have by (i) that $e_i \geq 2$ for $i = 1, 2, \ldots, k-1$. Now as

$$c_{i+1} = a_i e_i - c_i \leq \alpha_i e_i - c_i = c_i + \sqrt{d} - c_i = \sqrt{d}$$

So that

$$\alpha_i = \frac{c_i + \sqrt{d}}{e_i} \leq \frac{\sqrt{d} + \sqrt{d}}{2}$$

and so $a_i < \sqrt{d}$.

Now We have

$$\alpha_1 = \frac{1}{\sqrt{d} - [\sqrt{d}]}$$

and so

$$\alpha_1' = \frac{1}{-\sqrt{d} - [\sqrt{d}]}$$

which lies between $-1$ and 0. By question 6, $\alpha_1$ is purely periodic and $\alpha = [a_0, \alpha_1]$, the period starts at $a_1$. Let the period be $k$. Also, by question 6, we know that

$$a_k = \left[-\frac{1}{\alpha_{k+1}'}\right] = \left[-\frac{1}{\alpha_1'}\right] = [d + \sqrt{d}] = 2a_0$$

as required.
Finally, we have $\sqrt{d} = [a_0, \ldots, \frac{1}{-a_0 + \sqrt{d}}]$, and so apply Lemma 5.5, we have

$$\sqrt{d} = \frac{\frac{1}{-a_0+\sqrt{d}} p_k + p_{k-1}}{\frac{1}{-a_0+\sqrt{d}} q_k + q_{k-1}}$$

Rearrange the above, we have a quadratic equation for $d$, which is

$$x^2 - x\left(a_0 + \frac{p_{k-1}}{q_{k-1}} - \frac{q_k}{q_{k-1}}\right) - \frac{p_k}{q_{k-1}} + \frac{a_0 p_{k-1}}{q_{k-1}}$$

Compare the rational part and irrational part, so the coefficient of $x$ must be 0, and so we have

$$a_0 + \frac{p_{k-1}}{q_{k-1}} - \frac{q_k}{q_{k-1}} = 0$$

Now $\frac{p_{k-1}}{q_{k-1}} = [a_0, \ldots, a_{k-1}]$ and by question 2 we have

$$\frac{q_k}{q_{k-1}} = [a_k, \ldots, a_1]$$

But $a_k = 2a_0$, and so we rearrange the equation, we get

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots \frac{1}{a_{k-1}}}} = a_0 + \frac{1}{a_{k-1} + \frac{1}{a_{k-2} + \ldots \frac{1}{a_1}}}$$

The result follows by comparing both sides.

11. We need to find $n$ and $k$ such that

$$\frac{n(n+1)}{2} = k^2$$

Rearrange the above, we have $n^2 + n = 2k^2$. Multiply both sides by 4, we have $4n^2 + 4n = 8k^2$. completing the square, we have

$$(2n+1)^2 - 8k^2 = 1$$

Now, let $d = 8$ which is positive but not a square. As we have infinitely many solutions for the Pell's equation

$$x^2 - 8y^2 = 1$$

and each solution $\{x, y\}$ must have $x$ odd, so we have infinitely such pairs $\{n, k\}$.

# 6 Distribution of prime numbers and Riemannn zeta function

The study of the primes is one of the most important branches of number theory. The literature on the prime numbers is very extensive beginning withy Pythagoras and Euclid; even so, many problems remain. There are two pre-eminent results: Dirichlet's theorem and the prime number theorem(PNT). Dirichlet's theorem states that every arithmetic progression $\{an+b : n = 0, 1, 2, \ldots\}$, where $(a, b) = 1$ contains infinitely many primes. The PNT was postulated by both Legendre and Gauss and it was finally published by Hadamard, which states that

$$\pi(x) \sim \frac{x}{\log x}$$

A more precise version of this result is

$$\pi(x) \sim li(x) = \int_2^x \frac{dt}{\log t}$$

## 6.1 Basic properties

**Theorem 6.1.** *Let $P$ be the set of all prime numbers. Then*

$$\sum_{p\in P} \frac{1}{p} \text{ and } \prod_{p\in P} \left(1 - \frac{1}{p}\right)^{-1}$$

*both diverge to $\infty$.*

*Proof.* Let $x \geq 2$. We write

$$S(x) = \sum_{p\in P, p\leq x} \frac{1}{p} \text{ and } P(x) = \prod_{p\in P, p\leq x} \left(1 - \frac{1}{p}\right)^{-1}$$

Let $p_1, p_2, \ldots p_r$ be all prime numbers less than or equal to $x$. Then

$$\begin{aligned} P(x) &= \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^{-1} \\ &= \prod_{i=1}^{r} \left(1 + p_i^{-1} + p_i^{-2} + \ldots\right) \\ &= \sum_{a_1=0}^{\infty} \cdots \sum_{a_r=0}^{\infty} p_1^{-a_1} \cdots p_r^{-a_r} \\ &> \sum_{n=1}^{\infty} \frac{1}{n} \to \infty \text{ as } x \to \infty \end{aligned}$$

As each integer $n$ can be written as a product of prime factors.

$$\begin{aligned} \log P(x) &= -\sum_{i=1}^{r} \log\left(1 - \frac{1}{p_i}\right) \\ &= \sum_{i=1}^{r} \sum_{n=1}^{\infty} \frac{1}{np_i^n} \\ &= S(x) + \sum_{i=1}^{r} \sum_{n=2}^{\infty} (np_i^n)^{-1} \end{aligned}$$

For each $i$, we have

$$\sum_{n=2}^{\infty}(np_i^n)^{-1} < \sum_{n=2}^{\infty}\frac{1}{p_i^n} = \frac{p_i^{-2}}{1-\frac{1}{p_i}} \leq 2p_i^{-2}$$

So

$$\sum_{i=1}^{r}\sum_{n=2}^{\infty}\left(np_i^{-n}\right) \leq \sum_{i=1}^{r}2p_i^{-2} \leq \sum_{n=1}^{\infty}\frac{1}{n^2}$$

which converges. Hence, as $\log P(x)$ diverges to infinity, we have $S(x) \to \infty$. □

**Theorem 6.2.** *$\forall x \geq 2$, we have $P(x) \geq \log x$ and $S(x) \geq \log\log x - \frac{1}{2}$*

In fact we will strengthen the result in the next subsection.

*Proof.*

$$P(x) > \sum_{n=1}^{[x]}\frac{1}{n} > \int_1^{[x]}\frac{1}{n}dn = \log\left([x]+1\right) > \log x$$

As $0 < u < 1$, we have

$$-\log(1-u) - u = \frac{u^2}{2}\left(1 + \frac{u}{\frac{3}{2}} + \ldots\right) < \frac{u^2}{2}\left(1 + u + u^2 + \ldots\right) = \frac{u^2}{2(1-u)}$$

Apply the above with $u = \frac{1}{p}$ and sum over all prime less than or equal to $x$, we have

$$0 \leq \log P(x) - S(x) < \frac{1}{2}\sum_{p\in P, p\leq x}\frac{1}{p(p-1)} < \frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{n(n-1)} = \frac{1}{2}$$

So $S(x) \geq \log\log x - \frac{1}{2}$ □

## 6.2 Legendre formulae

**Definition 6.3.** *Let $p_n$ be the $n^{th}$ prime. For $x \geq 2, r \geq 1$, we define $N_r(x)$ to be the number of integers $n$ with $1 \leq n \leq x$ which are not divisible by any of the first $r$ primes.*

Intuitively, we would guess by inclusion exclusion that

$$N_r(x) = [x] - \sum_{i=1}^{r}\left[\frac{x}{p_i}\right] + \ldots + (-1)^r\left[\frac{x}{p_1\ldots p_r}\right]$$

Here is one special case: Let $r = \pi(\sqrt{x})$. Every composite in $[2, x]$ must be divisible by some prime number $p_i, i \leq r$ where $p_1, p_2, \ldots, p_r$ are all prime numbers $\leq \sqrt{x}$. Then we have (Remember to include 1)

$$N_r(x) = \pi(x) - \pi(\sqrt{x}) + 1$$

which is the number of prime in $[\sqrt{x}, x]$ plus 1. Hence

$$1 + \pi(x) = \pi(\sqrt{x}) + [x] + \ldots + (-1)^r\left[\frac{x}{p_1\ldots p_r}\right]$$

**Definition 6.4.** *We extend Definition 6.3 such that we write $N_r(x,h)$ to be the number of integers $\leq x$, not divisible by $p_1, \ldots, p_r$ but divisible by $h$. For example, $N_0(x,h)$ is the number of integers $\leq x$ which are divisible by $h$, and clearly, $N_0(x,h) = [\frac{x}{h}]$.*

**Lemma 6.5.** *Assume that $r \geq 1$ and $(h, p_r) = 1$. Then*

$$N_{r-1}(x,h) = N_r(x,h) + N_{r-1}(x, p_r h)$$

*Proof.* $N_{r-1}(x,h)$ counts the number of integers in the set

$$\{n : 1 \leq n \leq x \text{ with } h|n \text{ and } (n, p_1 p_2 \dots p_{r-1}) = 1\}$$

The set above can be written as a disjointunion of two sets, which are:

$$\{n : 1 \leq n \leq x \text{ with } h|n \text{ and } (n, p_1 p_2 \dots p_r) = 1\}$$

and

$$\{n : 1 \leq n \leq x \text{ with } h|n, p_r|n \text{ and } (n, p_1 p_2 \dots p_r) = 1\}$$

As $(h, p_r) = 1$, $h|n, p_r|n \iff hp_r|n$ and so the result follows. □

So we have

$$N_1(x,h) = N_0(x,h) - N_0(x,2h)$$

$$\dots\dots\dots\dots$$

$$N_r(x,h) = N_0(x,h) - \sum_i N_0(x, p_i h) + \dots + (-1)^r N_0(x, p_1 p_2 \dots p_r h)$$

This proves Legendre's formulae by setting $h = 1$ and using $N_0(y,m) = [\frac{y}{m}]$. Here is an application of Legendre's formulae.

**Theorem 6.6.** $\lim_{x \to 0} \frac{\pi(x)}{x} = 0$

*Proof.* Let $\zeta$ e any real number btween 2 and $x$ for a fixed $x$. Let $r(\zeta)$ be an integer that $p_{r(\zeta)} \leq \zeta < p_{r(\zeta)+1}$. We shall firstly prove that

$$\pi(x) < r(\zeta) + N_{r(\zeta)}(x)$$

Let $q$ be a prime $\leq x$, then either $q \in \{p_1, \dots p_{r(\zeta)}\}$ or it is not divisible by any $p_i, i \leq r(\zeta)$. But there are other composite number which is not divisible by these $p_i$. Counting in this way, we have the above inequality.

Now we look for an upper bound for $N_{r(\zeta)}(x)$. Apply Legendre's formulae

$$N_r(x) = [x] - \sum_{i=1}^{r} \left[\frac{x}{p_i}\right] + \dots + (-1)^r \left[\frac{x}{p_1 \dots p_r}\right]$$

and the error from dropping $[\cdot]$ is less than

$$1 + \binom{r}{1} + \binom{r}{2} + \dots + \binom{r}{r} = 2^r$$

by considering the number of terms in each sum. Hence we have

$$N_{r(\zeta)}(x) \leq 2^{r(\zeta)} + x - \sum_{i=1}^{r(\zeta)} \frac{x}{p_i} + \dots = 2^{r(\zeta)} + x \prod_{i=1}^{r(\zeta)} \left(1 - \frac{1}{p_i}\right)$$

Use the result above, we have

$$\pi(x) \leq r(\zeta) + 2^{r(\zeta)} + x \prod_{i=1}^{r(\zeta)} \left(1 - \frac{1}{p_i}\right) \leq 2 \cdot 2^{r(\zeta)} + \prod_{i=1}^{r(\zeta)} \left(1 - \frac{1}{p_i}\right)$$

because $r(\zeta) \leq 2^{r(\zeta)}$. By Theorem 6.2,we have

$$\prod_{i=1}^{r(\zeta)} \left(1 - \frac{1}{p_i}\right)^{-1} > \log \zeta$$

because $p_1, \ldots, p_{r(\zeta)}$ are all primes less than or equal to $\zeta$. and so

$$\prod_{i=1}^{r(\zeta)} \left(1 - \frac{1}{p_i}\right) < \frac{1}{\log \zeta}$$

Therefore,

$$\frac{\pi(x)}{x} \leq \frac{2^{r(\zeta)+1}}{x} + \frac{1}{\log \zeta} = 2e^{r(\zeta)\log 2 - \log x} + \frac{1}{\log \zeta}$$

Now we pick $\zeta = \frac{\log x}{2 \log 2}$ and use $r(\zeta) < \zeta$, so that

$$\frac{\pi(x)}{x} < 2e^{-\frac{\log x}{2}} + \frac{1}{\log\left(\frac{\log x}{2\log 2}\right)}$$

which tends to 0 as $x \to \infty$. □

## 6.3 The result of Chebyshev

We begin the subsection by some basic properties:

**Lemma 6.7.** *The exact order of each prime factor of* $n!$ *is*

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

*Proof.* The number of integers less than or equal to $n$ which are divisible by $p^i$ is $[\frac{n}{p^i}]$. The result follows by counting the number from each $i$. □

**Lemma 6.8.** *Let* $n \geq 1$ *throughout*

*(i)* $2^n \leq \binom{2n}{n} < 2^{2n}$.

*(ii)* $\prod_{n<p\leq 2n} p \Big| \binom{2n}{n}$, *where* $p$ *in the product runs through prime only.*

*(iii) Let* $r(p)$ *satisfies* $p^{r(p)} \leq 2n < p^{r(p)+1}$, *then*

$$\binom{2n}{n} \Big| \prod_{p\leq 2n} p^{r(p)}$$

*(iv) If* $n \geq 2$ *and* $\frac{2n}{3} < p \leq n$, *then* $p \nmid \binom{2n}{n}$.

*(v)* $\prod_{p\leq n} p < 4^n$.

*Proof.* (i) $2^{2n} = (1+1)^{2n}$, and the expansion contains the term $\binom{2n}{n}$, and so $2^{2n} \geq \binom{2n}{n}$. Also, $\binom{2n}{n} = \frac{(2n)(2n-1)\ldots(n+1)}{n(n-1)\ldots 1}$ and for each $i$, $\frac{2n-i}{n-i} \geq 2$, so that $\binom{2n}{n} \geq 2^n$.

(ii) Let $p$ be a prime such that $n < p \leq 2n$. Then $p \nmid n!$ but $p \big| (2n)!$. Let $k = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, and so $(n!)^2 k = (2n)!$. Then $p \big| (2n)! \Rightarrow p \big| (n!)^2$ or $p \big| k$. But $p \nmid n!$ and so $p \big| k$. As any two $(p_i, p_j) = 1$, therefore, the product of them also divides $k$.

(iii) By Lemma 6.7, we have the exact power of $p$ dividing $\binom{2n}{n}$ is

$$\sum_{j=1}^{\infty} \left( \left[ \frac{2n}{p^j} \right] - 2 \left[ \frac{n}{p^j} \right] \right) = \sum_{j=1}^{r(p)} \left( \left[ \frac{2n}{p^j} \right] - 2 \left[ \frac{n}{p^j} \right] \right) \leq \sum_{j=1}^{r(p)} 1 = r(p)$$

Hence $\binom{2n}{n} \big| \prod_{p \leq 2n} p^{r(p)}$.

(iv) Let $\frac{2n}{3} < p < n$. Then the factor $p$ occurs once only in $n!$ because $2p > \frac{4n}{3} > n$. Also $p$ occurs exactly twice in $(2n)!$ since $3p > 2n$ and $2p < 2n$. Therefore the factor $p$ has been canceled in $\frac{(2n)!}{(n!)^2}$, and so the result follows.

(v) Apply induction on $n$. It is easy to check that the result holds for $n = 1, 2, 3$. Let $m > 1$, suppose it is true for $2m-1$, then it is also true for $2m$ as

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} p < 4^{2m-1} < 4^{2m}$$

because $2m$ is not prime. So it remains to check that, if it is true for $m+1$, then it is also true for $2m+1$, and hence complete the proof. By (ii), every prime in the interval $[m+2, 2m+1]$ divides $\binom{2m+1}{m}$. So we have

$$\prod_{p \leq 2m+1} p \leq \left( \prod_{p \leq m+1} p \right) \binom{2m+1}{m} < 4^{m+1} \binom{2m+1}{m}$$

Now $\binom{2m+1}{m} = \binom{2m+1}{m+1}$, and they both occur in the expansion $(1+1)^{2m+1}$, so $\binom{2m+1}{m} \leq \frac{2^{m+1}}{2} = 4^m$. So

$$\prod_{p \leq 2m+1} p < 4^{m+1} 4^m = 4^{2m+1}.$$

□

Now we come to a version of Chebyshev's result; note that the constants can be improved by using more precise inequalities.

**Theorem 6.9.** **[Chebyshev]** *If $n > 1$, then*

$$\frac{n}{8 \log n} < \pi(n) < \frac{6n}{\log n}$$

*Proof.* By Lemma 6.8, $\binom{2n}{n} \big| \prod_{p \leq 2n} p^{r(p)}$ and each $p > n$ divides $\binom{2n}{n}$. So

$$n^{\pi(2n) - \pi(n)} < \prod_{n < p \leq 2n} p \leq \binom{2n}{n} \leq \prod_{p \leq 2n} p^{r(p)} \leq (2n)^{\pi(2n)} \qquad (\star)$$

using $p^{r(p)} \leq 2n$. Also by Lemma 6.8, $\binom{2n}{n} \leq 2^{2n}$, so we have

$$n^{\pi(2n)-\pi(n)} < \binom{2n}{n} \leq 2^{2n} \tag{A}$$

Also by Lemma 6.8, $\binom{2n}{n} > 2^n$, and so by $(\star)$

$$(2n)^{\pi(2n)} \geq \binom{2n}{n} > 2^n \tag{B}$$

Now, let $n = 2^k$ then for $(A)$, we have (Compare the exponent)

$$k\left(\pi(2^{k+1}) - \pi(2^k)\right) < 2^{k+1}$$

and for $(B)$

$$(k+1)\pi(2^{k+1}) > 2^k$$

Rewrite $(A)$ as

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k$$

because $\pi(2^{k+1}) \leq 2^k$ as every even number apart from 2 is not prime, and 1 is not prime. So we can sum over the above from $k = 0$ to $m$, that

$$\sum_{k=0}^{m}(k+1)\pi(2^{k+1}) - k\pi(2^k) < \sum_{k=0}^{m} 3 \cdot 2^k$$

But we can simplify LHS and use $\pi(1) = 0$, so we have

$$(m+1)\pi(2^{m+1}) < 3(2^{m+1} - 1) < 3 \cdot 2^{m+1}$$

and so

$$\pi(2^{m+1}) < \frac{3 \cdot 2^{m+1}}{m+1} \tag{$A'$}$$

By $(B)$, we have $(m+1)\pi(2^{m+1}) > 2^m$ and so

$$\pi(2^{m+1}) > \frac{2^m}{m+1} = 2^{m+1}2(m+1) \tag{$B'$}$$

So given any $n$, choose $m$ such that $2^{m+1} \leq n < 2^{m+2}$. Since $\frac{1}{2} < \log 2 < 1$, we have

$$\frac{t}{2} < \log 2^t < t \ \forall t \geq 1$$

Now by $(A')$,

$$\pi(n) \leq \pi(2^{m+2}) < \frac{3 \cdot 2^{m+2}}{m+2} < \frac{3 \cdot 2^{m+2}}{\log 2^{m+2}} = \frac{6 \cdot 2^{m+1}}{\log 2^{m+2}} \leq \frac{6n}{\log n}$$

and by $(B')$,

$$\pi(n) \geq \pi(2^{m+1}) > \frac{2^{m+1}}{2(m+1)} > \frac{2^{m+2}}{8\left(\frac{m+1}{2}\right)} > \frac{2^{m+2}}{8\log 2^{m+1}} > \frac{n}{8\log n}$$

□

## 6.4 Bertrand's postulate and some other results

We are going to strengthen some of the pervious results in this subsection. But before that, here is a simple but useful theorem about prime numbers by Bertrand:

**Theorem 6.10. [Bertrand's postulate]** *For every integer $n \geq 1$, there exists a prime $p$ such that $n < p \leq 2n$.*

*Proof.* We know there is no prime $p$ dividing $\binom{2n}{n}$ for $\frac{2n}{3} < p \leq n$. Suppose we have no prime between $n$ and $2n$, then the only prime divisors of $\binom{2n}{n}$ are those $\leq \frac{2n}{3}$. Let $S(p)$ be the exact power of $p$ dividing $\binom{2n}{n}$. By Lemma 6.8, $\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{r(p)}$ and so $p^{S(p)} \leq 2n$ because $p^{r(p)} \leq 2n$.

Suppose $S(p) > 1$, then $p \leq \sqrt{2n}$, and hence no more than $[\sqrt{2n}]$ primes can divide $\binom{2n}{n}$ more than once, and $p^{S(p)} \leq 2n$ so we have

$$\binom{2n}{n} \leq (2n)^{[\sqrt{2n}]} \prod_{p \leq \frac{2n}{3}} p$$

Also, $\binom{2n}{n}$ is the largest term in the expansion $(1+1)^{2n} = 4^n$ and there are in total $2n+1$ terms, so we have $\binom{2n}{n} > \frac{4^n}{2n+1}$ and so

$$(2n)^{\sqrt{2n}} \prod_{p \leq \frac{2n}{3}} p > \frac{4^n}{2n+1}$$

Since $\sqrt{2n} > [\sqrt{2n}]$.

Now by Lemma 6.8, $\prod_{p \leq m} p < 4^m$ and so

$$4^{\frac{2n}{3}} (2n)^{\sqrt{2n}} > \frac{4^n}{2n+1}$$

by above. Also $(2n+1) < (2n)^2$, so

$$4^{\frac{n}{3}} < (2n)^{2+\sqrt{2n}}$$

and so

$$\frac{n \log 4}{3} < \left(2 + \sqrt{2n}\right) \log 2n$$

Numerically, this gives a contradiction when $n \geq 750$. For the case when $n < 750$, we check manually than there is prime between $n$ and $2n$. Hence the result follows. □

Now we shall evaluate two important series defined on prims, they play a vital role in number theory. We shall denote for any real $x$, $\sum_{p \leq x} f(p)$ as the sum $f(2) + f(3) + \ldots f(p)$, where the value $p$ takes over all primes less than or equal to $x$.

**Theorem 6.11.**

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$$

*Proof.* This is derived for an integer variable first by estimating $\log n!$ in two distinct ways. By Lemma 6.7, we have

$$\begin{aligned} \log n! &= \log \prod_{p \leq n} p^{\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right)} \\ &= \log p \left( \sum_{p \leq n} \left[\frac{n}{p}\right] \right) + \log p \left( \sum_{p \leq n} \sum_{i \geq 2} \left[\frac{n}{p^i}\right] \right) \end{aligned}$$

We consider the sums separately. Clearly

$$\log p \sum_{p\le n}\left[\frac{n}{p}\right] \le \sum_{p\le n}\frac{n\log p}{p}$$

and

$$\begin{aligned}\log p\sum_{p\le n}\left[\frac{n}{p}\right] &> \log p\sum_{p\le n}\left(\frac{n}{p}-1\right)\\ &= \sum_{p\le n}\frac{n\log p}{p}-\sum_{p\le n}\log p\\ &> \sum_{p\le n}\frac{n\log p}{p}-\pi(n)\log n\\ &> \sum_{p\le n}\frac{n\log p}{p}-6n\end{aligned}$$

where the last inequality came from Theorem 6.9. For the second sum,

$$\begin{aligned}\log p\sum_{p\le n}\sum_{i=2}^{\infty}\left[\frac{n}{p^i}\right] &\le n\log p\sum_{p\le n}\sum_{i=2}^{\infty}\left(\frac{1}{p^i}\right)\\ &= n\sum_{p\le n}\frac{\log p}{p(p-1)}\\ &< n\sum_{j\le n}\frac{\log j}{j(j-1)}=cn\end{aligned}$$

for some constant $c$ as the last series is convergent. Combining these inequalities we have

$$n\sum_{p\le n}\frac{\log p}{p}-6n\le\log n!\le n\sum_{p\le n}\frac{\log p}{p}+cn$$

Now we estimate $\log n!$ in a different way. We have $\log n!=\sum_{j\le n}\log j$ and

$$\sum_{j\le n}\log j>\int_1^n\log y dy=n\log n-n+1$$

Also $n!<n^n$, so we have

$$n\log n-2n<n\log n-n+1<\log n!<n\log n$$

Now combine the two estimation, we have by the first estimation that

$$\log n!-cn\le n\sum_{p\le n}\frac{\log p}{p}\le\log n!+6n$$

and use the second estimation, we have

$$n\log n-(2+c)n<n\sum_{p\le n}\frac{\log p}{p}<n\log n+6n$$

which is the same as

$$\sum_{p\le n}\frac{\log p}{p}=\log n+O(1)$$

Finally, if replace the integer variable $n$ by a real variable $x$ we have, if $n \le x < n+1$,

$$\sum_{p\le x} \frac{\log p}{p} = \sum_{p\le n} \frac{\log p}{p} = \log n + O(1) = \log x + O(1)$$

as $\log x - \log n < 1$. □

For the our second result we need the following lemma:

**Lemma 6.12.** *Let $t_1, t_2, \ldots$ be a non-decreasing sequence of real numbers with limit infinity, let $z_1, z_2, \ldots$ be any sequence of real numbers, and suppose $f$ is a real function with a continuous derivative for arguments greater than or equal to $t_1$. Define $Z$ by*

$$Z(x) = \sum_{t_n\le x} z_n$$

*the sum of all $z_n$ for those $n$ which satisfy $t_n \le x$. Then*

$$\sum_{t_n\le x} z_n f(t_n) = Z(x)f(x) - \int_{t_1}^{x} Z(y)f'(y)dy$$

*Proof.* As $Z(t_{n+1}) - Z(t_n) = z_{n+1}$ because $t_n$ is non-decreasing, we have, if $m$ is the largest subscript such that $t_m \le x$,

$$\begin{aligned}\sum_{t_n\le x} z_n f(t_n) &= Z(t_1)f(t_1) + (Z(t_2) - Z(t_1))f(t_2) \\ &\quad + \ldots (Z(t_m) - Z(t_{m-1}))f(t_m) \\ &= Z(t_1)(f(t_1) - f(t_2)) + \ldots + Z(t_{m-1})(f(t_{m-1}) - f(t_m)) \\ &\quad + Z(t_m)(f(t_m) - f(x)) + Z(x)f(x)\end{aligned}$$

By definition of $m$, $Z(t_m) = Z(x)$. Now because $Z$ is constant on the interval $[t_i, t_{i+1})$ we have

$$Z(t_i)(f(t_i) - f(t_{i+1})) = -\int_{t_i}^{t_{i+1}} Z(y)f'(y)dy$$

Combining these equations we have

$$\begin{aligned}\sum_{t_n\le x} z_n f(t_n) &= Z(x)f(x) - \left\{\sum_{i=1}^{m-1} \int_{t_i}^{t_{i+1}} + \int_{t_m}^{x}\right\} Z(y)f'(y)dy \\ &= Z(x)f(x) - \int_{t_1}^{x} Z(y)f'(y)dy\end{aligned}$$

□

The method employed at the beginning of the proof is called **partial summation**; We shall use it often in the following pages. We shall finish the subsection by a stronger version of Theorem 6.2.

**Theorem 6.13.**

$$\sum_{p\le x} \frac{1}{p} = \log\log x + c + O\left(\frac{1}{\log x}\right)$$

*for some constant $c$.*

*Proof.* In Lemma 6.12 $t_n = p_n$ the $n^{th}$ prime, $z_n = \frac{\log p_n}{p_n}$ and $f(y) = \frac{1}{\log y}$, so we have if $x \geq 2$

$$\begin{aligned}
\sum_{p \leq x} \frac{1}{p} &= \sum_{p \leq x} \frac{\log p}{p} \frac{1}{\log p} = \frac{1}{\log x} \sum_{p \leq x} \frac{\log p}{p} + \int_2^x \left( \sum_{p \leq t} \frac{\log p}{p} \right) \frac{dt}{t \log^2 t} \\
&= \frac{1}{\log x}(\log x + O(1)) + \int_2^x \frac{\log t dt}{t \log^2 t} + \int_2^x \left( \sum_{p \leq t} \frac{\log p}{p} - \log t \right) \frac{dt}{t \log^2 t} \\
&= 1 + O\left( \frac{1}{\log x} \right) + \log\log x - \log\log 2 + \left( \int_2^\infty - \int_x^\infty \right) \frac{O(1) dt}{t \log^2 t} \\
&= \log\log x + c + O\left( \frac{1}{\log x} \right)
\end{aligned}$$

where we use Theorem 6.11 to evaluate $\sum_{p \leq x} \frac{\log p}{p}$. The constant $c$ exists as the first integral in the line above converges and the second has order $O(\frac{1}{\log x})$. □

## 6.5 Riemann zeta function

We have mentioned Riemann zeta function in Chapter 2, and now we are going to discuss in detail about some very important properties of Riemann zeta function. The function is given by:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

for $s$ a complex variable. If we write $s = \sigma + it (\sigma, t \text{ real})$, then it is convergent for $\sigma > 1, -\infty < t < \infty$. There are lots of connections between Riemann zeta function and the primes. We shall begin with:

**Theorem 6.14.** *(i) If $\sigma \geq 1 + \epsilon$, for $\epsilon > 0$, then the series*

$$\sum_{n=1}^{\infty} n^{-s}$$

*is absolutely and uniformly convergent.*

*(ii) For $\sigma > 1$,*

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}$$

*where the product is taken over all prime numbers $p$.*

*Proof.* (i) For an integer $j > 1$. we have

$$\left| \sum_{n=j}^{\infty} n^{-s} \right| \leq \sum_{n=j}^{\infty} \left| n^{-s} \right| = \sum_{n=j}^{\infty} n^{-\sigma} \leq \int_{j-1}^{\infty} x^{-\sigma} dx \leq \frac{(j-1)^{1-\sigma}}{\sigma - 1} < \frac{j^{-\epsilon}}{\epsilon}$$

Hence the result follows.

(ii) Let $P$ be a fixed prime. Then

$$\prod_{p \leq P} \left(1 - p^{-s}\right)^{-1} = \sum_{p \leq P} (1 + p^{-s} + p^{-2s} + \ldots) = \sum_{n \in X} n^{-s}$$

where $X$ contains all integer composed of primes $\leq P$. So

$$\left|\zeta(s) - \prod_{p\leq P}\left(1-p^{-s}\right)^{-1}\right| = \left|\sum_{n\notin X} n^{-s}\right| \leq \sum_{n\notin X} n^{-\sigma} \leq \sum_{n=P+1}^{\infty} n^{-\sigma}$$

as $n \notin X \Rightarrow n \geq P+1$. The last sum tends to 0 as $P$ tends to infinity as $\sigma > 1$.

□

**Corollary 6.15.** *$\zeta(s)$ has no zero when $\sigma > 1$.*

*Proof.* Let $P$ be a fixed prime.

$$\prod_{p\leq P}\left(1-p^{-s}\right)\zeta(s) = 1 + m_1^{-s} + m_2^{-s} + \dots$$

where $m_i$ are integers which have at least one prime factor $> P$. Then

$$\begin{aligned}\left|\prod_{p\leq P}\left(1-p^{-s}\right)\zeta(s)\right| &\geq 1 - m_1^{-\sigma} - m_2^{-\sigma} - \dots \\ &\geq 1 - (p+1)^{-s} - (p+2)^{-\sigma} - \dots \\ &\geq 1 - \frac{1}{2} = \frac{1}{2}\end{aligned}$$

for $P$ large enough. Therefore,

$$\left|\prod_{p\leq P}(1-p^{-s})\zeta(s)\right| \geq \frac{1}{2}$$

and $1 - p^{-s} \neq 0$ for $\sigma > 1$ since each $1 - p^{-s} \neq 0$, and so $\zeta(s) \neq 0$. □

**Lemma 6.16.** *Let $\{a_n\}, \{b_n\}$ be any sequence in $\mathbb{C}$ satisfying:*

*(i) $\sum_{n=1}^{\infty} a_n b_n$ converges.*

*(ii) $A_n b_n \to 0$, where $A_n = a_1 + \dots a_n$.*

*Then $\sum_{n=1}^{\infty} A_n(b_n - b_{n+1})$ converges to $\sum_{n=1}^{\infty} a_n b_n$.*

*Proof.* Define $A_0 = 0$. $S_N = \sum_{n=1}^{N} a_n b_n$ Then

$$\begin{aligned}S_N &= \sum_{n=1}^{N}(A_n - A_{n-1})b_n = \sum_{n=1}^{N}(A_n b_n - A_{n-1}b_n) \\ &= \sum_{n=1} A_n b_n - \sum_{n=0}^{N-1} A_n b_{n+1} \\ &= A_N b_N + \sum_{n=0}^{N-1} A_n(b_n - b_{n+1})\end{aligned}$$

As $N \to \infty$, as $S_N$ converges and $A_N b_N \to 0$, so

$$\sum_{n=0}^{N-1} A_n(b_n - b_{n+1}) \to S_N$$

as $N \to \infty$. □

The following theorem extends the domain of $\zeta$:

**Theorem 6.17.** *$\zeta(s) - \frac{1}{s-1}$ has an analytic continuation in the half plane $\mathcal{R}e(s) > 0$.*

*Proof.* Apply Lemma 6.16 to $\zeta(s)$ with $a_n = 1, b_n = n^{-s}$ So $\sum a_n b_n$ converges, and $A_n b_n = n n^{-s} \to 0$. Then we have

$$\sum A_n(b_n - b_{n+1}) \to \sum a_n b_n = \zeta(s)$$

Write

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) \\
&= s\sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1} dx \\
&= s\sum_{n=1}^{\infty} \int_n^{n+1} [x] x^{-s-1} dx \\
&= s\int_1^{\infty} [x] x^{-s-1} dx \\
&= s\int_1^{\infty} (x - (x)) x^{-s-1} dx \\
&= s\int_1^{\infty} x^{-s} - (x) x^{-s-1} dx \\
&= \frac{s}{s-1} - s\int_1^{\infty} x^{-s-1}(x) dx
\end{aligned}$$

Therefore,

$$\zeta(s) - \frac{1}{s-1} = 1 - s\int_1^{\infty} x^{-s-1}(x) dx$$

and the second term converges absolutely. Therefore we have an analytic continuation. □

For $\sigma \leq 0$, $\zeta(s)$ can be defined using the **functional equation** for $\zeta$ as follows. Let $\Gamma$, the *gamma* function, be given by (for $\sigma > 0$)

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1} dx$$

Note that $\gamma(s+1) = s\gamma(s)$ (integrate by parts), and so $\gamma(m) = (m-1)!$ for positive integer $m$. This relation can also be used to extend the domain of definition of $\gamma$ to the whole plane. $\gamma$ has a simple pole at $s = 0, -1, -2, \ldots$ and nowhere else.

Riemann showed that, if $\sigma < 0$,

$$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) \sin\left(\frac{\pi s}{2}\right)$$

We have many important properties of the Riemann zeta functions, for which we shall only state the results and will not go through any detail.

**Theorem 6.18.** *Define*

$$\Lambda = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

*for $\sigma > 0$ where $s = \sigma + it$. Then*

$$\Lambda(s) = \Lambda(1-s)$$

This theorem implies that the zeros of $\zeta(s)$ are symmetric about the line $(R)e(s) = \frac{1}{2}$. We also have $\zeta(s) < 0$ when $s \in [0, 1)$ and that $\zeta(s)$ has at most a simple 0 on the line $\mathcal{R}e(s) = 1$ (See Exercise 7). In fact we shall prove later that $\zeta(s)$ has no zero on the line $(R)e(s) = 1$. We also have

**Theorem 6.19. [Hardy]** *There are infinitely many zeros on the line* $\mathcal{R}e(s) = \frac{1}{2}$.

Riemann's hypothesis states that every 0 of $\zeta(s)$ (for $\mathcal{R}e(s) > 0$) lies on the line $\mathcal{R}e(s) = \frac{1}{2}$. Numerically, the first $10^9$ zeros lies on this line.

**Definition 6.20.** *Dirchlet Character mod N is a homomorphism*

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}^*$$

*and* $\bar{\chi} : \mathbb{Z} \longmapsto \mathbb{C}$ *by*

$$\bar{\chi}(n) = \begin{cases} 0 & \text{if } (n, N) > 1 \\ \chi(n + N\mathbb{Z}) & \text{if } (n, N) = 1 \end{cases}$$

*and We define* $L(\chi, S) = \sum_{n=1}^{\infty} \frac{\bar{\chi}}{n^s}$

The general Riemann's hypothesis states that fir every $\chi$, every zero of $L(\chi, s)$ in the region $\mathcal{R}e(s) \geq 0$ satisfies $\mathcal{R}e(s) = \frac{1}{2}$. The general Riemann's hypothesis plays a very important role in number theory.

*Applications*

The first application is a strong version of one of the facts we stated earlier.

**Theorem 6.21.** *For all real* $t$, $\zeta(1 + it) \neq 0$

*Proof.* By Theorem 6.14(ii)

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

so

$$\log \zeta(s) = -\sum_p \log (1 - p^{-s}) = \sum_p \sum_n \frac{p^{-ns}}{n}$$

Therefore,

$$\zeta(s) = \exp\left(\sum_p \sum_n \frac{p^{-ns}}{n}\right)$$

Let $s = \sigma + it$. Then

$$|\zeta(s)| = \exp\left(\sum_{p,n} \frac{\cos(nt \log p)}{np^{n\sigma}}\right)$$

because the modulus of $e^z$ is $e^{\mathcal{R}e(z)}$ and we write

$$p^{-ns} = p^{-n\sigma} e^{-int \log p}$$

Recall $\cos(2\phi) = 2\cos^2 \phi - 1$ and that

$$3 + 4\cos\phi + cos(2\phi) = 2(1 + \cos\phi)^2 \geq 0$$

Therefore,

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| = \exp\left(\sum_{p,n} \frac{3 + 4\cos(nt \log p) + \cos(2nt \log p)}{np^{n\sigma}}\right)$$

and the numerator is $\geq 0$ by above. Therefore,

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \geq 1$$

for $\sigma > 1$.

Now suppose $\zeta(1+it) = 0$. By Theorem 6.17 we know that $\zeta$ has a pole at 1. So we look at $\sigma + it$ and let $\sigma \to 1^+$. As $\sigma \to 1^+$, $\zeta^3(\sigma)$ has triple pole, and by assumption $\zeta^4(\sigma + it)$ has quadruple zero. So we have

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \to 0$$

as $\sigma \to 1$. But we have shown above that this expression is $\geq 1$, which is a contradiction. □

A typical analytic proof of PNT begins with the result:

**Theorem 6.22.** *For $\sigma > 1$,*

$$\log \zeta(s) = s \int_2^\infty \frac{\pi(x)}{x(x^s - 1)} dx$$

*Proof.* By Theorem 6.14(ii), using partial summation we have

$$\begin{aligned} \log \zeta(s) &= -\sum_p \log(1 - p^{-s}) = -\lim_{k\to\infty} \sum_{n=2}^{k} (\pi(n) - \pi(n-1)) \log(1 - n^{-s}) \\ &= \lim_{k\to\infty} \Bigg[ \sum_{n=2}^{k-1} \pi(n)(\log(1 - (n+1)^{-s}) - \log(1 - n^{-s})) \\ &\quad -\pi(k) \log(1 - k^{-s}) \Bigg] \end{aligned}$$

Now for $\sigma > 1$ the final term in the limit above tends to zero as $k \to \infty$, and so by the fundamental theorem of the calculus

$$\begin{aligned} \log \zeta(s) &= \sum_{n=2}^{\infty} \pi(n) \int_n^{n+1} \frac{d}{dx} \log(1 - x^{-s}) dx \\ &= s \sum_{n=2}^{\infty} \int_n^{n+1} \frac{\pi(x)}{x(x^s - 1)} dx = s \int_2^\infty \frac{\pi(x)}{x(x^s - 1)} dx \end{aligned}$$

□

Now PNT can be derived by solving this equation for $\pi(x)$, it uses a version of the Meliin transform. The accuracy of the estimate for $\pi(x)$ given by PNT is limited by Theorem 6.21, this estimate could be greatly improved if the Riemann hypothesis was available. We shall give another proof (in detail) of PNT later.

In the second application we define the function $M$ by

$$M(x) = \sum_{n \leq x} \mu(n)$$

where $\mu$ is the Möbius function. As $|\mu(n)| \leq 1$ holds for all $n$, we have immediately $M(x) = O(x)$. The question arises: what is the true order of $M(x)$?. In 1897 Mertens conjectured that, for all $\epsilon > 0$ and $x > 0$,

$$M(x) = o\left(x^{\frac{1}{2}+\epsilon}\right)$$

This is equivalent to Riemann hypothesis. One part of the equivalence can be demonstrated easily. In Lemma 2.22, we have shown that for $\sigma > 1$,

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

By partial summation we derive, as $M(0) = 0$,

$$\begin{aligned}\frac{1}{\zeta(s)} &= \sum_{n=1}^{\infty} \frac{M(n) - M(n-1)}{n^s} = \sum_{n=1}^{\infty} M(n) \left\{ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right\} \\ &= s \int_0^{\infty} M(x) x^{-s-1} dx\end{aligned}$$

It is a simple matter to show that if $M(n)$ grows less faster than $x^c$ than the integral above converges when $\sigma > c$. So to prove the Riemann hypothesis it is sufficient to derive

$$M(x) = o\left(x^{\frac{1}{2}+\epsilon}\right)$$

## 6.6 Bernoulli numbers

The last subsection of the chapter is an introduction to Bernoulli numbers and we shall use them to evaluate the zeta function at some integer arguments.

**Definition 6.23.** *The sequence $B_0, B_1, B_2, \ldots$ of rational numbers, called the* **Bernoulli numbers**, *is given by $B_0 = 1$, and if $m > 0$,*

$$(m+1)B_m = -\sum_{j=0}^{m-1} \binom{m+1}{j} B_j$$

So we have

$$2B_1 = -1, 3B_2 = -3B_1 - 1$$

and so on, and we may use this to calculate the first few $B_i$:

$$B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}, \ldots$$

We shall see below that, for all positive integers $n$, $B_{2n+1} = 0$ and $B_2 n$ alternates in sign. First we give an equivalence definition:

**Lemma 6.24.** *If we expand $\frac{t}{e^t - 1}$ as a power series in $t$, then*

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}$$

The proof is left as an exercise. (Exercise 11).

**Corollary 6.25.** *If $n > 0$, then $B_{2n+1} = 0$.*

*Proof.* As $B_1 = -\frac{1}{2}$ we have by Lemma 6.24

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{n=2}^{\infty} \frac{B_n t^n}{n!}$$

But

$$\frac{t}{e^t - 1} + \frac{t}{2} = \frac{t(e^t + 1)}{2(e^t - 1)}$$

which is an even function of $t$. Hence the odd power coefficients $\frac{B_3}{3!}, \frac{B_5}{5!}, \ldots$ are all zero. □

In the next result we evaluate $\zeta(2t)$ in terms of $B_{2t}$ where $t$ is a positive integer.

**Theorem 6.26.** **[Euler]** *If $t$ is a positive integer, then*

$$2(2t)!\zeta(2t) = (-1)^{t+1}(2\pi)^{2t}B_{2t}$$

*Proof.* We quote a standard result from analysis:

$$\sin x = x\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2\pi^2}\right)$$

(Intuitively, we came up with this expression by expanding $\sin x$ as a series in $x$ and so we may regard $\frac{\sin x}{x}$ as an infinite polynomial in $x$ which, may be written as

$$\left(1-\frac{x}{r_1}\right)\left(1-\frac{x}{r_2}\right)\cdots$$

because 0 is not a root of the polynomial and the constant term is 1 by taking the limit of $x \to 0$. The roots of $\frac{\sin x}{x}$ are $\pm\pi, \pm 2\pi, \ldots$ and so we may write it intuitively as

$$\frac{\sin x}{x} = \prod_{n=1}^{\infty}\left(1-\frac{x}{n\pi}\right)\left(1-\frac{x}{-n\pi}\right)$$

which is what we want. But in order to write down the expression as an infinite product, we must show that the product is absolutely convergent and so we may swap to order of terms. We shall not explain in detail of the proof. Taking the logarithm of the product, we have an infinite sum, and it is equivalent to show the infinite sum is absolutely convergent. But for each $x$, there is $n$ such that $\frac{x}{n}$ is small enough and the expansion of $\log 1 - t$ is roughly $-t$ for $t$ small but positive, and we use the fact that $\sum_{n=1}^{\infty}\frac{1}{n^2}$ converges.)

Now take the logarithmic derivative we have

$$\cot x = \frac{1}{x} - 2\sum_{n=1}^{\infty}\frac{x}{n^2\pi^2 - x^2}$$

and so, expanding each term in this sum as a geometric series,

$$x\cot x = 1 - 2\sum_{n=1}^{\infty}\sum_{t=1}^{\infty}\left(\frac{x}{n\pi}\right)^{2t} = 1 - 2\sum_{t=1}^{\infty}\zeta(2t)\left(\frac{x}{\pi}\right)^{2t}$$

Further, as $\cot x = i\frac{(e^{ix}+e^{-ix})}{e^{ix}-e^{-ix}}$, we also have

$$\begin{aligned} x\cot x &= ix\frac{e^{2ix}+1}{e^{2ix}-1} \\ &= ix + \frac{2ix}{e^{2ix}-1} \\ &= 1 + \sum_{t=2}^{\infty}\frac{B_t(2ix)^t}{t!} \end{aligned}$$

by Lemma 6.24. Equating coefficient of $x^{2t}$ $(t > 0)$ these equations yield

$$-\frac{2\zeta(2t)}{\pi^{2t}} = (-1)^t 2^{2t}\frac{B_{2t}}{(2t)!}$$

as required. □

**Corollary 6.27.** *(i) If $t > 0$, $(-1)^{t+1}B_{2t} > 0$*

*(ii)* $|B_{2t}| > 2(\frac{t}{\pi e})^{2t}$

*Proof.* (i) By Theorem 6.26, when $t > 0$,

$$(-1)^{t+1}B_{2t} = \frac{2(2t)!\zeta(2t)}{(2\pi)^{2t}} > 0$$

(ii) Take modulus of the above expression, we have

$$|B_{2t}| = \frac{2(2t)!\zeta(2t)}{(2\pi)^{2t}} > 2\frac{(2t)!}{(2\pi)^{2t}}$$

as $\zeta(2t) > 1$. Now we use

$$\log n! > n\log n - n$$

by considering the area bounded by $\log x$ from 1 to $n$. So that

$$e^n > \frac{n^n}{n!}$$

and hence the result follows by setting $n = 2t$ above.

□

Here is another immediate useful consequence:

**Corollary 6.28.** $\zeta(2) = \frac{\pi^2}{6}$

*Proof.* Put $t = 1$ in Theorem 6.26 and use $B_2 = \frac{1}{6}$. □

In fact, we can also calculate that $\zeta(4) = \frac{\pi^4}{90}, \zeta(6) = \frac{\pi^6}{945}$ and so on by using Theorem 6.26. No similar expression is known for $\zeta(2n+1)$. Note further that if we accept the functional equation

$$\zeta(s) = 2^s\pi^{s-1}\Gamma(1-s)\zeta(1-s)\sin(\frac{\pi s}{2})$$

we can calculate $\zeta(-n)$ for $n \geq 0$. We can show that $\zeta(-2n) = 0$ if $n > 0$ (Exercise 12) and the functional equation and Theorem 6.26 give, again if $n > 0$

$$\begin{aligned}\zeta(1-2n) &= 2^{1-2n}\pi^{-2n}\zeta(2n)\Gamma(2n)\sin(\frac{\pi}{2} - n\pi) \\ &= 2^{1-2n}\pi^{-2n}(-1)^{(n-1)}\frac{2^{2n}\pi^{2n}}{2(2n)!}B_{2n}(2n-1)!(-1)^n = -\frac{B_{2n}}{2n}\end{aligned}$$

We shall see some further properties of Bernoulli numbers in the exercise.

## 6.7 Exercises

1. Let $N$ be a positive integer. Using $N! > (\frac{N}{e})^N$, prove that

$$\prod_{p \leq N} \frac{\log p}{p-1} > \log N - 1$$

2. Prove that every non-constant polynomial with integer coefficients assumes infinitely many composite values.

3. Prove that every integer $N > 6$ can be expressed as a sum of distinct primes.

4. (i) By considering the case $k < n$ and $k \geq n$ separately, show that

$$\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k} = m$$

is not soluble.

(ii) Show that the equation

$$n! = m^k$$

is only soluble if at least one of $k, m$ or $n$ is 1.

5. (i) Let $p_n$ be the $n^{th}$ prime, show that there exist constants $c$ and $c'$ such that for $n > 1$

$$cn \log n < p_n < c' n \log n$$

(Hint: Use the result $\log n = o(\sqrt{x})$).)

(ii) Hence show that consecutive primes can be arbitrarily far apart.

6. Recall from question 6 in Exercise 2, that

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of prime } p \\ 0 & \text{otherwise} \end{cases}$$

Prove that

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1)$$

7. Prove that if there is a zero of $\zeta(s)$ on the line $\mathcal{R}e(s) = 1$, then it must be a simple zero.

8. Use Lemma 6.12 to prove

(i) $\sum_{n \leq x} \log n = x \log x - x + O(\log x)$.

(ii) $\sum_{n \leq x} \log^2 n = x \log^2 x - 2x \log x + 2xO(\log^2 x)$.

9. (i) Show that

$$\sum_{p \leq x} \left( \log \left( 1 - \frac{1}{p} \right) + \frac{1}{p} \right) = O(1)$$

(ii) Hence show that

$$\phi(n) > \frac{cn}{\log \log n}$$

for some constant $c$, by considering the primes less than $\log n$ which divides $n$.

10. (i) Find
$$\lim_{s\to 1^+}(s-1)\zeta(s)$$
(ii) Use the functional equation to calculate $\zeta(0)$.

11. Prove Lemma 6.24.

12. Show that $\zeta(-2n)=0$, where $n$ is a positive integer.

13. Let $S_k(m)=\sum_{n=1}^{m-1}n^k$. Show that
$$\sum_{j=0}^{m-1}e^{jt}=\sum_{k=0}^{\infty}S_k(m)\frac{t^k}{k!}$$
and so derive the formula
$$(k+1)S_k(m)=\sum_{j=0}^{k}\binom{k+1}{j}B_j m^{k+1-j}$$
Deduce that $S_3(m)=\frac{m^2(m-1)^2}{4}=(S_1(m))^2$.

⋆ 14. In this question we are going to derive the Clausen-von Staudt theorem which determines the denominators of the Bernoulli numbers. Let $f(t)=\sum_{n=0}^{\infty}\frac{a_nt^n}{n!}$ and $g(t)=\sum_{n=0}^{\infty}\frac{b_nt^n}{n!}$. The series $f$ is called integral if each $a_n$ is an integer, and we write $f\equiv g\pmod m$ when $a_n\equiv b_n\pmod m$ for all $n$, and $f$ and $g$ are integral. It is a simple matter to show that if $f$ and $g$ are both integral, so are $f'$, $\int_0^t f(x)dx$ and $fg$. Using these, prove that:

(i) If $f$ is integral, so is $\frac{f^m}{m!}$ provided that $f(0)=0$.

(ii) Deduce that if $m>4$ and is composite, then
$$(e^t-1)^{m-1}\equiv 0\pmod m$$
and
$$(e^t-1)^3\equiv 2\sum_{k=1}^{\infty}\frac{t^{2k+1}}{(2k+1)!}\pmod 4$$
and if $p$ is an odd prime, then
$$(e^t-1)^{p-1}\equiv -\sum_{k=1}^{\infty}\frac{t^{kp-k}}{(kp-k)!}\pmod p$$

(iii) Write $t=\log(1+(e^t-1))$ and so expand $\frac{t}{e^t-1}$ as a power series in $e^t-1$. Further, use the previous parts, show that
$$\sum_{p-1\,|\,2n}\frac{1}{p}+B_{2n}$$
is an integer, where the sum is taken over all primes $p$ satisfying $p-1\,|\,2n$. This determines the denominator of $B_{2n}$.

(iv) Deduce that the denominator of the Bernoulli number $B_{2n+1}$ is divisible by 6.

## 6.8 Hint and Solutions

1. It is equivalent to show:
$$\prod_{p\leq N} p^{\frac{N}{p-1}} \geq \left(\frac{N}{e}\right)^N$$
By Lemma 6.7, the exact power of $p$ diving $N!$ is
$$\sum_{k=1}^{\infty}\left[\frac{N}{p^k}\right] \leq N\sum_{k=1}^{\infty}\frac{1}{p^k} = \frac{N}{p-1}$$
and so we have
$$\prod_{p\leq N} p^{\frac{N}{p-1}} \geq N! \geq \left(\frac{N}{e}\right)^N$$

2. Let $f(x)$ be a polynomial, so it has finitely many $x$ such that $f(x)\leq 1$. WLOG, let $f(a) = p > 1$. Then, as $kp + a \equiv a \pmod{p}$, so that
$$f(kp+a) \equiv f(a) \pmod{p}$$
because $f(b)-f(a)$ always has a factor $b-a$. Hence $p\big|f(kp+a)\ \forall k$. Now we only have finitely many $x$ such that $f(x) = p$, and finitely many $x$ such that $f(x) = 2p, 3p, \ldots$ and so the results follows as we can take any multiple of $p$.

3. We prove the following inductive statement. If every integer less than or equal to $2p_k + 6$ can be written as sum of distinct primes less than or equal to $p_k$ then every integer less than or equal to $2p_{k+1}+6$ can be written as sum of distinct primes less than or equal to $p_{k+1}$ where $p_k$ is the $k$th prime bigger than 11 (so $p_1 = 13$). So we consider $y$ with $2p_k + 6 < y \leq 2p_{k+1} + 6$, then $y - p_{k+1} \leq p_{k+1} + 6 < 2p_k + 6$ by Berstrand's postulate and $y - p_{k+1} \geq 2p_k + 6 - p_{k+1} > 6$, again by Berstrand's postulate. By assumption $y - p_{k+1}$ can be as sum of distinct primes less than or equal to $p_k$ and so we have proved our claim. So to finish the proof we need to check the case for $k = 1$, i.e. writing every integer less than or equal to 32 as sum of distinct primes less than or equal to 13.

$$\begin{aligned}
&7{,}8 = 3+5, 9 = 2+7, 10 = 3+7, 11, 12 = 5+7, 13, 14 = 2+5+7, 15 = 3+5+7,\\
&16 = 3+13, 17 = 2+3+5+7, 18 = 7+11, 19 = 3+5+11, 20 = 2+7+11,\\
&21 = 2+3+5+11, 22 = 2+7+13, 23 = 2+3+5+13, 24 = 11+13, 25 = 5+7+13,\\
&26 = 2+11+13, 27 = 2+5+7+13, 28 = 3+5+7+13, 29 = 5+11+13,\\
&30 = 2+3+5+7+13, 31 = 2+5+11+13, 32 = 3+5+11+13.
\end{aligned}$$

4. (i) If $k < n$, then
$$\frac{1}{n} + \ldots + \frac{1}{n+k} \leq \frac{1}{n} + \ldots + \frac{1}{2n-1} < n\frac{1}{n} = 1$$
and so it is not soluble
If $k \geq n$, then by Bertrand's postulate, we have a prime $p$ between $n$ and $2n$. Let $p$ be the largest prime between $n$ and $n+k$. Then we multiply both sides by $\frac{(n+k)!}{p}$. Clearly, that $m\frac{(n+k)!}{p}$ is still an integer. On the other hand, each term on the left hand side is an integer apart from the term $\frac{1}{p}\frac{(n+k)!}{p}$. And so it is not soluble.

(ii) If $k, m$ and $n > 1$, then let $p \big| n!$, and so $p < n$. Then $p|m^k$ and hence $p|m$. So the exact order of $p$ in $n!$ is at least two. But by Bertrand's postulate, there is a prime $p$ between $[\frac{n}{2}]$ and $n$. This prime can only occur once in $n!$, which is a contradiction. Hence at least one of $k, m$ ad $n$ is 1.

5. (i) By Theorem 6.9, we have $\pi(n) < \frac{6n}{\log n}$. Replace $n$ by $p_n$ and use $\pi(p_n) = n$. we have $p_n > \frac{1}{6} n \log p_n > \frac{1}{6} n \log n$. Also we have $\frac{1}{8} < \frac{n \log p_n}{p_n}$ by the other part of inequality in Theorem 6.9. Now we want to find some $n$ such that $\log n < \frac{\sqrt{n}}{8}$. But as $\log n = o(\sqrt{n})$, we have some $n_0$, such that $\log n < \frac{\sqrt{n}}{8}$ for $n \geq n_0$. Then for $p_n \geq n_0$, we have $\frac{p_n}{8 \log n} > \frac{n}{\sqrt{n}}$ and hence we have

$$p_n < n^2$$

Therefore, we have $p_n < 8n \log p_n < 16n \log n$, for $p_n \geq n_0$. And for $p_n \leq n_0$, we can check manually and get a suitable constant if necessary. Hence, both $c$ and $c'$ exist.

(ii) Suppose we have an upper bound, say $k$, such that for all $n$, $p_{n+1} - p_n < k$. Then $p_{n+t} - p_n < tk$ and use (i) we have

$$c(n+t) \log n + t < p_{n+t} < c' n \log n + kt$$

for some constants $c$ and $c'$ and any $t \geq 1$. But this is false for $t$ large enough.

6. We have

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \sum_{p \leq x} \frac{\log p}{p} + \sum_{p^2 \leq x} \frac{\log p}{p^2} + \dots$$

The first term is $\log x + O(1)$ by Theorem 6.11. The other terms are convergent and there are only finitely many terms as we have some $k$ such that $2^k > x$. Hence the result follows by combining these two.

7. By Lemma 2.22,

$$\frac{1}{\zeta(s)} = \sum_{n=0}^{\infty} \frac{\mu(n)}{n^s}$$

Let $s = \sigma + it$ and hence

$$\left| \frac{1}{\zeta(s)} \right| \leq \zeta(\sigma)$$

by triangle inequality. If we have a double zero at $1 + it$. Then we have a double pole for $\zeta(s)$. But $\zeta(s)$ has only a simple pole at $\sigma = 1$, which is a contradiction.

8. (i) Let $t_n = n, z_n = 1, f(x) = \log x$ in Lemma 6.12. Then we have

$$Z(x) = [x] \text{ and } f'(y) = \frac{1}{y}$$

$$\sum_{n \leq x} \log n = [x] \log x - \int_1^x \frac{[y]}{y} dy = x \log x - x + O(\log x)$$

using $(y) \leq 1$ and so $\int_1^x \frac{1}{y} dy = \log x$.

(ii) Let $t_n = n, z_n = 1, f(x) = \log^2 x$ in Lemma 6.12. Then we have

$$z(x) = [x] \text{ and } f'(y) = \frac{2\log y}{y}$$

$$\begin{aligned}\sum_{n\le x} \log^2 n &= [x]\log^2 x - \int_1^x \frac{2[y]\log y}{y} dy \\ &= x\log^2 x - 2x\log x + 2x + O(\log^2 x)\end{aligned}$$

using $(y) \le 1$ and so $\int_1^x \frac{2\log y}{y} = \log^2 x$.

9. (i) Expand $\log(1-x)$ for $0 < x \le 1$ and use the fact that

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

converges for $s > 1$.

(ii)

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Use (i), we have

$$\log\frac{\phi(n)}{n} = -\sum_{p|n}\left(\log\left(1-\frac{1}{p}\right) + \frac{1}{p}\right) > -\sum_{p|n}\frac{1}{p} - c$$

for some constant $c$. Let $p_1, p_2, \ldots p_r$ be prime factors of $n$ and $p_1, \ldots, p_s$ be those less than $\log n$. Then

$$\sum_{p|n}\frac{1}{p} = \sum_{i=1}^{s}\frac{1}{p_i} + \sum_{i=s+1}^{r}\frac{1}{p_i} = S_1 + S_2$$

By Theorem 6.13, we have

$$S_1 < \log\log p_s + c < \log\log\log n + c$$

10. (i) By Theorem 6.17, we have

$$(s-1)(\zeta_s) = 1 + (s-1)(1 - s\int_1^{\infty} x^{-s-1}(x)dx$$

and so the result follows immediately by taking the limit when $s \to 1^+$.

(ii) The functional equation works for $\sigma < 0$ and so we have

$$\zeta(0) = \lim_{s\to 0^-} 2^s\pi^{s-1}\Gamma(1-s)\zeta(1-s)\sin\left(\frac{\pi s}{2}\right)$$

which can be rearranged as:

$$\left(\frac{1}{2}\right)\lim_{s\to 0-} 2^s\Gamma(1-s)(-s)\zeta(1-s)\left[\frac{\sin\left(\frac{\pi s}{2}\right)}{\frac{\pi^{1-s}s}{2}}\right]$$

as $s \to 0$, $2^s\Gamma(1-s) \to 1$ and $\left[\frac{\sin\left(\frac{\pi s}{2}\right)}{\frac{\pi^{1-s}s}{2}}\right] \to 1$. Now consider that

$$\lim_{s\to 0^-}(-s)\zeta(1-s) = \lim_{t\to 1^+}(t-1)\zeta(t)$$

Recall by Theorem 6.17 that

$$\zeta(t)(t-1) = t - t(t-1)\int_1^\infty x^{-t-1}(x)dx$$

and so

$$\lim_{s\to 0^-}(-s)\zeta(1-s) = \lim_{t\to 1^+}(t-1)\zeta(t) = 1$$

Therefore $\zeta(0) = -\frac{1}{2}$.

(a) Let $\frac{t}{e^t-1} = \sum_{n=0}^\infty \frac{b_n t^n}{n!}$. Then multiply both sides by $e^t - 1$ and expand in $t$, we have

$$t = \sum_{m=1}^\infty \frac{t^m}{m!}\sum_{n=0}^\infty \frac{b_n t^n}{n!}$$

Equating the coefficient for $t$ we have (if $k+1 = m+n$)

$$b_0 = 1 \text{ and } \frac{1}{(k+1)!}\sum_{j=0}^{k+1}\binom{k+1}{j}b_j = 0$$

for each $k$. Hence we have

$$b_k(k+1) = -\sum_{j=0}^{k-1}\binom{k+1}{j}b_j$$

as required.

(b) This follows immediately by substituting $-2n$ into the functional equation and use $\sin(-\pi n) = 0$.

11. Expand $e^{jt}$ as $\sum_{k=0}^\infty \frac{(jt)^k}{k!}$ and then swap the summation as the series is absolutely convergent, and the result follows by definition of $S_k(m)$. Now

$$\sum_{j=0}^{m-1} e^{jt} = \frac{e^{mt}-1}{e^t-1} = \frac{e^{mt}-1}{t}\frac{t}{e^t-1}$$

Use Lemma 6.24, and expand $e^{mt}$, we have

$$\left(\sum_{r=0}^\infty \frac{m^r t^{r-1}}{r!}\right)\left(\sum_{n=0}\frac{B_n t^n}{n!}\right)$$

Use the previous part and compare the coefficients (if $r-1+n = k$), we have

$$\sum_{r+n=k+1}\frac{m^r B_n}{r!n!} = \frac{S_k(m)}{k!}$$

and hence

$$(k+1)S_k(m) = \sum_{j=0}^{k} \binom{k+1}{j} B_j m^{k+1-j}$$

The last part follows immediately by applying the above formulae and we have

$$4S_3(m) = m^4 - 2m^3 + m^2$$

12. (i) Use induction on $m$. It is true for $m = 1$. Suppose true for $m$, that $\frac{f^m}{m!}$ is integral, then notice that

$$\frac{f^{m+1}}{(m+1)!} = \int_0^x \frac{f^m(t)}{m!} f'(t)dt$$

We have $f'(t)$ integral and by assumption we have $\frac{f^m}{m!}f'(t)$ integral, and hence

$$\frac{f^{m+1}}{(m+1)!} = \int_0^x \frac{f^m(t)}{m!} f'(t)dt$$

is integral.

(ii) We have

$$(e^t - 1)^m = \sum_{k=0}^{m} (-1)^{m-1-k} e^{kt} \binom{m}{k}$$

Then expand $e^k t$ and so we have

$$(e^t - 1)^m = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} k^n \right) \frac{t^n}{n!}$$

Hence,

$$(e^t - 1)^3 = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{3} (-1)^{3-k} \binom{3}{k} k^n \right) \frac{t^n}{n!}$$

and each coefficient for $\frac{t^n}{n!}$ is

$$\sum_{k=0}^{3} (-1)^{3-k} \binom{3}{k} k^n = 0 = \begin{cases} 0 & \text{if } n = 0 \\ 3 - 3 \cdot 2^n + 3^n & \text{otherwise} \end{cases}$$

Therefore, when $n \geq 2$, $2^n \equiv 0 \pmod 4$ and so

$$(e^t - 1)^3 \equiv \sum_{n=2}^{\infty} \frac{(3^n - 1)t^n}{n!} \pmod 4$$

Now

$$3^n - 1 \equiv \begin{cases} 0 \pmod 4 & \text{if } n \text{ is even} \\ 2 \pmod 4 & \text{if } n \text{ is odd} \end{cases}$$

So the result follows.

For the first and last part, we use

$$(x-1)^m = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} x^j$$

Differentiate, and put $x = 1$ we have

$$0 = \sum_{j=1}^{m} (-1)^{m-j} \binom{m}{j} j = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j$$

Further, if we differentiate the above twice, and put $x = 1$, we have

$$0 = \sum_{j=2}^{m} (-1)^{m-j} \binom{m}{j} j(j-1) = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j(j-1)$$

and so we have

$$0 = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j^2$$

Continue this we have

$$0 = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j^n \text{ for } 0 \leq n \leq m-1$$

For $m$, we differentiate the above $m$ times and so we have

$$m! = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j^m$$

For the first part, replace $m$ by $m-1$ above, and so, as $m$ is composite, so $(m-1)! \equiv 0 \pmod{m}$. Then we have

$$\sum_{j=0}^{m-1} (-1)^{m-1-j} \binom{m-1}{j} j^n \equiv 0 \pmod{m}$$

for $0 \leq n \leq m$. If $n > m$, then $n > \phi(m)$ and so we write

$$n = k\phi(m) + r, 0 \leq r < \phi(m) < m$$

and so

$$j^n \equiv j^r \pmod{m}$$

and therefore we conclude that

$$\sum_{j=0}^{m-1} (-1)^{m-1-j} \binom{m-1}{j} j^n \equiv 0 \pmod{m}$$

for all $n$.

For the last part, we have $(p-1)! \equiv -1 \pmod{p}$ and so the expression is 0 mod $p$ if $0 \leq n \leq p-2$ and is $-1$ mod $p$ if $n = p-1$. Now as $\phi(p) = p-1$ and as $(\mathbb{Z}/p\mathbb{Z})^*$ so the period is $p-1$ and so the result follows.

(iii) We have $\frac{t}{e^t-1} = \frac{\log(1+y)}{y}$ where $y = e^t - 1$. Use the expansion of $\log 1 + t = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{t^n}{n}$ and so we have

$$\frac{\log(1+y)}{y} = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{y^{n-1}}{n} = \sum_{n=0}^{\infty} (-1)^n \frac{y^n}{n+1}$$

Now use part (ii) and

$$(e^t-1)^m \equiv \sum_{n=0}^{\infty} \frac{b_n t^n}{n!} \pmod{m+1}$$

means that

$$\frac{(e^t-1)^m}{m+1} - \frac{1}{m+1}\sum_{n=0}^{\infty}\frac{b_n t^n}{n!} = \sum_{n=0}^{\infty}\frac{c_n t^n}{n!}$$

with $c_n$ integers. Therefore,

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}\frac{a_k t^k}{k!} - \frac{1}{2}\sum_{k=1}^{\infty}\frac{t^k}{k!} - \frac{2}{4}\sum_{k=1}^{\infty}\frac{t^{2k+1}}{(2k+1)!} - \sum_{p>2}\frac{1}{p}\sum_{k=1}^{\infty}\frac{t^{kp-k}}{(kp-k)!}$$

By Lemma 6.24, we have

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty}\frac{B_n t^n}{n!}$$

and so compare the coefficient of $t^2 n$ on both sides for each $n$, then consider $k(p-1)=2n$, and so $p-1\Big|2n$. Therefore, we have

$$B_n + \frac{1}{2} + \sum_{p>2, p-1\Big|2n}\frac{1}{p}$$

is an integer, in other words

$$B_n + \sum_{p-1\Big|2n}\frac{1}{p}$$

is an integer.

(iv) This is clear, as $2-1\Big|2n+2$ and $2=3-1\Big|2n+2$.

# 7 Algebraic background-Integral domain

The next few chapters are intended as detailed explanations in the ring theory and modules for those beginner of algebra. Readers with strong background of ring theory may skip those chapters. Basic properties and definition of the group theory will be assumed.
Sometimes we shall use the notation $\mathbb{Z}[a]$ to mean $\mathbb{Z} + \mathbb{Z}a$.

## 7.1 Basic properties

**Definition 7.1.** *An* **integral domain** *is a commutative ring that has a multiplicative identity but no divisor of zero. In other words, if $ab = 0$, then $a = 0$ or $b = 0$.*

*An integral domain $D$ is called a field if for each $a \in D$, $a \neq 0$, there exists $b \in D$ with $ab = 1$.*

**Example 7.2.** *The ring $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ of all integers is an integral domain.*

**Example 7.3.** *The Gaussian integer is of the form $\mathbb{Z}+\mathbb{Z}i$, which is an integral domain and is $\mathbb{Z}+\mathbb{Z}i$ is called the* **Gaussian domain**.

**Example 7.4.** *The set $\mathbb{Z} + \mathbb{Z}\omega = \{a + b\omega : a, b \in Z\}$, where $\omega$ is the complex cube root given by $\omega = \frac{-1+\sqrt{-3}}{2}$, is an integral domain, and the element in the set is called* **Eisenstein integers**, *and the set is called* **Eisenstein domain**.

**Example 7.5.** *$\mathbb{Z} + \mathbb{Z}\sqrt{m} = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$, where $m$ is a positive or negative integer that is not a perfect square, is an integral domain. $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is called a* **quadratic domain**.

**Example 7.6.** *$F[X]$ = the ring of polynomials in the indeterminate $x$ with coefficients from a field $F$ is an integral domain. Similarly, $F[x, y]$ = the ring of polynomials in the two indeterminates $x$ and $y$ with coefficients from the field $F$ is an integral domain.*

**Example 7.7.** *$\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Z}\}$, where $\theta$ is a root of the cubic equation $\theta^3 + \theta + 1 = 0$, is an integral domain. It is called a cubic domain.*

**Lemma 7.8.** *Let $D$ be a integral domain. Then:*

*(i) The identity element of $D$ is unique.*

*(ii) $D$ possesses a left cancellation law, that is:*

$$ab = ac, a \neq 0 \Rightarrow b = c$$

*as well as a right cancellation law*

$$ac = bc, c \neq 0 \Rightarrow a = b$$

*(iii) There exists a field $F$, called the field of quotients of $D$ or the quotient field of $D$, that contains an isomorphic copy $D'$ of $D$.*

*Proof.* (i) Let 1,1′ both be identities for $D$ then

$$1 = 1 \cdot 1' = 1'$$

(ii)

$$ab = ac \Rightarrow a(b - c) = 0 \Rightarrow a = 0 \text{ or } b - c = 0$$

But $a \neq 0$ and so $b = c$. The other case is similar.

(iii)

□

**Definition 7.9.** *Let $a$ and $b$ belong to the integral domain $D$. The element $a$ is said to be a* **divisor** *of $b$ (or $a$ divides $b$), written $a|b$ if there exists an element $c$ of $D$ such that $b = ac$. If $a$ is not a divisor of $b$, we write $a \nmid b$.*

**Example 7.10.** *In $\mathbb{Z} + \mathbb{Z}i$, $1 + i|2$ as $2 = (1 + i)(1 - i)$.*

**Properties of divisors**

(i) $a|a$ (reflexive).

(ii) $a|b$ and $b|c$ implies $a|c$ (transitivity).

(iii) $a|b$ and $a|c$ implies that $a|xb + yc$ for any $x, y \in D$

(iv) $a|b \Rightarrow ac|bc$.

(v) $ac|bc$ and $c \neq 0$ implies $a|b$, because we have some $d \in D$ such that

$$acd = bc \Rightarrow ad = b$$

(vi) $1|a$.

(vii) $a|0$.

(viii) $0|a \Rightarrow a = 0$.

**Definition 7.11.** *An element $a$ of an integral domain $D$ is called a* **unit** *if $a|1$. The set of units of $D$ is denoted by $U(D)$.*

**Properties of Units**

(i) $\pm 1 \in U(D)$.

(ii) If $a \in U(D)$ then $-a \in U(D)$.

(iii) If $a \in U(D)$ then $a^{-1} \in U(D)$ because if we have $ab = 1$, then $a^{-1}b^{-1} = 1$

(iv) If $a \in U(D)$ and $b \in U(D)$ then $ab \in U(D)$.

(v) If $a \in U(D)$ then $\pm a^n \in U(D)$ for any $n \in Z$.

**Example 7.12.** *$i$ is a unit in $\mathbb{Z}+\mathbb{Z}i$ because $i\cdot(-i)=1$.*

**Theorem 7.13.** *If $D$ is an integral domain then $U(D)$ is an Abelian group with respect to multiplication.*

*Proof.* By property (iv) $U(D)$ is closed under multiplication. As $D$ is an integral domain, so multiplication is both associative and commutative. The identity element is $1\in U(D)$. By property (iii) every element in $U(D)$ has an inverse. □

**Definition 7.14.** *Two non-zero elements $a$ and $b$ of an integral domain $Dd$ are associates, or said to be associated, if each divides the other. If $a$ and $b$ are associates, we write $a\sim b$, and if they are not associates, we write $a\not\sim b$.*

**Properties of Associates**

Let $a,b,c\in D^*=D\backslash\{0\}$, where $D$ is an integral domain. Then:

(i) $a\sim a$.

(ii) $a\sim b\Rightarrow b\sim a$.

(iii) $a\sim b$ and $b\sim c$ implies $a\sim c$.

(iv) $a\sim b$ if and only if $ab^{-1}\in U(D)$.

(v) $a\sim 1$ if and only if $a$ is a unit.

For (iv), suppose $ab^{-1}\in U(D)$ then we have some $c$ such that $ab^{-1}c=1$ and so $ac=b$ and $a|b$. Similarly, $ba^{-1}\in U(D)$ as it is a group and so we have $b|a$. Conversely, suppose $a\sim b$, then we can write $a=bc, b=ad$ for some $c,d$ and so $cd=1$. Hence $ab^{-1}=c\in U(D)$. (v) is a consequence of (iv).

**Example 7.15.** *In $D=\mathbb{Z}+\mathbb{Z}i$ we have $1+i\sim 1-i$ as $\frac{1+i}{1-i}=i\in U(D)$.*

## 7.2 Irreducible and Primes

**Definition 7.16.** *A non-zero, non-unit element $a$ of an integral domain $D$ is called an* **irreducible**, *or said to be irreducible, if $a=bc$ where $b,c\in D$ implies either $b$ or $c$ is a unit.*

*A non-zero non-unit element which is not irreducible is said to be reducible.*

**Example 7.17.** *2 is irreducible in $\mathbb{Z}$, but is reducible in $\mathbb{Z}+\mathbb{Z}i$ because $2=(1+i)(1-i)$ and $1\pm i$ are not units.*

**Definition 7.18.** *A non-zero, non-unit element $p$ of an integral domain $D$ is called a prime if $p|ab$, where $a,b\in D$ implies $p|a$ or $p|b$.*

**Example 7.19.** *2 is prime in $\mathbb{Z}$, but it is not prime in $\mathbb{Z}+\mathbb{Z}i$, because $2|2i=(1+i)(1+i)$ but $2\nmid 1+i$.*

**Theorem 7.20.** *In any integral domain $D$,a prime is irreducible.*

*Proof.* Let $D$ be an integral domain and suppose that $p$ is a prime and $p = ab$. Then $p|p$ and so $p|ab$. By definition, $p|a$ or $p|b$. WLOG, we may assume that $p|a$ and so $a = pc$.

Then substitute this into $p = ab$ we have $p = pbc \Rightarrow bc = 1$. Then $b$ is a unit and so $p$ is irreducible. □

**Remark 7.21.** *The converse is not true. For example, 2 is irreducible in $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ but not prime. (see Exercise 2).*

But we have the following theorem which gives a class of integral domain in which every irreducible is prime

**Theorem 7.22.** *Let $D$ be an integral domain which has the following property: Every quadratic polynomial in $D[X]$ having roots in the quotient field $F$ of $D$ is a product of linear polynomials in $D[X]$. Then every irreducible is prime.*

*Proof.* Let $p$ be an irreducible element in $D$, which is not prime. Then there exists $a, b \in D$ such that

$$p|ab, p \nmid a, b$$

Let $pr = ab$ and consider the quadratic polynomial

$$f(X) = pX^2 - (a+b)X + r$$

In $F(X)$ we have

$$f(X) = p\left(X - \frac{a}{p}\right)\left(X - \frac{b}{p}\right)$$

Suppose that $f(X) = (cX + s)(dX + t)$ which are linear factors in $D[X]$. Then we have $cd = p$. As $p$ is irreducible, then one of $c$ and $d$ is unit, and WLOG, say $d$. So we have $c = d^{-1}p$. Then the roots of $f(X)$ in $F$ are $-\frac{ds}{p}$ and $-\frac{t}{d}$. But $-\frac{t}{d} \in D$, and so we know that one of the root is in $D$. But the two roots are $\frac{a}{p}, \frac{b}{p}$ and so neither of them lies in $D$. Hence we have no such factorisation, which contradicts the assumption. Therefore, $p$ is prime. □

## 7.3 Ideals

**Definition 7.23.** *An* **ideal** *$I$ of an integral domain $D$ is a non-empty subset of $D$ having the following properties:*

*(i)* $a \in I, b \in I \Rightarrow a + b \in I$

*(ii)* $a \in I, r \in D \Rightarrow ra \in I$

It follows immediately from the definition that if $a_1, a_2, \ldots, a_n \in I$ then $r_1a_1 + \ldots r_na_n \in I$ for any $r_1, \ldots, r_n \in D$. 0 is always in $I$ and most importantly, if $1 \in I$ then $D = I$.

**Definition 7.24.** *An ideal $I$ of an integral domain $D$ is called a principal ideal if there exists an element $a \in I$ such that $I = \langle a \rangle$. The element $a$ is called a generator of the ideal $I$.*

If $D$ is an integral domain the principal ideal $\langle a \rangle$ generated by $a \in D$ is just the set $\{ra : r \in D\}$. The principle ideal $\langle 1 \rangle$ is $D$.

**Definition 7.25.** *An ideal $I$ of an integral domain $D$ is called a proper ideal of $D$ if $I \neq \langle 0 \rangle, \langle 1 \rangle$.*

**Remark 7.26.** *The generator of the ideal is not necessarily unique. For example, in $D = \mathbb{Z}$, the ideal $k\mathbb{Z} = \langle k \rangle = \langle -k \rangle$.*

**Theorem 7.27.** *Let $D$ be an integral domain and let $a, b \in D^* = D\backslash\{0\}$. Then*

$$\langle a\rangle = \langle b\rangle \iff ab^{-1} \in U(D)$$

*Proof.* Suppose $ab^{-1} \in U(D)$ then $a = bu$ for some $u \in U(D)$. Let $x \in \langle a\rangle$. Then $x = ac$ for some $c \in D$ and so $x = bcu \in \langle b\rangle$. Similarly, we can write $b = a^{-1}u$ and so for any $x \in \langle b\rangle, x \in \langle a\rangle$. Therefore $\langle a\rangle = \langle b\rangle$.

Conversely, suppose $\langle a\rangle = \langle b\rangle$, then $a = bc$ for some $c \in D$ and $b = ad$ for some $d \in D$. Hence $b = bd$, and as $b \neq 0$ we have $1 = cd$ and so $c = ab^{-1} \in U(D)$. □

## 7.4 Principal Ideal Domains

**Definition 7.28.** *An integral domain $D$ is* **principal ideal domain** *if every ideal in $D$ is principal.*

**Theorem 7.29.** *$\mathbb{Z}$ is a principal ideal domain.*

*Proof.* Let $I$ be a non-zero ideal of $\mathbb{Z}$. Let $a$ be the least positive element in $I$ (it must exist) and we shall prove that $I = \langle a\rangle$. Let $b \in I$, and so we can write $b = ap + r$ with $0 \leq r < a$. By definition of $a$, $r = 0$ and so $b \in \langle a\rangle$. Therefore $I = \langle a\rangle$, and so it is a principal ideal domain. □

**Theorem 7.30.** *Let $D$ be a principal ideal domain. Then any irreducible element is prime.*

*Proof.* Let $p$ be irreducible in $D$ and suppose $p|ab$, with $a, b \in D$. Suppose $p \nmid a$, then consider the ideal $I$ generated by $a$ and $p$. As $D$ is principal ideal domain, so we have some $d$ such that $\langle d\rangle = \langle a, p\rangle$. Therefore, we have $x, y \in D$ such that $ax + yp = d$. Also we have $d|p$, and so we have some $c$ such that $p = cd$. But $p$ is irreducible, so $c$ or $d$ is unit. Suppose $c$ is unit then $d = pc^{-1}$ and so $pc^{-1} = ax + py$ then we have $p|a$ which is a contradiction. Therefore, $d$ is a unit.

Then let $de = 1$ and so $ax' + py' = 1$, where $x' = xe, y' = ye$ and so

$$abx' + pby' = b$$

As $p|ab$, therefore we have $p|b$ and so $p$ is prime. □

Therefore, we conclude that:

**Theorem 7.31.** *In a principal ideal domain, an element is prime if and only if it is irreducible.*

*Proof.* Combine Theorem 7.20 and 7.30. □

**Definition 7.32.** *Let $D$ be a principal ideal domain and let $\{a_1, \ldots, a_n\}$ be a set of elements of $D$. Then the ideal $\langle a_1, \ldots, a_n\rangle$ is a principal ideal. A generator of this ideal is called a* **greatest common divisor** *of $a_1, \ldots, a_n$.*

Let $D$ be a principal ideal domain. If $a$ and $b$ are greatest common divisors of $a_1, \ldots, a_n \in D$ then

$$\langle a\rangle = \langle a_1, \ldots, a_n\rangle = \langle b\rangle$$

So that $\frac{a}{b} \in U(D)$ by Theorem 7.27 (equivalently, $a \sim b$). We write $(a_1, \ldots, a_n)$ for a greatest common divisor of $a_1, \ldots, a_n$, understanding that $(a_1, \ldots, a_n)$ is only defined up to a unit. Note that $(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1})$ if $a_n = 0$.

Further more, we can justify the definition by the following:

$$a \in \langle a\rangle = \langle a_1, \ldots, a_n\rangle$$

so that $\exists r, 1, \ldots, r_n \in D$ such that

$$a = r_1a_1 + \ldots r_na_n$$

Thus, if $c \in D$ such that $c|a_j \ \forall j$, then $c|a$, which justifies that $a$ is the greatest common divisor in the usual sense.

**Definition 7.33.** *The elements $a_1, \ldots, a_n$ are called relatively prime if $(a_1, \ldots, a_n)$ is a unit, and so*

$$\langle a_1, \ldots, a_n\rangle = \langle 1\rangle = D$$

## 7.5 Maximal ideals and prime ideals

**Definition 7.34.** *A proper ideal $M$ of an integral domain $D$ is called a* **maximal ideal** *if whenever $I$ is an ideal of $D$ such that $M \subseteq I \subseteq D$, then $I = M$ or $I = D$.*

**Example 7.35.** *The ideal $\langle x^2+1\rangle$ is maximal in $D = \mathbb{R}[x]$. To show shit, suppose we have an ideal $I$ which properly contains $\langle x^2+1\rangle$, then we have some $f(x) \in I$ but $f(x) \notin \langle x^2+1\rangle$, apply division algorithm so we may write:*

$$f(x) = (x^2+1)q(x) + r(x)$$

*with the degree of $r(x)$ being 0 or 1 and we may assume in general that $r(x) = ax + b$. Now $(x^2+1)q(x), f(x) \in I$, so $r(x) = f(x) - (x^2+1)q(x) \in I$. Then*

$$a^2x - b^2 = (ax+b)(ax-b) = r(ax-b) \in I$$

*and*

$$a^2(x^2+1) \in I$$

*Therefore, we have $a^2 + b^2 \in I$ but $a, b$ are not both 0 and so $a^2 + b^2$ is a unit $R[x]$. Hence $1 \in I$ and so $I = D$.*

**Theorem 7.36.** *Let $D$ be an integral domain. Let $a \in D$ be a non-zero and non-unit element. If $\langle a\rangle$ is a maximal ideal, then $a$ is irreducible.*

*Proof.* Suppose that $a$ is not an irreducible element of $D$. Then, aa $a$ is neither 0 nor a unit, it must be reducible and we may write $a = bc$ for some $b, c \in D$. Thus, we have

$$\langle a\rangle \subset \langle b\rangle \subset D$$

and so $a$ is not maximal. □

**Remark 7.37.** *The converse of Theorem 7.36 is not true. For example, $x$ is irreducible in mathbbZ$[x]$ but $\langle x\rangle$ is not maximal as we have*

$$\langle x\rangle \subset \langle 2, x\rangle \subset \mathbb{Z}[x]$$

**Theorem 7.38.** *Let $D$ be a principal ideal domain. Let $a \in D$ be a non-zero and non-unit element. Then $\langle a\rangle$ is a maximal ideal if and only if $\langle a\rangle$ is irreducible in $D$.*

*Proof.* One direction follows from Theorem 7.36. For the other direction, suppose $a$ is irreducible but $\langle a\rangle$ is not a maximal ideal. Then we have some intermediate ideal $I$ between $\langle a\rangle$ and $D$ and we have some $b$ such that $I = \langle b\rangle$ because $D$ is a principal ideal domain. Therefore, we have $a = bc$ for some $c \in D$. But $a$ is irreducible and so one of $b$ and $c$ is unit. $b$ cannot be unit as we assume that $I$ is not $D$, so $c$ is unit. But then $a \sim b$ and so $\langle a\rangle = \langle b\rangle = I$, which is a contradiction. □

**Theorem 7.39.** *Let $D$ be an integral domain and let $I$ be an ideal of $D$. Then $D/I$ is a field if and only if $I$ is maximal.*

*Proof.* Suppose $D/I$ is a field and let $I \subseteq J \subseteq D$. Then as $J$ is an ideal of $D$, it is a simple matter to check that $J/I \subseteq D/I$. But $D/I$ is a field and so the only ideals in $D/I$ is 0 and $D/I$ itself. Clearly $J/I$ is not 0 and so it must be $D/I$, and so $J = D$.

Conversely, suppose $I$ is a maximal ideal. Take any $b \notin I$ and so $b + I \neq I$. Consider the set

$$B = \{x \in D : x = by + w \text{ for some } y \in D \text{ and some } w \in I\}$$

Then it is clear that $B$ is an ideal of $B$. We can also show that $I \subset B$ (see Exercise 7). Since $I$ is maximal and so we have $B = D$ and so we have some $y \in D$ and $w \in I$ such that

$$1 = by + w$$

Then

$$(b+I)(y+I) = by + I = 1 - w + I = 1 + I$$

which has an inverse and so $D/I$ is a field. □

**Definition 7.40.** *A proper ideal $P$ of an integral domain $D$ is called a* **prime ideal** *if*

$$a, b \in D \text{ and } ab \in P \Rightarrow a \in P \text{ or } b \in P$$

**Example 7.41.** *The principal ideal $I = \langle x^2 + 1 \rangle$ is not a prime ideal of $\mathbb{C}[x]$ as $x \pm i \in \mathbb{C}[x], (x + i)(x - i) = x^2 + 1 \in I$ but $x \pm i \notin I$.*

**Theorem 7.42.** *Let $D$ be an integral domain and let $a$ be a non-zero non-unit element in $D$. Then $\langle a \rangle$ is a prime ideal of $D$ if and only if $a$ is prime in $D$.*

*Proof.* Suppose that $\langle a \rangle$ is a prime ideal of $D$. Let $a|bc$ for some $b, c \in D$ and then $bc \in \langle a \rangle$, but $\langle a \rangle$ is prime and so either $b$ or $c$ is in $\langle a \rangle$, which means $a$ divides either $b$ or $c$.

Conversely, suppose $a$ is prime, and let $bc \in \langle a \rangle$. Then $a|bc$ and $a$ is prime, so $a|b$ or $a|c$, which means either $b$ or $c$ is in $\langle a \rangle$. □

**Theorem 7.43.** *Let $D$ be an integral domain and let $I$ be an ideal of $D$. Then $D/I$ is an integral domain if and only if $I$ is prime.*

*Proof.* Suppose $D/I$ is an integral domain, and let $ab \in I$. Then $(a + I)(b + I) = I$, and so $a + I$ or $b + I = I$, which means either $a$ or $b$ is in $I$.

Conversely, suppose $I$ is prime, and let $(a + I)(b + I) = I$. Then we have $ab \in I$ and so $a \in I$ or $b \in I$ which means either $a + I = I$ or $b + I = I$. Hence $D/I$ is an integral domain. □

**Theorem 7.44.** *Let $D$ be an integral domain. Let $I$ be a maximal ideal of $D$. Then $I$ is a prime ideal of $D$.*

*Proof.* $I$ is maximal, and so $D/I$ is a field, by theorem 7.39 and hence an integral domain. Then by Theorem 7.43. □

**Theorem 7.45.** *Let $D$ be a principal ideal domain and $I$ a proper ideal of $D$. Then $I$ is maximal if and only if $I$ is prime.*

*Proof.* One direction follows from Theorem 7.44. For the other direction, suppose we have some prime ideal $I$ which is not maximal in $D$. Then we have some $J$ such that

$$I \subset J \subset D$$

As $D$ is a principal ideal domain so we may assume, WLOG, that $I = \langle a \rangle$ and $J = \langle b \rangle$. Then we have $b|a$ and so we have some $c$ such that $a = bc$. But $a \in I$ and $I$ is prime so either $b$ or $c$ is in $I$. We assume that $J$ properly contains $I$ so that $b \notin I$. Then $c \in I$ and so we have some $d$ such that $c = ad$. Therefore,

$$a = bc = abd$$

and so $bd = 1$ which means that $b$ is a unit. Then $J = D$, which is a contradiction. Hence $I$ is maximal. □

## 7.6 Sum and products of ideals

**Definition 7.46.** *Let $I$ and $J$ be ideals of an integral domain $D$. The sum of $I$ and $J$, written $I + J$ is defined by:*

$$I + J = \{i + j : i \in I, j \in J\}$$

It is easy to check that the sum of ideals is an ideal. Notice that, as $0 \in I$ we have $I + \langle 1 \rangle = \langle 1 \rangle$.

**Definition 7.47.** *Let $I$ and $J$ be ideals of an integral domain $D$. The product of $I$ and $J$, written $IJ$ is defined by:*

$$\begin{aligned} IJ &= \{x \in D : x = i_1 j_1 + \dots i_r j_r : \text{ for some } r \in N, \\ &\qquad \text{some } i_1, \dots, i_r \in I, \text{ some } j_1, \dots, j_r \in J\} \end{aligned}$$

*and it is not hard to check this is an ideal of $D$.*

**Lemma 7.48.** *For any ideals $I, J, K$ of an integral domain $D$, we have*

$$(I + J)K = IK + JK$$

*Proof.* Take any element on LHS, it has the form

$$a_1 k_1 + \dots a_r k_r$$

where $a_i = b_i + c_i$ with $b_i \in I, c_i \in J$. It can be rearranged as

$$(b_1 k_1 + \dots b_r k_r) + (c_1 k_1 + \dots c_r k_r)$$

which has the form $IK+JK$ and so $(I+J)K \subset IK+JK$. Similarly we can show $IK+JK \subset (I+J)K$ and so they are equal. □

Similarly we can also show that, if $I = \langle a \rangle$ and $J = \langle b \rangle$ then $IJ = \langle ab \rangle$.

**Theorem 7.49.** *Let $P$ be a proper ideal of an integral domain $D$. Then $P$ is a prime ideal if and only if for any two ideals $A$ and $B$ of $D$ with $AB \subset P$, we have either $A \subset P$ or $B \subset P$.*

*Proof.* Suppose we have such $P$ satisfying the above property, and let $ab \in P$. Then the ideal generated by $ab$ lies in $P$ and hence

$$\langle ab \rangle = \langle a \rangle \langle b \rangle \subset P$$

and so we have $\langle a \rangle \subset P$ or $\langle b \rangle \subset P$ and so either $a \in P$ or $b \in P$.

Conversely, suppose we have some $A$ and $B$ such that $AB \subset P$ but $A, B \not\subset P$. Then we have some $a \in A, b \in B$ such that $a, b \notin P$. But $ab \in P$ and so $P$ is not prime. □

**Theorem 7.50.** *Let $D$ and $D_1$ be integral domain satisfying $D \subset D_1$. Let $P$ be a prime ideal of $D_1$ such that $P \cap D \neq \{0\}, D$. Then $P \cap D$ is a prime ideal of $D$.*

*Proof.* We firstly check that $P \cap D$ is an ideal of $D$. Let $a, b \in P \cap D$. Then as $P$ is an ideal of $D_1$, we have $a + b \in P$ and as $a, b \in D$ so $a + b \in D$. So $a + b \in P \cap D$. Let $r \in D$. Then $ar \in D$. Also $r \in D \Rightarrow r \in D_1$, and as $P$ is an ideal of $D_1$ so we have $ar \in P$. Therefore, $ar \in P \cap D$. Hence $P \cap D$ is an ideal of $D$.

Then we check that $P \cap D$ is prime. Let $ab \in P \cap D$ and as $P$ is prime, so WLOG we assume that $a \in P$. But $a \in D$ so $a \in P \cap D$. □

## 7.7 Exercises

1. Show that $1 + i$ is a prime in $\mathbb{Z} + \mathbb{Z}i$.

2. Show that in $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not prime.

3. Show that the ideal $\langle 2, 1 + \sqrt{-7} \rangle$ is not principal in $\mathbb{Z}[\sqrt{-7}]$.

4. Let $A$ and $B$ be ideals of an integral domain $D$. Prove that $AB \subseteq A \cap B$.

5. Let $A$ and $B$ be ideals of an integral domain $D$. Show that
$$(A \cap B)(A + B) \subseteq AB$$

6. Let $p$ be a prime. Let $m$ be an integer with $m \leq -(p+1)$. Prove that $p$ is irreducible in $\mathbb{Z}[\sqrt{m}]$.

7. Prove that the set $B$ defined in Theorem 7.39 is an ideal and $I \subset B$.

8. Let $P$ be a prime ideal of an integral domain $D$. Let $A_1, \ldots, A_k$ be ideals of $D$ such that $P \supseteq A_1 \cdots A_k$. Prove that $P \supseteq A_i$ for some $i \in \{1, 2, \ldots, k\}$.

9. Show that any finite integral domain is a field.

10. Let $D$ be an integral domain and $I, J$ be ideals of $D$ such that
$$I = \langle x_1, \ldots, x_m \rangle, J = \langle y_1, \ldots, y_n \rangle$$
Show that
$$IJ = \langle x_i y_j : 1 \leq i \leq m, 1 \leq j \leq n \rangle$$
(where some of the generators might be redundant.)

## 7.8 Hint and Solutions

1. Suppose $1 + i | (a + bi)(c + di)$ for some $a, b, c, d \in \mathbb{Z}$ and so $(1 + i)(x + iy) = (a + bi)(c + di)$ for some $x, y$. We take the modulus on both sides, so that
$$2(x^2 + y^2) = (a^2 + b^2)(c^2 + d^2)$$
and so at least one of $a^2 + b^2$ and $c^2 + d^2$ is even, and WLOG, say $a^2 + b^2$. If $a$ is even, so is $b$ and so we have $a = 2r, b = 2s$ for some $r$ and $s$ and
$$a + bi = 2(r + si) = (1 + i)((r + s) + (-r + s)i)$$
If $a$ and $b$ are both odd, then $a = 2r + 1, b = 2s + 1$ for some $r$ and $s$ and
$$a + bi = 2(r + si) + (1 + i) = (1 + i)((r + s + 1) + (-r + s)i)$$
Hence $1 + i | a + bi$.

2. Suppose $2 = xy$ in $D = \mathbb{Z}[\sqrt{-5}]$. We may define the norm of an element $a + b\sqrt{-5}$ in $D$ to be $|a + b\sqrt{-5}| = a^2 + 5b^2$. Then if $u$ is a unit in $D$, then $uu^{-1} = 1$ and 1 has norm 1. It is clear that the norm is multiplicative and so the norm of $u$ must be 1 as it is always a positive integer and divides 1. Now as the norm of 2 is 4, so
$$|x||y| = |2| = 4$$
It is also easy to check that we have no element having norm 2, therefore, we must have that either $|x|$ or $|y|$ is 1, WLOG, say $x$. Then the only elements having norm 1 is $\pm 1$ and so 2 is irreducible as $\pm 1$ are units.

   To show 2 is not prime, we have $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 divides neither of them, because if so, we have the norm of 2 divides the norm of $1 \pm \sqrt{-5}$ but clearly 4 does not divide 6.

3. Suppose it is principal, then there exists $a$ such that

$$\langle a \rangle = \langle 2, 1 + \sqrt{-7} \rangle$$

and then $a|2, 1 + \sqrt{-7}$. We use a similar method as above: define the norm of $a + b\sqrt{-7}$ to be $|a + b\sqrt{-7}| = a^2 + 7b^2$. Then if $a|2, 1 + \sqrt{-7}$, we have the norm of $a$ divides the norm of 2 and $1 + \sqrt{-7}$ and so the norm of $a$ divides 4. Then as we have no element with norm 2 so the norm of $a$ is 4 or 1. If $|a| = 4$, then $a = \pm 2$ but clearly, $2 \nmid 1 + \sqrt{-7}$. So $|a| = 1$ and so $a = \pm 1$ which is a unit and then $\langle a \rangle = D$, which is a contradiction because clearly, 3 does not lie in $\langle 2, 1 + \sqrt{-7} \rangle$.

4. Take any element in $AB$, say $a_1b_1 + \ldots a_rb_r$ for some $r$ and $a_i \in A$, $b_i \in B$. But clearly, as $A$ is an ideal, so $a_ib_i \in A$ and so the sum of them still lies in $A$. Similarly, it also lies in $B$ and so it lies in $A \cap B$. Hence $AB \subseteq A \cap B$.

5. Take any element in $(A \cap B)(A + B)$, which can be written as

$$x_1(y_1 + z_1) + \ldots x_r(y_r + z_r) \text{ where } x_i \in A, B, y_i \in A \text{ and } z_i \in B$$

Now we can expand the bracket and notice that $x_iy_1 \in A$ and 1 is always in $B$ so that

$$x_1y_1 + \ldots x_ry_r \in AB$$

Also, $z_i \in B$ and so

$$x_1z_1 + \ldots x_rz_r \in AB$$

Therefore,

$$x_1(y_1 + z_1) + \ldots x_r(y_r + z_r) \in AB$$

because $AB$ is an ideal.

6. As $m < 0$ so we define the norm of $a + b\sqrt{m}$ to be $a^2 - b^2m$. Suppose $p$ is reducible and as $p$ is prime, the norm of $p$ is $p^2$. So $p$ is reducible only if we have some element with norm $p$. But we shall prove this is impossible. Let $a^2 - b^2m = p$ and since $m \leq -(p + 1)$, we have $p = a^2 - b^2m \geq a^2 + (p + 1)b^2$ and so

$$0 \geq a^2 + b^2 + p(b^2 - 1)$$

which is impossible. Therefore, it is irreducible.

7. The set $B = \{x \in D : x = by + w \text{ for some } y \in D \text{ and some w } \in I\}$ Let $x_1, x_2 \in B$ and WLOG, we assume that $x_1 = by_1 + w_1, x_2 = by_2 + w_2$, the

$$x_1 + x_2 = b(y_1 + y_2) + (w_1 + w_2)$$

which still lies in $B$ as $I$ is an ideal. Similarly, let $x \in B$ and $d \in D$, say $x = by + w$. Then $xd = b(yd) + wd$ and $wd \in I$, $yd \in D$. So $xd \in B$. Hence it is an ideal. Finally, it is easy to check that $I \subset B$ because $0 \in D$ and so for each $i \in I$ we have

$$i = b \cdot 0 + i \in B$$

8. This is an immediate application of Theorem 7.49. Having set $A_2 \cdots A_k = B$, we have

$$A_1B \subseteq P \Rightarrow A_1 \subseteq P \text{ or } B \subseteq P$$

because $P$ is prime. Repeat the above and so the result follows.

9. It suffices to show that every non-zero element has an multiplicative inverse. Let $a \in D$ and $a \neq 0$. Define $f_a : D \longmapsto D$ with $f_a(x) = ax$ for all $x \in D$. This is clearly an ring homomorphism and is injective. But $D$ is finite and so it is bijective. Therefore, we have some $x$ such that $ax = 1$.

10. Let $K = \langle x_i y_j : 1 \leq i \leq m, 1 \leq j \leq n \rangle$. It is clear that $K$ is an ideal and $K \subseteq IJ$. Now let $\alpha \in IJ$ then $x = \sum r_i s_j$, $r_i \in I$, $s_j \in J$. Then each $r_i$ can be written as a linear combination of $x_i$ and each $s_j$ can be written as a linear combination of $s_j$. Thus we may recollect the coefficient of each $x_i y_j$ and so it is a linear combination of $x_i y_j$ and so $IJ \subseteq K$. Hence $K = IJ$.

# 8 Algebraic background-Euclidean domain

## 8.1 Euclidean Domains

**Definition 8.1.** *Let $D$ be an integral domain. A function $\phi$ is called an* **Euclidean function** *on $D$ if it satisfies the following:*

1. $\phi : D \longmapsto \mathbb{Z}$. *(In other words, $\phi$ takes values in integers.*

2. $\phi(ab) \geq \phi(a)$, *for all $a, b \in D$ with $b \neq 0$.*

3. *If $a, b \in D$ with $b \neq 0$, then there exists $q, r \in D$ such that $a = qb + r$ and $\phi(r) < \phi(b)$*

**Example 8.2.** *Let $D = F[x]$, where $F$ is a field. Let $p(x) \in D$, then*

$$\phi(p(x)) = \begin{cases} deg(p(x)) & \text{if } p(x) \neq 0 \\ -1 & \text{if } p(x) = 0 \end{cases}$$

*is a Euclidean function on $D$.*

**Lemma 8.3.** *Let $D$ be an integral domain which possesses a Euclidean function $\phi$. Let $a, b \in D$, then:*

*(i)* $a \sim b \Rightarrow \phi(a) = \phi(b)$.

*(ii)* $a|b$ *and* $\phi(a) = \phi(b) \Rightarrow a \sim b$.

*(iii)* $a \in U(D) \iff \phi(a) = \phi(1)$.

*(iv)* $\phi(a) > \phi(0)$ *if* $a \neq 0$.

*Proof.* (i) We have $a = bp$ and $b = aq$ for some $p, q \in D$ and so we have

$$\phi(a) = \phi(bp) \geq \phi(b) \text{ and } \phi(b) = \phi(aq) \geq \phi(a)$$

Therefore, $\phi(a) = \phi(b)$.

(ii) To show $a \sim b$, we have already got $a|b$, so we only need to check $b|a$. We can write $a = qb + r$ with $\phi(r) < \phi(b)$. Suppose $r \neq 0$, then $a|b \Rightarrow a|r$. and so$r = ac$ for some $c$. So $\phi(r) \geq \phi(a) = \phi(b)$, which is a contradiction.

(iii) If $a \in U(D)$, then $a \sim 1$ and so by (i), $\phi(a) = \phi(1)$. Conversely, if $\phi(a) = \phi(1)$, and clearly $1|a$, so by (ii), $a \sim U(1)$ and so $a \in U(D)$.

(iv) We have $0 = qa + r$ for some $q, r \in D$ with $\phi(r) < \phi(a)$. Suppose $r \neq 0$, then $-qa = r$ and so $\phi(r) \geq \phi(a)$ which is a contradiction. Hence $r = 0$ and so $\phi(0) < \phi(a)$.

□

**Definition 8.4.** *Let $D$ be an integral domain. If $D$ possesses a Euclidean function $\phi$, then $D$ is called a* **Euclidean domain** *with respect to $\phi$.*

**Theorem 8.5.** *If $D$ is a Euclidean domain, then $D$ is a principal ideal domain.*

*Proof.* Let $\phi$ be the Euclidean function, and $I$ be an ideal in $D$. Let $a$ be the non-zero element such that $\phi(a)$ is the smallest integer greater than $\phi(0)$. Take any $b \in I$, then we may write $b = qa + r$ with $\phi(r) < \phi(a)$. But by the choice of $a$, we must have $r = 0$. Therefore, $a|b$ for any $b \in I$ and so $I = \langle a \rangle$. □

**Remark 8.6.** *The converse of Theorem 8.5 is not true.*

Also, we shall extend the Euclidean algorithm in Chapter 1 to every Euclidean domain. (In $\mathbb{Z}$, the Euclidean function is $\phi(a) = |a|$, and we can use exactly the same method to prove that Euclidean algorithm gives a way to calculate the greatest common divisor of two elements. We shall see many examples of Euclidean domains in the exercises.

## 8.2 Almost Euclidean domains

**Definition 8.7.** *Let $D$ be an integral domain, a function $\phi : D \longmapsto \mathbb{N} \cup \{0\}$ is called an* **almost Euclidean function** *on $D$ if it satisfies the following:*

1. $\phi(0) = 0$.

2. $\phi(a) > 0$ *for all* $a \in D$ *with* $a \neq 0$.

3. $\phi(ab) \geq \phi(a)$.

4. *if* $a, b \in D$ *with* $b \neq 0$ *then either* $a = bq$ *for some* $q \in D$ *or*

$$0 < \phi(ax + by) < \phi(b)$$

*for some* $x, y \in D$.

It is clear from the definition that if $\phi$ is a Euclidean function satisfying $\phi(0) = 0$ then $\phi$ is an almost Euclidean function.

**Definition 8.8.** *Let $D$ be an integral domain. If $D$ possesses an almost Euclidean function $\phi$ then $D$ is called an* **almost Euclidean domain** *with respect to $\phi$.*

**Theorem 8.9.** *An almost Euclidean domain is a principal ideal domain.*

*Proof.* Let $D$ be an almost Euclidean domain and $\phi$ be an almost Euclidean function. Let $I$ be an ideal of $D$ and take $b$ to be a non-zero element in $I$ such that $\phi(b)$ is the least positive integer. Let $a \in I$, then either $a = qb$ for some $q$ or we have

$$0 < \phi(ax + by) < \phi(b)$$

But this is impossible because $ax + by \in I$, which contradicts the definition of $b$. So we have $b|a$ for any $a \in I$ and so $I = \langle a \rangle$. □

Now we see that an almost Euclidean domain is always a principal ideal domain. In many other context, the definition of Euclidean domain is different from the one we give, but the properties are almost the same.

**Definition 8.10.** *Let $D$ be an integral domain. A function $\phi : D\backslash\{0\} \longmapsto \mathbb{N}$ is called a* **Euclidean function** *if it satisfies the following:*

1. *For all non-zero $a, b$ we have $\phi(a) \leq \phi(ab)$.*

2. *If $a$ and $b$ are in $D$ and $b$ is non-zero, then there are $q, r \in D$ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$.*

It is clear that Definition 8.1 is a more general version, but with not much difference. Readers may use either definition where appropriate.

## 8.3 Exercises

1. Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

2. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

   In the remaining questions, we are going to discuss some properties of the norm function. Formally, Let $m$ be a square free integer, we define the norm $\phi : \mathbb{Q}[\sqrt{m}] \longmapsto \mathbb{Q}$ by:

   $$\phi(a + b\sqrt{m}) = |a^2 - mb^2|$$

   for all $a, b \in \mathbb{Q}$. (Use definition 8.1 in the following question).

3. Show that:

   (i) $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ for all $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$.

   (ii) Let $\alpha \in \mathbb{Q}[\sqrt{m}]$. Then $\phi(\alpha) = 0$ if and only if $\alpha = 0$.

   (iii) $\phi(\alpha\beta) \geq \phi(\alpha)$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$ with $\beta \neq 0$.

4. Let $m \equiv 1 \pmod 4$. Show that

   (i) $\phi : \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \longmapsto \mathbb{N} \cup \{0\}$.

   (ii) $\phi(\alpha\beta) \geq \phi(\alpha)$ for all $\alpha, \beta \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ with $\beta \neq 0$.

5. Let $m$ be a square free integer. Then the integral domain $\mathbb{Z}[\sqrt{m}]$ is Euclidean with respect to $\phi$ if and only if for all $x, y \in \mathbb{Q}$, there exists $a.b \in \mathbb{Z}$ such that

   $$\phi((x + y\sqrt{m}) - (a + b\sqrt{m})) < 1$$

6. Using question 5, deduce that if $m$ is a negative square free integer, then $\mathbb{Z}[\sqrt{m}]$ is Euclidean with respect to $\phi$ if and only if $m = -1, -2$.

7. Let $m \equiv 1 \pmod 4$. Show that $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ is Euclidean with respect to $\phi$ if and only if for all $x, y \in \mathbb{Q}$, there exist $a, b \in \mathbb{Z}$ such that

   $$\phi\left((x + y\sqrt{m}) - \left(a + b\left(\frac{1+\sqrt{m}}{2}\right)\right)\right) < 1$$

   Hence, prove that if $m$ is a negative square free integer, then $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ is Euclidean with respect to $\phi$ only if $m = -3, -7, 11$.
   (The converse is also true, and is not hard to check, but it takes some time).

## 8.4 Hint and Solutions

1. Define the norm of $a+b\sqrt{-2}$ to be $a^2+2b^2$. Take $\phi$ to be the norm function. It is clear that $\phi$ is multiplicative and so for any non-zero elements $\alpha, \beta$, we have $\phi(\alpha\beta) \geq \phi(\alpha)$. Now for any $a+b\sqrt{-2}$ and $c+d\sqrt{-2}$,

2.

3. (i) Let $\alpha = a+b\sqrt{m}, \beta = c+d\sqrt{m}$, then $\alpha\beta = (ac+bdm)+(ad+bc)\sqrt{m}$. We have

$$\phi(\alpha\beta) = |(ac+bdm)^2 - m(ad+bc)^2| = |a^2-b^2m||c^2-d^2m|$$

   (ii) Suppose $\alpha = 0$, then by definition $\phi(\alpha) = 0$. Conversely, if $\alpha = a+b\sqrt{m}$ and $\phi(\alpha) = 0$, then we have $a^2 = mb^2$. But we assumed that $m$ is square free so that $a = b = 0$.

   (iii) Let $\beta \neq 0$, then by (i)

$$\phi(\alpha\beta) = \phi(\alpha)\phi(\beta) \geq \phi(\alpha)$$

   because $\phi(\beta)$ is integer and by (ii) is not zero.

4. (i) Let $\alpha = a+b(\frac{1+\sqrt{m}}{2})$ and so

$$\phi(\alpha) = \left|\left(a+\frac{b}{2}\right)^2 - m\frac{b^2}{4}\right|$$

   But $\frac{b^2}{4}(1-\frac{m}{4})$ is an integer as $m \equiv 1 \pmod 4$. So it is clear that the range of $\phi$ is non-negative integer. Also $0 \in D$ and $\phi(0) = 0$.

   (ii) Notice that $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ is a subdomain of $\mathbb{Q}[\sqrt{m}]$ and so by the previous question, the result follows immediately.

5. Suppose it is an Euclidean domain with respect to $\phi$, then for any $x, y \in \mathbb{Q}$, let $x+y\sqrt{m} = \frac{r+s\sqrt{m}}{t}$, where $(r,s,t) = 1$. Then we have some $\alpha, \beta$ such that

$$r+s\sqrt{m} = t\alpha+\beta \text{ where } \phi(\beta) < \phi(t)$$

   Hence, writing $\alpha = a+b\sqrt{m}$, we have

$$\phi(x+y\sqrt{m}-(a+b\sqrt{m})) = \phi\left(\frac{\beta}{t}\right)$$

   and by multiplicative property, we have $\phi(\frac{\beta}{t}) < 1$.

   Conversely, suppose for each $x, y \in \mathbb{Q}$, we have $a, b \in \mathbb{Z}$ such that the condition holds. Then for each pairs $\alpha = r+s\sqrt{m}$ and $\beta = u+v\sqrt{m}$ with $\beta \neq 0$, let

$$x+y\sqrt{m} = \frac{\alpha}{\beta}$$

   and so we may simplify the above:

$$x = \frac{ru-msv}{u^2-mv^2}, y = \frac{su-rv}{u^2-mv^2}$$

   We have $a, b \in \mathbb{Z}$ such that

$$\phi(x+y\sqrt{m}-(a+b\sqrt{m})) < 1$$

Let $c, d \in \mathbb{Z}$ such that

$$\alpha = (a + b\sqrt{m})\beta + (c + d\sqrt{m})$$

and we may write $c + d\sqrt{m} = \beta(x + y\sqrt{m} - (a + b\sqrt{m})$.

$$\phi(c + d\sqrt{m}) = \phi(\beta)\left(\phi\left(x + y\sqrt{m} - (a + b\sqrt{m})\right)\right) < \phi(\beta)$$

It is also clear that $\phi(\alpha\beta) \leq \phi(\alpha)$ by multiplicative property.

6. By question 1, $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. The case when $m = -1$ can be shown in a similar manner. Conversely, if it is a Euclidean domain, by question 5, we pick $x, y = \frac{1}{2}$. Then we should have some $a, b \in \mathbb{Z}$ such that

$$\phi\left(\frac{1}{2} + \frac{1}{2}\sqrt{m} - (a + b\sqrt{m})\right) < 1$$

then we have

$$\left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2 < 1$$

For any integer $a$, we have $(\frac{1}{2} - a)^2 \geq \frac{1}{4}$, and as $-m > 0$, we have

$$\frac{1}{4} - \frac{1}{4}m \leq \left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2 < 1$$

and so $m > -3$ we have $m = -1, -2$.

7. We can always write

$$x + y\sqrt{m} = \frac{r + s\left(\frac{1+\sqrt{m}}{2}\right)}{\frac{1+\sqrt{m}}{2}t}$$

for suitable $s, r$ and $t \in \mathbb{Z}$. The one direction of the proof follows immediately in exactly the same argument of question 6. The other half follows by writing

$$\frac{r + s\left(\frac{1+\sqrt{m}}{2}\right)}{u + v\left(\frac{1+\sqrt{m}}{2}\right)} = x + y\sqrt{m}$$

and define $c, d$ in a similar way as in question 6.

Finally, pick $a = b = \frac{1}{2}$, and use the fact that $(\frac{1}{4} - x)^2 \geq \frac{1}{16}$, so we have $m > -15$ if we follow the same procedure of question 6. Use $m \equiv 1 \pmod 4$ and so the result follows.

# 9 Algebraic background-Noetherian domain

## 9.1 Noetherian domains

Suppose we have an integral domain $D$, and let $a_i$ be non-zero elements. Let $A_i$ be the ideals generated by $\{a_1, \ldots, a_i\}$. Clearly, we have

$$A_1 \subseteq A_2 \ldots \subseteq A_n \subseteq \ldots$$

Is it going to stop at some stage? Or it goes on to infinity?

**Definition 9.1.** *An infinite sequence of ideals $\{I_n : n = 1, 2, \ldots\}$ in an integral domain is said to be an* **ascending chain** *if*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

*The chain is said to be a strictly ascending chain if*

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

**Definition 9.2.** *An ascending chain of ideals*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

*in an integral domain is said to* **terminate** *if there exists a positive integer $n_0$ such that*

$$I_n = I_{n_0} \text{ for all } n \geq n_0$$

**Definition 9.3.** *An integral domain $D$ is said to satisfy the* **ascending chain condition** *if every ascending chain of ideals in $D$ terminates. Equivalently, $D$ does not contain a strictly ascending chain of ideals.*

**Definition 9.4.** *An integral domain which satisfies the ascending chain condition is called a* **Noethetian domain**. *More generally, we define a Noetherian ring to be a ring $R$ in which every ascending chain of ideals in $R$ terminates.*

**Example 9.5.** *$\mathbb{Z}$ is a Noetherian domain because it is a Euclidean domain and hence principal ideal domain. Also $\langle a \rangle \subseteq \langle b \rangle$ if and only if $b|a$, and if*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

*we have only finitely many divisors of $I_1$ and so the chain must terminate.*

**Theorem 9.6.** *Let $D$ be an integral domain. Then $D$ is Noetherian if and only if every ideal of $D$ is finitely generated.*

*Proof.* Let $D$ be a Noetherian domain. Suppose we have some ideal $I$ in $D$ which is not finitely generated and we may pick any non-zero $a_1 \in I$ and let $I_1$ in $D$. For $n \geq 2$, having got $I_{n-1}$, we pick $a_n$ to be the element in $I$ such that $a_n \notin I_{n-1}$ and let the ideal $I_n$ contains both $I_{n-1}$ and $a_n$. In other words, $I_n = \langle a_1, \ldots, a_n \rangle$. Thus we have

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

which is an strictly ascending chain and so $D$ is not Noetherian, which is a contradiction.

Conversely, suppose every ideal in $D$ is finitely generated. Then let

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

be an ascending chain of ideals in $D$. Let $I = \bigcup_{i=1}^{\infty} I_i$ and it is easily checked that this is an ideal of $D$ and by assumption this is finitely generated, say by $a_1, \ldots, a_N$, and let $a_i \in I_{n_i}$ and set $n_0 = \max_i(n_i)$. Then for any $n \geq n_0$, we have

$$I = \langle a_1, \ldots, a_N \rangle \subseteq I_n \subseteq I$$

and so $I_n = I = I_{n_0}$ for all $n \geq n_0$. □

**Theorem 9.7.** *Let $D$ be a principal ideal domain, then $D$ is a Noetherian domain.*

*Proof.* This follows immediately from Theorem 9.6 as every ideal is generated by one element. □

**Definition 9.8.** *An integral domain $D$ is said to satisfy the* **maximal condition** *if every non-empty set $S$ of ideals in $D$, there exists an ideal $I$ such that for all $J \in S$, if $I \subseteq J$, then $I = J$.*

**Theorem 9.9.** *Let $D$ be an integral domain. Then $D$ is Noetherian if and only if it satisfies the maximal condition.*

*Proof.* Suppose $D$ does not satisfy the maximal condition. Then we have some set $S$ of ideals in $D$ and for each $I \in S$, we have some $J \in S$ such that $I \subset J$. Then we may construct an infinite strictly increasing chain and so $D$ is not Noetherian.

Conversely, let $D$ be an integral domain which satisfies the maximal condition. Let

$$I_1 \subseteq I_2 \subseteq \dots$$

be an ascending chain of ideals in $D$. Let $S$ be the set which contains every $I_n$. Then $S$ contains some $I_{n_0}$ such that if $I_{n_0} \subseteq I_j$ then $I_{n_0} = I_j$. Therefore, we have $I_n = I_{n_0}$ for all $n \geq n_0$. □

We end the subsection by a famous theorem:

**Theorem 9.10. Hilbert Basis Theorem** *Let $R$ be a Noetherian ring, then $R[x]$ is also Noetherian.*

*Proof.* □

**Corollary 9.11.** *Let $R$ be a Noetherian ring, then $R[X_1, X_2, \dots]$ is also Noetherian.*

*Proof.* We apply induction on $n$. For $n = 1$, use Theorem 9.10. Suppose true for $n-1$, $n \geq 2$, then $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$ and we know $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}]$ is Noetherian, and so by the case when $n = 1$, we have $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$ Noetherian. □

## 9.2 Factorisation domain and unique factorisation domains

Let $D$ be a field. Then $D$ does not contain any irreducible element as every non-zero element is a unit. What about integral domain? Does every integral domain which is not a field necessarily have at least one irreducible element? We will see (exercise 4) some examples of integral domain, which is not a field, yet does not contain any irreducible element. But we have:

**Theorem 9.12.** *Let $D$ be an Noetherian domain, which is not a field. Then $D$ contains elements that are irreducible.*

*Proof.* Suppose not. $D$ contains no irreducible element. As we assume that $D$ is not a field, so $D$ contains non-zero, non-unit elements. Let $a$ be one of these. Then $a$ is reducible, say $a = a_1 b_1$. By assumption, $a_1$ is not irreducible and is not unit. So $a_1$ is reducible, say $a_1 = a_2 b_2$ and so on. This process will never terminate. Also $a \nmid a_1$ because $a_2$ is not unit. Then we have a strictly ascending chain

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \dots$$

which is a contradiction as $D$ is Noetherian. □

**Definition 9.13.** *Let $D$ be an integral domain. Then $D$ is called a* **factorisation domain** *if every non-zero, non-unit element of $D$ can be expressed as a finite product of irreducible elements of $D$.*

**Theorem 9.14.** *Let $D$ be a Noetherian domain. Then $D$ is a factorisation domain.*

*Proof.* Suppose $D$ is Noetherian. Take any non-zero, non-unit element $a$. If $a$ is irreducible, then we are done. If not, we may write $a = a_1b_1$, both of which are non-unit. If $a_1, b_1$ can both be written as a finite product of irreducibles, so is $a$. If not, say $a_1$ cannot be written as a finite product of irreducibles, then $a_1$ itself is not irreducible and $a_1 = a_2b_2$. Notice that $a \nmid a_1$ as $b_1$ is not unit. Continue this and so at each stage if we assume $a_i$ is not a finite product of irreducibles, then the process will not terminate and

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \dots$$

is a strictly ascending chain, which contradicts $D$ being Noetherian. Therefore, the original assumption for $a_1, b_1$ is not true and so $a$ is a finite product of irreducibles. □

**Theorem 9.15.** *Let $D$ be a principal ideal domain. Then $D$ is a factorisation domain.*

*Proof.* If $D$ is a principal ideal domain, then it is Noetherian and so is a factorisation domain by Theorem 9.14. □

In $\mathbb{Z}$, we know that every positive integer greater than 1 can be written uniquely as a product of prime numbers. Is this necessarily true in any factorisation domain? Is every factorisation necessarily unique? Here is an example

**Example 9.16.** *In $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and $2, 3, 1 \pm \sqrt{-5}$ are all irreducibles by considering the norm.*

Thus, we may introduce the following concept:

**Definition 9.17.** *Let $D$ be a factorisation domain. Suppose that every non-zero, non-unit element in $D$ can be uniquely (up to modulo units) expressed into a finite product of irreducibles, then $D$ is called a* **unique factorisation domain**.

**Theorem 9.18.** *Let $D$ be a principal ideal domain. Then $D$ is a unique factorisation domain.*

*Proof.* Suppose $D$ is a principal ideal domain, then it is a factorisation domain by Theorem 9.15. So we want to show the factorisation is unique. Let $a = p_1p_2 \dots p_n = q_1q_2 \dots q_m$ be factorisations into irreducibles. Then by theorem 7.30, any irreducible element in a principal ideal domain is prime. Thus we have $p_1 | q_1q_2 \dots q_m$ and so $p_1 | q_j$ for some $j$. But $q_j$ is irreducible and so writing $q_j = p_1u_j$ we have $u_j \in U(D)$ and then we may rearrange $q_i$ so that $q_j$ is $q_1$ above. Hence

$$p_2p_3 \dots p_n = q_2q_3 \dots q_mu_1$$

Continue this, and so we must have $m = n$ because, if not, say $n > m$, we will have

$$1 = u_1 \dots u_nq_{n+1} \dots q_m$$

which is impossible because this implies that $q_j$ is unit. Then $m = n$ and $p_i \sim q_i$ and so the factorisation is unique up to modulo units. □

**Remark 9.19.** *The converse is not true. For example, $\mathbb{Z}[X]$ is a unique factorisation domain but it contains $\langle 2, X \rangle$ which is not principal.*

**Theorem 9.20.** *Let $D$ be a unique factorisation domain. Then an element of $D$ is irreducible if and only if it is prime.*

*Proof.* A prime is always irreducible by Theorem 7.20. Now let $p$ be irreducible in $D$. Let $p | ab$ then we may write $ab = pc$ for some $c \in D$. Then as $D$ is a unique factorisation domain, we may write

$$a = a_1a_2 \dots a_k, b = b_1b_2 \dots b_m, c = c_1c_2 \dots c_n$$

where the factorisation is unique up to modulo units. Then we must have $p \sim a_i$ or $p \sim b_j$ for some $a_i$ or $b_j$ because $p$ is irreducible. WLOG, say $p \sim a_i$, then $p | a_i$ and $a_i | a$ so we have $p | a$ and hence $p$ is prime. □

What does a factorisation tell us? Consider $a_1, \ldots, a_n$ non-zero elements in a unique factorisaiton domain. Let $\{p_1, \ldots, p_k\}$ be a set of irreducibles such that:

1. Each $p_i$ divides at least one of $a_1, \ldots, a_n$.

2. $p_i \not\sim p_j$.

3. If $p$ is any irreducible which divides at least one of $a_1, \ldots, a_n$, then $p \sim p_i$ for some $i$.

In other words, these are all possible irreducible factors of $a_1, \ldots, a_n$ modulo units. Then we have, for each $i$, that

$$a_i = u_i \prod_{j=1}^{k} p_i^{e_{ij}} \text{ where } e_{ij} \geq 0$$

and let $e_j = \min_{1 \leq i \leq n} e_{ij}, j = 1, 2 \ldots, k$. Define

$$a = \prod_{j=1}^{k} p_j^{e_j}$$

By construction, we have $a | a_i$ for all $i$, and if $b | a_i$ for all $i$, we have $b | a$. Thus we shall see that $a$ is the greatest common divisor of $a_1, \ldots, a_k$, and since the factorisation is defined up to modulo units, so the greatest common divisor is also unique up to modulo units.

In a principal ideal domain $D$, a greatest common divisor $a$ of $a_1, \ldots, a_k$ is always a linear combination of $a_1, \ldots, a_k$ with coefficients in $D$ (This is because the generator of the ideal containing these elements is the greatest common divisor). But this is not necessarily the case in a unique factorisation domain.

**Example 9.21.** *Let $D = \mathbb{Z}[X]$, which is a unique factorisation domain. The greatest common divisor of $2x$ and $3x^2$ is $x$ but we are not able to write $x$ as a linear combination of $2x$ and $3x^2$ with coefficients in $\mathbb{Z}[X]$.*

**Theorem 9.22.** *A principal ideal domain is an almost Euclidean domain.*

*Proof.* Let $D$ be a principal ideal domain. Then it is a unique factorisation domain by Theorem 9.18. We shall define the function $\phi$ as follows and check it is an almost Euclidean function.

$$\phi(a) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \in U(D) \\ 2^n & \text{if } a \notin U(D) \text{ and } a = p_1 \ldots p_n \text{ where } p_1, \ldots, p_n \text{ are irreducibles} \end{cases}$$

It is clear that $\phi$ is well-defined because the factorisation is unique up to modulo units and it is easy to check that $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in D$. Therefore, $\phi(ab) \geq \phi(a)$ if $b \neq 0$. So it remains to check that for each $a, b \in D$, $b \neq 0$, one of the following holds:

1. $a = bq$ for some $q \in D$

2. There exists $x, y \in D$ such that
$$0 < \phi(ax + by) < \phi(b)$$

Take any $a, b \in D$ with $b \neq 0$ and let $I = \langle a, b \rangle = \langle c \rangle$ for some $c$ because $D$ is a principal ideal domain. Suppose $a \neq bq$ for any $q \in D$, then $I \neq \langle b \rangle$. Since $b \in I$, so $b = cd$ for some $d \notin U(D)$ because $I \neq \langle b \rangle$. Thus we have

$$\phi(b) = \phi(cd) = \phi(c)\phi(d) > \phi(c)$$

But $c \in I$ and so there exist $x, y$ such that $ax + by = c$ and so we have $x, y$ such that

$$0 < \phi(ax + by) = \phi(c) < \phi(b)$$

□

**Theorem 9.23.** **[Greene's Theorem]** *An integral domain is a principal ideal domain if and only if it is an almost Euclidean domain.*

*Proof.* Combine Theorem 8.9 and Theorem 9.22 □

# 10 Algebraic background-Modules

## 10.1 Modules

**Definition 10.1.** *Let $R$ be a ring with identity and $M$ and additive Abelian group. A function $f : R \times M \longmapsto M$ is called an $R$-**action** on $M$ if it has the following properties:*

1. $f(r+s, m) = f(r, m) + f(s, m)$.

2. $f(r, m+n) = f(r, m) + f(r, n)$.

3. $f(r, f(s, m)) = f(rs, m)$.

4. $f(1, m) = m$.
   *for all $r, s \in R$ and $m, n \in M$.*

**Definition 10.2.** *Let $R$ a ring with identity. An additive Abelian group $M$ together with an $R$-action on $M$ is called an $R$-**module**.*

In fact, what we defined above is a left $R$-module since we can see the action is on the left. We can define the right $R$-module in a similar notion. Unless otherwise stated, the $R$-action in this book will be defined on the left. To make the notation simpler, we may write $rm$ as $f(r, m)$.

**Lemma 10.3.** $(-r)m = -(rm) = r(-m)$

*Proof.* $(-r)m + rm = (-r + r)m = 0 \cdot m = 0$. So $(-r)m = -(rm)$. Similarly, $r(-m) = r(-1 \cdot m) = (r \cdot (-1))m = (-r)m$ □

**Example 10.4.** *Let $F$ be a field. Then an $F$-module is the same as a vector space over $F$.*

**Example 10.5.** *Any additive Abelian group $A$ can be thought of as a $\mathbb{Z}$-module in a nartural way. The $\mathbb{Z}$-action on $A$ is just the map $(n, a) \mapsto na$ from $\mathbb{Z} \times A$ to $A$.*

**Example 10.6.** *Any ring $R$ with identity can be thought of as a module over itself in a natural way. The $R$-action is just the mao $(a, b) \mapsto ab$ from $R \times R$ to $R$.*

**Definition 10.7.** *Let $M$ be an $R$-module. A subgroup $N$ of $M$ is called a* **submodule** *of $M$ if $rn \in N$ for all $r \in R$, $n \in N$.*

**Example 10.8.** *Let $V$ be a vector space over $F$ and so $V$ is an $F$-module. Then any subspace of $V$ is a submodule of $V$.*

**Definition 10.9.** *If $N$ is a submodule of $M$, then the quotient module $M/N$ is the (additive) quotient group with elements $m + N, m \in M$ and the action is defined by*

$$R \times M/N \longmapsto M/N \text{ by } (r, m+N) \mapsto rm + N.$$

*It is well-defined since $N$ is a submodule.*

**Definition 10.10.** *Let $M, N$ be $R$-modules, $\theta : M \longmapsto N$ is an $R$-module homomorphism if*

$$\theta(m_1 + m_2) = \theta(m_1) + \theta(m_2), \theta(rm) = r\theta(m), \forall m_i \in M, r \in R.$$

*The image of $\theta$ is a submodule of $N$. The kernel is*

$$\ker \theta = \{m \in M : \theta(m) = 0\}$$

*and it is a submodule of $M$. If $\theta$ is bijective, then we say $\theta$ is an isomorphism.*

**Example 10.11.** *Take $a \in R$, then the map*

$$\theta_a : M \longmapsto M \text{ by } \theta_a(m) = am$$

*is an $R$-module homomorphism.*

**Theorem 10.12.** *Let $\theta : M \longmapsto N$ be an $R$-module homomorphism, then*

$$M/\ker\theta \cong Im\theta \subset N.$$

The proof is identical to the first isomorphism theorem of rings or groups.
Note that for $N \subset M$ we have a bijection that

$$\{\text{submodules of } M/N\} \longleftrightarrow \{\text{submodules of } M \text{ containing } N\}.$$

If $N \subset L \subset M$, then $\frac{M/N}{L/N} \cong M/L$.

**Definition 10.13.** *Let $M$ be an $R$-module. The* **annihilator** *of an element $m \in M$ is*

$$Ann(m) = \{r \in R : rm = 0\}.$$

*The* **annihilator** *of $M$ is*

$$Ann(M) = \{r \in R : rm = 0 \ \forall m \in M\}.$$

*It is easy to check that $Ann(m)$,$Ann(M)$ are both ideals of $R$.*

**Definition 10.14.** *For $m \in M$, the submodule of $M$ generated by $m$ is the smallest submodule containing $m$, given by $Rm = \{rm : r \in R\}$. More generally, if $X$ is a subset of an $R$-module $M$ then the submodule generated by $X$ is the smallest submodule of $M$ containing $X$. The definition is well-defined because any intersection of submodules is still a submodule.*

**Lemma 10.15.** *Let $X$ be a non-empty subset of $M$. The submodule of $M$ generated by $X$ has the form*

$$\left\{\sum_{i=1}^{n} r_i x_i : r_i \in R, x_i \in X, n \geq 1\right\}$$

*Proof.* This is clearly a submodule of $M$ and it contains the set $X$. Now Let $Y$ be the submodule which contains $X$. Then it contains every element of the form

$$\sum_{i=1}^{n} r_i x_i : r_i \in R, x_i \in X, n \geq 1$$

because $Y$ is a submodule. Therefore the submodule generated by $X$ has the above form. □

**Definition 10.16.** *An $R$-module $M$ is called* **finitely generated** *if $M$ is generated by some finite set of elements of $M$.*

**Lemma 10.17.** *$Rm \cong R/Ann(m)$.*

*Proof.* Consider $R$ as an $R$-module and apply the isomorphism theorem to the map

$$\theta : R \longmapsto Rm \text{ by } \theta(r) = rm.$$

□

## 10.2 Direct Sum, Free Modules

**Definition 10.18.** *Given some $R$-modules $M_1, \ldots, M_k$ the* **external direct sum**, *written $M_1 \oplus \cdots \oplus M_k$ is $\{m_1, \ldots, m_k\}$, $m_i \in M_i$ and we have the pairwise operation, namely*

$$(m_1, \ldots, m_k)+(m_1', \ldots, m_k') = (m_1+m_1', \ldots, m_k+m_k'), (m_1, \ldots, m_k)(m_1', \ldots, m_k') = (m_1m_1', \ldots, m_km_k').$$

**Definition 10.19.** *Let $M$ be an $R$-module and $S = \{m_1, \ldots, m_k\}, m_i \in M$. We say $S$ is an independent set if the only solution $\{r_i\}$ such that$r_1m_1 + \cdots + r_km_k = 0$ is $r_1 = \ldots = r_k = 0$.*

**Definition 10.20.** *Let $M$ be an $R$-module. We say a set $S \subset M$ generates $M$ freely if $S$ generates $M$ and every map $\psi : S \longmapsto N$ for $N$ an $R$-module extends to an $R$-module homomorphism $\theta : M \longmapsto N$. $S$ is called a basis of $M$.*

**Remark 10.21.** *The extension in the above definition is unique. Suppose $\theta_1, \theta_2$ are both extensions, take $\theta = \theta_1 - \theta_2$. So $S$ lies in the kernel of $\theta$. But $M$ is generated by $S$ and so $M$ is the kernel, which says that the image of $\theta$ is $0$ and so $\theta = 0$.*

**Proposition 10.22.** *Suppose $S = \{m_1, \ldots, m_k\} \subset M$, then the following are equivalent:*

*(i) $S$ generates $M$ freely.*

*(ii) $S$ generates $M$ and $S$ is independent.*

*(iii) Every element in $M$ is uniquely expressed as $r_1m_1 + \cdots + r_km_k$ for some $r_i$.*

*Proof.* (i)⇒(ii): Let $r_1m_1 + \cdots + r_km_k = 0$. Let $N = R^k$ an $R$-module where $R^k$ means $R \oplus R \cdots \oplus R$. Define the map

$$\psi : S \longmapsto R^k$$

by sending $m_i$ to $(0, 0, \ldots, 1, \ldots, 0)$ where the only non-zero entry 1 is in the $i^{\text{th}}$ position.

Let $\theta : M \longmapsto R^k$ be the homomorphism given by

$$\theta(r_1m_1 + \cdots + r_km_k) = (r_1, \ldots, r_k).$$

This is well-defined because $S$ generates $M$ freely so the extension is well-defined. Then

$$(0, \ldots, 0) = \theta(0) = \theta(r_1m_1 + \cdots + r_km_k) = (r_1, \ldots, r_k)$$

and so $r_1 = \ldots = r_k = 0$ is the only solution.

(ii)⇒(iii): Let $S$ generate $M$ and $S$ is independent. So firstly every element can be written as $r_1m_1 + \cdots + r_km_k$ so we need to check uniqueness.

Suppose $r_1m_1 + \cdots + r_km_k = r_1'm_1 + \cdots + r_k'm_k$ then

$$(r_1 - r_1')m_1 + \cdots + (r_k - r_k')m_k = 0.$$

By independence, $r_i = r_i'$ for all $i$.

(iii)⇒(i): If every element can be written uniquely in such form, then $S$ generates $M$. Let $\psi : S \longmapsto N$ be any map. Define

$$\theta : M \longmapsto N \text{ by } \theta(r_1m_1 + \cdots + r_km_k) = r_1\psi(m_1) + \cdots + r_k\psi(m_k).$$

This is well-defined because the expression $r_1m_1 + \cdots + r_km_k$ is unique. □

**Example 10.23.** *Let $R = \mathbb{Z}, \{2, 3\}$ is a generating set for $\mathbb{Z}$, but it is not independent, because $2 \times 3 - 3 \times 2 = 0$. $\{2\}$ is independent but not a generating set.*

**Proposition 10.24.** *Let $M$ be an $R$-module, $M$ is freely generated by $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$, then $n = m$.*

*Proof.* Suppose $m \geq n$. Let $A$ be $m \times n$ matrix given by

$$v_j = \sum_{i=1}^{m} A_{ij} u_i.$$

Define $B$ to be an $n \times m$ matrix with

$$u_k = \sum_{j=1}^{n} B_{jk} v_j.$$

So we have

$$u_k = \sum_{i=1}^{n} \sum_{j=1}^{m} (A_{ij} B_{jk}) u_i = \sum_{i=1}^{m} (AB)_{ik} u_i.$$

But $\{u_1, \ldots, u_m\}$ is independent so $AB = id$.

If $m > n$ then extend $A$ to be a square $m \times m$ matrix by inserting columns with entries 0. Similarly, extend $B$ to a $m \times m$ matrix by inserting rows with entries 0. Then we have

$$(A|0) \begin{pmatrix} B \\ 0 \end{pmatrix} = id.$$

This is impossible, and so $m = n$. □

**Proposition 10.25.** *Let $M$ be an $R$-module generated by $\{m_1, \ldots, m_k\}$. Then there is a surjective homomorphism*

$$\theta : R^k \longmapsto M$$

*and so $M \cong R^k / \ker \theta$.*

*Proof.* Define

$$\theta : R^k \longmapsto M \text{ by } \theta(r_1, \ldots, r_k) = r_1 m_1 + \cdots + r_k m_k.$$

Clearly it is surjective and it is a homomorphism. □

**Definition 10.26.** *The kernel in the previous proposition is called the* **relation module** *$N \subset R^k$. It depends on the choice of generators. For $(r_1, \ldots, r_k) \in N$, we say $r_1 m_1 + \cdots + r_k m_k = 0$ is a relation in $M$. $M$ is* **finitely presented** *if it is freely generated by $S$ and the corresponding relation module is finitely generated.*

## 10.3 Matrices Over Euclidean Domain, Smith Normal Form

**Definition 10.27.** *The elementary operation of the matrix $A$ is one of the followings:*

*(i) Add $c$ times $j^{th}$ row to the $i^{th}$ row $i \neq j$.*

*(ii) Interchange $i^{th}$ row and $j^{th}$ row.*

*(iii) Multiply the $i^{th}$ row by a unit $n \in R$.*

*Note that these operations are reversible.*

**Lemma 10.28.** *Let $M$ be a free $R$-module of rank $m$ over an Euclidean domain $R$, $N \subset M$. Then $N$ is freely generated.*

*Proof.* $M \cong R^m$. Let $I = \{r_1 \in R : (r_1, \ldots, r_m) \in N \text{ for some } r_2, \ldots, r_m \in R\}$. It is easy to check $I$ is an ideal of $R$. Since $R$ is a Euclidean domain so it is a principal ideal domain and so we may assume $I = \langle a_1 \rangle$. Choose $n_1 = (a_1, \ldots, a_m) \in N$. Then for any $(r_1, \ldots, r_m) \in N$ we have $r_1 = ra_1$ for some $r \in R$. Thus,

$$(r_1, \ldots, r_m) - r(a_1, \ldots, a_m) = (0, r_2 - ra_2, \ldots, r_n - ra_n) \in N.$$

Let $H = \{(0, r_2, \ldots, r_m) \in N\} \subset \{(0, r_2, \ldots, r_m) \subset R^m\} \cong R^{m-1}$. Now use induction on $m$, so we may assume that $H$ is freely generated by $n_2, \ldots, n_s$ and so $N$ is freely generated by $n_1, \ldots, n_s$ (The case $m = 1$ is clear as $R$ is a principal ideal domain). □

**Theorem 10.29.** **[Smith Normal Form]** *If $A$ is a matrix with entries in a principal ideal domain $R$, then there are invertible matrices $P$ and $Q$ over $R$ such that $PAQ$ is in Smith normal form, which is diagonal with entries $d_1, \ldots, d_n$ such that $d_1 \big| d_2 \cdots \big| d_n$.*

*Proof.* We firstly show that we can diagonalise the matrix. We may assume $A_{11}$ is non-zero, otherwise we can swap columns or rows. For any $a, b \in R$, we know that there exists $c, d$ such that

$$ac + bd = e$$

where $e$ is the highest common factor of $a$ and $b$. Let $a = \alpha e, b = \beta e$. Then

$$1 = \alpha c + \beta d$$

and so

$$\begin{pmatrix} c & d \\ -\beta & \alpha \end{pmatrix}^{-1} = \begin{pmatrix} \alpha & -d \\ \beta & c \end{pmatrix}.$$

Now observe that

$$\begin{pmatrix} c & d \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a & * \\ b & * \end{pmatrix} = \begin{pmatrix} e & * \\ -a\beta + b\alpha & * \end{pmatrix}.$$

So let $A_{11} = a$ and for any non-zero $b$ in the first column, say $A_{1j}$, we can multiply $A$ by a matrix which is identity with the above $2 \times 2$ matrix inserted in the first and $j^{\text{th}}$ row. Note that $-a\beta + b\alpha$ is divisible by $e$.

Similarly, we can do this for all $A_{1j}$ so that $A_{11}$ divides each element of the first column. We then clear the first column so that the only non-zero entry is $A_{11}$. Now repeat the above for the first row (multiply an invertible matrix on the right). It will probably result in the case that the zero entries in the first column become non-zero again. Then we again repeat this for the first column and so on.

Note that every principal ideal domain is Noetherian, and each time when we repeat the above process (either for column or row), $A_{11}$ becomes a factor of the previous $A_{11}$. So this must terminate because any ascending chain in Noetherian ring is going to terminate. Thus, after the above process, we have made the first row and the first column zero except $A_{11}$.

Now repeat this for $A_{22}$ and so on and we end up with a matrix which is diagonal with entries $a_1, a_2, \ldots, a_n$. Finally, if $a_1 \nmid a_2$, we can add the second row to the first row and then use the previous method so that $a_1$ becomes the highest common factor of $a_1$ and $a_2$. By doing this, the matrix can be reduced with entries $d_1, \ldots, d_n$ with $d_1 \big| d_2 \cdots \big| d_n$. □

**Theorem 10.30.** *Let $R$ be a Euclidean domain. $R^m$ is a free module of rank $m$ and let $N \subset R^m$. Then there exists $v_1, \ldots, v_m \in R^m$ and $d_1, \ldots, d_r \in R$ such that*

*(i) $R^m$ is finitely generated by $\{v_1, \ldots, v_m\}$.*

*(ii) $N$ is freely generated by $d_1v_1, \ldots, d_rv_r$.*

*(iii)* $d_1 \big| d_2 \cdots \big| d_r$.

*Proof.* By previous lemma, say $N$ is freely generated by $x_1, \ldots, x_n$. Write these as columns of an $m \times n$ matrix $A$. In other words,

$$x_i = \sum_{j=1}^{m} A_{ij} x_j.$$

If $m \neq n$, insert zero columns or zero rows so that $A$ is square. Then transfer $A$ into Smith Normal Form with diagonal entries $d_1, \ldots, d_r, 0, \ldots, 0$ such that $d_1 \big| d_2 \big| \cdots \big| d_r$.

But $A$ is turned into Smith Normal Form by multiplying invertible matrices on the left and on the right, which is just a change of basis. So we have a basis $\{v_1, \ldots, v_m\}$ for $R^m$ such that $\{d_1v_1, \ldots, d_rv_r\}$ is a basis for $N$. □

**Corollary 10.31.** *Any submodule of a free module of rank $m$ over a Euclidean domain is free and has rank at most $m$.*

*Proof.* By the proof above we see that $n \leq m$. □

**Theorem 10.32.** *Let $M$ be finitely generated by an $R$-module of rank $k$, where $R$ is a Euclidean domain. Then*

$$M \cong R/\langle d_1 \rangle \oplus R/\langle d_2 \rangle \oplus \cdots R/\langle d_r \rangle \oplus \underbrace{R \oplus \cdots \oplus R}_{k-r}.$$

*Thus $M$ is a direct sum of cyclic module. Note that if $d_k$ is a unit then $R/\langle d_k \rangle = 0$.*

# 11 Field extension

Now we can start the algebraic topics of Number theory. Why is algebraic number theory helpful? What is the main difference between algebraic number theory and analytic number theory? We shall begin with the following example:
Find all integer solutions to the equation:

$$x^2 + 2 = y^3$$

It is not hard to see (probably after staring the equation for seconds) that $x = \pm 5, y = 3$ are both solutions. Are there any other solution? Readers might have tried lots of other values of $x$ and $y$ and may be convinced numerically that $x = \pm 5, y = 3$ are the only solutions. How can we prove this? The algebraic number theory studies the structure theorem about the ring of integers (which we will define later) and use those to find the solution to equations such as $y^3 = x^2 + a$ etc. This section is intended as an introduction to some algebraic concept in number theory. Any basic ring theory will be assumed.

## 11.1 Basic properties

**Definition 11.1.** *When a subring $K$ of a field $F$ is a field. We call $K$ a subfield of $F$ and $F$ an extension of $K$. Usually, the pair of $K$ and its extension $F$ is called an extension $F/K$. A field $L$ satisfying*

$$K \subset L \subset F$$

*is called an intermediate field of the extension $F/K$, and $L/K$ is called a subextension of $K$.*

**Definition 11.2.** *Let $F/K$ be a field extension. The* **degree** *of the extension is the dimension of $F$ as a $K$-vector space and is denoted by $[F : K]$. When $[F : K] = n$ for some $n \in \mathbb{N}$, we say $F/K$ is a* **finite** *extension (of degree $n$), and when $[F : K] = \infty$, we say $F/K$ is an infinite extension.*

**Remark 11.3.** *It is clear that $[F : K] = 1$ if and only if $F = K$.*

**Proposition 11.4.** **[Tower Law]** *Let $K \subset L \subset F$. Then $[F : K] = [F : L][L : K]$.*

*Proof.* This is clear if at least one of $[F : L]$ or $[L : K] = \infty$. So we may assume that both of them are finite, say $[F : L] = m, [L : K] = n$. Then we may pick an $L$-basis $\{l_1, \ldots, l_m\}$ for $F$ and a $K$-basis $\{k_1, \ldots, k_n\}$ for $L$. Let $S = \{l_i k_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ and we check that $S$ is a $K$-basis for $F$ and so the result follows.
Linear independence: Let $\sum_{i,j} \lambda_{i,j} l_i k_j = 0$, and so we have $\sum_i \lambda l_i \sum_j \lambda_{i,j} k_j = 0$. As $\{l_1, \ldots, l_m\}$ is linearly independent, so for each $i$ we have

$$\sum_j \lambda_{i,j} k_j = 0$$

which implies $\lambda_{i,j} = 0$ for each $i, j$ because $\{k_1, \ldots, k_n\}$ is linearly independent.
Spanning: Let $f \in F$ and so we have some $\lambda_i \in L$ such that

$$f = \sum_{i=1}^{m} \lambda_i l_i$$

For each $i$, we have $\lambda_{i,j}$ such that

$$\lambda_i = \sum_{j=1}^{n} \lambda_{i,j} k_j$$

and hence

$$f = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{i,j} l_i k_j$$

. □

**Proposition 11.5.** *Let $P$ be a monic irreducible polynomial over a field $K$. Then $[K_P : K] = \deg P$.*

*Proof.* Let $d = \deg P$ and $S = \{1, \bar{x}, \ldots, \bar{x}^{d-1}\}$ where $\bar{f}$ means $f$ modulo $P$. the set $S$ is a $K$-basis for $K_p$. □

## 11.2 K-Homomorphism

This short subsection will introduce the concept of $K$-homomorphism.

**Definition 11.6.** *Let $F, F'$ be two field extensions of $K$. A ring homomorphism*

$$f : F \longmapsto F'$$

*is a $K$-**homomorphism** if it satisfies $f|_K = id$.*

*The set of all $K$-homomorphism from $F$ to $F'$ is denoted by $Hom_K(F, F')$. A bijective $K$-homomorphism is called a $K$-isomorphism. We say $F$ and $F'$ are $K$-isomorphic if there exists a $K$-isomorphism between $F$ and $F'$ and write $F \cong F'$. In particular, a $K$-isomorphism $F \longmapsto F$ is called a $K$-automorphism of $F$, and the group consisting of all $K$-automorphisms of $F$ is denoted by $Aut_K(F)$.*

**Example 11.7.** *If $F \cong F'$, then $[F : K] = [F' : K]$. because if $S$ be a $K$-basis for $F$ and let $f$ be a $K$-isomorphism from $F$ to $F'$. Then it is easy to check that $f(S)$ is a $K$-basis for $F'$.*

**Remark 11.8.** *We know that the kernel* $\ker f$ *is always an ideal of $F$ and so it must be $0$ or $F$. But $1 \in K$ and $f(1) = 1$ so that every $K$-homomorphism $f$ is injective. And the image is a subextension of $F'/K$.*

**Lemma 11.9.** *If $[F : K] = [F' : K]$ then any $K$-homomorphism from $F$ to $F'$ must be a $K$-isomorphism.*

*Proof.* Let $f$ be any $K$-homomorphism from $F$ to $F'$ and so we know $f$ is injective. But as $K$-vector spaces, the dimension of $F$ is the same as the dimension of $F'$. Then by **Rank-Nullity** of Linear Algebra, $f$ must be surjective. Hence it is an isomorphism. □

## 11.3 Algebraic extension

**Definition 11.10.** *Let $F$ be a field and $K$ be a subfield of $F$. An element $\alpha$ of $F$ is called an* **algebraic element** *over $K$ or said to be* **algebraic** *over $K$ if there exists a polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. An element $\alpha$ is said to be* **transcendental** *over $K$ if it is not algebraic.*

**Definition 11.11.** *Let $F/K$ be a field extension and $\alpha \in F$. The* **substitution map** *$f_\alpha$ is defined as*

$$f_\alpha : K[x] \ni P(x) \longmapsto P(\alpha) \in F$$

Then in the sense of field extension, an element $\alpha$ is said to be algebraic if we have the substitution map $f_\alpha$ with $\ker f_\alpha \neq 0$ and transcendental if $\ker f_\alpha = 0$.

**Definition 11.12.** *Let $F/K$ be a field extension. We say $F/K$ is algebraic if $\alpha$ is algebraic for every $\alpha \in F$.*

**Proposition 11.13.** *Finite extensions are algebraic.*

*Proof.* Let $F/K$ be a finite extension. Pick any $\alpha \in F$, and consider the substitution map $f_\alpha$. It is clear that $f_\alpha$ is linear. But the dimension of $K[x]$ over $K$ is infinite, while the dimension of $F$ over $K$ is finite. By Rank-Nullity, we have $\ker f \neq 0$. □

Let $F$ be a field and $K$ be a subfield of $F$. We know that if $K$ is a field then clearly $K[x]$ is a Euclidean domain and hence a principal ideal domain. Let $\alpha$ be algebraic over $K$. Consider the set

$$I_K(\alpha) = \{f(x) \in K[x] : f(\alpha) = 0\}$$

It is easy to check that $I_K(\alpha)$ is an ideal of $K[x]$ and thus is generated by a single element. The generator is unique up to modulo units because we know that if $a \sim b$, then $\langle a \rangle = \langle b \rangle$. As $K$ is a field, so we may assume the generating polynomial is monic. Therefore we may introduce the following concept:

**Definition 11.14.** *Let $F/K$ be a field extension. Let $\alpha \in F$ be algebraic over $K$. The* **minimal polynomial** *of $\alpha$ over $K$ is the unique monic polynomial $p(x) \in K[x]$ such that*

$$\langle p(x) \rangle = I_K(\alpha)$$

*and is denoted by $min_{K,\alpha}(x)$.*

Equivalently, in the sense of field extension, the minimal polynomial $min_{K,\alpha}(x)$ is defined by the generator of the ideal $\ker f_\alpha$

**Lemma 11.15.** *Let $F/K$ be a field extension. Let $\alpha \in F$ be algebraic over $K$. Then $min_{K,\alpha}(x)$ is irreducible in $K[x]$.*

*Proof.* Suppose not, say $min_{K,\alpha}(x) = f(x)g(x)$ where $f(x), g(x) \in K[x]$. Then As $min_{K,\alpha}(\alpha) = 0$, we have $f(\alpha)$ or $g(\alpha) = 0$, and WLOG, say $f$. Thus we have $f | min_{K,\alpha}(x)$ but $min_{K,\alpha}(x) \nmid f$ and so the minimal polynomial is $f$, which is a contradiction. □

**Definition 11.16.** *Let $K$ be a field and let $P$ be a monic irreducible polynomials in $K[X]$ and so the ideal $\langle P \rangle$ is maximal. Hence the quotient ring*

$$K_P = K[X]/\langle P \rangle$$

*is a field. We say $K_P$ is an field extension of $K$ by* **adjoining** *a root of $P$ and we write $K \subset K_P$.*

Equivalently,

**Definition 11.17.** *Let $F/K$ be a field extension. Let $\alpha \in F$ be algebraic over $K$. The subextension $Imf_\alpha$ of $F/K$ is denoted by $K(\alpha)$, and called the field generated by $\alpha$ over $K$. A finite extension $F/K$ is called a simple extension if $F = K(\alpha)$ for some $\alpha \in F$. In this case we have:*

$$K_P \cong F$$

*for $P = min_{K,\alpha}(x)$.*

We shall extend Definition 11.17 as follows:

**Definition 11.18.** *Let $F/K$ be a field extension and $\alpha_1, \ldots, \alpha_n \in F$ be algebraic over $K$. We define the subextension $K(\alpha_1, \ldots, \alpha_n)$ inductively by:*

$$K_0 = K; K_{i+1} = K_i(\alpha_{i+1}), 0 \leq i \leq n-1; K_n = K(\alpha_1, \ldots, \alpha_n)$$

*This is the smallest subfield of $F$ which contains $\alpha_1, \ldots, \alpha_n$. The definition is independent of the ordering of $\alpha_i$.*

**Proposition 11.19.** *For $F/K$ a finite extension, there exists $\alpha_1, \ldots, \alpha_n$ such that $F = K(\alpha_1, \ldots, \alpha_n)$.*

*Proof.* We can find these $\alpha_i$ inductively by the following procedure. Let $\alpha_1 \in F$ be any element not in $K$. Define $K_1 = K(\alpha_1)$. For $i \geq 1$, having defined $K_i$, let $K_{i+1} = K_i(\alpha_{i+1})$ for some $\alpha_{i+1} \in F$ not in $K_i$. This process must terminate because by Tower Law (Proposition 11.4) we have

$$[K_n : K] = [K_n : K_{n-1}] \ldots [K_1 : K]$$

and each $[K_i : K_{i-1}] \geq 2$ by construction. Therefore, as $F/K$ is finite, the process will terminate. □

## 11.4 Automorphism group

Let $F/K$ be a field extension and $\alpha \in F$ be algebraic over $K$ and let $P = min_{K,\alpha}(x)$ be its minimal polynomial. Let $\sigma \in \mathrm{Hom}_K(K_P, F)$ be a $K$-homomorphism. What can $\sigma(\alpha)$ be?

Consider $f(x) \in K[x]$ be any polynomials with coefficients in $K$. Then as $\sigma$ is a ring homomorphism and identity on $K$, we have

$$\sigma(f(\alpha)) = f(\sigma(\alpha))$$

Thus, if we take $f = P$, then we have $P(\alpha) = 0$ and $\sigma(0) = 0$. Therefore, we have

$$P(\sigma(\alpha)) = 0$$

In other words, $\sigma(\alpha)$ must also be a root of the minimal polynomial $P$. Therefore, $\sigma$ may be viewed as a permutation of the roots of $P$. Also, the structure of $K_P$ does not depend on which root of $P$ we took in the first place and $K_P \cong K(\alpha)$. Hence, the field extension $K_P/K$ is generated by a single element (some root of $P$) and therefore the homomorphism $\sigma$ is determined by the image of the generator.

**Proposition 11.20.** *Let $R(P)$ be the set of roots of $P$. Then the following maps are inverse to each other:*

$$R(P) \ni \alpha \longmapsto f_\alpha \in Hom_K(K_P, F)$$
$$Hom_K(K_P, F) \ni \sigma \longmapsto \sigma(\bar{x}) \in R(P)$$

*where $\bar{x}$ is $x$ modulo $P$ in the quotient ring.*
*In particular, $|Hom_K(K_P, F)| = |R(P)| \leq \deg P = [K_P : K]$*

*Proof.* It is clear that $\bar{x}$ is a root of $P$ and so by the previous observation, $\sigma(\bar{x}) \in R(P)$. Let $\alpha \in R(P)$, and so clearly $f_\alpha(\bar{x}) = \alpha$. □

If in particular $F/K$ is a simple extension, say $F = K(\alpha)$. Then we can interprete the permutations of roots as $K$-automorphisms of a simple extension. In general, the group of $K$-automorphisms $Aut_K(F)$ of $F$ acts on the set $Hom_K(K_P, F)$ as follows:

$$\mathrm{Aut}_K(F) \times \mathrm{Hom}_K(K_P, F) \ni (\sigma, f) \longmapsto \sigma \circ f \in \mathrm{Hom}_K(K_P, F)$$

Thus we have:

**Proposition 11.21.** *Let $F \cong K_P$. For any root $\alpha \in R(P)$, the map:*

$$Aut_K(F) \ni \sigma \longmapsto \sigma(\alpha) \in R(P)$$

*is bijective. In particular, $Aut_K(F)| = |R(P)| \leq [F : K]$*

*Proof.* As $[F : K] = [K_P : K]$, the map $f_\alpha \in \mathrm{Hom}_K(K_P, F)$ is a $K$-isomorphism. Therefore, we have a bijection:

$$\mathrm{Aut}_K(F) \ni \sigma \longmapsto \sigma \circ f_\alpha \in \mathrm{Hom}_K(K_P, F)$$

Now use Proposition 11.20, the map

$$\mathrm{Hom}_K(K_P, F) \ni f \longmapsto f(\bar{x}) \in R(P)$$

is a bijection and hence the composition is also bijective and use $f_\alpha(\bar{x}) = \alpha$. □

## 11.5 Splitting field and separability

We shall very briefly introduce the concepts of splitting field and separability here. Detailed explanations will not be given in this book.

**Definition 11.22.** *Let $K$ be a field and $P(x) \in K[x]$. We say $P$ splits in a field extension $F$ of $K$ if $P$ can be written as a linear product in $F[x]$. The splitting field of $P$ is the smallest field extension $F$ such that $P$ splits in $F$.*

In fact, this definition can be generalised if we modify and extend the definition of field extension as follows

**Definition 11.23.** *Let $K$ be a field. An extension $F_\tau/K$ is defined as a pair $(F, \tau)$ of a field $F$ and a ring homomorphism $\tau : K \longmapsto F$. A $K$-homomorphism from $F_\tau$ to $F'_{\tau'}$ is a ring homomorphism $\psi : F \longmapsto F'$ such that $\tau' = \psi \circ \tau$. By a subextension $L_\tau/K$ of $F_\tau/K$, we mean an intermediate field $L$ of $F/\tau(K)$ and $\tau : K \longmapsto L$.*

But we shall not give details in this book.

**Example 11.24.** *The splitting field of $P(x) = x^2 - 2$ in $\mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt{2})$. The splitting field of $P(x) = x^4 + 2$ in $\mathbb{Q}[x]$ is $\mathbb{Q}(i, \sqrt[4]{2})$.*

(In the sense of field extension, Let $P \in K[x]\backslash K$. If $P$ splits in an extension $F'$ if and only if $\mathrm{Hom}_K(F, F') \neq \varnothing$, then we call $F$ a splitting field of $P$ over $K$).

**Definition 11.25.** *(i) A polynomial $P \in K[X]\backslash K$ is called separable if $|R(P, E)| = \deg P$ for some extension $E/K$.*

*(ii) Let $F/K$ be an algebraic extension and an element $\alpha \in F$ is separable if the minimal polynomial $min_{K,\alpha}(x)$ is separable.*

*(iii) A finite extension $F/K$ is called separable if $|Hom_K(F, E)| = [F : K]$ for some extension $E/K$.*

To be concrete, a polynomial is separable if it has no repeated roots in the splitting field. For example, $P(x) = (x-3)^2$ is not separable in any field. $P(x) = x(x-1)(x-2)$ is separable in $\mathbb{Q}[x]$ but is not separable in a field with characteristic 2 because it is the same as $P(x) = x^2(x-1)$.

**Lemma 11.26.** *Let $F/L/K$ be finite with $F = L(\alpha)$, and $E/K$ arbitrary. Let $P$ be the minimal polynomial of $\alpha$ over $L$. Then*

$$|Hom_K(F, E)| \leq |Hom_K(L, E)| \cdot [F : L]$$

*and the equality holds if and only if $|R(\tau P, E)| = \deg P$ for all $\tau \in Hom_K(L, E)$ where $R(\tau P, E)$ is the root of $\tau P$ in $E$.*

*Proof.* It is not hard to check that:

$$\mathrm{Hom}_K(F, E) = \bigsqcup_{\tau \in \mathrm{Hom}_K(L,E)} \mathrm{Hom}_L(F, E_\tau)$$

Use Proposition 11.20 that $|\mathrm{Hom}_L(F, E_\tau)| = |R(\tau P, E)|$ and also $\deg P = [F : L]$. □

**Lemma 11.27.** *Let $F/K$ be a finite separable extension. Let $L, L'$ be subextensions of $F/K$ with $L \subset L'$. Then*

$$|Hom_L(L, E)| = [L' : L]$$

*Proof.* WLOG, we can write $F = K(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_i \in F$. Let $(L_i)_{0 \leq i \leq n}$ be a chain of subextensions such that:

$$L_0 = K, L_n = F, L_{i+1} = L_i(\alpha_{i+1})$$

Let $P_i$ be the minimal polynomial of $\alpha_i$ over $L_{i-1}$. Then the equality in Lemma 11.26 holds by using Tower Law and the definition of separability. Hence by Lemma 11.26

$$|R(\tau P_i, E)| = \deg P_i \text{ for all } \tau \in \mathrm{Hom}_K(L_{i-1}, E)$$

Then we let $L = L_i, L' = L_j$ for some $i, j$ in the chain. Then at each stage, the above equation holds, and so the equality in Lemma 11.26 holds and hence the result follows. □

The most important theorem we are going to prove in this subsection which will be quoted frequently later is:

**Theorem 11.28.** [**Primitive Element Theorem**] *Every separable finite extension is simple.*

*Proof.* Let $F/K$ be a finite extension. If $K$ is finite then so is $F$ and so the group $F^*$ is cyclic. Assume now $K$ is infinite. Let $F = K(\alpha_1, \ldots, \alpha_m)$ and we prove the case when $m = 2$ first. So let $F = K(\alpha, \beta)$, $[F : K] = n$ and $\mathrm{Hom}_K(F, E) = \{\sigma_1, \ldots, \sigma_n\}$. for some extension $E/K$. Each homomorphism $\sigma_i$ is determined by the images of $\alpha$ and $\beta$. So we have, for $\imath \neq j$, $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ or $\sigma_i(\alpha) \neq \sigma_j(\beta)$. Consider the polynomial:

$$P(x) = \prod_{i \neq j} ((\sigma_i(\alpha) - \sigma_j(\alpha))x + (\sigma_i(\beta) - \sigma_j(\beta)))$$

As $K$ is infinite, there exists $\gamma \in K$ which is not a root of $P(x)$. Let $\delta = \alpha\gamma + \beta \in F$. Then

$$0 \neq P(\gamma) = \prod_{i \neq j} (\sigma_i(\delta) - \sigma_j(\delta))$$

Thus $\sigma_i(\delta) \neq \sigma_j(\delta)$ whenever $i \neq j$. Therefore, $\sigma_1, \ldots, \sigma_n$ are $n$ different $K$-homomorphisms from $K(\delta)$ to $E$. So

$$n \leq |\mathrm{Hom}_K(K(\delta), E)| \leq [K(\delta) : K]$$

where the second inequality came from proposition 11.20. But $[K(\delta) : K] \leq [F : K] = n$. Therefore, the equality holds and so $K(\delta) = F$. This completes the proof for the case $m = 2$.

For $m \geq 2$, observe that we have

$$K(\alpha_1, \alpha_2, \ldots, \alpha_m) = K(\alpha_1, \alpha_2)(\alpha_3, \ldots, \alpha_m) = K(\beta, \alpha_3)(\alpha_4, \ldots, \alpha_m)$$

for some suitable $\beta$ by the case $m = 2$. Since each subextension is separable by Lemma 11.27, we can apply this argument repeatedly and hence the result follows. □

**Theorem 11.29.** *Any finite extension of $\mathbb{Q}$ is separable. (This is one of the important facts we shall quote and use in the next chapter)*

*Proof.* Let $K/\mathbb{Q}$ be a finite extension. We will show firstly that if $P(x) \in \mathbb{Q}[x]$ is irreducible, then $P(x)$ is separable. Clearly, $P(x)$ is non constant and so the differential $D(P) \neq 0$. As $\deg D(P) < \deg P$ so $D(P) \not\subseteq \langle P \rangle$. Thus, the sum

$$\langle P \rangle + \langle D(P) \rangle = \mathbb{Q}[x]$$

because $P(x)$ irreducible implies that $\langle P(x) \rangle$ is a maximal ideal. So there exists $f(x), g(x) \in \mathbb{Q}[x]$ such that

$$f(x)P + g(x)D(P) = 1$$

and so the linear factor of $P(x)$ does not divide $D(P)$. Hence we have no repeated roots and so $P(x)$ is separable. Thus, if $K = \mathbb{Q}(\alpha)$, with $\alpha$ algebraic, then $K/\mathbb{Q}$ is separable and similarly, if $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is a finite extension of $\mathbb{Q}$, then $K/\mathbb{Q}$ is separable. □

## 11.6 Exercises

1. (i) Let $F/K$ be a field extension whose degree is prime. Show that there is no intermediate extension
$$F \supsetneq K' \supsetneq K$$

   (ii) Let $F/K$ be an extension and suppose that $\alpha \in F$ be algebraic over $K$ of odd degree, i.e. $[K(\alpha) : K]$ is odd. Show that $K(\alpha) = K(\alpha^2)$.

   (iii) Let $F = K(\alpha, \beta)$ with $[K(\alpha) : K] = m, [K(\beta) : K] = n$ and $(m, n) = 1$. Show that $[F : K] = mn$.

2. Let $F/K$ be an extension of degree 2. Show that if the characteristic of $K$ is not 2, then $F = K(\alpha) = \{a + b\alpha : a, b \in K\}$ for some $\alpha \in F$ with $\alpha^2 \in K$. Show that if the characteristic is 2, then either $F = K(\alpha)$ with $\alpha^2 \in K$ or $F = K(\alpha)$ with $\alpha^2 + \alpha \in K$.

3. Prove that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$.

4. Prove that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

5. Let $F/K$ be a finite extension and $P(x) \in K[x]$. an irreducible polynomial of degree $d > 1$. Show that if $(d, [F : K]) = 1$, then $P$ has no roots in $F$.

6. Let $L/K$ be a field extension. Show that $\alpha$ is algebraic over $K$ if and only if the field $K(\alpha)$ is finite dimensional as a vector space over $K$. Let $F/L$,$L/K$ be algebraic extensions. Show that $F/K$ is also algebraic.

7. Let $F/K$ be a field extension and let $\alpha, \beta \in F$. Show that $\alpha + \beta$ and $\alpha\beta$ are algebraic over $K$ if and only if $\alpha$ and $\beta$ are algebraic.

8. Let $F/K$ be an extension and $\alpha, \beta \in F$ be transcendental over $K$. Show that $\alpha$ is algebraic over $K(\beta)$ if and only if $\beta$ is algebraic over $K(\alpha)$.

9. Let $\alpha$ be algebraic over $K$. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(\alpha)$. (Hint: consider the minimal polynomial $P$ of $\alpha$ over $K$ and show that $P$ determines $K'$.) Now let $F/K$ be a finite extension for which there exists only finitely many intermediate subfields $K \subset K' \subset F$, then $F = K(\alpha)$ for some $\alpha \in F$. (Hint: Discuss the case when $K$ is finite and the case when $K$ is infinite separately)

10. Show that if $F$ is a splitting field over $K$ for $P \in K[x]$ of degree $n$, then $[F : K] \leq n!$.

11. Let $K$ be a field and $\alpha \in K$. If $m, n \in \mathbb{N}$ with $(m, n) = 1$. Show that $x^{mn} - \alpha$ is irreducible if and only if $x^m - \alpha$ and $x^n - \alpha$ are irreducible.

12. Let $a, b$ be square free positive integer $> 1$. Show that the minimal polynomial of $\sqrt{a} + \sqrt{b}$ over $\mathbb{Q}$ is reducible mod $p$ for all primes $p$. (Hint: You may find it helpful to show firstly that for every prime $p$, one of $a, b$ or $ab$ is a square in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$)

## 11.7 Hint and Solutions

1. (i) Suppose we have some intermediate field $K'$, then by Tower Law we have

$$[F : K'][K'K] = [F : K]$$

which is impossible as $[F : K]$ is a prime.

(ii) It is clear that $K(\alpha^2) \subseteq K(\alpha)$. Now by Tower Law, we have

$$[K(\alpha) : K(\alpha^2)][K(\alpha^2) : K] = [K(\alpha) : K]$$

Also, $[K(\alpha) : K(\alpha^2)]$ is at most two because $\alpha$ satisfies $x^2 - \alpha^2$ in $K(\alpha^2)[x]$ and so $[K(\alpha) : K(\alpha^2)] = 1$ or 2. But $[K(\alpha) : K]$ is odd and so the factor $[K(\alpha) : K(\alpha^2)]$ must also be odd. Therefore, $[K(\alpha) : K(\alpha^2)] = 1$ and $K(\alpha) = K(\alpha^2)$.

(iii) Using Tower Law, we have

$$[F : K(\alpha)][K(\alpha) : K] = [F : K(\beta)][K(\beta) : K] = [F : K]$$

Then $m, n | [F : K]$ and since $(m, n) = 1$ so $mn | [F : K]$. Now $[K(\alpha) : K] = m$ so the minimal polynomial of $\alpha$ over $K$ has degree $m$, and as $K \subset K(\beta)$, so the minimal polynomial of $\alpha$ over $K(\beta)$ divides that over $K$. Hence

$$[F : K(\beta)] = [K(\beta)(\alpha) : K(\beta)] \leq m$$

and hence by Tower Law $[F : K] \leq mn$. But $mn | [F : K]$ and so $[F : K] = mn$

2. WLOG, let $y \in F \backslash K$. Then we must have some $u, v \in K$ such that $y^2 = uy + v$ because $[F : K] = 2$. Then since the characteristic of $F$ is not 2 so we may assume complete the square and so we have

$$\alpha^2 = v + \frac{u^2}{4} \in K$$

where $\alpha = y - \frac{u}{2}$. Thus, as $\alpha \notin K$ and so $[K(\alpha) : K] = 2$ and $K(\alpha) \subseteq F$. So we have $F = K(\alpha)$.

Now suppose the characteristic of the field is 2. Then take any $y \in F \backslash K$, we still have some $u, v \in K$ such that $y^2 = uy + v$. We have the following two cases:

(i) $u = 0$: Then $y^2 = v \in K$ and so $F = K(y)$ with $y^2 \in K$.

(ii) $a \neq 0$ then $a^{-1}$ exists and so we have

$$y^2 a^{-2} = ya^{-1} + ba^{-2}$$

But $ya^{-1} = -ya^{-1}$ because the characteristic is 2. Hence

$$(ya^{-1})^2 + ya^{-1} = ba^{-2}$$

and let $\alpha = ya^{-1}$ then we have $\alpha^2 + \alpha \in K$. $F = K(\alpha)$. (We cannot complete the square as $2 = 0$ has no inverse in the field)

3. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}(\sqrt{2})$. Then it is easy to check that $[F : L] = [L : K] = [K : \mathbb{Q}] = 2$ by considering the minimal polynomial in the corresponding field. Then use Tower Law.

4. It is clear that $\mathbb{Q}(\sqrt{2} + i) \subset \mathbb{Q}(\sqrt{2}, i)$. Conversely, the inverse of $\sqrt{2} + i$ is $\frac{1}{3}(\sqrt{2} - i)$ and so $\sqrt{2} - i \in \mathbb{Q}(\sqrt{2} + i)$. Hence $\sqrt{2}$ and $i$ are both in $\mathbb{Q}(\sqrt{2} + i)$.

5. Suppose $P$ has a root in $F$, say $\alpha$. Then by Tower Law

$$[F : K] = [F : K(\alpha)][K(\alpha) : K]$$

As $P$ is irreducible in $K$ and so $[K(\alpha) : K] = d$. Then d divides $[F : K]$, which is a contradiction as $(d, [F : K]) = 1$.

6. Suppose $\alpha \in L$ and $[K(\alpha) : K]$ is finite. Then by Proposition 11.13, any finite extension is algebraic, and in particular $\alpha$ is algebraic. Conversely, let $\alpha$ be algebraic then we have some non-trivial polynomial $P(x) \in K[x]$ such that $p(\alpha) = 0$ with $\deg P = d$. Then $[K(\alpha) : K] \leq d$.

   Now take any $\alpha \in F$. Then there exist $a_0, \ldots, a_m \in L$ such that $\alpha$ is a root of

$$P(x) = \sum_{i=0}^{m} a_i x^i \in L[x]$$

   Since $L/K$ is algebraic, and so by previous part that each $[K(a_i) : K]$ is finite. Hence $K[(a_0, \ldots, a_m) : K]$ is finite. Also, it is clear that

$$[K(a_0, \ldots, a_m, \alpha) : K(a_0, \ldots, a_m)] \leq m$$

   Hence $[K(a_0, \ldots, a_m, \alpha) : K]$ is finite, and hence algebraic by Proposition 11.13. Then $\alpha$ is algebraic over $K$. Since $\alpha$ is arbitrary, we have $F/K$ algebraic.

7. Let $u = \alpha + \beta, v = \alpha\beta$. Suppose $\alpha, \beta$ is algebraic, then $[K(\alpha, \beta) : K]$ is finite, because $[K(\alpha) : K], [K(\beta) : K]$ are both finite. (because they satisfy some polynomials over $K$) Then $K(u), K(v) \subset K(\alpha, \beta)$ and so $[K(u) : K], [K(v) : K]$ are both finite and hence algebraic by Proposition 11.13.

   Conversely, suppose $u, v$ are algebraic over $K$. Observe that $\alpha, \beta$ are roots of

$$x^2 - ux + v \in K(u, v)[x]$$

   So $[K(u, v, \alpha) : K(u, v)], [K(u, v, \beta) : K(u, v)] \leq 2$ But $[K(u, v) : K]$ is algebraic and so $[K(u, v, \alpha) : K], [K(u, v, \beta) : K]$ are both finite. Hence $\alpha, \beta$ are algebraic by Proposition 11.13.

8. Since the statement is symmetric so we only need to check one direction holds. Suppose $\alpha$ is algebraic over $K(\beta)$. Then there exists a non-trivial $P(x) \in K(\beta)[x]$ such that $P(\alpha) = 0$. WLOG, let

$$P(x) = \sum_{i=0}^{m} a_i x^i$$

   Each $a_i \in K(\beta)$ so we have

$$a_i = \sum_{j=0}^{m_i} b_{ij} \beta^j$$

Thus we have

$$\sum_{i=0}^{m}\sum_{j=0}^{m_i} b_{ij}\beta^j\alpha^i = 0$$

which can be viewed as a polynomial in $K(\alpha)[x]$ which vanishes at $\beta$. We need to check this polynomial is not a zero polynomial. Indeed, if it is zero, then for each $j$, the coefficient for $\beta^j$ is zero, which is

$$\sum_{i=1}^{m} \alpha^i b_{ij} (\text{if we don't have } b_{ij} \text{ for some } i,j \text{ then let } b_{ij}=0)$$

But $\alpha$ is transcendental and so this is possible only if $b_{ij} = 0$ for all $i, j$. But then the polynomial $P(x)$ itself is a zero polynomial, which is a contradiction. Hence $\beta$ is algebraic over $K(\alpha)$.

9. Let $P$ be the minimal polynomial of $\alpha$ over $K'$, where $K \subset K' \subset K(\alpha)$. WLOG, let $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Let $K'' = K(a_0, \ldots, a_{n-1})$. Then $[K''(\alpha) : K''] = n$. Also $[K'(\alpha) : K'] = n$ by definition of $P$. But $a_i \in K'$, so $K'' \subseteq K' \subset K(\alpha)$. Hence

$$[K(\alpha) : K''] = [K(\alpha) : K'][K' : K'']$$

Also as $K' \subset K(\alpha)$, so $K'(\alpha) \subset K(\alpha)$, but $K(\alpha) \subset K'(\alpha)$ as $K \subset K'$. So we have $K(x) = K'(x)$. Similarly, $K(x) = K''(x)$ as $K'' \subset K'$. Then the above equation becomes:

$$[K''(\alpha) : K''] = [K'(\alpha) : K'][K' : K'']$$

But $n = [K''(\alpha) : K] = [K'(\alpha) : K']$ and so $[K' : K'']$, which implies that $K' = K''$, and so $K'$ is generated by $a_0, \ldots, a_{n-1}$. Let $Q$ be the minimal polynomial of $\alpha$ over $K$ and so $Q$ is independent of $K'$. Then $P|Q$ and so there are only finitely many possible sets of values of $\{a_0, \ldots, a_{n-1}\}$ and hence finitely many $K'$.

If $K$ is finite, so is $F$ and so $F^*$ is generated by some element say $\alpha$ and so $F = K(\alpha)$. So we may assume now $K$ is infinite. One way to do this is a Linear Algebra approach. Suppose $F \neq K(\alpha)$ for all $\alpha \in F$. But we only have finitely intermediate field, so only finitely many $K(\alpha)$ for different $\alpha \in F$. But

$$F = \bigcup_{\alpha \in F} K(\alpha)$$

and so the above union must be a finite union. Now $K$ is infinite and so if $F$. This is impossible as an infinite vector space cannot be written as a finite union of proper subspaces.

The second approach is purely algebraic. Consider for two elements $\alpha, \beta \in F$, the field $K(\alpha + a\beta)$ for some $a \in K$. We have $K \subset K(\alpha+a\beta) \subset F$. As we have only finitely many intermediate fields, and since $K$ is infinite, so there exist $a \neq b$ such that

$$K(\alpha + a\beta) = K(\alpha + b\beta)$$

Also,

$$\beta = \frac{(\alpha + a\beta) - (\alpha + b\beta)}{a - b}, \alpha = (\alpha + a\beta) - a\beta$$

Since $\alpha + b\beta \in K(\alpha + a\beta)$, so $\beta \in K(\alpha + a\beta)$ and hence $\alpha \in K(\alpha + a\beta)$. Therefore, $K(\alpha, \beta) = K(\alpha+a\beta)$ for some $a$. Now $F/K$ is finite, so there exist $\alpha_1, \ldots, \alpha_n$ such that $F = K(\alpha_1, \ldots, \alpha_n)$. Apply the above $n-1$ times (i.e $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1 + a\alpha_2, \ldots, \alpha_n)$ etc) so we conclude that $F = K(\alpha)$ for some $\alpha$

10. Use induction on $n$. It is clear that if $n = 1$, then $P$ is linear and so the splitting field $F = K$. Now suppose it is true for $n-1, n \geq 2$. Then let $\deg P = n$. Let $x - \alpha$ be a linear factor in the splitting field of $P$, say $F$. Then $[K(\alpha), K] \leq n$. Let $P(x) = (x-\alpha)Q(x)$. By induction, the splitting field of $Q(x)$, say $F'$ has $[F' : K] \leq (n-1)!$. Clearly, $F$ is contained in the field $F'(\alpha)$ because $P$ splits in $F'(\alpha)$. Hence $[F : K] \leq n!$.

11. If $x^m - \alpha, x^n - \alpha$ are both reducible, then $x^{mn} - \alpha = (x^m)^n - \alpha$ is also reducible.

    Conversely, suppose $x^m - \alpha, x^n - \alpha$ are both irreducible, then let $u$ be any root of $x^{mn} - \alpha$. Then $u^n$ is a root of $x^m - \alpha$ and $u^m$ is a root of $x^n - \alpha$. Since $x^m - \alpha, x^n - \alpha$ both irreducible, we have

    $$[K(u^m) : K] = n \text{ and } [K(u^n) : K] = m$$

    Also

    $$[K(u) : K] = [K(u) : K(u^m)][K(u^m) : K] = [K(u) : K(u^n)][K(u^n) : K]$$

    and so $mn$ divides $[K(u) : K]$ because $(m, n) = 1$. But $u$ is a root of $x^{mn} - \alpha$ so $[K(u) : K] = mn$. Hence $x^{mn} - \alpha$ is the minimal polynomial of $u$ over $K$ and so it is irreducible.

12. The minimal polynomial is

    $$P(x) = x^4 - 2(a+b)x^2 + (a-b)^2$$

    Now, using Legendre symbol, either one of $(\frac{a}{p}), (\frac{b}{p})$ is 1, or both of them are $-1$, which gives $(\frac{ab}{p}) = 1$ so one of them is a square for any prime $p$. Then denote $\alpha, \beta, \gamma$ by the square root of $a, b, ab$ mod $p$ respectively. (We know at least one of them exists) Then we can factorise $P(x)$ mod $p$ into one of the following forms:

    $$(x^2 - 2\alpha x + a - b)(x^2 + 2\alpha x + a - b) \text{ if } a \text{ is a square}$$

    $$(x^2 - 2\beta x + b - a)(x^2 + 2\beta x + b - a) \text{ if } b \text{ is a square}$$

    $$(x^2 - (a + b + 2\gamma))(x^2 - (a + b - 2\gamma)) \text{ if } c \text{ is a square}$$

# 12 Algebraic Number field

## 12.1 Basic concepts

We have seen in the previous chapter the definition of algebraic element. We shall enhance this definition in this chapter.

**Definition 12.1.** *A* **number field** *is a field $K$ that is a finite extension of $\mathbb{Q}$. For example, $K = \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle$.*

**Definition 12.2.** *Let $K$ be a number field. An element $\alpha \in K$ is called an* **algebraic number** *if it satisfies a non-trivial polynomial with coefficients in $\mathbb{Q}$. For example, $\sqrt{2}, \sqrt[3]{2}$ are algebraic numbers.*

**Definition 12.3.** *Let $K$ be a number field. An element $\alpha \in K$ is called an* **algebraic integer** *if it satisfies a non-trivial* **monic** *polynomial with* **integer** *coefficients. For example, $\sqrt{2}$ is an algebraic integer, while $\frac{1}{\sqrt{2}}$ is not an algebraic integer.*

*More generally, let $A \subset B$ be two rings and $x \in B$. We say $x$ is integral over $A$ if there exists a monic polynomial $P$ with coefficients in $A$ such that $P(x) = 0$.*

**Remark 12.4.** *To check whether $\alpha$ is an algebraic integer, we only need to check whether the minimal polynomial has coefficients in $\mathbb{Z}$. Suppose $\alpha$ satisfies $g(x)$, which is monic and has integer coefficients. Let $f$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$ and we assume that $g \neq f$. So $f|g$ and so by Gauss's lemma $g$ is reducible in $\mathbb{Q}[X]$ and so must be reducible in $\mathbb{Z}[X]$ and so $f$ has integer coefficients.*

**Definition 12.5.** *Let $K$ be a number field. The* **ring of integers** *is defined by the set of algebraic integers in $K$, and is denoted by $\mathcal{O}_K$*

The main aim of this subsection is to prove that $\mathcal{O}_K$ is a ring for any number field $K$.

## 12.2 Cayley-Hamilton Theorem

**Theorem 12.6. [Cayley-Hamilton theorem]** *Let $A$ be a ring and $I$ be an ideal of $A$. Let $M$ be an $A$-module generated by $m_1, \ldots, m_n$ and $\phi : M \longmapsto M$ is an $A$-endomorphism such that $\phi(M) \subseteq IM$. Then $\phi$ satisfies an equation*

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

*for some $a_i \in I$.*

*Proof.* Let $\phi(m_i) = \sum_{j=1}^{n} a_{ij}m_j$ for some $a_{ij} \in I$ because $\phi(M) \subseteq IM$. Hence

$$\sum_{j=1}^{n}(\delta_{ij}\phi - a_{ij})m_j = 0 \text{ for all } i$$

Let $\mathrm{End}_A(M)$ be the set of $A$-endomorphism from $M$ to $M$, then $A[\phi] \subseteq \mathrm{End}_A(M)$. Since $\mathrm{End}_A(M)$ is a commutative ring. So $M$ is an $A[\phi]$-module. Thus we can write

$$P \cdot \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

Where $P_{ij} = \delta_{ij}\phi - a_{ij}$ which is an $n \times n$ matrix. Let $P^{adj}$ be the adjoint matrix of $P$ and so

$$P^{adj}P = (\det P)I_n$$

and so left multiply by $P^{adj}$ in the above matrix equation, we have

$$(\det P)I_n \cdot \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

Thus we have $\det P = 0$, because $m_i \neq 0$. Therefore,

$$\det P = \phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0$$

for some $a_i$ with each $a_i$ a polynomial in $a_{ij}$. As $a_{ij} \in I$ for all $i, j$, so $a_i \in I$ for all $i$. □

**Corollary 12.7.** **[Nakayama's Lemma]** *Let $A$ be a ring and $I$ be an ideal of $A$. $M$ is an $A$-module generated by $m_1, \ldots, m_n$. If $IM = M$, then there exists $x \in A$ such that $x \equiv 1$ (mod) $I$ and $xM = 0$.*

*Proof.* In Theorem 12.6, we take $\phi$ to be the identity map, and so all conditions in Theorem 12.6 are satisfied. Then we have some $a_i \in I$ such that

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

Take $x = 1 + a_{n-1} + \ldots + a_0$. So $x \equiv 1 \pmod{I}$, and let $m \in M$, so we have

$$xm = (1 + a_{n-1} + \ldots + a_0)m = (\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0)m = 0$$

because it is a zero map. □

## 12.3 Ring of integers

**Definition 12.8.** *An $A$-module $M$ is* **faithful** *if for all $a \in A$ with $a \neq 0$, there exists $m \in M$ such that $am \neq 0$. Equivalently, for all $a \neq b \in A$, there exists $m \in M$ such that $am \neq bm$.*

**Lemma 12.9.** *Let $A, B$ be two rings such that $A \subseteq B$. Let $x \in B$. Then the following are equivalent:*

*(i) $x$ is integral over $A$.*

*(ii) $A[x]$ is a finitely generated $A$-module.*

*(iii) $A[x]$ is contained in a subring $C$ of $B$ such that $C$ is finitely generated $A$-module.*

*(iv) There exists a faithful $A[x]$-module $M$ that is finitely generated as an $A$-module.*

*Proof.* The proof has the following four steps:

1. (i) ⇒ (ii): As $x$ is integral over $A$, then there exists $a_i \in A$ such that

   $$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

   Then $A[x]$ is finitely generated by $\{1, x, x^2, \ldots, x^{n-1}\}$ as an $A$-module.

2. (ii) ⇒ (iii): Take $C = A[x]$.

3. (iii) $\Rightarrow$ (iv): Take $M = C$ and clearly the subring $C$ is faithful.

4. (iv) $\Rightarrow$ (i): Define the map $\phi : M \longmapsto M$ by left multiplication by $x$. In other words, $\phi(m) = xm$. Let $I = A$. Then use the same notation as in Theorem 12.6, we have $\phi(M) \subset IM$ because $M$ is a finitely generated $A$-module. Hence by Theorem 12.6, we have some $a_i \in I = A$ such that

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

and so apply this to each $m \in M$, we have

$$P(x)m = (x^n + a_{n-1}x^{n-1} + \ldots + a_0)m = 0$$

This implies that $P(x) = 0$ because if not, then $0 \neq P(x) \in A[x]$. As $M$ is a faithful $A[x]$-module, so we must have some $m$ such that $P(x)m \neq 0$, which gives a contradiction. Hence $P(x) = 0$ and so $x$ is an algebraic integer over $A$.

□

**Corollary 12.10.** *Let $x_1, \ldots, x_n \in B$ which are algebraic integers over $A$. Then $A[x_1, \ldots, x_n]$ is a finitely generated $A$-module.*

*Proof.* Use induction on $n$. When $n = 1$, use (i) $\Rightarrow$ (ii) in Lemma 12.9. Suppose true for $n-1, n \geq 2$ then $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$, and use the case $n = 1$, we conclude that $A[x_1, \ldots, x_n]$ is a finitely generated $A[x_1, \ldots, x_n]$-module. Also, by inductive hypothesis, $A[x_1, \ldots, x_{n-1}]$ is a finitely generated $A$-module, and so combine these two, we have $A[x_1, \ldots, x_n]$ is a finitely generated $A$-module. □

**Corollary 12.11.** *$D = \{x \in B : x$ is integral over $A\}$ is a subring of $B$. In particular, take $A = \mathbb{Q}$, $B$ any number field, then the ring of integers $\mathcal{O}_K$ is a ring.*

*Proof.* Suppose $y, z \in D$. Then $C = A[y, z]$ is a finitely generated $A$-module by Corollary 12.10. Then use (iii) $\Rightarrow$ (i) in Lemma 12.9, since $A[y + z], A[yz] \subseteq A[y, z]$, we have $y + z, yz$ integral over $A$. Hence $D$ is a subring. □

## 12.4 Integral elements and integral closure

In this subsection we shall derive some basic properties of integral elements.

**Definition 12.12.** *Let $A \subseteq B$ be two rings. We say $B$ is* **integral** *over $A$ if every element in $B$ is integral over $A$.*

**Proposition 12.13.** *Let $A \subseteq B \subseteq C$ be a tower of rings. If $x \in C$ is integral over $A$ then $c$ is integral over $B$.*

*Proof.* As $c \in C$ is integral over $A$ there exist $a_i \in A, n \in \mathbb{N}$ such that

$$c^n + a_{n-1}c^{n-1} + \ldots + a_0 = 0$$

As $A \subseteq B$ so $a_i \in B$ and hence the result follows. □

**Theorem 12.14.** *Let $A \subseteq B \subseteq C$ be a tower of rings. Suppose $B$ is integral over $A$, and $x \in C$ is integral over $B$. Then $x$ is integral over $A$.*

*Proof.* As $x$ is integral over $B$, there exist $b_i \in B$ and $n \in \mathbb{N}$ such that

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0$$

Let $R = A[b_0, \ldots, b_{n-1}]$. Since $B$ is integral over $A$ then by Corollary 12.10, $R$ is a finitely generated $A$-module, say by $r_1, \ldots, r_m$. Also $R[x]$ is a finitely generated $R$-module by $\{1, x, \ldots, x^{n-1}\}$. So $R[x]$ is a finitely generated $A$-module by $\{r_i x^j : 1 \leq i \leq m, 1 \leq j \leq n-1\}$. Now apply (iii) $\Rightarrow$ (i) in Lemma 12.9 to conclude that $x$ is integral over $A$. □

**Definition 12.15.** *Let $A \subseteq B$ be two rings. The* **integral closure** *of $A$ in $B$ is the set of elements in $B$ which are integral over $A$. Usually, we denote the integral closure of $A$ in $B$ by $A^B$.*

**Corollary 12.16.** *Let $A \subseteq B \subseteq C$ be a tower of rings. Suppose $B$ is integral over $A$. Then the integral closure of $A$ in $C$ and the integral closure of $B$ in $C$ are the same.*

*Proof.* Combine Proposition 12.13 and Theorem 12.14. □

**Theorem 12.17.** *Let $D$ be a unique factorisation domain. Let $F$ be the field of quotients of $D$. Then $c \in F$ is integral over $D$ if and only if $c \in D$.*

*Proof.* If $c \in D$ then $c$ satisfies $x - c$ and so is integral over $D$ and also $c \in F$. Conversely, suppose $c \in F$ is integral over $D$. Then there exist $a_i \in D$, $n \in \mathbb{N}$ such that

$$c^n + a_{n-1}c^{n-1} + \ldots + a_0 = 0$$

As $c \in F$ so we have $c = \frac{r}{s}$ for some $r, s \in D$ with $(r, s) = 1$ and $s \neq 0$. Substitute this into the equation and clear the denominator, we have

$$r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0$$

Since $D$ is a unique factorisation domain, so each element can be expressed uniquely as a finite product of irreducibles. But each irreducible is prime in unique factorisation domain. So if $s$ is not a unit, we have some prime $p|s$. Then $p|r^n$ and hence $p|r$ as $p$ is prime, which contradicts $(r, s) = 1$. So $s$ must be a unit and so $c \in D$. □

**Corollary 12.18.** *Let $q \in \mathbb{Q}$. Then $q$ is an algebraic integer if and only if $q \in \mathbb{Z}$.*

*Proof.* Clearly every integer is an algebraic integer. Conversely, as $\mathbb{Z}$ is a unique factorisation domain and $\mathbb{Q}$ is its field of quotient. Thus by Theorem 12.17, if $q \in \mathbb{Q}$ is an algebraic integer (integral over $\mathbb{Z}$), then $q \in \mathbb{Z}$. □

**Proposition 12.19.** *Let $A = \mathbb{Z}$ and $B = \mathbb{Q}(i)$. Then the integral closure of $A$ in $B$ is*

$$A^B = \mathbb{Z}[i]$$

*Proof.* By Remark 12.4, it is enough to check the minimal polynomials. Let $\alpha = u + iv \in B$. Then if $v \neq 0$ then the minimal polynomial of $\alpha$ over $\mathbb{Z}$ is

$$P(x) = x^2 - 2ux + u^2 + v^2$$

Then we must have $2u \in \mathbb{Z}$ and $u^2 + v^2 \in \mathbb{Z}$. If $u$ has denominator 2, then it is impossible for $v \in \mathbb{Q}$ such that $u^2 + v^2 \in \mathbb{Z}$. Hence $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$.

If now $v = 0$ then the only algebraic integer in $\mathbb{Q}$ is integer by Corollary 12.18. Hence we conclude that $A^B = \mathbb{Z}[i]$. □

**Definition 12.20.** *An integral domain $D$ is said to be* **integrally closed** *or* **normal** *if and only if elements of its field of quotient that are integral over $D$ are those of $D$ itself.*

**Example 12.21.** *$D = \mathbb{Z}[\sqrt{-3}]$ is not integrally closed. The field of quotient is $F = \mathbb{Q}[\sqrt{-3}]$. Let $\alpha = \frac{1+\sqrt{-3}}{2} \in F$ and $\alpha \notin D$. Moreover, $\alpha$ satisfies the equation*

$$x^2 - x + 1 = 0$$

*and so it is not integrally closed. Hence by Theorem 12.17, it is not a unique factorisation domain.*

**Theorem 12.22.** *Every algebraic number is of the form $\frac{a}{b}$, where $a$ is an algebraic integer and $b$ is a non-zero ordinary integer.*

*Proof.* Let $c$ be an algebraic number. Then there exist $a_i \in \mathbb{Q}$ and $n \in \mathbb{N}$ such that

$$c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0 = 0$$

Let $b$ be the least common multiple of the denominator of $a_i$. Thus $b \in \mathbb{N}$ and $ba_i \in \mathbb{Z}$. Then clear the denominators, we have

$$(bc)^n + (ba_{n-1})(bc)^{n-1} + \ldots + (b^{n-1}a_1)(bc) + (b^n a_0) = 0$$

which shows that $bc$ is an algebraic integer, say $a$. Thus $c = \frac{a}{b}$ is of the required form. □

**Theorem 12.23.** *Let $K$ be a number field. Then the field of quotient of $\mathcal{O}_K$ is $K$.*

*Proof.* Let $F$ be the field of quotient of $\mathcal{O}_K$. Take $\alpha \in F$, then $\alpha = \frac{x}{y}$ for some $x, y \in \mathbb{O}_K$ and so $x, y \in K$, which means $\alpha \in K$. Hence $F \subseteq K$.

Now take any $\alpha \in K$. Since $K$ is a finite extension, hence algebraic, and so $\alpha$ is algebraic and therefore $\alpha = \frac{x}{y}$ for some algebraic integer $x$ and ordinary integer $y$ by Theorem 12.22. Also $x = \alpha y \in K$ and so $x \in \mathcal{O}_K$. Then $\alpha = \frac{x}{y} \in F$ and so $K \subset F$. Therefore, $F = K$. □

**Theorem 12.24.** *Let $K$ be a number field then $\mathcal{O}_K$ is integrally closed.*

*Proof.* Let $\alpha$ be integral over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is integral over $\mathbb{Z}$, so $\alpha$ is integral over $\mathbb{Z}$ by Theorem 12.14. So $\alpha$ must be an algebraic integer. By Theorem 12.23, the field of quotient of $\mathcal{O}_K$ is $K$ and so the result follows. □

## 12.5 Trace and norm

**Definition 12.25.** *Let $L/K$ be a finite field extension, define for any $x \in L$ the map:*

$$\phi_x : L \longmapsto L$$

*by*

$$\phi_x(y) = xy$$

*Clearly, this is a $K$-linear map. Then*

*(i) Denote the trace of $\phi_x$ by $T_{L/K}(x)$.*

*(ii) The bilinear form $T : L \times L \longmapsto K$ is defined by $T(x, y) = T_{L/K}(xy)$.*

*(iii) Denote the norm (determinant) of $\phi_x$ by $N_{L/K}(x)$.*

**Theorem 12.26.** **[Dedekind]** *Let $F, E$ be fields and $\sigma_1, \ldots, \sigma_n$ be $n$ distinct field homomorphisms from $F$ to $E$. Then they are linearly independent over $E$ in the $E$-vector space of all additive group homomorphisms from $F$ to $E$. In other words, if $c_1, \ldots, c_n \in E$, with $\sum_{i=1}^n c_i\sigma_i(x) = 0$ for all $x \in F$. Then $c_i = 0$ $\forall i$.*

*Proof.* Suppose not and let $k$ be the minimal integer for which $\{\sigma_1, \ldots, \sigma_k\}$ is linearly depend. So there exist $c_i \in E$ such that $\sum_{i=1}^{k} c_i\sigma_i(x) = 0$ and $c_k \neq 0$. As $\sigma_k \neq 0$, there is some $t \leq k$ such that $c_t \neq 0$. As $\sigma_t \neq \sigma_k$, choose $x \in F$ with $\sigma_t(x) \neq \sigma_k(x)$. For all $y \in F$, we have

$$\sum_{i=1}^{k} c_j\sigma_j(x)\sigma_j(y) = \sum_{j=1}^{k} c_j\sigma(xy) = 0$$

and hence

$$\sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j = 0$$

Therefore,

$$\sum_{j=1}^{k-1} c_j(\sigma_j(x) - \sigma_k(x))\sigma_j = \sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j - \sigma_k(x)\sum_{j=1}^{k} c_j\sigma_j = 0$$

As $\sigma_t(x) \neq \sigma_k(x)$, and $c_t \neq 0$, we conclude that $\{\sigma_1, \ldots, \sigma_{k-1}\}$ is linearly dependent, which is a contradiction. □

**Lemma 12.27.** *Let $F/K$ a finite separable extension with $[F : K] = n$, and*

$$Hom_K(F, E) = \{\sigma_1, \ldots, \sigma_n\}$$

*for an extension $E/K$. Then a subset $X = x_1, \ldots, x_n \subset F$ is a $K$-basis of $F$ if and only if the matrix $A \in GL_n(E)$, where $A_{ij} = \sigma_i(x_j)$*

*Proof.* If $X$ is a basis for of $F$. Let $X^* = \{x_1^*, \ldots, x_n^*\}$ be the dual basis. Then it is easy toe check that $X^*$ forms a $E$-basis for the set of $K$-linear maps from $F$ to $E$. Also, by Theorem 12.24, the set $\mathrm{Hom}_K(F, E) = \{\sigma_1, \ldots, \sigma,n\}$ also forms a $E$-basis for the set of $K$-linear maps from $F$ to $E$. Thus we have

$$\sigma_i = \sum_{j=1}^{n} \sigma_i(x_j)x_j^*$$

and as we can write $x_j^*$ in terms of linear combination of $\sigma_i$'s, the matrix $A_{ij} = \sigma_i(x_j)$ must be invertible and hence $\in GL_n(E)$.

Conversely, suppose the matrix $A_{ij} = \sigma_i(x_j) \in GL_n(E)$ and let

$$\sum_{j=1}^{n} c_j x_j = 0 \text{ for some } c_j \in K$$

Then $\sum_{j=1}^{n} c_j\sigma_i(x_j) = 0$ for all $i$. Thus we may invert the matrix $A$ and we have $c_i = 0$ for all $i$ and since $[F : K] = n$, so linear independence implies that $\{x_1, \ldots, x_n\}$ is a $K$-basis for $F$. □

**Theorem 12.28.** *Let $F/K$ be separable and $[L : K] = n$. Then*

$$T_{F/K}(x) = \sum_{i=1}^{n} \sigma_i(x), N_{F/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

*where $Hom_K(F, E) = \{\sigma_1, \ldots, \sigma_n\}$ for an extension $E$. In particular, $T_{F/K}(x)$ is not a zero map by Theorem 12.24 and hence surjective (as the dimension of $K$ as a $K$-vector space is 1.)*

*Proof.* The trace and norm is independent of the choice of basis. Let $X = \{x_1, \ldots, x_n\}$ be a $K$-basis of $F$, and let $X^* = \{x_1^*, \ldots, x_n^*\}$ be the dual basis. $\phi_x$ is a $K$-linear map from $F$ to $F$. By a simple fact of Linear Algebra, if $A$ is the matrix for $\phi_(x)$ with respect to the basis $X$, and $\phi_x^*$ is the dual map of $\phi_x$, then the matrix $B$ for $\phi_x^*$ with respect to the basis $X^*$ is the transpose of $A$. Thus, they have

the same trace and determinant. Hence we may calculate the trace and norm of $\phi_x^*$. By Theorem 12.24, $\mathrm{Hom}_K(F,E) = \{\sigma_1, \ldots, \sigma_n\}$ is a $E$-basis for the $K$-linear maps from $F$ to $E$. Also,

$$\phi_x^*(\sigma_j)(x_i) = \sigma_j m_x(x_i) = \sigma_j(xx_i) = \sigma_j(x)\sigma_j(x_i)$$

and so $\phi_x^*(\sigma_j) = \sigma_j(x)\sigma_j$. Therefore, the linear map $\phi_x^*$ is diagonal with entries $\sigma_j(x)$ with respect to the basis $\sigma_j$. Hence the result follows. □

## 12.6 Conjugates

We define the conjugates of an element over a subfield of $\mathbb{C}$

**Definition 12.29.** *Let $\alpha \in \mathbb{C}$ be algebraic over a subfield $K$ of $\mathbb{C}$. The* **conjugates** *of $\alpha$ over $K$ are the roots of $min_{K,\alpha}(x)$ in $\mathbb{C}$.*

**Example 12.30.** *The conjugates of $\sqrt{2}$ are $\pm\sqrt{2}$. The conjugates of $\frac{1+i}{\sqrt{2}}$ are $\frac{1\pm i}{\sqrt{2}}, \frac{-1\pm i}{\sqrt{2}}$.*

**Remark 12.31.** *If $K$ is a number field, then $K/\mathbb{Q}$ is separable and so the conjugates must be distinct.*

**Lemma 12.32.** *The conjugates of an algebraic integer is algebraic integers.*

*Proof.* Let $\alpha$ be an algebraic integer and let $h(x)$ be a monic polynomial in $\mathbb{Z}[x]$ such that $h(\alpha) = 0$. Then $min_{\mathbb{Q},\alpha}(x) \big| h(x)$ and so the conjugates of $\alpha$ are roots of $h(x)$ and so they are algebraic integers. □

By using the notation of conjugates, we may reprove an important fact as stated in Remark 12.4 without using Gauss's Lemma:

**Theorem 12.33.** *Let $\alpha$ be an algebraic integer. Then $min_{\mathbb{Q},\alpha}(x) \in \mathbb{Z}[x]$.*

*Proof.* Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be the conjugates of $\alpha$. Then

$$\begin{aligned} min_{\mathbb{Q},\alpha}(x) &= \prod_{i=1}^{n}(x - \alpha_i) \\ &= x^n - (\alpha_1 + \ldots \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n)x^{n-2} \\ &\quad + \ldots + (-1)^n\alpha_1 \ldots \alpha_n \end{aligned}$$

Let $e_i$ be the $i^{th}$ elementary symmetric function of $\alpha_j$'s. In other words,

$$e_i = \sum_{j_k} \prod_{k=1}^{i} \alpha_{j_k}$$

where the sum runs through all possible ordered $i$-subsets of $\{1, \ldots, n\}$. Then $e_i \in \mathbb{Q}$ as $min_{\mathbb{Q},\alpha}(x) \in \mathbb{Q}[x]$.

As the conjugates of an algebraic integer must also be algebraic integers, and the ring of integer is a ring. Hence the sum, product of algebraic integers are algebraic integers and so $e_i$ are algebraic integers. But $e_i \in \mathbb{Q}$ and hence $e_i \in \mathbb{Z}$. □

## 12.7 Complex embeddings

Let $K$ be a number field. $[K:\mathbb{Q}] = n$. We can write $n = r + 2s$ in such a way that there are exactly $r$ embeddings

$$\sigma_1, \ldots, \sigma_r : K \longmapsto \mathbb{R}$$

and $2s$ complex embeddings

$$\sigma_{r+1}, \ldots, \sigma_{2s+r} : K \longmapsto \mathbb{C}$$

To be precise, we start with some examples.

**Example 12.34.** *1. $K = \mathbb{Q}[x]/\langle x^2 - 5\rangle$ where $n = 2, r = 2, s = 0$. $K = \mathbb{Q}(\bar{x})$, where $\bar{x} = x \pmod{x^2 - 5}$. We have $\sigma_1(\bar{x}) = \sqrt{5}, \sigma_2(\bar{x}) = -\sqrt{5}$.*

*2. $K = \mathbb{Q}[x]/\langle x^2 + 5\rangle$ where $n = 2, r = 0, s = 2$. $K = \mathbb{Q}(\bar{x})$, where $\bar{x} = x \pmod{x^2 + 5}$. We have $\sigma_1(\bar{x}) = i\sqrt{5}, \sigma_2(\bar{x}) = -i\sqrt{5}$.*

*3. $K = \mathbb{Q}[x]/\langle x^3 - 2\rangle$ where $n = 3, r = 1, s = 2$. $K = \mathbb{Q}(\theta)$, where $\theta = x \pmod{x^3 - 2}$. We have $\sigma_1(\theta) = \sqrt[3]{2}, \sigma_2(\theta) = e^{\frac{2\pi i}{3}}\sqrt[3]{2}, \sigma_3(\theta) = e^{-\frac{2\pi i}{3}}\sqrt[3]{2}$*

We see from the above that these embeddings are just sending $x$ to roots of the polynomials. Because when we define the number field $K = \mathbb{Q}[x]/\langle P\rangle$ for a monic irreducible polynomial $P$, we do not identify the roots of $P$. In other words, every root of $P$ has the equal weight and so these embeddings make the extension more concrete.

Now we shall justify what we did above is valid. By the primitive element theorem, we may assume $K = \mathbb{Q}(\alpha)$ for some $\alpha$ and let $P = min_{\mathbb{Q},\alpha}(x)$. Then $K \cong \mathbb{Q}[x]/\langle P\rangle$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be the conjugates of $\alpha$. Define:

$$\sigma_i : K \ni \bar{x} \longmapsto \alpha_i\mathbb{C}$$

and extend linearly so that $\sigma_i$ is an embedding for all $i$. Let $r$ be the number of real roots and $2s$ be the number of complex roots (as they appear as conjugate pair), then we have $r$ real embeddings and $2s$ complex embeddings.

Then, we need to check that the definition of $\sigma_i$ is independent of the choice $\alpha$. Suppose $K = \mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. Let $Q(x) = min_{K,\beta}(x)$ and so we have

$$\mathbb{Q}[x]/\langle P\rangle \cong \mathbb{Q}[x]/\langle Q\rangle$$

and let $\phi$ be the ring homomorphism from $\mathbb{Q}[x]/\langle P\rangle$ to $\mathbb{Q}[x]/\langle Q\rangle$ such that $\phi(\lambda) = \lambda$ for all $\lambda \in \mathbb{Q}$. As each real number is a limit point of a rational sequence, thus $\phi$ extends to an isomorphism

$$\phi : \mathbb{R}[x]/\langle P\rangle \longmapsto \mathbb{R}[x]/\langle Q\rangle$$

and we now factorise $P$ and $Q$ in $\mathbb{R}[x]$. Use the fact that the only finite extension of $\mathbb{R}$ is $\mathbb{C} = \mathbb{R}[i]$. So each irreducible factors in $\mathbb{R}[x]$ has degree 1 or 2. Thus, writing $P = P_1 \ldots P_m$ with $P_i$ irreducible and let $r$be the number of $P_i$ of degree 1 and $s$ be the number of $P_i$ of degree 2. Thus by Chinese Remainder Theorem, we have

$$\mathbb{R}[x]/\langle P\rangle \cong \mathbb{R}[x]/\langle P_1\rangle \times \ldots \mathbb{R}[x]/\langle P_m\rangle$$

Similarly, factorise $Q$ into irreducible factors $Q_1, \ldots, Q_k$ and let $r'$ be the number of $Q_i$ of degree 1 and $s$ be the number of $Q_i$ of degree 2. Then as $\phi$ is isomorphism, we have

$$\mathbb{R}[x]/\langle P_1\rangle \times \ldots \times \mathbb{R}[x]/\langle P_m\rangle \cong \mathbb{R}[x]/\langle Q_1\rangle \times \ldots \times \mathbb{R}[x]/\langle Q_k\rangle$$

Thus we have $r + 2s = r' + 2s' = n$ because the degree of the extension must be the same and it is equal to the degree of the polynomial.

Also, consider the number of solutions to $x(x^2 + 1) = x^3 + x = 0$ on both sides. Then the quotient ring $\mathbb{R}[x]/\langle P_i \rangle$ with $P_i$ of degree 1 has only one root 0 and in each complex quotient ring, we have some element corresponding to the complex number $i$ because $\mathbb{R}[\alpha] = \mathbb{R}[i]$ if $\alpha \notin \mathbb{R}$. So each $\mathbb{R}[x]/\langle P_i \rangle$ with $P_i$ of degree 2 has three roots. Therefore, the number of roots is $3^s$ on the left hand side. Similarly, the number of roots is $3^{s'}$ on the right hand side. As they are isomorphic, we have $3^s = 3^{s'}$ and so $s = s'$. Therefore, $r = r', s = s'$ and each $\mathbb{R}[x]/\langle P_i \rangle \cong \mathbb{R}[x]/\langle Q_j \rangle$ for some $j$ and hence the embedding defined above is independent of the choice of $\alpha$ for which $K = \mathbb{Q}(\alpha)$.

Use this notation, we may define the conjugates of any $\alpha \in K$ to be $\sigma_1(\alpha), \ldots, \sigma_{r+2s}(\alpha)$. Here, we slightly modify the definition of conjugates in the sense that if $\alpha$ has minimal polynomial of degree less than $n$, then some of the above might be the same. But we still take those as a complete set of conjugates. For example, if $\alpha \in \mathbb{Q}$, then the conjugates of $\alpha$ is $\alpha, \alpha, \ldots, \alpha$ and we have $n$ of them.

**Proposition 12.35.** *Let $x, y$ be algebraic integers. Then each conjugate of $x + y, x - y, xy, xy^{-1}$ are of the form $x' + y', x' - y', x'y', x'y'^{-1}$ where $x', y'$ are conjugates of $x, y$ respectively.*

The proof is left as an exercise (see exercise 9).

## 12.8 $\mathcal{O}_K$ as finitely generated $\mathbb{Z}$-module

We proved earlier that $\mathcal{O}_K$ is a ring for any number field $K$. The last topic in the chapter is to prove that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module.

**Lemma 12.36.** *The bilinear form $T$ defined in Definition 12.25 is non-degenerate if $F/K$ is separable.*

*Proof.* Let $F = K(x)$ for some $x \in F$ and so $\{1, x, \ldots, x^{n-1}\}$ is a basis. Let $x_1 = x, \ldots, x_n$ be the conjugates of $x$. Then by Proposition 12.35, the conjugates of $x^r$ are $x_1^r, \ldots, x_n^r$. Thus the $i, j$ entry of the matrix $T$ is $T(x^{i-1}, x^{j-1})$, which is precisely $T_{F/K}(x^{i+j-2}) = \sum_{q=1}^{n} x_q^{i+j-2}$. Let $V$ be the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ . & . & \ldots & . \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}$$

Then $T = V^t V$ and so the determinant

$$\det T = (\det V^t)(\det V) = (\det V)^2$$

But $x_i \neq x_j$ as $L/K$ separable, so $\det V \neq 0$ and so $\det T \neq 0$. Therefore, it is non-degenerate. □

**Lemma 12.37.** *Suppose $A \subseteq B$ be integral domains and $A$ is integrally closed (normal). Let $F$ be the field of quotient of $A$ and $z \in B$ be integral over $A$. Then the minimal polynomial $P$ of $z$ over $F[x]$ lies in $A[x]$.*

*Proof.* WLOG, let $P(x) = x^n + e_{n-1}x^{n-1} + \ldots + e_1 x + e_0$ with $e_i \in F$. Now $e_i$ is the elementary function of conjugates of $z$ (see Theorem 12.33). As $z$ is integral over $A$, so then $z$ satisfies a monic polynomial $f \in A[x]$, such that $f(z) = 0$ and hence $f(z_i) = 0$ for all $z_i$ conjugate of $z$ because $P|f$. Thus $z_i$ is integral over $A$. Hence, the sum and product of $z_i$ are integral over $A$ and so $e_i$ is integral over $A$ for all $i$. But $A$ is integrally closed. Therefore $e_i \in A$ for all $i$ and so $P \in A[x]$. □

**Theorem 12.38.** *Let $A$ be a Noetherian domain which is integrally closed. Let $F$ be the field of quotient of $A$ and $K/F$ a finite separable extension. Then the integral closure $A^K$ of $A$ in $K$ is a finitely generated $A$-module. In particular, by taking $A = \mathbb{Z}, F = \mathbb{Q}$ and $K$ be any number field, the ring of integers $\mathcal{O}_K$ is a finitely generated $Z$-module.*

*Proof.* As $K/F$ is finite, it is algebraic and so let $u \in K$, there exist $q_i \in F$ and $n \in \mathbb{N}$ such that

$$u^n + q_{n-1}u^{n-1} + \ldots + q_1 u + q_0 = 0$$

Clearing the denominators, we have $a_i \in A$ such that

$$a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 = 0$$

Multiply both sides by $a_n^{n-1}$, so

$$(a_n u)^n + (a_n u)^{n-1} + \ldots + (a_n u)an - 2_n a_1 + a_n^{n-1}a_0 = 0$$

Thus, $a_n u$ is integral over $A$. (This is an analogue of Theorem 12.22.) So $a_n u \in A^K$. Hence, given any $F$-basis $V \subset K$ of $K$ we can multiply them by some suitable elements so that it is an $F$-basis $V'$ of $K$ such that $V' \subset A^K$.

By Lemma 12.36, the bilinear form $T$ is non-degenerate as $K/F$ separable. So we can choose a basis $U = \{u_1, \ldots, u_n\} \subset K$ such that

$$T(u_i, u_j) = \delta_{ij}$$

and a basis $V = \{v_1, \ldots, v_n\}$ such that $v_i = a_i u_i$ for some $a_i$ that $v_i \in A^K$. Then

$$T(v_i, v_j) = a_i a_j \delta_{ij}$$

Now for any $x \in A^K$ we have $x = \sum_{j=1}^n x_j v_j$ for some $x_j \in F$ and $v_j \in A^K$. As $A^K$ is a ring, $xv_i \in A^K$ for all $i$. By Lemma 12.37, as $A$ is integrally closed, so $min_{F,xv_i}(x) \in A[x]$, in particular, $T_{K/F}(xv_i) \in A$ because it is the coefficient of subleading term of $min_{F,xv_i}(x)$. But

$$T_{K/F}(xv_i) = T_{K/F}(\sum_{j=1}^n x_j v_j v_i) = \sum_{j=1}^n x_j T(v_i, v_j) = a_i x_i$$

So $a_i x_i \in A$ and since $a_i \in A$, we conclude that $x_i \in A$. Thus, $A^K$ is contained in an $A$-module generated by $v_1, \ldots, v_n$. As $A$ is Noetherian, so $A^K$ is finitely generated. □

**Corollary 12.39.** *Let $K$ be a number field. Then $\mathcal{O}_K$ is a Noetherian domain.*

*Proof.* By Theorem 12.38, $\mathcal{O}_K$ is a finitely generated $Z$-module. Then as $Z$ is Noetherian, $\mathcal{O}_K$ is Noetherian. □

## 12.9 Exercises

1. Let $\theta$ be aroot of $x^3 + 6x + 34$. Prove that $\mathbb{Z}[\theta]$ is not integrally closed.

2. Prove that $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$ is not integrally closed. Show further that $\mathbb{Z}[\sqrt{2}, \sqrt{a}]$ is not integrally closed whenever $a$ is a square free odd integer and hence show that it holds for every square free integer $a$.

3. Let $K = \mathbb{Q}(\sqrt{5})$. Prove that the ring of integer $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

4. Let $K = \mathbb{Q}(\sqrt{3})$. Prove that the ring of integer $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$.

5. Let $A$ and $B$ be integral domains with $A \subseteq B$ and $B$ integral over $A$. If $I$ is a non-zero ideal of $B$, prove that $I \cap A$ is a non-zero ideal of $A$.

6. Prove that $\frac{10^{\frac{2}{3}}-1}{\sqrt{-3}}$ is an algebraic integer.

7. Let $m$ be a square free integer, and $m \equiv 1 \pmod 4$. Prove that $\mathbb{Z}[\sqrt{m}]$ is not integrally closed.

⋆ 8. Let $F/K$ be a cyclic extension of degree $n$, i.e. $[F : K] = n$ and $\mathrm{Hom}_K(F, F) = \{\sigma, \sigma^2, \ldots, \sigma^n = id\}$. Prove that $T_{F/K}(\sigma(x) - x) = 0$ for all $x \in F$. Deduce that if $y \in F$ then $T_{F/K}(y) = 0$ if and only if $y = \sigma(x) - x$ for some $x \in F$. The last part of this question may be referred to **Hilbert's Theorem 90**.

9 Prove Proposition 12.35

## 12.10 Hint and Solutions

1. Consider $\frac{1+\theta}{3} \in \mathbb{Q}[\theta]$, the field of quotient of $\mathbb{Z}[\theta]$. We have
$$\theta^3 + 6\theta + 34 = 0$$
and so
$$\frac{\theta^3}{27} + \frac{2\theta}{9} + \frac{34}{27} = 0$$
But this is
$$y^3 - y^2 + y + 1 = 0$$
where $y = \frac{1+\theta}{3}$ and so it is algebraic but it is not in $\mathbb{Z}[\theta]$.

2. $\sqrt{10} = \sqrt{2}\sqrt{5} \in \mathbb{Z}[\sqrt{2}, \sqrt{5}]$, and so $y = \frac{\sqrt{2}+\sqrt{10}}{2} \in F$, the field of quotient of $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$. $y^2 = 3 + \sqrt{5}$ and so
$$y^4 - 6y^2 + 4 = 0$$
Hence $y$ is an algebraic integer but not in $\mathbb{Z}[\sqrt{2}, \sqrt{10}]$

Now if $a$ is square free and odd, we consider the element $y = \frac{\sqrt{2}+\sqrt{2a}}{2}$ in the field of quotient of $\mathbb{Z}[\sqrt{2}, \sqrt{a}]$. Then $y^2 = \frac{1+a}{2} + \sqrt{a}$, where $\frac{1+a}{2}$ is an integer because $a$ is odd. Thus,
$$y^4 - (1 + a)y^2 - a = 0$$
and so $\mathbb{Z}[\sqrt{2}, \sqrt{a}]$ is not integrally closed.

If $a$ is square free and even, then observe that
$$\mathbb{Z}[\sqrt{2}, \sqrt{a}] = \mathbb{Z}\left[\sqrt{2}, \sqrt{\frac{a}{2}}\right]$$
where $\frac{a}{2}$ is odd as $a$ is square free, and so use the previous part.

3. Let $\alpha = a + b\sqrt{5}, a, b \in \mathbb{Q}$. If $b = 0$ then $a \in \mathbb{Z}$. If $b \neq 0$, the minimal polynomial is $x^2 - 2ax + a^2 - 5b^2$. So we need $2a, a^2 - 5b^2 \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$. If $a$ has denominator 2, i.e. $a = \frac{c}{2}$, where $c$ is odd. Then $b$ has denominator at most 2 and $b \notin \mathbb{Z}$. So we may assume $b = \frac{d}{2}$ for some $d$ odd. Thus,
$$a^2 - 5b^2 = \frac{c^2 - 5d^2}{4} \in \mathbb{Z}$$
because $c^2, 5d^2 \equiv 1 \pmod 4$. Hence, combine the case $a \in \mathbb{Z}$, and the case when $a = \frac{c}{2}$, we conclude that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

4. Let $\alpha = a + b\sqrt{3}, a, b \in \mathbb{Q}$. If $b = 0$ then $a \in \mathbb{Z}$. If $b \neq 0$, the minimal polynomial is $x^2 - 2ax + a^2 - 3b^2$. Thus $2a, a^2 - 3b^2 \in \mathbb{Z}$. If $a \in \mathbb{Z}$, so is $b$. If $a$ has denominator 2, say $a = \frac{c}{2}$, then $b$ has denominator at most 2 and $b \notin \mathbb{Z}$. If $b = \frac{d}{2}$ for some $d$ odd. Then we must have

$$\frac{c^2 - 3d^2}{4} \in \mathbb{Z}$$

But this is impossible, as $c^2 - 3d^2 \equiv 2 \pmod 4$. Hence we have $a, b \in \mathbb{Z}$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$.

5. Pick any $0 \neq x \in I$, so $x \in B$ and there exist $a_i \in A$ and a smallest $n \in \mathbb{N}$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

and we may assume $a_0 \neq 0$ otherwise we can divide the equation by $x$ and get a lower degree. As $x \in I$, each $a_i x^i \in I$ and $0 \in I$, we have $a_0 \in I$. Hence $a_0 \in I \cap A$, and so $I \cap A$ is non-zero.

6. Let $x = \frac{10^{\frac{2}{3}} - 1}{\sqrt{-3}}, y = 10^{\frac{1}{3}}, z = \sqrt{-3}$. Then we have

$$zx + 1 = y^2 \text{ and so } zx^3 + 3x^2 - zx + 33 = 0$$

Rearrange, we have

$$z(x^3 - x) = (-3x^2 - 33) \text{ and so } x^6 + x^4 + 67x^2 + 363 = 0$$

and so it is an algebraic integer.

7. Consider the element $x = \frac{1+\sqrt{m}}{2}$. Then $x^2 - x + \frac{1-m}{4} = 0$ and $\frac{1-m}{4}$ is an integer because $m \equiv 1 \pmod 4$.

8. $|\mathrm{Hom}_K(F, F)| = n = [F : K]$, so we have $F/K$ separable and so by Theorem 12.28,

$$T_{F/K}\left(\sigma(x) - x\right) = \sum_{i=1}^{n} \sigma^i\left(\sigma(x) - x\right) = 0$$

Then we need to prove the converse. Let $Tr_{F/K}(y) = 0$ for some $y \in F$. By Theorem 12.28, $Tr_{F/K}$ is not a zero map and hence there exists $z \in F$ such that $T_{F/K}(z) \neq 0$. Define $x \in F$ by

$$\begin{aligned} -xT_{F/K}(z) &= yz + \left(y + \sigma(y)\right)\sigma(z) + \ldots + \\ &\quad \left(y + \sigma(y) + \ldots + \sigma^{n-1}(y)\right)\sigma^{n-1}(z) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{i} \sigma^j(y)\sigma^i(z) \end{aligned}$$

Then

$$-\left(\sigma(x) - x\right)T_{F/K}(z) = -y\sum_{i=1}^{n-1}\sigma^i(z) + z\sum_{i=1}^{n-1}\sigma^i(y) = -yT_{F/K}(z)$$

using $\sum_{i=0}^{n-1}\sigma^i(y) = 0$. Thus, we have $y = \sigma(x) - x$.

9. It is easy to check that any embedding $\sigma$ is a homomorphism (in fact isomorphism) and hence the result follows. Suppose $K = \mathbb{Q}(\theta)$ for some $\theta$ and $\sigma(\theta) = \alpha$ for some $\alpha$. Then:

(i) Let

$$a = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, b = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1} \in K$$

with $a_i, b_i \in \mathbb{Q}$. Then

$$\sigma(a+b) = a_0 + b_0 + (a_1 + b_1)\alpha + \ldots + (a_{n-1} + b_{n-1})\alpha^{n-1}$$

(ii) Let

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}, g(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$$

such that $f(\theta) = a, g(\theta) = b$. Let $P(x) = min_{\mathbb{Q},\theta}(x)$. Then there exist $q(x), r(x)$ such that

$$f(x)g(x) = P(x)q(x) + r(x) \text{ with } \deg r < \deg P$$

Let $x = \theta$, so we have $r(\theta) = ab$. Also

$$P(\alpha) = P(\sigma(\theta)) = \sigma(P(\theta)) = 0$$

so

$$\begin{aligned} \sigma(ab) &= \sigma(r(\theta)) = r(\sigma(\theta) = r(\alpha) \\ &= r(\alpha) + P(\alpha)q(\alpha) \\ &= f(\alpha)g(\alpha) \\ &= \sigma(a)\sigma(b) \end{aligned}$$

# 13 Dedekind Domain

## 13.1 Dedekind domains

We have proved that if $K$ is a number field, then by Theorem 12.24 and Theorem 12.39, $\mathcal{O}_K$ is integrally closed and Noetherian. We shall prove firstly some other important facts of $\mathcal{O}_K$.

**Lemma 13.1.** *Let $K$ be a number field. Let $I$ be a non-zero ideal of $\mathcal{O}_K$. Then $I \cap \mathbb{Z} \neq \varnothing$ and $\mathcal{O}_K/I$ is finite.*

*Proof.* Let $0 \neq x \in I$. Then there exist $a_i \in \mathbb{Z}$ and $n \in \mathbb{N}$ such htat

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

and we may assume $a_0 \neq 0$ (otherwise we divide the equation by $x$). Then

$$a_0 = -x^n - a_{n-1}x^{n-1} - \ldots - a_1 x \in I$$

and so $I \cap \mathbb{Z} \neq \varnothing$.

Now let $\{e_1, \ldots, e_n\}$ generates $\mathcal{O}_K$ as a $\mathbb{Z}$-module and let $\bar{e_i} = e_i \pmod{I}$. Then $\{\bar{e_1}, \ldots, \bar{e_n}\}$ generates $\mathcal{O}_K/I$ over the ring $\mathbb{Z}/I \cap \mathbb{Z}$. As $\mathbb{Z}$ is a principal ideal domain and so we may assume $I \cap \mathbb{Z} = \langle \alpha \rangle$ and so $\mathbb{Z}/I \cap \mathbb{Z} \cong \{0, 1, \ldots, \alpha - 1\}$ is finite. Hence $\mathcal{O}_K/I$ a is finitely generated module by a finite ring, which must be finite. □

**Theorem 13.2.** *Every non-zero prime ideal $P \subseteq \mathcal{O}_K$ is maximal.*

*Proof.* Since $P$ is prime, $\mathcal{O}_K/P$ is an integral domain and it is finite by Lemma 13.1. But any finite integral domain is a field. Thus $\mathcal{O}_K/P$ is a field and so $P$ is maximal. □

**Theorem 13.3.** *For all primes $p \in \mathbb{Z}$, there exists a prime ideal $Q \subset \mathcal{O}_K$ such that $Q \cap \mathbb{Z} = p\mathbb{Z}$. Moreover, there exists only finitely many such $Q$.*

*Proof.* If $\langle p \rangle \mathcal{O}_K \neq \mathcal{O}_K$, then pick any maximal ideal $Q$ in $\mathcal{O}_K$ containing $\langle p \rangle \mathcal{O}_K$ and hence prime and clearly $Q \cap \mathbb{Z} = p\mathbb{Z}$ because $p$ is a prime number so $Q$ cannot contain any other integer which is not multiple of $p$, otherwise $Q \cap \mathbb{Z} = \mathbb{Z}$, which is impossible. If $\langle p \rangle \mathcal{O}_K = \mathcal{O}_K$. Then as $1 \in \mathcal{O}_K$, so we must have $\frac{1}{p} \in \mathcal{O}_K$, which is impossible.

Moreover, we look at the prime ideals $Q$ in $\mathcal{O}_K$ containing $\langle p \rangle \mathcal{O}_K$. But $\mathcal{O}_K/\langle p \rangle \mathcal{O}_K$ is finite by Lemma 13.1. So each prime ideal $Q$ containing $\langle p \rangle \mathcal{O}_K$ corresponds to a prime ideal in $\mathcal{O}_K/\langle p \rangle \mathcal{O}_K$ and so we must have finitely many of them. □

These give all the properties we need so far for $\mathbb{O}_K$. An integral domain with these properties is called a **Dedekind** domain named after Richard Dedekind, the creator of modern theory of ideals. Formally,

**Definition 13.4.** *An integral domain $D$ which satisfies:*

1. *$D$ is a Noetherian domain.*

2. *$D$ is integrally closed.*

3. *each prime ideal of $D$ is a maximal ideal*

*is called a* **Dedekind** *domain.*

Therefore, we have shown that $\mathcal{O}_K$ is a Dedekind domain.

**Theorem 13.5.** *Let $D$ be a principal ideal domain. Then $D$ is a Dedekind domain.*

*Proof.* $D$ is a principal ideal domain and hence Noetherian. Also a unique factorisation domain and hence integrally closed by Theorem 12.17. Finally, each prime ideal in a principal ideal domain is maximal. Hence $D$ is a Dedekind domain. □

The main objective of this chapter is to show that every non-zero proper ideal in a Dedekind domain can be expressed uniquely as a product of prime ideals.

## 13.2 Ideals in a Dedekind domain

The first step of our objective is to show that every proper ideal contains a product of prime ideals.

**Theorem 13.6.** *In a Noetherian domain, every non-zero ideal contains a product of prime ideals.*

*Proof.* Suppose not. Let $D$ be Noetherian which has at least one non-zero ideal that does not contain a product of prime ideals. Let $S$ be the set of such ideals and so $S$ is non-empty. As $D$ is Noetherian, we have an ideal $A$ which is maximal with the above property, i.e. $A \in S$ and if $B \in S$, then $B \subseteq A$. Clearly, $A$ is not prime and so (by Theorem 7.49) we have ideals $B$ and $C$ such that

$$BC \subseteq A, B \nsubseteq A, C \nsubseteq A$$

Define the ideals $B_1$ and $C_1$ of $D$ by

$$B_1 = A + B, C_1 = A + C$$

and so $A \subset B_1, A \subset C_1$. So $B_1, C_1 \notin S$ by maximality of $A$. Then we have prime ideals $P_1, \ldots, P_m$, $Q_1, \ldots, Q_n$ such that

$$P_1 \cdots P_m \subseteq B_1, Q_1 \cdots Q_n \subseteq C_1$$

But $B_1C_1 = (A + B)(A + C) \subseteq A$ because $BC \subseteq A$. So

$$P_1 \cdots P_m Q_1 \cdots Q_n \subseteq A$$

contradicting $A \in S$. □

As a Dedekind domain is Neotherian, so we have an immediate consequence:

**Theorem 13.7.** *In a Dedekind domain every non-zero ideal contains a product of prime ideals.*

We shall extend the definition of ideals in an integral domain.

**Definition 13.8.** *Let $D$ be an integral domain. Let $K$ be the field of quotient of $D$. A non-empty set $I$ of $K$ with the following properties:*

*(i)* $\alpha \in I, \beta \in I \Rightarrow \alpha + \beta \in I$.

*(ii)* $\alpha \in I, r \in D \Rightarrow r\alpha \in I$.

*(iii) there exists $\gamma \in D$ with $\gamma \neq 0$ such that $\gamma I \subseteq D$*

*is called a* **fractional ideal** *of $D$. Equivalently, it is a $D$-submodule of $K$ such that there exists $0 \neq \gamma$ with $\gamma I \subseteq D$. The element $\gamma$ can be thought of as a 'common denominator'.*

**Example 13.9.** *The set*

$$I = \left\{ \frac{n}{25} : n \in \mathbb{Z} \right\}$$

*is a fractional ideal of* $\mathbb{Z}$ *because clearly it satisfies (i) and (ii) and* $25I \subseteq \mathbb{Z}$.

**Example 13.10.** *The set*

$$I = \left\{ \frac{n}{3^m} : n \in \mathbb{Z}, m \in \mathbb{N} \cup 0 \right\}$$

*is not a fractional ideal of* $\mathbb{Z}$ *because we have no such* $\gamma$ *with* $\gamma I \subseteq \mathbb{Z}$.

It is clear that the usual ideal of $D$ is also a fractional ideal of $D$ by taking $\gamma = 1$. We often refer to the usual ideals of $D$ in the ordinary sense as **integral ideal**. It is easy to check that if $I$ is a fractional ideal and $\gamma$ is the 'common denominator', then $\gamma I$ is an integral ideal of $D$. Therefore, if $I$ is a fractional ideal, then

$$I = \frac{1}{\gamma} I'$$

for some integral ideal $I'$ of $D$. Note this representation is non unique as we have

$$\frac{1}{\gamma} I' = \frac{1}{\gamma\delta}(\delta I')$$

In a Dedekind domain $D$, as $D$ is Noetherian, so every ideal is finitely generated, say

$$I' = \langle \alpha_1, \ldots, \alpha_n \rangle$$

Then

$$I = \frac{1}{\gamma} I' = \frac{1}{\gamma} \langle \alpha_1, \ldots, \alpha_n \rangle$$

that is, every fractional ideal $I$ of $D$ is also finitely generated. We can also extend the definition of sum and product of ideals to fractional ideals. It is easily checked that (see exercise 2) if $I_1, I_2$ are fractional ideals of $D$, so are $I_1 + I_2, I_1 I_2$.

**Definition 13.11.** *Let* $D$ *be an integral domain and* $K$ *the field of quotient. For any fractional ideal* $I$ *of* $D$*, define*

$$I^{-1} = \{ x \in K : xI \subseteq D \}$$

**Lemma 13.12.** *Let* $D$ *be an integral domain and* $K$ *the field of quotient. Then* $I^{-1}$ *is a fractional ideal for any fractional ideal* $I$ *of* $D$.

*Proof.* We check that $I^{-1}$ satisfies the properties of a fractional ideal.

(i) Let $\alpha, \beta \in I^{-1}$, then $(\alpha+\beta)x = \alpha x + \beta x \in D$ for all $x \in I$ because $D$ is a ring and so $\alpha+\beta \in I^{-1}$.

(ii) Let $\alpha \in I^{-1}$ then $\alpha I \subset D$ and so $r\alpha I \subset D$ for all $r \in D$.

(iii) Pick any $0 \neq \gamma \in I$ and $\alpha \in I^{-1}$ then $\gamma\alpha \in D$ because $\alpha I \subseteq D$. Therefore, $\gamma I^{-1} \subseteq D$

Thus, $I^{-1}$ is a fractional ideal of $D$. □

The notation of $I^{-1}$ suggests that it is in some sense the inverse of $I$. We need several steps to prove this. We shall firstly deduce that

**Theorem 13.13.** *Let* $D$ *be a Dedekind domain. Let* $P$ *be a prime ideal of* $D$*. Then* $PP^{-1} = D$.

*Proof.* As $P$ is an integral ideal of $D$, so $1 \in P^{-1}$ and so $P \subseteq PP^{-1}$. But in a Dedekind domain, every prime ideal is maximal, so $PP^{-1} = P$ or $D$. Further, if $\alpha \in D$, then $\alpha P \subseteq D$ , and so we have $D \subseteq P^{-1}$.

Next we show that $D$ is strictly contained in $P^{-1}$. Let $0 \neq \beta \in P$. By Theorem 13.7 there exist prime ideals $P_1, \ldots, P_k$ $(k \geq 1)$ such that

$$P \subseteq \langle \beta \rangle \supseteq P_1 \cdots P_k$$

Let $k$ be the least integer such that this inclusion holds. As $P$ is a prime ideal, so we have by Theorem 7.49 that $P_i \subseteq P$ for some $i$ and we may relabel $P_1$ as $P_1$. then we have $P_1 \subseteq P$. But $P_1$ is prime and $D$ is a Dedekind domain, so $P_1$ is maximal and so

$$P_1 = P$$

If $k = 1$ then $P_1 = P = \langle \beta \rangle$ and $\beta$ is not a unit. Let $\gamma = \frac{1}{\beta} \in K$ so that

$$\gamma P = \frac{1}{\beta}\langle \beta \rangle = \langle 1 \rangle = D$$

and so $\gamma \in P^{-1}$. But $\gamma \notin D$ because $\beta$ is not a unit. Thus $D \subset P^{-1}$ in this case.

If $k \geq 2$, then by minimality of $k$, we have

$$P_2 \cdots P_k \not\subseteq \langle \beta \rangle$$

Hence there exists $\delta \in P_2 \cdots P_k$ such that $\delta \notin \langle \beta \rangle$. Define $\gamma = \frac{\delta}{\beta} \in K$, and so $\gamma \notin D$ because $\delta \notin \langle \beta \rangle$. Then

$$P\langle \delta \rangle = P_1\langle \delta \rangle \subseteq P_1 \cdots P_k \subset \langle \beta \rangle$$

so

$$P\gamma = P\frac{\delta}{\beta} \subseteq D$$

and thus $\gamma \in P^{-1}$. So in both cases we have proved that there exists some $\gamma \in P^{-1}$ but not in $D$. Hence $D \subset P^{-1}$.

Finally, we show that $PP^{-1} \neq P$ and so we have $PP^{-1} = D$. Suppose $PP^{-1} = P$. Then if $\alpha \in P^{-1}, \beta \in P^{-1}$, we have

$$\alpha P \subseteq P, \beta P \subseteq P$$

and so

$$\alpha\beta P \subseteq \alpha P \subseteq P \subset D$$

Thus, $\alpha\beta \in P^{-1}$ and so $P^{-1}$ is an integral domain in $D$. As $D$ is Noetherian, $P^{-1}$ is finitely generated $D$-module. Then in Lemma 12.9, take $A$ to be $D$ and $B$ to be $P^{-1}$ here. Let $C = B = P^{-1}$ in Lemma 12.9 (iii) then (iii) $\Rightarrow$ (i) implies that for any $x \in P^{-1}$, $x$ is integral over $D$ and hence $P^{-1}$ is integral over $D$. But $D$ is integrally closed so we have $D = P^{-1}$ which contradicts $D \subset P$. Therefore, $PP^{-1} = D$. □

## 13.3 Factorisation into prime ideals

In this subsection we shall prove the fundamental property of a Dedekind domain $D$, namely, that every proper integral ideal of $D$ can be expressed uniquely up to reordering as a product of prime ideals.

Note: There is a proof using the knowledge of Artinian ring which will be given later when we introduce the concept of Artianian ring. The proof given here is however, based on the Theorem 13.13 and is elementary.

**Theorem 13.14.** *Let $D$ be a Dedekind domain. Then every integral ideal is a product of prime ideals and this factorisation is unique up to reordering. In other words, if*

$$P_1 \cdots P_k = Q_1 \cdots Q_l$$

*Then $k = l$ and $P_i = Q_i$ after relabeling.*

*Proof.* Suppose there exist integral ideals of $D$ which are not products of prime ideals. Let $S$ be the set of such ideals. As $D$ is Dedekind, it is Noetherian, and so there exists an ideal $A$ which is maximal with such property, i.e. $A \in S$ and $J \subseteq A$ if $J \in S$ and since $D$ is Noetherian, there exists a maximal ideal $B$ containing $A$. Let $C$ be the inverse of $B$, $C = B^{-1}$. Then as $B$ is an integral ideal, it is clear that $D \subseteq C$ and so

$$A = AD \subseteq AC \subseteq BC = D$$

Therefore, from above $AC$ is an integral ideal of $D$.

Now as $B$ is a maximal ideal, so $B$ is prime and so from the proof of Theorem 13.13, we have $D \subset C$. Thus $A \subset AC$ and so by maximality of $A$, there exist prime ideals $P_1, \ldots, P_k$ $(k \geq 1)$ such that

$$AC = P_1 \cdots P_k$$

Multiply both sides by $B$ so we have

$$A = P_1 \cdots P_k B$$

which is a product of prime ideals and so $A \notin S$, which is a contradiction.

To prove uniqueness, suppose we have two prime factorisation

$$P_1 \cdots P_k = Q_1 \cdots Q_l$$

Then

$$P_1 \cdots P_k \subseteq Q_1$$

and so as $Q_1$ is prime, we have

$$P_i \subseteq Q_1$$

for some $i$. We may relabel so that $P_1 \subseteq Q_1$. As $P_1$ is prime and so $P_1$ is maximal so $P_1 = Q_1$ since $Q_1 \neq D$. Thus we may multiply the inverse $P_1^{-1}$ on both sides so that

$$P_2 \cdots P_k = Q_2 \cdots Q_l$$

Continue the above process inductively and thus we conclude that $k = l$ and $P_i = Q_i$ after relabeling. □

If we use the notation of exponential, i.e. $P^k$ is the the multiplication of $k$ lots of $P$, and $P^{-k}$ means $(P^{-1})^k$ for $k > 0$, then we have

**Theorem 13.15.** *Let $D$ be a Dedekind domain. Then every fractional ideal $I$ can be factorised uniquely into the form*

$$\prod_{i=1}^{k} P_i^{e_i}$$

*for some $k$ and $P_1, \ldots, P_k$, where $P_i$ is prime ideal and $e_i \neq 0$ for all $i$.*

*Proof.* The case when $I$ is an integral ideal is proved in Theorem 13.14. To prove it also holds for fractional ideal, we simply notice that there exists $\gamma$ such that $\gamma I \subseteq D$. So we have a factorisation for $\gamma I$ and hence for $I$ since we have $I = \frac{1}{\gamma}(\gamma I)$. The uniqueness is proved in a similar manner. If

$$P_1^{e_1} \cdots P_k^{e_k} = Q_1^{f_1} \cdots Q_l^{f_l}$$

Then we multiply both sides by suitable $P_i^{e_i}$ and $Q_j^{f_j}$ to delete the negative exponential. Then the proof is identical to the integral ideal case. □

**Example 13.16.** *Let $D = \mathbb{Z}[\sqrt{-5}]$, as $D$ is $\mathbb{O}_K$ for $K = \mathbb{Q}[\sqrt{-5}]$ so it is a Dedekind domain. $D$ is not a unique factorisation domain as $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. But by Theorem 13.15 the ideal $\langle 6\rangle$ can be uniquely factorised into prime ideals. We shall see how this happens. Let*

$$P_1 = \langle 2, 1+\sqrt{-5}\rangle, P_2 = \langle 3, 1+\sqrt{-5}\rangle, P_3 = \langle 3, 1-\sqrt{-5}\rangle$$

*Then we have*

$$\begin{aligned} P_2P_3 &= \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle \\ &= \langle 9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6\rangle \\ &= \langle 3\rangle\langle 3, 1+\sqrt{-5}, 1-\sqrt{-5}, 2\rangle \\ &= \langle 3\rangle\langle 1\rangle = \langle 3\rangle \end{aligned}$$

*and clearly $P_1 = \langle 2, 1+\sqrt{-5}\rangle = \langle 2, 1-\sqrt{-5}\rangle$ so*

$$\begin{aligned} P_1^2 &= \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle \\ &= \langle 4, 2(1+\sqrt{-5}), 2(1-\sqrt{-5}), 6\rangle \\ &= \langle 2\rangle\langle 2, 1+\sqrt{-5}, 1-\sqrt{-5}, 3\rangle \\ &= \langle 2\rangle\langle 1\rangle = \langle 2\rangle \end{aligned}$$

*Similarly,*

$$\begin{aligned} P_1P_2 &= \langle 2, 1+\sqrt{-5}\rangle\langle 3, 1+\sqrt{-5}\rangle \\ &= \langle 6, 2(1+\sqrt{-5}), 2(1-\sqrt{-5}, (1+\sqrt{-5})^2\rangle \\ &= \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}, 2, 3, 1+\sqrt{-5}\rangle \\ &= \langle 1+\sqrt{-5}\rangle\langle 1\rangle = \langle 1+\sqrt{-5}\rangle \end{aligned}$$

*and*

$$\begin{aligned} P_1P_3 &= \langle 2, 1-\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle \\ &= \langle 6, 2(1-\sqrt{-5}), 3(1-\sqrt{-5}), (1-\sqrt{-5})^2\rangle \\ &= \langle 1-\sqrt{-5}\rangle\langle 1+\sqrt{-5}, 2, 3, 1-\sqrt{-5}\rangle \\ &= \langle 1-\sqrt{-5}\rangle\langle 1\rangle = \langle 1-\sqrt{-5}\rangle \end{aligned}$$

*Thus, we see that*

$$\langle 2\rangle = P_1^2, \langle 3\rangle = P_2P_3, \langle 1+\sqrt{-5}\rangle = P_1P_2, \langle 1-\sqrt{-5}\rangle = P_1P_3$$

*and so we have*

$$\langle 6\rangle = \langle 2\rangle\langle 3\rangle = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle = P_1^2P_2P_3$$

**Definition 13.17.** *Let $D$ be a Dedekind domain. Let $A$ and $B$ be non-zero integral ideals of $D$. We say $A$* **divides** *$B$, written $A|B$, if there exists an integral ideal $C$ of $D$ such that $B = AC$.*

It is clear that once we have unique factorisation of each integral ideal, we have many similar properties of the ideals in Dedekind domain as integers in $\mathbb{Z}$. For example, Let

$$A = \prod_{i=1}^{n} P_i^{e_i} \text{ and } B = \prod_{i=1}^{n} P_i^{f_i}$$

$e_i, f_i \geq 0$. Then $A|B \iff e_i \leq f_i$ for all $i$. More importantly, the factorisation of fractional ideal suggests that the set of non-zero fractional ideals form a group under multiplication. The only property we need to check now is that, for every fractional ideal $I$, the inverse exists and is $I^{-1}$. We have proved this for prime ideal, and so it is also true for any non-zero fractional ideal by writing out the prime factorisation and take inverse for each prime ideal, formally

**Theorem 13.18.** *The set of all non-zero integral and fractional ideals of a Dedekind domain $D$ forms an Abelian group under multiplication. The identity of the group is $D$ and the inverse of $A = \prod_{i=1}^{n} P_i^{e_i}$ , where $P_1, \ldots, P_n$ distinct and $e_i \mathbb{Z}$ is*

$$A^{-1} = \prod_{i=1}^{n} P_i^{-e_i}$$

## 13.4 Order of an ideal

We shall extend the definition of divisibility of integral ideal to fractional ideal.

**Definition 13.19.** *Let $D$ be a Dedekind domain. Let $A$ and $B$ be non-zero fractional ideals of $D$. We say $A$ divides $B$, written $A|B$ if there exists an integral ideal $C$ of $D$ such that $B = AC$.*

Further, we shall introduce the notation:

**Definition 13.20.** *Let $D$ be a Dedekind domain, and $A = \prod_{i=1}^{n} P_i^{e_i}$ a fractional ideal of $D$. Then we write $ord_{P_i}(A) = e_i$, which is called the* **order** *of $A$ with respect to $P_i$.*

Then clearly, if $A|B$ then $ord_{P_i}(A) \leq ord_{P_i}(B)$ for any $P_i$ in the factorisation. The next theorem gives a necessary and sufficient condition for an ideal $A$ to divide an ideal $B$.

**Proposition 13.21.** *Let $D$ be a Dedekind domain. Let $A$ and $B$ be any non-zero fractional ideal of $D$. Then*

$$A|B \iff A \supseteq B$$

*Proof.* $A|B \iff BA^{-1}$ is an integral ideal and so we have

$$A|B \iff BA^{-1} \subseteq D \iff B \subseteq A$$

□

The two basic properties of order is given in the next theorem.

**Proposition 13.22.** *Let $D$ be a Dedekind domain and $P$ be a prime ideal of $D$. Let $A$ and $B$ be non-zero fractional ideals of $D$. Then*

*(i)* $ord_P(AB) = ord_P(A) + ord_P(B)$.

*(ii)* $ord_P(A + B) = \min(ord_P(A), ord_P(B))$.

*Proof.* Let

$$A = P^e \prod_{i=1}^{n} P_i^{e_i}, B = P^f \prod_{i=1}^{m} Q_i$$

where $P_i, Q_i \neq P$. Then

(i) $ord_P(AB) = e + f = ord_P(A) + ord_P(B)$.

(ii) Let $C = A + B$. Then $AC^{-1} + BC^{-1} = D$. Hence $AC^{-1}, BC^{-1} \subseteq D$ and so both of them are integral. Also if $AC^{-1}, BC^{-1} \subseteq P$ then $D \subseteq P$ which is impossible. So we may assume $AC^{-1} \not\subseteq P$ and so $\min(ord_P(AC^{-1}), ord_P(BC^{-1})) = 0$. Thus by (i),

$$\min(ord_P(A), ord_P(B)) = ord_P(C) = ord_P(A + B)$$

□

We extend the order of an ideal to order of an element.

**Definition 13.23.** *Let $D$ be a Dedekind domain with field of quotient $K$. For $0 \neq \alpha \in K$, define*

$$ord_P(\alpha) = ord_P(\langle \alpha \rangle)$$

*the* **order** *of $\alpha$ with respect to a prime ideal $P$.*

**Lemma 13.24.** *Let $D$ be a Dedekind domain with field of quotient $K$. Let $A$ be a fractional ideal of $D$ and $0 \neq \alpha \in K$. Then*

$$\alpha \in A \iff ord_P(\alpha) \geq ord_P(A) \text{ for all prime ideals } P \text{ of } D$$

*Proof.*

$$\alpha \in A \iff \langle \alpha \rangle \subseteq A \iff ord_P(\alpha) \leq ord_P(A)$$

The last step is clear if $P$ divides $\alpha$ or $A$. If $P$ does not divide either of them, then the order is 0 for both of them. □

The following proposition extends Proposition 13.22

**Lemma 13.25.** *Let $D$ be a Dedekind domain with quotient field $K$. Let $P$ be a prime ideal of $D$. Then for any non-zero $\alpha, \beta \in K$*

*(i)* $ord_P(\alpha\beta) = ord_P(\alpha) + ord_P(\beta)$.

*(ii) If $\alpha + \beta \neq 0$, then*

$$ord_P(\alpha + \beta) \geq \min\left(ord_P(\alpha), ord_P(\beta)\right)$$

*(iii) If $\alpha + \beta \neq 0$, and $ord_P(\alpha) \neq ord_P(\beta)$, then equality holds in (ii).*

*Proof.* (i) This follows from proposition 13.22 as $ord_P(\alpha\beta) = ord_P(\langle \alpha\beta \rangle)$.

(ii) Since $\alpha + \beta \in \langle \alpha \rangle + \langle \beta \rangle$, thus by Lemma 13.24, we have

$$ord_P(\alpha + \beta) \geq ord_P(\langle \alpha \rangle + \langle \beta \rangle)$$

Hence the result follows by Proposition 13.22(ii)

(iii) WLOG, assume that $ord_P(\alpha) > ord_P(\beta)$. Then we have

$$ord_P(\beta) = ord_P((\alpha + \beta) - \alpha) \geq \min\left(ord_P(\alpha + \beta), ord_P(\alpha)\right)$$

Now since $ord_P(\beta) < ord_P(\alpha)$ so the above can only hold if

$$\min\left(ord_P(\alpha + \beta), ord_P(\alpha)\right) = ord_P(\alpha + \beta)$$

Then

$$ord_P(\beta) \leq ord_P(\alpha + \beta) \geq ord_P(\beta)$$

and so the equalities must hold and so

$$ord_P(\alpha + \beta) = ord_P(\beta) = \min\left(ord_P(\alpha), ord_P(\beta)\right)$$

□

**Example 13.26.** *We give an example to show that the inequality can actually be strict in Proposition 13.25(ii). Let* $D = \mathbb{Z}, \alpha = 1, \beta = 2, P = \langle 3 \rangle$. *Then*

$$ord_P(\alpha) = 0, ord_P(\beta) = 0, ord_P(\alpha + \beta) = 1$$

**Theorem 13.27.** *Let* $D$ *be a Dedekind domain and* $K$ *be the field of quotient. Given any finite set of prime ideal* $P_1, \ldots, P_k$ *of* $D$ *and a set of integers* $e_1, \ldots, e_k$ *then there exists* $\alpha \in K$ *such that*

$$ord_{P_i}(\alpha) = e_i, i = 1, 2, \ldots, k$$

*and*

$$ord_P(\alpha) \geq 0 \text{ for any prime ideal distinct from } P_i, i = 1, 2, \ldots, k$$

*Proof.* For the prime ideal $P_i$ and integer $e_i$. Consider

$$I_i = P_i^{e_i} \prod_{j \neq i} P_j^{e_j+1}, J_i = \prod_{j=1}^{k} P_j^{e_j+1}$$

$I_i | J_i$ and so by Proposition 13.21, $J_i \subseteq I_i$. By unique factorisation, we have $J_i \neq I_i$ and so $J_i \subset I_i$. Hence there exists $\alpha_i$ for each $i$ such that

$$\alpha_i \in I_i \text{ but } \alpha_i \notin J_i$$

Then $ord_{P_i}(\alpha_i) = e_i$ by Lemma 13.24. Also $ord_{P_j}(\alpha_i) \geq e_j + 1$ for $j \neq i$, again by Lemma 13.24. Now define

$$\alpha = \alpha_1 + \ldots + \alpha_k \in K$$

By repeatedly applying Lemma 13.25(ii), we have

$$ord_{P_i}\left(\sum_{j \neq i} \alpha_j\right) \geq \min_{j \neq i}(ord_{P_i}(\alpha_j)) \geq e_i + 1 > ord_{P_i}(\alpha_i)$$

Therefore, using $\sum_{j=1}^{k} \alpha_j = \alpha_i + (\sum_{j \neq i} \alpha_j)$, we have

$$ord_{P_i}(\alpha) = ord_{P_i}\left(\sum_{j=1}^{k} \alpha_j\right) = \min\left(ord_{P_i}(\alpha_i), ord_{P_i}(\sum_{j \neq i} \alpha_j)\right) = ord_{P_i}(\alpha_i)$$

by using Lemma 13.25(iii). Hence we have

$$ord_{P_i}(\alpha) = e_i$$

Finally, if $P \neq P_i$ for any $i$, then

$$ord_P(\alpha_i) \geq 0$$

and so

$$ord_P(\alpha) \geq 0$$

□

## 13.5 Chinese Remainder Theorem

The last topic of this subsection is an analogue of Chinese Remainder Theorem in Dedekind domain. Let $D$ be a Dedekind domain and $K$ be the field of quotient. Let $I$ be a fractional ideal. We shall write for any $a, b \in I$

$$a \equiv b \pmod{I} \iff I | \langle a - b \rangle$$

It is easy to check that

$$I | \langle a - b \rangle \iff \langle a - b \rangle \subseteq I \iff a - b \in I \iff a + I = b + I$$

and if $c \in I$ then

$$ac \equiv bc \pmod{I}$$

**Theorem 13.28. [Chinese Remainder Theorem]** *Let $D$ be a Dedekind domain.*

*(i) Let $P_1, \ldots, P_k$ be distintct prime ideals in $D$. Let $e_1, \ldots, e_k$ be positive integers and $\alpha_1, \ldots, \alpha_k \in D$. Then there exists $\alpha \in D$ such that*

$$\alpha \equiv \alpha_i \ (mod\ P_i^{e_i}), i = 1, 2, \ldots, k$$

*(ii) Let $I_1, \ldots, I_k$ be pairwise relatively prime ideals of $D$. (in the sense of factorisation into prime ideals.) Let $\alpha_1, \ldots, \alpha_k$ be elements of $D$. Then there exists $\alpha \in D$ such that*

$$\alpha \equiv \alpha_i \ (mod\ I_i), i = 1, 2, \ldots, k$$

*Proof.* (i) Let $A_i = P_i^{e_i}, B_i = \sum_{j \neq i} P_j^{e_j}$, then define

$$Q_i = A_i + B_i$$

Suppose $P$ is any prime ideal dividing $Q_i$. Since $A_i, B_i \subseteq Q_i$, then by Proposition 13.21, we have

$$Q_i \big| A_i \text{ and } Q_i \big| B_i$$

and so

$$P \big| A_i \text{ and } P \big| B_i$$

But $A_i = P_i^{e_i}$ and since $P_i$ is prime. Then $P \big| P_i$, and so by maximality of prime ideal in Dedekind domain, we have $P = P_i$. Thus $P_i \big| B_i$ is a contradiction. Hence there exists no prime ideal dividing $Q_i$ and so $Q_i = D$ for each $i$. Thus we have

$$x_i \in A_i, y_i \in B_i$$

such that

$$x_i + y_i = 1$$

which implies that

$$y_i \equiv 1 \pmod{P_i^{e_i}} \text{ and } y_i \equiv 0 \pmod{P_j^{e_j}}, j \neq i$$

Now define

$$\alpha = \sum_{i=1}^{k} e_i y_i$$

and so

$$\alpha \equiv e_i \pmod{P_i^{e_i}}$$

(ii) This follows from the unique factorisation of each $I_i$ into prime ideals and apply (i) since $I_i$ are relatively prime to each other.

□

We shall see many other properties of a Dedekind domain in the exercises.

## 13.6 Exercises

1. Let $D$ be a Dedekind domain. Let $A$ and $B$ be proper integral ideals of $D$. Show that $AB \neq D$.

2. Let $D$ be a Dedekind domain. Let $I$ and $J$ be fractional ideals. Show that $I + J$ and $IJ$ are also fractional ideals.

3. Let $D$ be a principal ideal domain with field of quotient $K$. Prove that every fractional ideal of $D$ is of the form $\{d\alpha : d \in D\}$ for some $\alpha \in K$.

4. Let $K$ be a number field and $\mathcal{O}_K$ the ring of integer. If $[K : \mathbb{Q}] = n$, show that every ordinary integer $\alpha \in \mathbb{Z}$ lies in at most $\alpha^n$ integral ideals of $\mathcal{O}_K$.

5. Let $K = \mathbb{Q}[\sqrt{-5}]$, find the inverse of $\langle 2, 1 + \sqrt{-5} \rangle$.

6. Let $D$ be a Dedekind domain. Show that if $D$ is a unique factorisation domain, then $D$ is a principal ideal domain.

7. Let $D$ be a Dedekind domain. Let $I$ and $J$ be integral ideals of $D$ and let

$$I = \prod_{i=1}^{k} P_i^{e_i}, J = \prod_{i=1}^{k} P_i^{f_i}$$

where $P_1, \ldots, P_k$ are all possible divisors of $I$ or $J$ and $e_i, f_i$ are non-negative integers. Define the greatest common divisor $(I, J)$ and the least common multiple $\{I, J\}$ by:

$$(I, J) = \prod_{i=1}^{k} P_i^{\min(e_i, f_i)}, \{I, J\} = \prod_{i=1}^{k} P_i^{\max(e_i, f_i)}$$

Show that

$$(I, J) = I + J \text{ and } \{I, J\} = I \cap J$$

8. Prove that the cancelation law holds in Dedekind domain. That is, if $D$ is a Dedekind domain, and $I, J, K$ are ideals of $D$ such that $I \neq 0$. Then

$$IJ = IK \iff J = K$$

9. Let $K$ be a number field. Prove that $\mathcal{O}_K$ contains infinitely many prime ideals.

10. Prove the ring version of Chinese Remainder Theorem in Dedekind domain. That is, if $D$ is a Dedekind domain, then

$$D/I \cong D/P_1^{e_1} \times \cdots \times D/P_k^{e_k}$$

where

$$I = \prod_{i=1}^{k} P_i^{e_i}, e_i \geq 1$$

11. Let $K$ be a number field and $\mathcal{O}_K$ be its ring of integers.

(i) Let $P$ be a prime ideal. Show that the only non-zero proper ideals in the ring $\mathcal{O}_K/P^n$ are $P^j\mathcal{O}_K/P^n$, $j = 1, 2, \ldots, n-1$.

(ii) Show that if $\alpha \in P \backslash P^2$, then

$$P^i = \langle \alpha^i \rangle + P^n, i = 1, 2, \ldots, n$$

(iii) Hence show that any ideal of the ring $\mathcal{O}_K/I$ can be generated by one element where $I$ is any non-zero integral ideal of $\mathcal{O}_K$.

(iv) Show further that any fractional ideal in $\mathcal{O}_K$ can be generated by at most two elements.

*12. Let $D$ be a Dedekind domain and $I$ any non-zero ideal of $D$ such that $I \neq D$. Let $0 \neq \alpha \in I$.

(i) Show that $\langle \alpha \rangle = IJ$ for some integral ideal $J$. Let $P_1, \ldots, P_k$ be all possible prime ideals such that either

$$ord_{P_i}(I) \neq 0 \text{ or } ord_{P_i}(IJ) \neq 0$$

Prove that that there exists $\beta \in K$, the field of quotient of $D$ such that

$$ord_{P_i}(\beta) = ord_{P_i}(I), i = 1, 2, \ldots, k$$

and

$$ord_P(\beta) \geq 0, P \neq P_1, \ldots, P_k$$

(ii) Show further that

$$ord_P(I) = ord_P(\langle \beta \rangle + IJ) \text{ for all prime ideals } P$$

(iii) Hence conclude that $I$ is generated by at most two elements. Thus, we have proved that in any Dedekind domain $D$, any ideal of $D$ is generated by at most two elements in $K$. We see that question 11 is a special case.

13. This is an alternative proof of the consequence of the previous question without using valuation argument. Let $R$ be a Dedekind domain.

(i) Let $\mathfrak{a} \subset R$ be a non-zero ideal. Show that every ideal in the ring $R/\mathfrak{a}$ is principal.

(ii) Deduce that every ideal in $R$ can be generated by 2 elements.

## 13.7 Hint and Solutions

1. Suppose $AB = D$, then $A|D$ and so we have $D \subseteq A$, which is a contradiction.

2. Let $\gamma I \subseteq D$ and $\delta J \subseteq D$ since $I$ and $J$ are fractional ideals. Clearly $I + J$ and $IJ$ satisfy the first two properties of a fractional ideal, just as what we checked for integral ideal. For the third property, let $i \in I$ and $j \in J$, then

$$\gamma\delta(i + j) = \delta(\gamma i) + \gamma(\delta j) \in D$$

and so $\gamma\delta(I + J) \subseteq D$. Similarly we have $\gamma\delta IJ \subseteq D$ and so $I + J$ and $IJ$ are both fractional ideals.

3. Let $I$ be a fractional ideal of $D$. Then there exists $0 \neq \gamma \in D$ such that $\gamma I \subseteq D$ is an integral ideal. Since $D$ is a principal ideal domain, we have some $\delta$ such that

$$\gamma I = \langle \delta \rangle$$

So

$$I = \{\alpha d : d \in D\} \text{ where } \alpha = \frac{\delta}{\gamma} \in K$$

4. In the proof of Lemma 13.1, we see that $\mathcal{O}_K/\langle\alpha\rangle$ has at most $\alpha^n$ elements because $\mathbb{Z}/\alpha\mathbb{Z} = \alpha$. Hence, for each integral ideal $I$ containing $\alpha$ (and hence $\langle\alpha\rangle$), it corresponds to the element $I/\langle\alpha\rangle$ in $\mathcal{O}_K/\langle\alpha\rangle$. Hence we have at most $\alpha^n$ such $I$.

5. Consider $\alpha = x + y\sqrt{-5}$, $x, y \in \mathbb{Q}$ such that $\alpha\langle 2, 1+\sqrt{-5}\rangle \subseteq \mathcal{O}_K$. because $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Thus we have

$$2(x + y\sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}], (x + y\sqrt{-5})(1 + \sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$$

and so

$$2x, 2y, x - 5y, x + y \in \mathbb{Z}$$

If $x \in \mathbb{Z}$, so is $y$. If $x = \frac{a}{2}$ for some $a$ odd, then $y = \frac{b}{2}$ for some $b$ odd and all the above hold. Therefore, we conclude that the inverse of $\langle 2, 1+\sqrt{-5}\rangle$ is

$$\mathbb{Z} + \frac{1+\sqrt{-5}}{2}\mathbb{Z} = \frac{1}{2}\langle 2, 1+\sqrt{-5}\rangle$$

6. Let $D$ be a Dedekind domain. Suppose $D$ is a unique factorisation domain. Let $P$ be any prime ideal in $D$. Take $0 \neq x \in P$. As $P \neq D$, so $x$ is not a unit and so

$$x = p_1^{e_1} \cdots p_k^{e_k}$$

where $e_i \geq 1$ and $p_i$ is irreducible, $i = 1, \ldots, k$. Since $P$ is a prime ideal, so $p_j \in P$ for some $j$ and in a unique factorisation domain, an irreducible element is prime. So $p_j$ is prime and so $\langle p_j\rangle$ is a prime ideal and hence maximal in a Dedekind domain. But $\langle p_j\rangle \subseteq P$. Thus $\langle p_j\rangle = P$ and so $P$ is principal. Finally, since each ideal can be factorised into prime ideals. Therefore, we conclude that every ideal is principal and hence $D$ is a principal ideal domain.

7. It is clear that the definition coincides with the definition of greatest common divisor and least common multiple in $\mathbb{Z}$. That is, $(I, J)$ is the common divisor of $I$ and $J$ such that if $K \big| I, J$ then $K \big| (I, J)$ because $K$ must be a product of $P_i$'s with exponent less than the minimum of $e_i$ and $f_i$. Similarly the least common multiple $\{I, J\}$ is an ideal such that $I, J \big| \{I, J\}$ and for any $L$ such that $I, J \big| L$, we have $\{I, J\} \big| L$. Note also that they are unique by the uniqueness of factorisation.

   Using the above observation, for $(I, J)$. Suppose $K \big| I, J$ then $K \supseteq I, J$ and hence $K \supseteq I + J$. Therefore, $K \big| I + J$ and so $(I, J) = I + J$.

   Similarly, let $I, J \big| L$ then $L \subseteq I, J$ and hence $L \subseteq I \cap J$. Therefore, $I \cap J \big|$ and so $\{I, J\} = I \cap J$.

8. If $J = K$ then clearly $IJ = JK$.

   Conversely, if $IJ = IK$. Then by uniqueness of the inverse of an ideal in $D$ (since $I$ is non-zero), we multiply by the inverse of $I$ and so we have $J = K$.

9. Let $p$ and $q$ be distinct prime numbers in $\mathbb{N}$. Use the notation in question 7, we have

$$(\langle p\rangle, \langle q\rangle) = \langle p\rangle + \langle q\rangle$$

But since $(p, q) = 1$ there exists $x, y \in \mathbb{Z}$ such that

$$px + qy = 1$$

Thus

$$\langle p\rangle + \langle q\rangle = \langle 1\rangle = \mathcal{O}_K$$

Therefore, the prime ideal dividing $\langle p\rangle$ does not divide $\langle q\rangle$ and since there are infinitely many prime numbers in $\mathbb{N}$, so we conclude that there are infinitely many prime ideals in $\mathbb{O}_K$ because each $\langle p\rangle$ must be divisible by some prime ideals.

10. Define a ring homomorphism

$$f : D/I \longmapsto D/P_1^{e_1} \times \cdots d/P_k^{e_k}$$

by

$$f(a + I) = (a_1 + P_1^{e_1}, \ldots, a_k + P_k^{e_k}) \text{ where } a_i \equiv a \pmod{P_i^{e_i}}$$

It is clearly a ring homomorphism since the congruence is additive and multiplicative. It is injective, because if $f(a + I) = 0$, then

$$a \equiv 0 \pmod{P_i^{e_i}} \text{ for all } i$$

and so $a \in P_i^{e_i}$ for all $i$. Hence $P_i^{e_i} \big| \langle a\rangle$ and since $P_i$ are distinct, so we have $I \big| \langle a\rangle$ and so $a = 0$. It is surjective, because there exists $\alpha$ such that

$$\alpha \equiv \alpha_i \pmod{P_i^{e_i}} \text{ for all } i$$

by Theorem 13.28 (Chinese Remainder Theorem). Hence it is an isomorphism and so the result follows.

11. (i) Each ideal in $\mathcal{O}_K/P^n$ corresponds to an ideal containing $P^n$. Thus let $I \supseteq P^n$, then $I \big| P^n$ and so $I = P^j, j = 1, \ldots, n$. Hence the result follows.

(ii) Use question 7, that

$$\langle \alpha^i\rangle + P^n = (\langle \alpha^i\rangle, P^n)$$

Since $\alpha \in P \backslash P^2$, so $\langle \alpha\rangle \subseteq P$ but $\not\subseteq P^2$. Hence $P \big| \langle \alpha\rangle, P^2 \big| \langle \alpha\rangle$. Therefore the greatest common divisor

$$(\langle \alpha^i\rangle, P^n) = P^i \text{ for } i = 1, 2, \ldots, n$$

(iii) Use (i) that any non-zero proper ideal in $\mathcal{O}_K/P^n$ has the form $P^j\mathcal{O}_K/P^n$. Then by (ii) we conclude that

$$P^j\mathcal{O}_K/P^n = \langle \alpha^j + P^n\rangle \text{ for any } \alpha \in P \backslash P^2$$

Therefore every ideal in $\mathcal{O}_K/P^n$ is generated by one element. Now use Chinese Remainder Theorem in question 10, for any ideal $I$ of $\mathcal{O}_K$, we have

$$\mathcal{O}_K/I \cong \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_k^{e_k}$$

where $I = P_1^{e_1} \cdots P_k^{e_k}$. Since each ideal of $\mathcal{O}_K/P_j^{e_j}$ can be generated by one element, so is the ideal of $\mathcal{O}_K/I$.

(iv) Let $I$ be an integral ideal of $\mathcal{O}_K$ and let $0 \neq \alpha \in I$. Let $J = \langle \alpha \rangle$. Then $I/J \subseteq \mathcal{O}_K$ and so is generated by one element $\beta$, by (iii). Thus $I/J = \langle \beta + J \rangle$. Now for any $x \in I$, let $x \equiv y \pmod{J}$ and so $x = j + y$ for some $j \in J$. But $y \in \langle \beta \rangle$ and $j \in J = \langle \alpha \rangle$. Therefore,

$$I = \langle \alpha, \beta \rangle$$

Suppose more generally that $I$ is a fractional ideal. Then take $\gamma \in D$ such that

$$\gamma I \subseteq D \text{ is an integral ideal}$$

Thus, there exists $\alpha, \beta$ such that $\gamma I = \langle \alpha, \beta \rangle$ and hence

$$I = \left\langle \frac{\alpha}{\gamma}, \frac{\beta}{\gamma} \right\rangle$$

12. (i) $\alpha \in I \Rightarrow \langle \alpha \rangle \subseteq I$ so $I \big| \langle \alpha \rangle$. So there exists an integral ideal $J$ such that $IJ = \langle \alpha \rangle$. Then apply Theorem 13.27.

(ii) Now since $J$ is an integral ideal, we have, for $i = 1, \ldots, k$, we have

$$\begin{aligned} ord_{P_i}(I) &= \min\left(ord_{P_i}(I), ord_{P_i}(IJ)\right) \\ &= \min\left(ord_{P_i}(\beta), ord_{P_i}(IJ)\right) \\ &= \min\left(ord_{P_i}(\langle \beta \rangle), ord_{P_i}(IJ)\right) \\ &= ord_{P_i}(\langle \beta \rangle + IJ) \end{aligned}$$

by using Proposition 13.22(ii). For $P \neq P_i, i = 1, \ldots, k$, we have

$$ord_P(I) = ord_P(IJ) = 0$$

and since $ord_P(\beta) \geq 0$, so

$$ord_P(I) = \min\left(ord_P(\beta), ord_P(IJ)\right) = ord_P(\langle \beta \rangle + IJ)$$

Hence

$$ord_P(I) = ord_P(\langle \beta \rangle + IJ) \text{ for all prime ideals } P$$

(iii) Use (ii) and unique factorisation of ideals into prime ideals, we conclude that

$$I = \langle \beta \rangle + IJ = \langle \beta \rangle + \langle \alpha \rangle = \langle \alpha, \beta \rangle$$

13. By Chinese Remainder Theorem, it suffices the prove (i) in the case when $\mathfrak{a}$ is a power of prime ideal. Or in more detail, Chinese Remainder Theorem shows that for any $\mathfrak{a}$ and $\mathfrak{b}$ coprime we have

$$R/\mathfrak{ab} \cong R/\mathfrak{a} \times R/\mathfrak{b}.$$

Let $\mathfrak{a} = \mathfrak{p}^r$. Then

$$R/\mathfrak{p}^r \cong R/\mathfrak{p} \times \mathfrak{p}/\mathfrak{p}^2 \times \cdots \mathfrak{p}^{r-1}/\mathfrak{p}^r.$$

Each of the component on the right hand side can be generated by a single element and hence we conclude that the left hand side is principal.

For the second part, for each ideal $I$, pick any non-zero element $a \in I$ and consider the quotient $R/\langle a \rangle$. This is principal by the first part say generated by $\bar{b}$. Now lift $\bar{b}$ in $R$ in the sense that the reduction of $b$ is $\bar{b}$. Then $I = \langle a, b \rangle$.

# 14 Discriminant and norm

## 14.1 Discriminant

We know $\mathcal{O}_K$ is a subring of the number field $K$. How large is $\mathcal{O}_K$ in terms of $K$? We shall introduce the concept of discriminant to measure the 'size' of $\mathcal{O}_K$.

**Definition 14.1.** *Suppose $M$ is a finitely generated free $\mathbb{Z}$-module, and*

$$T : M \times M \longmapsto \mathbb{Q}$$

*a bilinear form. Pick a basis $\{e_1, \ldots, e_n\}$ of $M$. Let $A$ be the matrix such that $A_{ij} = T(e_i, e_j)$. Then the* **discriminant** *of $M$ with respect to the bilinear form $T$ is defined as*

$$D(M) = disc(M) = \det(A)$$

*When $M = \mathcal{O}_K$ for any number field $K$, we take $T$ be the bilinear form defined in Definition 12.25, that $T_(x, y) = T_{K/\mathbb{Q}}(xy)$.*

Note the definition makes sense as we have proved that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Further, in the proof of Theorem 12.38, if $[K : \mathbb{Q}] = n$, then $\mathcal{O}_K$ is generated by $n$ elements. Thus $A$ is an $n \times n$ matrix. But suppose we pick another basis for $M$, does it change the discriminant?

**Lemma 14.2.** *$disc(M)$ is independent of the choice of $\mathbb{Z}$-basis.*

*Proof.* Let $\{e_1, \ldots, e_n\}$ be a basis and $\{f_1, \ldots, f_n\}$ be another basis. Let $P$ be the change of basis matrix and $B_{ij} = T(f_i, f_j)$. Then

$$B = PAP^t, \det B = (\det P)^2 \det A$$

But $P$ is the change of basis matrix so $\det P$ is invertible in $\mathbb{Z}$. Hence $\det P = \pm 1$ and so $(\det P)^2 = 1$. Hence $\det B = \det A$. □

Observe that for $x, y \in \mathbb{Z}$, $T(x, y) \in \mathbb{Z}$. For shorthand, write $\mathcal{D}_k = disc(\mathcal{O}_K)$. We can also define discriminant for other finitely generated $Z$-module, for example, the ideals. Since each ideal in $\mathcal{O}_K$ is a submodule of $\mathcal{O}_K$ and hence finitely generated $\mathbb{Z}$-module.

**Lemma 14.3.** *Let $K$ be a number field and $[K : \mathbb{Q}] = n$. Let $\{x_1, \ldots, x_n\}$ be a $\mathbb{Z}$-basis of $M$. Let $x_{i,1} = x_i, \ldots, x_{i,n}$ be conjugates of $x_i, i = 1, \ldots, n$. Then*

$$disc(M) = (\det X)^2$$

*where $X_{ij} = x_{ij}$.*

*Proof.* Let $A_{ij} = T(x_i, x_j)$. So the conjugates of $x_i x_j$ are $x_{ip}x_{jp}$, $p = 1, \ldots, n$. But

$$T(x_i, x_j) = T_{K/\mathbb{Q}}(x_i x_j) = \sum_{p=1}^{n} x_{ip}x_{jp}$$

Define the matrix $X_{ip} = x_{ij}$. Then

$$A = XX^t \text{ and so } \det A = (\det X)^2$$

□

Now, let $e_1, \ldots, e_n$ be $n$ elements in $K$ and let

$$e_i^{(1)} = \sigma_1(e_i), e_i^{(2)} = \sigma_2(e_i), \ldots, e_i^{(n)} = \sigma_n(e_i)$$

For convention, we define

$$D(e_1, \ldots, e_n) = \begin{vmatrix} e_1^{(1)} & \ldots & e_n^{(1)} \\ \vdots & \ldots & \vdots \\ e_1^{(n)} & \ldots & e_n^{(n)} \end{vmatrix}^2$$

and for any element $\alpha \in K$, we define $D(\alpha) = D(1, \alpha, \ldots, \alpha^n)$.

**Example 14.4.** *Let $m$ be a non-zero square free integer and $m \neq 1$ and $K = \mathbb{Q}[\sqrt{m}]$. It is easy to check that if $m \not\equiv 1$ (mod 4) then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ and if $m \equiv 1$ (mod 4), then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.*

*If $m \not\equiv 1$ (mod 4), then $\{1, \sqrt{m}\}$ is a basis for $\mathcal{O}_K$ and so*

$$\mathcal{D}_K = \left( \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix} \right)^2 = (-2\sqrt{m})^2 = 4m$$

*If $m \equiv 1$ (mod 4), then $\{1, \frac{1+\sqrt{m}}{2}\}$ and so*

$$\mathcal{D}_K = \left( \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix} \right)^2 = (\sqrt{m})^2 = m$$

*We can see that $\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ and so this indicates that the larger the $\mathbb{Z}$-module, the smaller the discriminant.*

**Theorem 14.5.** *Suppose $N \subseteq M$ is a $\mathbb{Z}$-submodule which has index $r$. In other words, $M/N$ is a finite Abelian group of order $r$. Then*

$$disc(N) = r^2 disc(M)$$

*Proof.* Let $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_n\}$ be bases for $M$ and $N$ respectively. Since $N \subseteq M$, so there exist $a_{ij} \in \mathbb{Z}$ such that

$$f_i = \sum_{j=1}^{n} a_{ij} e_j, i = 1, \ldots, n$$

By structure theorem for finitely generated module over $\mathbb{Z}$ (Smith Normal Form), we can obtain $x_1, \ldots, x_n \in M$ and $r_i \in \mathbb{Z}$ such that $\{x_1, \ldots, x_n\}$ is a basis for $M$ and $\{r_1 x_1, \ldots, r_n x_n\}$ is a basis for $N$. Then it is easy to see that

$$\{x_1 z_1 + \ldots x_n z_n : z_1 = 0, 1, \ldots, |r_1| - 1; \ldots; z_n = 0, 1, \ldots, |r_n| - 1\}$$

is a complete set of coset representatives for $M/N$. So $r = r_1 \cdots r_n$. (Moreover, by the algorithm, we have $r = \det(a_{ij})$.) Hence

$$disc(N) = (\det X)^2 = r^2 disc(M)$$

where $X_{ij} =$ the $j^{th}$ conjugate of $r_i x_i = r_i x_{ij}$ because $r_i \in \mathbb{Z}$. Hence $\det X = \prod_i r_i \det(x_{ij})$ and so $\det X = r^2 disc(M)$. □

**Corollary 14.6.** *If $N \subseteq \mathcal{O}_K$ has $disc(N)$ square free. Then $N = \mathcal{O}_K$.*

*Proof.* By Theorem 14.5, the index of $N$ in $\mathcal{O}_K$ must be 1 since $disc(N)$ is square free. Hence $\mathcal{O}_K/N$ is a group of order 1 and so $\mathcal{O}_K = N$. □

Theorem 14.5 also tells that if $N \subseteq M$ and $disc(N) = disc(M)$, then $N = M$.

## 14.2 Discriminant of a polynomial

When we solve the quadratic equation

$$ax^2 + bx + c = 0$$

we usually define the discriminant $d$ to be $b^2 - 4ac$. Then the two roots are

$$\frac{-b \pm \sqrt{d}}{2a}$$

What about the discriminant of general polynomial?

**Definition 14.7.** *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$$

*where $n \in \mathbb{N}$ and $a_n \neq 0$. Let $x_1, \ldots, x_n$ be the roots of $f(x)$. The discriminant of $f(x)$ is defined by*

$$disc(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

**Theorem 14.8.** *Let $K$ be a number field od degree $n$. Let $\alpha \in K$. Then*

$$D(\alpha) = disc(min_{\mathbb{Q},\alpha}(x)^d)$$

*where $d$ is an integer such that $de = n, e = \deg min_{\mathbb{Q},\alpha}(x)$.*

*Proof.* By Vanmdermonde determinant, it is easy to check that

$$D(\alpha) = \prod_{1 \leq i < j \leq n} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2$$

where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are conjugates of $\alpha$ in $K$. So the roots of $min_{\mathbb{Q},\alpha}(x)^d$ are $\alpha^{(1)}, \ldots, \alpha^{(n)}$, and so the discriminant

$$disc(min_{\mathbb{Q},\alpha}(x)^d) = \prod_{1 \leq i < j \leq n} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2 = D(\alpha)$$

because the leading coefficient is 1. □

The following theorem gives an criteria for the generator of the number field $K$.

**Theorem 14.9.** *Let $K$ be a number field of degree $n$. Let $\alpha \in K$. Then*

$$K = \mathbb{Q}(\alpha) \iff D(\alpha) \neq 0$$

*Proof.*

$$K = \mathbb{Q}(\alpha) \iff min_{\mathbb{Q},\alpha}(x) \text{ has } n \text{ distinct root} \iff D(\alpha) \neq 0$$

by using Vandermonde determinant. □

**Theorem 14.10.** *Let $K$ be a number field of degree $n$.*

*(i) If $e_1, \ldots, e_n \in K$, then*

$$D(e_1, \ldots, e_n) \in \mathbb{Q}$$

*(ii) If $e_1, \ldots, e_n \in \mathcal{O}_K$, then*

$$D(e_1, \ldots, e_n) \in \mathbb{Z}$$

*In particular, $\mathcal{D}_K \in \mathbb{Z}$.*

*(iii) If $e_1, \ldots, e_n \in K$, then*

$$D(e_1, \ldots, e_n) \neq 0 \iff e_1, \ldots, e_n \text{ are linearly independent over } \mathbb{Q}$$

*Proof.* (i) Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Let $e_i^{(j)}$ be the conjugates of $e_i$, $i = 1, \ldots, n; j = 1, \ldots, n$. Then there exist $a_{ij} \in \mathbb{Q}$ such that

$$e_i^{(j)} = a_{0i} + a_{1i}\alpha_j + \cdots + a_{n-1i}\alpha_j^{n-1}$$

Then by definition, $D(e_1, \ldots, e_n)$ is the square of the determinant of the matrix whose entries are now of the form

$$a_{0i} + a_{1i}\alpha_j + \cdots + a_{n-1i}\alpha_j^{n-1}$$

for $1 \leq i, j \leq n$. If we swap $i$ and $j$ then it is same as swapping rows and columns of the matrix, which may only change the sign of the determinant. But we take the square of the determinant so it then will be the same if we swap $i$ and $j$. Hence it is a symmetric function in $\alpha_1, \ldots, \alpha_n$. Now let

$$(x - \alpha_1) \cdots (x - \alpha_n) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

where $b_0, \ldots, b_n \in \mathbb{Q}$. Then the symmetric function in $\alpha_1, \ldots, \alpha_n$ can be expressed in terms of $b_0, \ldots, b_n$ and so it must be rational. So $D(e_1, \ldots, e_n) \in \mathbb{Q}$.

(ii) Since $e_1, \ldots, e_n \in \mathcal{O}_K$ and $\mathcal{O}_K$ is a ring, so $D(e_1, \ldots, e_n)$ is obtained by the determinant of the matrix whose entries are algebraic integers. But the determinant is obtained by a series of addition and multiplication. Hence it is still an algebraic integer. By (i) it also rational, hence must be an integer.

(iii) Let $K = \mathbb{Q}(\alpha)$ Suppose $e_1, \ldots, e_n$ are linearly independent over $\mathbb{Q}$, then $\{e_1, \ldots, e_n\}$ is a basis and so there exists $a_{ij} \in \mathbb{Q}$ such that

$$\alpha^{i-1} = \sum_{j=1}^{n} a_{ij} e_j$$

Let $\alpha_1 = \alpha, \ldots, \alpha_n$ be the conjugates of $\alpha$ and $e_j^{(k)}, k = 1, \ldots, n$ be the conjugates of $e_j$ for each $j$. Then

$$\alpha_k^{i-1} = \sum_{j=1}^{n} a_{ij} e_j^{(k)}$$

Therefore, we have

$$D(\alpha) = |\det(a_{ij})|^2 D(e_1, \ldots, e_n)$$

By Theorem 14,9, $D(\alpha) \neq 0$ and so $D(e_1, \ldots, e_n) \neq 0$.

Conversely, suppose $e_1, \ldots, e_n$ are linearly dependent. Then there exist $a_1, \ldots, a_n \in \mathbb{Q}$ such that

$$a_1 e_1 + \cdots a_n e_n = 0$$

and so

$$\sum_{i=1}^{n} a_i e_i^{(k)} = 0$$

where $e_i^{(k)}, k = 1, \ldots, n$ are conjugates of $e_i$ for each $i$. This is a system of $n$ linear equations in $n$ quantities $c_1, \ldots, c_n$ and has a non-trivial solution. Therefore, we must have the determinant

$$D(e_1, \ldots, e_n) = 0$$

□

## 14.3 Norm of an ideal

**Definition 14.11.** *Let $I$ be an integral ideal of $\mathcal{O}_K$. The* **norm** *of $I$, written $N(I)$ is defined as*

$$N(I) = \sqrt{\frac{D(I)}{\mathcal{D}_K}}$$

The main results we are going to deduce in this subsection is

$$N(I) = card(\mathcal{O}_K/I)$$

**Theorem 14.12.** *Let $G$ be a free $\mathbb{Z}$-module generated by $e_1, \ldots, e_n$. Let $H \subseteq G$ generated by $f_1, \ldots, f_n$ so that*

$$H = \{y_1 f_1 + \ldots + y_n f_n : y_1, \ldots, y_n \in \mathbb{Z}\}$$

*As each $f_i \in H \subseteq G$, we have*

$$f_i = \sum_{j=1}^{n} a_{ij} e_i \text{ where } a_{ij} \in \mathbb{Z}$$

*Let $A$ be the matrix such that $A_{ij} = a_i j$. Then*

$$[G : H] = \begin{cases} |\det A| & \text{if } \det A \neq 0 \\ \infty & \text{if } \det A = 0 \end{cases}$$

*Proof.* This is in fact a restatement of Theorem 14.5. We can find a $\mathbb{Z}$-basis $\{x_1, \ldots, x_n\}$ for $G$ such that there exists $r_i \in \mathbb{Z}$ such that $\{r_1 x_1, \ldots, r_n x_n\}$ is a basis for $H$ by applying elementary operations to the matrix $A$ to the diagonal matrix $D = diag(r_1, \ldots, r_n)$. So $\det A = \det D = d_1 \cdots d_n$. So it is clear that if $r_i \neq 0$ for each $i$, then

$$z_1 x_1 + \ldots z_n x_n \in H \iff z_i = y_i r_i, y_i \in \mathbb{Z}, i = 1, \ldots, n \iff r_i | z_i$$

and so in this case $\det A \neq 0$ and we can check that $\{z_1 x_1 + \ldots + z_n x_n : z_1 = 0, 1, \ldots, |r_1| - 1; \ldots; z_n = 0, 1 \ldots, |r_n| - 1\}$ form a complete set of coset representatives for $G/H$. Thus

$$[G : H] = |r_1| \cdots |r_n| = |\det A|$$

If $\det A = 0$, i.e. $r_i = 0$ for some $i$. Then $kx_i + H, k = 1, 2, \ldots$ are distinct cosets of $H$ in $G$ so that $[G : H] = \infty$. □

**Theorem 14.13.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Let $I$ be a non-zero integral ideal of $\mathcal{O}_K$. Then*

$$N(I) = card(\mathcal{O}_K/I)$$

*Proof.* Let $\{e_1, \ldots, e_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and $\{f_1, \ldots, f_n\}$ be a $\mathbb{Z}$-basis for $I$. Then there exists $a_{ij} \in \mathbb{Z}$ such that

$$f_i = \sum_{j=1}^{n} a_{ij} e_i, i = 1, 2, \ldots, n$$

Therefore, by Theorem 14.8,

$$N(I) = \sqrt{\frac{D(I)}{\mathcal{D}_K}} = r = \det A = [\mathcal{O}_K : I] = card(\mathcal{O}_K/I)$$

where $r$ is the index of $I$ in $\mathcal{O}_K$ in Theorem 14.5. □

## 14.4 Norm of a product of ideals

The main result we are going to deduce n the subsection is $N(IJ) = N(I)N(J)$ for any integral ideals $I, J$. We shall give two proofs. The first proof requires some ring theory and Chinese Remainder Theorem.

**Lemma 14.14.** *Let $K$ be a number field and $P$ a prime ideal of $\mathcal{O}_K$. Then, for any $n \geq 1$,*

$$P^n\mathcal{O}_K/P^{n+1} \cong \mathcal{O}_K/P$$

*Proof.* Since $P^n \supset P^{n+1}$, so there exists $\alpha \in P^n$ and $\alpha \notin P^{n+1}$. Define a ring homomorphism:

$$f : \mathcal{O}_K \longmapsto P^n\mathcal{O}_K/P^{n+1}$$

by $f(x) \equiv x\alpha \pmod{P^{n+1}}$. Then

$$f(x) = 0 \iff x\alpha \equiv 0 \pmod{P^{n+1}} \iff x \in P$$

So the kernel of $f$ is $P$.

Now suppose we have $c \in P^n$. Then by Chinese Remainder Theorem, we have $\beta \in \mathbb{O}_K$ such that

$$\beta \equiv c \pmod{P^{n+1}} \text{ and } \beta \equiv 0 \pmod{I}$$

where $IP^n = \langle\alpha\rangle$, because $P^n \big| \langle\alpha\rangle$. Clearly, since $c \in P^n$ so if $\beta - c \in P^{n+1}$ then $\beta = c + d$ for some $d \in P^{n+1}$ and so

$$\beta \in P^n + P^{n+1} \in P^n$$

Then $P^n \big| \langle\beta\rangle$. Also $\beta \in I$ and so $I \big| \langle\beta\rangle$. But $P \nmid I$ because $\alpha \notin P^{n+1}$, so $P^n$ and $I$ are coprime. So

$$\langle\alpha\rangle = P^nI \big| \langle\beta\rangle$$

and so $\frac{\beta}{\alpha} \in \mathcal{O}_K$. Further,

$$f\left(\frac{\beta}{\alpha}\right) = \beta \equiv c \pmod{P^{n+1}}$$

Hence, the map is also surjective. The result follows by using isomorphism theorem. □

**Theorem 14.15.** *Let $K$ be a number field. Let $I$ and $J$ be non-zero integral ideals of $\mathcal{O}_K$. Then*

$$N(I)N(J) = N(IJ)$$

*Proof.* Suppose $I$ and $J$ are coprime, then the result follows by the ring version of Chinese Remainder Theorem (exercise 10 of chapter 13). Also, since each ideal can be factorised into product of prime ideals, so we only need to check for the case $I = P^m, J = P^n$ for some $m, n \geq 1$ and $P$ prime ideals.

Now since

$$\mathcal{O}_K/P^n \cong \mathcal{O}_K/P \times P\mathcal{O}_K/P^2 \times \cdots \times P^{n-1}\mathcal{O}_K/P^n$$

and for each $i$,

$$P^i\mathcal{O}_K/P^{i+1} \cong \mathcal{O}_K/P$$

by Lemma 14.14. Therefore,

$$card(\mathcal{O}_K/P^n) = (card(\mathcal{O}_K/P))^n$$

Use this, we have

$$card(\mathcal{O}_K/P^{m+n}) = card(\mathcal{O}_K/P^n)card(\mathcal{O}_K/P^m) = (card(\mathcal{O}_K/P))^{m+n}$$

This proves the remaining case and hence the result follows. □

The second proof is independent of the first one, It uses the order of ideals, together with Chinese Remainder Theorem. We shall begin with:

**Lemma 14.16.** *Let $I$ be a non-zero fractional ideal of $\mathcal{O}_K$ with $I \neq \mathcal{O}_K$. Let $J$ be a non-zero integral ideal of $\mathcal{O}_K$ with $J \neq \mathcal{O}_K$. Then there exists $\gamma \in I$, such that*

$$I = \langle \gamma \rangle + IJ$$

*Proof.* Let $P_1, \ldots, P_n$ be all possible prime ideals such that either

$$ord_{P_i}(I) \neq 0 \text{ or } ord_{P_i}(IJ) \neq 0$$

This is non-empty since $I \neq \mathcal{O}_K$. Then by Theorem 13.27, there exists $\gamma \in K$ such that

$$ord_{P_i}(\gamma) = ord_{P_i}(I), i = 1, 2, \ldots, n$$

and

$$ord_P(\gamma) \geq 0 \text{ for all prime ideals } P \neq P_1, \ldots, P_n$$

Then it is clear that

$$ord_P(\gamma) \geq ord_P(I) \text{ for all prime ideals } P$$

and so $\gamma \in I$ by Lemma 13.24. Now for $i = 1, 2, \ldots, n$ we have

$$\begin{aligned} ord_{P_i}(\langle \gamma \rangle + IJ) &= \min\left(ord_{P_i}(\langle \gamma \rangle), ord_{P_i}(IJ)\right) \\ &= \min\left(ord_{P_i}(I), ord_{P_i}(IJ)\right) \\ &= ord_{P_i}(I) \end{aligned}$$

because $J$ is an integral ideal. For any prime ideal $P \neq P_1, \ldots, P_n$, we have $ord_P(IJ) = ord_P(I) = 0$, and so

$$ord_P(\langle \gamma \rangle + IJ) = \min\left(ord_P(\langle \gamma \rangle), ord_P(IJ)\right) = 0 = ord_P(I)$$

Hence $ord_P(\langle \gamma \rangle + IJ) = ord_P(I)$ for all prime ideals $P$ and so

$$I = \langle \gamma \rangle + IJ$$

□

**Theorem 14.17.** *For any non-zero integral ideals $I, J \in \mathcal{O}_K$, we have*

$$N(IJ) = N(I)N(J)$$

*Proof.* This is clear if $I$ or $J = \mathcal{O}_K$. Hence we may assume $I, J \neq \mathcal{O}_K$ and let $m = N(I), n = N(J)$. Then by Theorem 14.13, $card(\mathcal{O}_K/I) = m, card(\mathcal{O}_K/J) = n$, where $m, n > 1$. Let

$$\mathcal{O}_K/I = \alpha_1 + I, \ldots, \alpha_m + I$$

and

$$\mathcal{O}_K/J = \beta_1 + J, \ldots, \beta_n + J$$

By Lemma 14.12, there exists $\gamma \in I$ such that

$$I = \langle \gamma \rangle + IJ$$

and $\gamma \neq 0$ otherwise $J = \mathcal{O}_K$. For any $x \in \mathcal{O}_K$, we have some $i$ such that

$$x \equiv \alpha_i \pmod{I}$$

Thus, $x - \alpha_i \in I = \langle \gamma \rangle + IJ$. So there exists $d \in \mathcal{O}_K$ and $y \in IJ$ such that

$$x - \alpha_i = \gamma d + y$$

Then there exists some $j$ such that

$$d \equiv \beta_j \pmod{J}$$

which implies $d - \beta_j \in J$. As $\gamma \in A$, we have

$$(d - \beta_j)\gamma \in IJ$$

and so

$$x = \alpha_i + \gamma d + y = \alpha_i + \beta_j \gamma + (d - \beta_j)\gamma + y \equiv \alpha_i + \beta_j \gamma \pmod{IJ}$$

This shows that $\alpha_i + \beta_j \gamma + IJ$ for ms a complete set of coset representatives of $\mathcal{O}_K / IJ$. Now we shall show they are distinct. Suppose

$$\alpha_i + \beta_j \gamma + IJ = \alpha_p + \beta_q \gamma + IJ$$

Then

$$\alpha_i + \beta_j \gamma \equiv \alpha_p + \beta_q \gamma \pmod{IJ}$$

and hence

$$\alpha_i - \alpha_p \equiv (\beta_q - \beta_j)\gamma \pmod{IJ}$$

But $IJ \subseteq I$ and $\gamma \in I$ so $\alpha_i - \alpha_p \in I$ and so $i = p$. So we have

$$(\beta_j - \beta_q)\gamma \in IJ$$

Let $P$ be any prime ideal which divides $J$. Then

$$\begin{aligned} ord_P(I) &= ord_P(\langle \gamma \rangle + IJ) \\ &= \min\left(ord_P(\gamma), ord_P(IJ)\right) \\ &= \min\left(ord_P(\gamma), ord_P(I) + ord_P(J)\right) \end{aligned}$$

Since $ord_P(J) \geq 1$ because $J$ is integral. So the above implies that

$$ord_P(I) = ord_P(\gamma) \text{ for any prime ideal } P \text{ which divides } J$$

Suppose $\beta_j \neq \beta_q$, then $(\beta_j - \beta_q)\gamma$ is a non-zero element of $IJ$, and so for any $P$ which divides $J$, we have

$$ord_P((\beta_j - \beta_q)\gamma) \geq ord_P(IJ)$$

and so

$$ord_P(\beta_j - \beta_q) + ord_P(\gamma) \geq ord_P(I) + ord_P(J)$$

which implies that

$$ord_P(\beta_j - \beta_q) \geq ord_P(J)$$

Also if $P$ does not divide $J$ then $ord_P(J) = 0$ but $ord_P(\beta_j - \beta_q) \geq 0$. So $\beta_j - \beta_q \in J$ by Lemma 13.24, contradicting $\beta_j \neq \beta_q$. Therefore, $\beta_j = \beta_q$. This proves that each $\alpha_i + \beta_j \gamma + IJ$ is distinct from others and so

$$card(\mathcal{O}_K / IJ) = mn$$

□

## 14.5 Norm of an element

We have seen the definition of norm of an element in Definition 12.35. In this subsection we are going to discuss the relation between $N(\alpha)$ and $N(\langle\alpha\rangle)$ for any $\alpha \in \mathcal{O}_K$. Recall that the norm of an element $\alpha$ is defined by

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and by previous knowledge, we know that $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are conjugates of $\alpha$.

**Theorem 14.18.** *Let $K$ be a number field of degree $n$. Let $\alpha \in \mathcal{O}_K$. Then*

$$N(\langle\alpha\rangle) = |N(\alpha)|$$

*Proof.* Let $\{e_1, \ldots, e_n\}$ be a basis for $\mathcal{O}_K$ and so $\{\alpha e_1, \ldots, \alpha e_n\}$ is a basis for $\langle\alpha\rangle$. Then the discriminant

$$D(\langle\alpha\rangle) = \begin{vmatrix} \sigma_1(\alpha e_1) & \ldots & \sigma_1(\alpha e_n) \\ \vdots & \ldots & \vdots \\ \sigma_n(\alpha e_1) & \ldots & \sigma_n(\alpha e_n) \end{vmatrix}^2$$

But since $\sigma$ is homomorphism, so $\sigma(\alpha e_i) = \sigma(\alpha)\sigma(e_i)$. Hence

$$D(\langle\alpha\rangle) = \prod_{i=1}^{n} (\sigma_i(\alpha))^2 \begin{vmatrix} \sigma_1(e_1) & \ldots & \sigma_1(e_n) \\ \vdots & \ldots & \vdots \\ \sigma_n(e_1) & \ldots & \sigma_n(e_n) \end{vmatrix}^2 = N(\alpha)^2 \mathcal{D}_K$$

Therefore,

$$N(\langle\alpha\rangle) = \sqrt{\frac{D(\langle\alpha\rangle)}{\mathcal{D}_K}} = \sqrt{N(\alpha)^2} = |N(\alpha)|$$

□

**Theorem 14.19.** *Let $K$ be a number field of degree $n$. Let $\alpha \in K$. Let*

$$min_{\mathbb{Q},\alpha}(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$$

*Then*

$$N(\langle\alpha\rangle) = |a_0|^{\frac{n}{m}}$$

*Proof.* Clearly, as $\mathbb{Q}(\alpha) \subseteq K$, so $m|n$. Let $\alpha_1 = \alpha, \ldots, \alpha_m$ be conjugates of $\alpha$ in $\mathbb{Q}(\alpha)$, and so

$$min_{\mathbb{Q},\alpha}(x) = \prod_{i=1}^{m} (x - \alpha_i)$$

and so

$$a_0 = (-1)^m \prod_{i=1}^{m} \alpha_i$$

Further, the conjugates of $\alpha \in K$ are:

$$\alpha, \alpha, \ldots, \alpha; \alpha_1, \ldots, \alpha_1; \ldots, \alpha_m, \ldots, \alpha_m$$

with each $\alpha_i$ repeated $\frac{n}{m}$ times. Thus, by Theorem 14.18,

$$N(\langle\alpha\rangle) = |N(\alpha)| = |(-1)^n a_0^{\frac{n}{m}}| = |a_0|^{\frac{n}{m}}$$

□

## 14.6 Norm of fractional ideal

In the last subsection of the chapter, we shall extend the definition of norm of an integral ideal to the norm of fractional ideal.

**Definition 14.20.** *Let $K$ be a number field and $\mathcal{O}_K$ be the ring of integers. Let $J$ be a fractional ideal and so there exists $0 \neq \gamma \in \mathcal{O}_K$ such that*

$$J = \frac{1}{\gamma} I$$

*for some integral ideal $I$. We shall define the* **norm** *of $J$ by*

$$N(J) = \frac{N(I)}{N(\langle \gamma \rangle)}$$

**Proposition 14.21.** *Definition 14.20 is well-defined. In other words, if*

$$J = \frac{1}{\alpha} I_1 = \frac{1}{\beta} I_2$$

*for integral ideals $I_1, I_2$ and $0 \neq \alpha, \beta \in \mathcal{O}_K$, then the norm of $J$ is independent of whether we choose $\alpha$ or $\beta$ in the first place.*

*Proof.* Let

$$J = \frac{1}{\alpha} I_1 = \frac{1}{\beta} I_2$$

Then

$$\alpha I_2 = \beta I_1 \Rightarrow \langle \alpha \rangle I_2 = \langle \beta \rangle I_1$$

as they are all integral ideals, then by Theorem 14.11, we have

$$N(\langle \alpha \rangle) N(I_2) = N(\langle \beta \rangle) N(I_1)$$

and hence

$$\frac{N(I_1)}{N(\langle \alpha \rangle)} = \frac{N(I_2)}{N(\langle \beta \rangle)}$$

Therefore, the norm of $J$ is independent of the choice of denominator. □

The next theorem shows that the multiplicative property for the norm of integral ideals carries over to fractional ideals.

**Theorem 14.22.** *Let $K$ be a number field. Let $I$ and $J$ be fractional ideals of $\mathcal{O}_K$. Then*

$$N(IJ) = N(I)N(J)$$

*Proof.* There exist $0 \neq \alpha, \beta \in \mathcal{O}_K$ such that

$$I = \frac{1}{\alpha} K_1, J = \frac{1}{\beta} K_2$$

for some integral ideals $K_1, K_2$ of $\mathcal{O}_K$. Then

$$IJ = \frac{1}{\alpha\beta} K_1 K_2$$

and so

$$N(IJ) = \frac{N(K_1 K_2)}{N(\langle \alpha\beta \rangle)}$$

By Theorem 14.15,

$$N(K_1K_2) = N(K_1)N(K_2)$$

and $\langle\alpha\beta\rangle = \langle\alpha\rangle\langle\beta\rangle$. Hence

$$N(IJ) = \frac{N(K_1)}{N(\langle\alpha\rangle)}\frac{N(K_2)}{N(\langle\beta\rangle)} = N(I)N(J)$$

□

Here is a useful remark.

**Remark 14.23.** *For any integral ideal $I \subseteq \mathcal{O}_K$, we have*

$$[I^{-1} : \mathcal{O}_K] = [\mathcal{O}_K : I]$$

*We shall prove this by establishing a map:*

$$f : I^{-1} \longmapsto \mathcal{O}_K/I$$

*by*

$$f(x) \equiv xy \ (mod\ I) \text{ where } y \in I \text{ is fixed}$$

*It is clear that $f$ is a module homomorphism. Now suppose $xy \in I$. If we have some $x \notin \mathcal{O}_K$ such that $xy \in I$, then $I|\langle x\rangle\langle y\rangle$ which is impossible by considering the factorisation of ideals. Hence the kernel is precisely $\mathcal{O}_K$. Then by module isomorphism theorem, we have*

$$I^{-1}/\mathcal{O}_K \cong \mathcal{O}_K/I$$

*and hence the result follows.*

## 14.7 Exercises

1. Let $K$ be a number field of degree $n = r + 2s$, where $r$ is the number of real embeddings and $2s$ is the number of complex embeddings. Show that the sign of discriminant $\mathcal{D}_K$ is $(-1)^s$.

2. Calculate the discriminant of the polynomial $f(x) = x^3 + ax + b$ where $a, b \in \mathbb{R}$. Hence or otherwise, show that $f(x)$ has three real distinct roots if $-4a^3 - 27b^2 > 0$, one real root, two non-real complex roots if $-4a^3-27b^2 < 0$ and at least two equal real roots if $-4a^3-27b^2 = 0$.

3. Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - 4\alpha + 2 = 0$. Let $\theta = \alpha + \alpha^2$. Compute $D(\theta)$. Is $K = \mathbb{Q}(\theta)$?

4. Let $K$ be a number field of degree $n$ and let $K = \mathbb{Q}(\alpha)$. Suppose that every root of $min_{\mathbb{Q},\alpha}(x)$ lies in $K$.

   (i) Let $\mathcal{D}_K = d^2$, where $d = \det(\sigma_i(x_j))$, $\sigma_1, \ldots, \sigma_n$ are embeddings and $\{x_1, \ldots, x_n\}$ is a basis for $\mathcal{O}_K$. Recall from the definition of determinant. For any matrix $A$,

   $$\det A = \sum_{\tau \in S_n} sgn(\tau) \prod_{i=1}^{n} A_{i\tau(i)}$$

   Let $d = P - N$ where $P$ is the sum in the determinant corresponds to even permutations in $S_n$ and $N$ corresponds to odd permutations. Show that $P + N, PN \in \mathbb{Z}$

(ii) Hence prove that

$$\mathcal{D}_K \equiv 0, 1 \pmod 4$$

The result is true in general and is known as Stickelberger's criteria, that

$$\mathcal{D}_K \equiv 0, 1 \pmod 4$$

which can be proved by using what we have done and taking **Galois closure** for the general number field $K$.

5. In this question we are going to deduce the discriminant of the polynomial which has the form

$$f(x) = x^n + px + q$$

(i) Consider the polynomial

$$P(x) = \prod_{i=1}^{n}(x - x_i)$$

Show that

$$disc(P(x)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(x_i)$$

where $P'(x)$ is the derivative of $P(x)$.

(ii) Let $f(x) = x^n + px + q$. Show that

$$x_i f'(x_i) = (n-1)p\left(-\frac{nq}{(n-1)p} - x_i\right)$$

and deduce that

$$disc(f) = (-1)^{\frac{n(n-1)}{2}}((1-n)^{n-1}p^n + n^n q^{n-1})$$

6. Let $K = \mathbb{Q}(\sqrt{p})$

(i) Suppose $p$ is a prime such that $p \equiv \pm 3 \pmod 8$. Prove that there does not exist an element $\alpha \in \mathcal{O}_K$ such that $N(\alpha) = 2$.

(ii) Suppose $p$ is a prime such that $p \equiv 5$ or $7 \pmod 8$. Prove that there does not exist an element $\alpha \in \mathcal{O}_K$ such that $N(\alpha) = -2$.

7. Let $K$ be a number field and let $I$ be a proper integral ideal. Show that

(i) If $N(I)$ is a prime, then $I$ is a prime ideal.

(ii) $\langle N(I) \rangle \subseteq I$.

8. Let $K$ be a number field and $P$ a prime ideal of $\mathcal{O}_K$. Prove that

$$G = \{a + P : a \in \mathcal{O}_K, a \notin P\}$$

is a cyclic group under multiplication. What is the order of $G$?

9. Let $K$ be a number filed and $I$ an integral ideal of $\mathcal{O}_K$ such that $N(I) = |N(\alpha)|$ for some $\alpha \in I$. Prove that $I = \langle \alpha \rangle$.

10. Let $K$ be a number field and $P$ a prime ideal of $\mathcal{O}_K$. Show that $P \cap \mathbb{Z} = \langle p \rangle$ for some prime number $p$.

11. Let $K$ be a number field. Let $n$ be a given positive integer. Prove that there are only finitely many integral ideals $I$ of $\mathcal{O}_K$ such that $N(I) = n$.

12. Let $K$ be a number field and $P$ a prime ideal of $\mathcal{O}_K$. Let $a \in \mathcal{O}_K$ such that $P \nmid \langle a \rangle$. Prove that

$$a^{N(P)} - 1 \equiv 0 \pmod{P}$$

13. Let $K$ be a number field and $I$ an integral ideal of $\mathcal{O}_K$ such that $pq \big| N(I)$, where $p$ and $q$ are distinct prime numbers. Prove that $I$ is not a prime ideal.

14. Let $K$ be a number field of degree 2. Let $\alpha \in \mathcal{O}_K$ such that $|N(\alpha)| = pq$, where $p$ and $q$ are coprime positive integers. Prove that

$$\langle \alpha, p \rangle \langle \alpha, q \rangle = \langle \alpha \rangle$$

⋆ 15. Let $K$ be a number field. Define the **inverse different** $\mathcal{R}_K^{-1}$ by

$$\mathcal{R}_K^{-1} = \{x \in K : T_{K/\mathbb{Q}}(xy) \in Z, \forall y \in \mathcal{O}_K\}$$

(i) Show that $\mathcal{R}_K^{-1}$ is a fractional ideal.
Now define the **different** to be the inverse of $\mathcal{R}_K^{-1}$, written $\mathcal{R}_K$

(ii) Show that $\mathcal{R}_K$ is an integral ideal of $\mathcal{O}_K$.

(iii) Show that $N(\mathcal{R}_K) = |\mathcal{D}_K|$.

(iv) Assume $\mathcal{O}_K = \mathbb{Z}[x]$ for some $x$ and let $f$ be the minimal polynomial of $x$ over $\mathbb{Q}$. Suppose $x_1 = x, \ldots, x_n$ are conjugates of $x$. Show that

$$\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(x_i)(T - x_i)}$$

(v) Deduce that

$$T_{K/\mathbb{Q}}\left(\frac{x^r}{f'(x)}\right) = \begin{cases} 0 & \text{if } 0 \leq r < n-1 \\ 1 & \text{if } r = n-1 \end{cases}$$

(vi) Deduce that

$$\mathcal{R}_K = \langle f'(x) \rangle$$

⋆ 16. Let $K$ be a number field. Define the Dedekind $\zeta$ function $\zeta_K(s)$ by

$$\zeta_K(s) = \sum_{0 \neq I \subseteq O_K} \frac{1}{N(I)^s}$$

summing over all non-zero integral ideals.

(i) Show that

$$\zeta_K(s) = \prod_P \frac{1}{1 - N(P)^{-s}}$$

where the sum is taking over all non-zero prime ideals $P$. Show that the product converges on the region $\mathcal{R}e(s) > 1$.

(ii) We have seen that the primes in $\mathbb{Z}[i]$ are (up to associate):
$1 \pm i$;
$p$ with $p \equiv 3 \pmod 4$;
$a + ib$ with $a^2 + b^2 = p$ where $p$ is a prime number with $p \equiv 1 \pmod 4$.
Let $K = \mathbb{Q}(i)$ and define the function $L$ by:

$$L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

where $\chi(p) = (-1)^{\frac{p-1}{2}}$ and the product is running over all odd prime numbers $p$. Show that

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s) \cdot L(\chi, s)$$

(iii) Show that

$$L(\chi, s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} \pm \cdots$$

17 Let $K = \mathbb{Q}(\sqrt{d})$ where $d > 3$ is a square-free integer. Show that if $\mathcal{O}_K$ is a Euclidean domain then it contains a principal ideal of norm 2 or 3.

## 14.8 Hint and Solutions

1. Let $\{x_1, \ldots, x_n\}$ be a basis for $\mathcal{O}_K$ and let $x_i^{(j)}, j = 1, 2, \ldots, n$ be the conjugates of $x_i$ for each $i$ and define the matrix $X$ with entry $X_{ij} = x_i^{(j)}$. Then

$$\mathcal{D}_K = (\det X)^2$$

Let $\det X = A + iB$, where $A, B \in \mathbb{R}$. Take conjugate, so we have

$$(\det X)^* = A - iB = \det X^*$$

But the complex embeddings appear as conjugate pairs, so taking the conjugate of the matrix is the same as swapping $s$ rows. So we have

$$(-1)^s(A + iB) = A - iB$$

If $s$ is odd, then $-A - iB = A - iB$ and so $A = 0$. Then

$$(\det X)^2 = i^2B^2 = -B^2 < 0$$

If $s$ is even, then $A + iB = A - iB$ and so $B = 0$. Then

$$(\det X)^2 = A^2 > 0$$

2. Let $\alpha, \beta$ and $\gamma$ be the roots of $x^3 + ax + b = 0$. So we have

$$\alpha + \beta + \gamma = 0 \Rightarrow \alpha = -\beta - \gamma$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = a \Rightarrow \beta^2 + \gamma^2 + \beta\gamma = -a$$

$$\alpha\beta\gamma = -b \Rightarrow \beta^2\gamma + \beta\gamma^2 = b$$

The discriminant $d^2$ is

$$(\beta - \alpha)^2(\gamma - \beta)^2(\alpha - \gamma)^2 = (2\beta + \gamma)^2(\gamma - \beta)^2(2\gamma + \beta)^2$$

Then we have

$$\begin{aligned} d^2 &= (4\beta^2 + \gamma^2 + 4\beta\gamma)(4\gamma^2 + 4\beta\gamma + \beta^2)(\beta^2 + \gamma^2 - 2\beta\gamma) \\ &= (33\beta^2\gamma^2 + 4\gamma^4 + 4\beta^4 + 20\beta^3\gamma + 20\beta\gamma^3)(\beta^2 + \gamma^2 - 2\beta\gamma) \\ &= 4\beta^6 + 4\gamma^6 - 3\beta^2\gamma^4 - 3\beta^4\gamma^2 - 26\beta^3\gamma^3 + 12\beta\gamma^5 + 12\beta^5\gamma \end{aligned}$$

Now we have

$$-a^3 = \beta^6 + \gamma^6 + 3\beta^5\gamma + 3\beta\gamma^5 + 6\beta^4\gamma^2 + 6\beta^2\gamma^4 + 7\beta^3\gamma^3$$

and

$$b^2 = \beta^4\gamma^2 + \beta^2\gamma^4 + 2\beta^3\gamma^3$$

Hence the discriminant $d^2 = -4a^3 - 27b^2$.

The result follows by the following observation:
We have two equal roots if and only if discriminant is 0. If the discriminant is not zero, then two roots are complex conjugate, say $\alpha$ and $\beta$ then

$$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 < 0$$

because

$$(\alpha - \gamma)^2(\beta - \gamma)^2 = |\alpha - \gamma|^4 > 0$$

and

$$(\alpha - \beta)^2 = 4(Im(\alpha))^2 < 0$$

3. We have

$$\theta^2 = \alpha^4 + 2\alpha^3 + \alpha^2 = 5\alpha^2 + 6\alpha - 4$$

$$\theta^3 = 22\alpha^2 + 30\alpha - 22$$

Hence, we have

$$\theta^3 - 8\theta^2 + 18\theta - 10 = 0$$

Since the discriminant only depends on the difference of the roots, so we may shift each root by $\frac{8}{3}$, i.e let $f(x) = x^3 - 8x^2 + 18x - 10$ and $y = (x - \frac{8}{3})$, then

$$g(y) = y^3 - \frac{10}{3}y + \frac{2}{27}$$

so the discriminant of $g(y)$ is (Use question 2)

$$-4\left(-\frac{10}{3}\right)^3 - 27\left(\frac{2}{27}\right)^2 = 148$$

Hence the discriminant of $f(x)$ is also 148. By Theorem 14.8, we conclude $D(\theta) = 148$. Since $D(\theta) \neq 0$, then $K = \mathbb{Q}(\theta)$.

4. (i) By definition,

$$P + N = \sum_{\tau \in S_n} \prod_{i=1}^{n} A_{i\tau(i)}$$

and

$$PN = \left( \sum_{\tau \text{ even} \in S_n} \prod_{i=1}^{n} A_{i\tau(i)} \right) \left( \sum_{\tau \text{ odd} \in S_n} \prod_{i=1}^{n} A_{i\tau(i)} \right)$$

Since every root lies in the field $K$, so the embeddings $\{\sigma_1, \ldots, \sigma_n\}$ is the automorphism group of $K$ over $\mathbb{Q}$. (Recall that $|Aut_{\mathbb{Q}}(K, K)| \leq [K : \mathbb{Q}]$.) Let $\sigma$ be any element in the automorphism group $G$. But each entry $A_{ij} = \sigma_i(x_j)$, so consider

$$\sigma(P + N) = \sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma(\sigma_i(x_{\tau(i)})) = (P + N)$$

because the product running through $\sigma\sigma_i$ will again run though $\sigma_i$ for all $i$ and so for each $\tau$ the effect of $\sigma$ is to replace $\tau$ by $\tau\sigma^{-1}$ where $\sigma$ is a permutation on $i$ induced by the action of $\sigma$ on $\sigma_i$s. For the same reason, we have $\sigma(PN) = PN$. Hence $P + N, PN$ are invariant under the action of $G$, and hence is fixed by $G$. But $G = Aut_{\mathbb{Q}}(K)$, so $P + N, PN \in \mathbb{Q}$. Finally, since $\sigma_i(x_j)$ is algebraic integer for all $i, j$ and so $P$,$N$ are both algebraic integers. Therefore, $P + N, PN$ are rational and algebraic integers, and so they must be ordinary integers.

$$P + N, PN \in \mathbb{Z}$$

(ii) Observe that $d^2 = (P + N)^2 = (P - N)^2 + 4PN$. Hence

$$\mathcal{D}_K = d^2 = (P - N)^2 + 4PN \equiv 0, 1 \pmod 4$$

because any square is either 0 or 1 mod 4.

5. (i) For any $i$,

$$P'(x_i) = \sum_{k=1}^{n} \prod_{j \neq k} (x_i - x_j) = \prod_{j \neq i} (x_i - x_j)$$

Hence

$$disc(P(x)) = \prod 1 \leq j < i \leq n (x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(x_i)$$

because the factor $(x_i - x_j)^2$ comes from the factor $x_i - x_j$ in $P'(x_i)$ and $x_j - x_i$ in $P'(x_j)$ and the sign changes each time. Since we have $\binom{n}{2} = \frac{n(n-1)}{2}$ such factors, so the sign changes $(-1)^{\frac{n(n-1)}{2}}$ times.

(ii)

$$\begin{aligned} x_i f'(x_i) &= n x_i^{n-1} + p x_i \\ &= n(x_i^n + p x_i + q) - (n-1) p x_i - nq \\ &= -(n-1) p x_i - nq \end{aligned}$$

which is what we want because $x_i^n + p x_i + q = 0$. Then

$$\begin{aligned} \prod_{i=1}^{n} x_i f'(x_i) &= (-1)^n (nq + (n-1) p x_1)(nq + (n-1) p x_2) \\ &\quad \cdots (nq + (n-1) p x_n) \end{aligned}$$

But

$$x^n + px + q = (x - x_1) \cdots (x - x_n)$$

and so the elementary functions of degree $k$ is zero except $k = n-1, n$. Hence in the above product, the only two non-zero terms are

$$(nq)^n = n^n q^n \text{ and } ((n-1)p)^n \prod_{i=1}^{n} x_i = ((n-1)p)^n (-1)^n q$$

Therefore,

$$\prod_{i=1}^{n} x_i f'(x_i) = (-1)^n (n^n q^n + ((n-1)p)^n (-1)^n q)$$

and so using the previous part,

$$disc(f(x)) = (-1)^{\frac{n(n-1)}{2}} (n^n q^{n-1} + (1-n)^n p^n)$$

because $\prod_{i=1}^{n} x_i = (-1)^n q$.

6. Both questions can be done by the following observation. If $p \not\equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{p}]$ and so for any $\alpha \in \mathcal{O}_K$, we have $\alpha = a + b\sqrt{p}$, $a, b \in \mathbb{Z}$. Then $N(\alpha) = a^2 - bp^2$. Then to check there does not exist $\alpha$ such that $N(\alpha) = k$, we can reduce the above modulo $p$. So check whether

$$a^2 \equiv k \pmod p$$

exists.

If $p \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ and so for any $\alpha \in \mathcal{O}_K$, we have $\alpha = a + b(\frac{1+\sqrt{p}}{2})$. Then $N(\alpha) = a^2 + ab + b^2(\frac{1-p}{4})$. Then if there exists $\alpha$ whose norm is $k$, then

$$4a^2 + 4ab + b^2 - b^2 p = 4k$$

and so

$$(2a + b)^2 \equiv 4k \pmod p$$

But

$$\left(\frac{4k}{p}\right) = \left(\frac{k}{p}\right)$$

So in the first part,

$$\left(\frac{2}{p}\right) = -1 \text{ if } p \equiv \pm 3 \pmod 8$$

and in the second part,

$$\left(\frac{-2}{p}\right) = -1 \text{ if } p \equiv 5, 7 \pmod 8$$

So in fact, we have proved a stronger fact.

7. (i) Suppose not, then $I$ can be written as a product ideals. Say $I = JK$. Then $N(I) = N(J)N(K)$ and since $N(J)$ and $N(K)$ are both integers, so $N(I)$ is not prime, which is a contradiction.

   (ii) If $I = \mathcal{O}_K$, then $N(I) = 1$ and $1 \in I$. Suppose $I$ is a proper integral ideal, then consider

   $$1 + I, 2 + I, \ldots \in \mathcal{O}_K$$

   But $\mathcal{O}_K / I$ is finite, so there exists $k \in \mathbb{N}, k > 1$ such that $k \in I$. Hence the order of $1 + I \in \mathcal{O}_K$ is $k$. But the order of the (additive) group $\mathcal{O}_K$ is $N(I)$. Hence $k | N(I)$ and so $N(I) \in I$ because $k \in I$.

8. Since $P$ is prime, and so maximal in a Dedekind domain. Hence $\mathcal{O}_K/P$ is a field and is finite. So the multiplication group of a finite field is cyclic. The order of the group is $N(P)$.

9. $N(I) = |N(\alpha)| = N(\langle\alpha\rangle)$, and $\alpha \in I$, so $\langle\alpha\rangle \subseteq I$. Then

$$N(I)^2 = \frac{D(I)}{\mathcal{D}_K}, N(\langle\alpha\rangle)^2 = \frac{D(\langle\alpha\rangle)}{\mathcal{D}_K}$$

But $N(I) = N(\langle\alpha\rangle)$, so $D(I) = D(\langle\alpha\rangle)$, and so the index of $\langle\alpha\rangle$ in $I$ is 1, and so $I = \langle\alpha\rangle$.

10. Since $P$ is a prime ideal, so $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, so $P \cap \mathbb{Z} = \langle\alpha\rangle$. Hence $P \cap \mathbb{Z}$ is prime, so $\alpha = p$ is a prime number.

11. By question 7(ii),

$$I|\langle N(I)\rangle$$

so we have

$$I|\langle n\rangle$$

But $n$ is fixed, so we can factorise $\langle n\rangle$ into prime ideals, and so there are only finitely many integral ideals $I$ such that $I|\langle n\rangle$.

12. Since $a \notin P$, so we consider the order (under multiplication) of $a + P$ in $\mathcal{O}_K/P$. (It is a group because $P$ is prime and so maximal, so $\mathcal{O}_K/P$ is a field.) Since the order of the group (under multiplication) $\mathcal{O}_K/P$ is $N(P)$. So $(a + P)^{N(P)} = 1 + P$ and so

$$a^{N(P)} - 1 \equiv 0 \pmod{P}$$

13. Suppose $I$ is a prime ideal. Then $I$ is maximal and hence $\mathcal{O}_K/I$ is a finite field. Then $N(I) = p^k$ for some prime $p$ and $k > 0$, which contradicts $pq\big|N(I)$.

14. Let

$$I = \langle\alpha, p\rangle, J = \langle\alpha, q\rangle, K = \langle\alpha\rangle$$

It is clear that

$$I, J|K \text{ because } K \subseteq I, J$$

Also, since $(p, q) = 1$, so $I + J = \langle 1\rangle = \mathcal{O}_K$. Then $I$ and $J$ are coprime and so

$$IJ|K \Rightarrow N(I)N(J)|N(K) = pq$$

In particular, $N(I), N(J)|pq$. Now $I|\langle p\rangle$, so

$$N(I)|N(\langle p\rangle) = p^2 \text{ because } [K : \mathbb{Q}] = 2$$

Therefore, $N(I)|pq, p^2 \Rightarrow N(I)|p$ because $p$ and $q$ are coprime. Similarly, $N(J)|q$. But by question 7(ii), $N(I) \in I$ and clearly that $p$ is the least positive integer in $I$. Hence $N(I) = p$. Similarly, $N(J) = q$ and so $N(I)N(J) = pq = N(K)$. Therefore,

$$IJ = K$$

Alternatively, we can calculate the discriminant of $I, J$ and $K$ directly and conclude $IJ = K$.

15. (i) If $u, v \in \mathcal{R}_K^{-1}$, then

$$T_{K/\mathbb{Q}}((u+v)y) = T_{K/\mathbb{Q}}(vy) + T_{K/\mathbb{Q}}(vy) \in \mathbb{Z}, \forall y \in \mathcal{O}_K$$

If $u \in \mathcal{R}_K^{-1}$, and $d \in \mathcal{O}_K$, then

$$T_{K/\mathbb{Q}}(udy) = T_{K/\mathbb{Q}}(u(dy)) \in \mathbb{Z}, \forall y \in \mathcal{O}_K$$

Now we need to check the third property of fractional ideal. As in the proof of Theorem 12.38, there exists $\{e_1, \ldots, e_n\} \subseteq \mathcal{O}_K$ which is a $\mathbb{Q}$-basis for $K$. Since $K/\mathbb{Q}$ is separable, so the trace pairing $T$ is non-degenerate. Let $T$ be the matrix such that

$$P_{ij} = T(e_i, e_j)$$

Let $d = \det P$ and so $d \neq 0$. Let $Q = P^{adj}$ so that $PQ = dI$, so

$$\sum_{j=1}^{n} P_{ij}Q_{jk} = \begin{cases} d & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$$

Suppose now $x \in \mathcal{R}_K^{-1}$, then there exist $a_1, \ldots, a_n \in \mathbb{Q}$ such that

$$x = \sum_{i=1}^{n} a_i e_i$$

and so

$$T_{K/\mathbb{Q}}(xe_j) = \sum_{i=1}^{n} T_{K/\mathbb{Q}}(a_i e_i e_j) = \sum_{i=1}^{n} a_i P_{ij}$$

Therefore, we have

$$da_k = \sum_{j=1}^{n} T_{K/\mathbb{Q}}(xe_j)Q_{jk} \in \mathcal{O}_K$$

because the each entry of $Q_{jk}$ lies in $\mathcal{O}_K$ and $T_{K/\mathbb{Q}}(xe_j) \in \mathbb{Z}$. Therefore,

$$dx = \sum_{i=1}^{n} da_i e_i \in \mathcal{O}_K$$

and so

$$d\mathcal{R}_K^{-1} \subseteq \mathcal{O}_K$$

(ii) By definition, $\mathcal{R}_K = \{x \in K : x\mathcal{R}_K^{-1} \subseteq \mathcal{O}_K\}$. Pick any $x \in \mathcal{R}_K$ and any $y \in \mathcal{R}_K^{-1}$, then we have $xy \in \mathcal{O}_K$, in particular, since $1 \in \mathcal{R}_K^{-1}$, so

$$x = x \cdot 1 \in \mathcal{O}_K$$

Therefore, $\mathcal{R}_K \subseteq \mathcal{O}_K$.

(iii) Let $\{e_1, \ldots, e_n\}$ be a basis for $\mathcal{O}_K$ and $\{f_1, \ldots, f_n\}$ be its dual basis with respect to the trace pairing. In other words,

$$T(e_i, f_j) = \delta_{ij}$$

Then for any $x \in \mathcal{R}_K^{-1}$, we claim that

$$x = \sum_{i=1}^{n} T(x, e_i) f_i$$

because we can multiply both sides by $e_j$ and take the trace. Since the trace is a non-degenerate linear map, so this shows that

$$T_{K/\mathbb{Q}}(xe_j) = T(x, e_j) = T_{K/\mathbb{Q}}(xe_j)$$

for all $e_j$ and since $\{e_1, \ldots, e_n\}$ is a basis, so we have what we claimed. Since $T(x, e_i) \in \mathbb{Z}$ as $x \in \mathbb{R}_K^{-1}$, so $\{f_1, \ldots, f_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{R}_K^{-1}$.
Now for each $i$, write

$$e_i = \sum_{j=1}^{n} a_{ij} f_j \text{ for some } a_{ij} \in \mathbb{Z}$$

because $\mathcal{O}_K \subseteq \mathcal{R}_K^{-1}$. Then multiply both sides by $e_k$ and take trace, we have

$$T(e_i, e_k) = a_{ik}$$

and so the matrix $A$ has entries $a_{ij} = T(e_i, e_j)$. Hence we have

$$T(e_i, e_j) = T(\sum_{k=1}^{n} a_{ik} f_k, \sum_{k=1}^{n} a_{jk} f_k)$$

Taking determinant of both sides, we have

$$\mathcal{D}_K = (\mathcal{D}_K)^2 disc(\mathcal{R}_K^{-1})$$

and so the index

$$[\mathcal{R}_K^{-1} : \mathcal{O}_K] = |\mathcal{D}_K|$$

Finally, by Remark 14.23, we have

$$N(\mathcal{R}_K) = [\mathcal{O}_K : \mathcal{R}_K] = [\mathcal{R}_K^{-1} : \mathcal{O}_K] = |\mathcal{D}_K|$$

(iv) For each $i$, we have

$$f'(x_i) = \prod_{j \neq i} (x_i - x_j)$$

Consider

$$\sum_{i=1}^{n} \frac{1}{(T - x_i) f'(x_i)} = \frac{\sum_{i=1}^{n} A_i(T)}{f(T)} = \frac{C(T)}{f(T)}$$

where

$$A_i(T) = \frac{f(T)}{f'(x_i)(T - x_i)}$$

It is clear that $C(T)$ has degree at most $n - 1$. But let $T = x_i$ for a fixed $i$. Then

$$A_i(x_i) = \frac{\prod_{j \neq i} (x_i - x_j)}{f'(x_i)} = 1, A_j(x_i) = 0$$

and so $C(x_i) = 1$ for each $i$. Then $C(T) - 1$ has $n$ zeros but $C(T) - 1$ has degree at most $n - 1$. So we conclude that $C(T) - 1 = 0$ and so $C(T) = 1$.

(v) Since the embeddings are homomorphism, so

$$T_{K/\mathbb{Q}} \left( \frac{x^r}{f'(x)} \right) = \sum_{i=1}^{n} \left( \frac{x_i^r}{f'(x_i)} \right)$$

Consider

$$\sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)(T-x_i)} = \frac{\sum_{i=1}^n A_i(T)}{f(T)} = \frac{C(T)}{f(T)}$$

where

$$A_i(T) = \frac{f(T)}{f'(x_i)(T-x_i)} x_i^r$$

It is clear that for each $i$,

$$A_i(x_i) = x_i^r, A_j(x_i) = 0$$

So $C(x_i) = x_i^r$. Now the degree of $C(T) - T^r$ is at most $n-1$, and $C(T) - T^r$ has $n$ roots, $x_1, \ldots, x_n$. so $C(T) = T^r$. Then

$$\frac{T^r}{f(T)} = \sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)(T-x_i)}$$

and multiply both sides by $f(T)$, we have

$$T^r = \sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)} \prod_{j \neq i} (T - x_j)$$

Hence, by comparing the coefficient of $T^{n-1}$ on both sides and since $r < n-1$, we have

$$\sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)} = 0$$

For $r = n-1$, we again compare the coefficient of both sides, so

$$\sum_{i=1}^{n} \frac{x_1^{n-1}}{f'(x_i)} = 1$$

(vi) Since $\mathcal{O}_K = \mathbb{Z}[x]$ so $\{1, x, \ldots, x^{n-1}\}$ is a basis for $\mathcal{O}_K$. We have shown above that the dual basis of $\{1, x, \ldots, x^{n-1}\}$ with respect to the trace pairing is a basis for $\mathcal{R}_K^{-1}$. Let the minimal polynomial $f$ be

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$$

Consider the dual element of 1. Let $\alpha = \frac{b_{n-1}x^{n-1} + \cdots + b_1 x + b_0}{f'(x)}$, and we want

$$T(\alpha, 1) = 1, T(\alpha, x^r) = 0$$

Then we have $b_{n-1} = 1$ by $T(\alpha, 1) = 1$ and use (v). By the above relation, we have $x^n = -a_{n-1}x^{n-1} - \cdots - a_0$ so that $T(\alpha, x) = 0$ implies that $b_{n-2} = a_{n-1}$. Similarly, we may use the relation and continue in this way, so that we can uniquely determine the values of $b_i$. So we may write the dual basis as:

$$\left\{ \frac{\alpha_1}{f'(x)}, \ldots \frac{\alpha_n}{f'(x)} \right\}$$

where $\alpha_1, \ldots, \alpha_n$ is a polynomial in $x$ whose coefficients are sum and products of $a_i$ and so lies in $\mathcal{O}_K$. Therefore, we conclude that

$$\mathcal{R}_K^{-1} = \frac{\mathcal{O}_K}{f'(x)}$$

and so

$$\mathcal{R}_K = \langle f'(x) \rangle$$

16. (i) We firstly show that the product converges. For each $k \geq 1$ and $p$ prime, $\frac{1}{1-(p^k)^{-s}} \leq \frac{1}{1-p^{-s}}$ Also if $[K:\mathbb{Q}] = n$, then each each prime lies in at most $n$ prime ideals, and so we have

$$\prod_P \frac{1}{1-N(P)^{-s}} \leq \prod_p \frac{n}{1-p^{-s}}$$

and the right hand side converges on $\mathcal{R}e(s) > 1$ (which we have seen before) so the left hand side also converges on this region. Then we can expand the product as

$$\prod_P \frac{1}{1-N(P)^{-s}} = \prod_P \left( \sum_{k=0}^{\infty} \frac{1}{(N(P)^s)^k} \right)$$

and since each proper integral ideal can be factorised into prime ideals, so

$$\zeta_K(s) = \sum_{0 \neq I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s} = \prod_P \frac{1}{1-N(P)^{-s}}$$

(ii) Since $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, and each ideal is principal, so it is clear that $\zeta_{\mathbb{Q}}(s)$ is just the Riemann $\zeta$ function. Also $K = \mathbb{Q}[i]$ and so $\mathcal{O}_K = \mathbb{Z}[i]$, which is a Euclidean domain and so is a principal ideal domain. Thus, each prime ideal in $\mathbb{Z}[i]$ is generated by a prime element in $\mathbb{Z}[i]$. If the prime element is $a+ib$, where $b \neq 0$, then the norm must be a prime $p$ such that $p \equiv 1 \pmod 4$. (or $p = 2$), and if $a+ib$ is prime, so is $a-ib$. So each $p \equiv 1 \pmod 4$ appears twice in the product. On the other hand, the prime $p \equiv 3 \pmod 4$ is itself a prime element in $\mathbb{Z}[i]$ and so the norm of it is $p^2$. Therefore, using

$$p \equiv 1 \pmod 4 \iff (-1)^{\frac{p-1}{2}} = 1$$

we conclude that

$$\begin{aligned} \zeta_K(s) &= \prod_{p \equiv 3 \pmod 4} \frac{1}{1-p^{-2s}} \prod_{p \equiv 1 \pmod 4} \frac{1}{(1-p^{-s})^2} \\ &= \prod_p \frac{1}{1-p^{-s}} \prod_p \frac{1}{1-\chi(p)p^{-s}} \\ &= \zeta_{\mathbb{Q}}(s) \cdot L(\chi, s) \end{aligned}$$

(iii)

$$L(\chi, s) = \prod_{p \equiv 1 \pmod 4} \left( \sum_{k=0}^{\infty} \frac{1}{(p^{-s})^k} \right) \prod_{p \equiv 3 \pmod 4} \left( \sum_{k=0}^{\infty} \frac{(-1)^k}{(p^{-s})^k} \right)$$

Now each odd integer can be written as a product of odd primes, and from the above expression, we can see that the negative sign comes in if we have a prime which is 3 modulo 4. Hence the sign is negative if and only if it contains odd number of prime factors which are 3 modulo 4 and so itself is 3 modulo 4. Therefore,

$$L(\chi, s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}$$

17. Let $\phi$ be a Euclidean function on $\mathcal{O}_K$. By property of Euclidean function, we know that the units take the same value (as $\phi(1)$) and $\phi(1)$ take the minimal value (apart from 0). Then let $x$ be the element in $\mathcal{O}_K$ such that $\phi(x)$ is minimal among elements in $\mathcal{O}_K \backslash \{0, \pm 1\}$ since the only units in $\mathcal{O}_K$ are $\pm 1$.

Now for all $y \in \mathcal{O}_K$ there exists $q, b$ such that

$$y = qx + b$$

with either $b = 0$ or $\phi(b) < \phi(x)$. But by choice of $x$, $b = 0$ or $b = \pm 1$. Therefore, we conclude that for all $y \in \mathcal{O}_K$,

$$y \equiv 0, \pm 1 \pmod{x}.$$

This shows that $|\mathcal{O}_K/\langle x \rangle|$ is at most 3.

# 15 Factorisation of prime numbers

In this section we shall give many examples and deduce some useful results about the factorisation of ordinary prime numbers in the ring of integers $\mathcal{O}_K$ for some number field $K$.

## 15.1 Basic property

We shall begin with some restriction of the norm of prime ideals.

**Lemma 15.1.** *Let $K$ be a number field. Let $P$ be a prime ideal of $\mathcal{O}_K$. Then there exists a* **unique** *prime number $p \in \mathbb{Z}$ such that*

$$P \big| \langle p \rangle$$

*Proof.* It is clear that $P \cap \mathbb{Z}$ is a prime ideal and hence there exists a prime number $p$ such that

$$P \cap \mathbb{Z} = \langle p \rangle$$

since $\mathbb{Z}$ is a principal ideal domain. Now suppose there is a prime $q$ such that

$$P \big| \langle q \rangle$$

Then $q \in P \cap \mathbb{Z}$ and so $q \in \langle p \rangle$. Then $p|q$ and so $q = p$. This proves the uniqueness. □

**Theorem 15.2.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Let $P$ be a prime ideal of $\mathcal{O}_K$. Let $p$ be a prime number which lies in $P$ (which exists and is unique by Lemma 15.1.) Then*

$$N(P) = p^f$$

*for some $f \leq n$.*

*Proof.* By Lemma 15.1, we have $P \big| \langle p \rangle$ and hence

$$N(P) \big| N(\langle p \rangle) = |N(P)| = p^n$$

Therefore, $N(P) = p^f$ for some $f \leq n$ because $p$ is a prime. □

**Definition 15.3.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Let $P$ be a prime ideal and $p$ be a prime number lies in $P$. Then By Theorem 15.2, then the positive integer $f$ such that*

$$N(P) = p^f$$

*is called the* **inertial degree** *of $P$ in $\mathcal{O}_K$ and is denoted by $f_K(P)$.*

**Proposition 15.4.** *Let $K$ be a number field and $P$ a prime ideal of $\mathcal{O}_K$. Let $p$ be a prime number in $P$. Let $a, b \in \mathbb{Z}$. Then*

$$a \equiv b \ (mod\ p) \iff a \equiv b \ (mod\ P)$$

*Proof.* If $a \equiv b \pmod{p}$ then $a - b \in \langle p \rangle$ and so $a - b \in P$ because

$$P \big| \langle p \rangle$$

Conversely, if $a \equiv b \pmod{P}$ then $P \big| \langle a - b \rangle$. Then

$$p^f \big| (a-b)^n = N(\langle a - b \rangle)$$

and so

$$(a-b)^n \equiv 0 \pmod{p} \Rightarrow a \equiv b \ (textmodp)$$

□

**Theorem 15.5.** *Let $K$ be a number field with $[K:\mathbb{Q}] = n$. Let $p$ be a prime number. Suppose that the principal ideal $\langle p\rangle$ factors in $\mathcal{O}_K$ in the form*

$$\langle p\rangle = \prod_{i=1}^{g} P_i^{e_i}$$

*where $P_1, \ldots, P_g$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, \ldots, e_g$ are positive integers. Suppose $f_i$ is the inertia degree of $P_i$ in $K$, then*

$$\sum_{i=1}^{g} e_i f_i = n$$

*Proof.* This follows immediately by taking the norm of $\langle p\rangle$, so

$$N(\langle p\rangle) = p^n = \prod_{i=1}^{g} (p^{f_i})^{e_i}$$

and so

$$\sum_{i=1}^{g} e_i f_i = n$$

□

**Corollary 15.6.** *Let $K$ be a number field with $[K:\mathbb{Q}] = n$ and $P$ a prime ideal in $\mathcal{O}_K$. Let $p$ be a prime number in $P$. If $P^n \big| \langle p\rangle$, then*

$$P^n = \langle p\rangle$$

*Proof.* $N(P^n) = N(P)^n$. Let $f_K(P) = f$. Then we have

$$fn \leq n$$

which says $f \leq 1$ and so $f = 1$. So $N(P^n) = p^n$ and so $P^n = \langle p\rangle$. □

**Definition 15.7.** *Let $K$ be a number field. Let $p$ be a prime number. Then the number of distinct prime ideals of $\mathcal{O}_K$ which divide $p$ is called the* **decomposition number** *of $p$ in $K$, written $g_K(p)$.*

It follows immediately from Theorem 15.5 that the decomposition number $g_K(p) \leq n$ if $[K:\mathbb{Q}] = n$.

**Definition 15.8.** *Let $K$ be a number field and $P$ a prime ideal in $\mathcal{O}_K$. Let $p$ be the prime number in $P$. Then the unique positive integer $e$ such that*

$$P^e \big| \langle p\rangle, P^{e+1} \nmid \langle p\rangle$$

*is called the* **ramification index** *of $P$ in $K$ and is written $e_K(P)$. It is clear that $e_K(P) \leq n$.*

In the notation of Theorem 15.5, we have

$$e_K(P_i) = e_i, f_K(P_i) = f_i, g_K(p) = g$$

## 15.2 Ramification

**Definition 15.9.** *Let $K$ be a number field of degree $n$. Let $p$ be a prime number. Let $P_1, \ldots, P_{g_K(p)}$ be the prime ideals which divide $\langle p \rangle$, and let $e_i = e_K(P_i)$. If $e_i > 1$ for some $i \in \{1, \ldots, g\}$, then $p$ is said to* **ramify** *in $K$. If $e_i = 1$ for all $i$, then we say $p$ is* **unramified** *in $K$.*

The main result we are going to deduce in this subsection is to show that a prime $p$ ramifies in $K$ if and only if $p|\mathcal{D}_K$. We shall begin with:

**Theorem 15.10.** *$p$ ramifies in $K$ if and only if $\mathcal{O}_K/\langle p \rangle$ has a nilpotent element.*

*Proof.* By Chinese Remainder Theorem, suppose that

$$\langle p \rangle = \prod_{i=1}^{g} P_i^{e_i}$$

So we have

$$\mathcal{O}_K/\langle p \rangle \cong \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_k^{e_k}$$

Now for each $i$, consider $\mathcal{O}_K/P_i^{e_i}$. Either $e_i = 1$, so that it is a finite field because $P_i$ is prime and hence maximal; Or $e_i \geq 2$, and it has a non-zero nilpotent element, because we could take $\alpha \in P_i$ but $\alpha \notin P_i^2$, so we have $0 \neq \alpha + P_i^{e_i}$ in $\mathcal{O}_K/P_i^{e_i}$, such that

$$(\alpha + P_i^{e_i})^{e_i} = 0$$

because $\alpha^{e_i} \in P_i^{e_i}$.

So in the first case, $\mathcal{O}_K$ is a product of finite field, which contains no nilpotent element, and in the second case, we have a nilpotent element in the subring and so a nilpotent element in $\mathcal{O}_K$. □

**Theorem 15.11.** *Let $p$ be a prime number. Then $p$ ramifies in $K$ if and only if $p|\mathcal{D}_K$.*

*Proof.* Recall that the discriminant is the determinant of the matrix which represents the trace pairing. Let $T_{ij} = T(e_i, e_j)$ where $\{e_1, \ldots, e_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then

$$p|\mathcal{D}_K \iff p|\det T \iff \det T \equiv 0 \pmod{p}$$

Consider the matrix $\bar{T} = T$ modulo $p$. Then

$$\bar{T} : \mathcal{O}_K/\langle p \rangle \times \mathcal{O}_K/\langle p \rangle \longmapsto \mathbb{Z}/\langle p \rangle$$

and so by above

$$p|\mathcal{D}_K \iff \det \bar{T} = 0 \iff \bar{T} \text{ is degenerate}$$

Now as $p$ is a prime, so $\mathbb{Z}/p\mathbb{Z}$ is a field. Also $p \in P_i^{e_i}$ for each $i$, so $\mathcal{O}_K/P_i^{e_i}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space. Then we restrict $T$ on each $\mathcal{O}_K/P_i^{e_i}$. If $e_i = 1$, as in the proof of Theorem 15.10,$\mathcal{O}_K/P_i$ is a field and is finite. So it is a finite extension of field $\mathbb{F}_p$, which is separable. Therefore, if $e_i = 1$ for all $i$, then $T$ is non-degenerate on each subspace and so is non-degenerate on the whole vector space. If $e_i \geq 2$ for some $i$. Then again as in the proof of Theorem 15.10, we have a nilpotent element, say $\alpha$, in $\mathcal{O}_K/\langle p \rangle$ and let $\alpha^n = 0$. Then $(\alpha x)^n = 0$ for all $x \in \mathcal{O}_K/\langle p \rangle$. In particular, the linear map $\phi_{\alpha x}$ (Definition 12.25) is nilpotent. So every eigenvalue is 0 and since the trace is the sum of eigenvalues, so we conclude that

$$\bar{T}(\alpha x) = 0 \ \forall x \in \mathcal{O}_K/\langle p \rangle$$

Therefore, the bilinear form $\bar{T}$ is degenerate.

Combine the first and second paragraph, we conclude that

$$p|\mathcal{D}_K \iff p \text{ ramifies in } K$$

□

## 15.3 Application in a quadratic field

In this subsection we are going to deduce some properties of the factorisation of primes in a quadratic field, when $[K : \mathbb{Q}] = 2$. The decomposition number is then 1 or 2.

If $g = 2$ then we have

$$e_1 f_1 + e_2 f_2 = 2$$

so that

$$e_1 = e_2 = f_1 = f_2 = 1$$

If $g = 1$ then $e_1 f_1 = 2$. So we have

$$e_1 = 2, f_1 = 1 \text{ or } e_1 = 1, f_1 = 2$$

Then we have three cases in total. So we may get the factorisation of $\langle p \rangle$ in one of the following forms:

(i)
$$\langle p \rangle = P_1 P_2, N(P_1) = N(P_2) = p, P_1 \neq P_2$$

(ii)
$$\langle p \rangle = P^2, N(P) = p$$

(iii)
$$\langle p \rangle = P, N(P) = p^2$$

The next theorem gives a necessary and sufficient condisions for each of (i),(ii) and (iii) to occur, using Legendre symbol.

**Theorem 15.12.** *Let $K$ be a quadratic field so that we may write $K = \mathbb{Q}(\sqrt{m})$ for some square free integer $m$. Let $p$ be a prime number. Then we have the following conclusions. When $p > 2$,*

*(i) if $(\frac{m}{p}) = 1$, then $\langle p \rangle = P_1 P_2$, where $P_1$ and $P_2$ are prime.*

*(ii) if $p|m$, then $\langle p \rangle = P^2$, where $P$ is prime.*

*(iii) if $(\frac{m}{p}) = -1$, then $\langle p \rangle = P$, where $P$ is prime.*

*When $p = 2$,*

*(i) if $m \equiv 1 \pmod 8$, then $\langle 2 \rangle = P_1 P_2$ where $P_1$ and $P_2$ are prime.*

*(ii) if $m \equiv 2$ or $3 \pmod 4$, then $\langle 2 \rangle = P^2$ where $P$ is prime.*

*(iii) if $m \equiv 5 \pmod 8$, then $\langle 2 \rangle = P$ where $P$ is prime.*

*Proof.* When $p > 2$,

(i) if $(\frac{m}{p}) = 1$, then there exists $a$ such that $a^2 \equiv m \pmod p$, and $p \nmid a$ because $p \nmid m$. Consider the ideals

$$P_1 = \langle p, a + \sqrt{m} \rangle, P_2 = \langle p, a - \sqrt{m} \rangle$$

Then

$$P_1 P_2 = \langle p \rangle \langle p, a + \sqrt{m}, a - \sqrt{m}, \frac{a^2 - m}{p} \rangle = \langle p \rangle$$

because $a^2 - m$ is divisible by $p$, and also $(2a, p) = 1$, so the second ideal in the product above is $\mathcal{O}_K$. Also $P_1 \neq P_2$ because if so then $2a \in P_1$ and $p \in P_1$ then $P_1 = \langle 1 \rangle$, which is a contradiction.

(ii) if $p|m$, then $p|\mathcal{D}_K$ and so by Theorem 15.11, $p$ ramifies in $K$ so $p = \langle P\rangle^2$. We can write out explicitly the factorisation. Consider the ideal

$$P = \langle p, \sqrt{m}\rangle$$

Then

$$P^2 = \langle p\rangle\langle p, \sqrt{m}, \frac{m}{p}\rangle$$

Since $m$ is square free so $(p, \frac{m}{p}) = 1$ and so the second ideal in the product above is $\mathcal{O}_K$.

(iii) if $(\frac{m}{p}) = -1$, suppose $\langle p\rangle$ is not prime. Then let $P$ be a prime ideal, $P \neq \langle p\rangle$ and $P|\langle p\rangle$. Then since $N(p) = p^2$, we must have $N(P) = p$. Then it is easy to check that

$$\{P, 1 + P, \ldots, p - 1 + P\} \cong \mathbb{Z}/p\mathbb{Z}$$

is the field $\mathcal{O}_K/P$. Since $\sqrt{m} \in \mathcal{O}_K$, so there exists $a \in \{0, 1, \ldots, p - 1\}$ such that

$$\sqrt{m} \equiv a \pmod{P} \Rightarrow m \equiv a^2 \pmod{P}$$

Thus, by Proposition 15.4, we have

$$m \equiv a^2 \pmod{p}$$

which is a contradiction. Hence $\langle p\rangle$ is a prime.

When $p = 2$,

(i) if $m \equiv 1 \pmod 8$, then $\frac{1+\sqrt{m}}{2} \in \mathcal{O}_K$, so we consider the two ideals

$$P_1 = \langle 2, \frac{1 + \sqrt{m}}{2}\ rangle, P_2 = \langle 2, \frac{1 - \sqrt{m}}{2}\rangle$$

Then

$$P_1P_2 = \langle 2\rangle\langle 2, \frac{1 + \sqrt{m}}{2}, \frac{1 - \sqrt{m}}{2}, \frac{1 - m}{8}\rangle$$

Is is clear that $\frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} = 1$ and so the second ideal in the above product is $\mathcal{O}_K$. So

$$P_1P_2 = \langle 2\rangle$$

Also $P_1 \neq P_2$, because if $P_1 = P_2$, then $1 \in P_1$, which is a contradiction.

(ii) if $m \equiv 2$ or $3 \pmod 4$, then $\mathcal{D}_K = 4m$ and since $2|4m$ so 2 ramifies in $K$. To be more precise, if $m \equiv 2 \pmod 4$, then we consider the ideal

$$P = \langle 2, \sqrt{m}\rangle$$

Then

$$P^2 = \langle 2\rangle\langle 2, \sqrt{m}, \frac{m^2}{4}\rangle$$

Since $m \equiv 2 \pmod 4$ so $\frac{m^2}{4}$ is odd and hence the second ideal in the product above is $\mathcal{O}_K$ and so $P^2 = \langle 2\rangle$.
If $m \equiv 3 \pmod 4$, then we consider the ideal

$$P = \langle 2, 1 + \sqrt{m}\rangle$$

Then

$$P^2 = \langle 2 \rangle \langle 2, 1 + \sqrt{m}, \sqrt{m} + \frac{1+m}{2} \rangle$$

Since $m \equiv 3 \pmod 4$ so $\frac{1+m}{2}$ is even and since

$$(m-1) = \sqrt{m} + \frac{1+m}{2} - (1 + \sqrt{m})$$

is odd and lies in the second ideal in the product above, so it is $\mathcal{O}_K$ and

$$P^2 = \langle 2 \rangle$$

(iii) if $m \equiv 5 \pmod 8$. Suppose $\langle 2 \rangle$ is not prime, and let $P_1$ be a prime ideal which divides $\langle 2 \rangle$ and $N(P) = 2$. So $\mathcal{O}_K / P = \{P, 1 + P\}$. Since $m \equiv 1 \pmod 4$, so $\frac{1+\sqrt{m}}{2} \in \mathcal{O}_K$, then there exists $a = 0, 1$ such that

$$\frac{1 + \sqrt{m}}{2} \equiv a \pmod P$$

and

$$\frac{1 - \sqrt{m}}{2} = 1 - \frac{1 + \sqrt{m}}{2} \equiv 1 - a \pmod P$$

So

$$\frac{1-m}{4} \equiv a(1-a) \pmod P$$

and so by Proposition 15.4, and $a = 0$ or $1$, we have

$$\frac{1-m}{4} \equiv 0 \pmod 2$$

which is a contradiction because $m \equiv 5 \pmod 8$ and so $\frac{1-m}{4}$ is odd.

□

Thus from the proof we can also conclude that:

$$\langle 2 \rangle = \begin{cases} \langle 2 \rangle & \text{if } m \equiv 5 \pmod 8 \\ \langle 2, \frac{1}{2}(1 + \sqrt{m}) \rangle \langle 2, \frac{1}{2}(1 - \sqrt{m}) \rangle & \text{if } m \equiv 1 \pmod 8 \\ \langle 2, 1 + \sqrt{m} \rangle^2 & \text{if } m \equiv 3 \pmod 4 \\ \langle 2, \sqrt{m} \rangle^2 & \text{if } m \equiv 2 \pmod 4 \end{cases}$$

and for $p > 2$,

$$\langle p \rangle = \begin{cases} \langle p \rangle & \text{if } \left(\frac{m}{p}\right) = -1 \\ \langle p, x + \sqrt{m} \rangle \langle p, x - \sqrt{m} \rangle & \text{if } \left(\frac{m}{p}\right) = 1 \text{ and } x^2 \equiv m \pmod p \\ \langle p, \sqrt{m} \rangle^2 & \text{if } p | m \end{cases}$$

Further, we say $\langle p \rangle$ splits if $\langle p \rangle = P_1 P_2$ for different prime ideals $P_1, P_2$, and use Kronecker symbol (Definition 4.17) we have

**Corollary 15.13.** *Let $K$ be a number field. Let $d = \mathcal{D}_K$ and $p$ be a prime number. Then*

*(i) $\langle p \rangle$ splits if and only if $(\frac{d}{p}) = 1$.*

*(ii) $\langle p \rangle$ ramifies if and only if $(\frac{d}{p}) = 0$.*

*(iii)* $\langle p\rangle$ *is a prime if and only if* $(\frac{d}{p}) = -1$.

The proof is just a restatement of Theorem 15.12 using Kronecker symbol.

Now if $K$ is a quadratic field, then let $\sigma$ be the generator of the automorphism group. We write $\bar{\alpha} = \sigma(\alpha)$ for all $\alpha \in K$. In other words, if $K = \mathbb{Q}(\sqrt{m})$ then $\sqrt{\bar{m}} = -\sqrt{m}$ and $\bar{q} = \sigma(q) = q$ for all $q \in \mathbb{Q}$. For any ideal $I = \langle \alpha_1, \ldots, \alpha_n\rangle$, we write

$$\bar{I} = \langle \bar{\alpha}_1, \ldots, \bar{\alpha}_n\rangle$$

It is clear that for any ideals $I$ and $J$, since $\sigma$ is a homomorphism, so

$$\overline{IJ} = \bar{I}\bar{J}$$

The next proposition gives another expression for the norm of ideal in quadratic field.

**Proposition 15.14.** *Let* $K$ *be a quadratic field. Let* $I$ *be a ideal of* $\mathcal{O}_K$. *Then*

$$\langle N(I)\rangle = I\bar{I}$$

*Proof.* This is clear if $I$ is zero or $\mathcal{O}_K$. If not, we have

$$I = \prod_{i=1}^{m} P_i^{a_i}\bar{P}_i^{b_i}\prod_{j=1}^{n} Q_j^{c_j}\prod_{k=1}^{l} R_k^{d_k}$$

where $P_i, Q_j, R_k$ are pairwise distinct prime ideals. Also by Theorem 15.12, we know that each prime ideal which contains a prime number is one of the three following types:

(i) $P_i\bar{P}_i = \langle p_i\rangle$ where $p_i$ is a prime number in $P_i$ and $P_i \neq \bar{P}_i$.

(ii) $Q_j^2 = \langle q_j\rangle$ where $q_j$ is a prime number in $Q_j$ and $Q_j = \bar{Q}_j$.

(iii) $R_k = \langle r_k\rangle$ where $r_k$ is a prime number in $R_k$ and $R_j = \bar{R}_k$.

Then since $\bar{\bar{I}} = I$, for all $I$, we have

$$\bar{I} = \prod_{i=1}^{m} P_i^{b_i}\sigma(P)_i^{a_i})\prod_{j=1}^{n} Q_j^{c_j}\prod_{k=1}^{l} R_k^{d_k}$$

and so

$$I\bar{I} = \langle\prod_{i=1}^{m} p_i^{a_i+b_i}\prod_{j=1}^{n} q_j^{c_j}\prod_{k=1}^{l} r_k^{2d_k}\rangle$$

Now we consider the norm, the norm of $P_i$ is $p_i$, the norm of $Q_j$ is $q_j$ and the norm of $R_k$ is $r_k^2$. Hence

$$N(I) = \prod_{i=1}^{m} p_i^{a_i+b_i}\prod_{j=1}^{n} q_j^{c_j}\prod_{k=1}^{l} r_k^{2d_k}$$

and the result follows. □

Now since $\bar{\bar{I}} = I$ so we also have

$$\langle N(\bar{I})\rangle = I\bar{I}$$

by Proposition 15.14, and so $N(I) = uN(\bar{I})$ for some $u \in \mathcal{O}_K$ which is a unit. But since $N(I), N(\bar{I})$ are both positive integers, so $u = 1$, and so

$$N(I) = N(\bar{I})$$

**Definition 15.15.** *Let* $K$ *be a quadratic field. We say an ideal* $I$ *is* **self-conjugate** *if* $I = \bar{(I)}$.

## 15.4 Kummer-Dedekind theorem

We shall prove a very important result concerning the factorisation of prime numbers in a number field $K$ such that the ring of integer $\mathcal{O}_K$ has a power basis (In other words, $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$.) It was originally proved by Dedekind in 1878, and is known as Kummer-Dedekind Theorem.

**Theorem 15.16. [Kummer-Dedekind]** *Let $K = \mathbb{Q}(\theta)$ be a number field of degree $n$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let $p$ be a prime number. Let*

$$f(x) = min_{\mathbb{Q},\theta}(x)$$

*and $\bar{f(x)}$ be the reduction of $f(x)$ modulo $p$. Let*

$$\bar{f}(x) = \prod_{i=1}^{r} g_i(x)^{e_i}$$

*where $g_1(x), \ldots, g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ and $e_1, \ldots, e_r$ are positive integers. For each $i$, let $f_i(x)$ be any monic polynomial of $\mathbb{Z}[x]$ such that $\bar{f_i(x)} = g_i(x)$. Now set*

$$P_i = \langle p, f_i(\theta) \rangle$$

*for each $i$. Then*

$$\langle p \rangle = \prod_{i=1}^{r} P_i^{e_i}$$

*and $N(P_i) = p^{\deg f_i}$ for each $i$.*

*Proof.* For each $i$, let $\theta_i$ be a root of $g_i$ in some suitable extension of $\mathbb{F}_p$. Then since $g_i$ is irreducible, we have

$$\mathbb{F}_p[\theta_i] \cong \mathbb{F}_p[x]/\langle g_i(x) \rangle$$

and since $g_i(x)$ is irreducible, hence maximal and so $\mathbb{F}_p[\theta_i]$ is a field for each $i$. Now define the map:

$$\phi_i : \mathbb{Z}[\theta] \longmapsto \mathbb{F}_p[\theta_i]$$

by

$$\phi_i(h(\theta)) = \bar{h}(\theta_i)$$

Then it is clear that $\phi_i(\theta) = \theta_i$ and so the map is surjective, and so

$$\mathcal{O}_K / \ker(\phi_i) = \mathbb{Z}[\theta] / \ker(\phi_i) \cong \mathbb{F}_p[\theta_i]$$

is a field. So we conclude that $\ker(\phi_i)$ is a maximal and hence prime ideal in $\mathcal{O}_K$.

Next, we show that the kernel of $\phi_i$ is

$$P_i = \langle p, f_i(\theta) \rangle$$

It is clear that

$$\phi_i(p) = 0 \text{ and } \phi_i(f_i(\theta)) = \bar{f}_i(\theta_i) = g_i(\theta) = 0$$

and so $P_i \subseteq \ker(\phi_i)$.

Conversely, let $g(\theta) \in \ker(\phi_i)$, then

$$\phi_i(g(\theta)) = \bar{g}(\theta_i) = 0$$

Then since $g_i$ is the minimal polynomial of $\theta_i$ in $\mathbb{F}_p[x]$, then we have $g_i(x) | \bar{g}(x)$ in $\mathbb{F}_p[x]$ and so we have

$$\bar{g}(x) = \bar{f}_i(x)\bar{h_i}(x) \text{ for some } \bar{h} \in \mathbb{F}_p[x]$$

Therefore, $g(x) - f_i(x)h_i(x)$ is divisible by $p$. Hence,

$$g(\theta) = (g(\theta) - f_i(\theta)h_i(\theta)) + f_i(\theta)h_i(\theta) \in \langle p, f_i(\theta)\rangle$$

This proves that

$$\ker(\phi_i) = \langle p, f_i(\theta)\rangle = P_i$$

and hence $P_i$ is prime for each $i$.

Then we show $P_i \neq P_j$ if $i \neq j$. Suppose $P_i = P_j$, then we have $g(\theta), h(\theta) \in \mathbb{Z}[\theta]$ such that

$$f_i(\theta) = g(\theta)p + h(\theta)f_j(\theta)$$

Apply $\phi_j$, so we have

$$g_i(\theta_j) = \bar{h}(\theta_j)g_j(\theta_j) = 0$$

Since $g_j$ is the minimal polynomial of $\theta_j$ in $\mathbb{F}_p[x]$, so $g_j(x)|g_i(x)$. But $g_i(x)$ is irreducible and monic, so $g_i = g_j$ and so $i = j$.

We now show that

$$\langle p\rangle = \prod_{i=1}^{r} P_i^{e_i}$$

It is clear that

$$\begin{aligned}
\prod_{i=1}^{r} P_i^{e_i} &= \prod_{i=1}^{r} \langle p, f_i(\theta)\rangle^{e_i} \\
&= \prod_{i=1}^{r} (\langle p\rangle + \langle f_i(\theta)\rangle)^{e_i} \\
&\subseteq \langle p\rangle + \prod_{i=1}^{r} \langle f_i(\theta)\rangle^{e_i} \\
&= \langle p\rangle + \langle f(\theta)\rangle \\
&= \langle p\rangle
\end{aligned}$$

because for any ideals $A, B_1$ and $B_2$, we have

$$(A + B_1)(A + B_2) \subseteq A + B_1B_2$$

and $f(\theta) = 0$. So we have

$$\langle p\rangle \Big| \prod_{i=1}^{r} P_i^{e_i}$$

Now it is clear that $p \in P_i$ for each $i$ and so $P_i|\langle p\rangle$. So we write

$$\langle p\rangle = \prod_{i=1}^{r} P_i^{k_i}$$

where $k_i \in \{1, 2, \ldots, e_i\}, i = 1, 2, \ldots, r$.

Now we consider that

$$\mathcal{O}_K/P_i = \mathbb{Z}[\theta]/P_i \cong \mathbb{F}_p[\theta_i]$$

so that

$$N(P_i) = card(\mathcal{O}_K/P_i) = card(\mathbb{F}_p[\theta_i]) = p^{\deg g_i}$$

Hence we have

$$p^n = N(\langle p\rangle) = \prod_{i=1}^{r} N(P_i)^{k_i} = p^{\sum_{i=1}^{r} \deg g_i k_i}$$

and so

$$n = \sum_{i=1}^{r} k_i \deg g_i$$

But since $[K : \mathbb{Q}] = n = \deg f = \deg \bar{f}$, and

$$\bar{f}(x) = \prod_{i=1}^{r} g_i^{e_i}$$

Comparing the degree on both sides, we have

$$n = \sum_{i=1}^{r} e_i \deg g_i$$

Hence

$$\sum_{i=1}^{r} e_i \deg g_i = \sum_{i=1}^{r} k_i \deg g_i$$

and since $k_i \leq e_i$ for each $i$, so we conclude that

$$e_i = k_i$$

for each $i$. Therefore,

$$\langle p \rangle = \prod_{i=1}^{r} P_i^{e_i}$$

and

$$N(P_i) = p^{\deg g_i} = p^{\deg f_i}$$

□

The assumption that $\mathcal{O}_K$ has a power basis is essential in this theorem.

## 15.5 Generalisation of Kummer-Dedekind theorem

The following is a generalisation of Kummer-Dedekind theorem.

**Theorem 15.17.** *Let $K = \mathbb{Q}(\theta)$ be a number field with $\theta \in \mathcal{O}_K$. Let $p$ be a prime number. Let*

$$f(x) = min_{\mathbb{Q},\theta}(x) \in \mathbb{Z}[x]$$

*Let $\bar{f(x)}$ be the reduction of $f(x)$ modulo $p$ for any $f(x)$. Let*

$$\bar{f}(x) = \prod_{i=1}^{r} g_i^{e_i}$$

*where $g_1(x), \ldots, g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ and $e_1, \ldots, e_r$ are positive integers. For each $i$, let $f_i(x)$ be any monic polynomial of $\mathbb{Z}[x]$ such that $\bar{f}_i(x) = g_i(x)$. Set*

$$P_i = \langle p, f_i(\theta) \rangle$$

*for each $i$. If the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is not 0 modulo $p$, then $P_1, \ldots, P_r$ are distinct prime ideals and*

$$\langle p \rangle = \prod_{i=1}^{r} P_i^{e_i}$$

*and*

$$N(P_i) = p^{\deg f}$$

*for each $i$.*

*Proof.* The proof can be modeled on Theorem 15.16 with slight modification. For simplicity, write

$$A = \mathbb{Z}[\theta], I_i = \langle p, f_i(\theta)\rangle\mathbb{Z}[\theta]$$

In Theorem 15.16, we proved that $I_i$ is a prime ideal for each $i$ and $I_i \neq I_j$ if $i \neq j$. Define the map $\phi$ by:

$$\phi : A \longmapsto \mathcal{O}_K/P_i$$

by $\phi(x) = x \bmod P_i$. This is clear a ring homomorphism and it is clear that $I_i \in \ker(\phi)$. Conversely, suppose $h(\theta) \in \ker(\phi)$, then $h(\theta) = 0 \bmod P_i$. Hence $h(\theta) \in P_i$ and so $h(\theta) \in I_i$ because $I_i \subseteq P_i$.

Also, let $[\mathcal{O}_K : A] = n$, then for any $\alpha \in \mathcal{O}_K$, $n\alpha \in A$. Then since $(n, p) = 1$, so pick $m \in \mathbb{Z}$ such that

$$mn \equiv 1 \pmod{p}$$

Then $m(n\alpha) \in A$ and

$$\phi(m(n\alpha)) = mn\alpha \pmod{P_i}$$

but $mn - 1 \in \langle p\rangle \subseteq P_i$, so $mn\alpha \equiv \alpha \pmod{P_i}$. Hence

$$\phi(m(n\alpha)) = \alpha \pmod{P_i}$$

and so the map is surjective. Therefore, we have

$$A/I_i \cong \mathcal{O}_K/\langle p, f_i(\theta)\rangle$$

and we have proved in Theorem 15.16 that $A/I_i$ is a field, hence $P_i$ is maximal and hence prime in $\mathcal{O}_K$.

Now use the above isomorphism, suppose $P_i = P_j$, then $I_i = I_j$ and so $i = j$ by Theorem 15.6. Finally, the proof of

$$\langle p\rangle \prod_{i=1}^{r} P_i^{k_i}$$

is the same as before. We then use

$$\mathcal{O}_K/P_i \cong A/I_i$$

to conclude that

$$N(P_i) = card(\mathcal{O}_K/P_i) = card(A/I_i) = card(\mathbb{F}_p[\theta_i]) = p^{d_i}$$

where $d_i = \deg g_i = \deg \bar{f}_i$ as in Theorem 15.6. The rest of the proof is then identical to that in Theorem 15.6. □

## 15.6 Exercise

You may assume $\mathcal{D}_K \equiv 1$ or $0 \pmod 4$ for any number field $K$.

1. Factorise $\langle 2\rangle$ into prime ideals in $K = \mathbb{Q}[\sqrt{47}]$.

2. Let $K = \mathbb{Q}(\sqrt{26})$. Factorise the principal ideals

$$\langle 2\rangle, \langle 5\rangle, \langle 6 + \sqrt{26}\rangle$$

3. Let $K = \mathbb{Q}(\sqrt{35})$. Show that

$$\langle 2\rangle = \langle 2, 1 + \sqrt{35}\rangle^2, \langle 5\rangle = \langle 5, \sqrt{35}\rangle^2, \langle 5 + \sqrt{35}\rangle = \langle 2, 1 + \sqrt{35}\rangle\langle 5, \sqrt{35}\rangle$$

4. Let $K = \mathbb{Q}(\sqrt[3]{10})$. Does $\mathcal{O}_K$ has a power basis?

5. Let $K = \mathbb{Q}(\sqrt[3]{3})$.

   (i) Deduce that $\langle 3 \rangle = P^3$, where $P = \langle \sqrt[3]{3} \rangle$ is a prime ideal. Find its norm.

   (ii) Are there any prime numbers $p \neq 3$ such that

   $$\langle p \rangle = Q^3$$

   in $\mathcal{O}_K$ for some prime ideal $Q$?

6. Let $\zeta_m$ be an $m^{th}$ primitive root of 1. Let $K = \mathbb{Q}(\zeta_m)$. Show that $N(\zeta_m) = 1$.

7. Let $K$ be a number field with $[K : \mathbb{Q}] = n$. A prime number $p$ is called **totally ramified** if $\langle p \rangle = P^n$ for some prime ideal $P$.

   (i) Let $K$ be a number field. Show that if a prime number $p$ is ramified in $K$, then it is ramified in all intermediate field $M$.

   (ii) Let $K$ and $L$ be number fields. Suppose that the prime $p$ is totally ramified in $\mathcal{O}_K$ and unramified in $\mathcal{O}_L$. Prove that $K \cap L = \mathbb{Q}$.

8. Let $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta - 1 = 0$. Prove that

   $$\sqrt{\theta} \notin \mathbb{Q}(\theta)$$

9. (i) Let $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta + 4 = 0$. Show that the ideal $I = \langle 2, \theta \rangle$ is principal in $\mathcal{O}_K$ and is generated by $\theta + 2$.

   (ii) Hence or otherwise, show that the norm $N(2 + \theta) = 2$ or $-2$.

10. In this question, we are going to deduce prove that the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$ for all $p$ odd prime. Let $\pi = 1 - \zeta_p$.

    (i) By considering traces $Tr_{K/Q}(\zeta_p^j \alpha)$ show that $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}[\zeta_p]$.

    (ii) Show that $(1 - \zeta_p^r)/(1 - \zeta_p^s)$ is a unit for all $r, s \in \mathbb{Z}$ coprime to $p$, and that $\pi^{p-1} = up$ where $u$ is a unit.

    (iii) Prove that the natural map $\mathbb{Z} \to \mathcal{O}_K/\langle \pi \rangle$ is surjective. Deduce that for any $\alpha \in \mathcal{O}_K$ and $m \geq 1$ there exist $a_0, \ldots, a_{m-1} \in \mathbb{Z}$ such that

    $$\alpha \equiv a_0 + a_1\pi + \ldots + a_{m-1}\pi^{m-1} \ (\mathrm{mod}\pi^m \mathcal{O}_K).$$

    (iv) Deduce that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

* 11. In this question, we are going to prove the polynomial version of Fermat's Last Theorem. No knowledge in deep algebraic number theory is required.

    Let $n \geq 3$ be an integer. Suppose $f, g, h \in \mathbb{C}[X]$ are coprime polynomial satisfying $f^n + g^n = h^n$. Use unique factorisation in $\mathbb{C}[X]$ to construct a new solution to this equation involving polynomials of smaller degree. Deduce that $f, g, h$ must be constant.

12. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Describe the ring $\mathcal{O}_K/2\mathcal{O}_K$ as explicitly as you can. Show that $\mathbb{Z}[\sqrt{d}]^* \subset \mathcal{O}_K^*$ has index 1 or 3.

13. Let $K = \mathbb{Q}(\zeta_{p^2})$ where $p$ is an odd prime number. Prove there is a unique subfield $F$ of $K$ such that $[F : \mathbb{Q}] = p$. Prove that 2 splits completely in $F$ if and only if

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

(You may assume that for a Galois extension, the ramification degree and residue degree between different prime ideals above are the same. We will prove this in later sections.)

## 15.7 Hint and Solutions

1. $47 \equiv 3 \bmod 4$ and so by the remark following Theorem 15.12, we have

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{47} \rangle^2$$

2. It is clear that, since $26 \equiv 2 \pmod 4$,

$$\langle 2 \rangle = \langle 2, \sqrt{26} \rangle^2$$

and since $(\frac{26}{5}) = 1$, and $1^2 = 26 \pmod 5$, so

$$\langle 5 \rangle = \langle 5, 1 + \sqrt{26} \rangle \langle 5, 1 - \sqrt{26} \rangle$$

Now clearly, that $6 + \sqrt{26} \in \langle 2, \sqrt{26} \rangle, \langle 5, 1 + \sqrt{26} \rangle$, and it is clear that these two are different ideals since they contains different primes. (By Lemma 15.1, the prime is unique.) Now $N(6 + \sqrt{26}) = (6 + \sqrt{26})(6 - \sqrt{26}) = 10$ and so by consider the norm, we conclude that

$$\langle 6 + \sqrt{26} \rangle = \langle 2, \sqrt{26} \rangle \langle 5, 1 + \sqrt{26} \rangle$$

3. Using the same method, we have

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{35} \rangle^2$$

$$\langle 5 \rangle = \langle 5, \sqrt{35} \rangle^2$$

because $35 \equiv 3 \pmod 4$ and $5|35$.

Now clearly $5 + \sqrt{35} \in \langle 2, 1 + \sqrt{35} \rangle, \langle 5, \sqrt{35} \rangle$. $N(\langle 5 + \sqrt{35} \rangle) = 10$ and so by considering the norm, we conclude that

$$\langle 5 + \sqrt{35} \rangle = \langle 2, 1 + \sqrt{35} \rangle \langle 5, \sqrt{35} \rangle$$

4. Let $\theta = \sqrt[3]{3}$, and so the discriminant of $\mathbb{Z}[\theta]$ is $-2700$. Now, we have:

$$\langle 2, \theta \rangle^3 = \langle 2 \rangle \langle 4, 2\theta, \theta^2, 5 \rangle = \langle 2 \rangle$$

$$\langle 5, \theta \rangle^3 = \langle 5 \rangle \langle 25, 5\theta, \theta^2, 2 \rangle = \langle 5 \rangle$$

$$\langle 3, \theta - 1 \rangle^3 = \langle 3 \rangle \langle 9, \theta^2 - 2\theta + 1, 3\theta - 3, 3 - \theta^2 - \theta \rangle = \langle 3 \rangle$$

Hence, 2, 3 and 5 ramify in $K$ and so by Theorem 15.11, $2, 3, 5 | \mathcal{D}_K$. Since $diss(\mathbb{Z}[\theta]) = -2700$, so the only possible discriminant of $\mathcal{O}_K$ is $-2700$ or $-300$ because $2, 3, 5 | \mathcal{D}_K$. In either case, for any $\alpha \in \mathcal{O}_K$, we have $3\alpha \in \mathbb{Z}[\theta]$ because the index of $\mathbb{Z}[\theta]$ is either 1 or 3. If the index is 3, then for any $\alpha \in \mathcal{O}_K$, we have $3\alpha \in \mathbb{Z}[\theta]$, and so we may write

$$\alpha = a + b\theta + c\theta^2$$

where $a, b, c \in \frac{1}{3}\mathbb{Z}$. But 3 is a prime, and the index is the product of denominators of $a, b$ and $c$. Hence two of $a, b$ and $c$ must be integers and only one of them could possibly take the denominator 3. But none of the following is an algebraic integer:

$$\frac{1}{3}, \frac{2}{3}, \frac{1}{3}\theta, \frac{2}{3}\theta, \frac{1}{3}\theta^2, \frac{2}{3}\theta^2$$

So the index cannot be 3 and so is 1.

5. (i) Let $\theta = \sqrt[3]{3}$, Consider the ideal

$$P = \langle 3, \theta \rangle$$

then

$$P^3 = \langle 3 \rangle \langle 9, 3\theta, \theta^2, 1 \rangle = \langle 3 \rangle$$

and so $N(P)^3 = N(3) = 27$. Then $N(P) = 3$ and so $P$ is a prime ideal.

(ii) $p$ ramifies if and only if $p|\mathcal{D}_K$. So if

$$\langle p \rangle = Q^3$$

then $p|\mathcal{D}_K$. Since $\mathbb{Z}[\sqrt[3]{3}] \subseteq \mathcal{O}_K$, so we conclude that $p|disc(\mathbb{Z}[\sqrt[3]{3}]) = -81$. Then $p = 3$ since $p$ is a prime. Hence there does not exist any other such prime numbers.

6. By definition,

$$N(\zeta_m) = \prod_{i=1}^{\phi}(m)\phi_i(\zeta_m) = \prod_{(j,m)=1} e^{\frac{2\pi i}{m}j}$$

Consider now the sum

$$\sum_{(j,m)=1} j$$

It is clear that $(j, m) = 1$ if and only if $(m - j, j) = 1$. Therefore, we can pair $j$ and $m - j$ in the sum, so

$$m| \sum_{(j,m)=1} j$$

and hence

$$N(\zeta_m) = e^{\sum_{(j,m)=1} j\frac{2\pi i}{m}} = 1$$

7. (i) Let $[K : \mathbb{Q}] = n$ and so

$$\langle p \rangle \mathcal{O}_K = P^n$$

where $P$ is a prime ideal in $\mathcal{O}_K$. Let $M$ be an intermediate field and let $[M : \mathbb{Q}] = m$. Suppose there are distinct prime ideals $Q$ and $R$ in $\mathcal{O}_M$ which contains $P$. Then let $Q'$ and $R'$ be any ideals in $\mathcal{O}_K$ such that

$$Q' \cap \mathcal{O}_M = Q, R' \cap \mathcal{O}_M = R$$

Then it is clear that $Q', R'$ both divide $\langle p \rangle$ and they are coprime. Indeed, if not, then there exists $P' \supseteq Q', R'$. Hence $P \cap \mathcal{O}_M \supseteq Q, R$. Therefore, $Q$ and $R$ are not coprime, which is a contradiction. So this shows that if there are two prime ideals containing $p$ in $\mathcal{O}_M$, then there are at least two prime ideals containing $p$ in $\mathcal{O}_K$. Since $p$ is totally ramified in $\mathcal{O}_K$, so there is only one prime ideal containing $p$ in $\mathcal{O}_M$. Then we have

$$\langle p \rangle = Q^t$$

for some prime ideal $t$. Then we show $N(Q) = p$ and so that

$$\langle p \rangle = Q^m$$

Indeed, the homomorphism

$$f : \mathcal{O}_M/Q \longmapsto \mathcal{O}_K/P$$

by $f(a+Q) = a+P$ is clearly an injection. But both of them are fields, and $card(\mathcal{O}_K/P) = N(P) = p$ which is the base field of characteristic $p$. Therefore, $N(Q) = card(\mathcal{O}_M/Q) = p$.

(ii) Let $M = K \cap L$. Since $\langle p \rangle$ is totally ramified in $K$, so it is totally ramified in $M$ by (i) and let $[M : \mathbb{Q}] = n$ so

$$\langle p \rangle O_M = P^n$$

Then the factorisation of $\langle p \rangle$ in $O_L$ is:

$$\langle p \rangle O_M = (P\mathcal{O}_L)^n$$

But whatever the factorisation of $P\mathcal{O}_L$ is, each prime factor must has index $n$ (or at least $n$) and $\langle p \rangle$ is unramified in $O_L$. This shows that $n$ must be 1 and so

$$M = \mathbb{Q}$$

8. $disc(\mathbb{Z}[\theta]) = -4a^3 - 27b^2 = -23$ which is square free and so we conclude that

$$\mathbb{Z}[\theta] = \mathcal{O}_K$$

Suppose $\sqrt{\theta} \in \mathbb{Q}(\theta)$, then $\sqrt{\theta} \in \mathcal{O}_K$, because clearly it satisfies $x^6 - x^2 - 1 = 0$. Thus, there exist $a, b$ and $c \in \mathbb{Z}$ such that

$$\sqrt{\theta} = a + b\theta + c\theta^2$$

which gives

$$c^2\theta^4 + 2bc\theta^3 + (b^2 + 2ac)\theta^2 + (2ab - 1)\theta + a^2 = 0$$

Use $\theta^3 = \theta - 1$ we have

$$(b^2 + 2ac + c^2)\theta^2 + (2ab + 2bc - 2)\theta + a^2 - 2bc = 0$$

This polynomial must be identically zero, otherwise it contradicts that the minimal polynomial of $\theta$ has degree 3. So

$$b^2 + 2ac + c^2, ab + bc - 1, a^2 - 2bc = 0$$

But $ab + bc - 1 = 0 \Rightarrow (a + c)b = 1$ and since $a, b, c$ are all integers. So $b = \pm 1$. If $b = 1$, then $a + c = 1$ and $a^2 = 2c$, which gives

$$c^2 - 4c + 1 = 0$$

which has no integer solution. If $b = -1$, then $a + c = -1$ and $a^2 = -2c$, so $c^2 + 4c + 1 = 0$ which again has no integer solution. Therefore, the assumption is not true and we conclude that $\sqrt{\theta} \notin \mathbb{Q}(\theta)$.

9. (i) $disc(\mathbb{Z}[\theta]) = -4a^3 - 27b^2 = -104 = -2^2 26$. But $\mathcal{D}_K \equiv 1$ or $0 \pmod 4$, so it cannot be $-26$. Thus, $\mathcal{D}_K = -104$ and $\mathcal{O}_K = \mathbb{Z}[\theta]$. Then consider the element $2 + \theta \in \mathcal{O}_K$. We have

$$(2 + \theta)(\theta^2 - 2\theta + 3) = \theta^3 - \theta + 6 = 2$$

and hence 2 and $\theta \in \langle 2 + \theta \rangle$. Therefore,

$$\langle 2, \theta \rangle = \langle 2 + \theta \rangle$$

(ii) By Kummer-Dedekind, we have

$$\langle 2\rangle = \langle 2, \theta\rangle\langle 2, \theta - 1\rangle^2$$

and so $N(\langle 2, \theta\rangle) = 2$. Thus $N(\langle 2 + \theta\rangle) = \pm 2$.

10. (i) The trace of $\zeta_p^k$ is $-1$ for any $k = 1, 2, \ldots, p-1$. By writing $\alpha$ as $a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}$ we conclude that the trace is given by

$$(p-1)a_0 - \sum_{i=1}^{p-2} a_i, j = 0; -\sum_{i=0}^{p-2} a_i, j = 1; (p-1)a_{p-j} - \sum_{i\neq j} a_i, j \geq 2.$$

By taking the difference between the case $j = 1$ and any other case we conclude that $pa_i \in \mathbb{Z}$ for all $i$.

(ii) Since $r, s$ are both coprime to $p$ so there exists $n$ such that

$$r \equiv sn \ (\mathrm{mod} p).$$

Thus $(1 - \zeta_p^r)/(1 - \zeta_p^s) = (1 - \zeta_p^{sn})/(1 - \zeta_p^s)$ and this can be written as

$$1 + \zeta_p^s + \zeta_p^{2s} + \ldots + \zeta_p^{(n-1)s}$$

which is in $\mathbb{Z}[\zeta]$ so the given term is a unit.
By multiplying and dividing the same thing we conclude that

$$\pi^{p-1} = \prod_{i=1}^{p-1}(1 - \zeta_p^i)\dot{\prod}_{j=2}^{p-1}\frac{1 - \zeta_p}{1 - \zeta_p^j}.$$

The second term is a unit by above and the first term is $p$ by evaluating the cyclotomic polynomial at 1.

(iii) It is easy to check that the norm of $\pi$ is $p$ and so $\mathcal{O}_K/\langle\pi\rangle$ contains $p$ elements. To prove it is surjective, it suffices to prove that the image of $\{1, \ldots, p\}$ are different. Indeed, if any two give the same image then the difference lies in $\langle\pi\rangle$. But $\langle\pi\rangle$ is an ideal above $p$ so the smallest rational integer in $\pi$ is $p$.
Thus, for each $\alpha$ there exists some integer $a_0$ such that $\alpha \equiv a_0 \bmod \pi$ and so we have $\alpha_1$ so that

$$\alpha = a_0 + \alpha_1\pi.$$

Repeat this for $\alpha_1$ we conclude that $\alpha = a_0 + a_1\pi + \alpha_2$ for some $\alpha_2$. Now repeat this.

(iv) Take $m$ to be $p - 1$ in the previous part and use the fact from (ii) that $\pi^{p-1}\mathcal{O}_K = p\mathcal{O}_K$. So for each $\alpha \in \mathcal{O}_K$ we have integers $a_i$ such that

$$\alpha = a_0 + a_1\pi + \ldots + a_{p-2}\pi^{p-2} + p\beta, \text{ for some } \beta \in \mathcal{O}_K.$$

By (i) we know that $\beta \in \frac{1}{p}\mathbb{Z}[\zeta_p]$ and so $p\beta \in \mathbb{Z}[\zeta_p]$. Therefore, $\alpha \in \mathbb{Z}[\zeta_p]$ and so the result follows.

11. WLOG we may assume that $f, g, h$ have no common factors. Rearrange the equation so that

$$g^n = (f - h)(f - \zeta h)\cdots(f - \zeta^{n-1}h).$$

For $i \neq j$, $f - \zeta^i h$ and $f - \zeta^j h$ are coprime because if not then by taking differences etc. we see that the common factor must also divides $f$ and $h$, and hence $g$. Thus by unique factorisation we must have that for each $i$,

$$f - \zeta^i h = c_i^n, i = 0, 1, \ldots, n-1.$$

Since $n \geq 3$ we take the first three and use the first two to calculate $f, h$ which are given by

$$f = \frac{c_1^n - \zeta c_0^n}{1-\zeta}, h = \frac{c_1^n - c_0^n}{1-\zeta}.$$

Then substitute this into the equation for $i = 2$ we have

$$(1+\zeta)c_1^n - \zeta c_0^n = c_2^n.$$

Now over $\mathbb{C}$ the constants are again $n-th$ power and so we can absorb the constant in $c_i$ and so we have got a new equation

$$c_1'^n + c_0'^n = c_2^n.$$

If $f, h$ are not constant, then at most one of $c_0, c_1$ or $c_2$ is constant and the others have degree strictly less than the degree of $g$. But the degree of $g$ is finite and if we repeat the above we can reduce the degree infinitely many times, which gives a contradiction and hence $f, h$ are both constant.

12. Note $N(\langle 2 \rangle) = 4$ and the additive group structure of $\mathcal{O}_K/2\mathcal{O}_K$ is $C_2 \times C_2$ (because $2x \in \langle 2 \rangle$ for any $x \in \mathcal{O}_K$) so we consider ring of four elements, say $0, 1, a, b$, with $1+a = b, 1+b = a, a+b = 1$.

When $d \equiv 2, 3 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. In this case the minimal polynomial of $\sqrt{d}$ is $X^2 - d$ and by Kummer-Dedekind, $\langle 2 \rangle = P^2$ for some ideal $P$ above 2. Then we must have some nilpotent element in this ring because if $x \in P$ but $x \notin 2$ then $x^2 \in \langle 2 \rangle$ and so $x^2 = 0$ in $\mathcal{O}_K/2\mathcal{O}_K$. So we may assume that $a^2 = 0$ and then $b^2 = (1+a)^2 = 1 + a^2 = 1$. Also, $ab = a(1+a) = a$. This describes the ring structure of $\mathcal{O}_K/2\mathcal{O}_K$ and we call this $B_4$.

When $d \equiv 1 \bmod 8$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. In this case we consider the polynomial $X^2 - X + \frac{1-d}{4}$ and $\frac{1-d}{4}$ is even. So by Kummer-Dedekind $\langle 2 \rangle = P_2 Q_2$. By question 1 in the second sheet, we have $P_2 + Q_2 = \mathcal{O}_K$ and so we can pick $a, b$ such that $a + b = 1$ with $a \in P_2, b \in Q_2$. Then $ab = 0$ in $\mathcal{O}_K/2\mathcal{O}_K$. Since $a = 1 + b$ so $a^2 = a(1+b) = a$ and similarly $b^2 = b(1+a) = b$. Then

$$0 \mapsto (0,0), 1 \mapsto (1,1), a \mapsto (1,0), b \mapsto (0,1)$$

is an isomorphism between $\mathcal{O}_K/2\mathcal{O}_K$ and $\mathbb{F}_2 \times \mathbb{F}_2$.

When $d \equiv 5 \bmod 8$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. In this case we consider the polynomial $X^2 - X + \frac{1-d}{4}$ and $\frac{1-d}{4}$ is odd. So by Kummer-Dedekind $\langle 2 \rangle$ is a prime ideal and so $\mathcal{O}_K/2\mathcal{O}_K$ is a field. So it must be $\mathbb{F}_4$.

If $d \equiv 2, 3 \bmod 4$ we have $\mathbb{Z}[\sqrt{d}]^\times = \mathcal{O}_K^\times$ and so the index is 1. When $d \equiv 1 \bmod 4$, $2\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$ and so the index of $\mathbb{Z}[\sqrt{d}]^\times \subset \mathcal{O}_K^\times$ divides $(\mathcal{O}_K/2\mathcal{O}_K)^\times$. When $d \equiv 1 \bmod 8$, $(\mathcal{O}_K/2\mathcal{O}_K)^\times = (\mathbb{F}_2 \times \mathbb{F}_2)^\times = \{1\}$. So the index is 1. When $d \equiv 5 \bmod 8$, $(\mathcal{O}_K/2\mathcal{O}_K)^\times = \mathbb{F}_4^\times$ and so the index is either 1 or 3.

Example: we see this can only happen when $d \equiv 5 \bmod 8$. Take $d = 5$. We see $\frac{1+\sqrt{5}}{2}$ is a unit and it is not in $\mathbb{Z}[\sqrt{5}]^\times$ so the index is not equal to 1 and so the index must be 3.

13. The first part is clear by fundamental theorem of Galois as the extension is cyclic of order $p(p-1)$. 2 splits completely in $F$ if and only if the product of ramification and residue degree of 2 in $K$ is at most $p-1$. So it divides $p-1$.

Recall the Galois group of finite field is generated by Frobenius element. Consider $\mathfrak{p}$ a prime above 2 in $K$, and the residue field $\mathcal{O}_K/\mathfrak{p}$. Since we know the residue degree is a factor of $p-1$ then we know that for any element $x$ in the residue field we have $x^{2^{p-1}-1}=1$. Now the reduction of $\zeta_{p^2}$ is an element in the residue field. So we have

$$\zeta_{p^2}^{2^{p-1}-1} \equiv 1 \pmod{\mathfrak{p}}.$$

But $\mathfrak{p}$ is a prime above 2, hence the elements $\zeta_{p^2}^i$, $i$ coprime to $p$ are distinct modulo $\mathfrak{p}$. Hence we must have $\zeta_{p^2}^{2^{p-1}-1}=1$. Since it is a primitive root so we conclude that $p^2$ divides $2^{p-1}-1$.

For the converse, if the congruence relation holds then we know the residue degree is at most $p-1$. Now the degree $[F:\mathbb{Q}]$ is $p$ and so we conclude that either 2 is totally ramified or it splits completely by writing down the usual index equation $p=ref$. One way to do this question is to compute the discriminant of the cyclotomic extension and we see 2 does not divide the discriminant so it cannot ramify. Or we will see later that the only prime which can ramify in $\mathbb{Q}(\zeta_N)$ are those which divide $N$.

# 16 The ideal class group

## 16.1 Basic concept

We have already seen the factorisation of non-zero ideals of a Dedekind domain $D$ Let $K$ be the field of quotient of $D$. The ideals under multiplication form a group $I(K)$. The principal ideal in $D$ has the form $\langle\alpha\rangle = \{r\alpha : r \in D\}$ for some $\alpha \in K\backslash\{0\}$. In particular, the set of principal ideals $P(K)$ in forms a subgroup of the group $I(K)$. Further, since the multiplication is commutative, and so $I(K)$ is an Abelian group. Hence $P(K)$ is a normal subgroup. In this section, we are going to investigate the properties of the quotient group $I(K)/P(K)$.

**Definition 16.1.** *Let $K$ be a number field. Let $I(K)$ be the group of non-zero ideals of $D = \mathcal{O}_K$. Let $P(K)$ be the subgroup of principal ideals of $I(K)$. Then the quotient group $I(K)/P(K)$ is called the* **ideal class group** *of $K$ and is denoted by $Cl(K)$ (or $H(K)$ in some context.)*

We shall see later (with proof) that the ideal class group is always finite.

**Definition 16.2.** *Let $K$ be a number field and $D = \mathcal{O}_K$. The order of the class group $Cl(K)$ (or $H(K)$) is called the* **class number** *of $K$ and is denoted by $h(K)$.*

**Proposition 16.3.** *Let $K$ be a number field. Then $h(K) = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain.*

*Proof.*

$$h(K) = 1 \iff [I(K) : P(K)] = 1 \iff I(K) = P(K)$$

and $I(K) = P(K)$ if and only if every ideal of $\mathcal{O}_K$ is principal, and hence $\mathcal{O}_K$ is a principal ideal domain. □

## 16.2 Minkowski's convex body theorem

In this subsection, we are going to prove Minkowski's theorem from which we can deduce that the ideal class group is finite. We shall begin with some commutative algebra.

**Definition 16.4.** *A subset $H \subseteq V$ is* **discrete** *if for every compact subset $X \subseteq V$, $H \cap X$ is finite.*

In $\mathbb{R}^n$, we shall use the fact that a subset $H$ is compact if and only if it is closed and bounded.

**Lemma 16.5.** *Let $V$ be a $\mathbb{Z}$-module, which is a subset of $\mathbb{R}^n$. Suppose $H \subseteq V$ is a submodule. Then the followings are equivalent:*

1. *$H$ is discrete in $V$.*
2. *$H$ is finitely generated over $\mathbb{Z}$ and some generating set is linearly independent over $\mathbb{R}$.*
3. *$H$ is finitely generated over $\mathbb{Z}$ and every $\mathbb{Z}$-basis is linearly independent over $\mathbb{R}$.*

*Proof.* (a) $1 \Rightarrow 2$: Let $e_1, \ldots, e_r \in H$ be linearly independent over $\mathbb{R}$ with $r$ maximal. It is clear that $r \leq n$. Let $P$ be the set

$$P = \left\{ \sum_{i=1}^{r} a_i e_i : a_i \in [0, 1] \right\}$$

It is clear that $P$ is compact, and $P \cap H$ is finite by assumption.

Take $x \in H$. As $r$ is maximal, so $x = \sum_{i=1}^{r} b_i e_i$, where $b_i \in \mathbb{R}$. Write $b_i = [b_i] + a_i e_i$, where $0 \leq a_i < 1$ and so we have

$$x = \sum_{i=1}^{r} ([b_i] + a_i e_i)$$

Since $H$ is a $\mathbb{Z}$-module, so that $[b_i]e_i \in H$ and $x \in H$ and so $\sum_{i=1}^{r} a_i e_i \in H$, but this is also clearly in $P$ by definition. Hence

$$\sum_{i=1}^{r} a_i e_i \in P \cap H$$

Therefore, $H$ is generated as a $\mathbb{Z}$-module by $e_1, \ldots, e_r$ and $P \cap H$.

For each integer $j$, define

$$x_j = jx - \sum_{i=1}^{r} [jb_i] e_i = \sum_{i=1}^{r} (jb_i - [jb_i])\, e_i \in P$$

But $jx \in H$ and $\sum_{i=1}^{r} [jb_i] e_i \in H$, so $x_j \in H \cap P$. Therefore, there exists $j \neq k$ such that $x_j = x_k$ because $H \cap P$ is finite. Then we have

$$(j-k)b_i = [jb_i] - [kb_i]$$

for each $i$ because $e_1, \ldots, e_r$ are linearly independent. So

$$b_i = \frac{[jb_i] - [kb_i]}{j-k} \in \mathbb{Q}$$

and $b_i$ is independent of $x$. Let $b_i = \frac{B_i}{N}$ where $B_i \in \mathbb{Z}$. Then

$$x = \sum_{i=1}^{r} b_i e_i = \sum_{i=1}^{r} \frac{B_i e_i}{N}$$

So $H$ is a $\mathbb{Z}$ module generated by $\{\frac{e_1}{N}, \ldots, \frac{e_r}{N}\}$ and it is clear that they are linearly independent over $\mathbb{R}$ since $e_1, \ldots, e_r$ are linearly independent.

(b) $2 \Rightarrow 3$: It is clear that $H$ is finitely generated over $\mathbb{Z}$. There is a set $\{e_1, \ldots, e_r\}$ which is a $\mathbb{Z}$-basis for $H$ and is linearly independent over $\mathbb{R}$, then for any $\mathbb{Z}$-basis $\{f_1, \ldots, f_r\}$, write $f_i$ in terms of $e_i$.

$$f_i = \sum_{j=1}^{r} a_{ij} e_j$$

where $a_{ij} \in \mathbb{Z}$. Then suppose

$$\sum_{i=1}^{r} b_i f_i = 0$$

then

$$\sum_{i=1}^{r} b_i \sum j = 1^r a_{ij} e_j = 0$$

But since $e_1, \ldots, e_r$ is linearly independent over $\mathbb{R}$ so we have

$$\sum_{i=1}^{r} b_i a_{ij} = 0$$

for each $j$. But the matrix $A_{ij} = a_{ij}$ is invertible since we can also write $e_i$ in terms of $f_i$. Hence we have $b_i = 0$ for all $i$.

(c) $3 \Rightarrow 1$: Suppose $\{e_1, \ldots, e_r\}$ is a $\mathbb{Z}$-basis of $H$, which is also linearly independent over $\mathbb{R}$. So we can extend it to a $\mathbb{R}$-basis and add $e_{r+1}, \ldots, e_n$ such that $\{e_1, \ldots, e_n\}$ is a $\mathbb{R}$ of $\mathbb{R}^n$. Suppose $\{f_1, \ldots, f_n\}$ is the standard orthonormal basis for $\mathbb{R}^n$. Then there is a $\mathbb{R}$ linear transformation:

$$L : V \longmapsto V$$

such that $L(e_i) = f_i$. It is clear that both $L$ and $L^{-1}$ are continuous. Suppose $X \subseteq V$ is compact, then $L(X)$ is also compact in $V$. Then there is a ball $B \subseteq V$ centered at 0 such that

$$L(X) \subseteq B$$

Let $B$ have radius $R$ and so $B = B_R(0)$. Now observe that $L(H) \subseteq \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_n$. Then $L(H) \cap B$ is finite because there are only finitely many integer vectors $(m_1, \ldots, m_r)$ with $\sum_{i=1}^r m_i^2 \leq R^2$. Since $L$ is bijective, we have

$$H \cap L^{-1}(B) = L^{-1}(L(H) \cap B)$$

finite. But $X \subseteq L^{-1}(B)$ because $L(X) \subseteq B$ and so $H \cap X$ is finite. Hence $H$ is discrete.

□

**Definition 16.6.** *Let $V$ be a $\mathbb{Z}$ module in $\mathbb{R}^n$. A* **lattice** *in $V$ is an discrete additive subgroup (i.e. a $\mathbb{Z}$ submodule) $H \subseteq V$ such that $rank_{\mathbb{R}} H = n$.*

In other words, it is discrete subset in $V$ which achieves the full rank.

**Definition 16.7.** *Let $H$ be a lattice in $V$, then by Lemma 16.5, let $\{e_1, \ldots, e_n\}$ be a $\mathbb{Z}$-basis for $H$. Let*

$$P = \left\{ \sum_{i=1}^n a_i e_i : a_i \in [0, 1) \right\}$$

*The* **covolume** *of $H$ is defined as the volume of $P$, and is written as $cov(H)$.*

**Proposition 16.8.** *The definition of $cov(H)$ is independent of the choice of basis.*

*Proof.* Let $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_n\}$ be two $\mathbb{Z}$-bases for $H$. Let $A$ be the change of basis matrix. Define

$$P = \left\{ \sum_{i=1}^n a_i e_i : a_i \in [0, 1) \right\}, Q = \left\{ \sum_{i=1}^n b_i e_i : b_i \in [0, 1) \right\}$$

Then since $A$ has entries in $\mathbb{Z}$ and is invertible, so $\det(A) = \pm 1$. Therefore,

$$V(Q) = |\det A| V(P) = V(P)$$

the volume of $Q$ is the same as $P$ and so the definition is independent of the choice of basis. □

**Definition 16.9.** *A set $S \in \mathbb{R}^n$ is* **convex** *if $\forall x, y \in S$, $\lambda x + (1 - x)\lambda(y) \in S$ for all $\lambda \in [0, 1]$. A set $S$ is called a* **convex body** *if it is compact and convex.*

**Definition 16.10.** *Let $P$ be a subset of $\mathbb{R}^n$. Let $h \in \mathbb{R}^n$, the set*

$$P_h = \{h + p : p \in P\}$$

*is called the* **translate** *of $P$.*

**Remark 16.11.** *It is clear that if $H \subseteq V$ is a lattice with basis $\{e_1, \ldots, e_n\}$. Let*

$$P = \left\{ \sum_{i=1}^n a_i e_i : a_i \in [0, 1) \right\}$$

*then $V = \cup_{h \in H} P_h$. Moreover, the union is disjoint.*

**Definition 16.12.** *A set $S \subseteq \mathbb{R}^n$ is called* **symmetric** *if $-\alpha \in S$ for any $\alpha \in S$.*

**Theorem 16.13.** [**Minkowski's convex body theorem**] *Suppose $H \subseteq V$ is a lattice and $S \subseteq V$ is measurable ($S$ has a volume), and the measure of $S$ is denoted by $m(S)$, then*

1. *Suppose $m(S) > cov(H)$. Then there exists $x, y \in S$ such that $0 \neq x - y \in H$.*

2. *If $m(S) > 2^n cov(H)$, and $S$ is convex and symmetric, then there exists $x \neq 0$, such that $x \in S \cap H$.*

3. *If $m(S) \geq 2^n cov(H)$, and $S$ is a convex body and symmetric, then there exists $x \neq 0$ such that $x \in S \cap H$.*

*Proof.* Let $\{e_1, \ldots, e_n\}$ be a $\mathbb{Z}$-basis for $H$ and let

$$P = \left\{ \sum_{i=1}^{n} a_i e_i : a_i \in [0, 1) \right\}$$

1. Observe that the linear transformation does not change the measure (or volume) so we have

   $$m(S \cap P_k) = m(S_{-k} \cap P) \text{ where } P_k = \{k + p : p \in P\}$$

   Since $V = \sqcup_{k \in H} P_k$, we have

   $$S = \sqcup_{k \in H} (S \cap P_k) \text{ and so } m(S) = \sum_{k \in H} m(S \cap P_k)$$

   Suppose $(S_{-k} \cap P) \cap (S_{-h} \cap P) = \varnothing$ for all $h \neq h \in H$, then

   $$\sum_{k \in H} m(S_{-k} \cap P) \leq m(P) = cov(H)$$

   and so

   $$m(S) = \sum_{k \in H} m(S \cap P_k) = \sum_{k \in H} m(S_{-h} \cap P) \leq cov(H)$$

   which is a contradiction.

   Therefore, there exists $h \neq k \in H$ such that

   $$(S_{-h} \cap P) \cap (S_{-k} \cap P) \neq \varnothing$$

   Hence there exist $x, y \in S$ such that

   $$x - h = y - k \text{ and so } 0 \neq x - y = h - k \in H$$

2. Let $S' = \frac{1}{2} S = \{\frac{1}{2} s : s \in S\}$. Then $m(S') = \frac{1}{2^n} m(S)$ and so

   $$m(S') > cov(H)$$

   and so by previous part we have distinct $y, z \in S'$ such that $y - z \in H$. Then $2y, 2z \in S$ and so $-2z \in S$. Then

   $$x = y - z = \frac{1}{2} (2y + (-2z)) \in S$$

   because $S$ is convex. Thus $0 \neq x \in H$.

3. For any integer $m$, define the set
$$S_m = \left(1 + \frac{1}{m}\right) S$$
It is clear that for all $m$,
$$S \subset S_m \subset S_{m-1} \subset S_1$$
Thus, $m(S_m) > 2^n cov(H)$ for all $m$. By previous part, we can find $x_m \in S_m \cap H \subseteq S_1 \cap H$. Since $S_1$ is compact, and $H$ is a lattice, so we have $S_1 \cap H$ finite and so there exists $x$ such that $x_m = x$ for infinitely many $m$. Hence $x \in \bigcap_m S_m = S$ because $S$ is compact.

□

## 16.3 Finiteness of the ideal class group

**Definition 16.14.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n = r + 2s$ in the usual notation. Then define the map*
$$\sigma = (\sigma_1, \dots, \sigma_{r+s}) : K \longmapsto \mathbb{R}^r \times \mathbb{C}^s$$
*and for each complex pair, only one of the embedding appears. Another view of the map is*
$$\sigma = (\sigma_1, \dots, \mathcal{R}e\sigma_{r+1}, \mathcal{I}m\sigma_{r+1}, \dots, \mathcal{R}e\sigma_{r+s}, \mathcal{I}m\sigma_{r+s}) : K \longmapsto \mathbb{R}^n$$

Now we shall use Minkowski's convex body theorem to deduce that the ideal class group is finite.

**Proposition 16.15.** *Let $K$ be a number field of degree $n$. Then $\sigma(\mathcal{O}_K$ is a lattice of $\mathbb{R}^n$ with covolume $2^{-s}\sqrt{|\mathcal{D}_K|}$. Moreover,If $I$ is an integral ideal of $\mathcal{O}_K$, then $\sigma(I)$ is a lattice of $\mathbb{R}^n$ with covolum $2^{-s}\sqrt{|\mathcal{D}_K|}N(I)$*

*Proof.* Let $\{e_1, \dots, e_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. For any $x \in K$,
$$\sigma(x) = (\sigma_1(x), \dots, \sigma_r(x), \mathcal{R}e\sigma_{r+1}(x), \mathcal{I}m\sigma_{r+1}(x), \dots, \mathcal{R}e\sigma_{r+s}(x), \mathcal{I}m\sigma_{r+s}(x)\}$$
Let $X$ be the matrix such that the $i^{th}$ row is $\sigma(e_i)$. Recall that for any complex number $z$, let $z^*$ be the conjugate of $z$, we have
$$\mathcal{R}e(z) = \frac{z + z^*}{2}, \mathcal{I}m(z) = \frac{z - z^*}{2i}$$
Consider the entries
$$a = \frac{\sigma_j(e_i) + (\sigma_j(e_i))^*}{2}, b = \frac{\sigma_j(e_i) - (\sigma_j(e_i))^*}{2i}$$
We have $\sigma_j(e_i) = a + ib$, and then $(\sigma_j(e_i))^* = \sigma(e_i) - 2ib$. But the complex conjugate $(\sigma_j)^*$ is the complex pair of the embedding $\sigma_j$. Hence we can apply column operations so that the determinant
$$d = \frac{1}{(2i)^s} \det\left(\sigma_j(e_i)\right)$$
and so
$$d^2 = \frac{1}{(2i)^{2s}} \det\left(\sigma_j(e_i)\right)^2 = \frac{1}{(2i)^{2s}} \mathcal{D}_K \neq 0$$
So the vectors $\sigma_(x_1), \dots, \sigma_(x_n)$ are linearly independent, which is a basis and a $\mathbb{Z}$-basis for $\sigma(\mathcal{O}_K)$ because $\mathcal{O}_K$ is a $\mathbb{Z}$-module. Hence it is a lattice. By definition of determinant in real spaces, we have
$$cov(\mathcal{O}_K) = |d| = 2^{-s}\sqrt{|\mathcal{D}_K|}$$

Now let $I$ be an integral ideal. Then we have, by the above argument, we have
$$cov(I) = 2^{-s}\sqrt{|D(I)|} = 2^{-s}\sqrt{|\mathcal{D}_K|}N(I)$$

□

**Definition 16.16.** *Let $K$ be a number field of degree $n = r + 2s$. Define the* **Minkowski's bound** *by*

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathcal{D}_K|}$$

**Theorem 16.17.** *Let $K$ be a number field. Let $I$ be an integral ideal of $\mathcal{O}_K$. Then there exists $0 \neq x \in I$ such that*

$$|N(x)| \leq N(I)c_K$$

*Proof.* For any positive real number $t$, define the set

$$B(r,s)_t = B_t = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t\}$$

It is clear that the region $B(r,s)_t$ is symmetric and by triangle inequality the region is convex. It is also clear that the region is compact. So $B(r,s)_t$ is a convex body. We shall firstly show that the measure (volume) of $B(r,s)_t$ is

$$m(B(r,s)_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

We shall prove this by double induction. When $r = 1, s = 0$, it is clear that the volume is

$$\int_{-t}^{t} dy = 2t$$

When $s = 1, r = 0$, let $z = re^{i\theta}$ then $dz = 2\pi r dr$ since the volume is independent of $\theta$.

$$\int_0^{\frac{t}{2}} 2\pi r dr = \frac{\pi t^2}{4} = \frac{\pi}{2}\frac{t^2}{2}$$

So both of them satisfy the formula given above. Now suppose it is true for $(r,s)$. Then for $(r+1,s)$, we have

$$\sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t - |y_{r+1}|$$

and so the volume is, by induction

$$\int_{-t}^{t} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t - |y_{r+1|})^n}{n!} dy_{r+1} = 2^{r+1}\left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!}$$

Similarly, for $(r, s+1)$, let $z = re^{i\theta}$ and so $dz = 2\pi r dr$, so the volume is

$$\begin{aligned} V &= \int_{|z_{s+1} \leq \frac{t}{2}} \leq 2^r \left(\frac{\pi}{2}\right)^s \frac{(t - \frac{|z_{s+1}|}{2})^n}{n!} dz_{s+1} \\ &= \int_0^{\frac{t}{2}} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t - \frac{r}{2})^n}{n!} 2\pi r dr \\ &= 2^r \left(\frac{\pi}{2}\right)^{s+1} \frac{t^{n+2}}{(n+2)!} \end{aligned}$$

Hence it is true for all $(r,s)$.

Then since we have proved that $B(r,s)_t$ is a convex body and we pick some $t$ such that

$$m(B(r,s)_t) = 2^n cov(\sigma(I))$$

and so

$$t^n = \left(\frac{4}{\pi}\right)^s n!\sqrt{|\mathcal{D}_K|}N(I)$$

Apply Minkowski's convex body theorem (Theorem 16.13) there exists a non-zero $y \in B(r,s)_t \cap \sigma(I)$. Let $\sigma(x) = y = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in B(r,s)_t$. Then

$$|N(x)| = \left|\prod_{i=1}^r y_i\right| \left|\prod_{j=1}^s z_j z_j^*\right| = \prod_{i=1}^r |y_i| \prod_{j=1}^s |z_j|^2$$

because only one of the conjugate pair appears. Then apply AM-GM inequality, we have

$$|N(x)|^{\frac{1}{n}} \leq \frac{1}{n}\left(\sum_{i=1}^r |y_i| + 2\sum_{j=1}^s |z_j|\right) \leq \frac{t}{n}$$

So

$$|N(x)| \leq \left(\frac{t}{n}\right)^n = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathcal{D}_K|}N(I)$$

□

**Definition 16.18.** *In the ideal class group, the* **ideal class** $[I]$ *containing* $I$ *is the set of ideals which contains* $I$ *and* $I_1, I_2 \in [I]$ *if* $I_1 P(K) = I_2 P(K)$ *in the ideal class group.*

**Corollary 16.19.** *Every ideal class in* $\mathcal{O}_K$ *has an integral ideal representative* $J$ *such that* $N(J) \leq c_K$.

*Proof.* Let $M$ be any ideal in the given class. Then it is clear that $\alpha M$ is also in the given class for any $\alpha \in K\backslash\{0\}$ because

$$\alpha M P(K) = M P(K)$$

Then we may rescale $M$ by multiplying $M$ by suitable $\alpha$ such that $\alpha M \supseteq \mathcal{O}_K$ (For example, multiply $M$ by $\alpha$ so that one of the generator is 1.) Thus, we may assume that the given $M \supseteq \mathcal{O}_K$ (as we can always pick one in the given class.) and so $M^{-1}$ is integral. Then by Theorem 16.17, there exists $0 \neq x \in M^{-1}$ such that $|N(x)| < N(M^{-1})c_K$. By multiplicative property of ideal norm, we have

$$N(xM) \leq c_K$$

and it is clear that $xM$ is in the given class. □

**Proposition 16.20.** *Let* $K$ *be a number field. Let* $M$ *be a positive integer. Then there are only finitely many integral ideals* $I$ *of* $\mathcal{O}_K$ *such that* $N(I) = M$.

*Proof.* Let $I$ be an integral ideal with $N(I) = M$. Then we have

$$I \big| \langle M \rangle$$

by exercise 7 of chapter 14. Let

$$\langle M \rangle = \prod_{i=1}^r P_i^{e_i}$$

where $e_i \geq 1$. Then we have

$$I = \prod_{i=1}^r P_i^{f_i}$$

where $0 \leq f_i \leq e_i$. Hence there are at most $(e_1 + 1) \cdots (e_r) + 1$ such $I$. □

**Theorem 16.21.** *Let* $K$ *be a number field. Then the ideal class group* $Cl(K)$ *is finite.*

*Proof.* By Corollary 16.19, each class contains an integral ideal whose norm is less than or equal to $c_K$. So the class number must be less than or equal to the number of integral ideals with norm less than or equal to $c_K$. By Proposition 16.20, there are only finitely many integral ideals with norm equal to $M$ for each $M \leq c_K$ and hence finitely many integral ideals with norm less than or equal to $c_K$. Hence the ideal class group is finite. □

## 16.4 Further properties

We shall deduce some useful result using the Minkowski's bound.

**Theorem 16.22.** *Suppose ngr2, then* $|\mathcal{D}_K| \geq \frac{\pi}{3}(\frac{3\pi}{4})^{n-1} > 1$.

*Proof.* There exists some ideal $I$ such that $N(I) \leq c_K$ by Corollary 16.19. But $1 \leq N(I)$ and so $1 \leq c_K$. Therefore, we have

$$|\mathcal{D}_K|^{\frac{1}{2}} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}$$

But since $2s \leq n$ and $\frac{\pi}{4} \leq 1$, so

$$|\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$$

For $n \geq 2$, define

$$a_n = \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$$

It is clear that $a_2 = \frac{\pi^2}{4} > 1$. For $n > 2$,

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \\ &= \frac{\pi}{4}\sum_{i=0}^{2} n\binom{2n}{i}\left(\frac{1}{n}\right)^i \\ &> \frac{3\pi}{4} \end{aligned}$$

by taking the first two terms in the expansion. Hence

$$|\mathcal{D}_K| > \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

□

**Corollary 16.23.** *Let $K$ be a number field with degree $n \geq 2$. Then there exists a prime number $p$ which ramifies in $K$.*

*Proof.* By Theorem 16.22, $|\mathcal{D}_K| > 1$ and we know $|\mathcal{D}_K|$ is an integer. Therefore, it must have a prime factor $p$ and so $p$ ramifies in $K$ by Theorem 15.11. □

**Theorem 16.24.** **[Hermite]** *There are only finitely many number fields $K$ with $|\mathcal{D}_K|$ below a certain bound.*

*Proof.* Let $A$ be a constant bound and let $K$ be a number field such that $|\mathcal{D}_K| < A$. So we show prove that the number of $K$ such that $|\mathcal{D}_K| = M$ for each $M < A$ is finite. By Theorem 16.22,

$$M = |\mathcal{D}_K| > \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

and so the degree of extension $n$ is bounded. So we may check that for each $M$ and $n$, there are only finitely many number fields $K$ such that $|\mathcal{D}_K| = M$ and $[K : \mathbb{Q}] = n$. If $n$ is fixed, then there are only finitely many pairs $(r, s)$ and so we may then check that for each pair $(r, s)$ there are finitely many

number fields with fixed discriminant $|\mathcal{D}_K| = M$. We treat the cases $r = 0$ and $r \geq 1$ separately. If $r \geq 1$, consider the region

$$\begin{aligned} B &= \Big\{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_1| \leq 2^{n-1} \left(\frac{\pi}{2}\right)^{-s} \sqrt{|\mathcal{D}_K|} \\ &\quad |y_i|, |z_j| \leq \frac{1}{2} \forall i \neq 1, \forall j \Big\} \end{aligned}$$

If $r = 0$, consider the region

$$\begin{aligned} C &= \big\{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : \mathcal{R}e|z_1| \leq 2^{n-2} \\ &\quad \mathcal{I}m|z_1| \leq \frac{\pi}{4} \left(\frac{\pi}{2}\right)^{-s} \sqrt{|\mathcal{D}_K|}, \text{ and } |z_j| \leq \frac{1}{2} \ \forall j \neq 1 \Big\} \end{aligned}$$

It is clear that both $B$ and $C$ are convex bodies. The volumes

$$V(B) = V(C) = 2^n 2^{-s} \sqrt{|\mathcal{D}_K|} = 2^n cov(\sigma(\mathcal{O}_K))$$

Therefore in both cases, by Minkowski's convex body theorem, there exists $x \in \mathcal{O}_K$, such that

$$\sigma(x) \in \sigma(\mathcal{O}_K) \cap B$$

We shall check that $K = \mathbb{Q}(x)$.

If $r > 0$, then $|\sigma_j(x)| \leq \frac{1}{2}$ for all $j \neq 1$ and since $|N(x)|$ is an integer, we conclude that $|\sigma_1(x)| > 1$. Hence it is distinct from any other $\sigma_j(x)$ and so $K = \mathbb{Q}(x)$. If $r = 0$, then $\sigma_1(x)$ is the only element lying outside the unit sphere and so $K = \mathbb{Q}(x)$ as before.

Then by construction of the regions $B$ and $C$, each $|\sigma_i(x)|$ is bounded and since the coefficients of minimal polynomials of $x$ are the elementary functions of $|\sigma_i(x)|$ and so they are bounded. But they are integers so there are finitely many such polynomials and hence finitely many such $x$ and hence finitely many such number fields $K = \mathbb{Q}(x)$. Therefore, we conclude that there are only finitely many number fields whose discriminant is under a certain bound. □

**Theorem 16.25.** *There are only finitely many number fields $K$ where the degree $n$ is bounded and the set of ramified prime $p \in Z$ is bounded. (This is a more useful version of theorem 16.24).*

*Proof.* By Theorem 16.24, it is enough to bound $|\mathcal{D}_K|$ by $n$ and the set $S$ of ramified primes. We say $v_p(n) = r$ if the order of $p$ in $n$ is $r$. Then we quote a result from [Serre, Corps Locaux, III.6, p58]:

$$v_p(\mathcal{D}_K) \leq n + n \cdot \log_p n - 1$$

Since the set $S$ is bounded and $n$ is bounded, hence $\mathcal{D}_K$ is bounded. □

## 16.5 Algorithm to determine the ideal class group

The previous results give us a method of determining all the ideal classes of a given number field. To determine the representatives of the ideal classes, we need only look at the integral ideals of $\mathcal{O}_K$ less than or equal to $c_K$, the Minkowksi bound. Also, by unique factorisation, if $I$ is one such ideal, then $N(P) \leq c_K$ for all prime ideals which divide $I$. Now we have seen $N(P) = p^f$ for some prime number $p$ and inertia degree $f$, so the prime ideals in various integral ideals in $I$ are all factors of $p \leq c_K$. Thus if we take each prime number $p \leq c_K$, look at how $\langle p \rangle$ factorises in $\mathcal{O}_K$, and form all possible products of the prime ideals of these prime numbers that yield ideals with norm $\leq c_K$ then we can have at least one representatives of every ideal class.

In particular, if every prime number $\leq c_K$ factorises into a product of prime ideals of $\mathcal{O}_K$, each of which is a principal ideal, then we can conclude that the class number is 1. To sum up, we shall give the following algorithm:

**Algorithm to find the ideal class group of a number field $K$**

1. Determine $n = [K : \mathbb{Q}]$ and $r, s$ in the usual notation such that $r + 2s = n$.

2. Compute the discriminant $\mathcal{D}_K$ and hence the Minkowski bound
$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathcal{D}_K|}$$

3. For each prime number $p \leq c_K$, find the factorisation of $\langle p\rangle$. Take the list of prime ideals which contain $p$ for each $p$.

4. Consider all possible product of these prime ideals with norm $\leq c_K$. Determine the generators of the ideal class group $Cl(K)$.

We shall apply the above algorithm to several examples. In general, we do not need to find precisely the generators of the prime ideals which contain $p$ for each $p$. In fact, in many cases, we only need to consider the norm. We shall make this concrete in the following examples.

**Example 16.26.** *Compute the ideal class group of $K = \mathbb{Q}(\sqrt{-19})$. We have*
$$n = 2, r = 0, s = 1, \mathcal{D}_K = -19$$
*The Minkowski bound is*
$$c_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{19} = \frac{2}{\pi}\sqrt{19} < 4$$
*Consider $p = 2, 3$. But since*
$$\left(\frac{-19}{2}\right) = \left(\frac{-19}{3}\right) = -1$$
*so $\langle 2\rangle, \langle 3\rangle$ are both prime ideals. Hence $Cl(K)$ is the trivial group.*

**Example 16.27.** *Compute the ideal class group of $K = \mathbb{Q}(\sqrt{-14})$. We have*
$$n = 2, r = 0, s = 1, \mathcal{D}_K = -56$$
*The Minkowski bound is*
$$c_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{56} < 5$$
*Consider $p = 2, 3$. But $2| - 56$ and so 2 ramifies. Let*
$$\langle 2\rangle = P^2 \text{ where } N(P) = 2$$
*and since $(\frac{-56}{3})1$ so*
$$\langle 3\rangle = QR \text{ where } N(Q) = N(R) = 3$$
*It is clear that $P, Q$ and $R$ are not principal because we have no elements in $\mathcal{O}_K$ with norm 2 or 3. So the order of $[P]$ is 2 in the class group since $[P]^2 = [P^2] = [2]$ which is principal. Let $\alpha \in \mathcal{O}_K$, then $\alpha = a+b\sqrt{-14}$ for some $a, b \in \mathbb{Z}$. $N(\alpha) = a^2+14b^2$. Consider $\alpha = 2+\sqrt{-14}$ then $N(\alpha) = 18 = 2\cdot 3^2$. Since the norm of prime ideal must be a power of prime. Hence we know that $\langle\alpha\rangle$ must be divisible by a prime ideal of norm 2 and prime ideals of norm 3 or 9. But 3 splits in $\mathcal{O}_K$, so it is divisible by a prime ideal of norm 2 and two prime ideals of norm 3. So*
$$\langle\alpha\rangle = PQ^2, PQR \text{ or } PR^2$$

*But it cannot be $PQR$ because if so then since $QR = \langle 3 \rangle$, then $3|\alpha$ in $\mathcal{O}_K$, which is impossible. Then it is $PQ^2$ or $PR^2$. But these two cases can be treated in the same way. Suppose it is $PQ^2$ then we know that*

$$[PQ^2] = [\langle \alpha \rangle]$$

*which is identity in the class group. But since $[P]^2$ is identity, so we square $[PQ^2]$ so that $[Q^4]$ is the identity. It is clear that $[Q^2]$ cannot be the identity because if so then $P$ would be the identity. Hence $[Q]$ has order 4 in the class group. Since $[PQ]^2$ is the identity, so $[P] = [Q^2]$, and since $[QR] = [\langle 3 \rangle]$ is the identity, we have $[R] = [Q^3]$. Finally, the only integral ideals with norm $\leq 4$ are $P^2, Q, P, PQ$ and so the class group is*

$$Cl(K) = \{[Q], [Q^2] = P, [Q^3] = R, [Q^4] = [P^2] = 1\}$$

*which is a cyclic group of order 4. Similarly, if we consider the case when $\langle \alpha \rangle = PR^2$ then the group would be generated by $[R]$. But in both cases, $Cl(K) = C_4$*

In the second example above, we see that the explicit factorisation of $\langle 3 \rangle$ is not needed. The technique to find the class group is to find some 'suitable' element in the ring of integer $\mathcal{O}_K$ with norm $n$ such that $n$ contains only prime factors lies below the Minkowski bound. We shall use this technique very often and readers will find more examples in the exercises.

We shall give a table (table 1) of non-trivial class groups $Cl(\mathbb{Q}(\sqrt{k}))$ for $|k| < 30$, square free.

Table 1: $K = \mathbb{Q}(\sqrt{k})$,$|k| < 30$ square free.

| $k$ | $Cl(K)$ | generators |
|---|---|---|
| 10 | $C_2$ | $I = [\langle 2, \sqrt{10} \rangle]$ |
| 15 | $C_2$ | $I = [\langle 2, 1 + \sqrt{15} \rangle]$ |
| 26 | $C_2$ | $I = [\langle 2, \sqrt{26} \rangle]$ |
| 30 | $C_2$ | $I = [\langle 2, \sqrt{30} \rangle]$ |
| -5 | $C_2$ | $I = [\langle 2, 1 + \sqrt{-15} \rangle]$ |
| -6 | $C_2$ | $I = [\langle 2, \sqrt{-6} \rangle]$ |
| -13 | $C_2$ | $I = [\langle 2, \sqrt{-10} \rangle]$ |
| -14 | $C_4$ | $I = [\langle 3, 1 + \sqrt{-14} \rangle]$ |
| -15 | $C_2$ | $I = [\langle 2, \frac{1}{2}(3 + \sqrt{-15}) \rangle]$ |
| -17 | $C_4$ | $I = [\langle 3, 1 + \sqrt{-17} \rangle]$ |
| -21 | $C_2 \times C_2$ | $I = [\langle 2, 1 + \sqrt{-21} \rangle]$,$J = [\langle 3, \sqrt{-21} \rangle]$, $Cl(K) = \{I, J, IJ, 1\}$ |
| -22 | $C_2$ | $I = \langle [2, \sqrt{-22} \rangle]$ |
| -23 | $C_3$ | $I = [\langle 2, \frac{1}{2}(1 + \sqrt{-23}) \rangle]$ |
| -26 | $C_6$ | $I = [\langle 5, 2 + \sqrt{-26} \rangle]$ |
| -29 | $C_6$ | $I = [\langle 3, 1 + \sqrt{-29} \rangle]$ |
| -30 | $C_2 \times C_2$ | $I = [\langle 2, \sqrt{-30} \rangle]$,$J = [\langle 3, \sqrt{-30} \rangle]$, $Cl(K) = \{I, J, IJ, 1\}$ |

For a quadratic field $K$, Dirichlet has given an explicit formula for the class number $h(K)$, which states:

**Theorem 16.28.** *Let $K$ be a quadratic field of discriminant $d$. Then the class number*

$$h(K) = \frac{-w(d)}{2|d|} \sum_{r=1}^{|d|-1} r \left( \frac{d}{r} \right), \text{ if } d < 0$$

*and*

$$h(K) = \frac{-1}{\log u} \sum_{1 \leq r < \frac{d}{2}} \left( \frac{d}{r} \right) \log \sin \frac{\pi r}{d}, \text{ if } d > 0$$

*where $w(d)$ denotes the number of roots of unity in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}(d<0)$ so that*

$$w(d)=\begin{cases}6 & \text{if } d=-3\\ 4 & \text{if } d=-4\\ 2 & \text{if } d<-4\end{cases}$$

*and $(\frac{d}{n})$ is the Kronecker symbol and $u$ is the fundamental unit of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ which we shall define in the next chapter.*

The proof uses the $L$-series, and we shall introduce this later.
Now we can use the ideal class group to find the integer solutions to the equation of the form

$$x^2=y^3+k$$

for $k<0$. We shall see many examples in the exercises.

## 16.6 Exercises

1. Compute the ideal class group of $\mathbb{Q}(\sqrt{-30})$.

2. Compute the ideal class group of $\mathbb{Q}(\sqrt{-65})$.

3. Compute the ideal class group of $\mathbb{Q}(\theta)$ where $\theta^3-4\theta+2=0$.

4. Compute the ideal class group of $\mathbb{Q}(\sqrt[4]{2})$.
   The following few questions will give details in solving equations of the form

$$x^2=y^3+k$$

5. Consider the equation $x^2+13=y^3$.

   (i) Compute the ideal class group of $\mathbb{Q}(\sqrt{-13})$.

   (ii) Writing

$$\langle x+\sqrt{-13}\rangle\langle x-\sqrt{-13}\rangle=\langle y\rangle^3$$

   and consider the factorisation of these ideals. Find all integer solutions to the equation.

6. Find all integer solutions to $x^2+21=y^3$.

7. Let $m$ be a square-free even integer. Let $K$ be a number field such that the class number $h(K)$ is prime to 3. Show that $y^3=x^2+m$ has at most two integer solutions.

8. Let $K$ be a quadratic field. Let $I$ be an ideal of $\mathcal{O}_K$. If $I^2$ is a principal ideal, prove that $[I]=[\bar{I}]$, where $\bar{I}$ is the conjugate of $I$.

9. Let $K$ be an imaginary quadratic field with discriminant $d < -4$ and $d$ is odd. Use Dirichlet's class number formula to prove that

$$h(K) = \frac{1}{2 - \left(\frac{d}{2}\right)} \sum_{1 \leq r < \frac{|d|}{2}} \left(\frac{d}{r}\right)$$

(Hint: You may use the standard properties of Kronecker symbol from chapter 4 and use question 11 in Exercise 4).

10. Let $p$ be a prime which is congruent to 3 mod 4. Use Dirichlet's class number formula to prove that $h(\mathbb{Q}(\sqrt{-p})$ is odd.

11. Let $p$ be a prime which is congruent to 3 mod 4. Suppose $h(\mathbb{Q}(\sqrt{p})$ is odd. By considering the ideal $\langle 2, 1 + \sqrt{p} \rangle$, prove that there exists $a$ and $b$ such that

$$a^2 - pb^2 = (-1)^{\frac{(p+1)}{4}} 2$$

12. Use stirling's formula

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}} \ (0 < \theta < 1)$$

Show that as $n$ increases, the discriminant of a number field of degree $n$ converges to infinity.

13. Show that if $x^2 + 31 = y^3$ has an integer solution $(x, y)$, then $x$ must be odd. Hence, show that $x^2 + 31 = y^2$ has no integer solution, given the fact that the class number of $K = \mathbb{Q}(\sqrt{-31})$ is 3

14. Find all integer solutions to the equation

$$x^2 + 1175 = 4y^3$$

15. Let $p$ and $q$ be distinct odd primes such that $(\frac{p}{q}) = (\frac{q}{p}) = 1$.

    (i) Show that at least one of $p$ and $q$ is congruent to 1 mod 4. Let $p \equiv 1 \pmod 4$. Show also that there are integers $u, v$ such that

    $$u^2 \equiv p \pmod{4q}, p|u, v^2 \equiv q \pmod p, q|v$$

    (ii) Define

    $$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : z \equiv 0 \pmod 2, x \equiv uy + vz \pmod{2pq}\}$$

    Show that $\Lambda$ is a lattice in $\mathbb{R}^3$ and if $(x, y, z) \in \Lambda$, then

    $$x^2 - py^2 - qz^2 \equiv 0 \pmod{4pq}$$

    (iii) Consider the ellipsoid

    $$X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + py^2 + qz^2 < 4pq\}$$

    Show that

    $$x^2 - py^2 - qz^2 = 0$$

    has a non-trivial solution.

16. Let $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is the product of distinct primes $p_1, \ldots, p_k$. Show that $(p_i) = \mathfrak{p}_i^2$ where $\mathfrak{p}_i = (p_i, \sqrt{-m})$. When are the ideals $\prod \mathfrak{p}_i^{r_i}$ and $\prod \mathfrak{p}_i^{s_i}$ in the same ideal class? Deduce that the class group $Cl_k$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$.

17. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $f(X) = X^3 - 3X + 1$.

    (i) Show that $f$ is irreducible over $\mathbb{Q}$ and compute its discrminant.

    (ii) Show that $3\mathcal{O}_K = \mathfrak{p}^3$ where $\mathfrak{p} = \langle \alpha + 1 \rangle$ is a prime ideal in $\mathcal{O}_K$ with residue field $\mathbb{F}_3$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$.

    (iii) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Compute the class group of $K$.

18. Let $K$ be a number field. Show that there is a number field $L$ containing $K$ such that for every ideal $\mathfrak{a} \subset \mathcal{O}_K$ the ideal in $\mathcal{O}_L$ generated by $\mathfrak{a}$ (denoted $\mathfrak{a}\mathcal{O}_L$) is principal.

19. (i) Let $K = \mathbb{Q}(\sqrt{-23})$. Compute the ideal class group of $K$.

    (ii) Let $L/K$ be any extension of number fields. Show that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ then $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. [Hint: Let $x_1, \ldots, x_m$ generate $\mathcal{O}_L$ as an $\mathcal{O}_K$-module. If $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ then we can write $x_i = \sum a_{ij} x_j$ for some $a_{ij} \in \mathfrak{p}$.] Deduce that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$ with $\mathfrak{a}\mathcal{O}_L = \mathfrak{b}\mathcal{O}_L$, then $\mathfrak{a} = \mathfrak{b}$.

    (iii) Now again let $K = \mathbb{Q}(\sqrt{-23}) \subset L = \mathbb{Q}(\zeta_{23})$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime dividing 2. Show that if $\mathfrak{p}\mathcal{O}_L = x\mathcal{O}_L$ for some $x \in \mathcal{O}_L$ then $\mathfrak{p}^{11}\mathcal{O}_L = N_{L/K}(x)\mathcal{O}_L$. Deduce that $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

20. Let $L/K$ be an extension of number fields.

    (i) Show that if $\mathfrak{B}$ is a prime ideal in $\mathcal{O}_L$, then $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ and $N(\mathfrak{B})$ is a power of $N(\mathfrak{p})$.

    (ii) Let $L = \mathbb{Q}(i, \sqrt{5})$. Show that $|\mathcal{D}_L| \leq 400$ and that the primes 2 and 3 are inert in some quadratic field $K \subset L$. Deduce that $L$ has class number 1.

    (iii) Let $p$ be a rational prime. Use (i) and question 19(ii), show that if $p$ is unramified in $L$ then it is unramified in $K$. Show also that if $p$ is totally ramified in $L$ then it is totally ramified in $K$.

## 16.7 Hint and Solutions

In the following solutions, let [1] be the identity in the ideal class group.

1. Let $K = \mathbb{Q}(\sqrt{-30})$ and then $\mathcal{D}_K = -120$. The Minkowski bound is

$$c_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{120} < 7$$

Consider the primes $p = 2, 3, 5$. But $2, 3, 5 | -120$, so we have

$$\langle 2 \rangle = P^2, \langle 3 \rangle = Q^2, \langle 5 \rangle = R^2$$

and $N(P) = 2, N(Q) = 3, N(R) = 5$. Now, consider I=$\langle \sqrt{-30} \rangle$, and $N(I) = 30 = 2 \cdot 3 \cdot 5$. Then we conclude that

$$I = PQR \Rightarrow [P][Q][R] = [1]$$

But $[R]^2 = [1]$ and so $[P][Q] = [R]$. Then since $P, Q, R$ are not principal, since we have no element of norm $2, 3, 5$ and the ideals with norm less than or equal to 6 are: $P, Q, R, PQ$ and so the ideal class group is

$$Cl(K) = \{[P], [Q], [PQ] = [R], [1]\} \cong C_2 \times C_2$$

2. Let $K = \mathbb{Q}(\sqrt{-65})$ and then $\mathcal{D}_K = 260$. The Minkowski bound is

$$c_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{260} < 11$$

Consider the primes $p = 2, 3, 5, 7$. Since $2, 5 | -260$ so

$$\langle 2 \rangle = P^2, \langle 5 \rangle = R^2$$

where $N(P) = 2, N(R) = 5$ and $(\frac{-65}{3} = 1$, $(\frac{-65}{7}) = -1$, so

$$\langle 3 \rangle = Q\bar{Q} \text{ and } \langle 7 \rangle = S$$

where $N(Q) = N(\bar{Q}) = 3$ and $S$ is prime with $N(S) = 49$. Let $\alpha \in \mathcal{O}_K$, then $\alpha = a + b\sqrt{-65}$ for some $a, b \in \mathbb{Z}$. Then $N(\alpha) = a^2 + 65b^2$. Take $a = 4, b = 1$ then we have $N(4+\sqrt{-65}) = 81 = 3^4$. But it is clear that $4 + \sqrt{-65}$ is not divisible by 3, hence it is either $Q^4$ or $\bar{Q}^4$. Assume it is $Q^4$. Then

$$[Q]^4 = [1] = [\bar{Q}]^4$$

and so $[Q]$ has order 4 because it is not principal and $[Q]^2$ is not principal as the only principal ideal with norm 9 is $\langle 3 \rangle$. Hence $[\bar{Q}]$ also has order 4. Then consider $a = 5, b = 1$ we have $N(5 + \sqrt{-65}) = 90 = 3^2 \cdot 2 \cdot 5$. It is clear that $5 + \sqrt{-65}$ is not divisible by 3 and so it is $Q^2PR$ or $\bar{Q}^2PQ$. Assume it is $Q^2PR$. Then we have

$$[Q]^2[P][R] = [1] \Rightarrow [P][Q]^2 = [R]$$

because $[R]^2 = [1]$. Hence the ideal class group is

$$Cl(K) = \{[P], [Q], [Q]^2, [Q]^3, [P][Q], [P][Q]^2, [P][Q]^3, [1]\} \cong C_4 \times C_2$$

because the ideals with norm less than 11 are:

$$P, P^2, P^3, Q, Q^2, \bar{Q}, \bar{Q}^2, R, PR, PQ, P\bar{Q}$$

and each of these belongs to one of the above classes and so we have found them all. Also, we may observe that the two assumptions we made above does not matter because $Q$ and $\bar{Q}$ are in some sense symmetric, so we only need to find the order of them.

3. Let $f(x) = x^3 - 4x + 2$ and so

$$disc(f) = disc(\mathbb{Z}[\theta]) = -4(-4)^3 - 27(2)^2 = 148 = 2^2 \cdot 37$$

So the discriminant of $K = \mathbb{Q}(\theta)$ is either 148 or 37. Consider that

$$\langle \theta \rangle^3 = \langle \theta^3 \rangle = \langle 2 \rangle \langle 2\theta - 1 \rangle$$

and

$$(2\theta - 1)(-4\theta^2 - 2\theta + 15) = -8\theta^3 + 32\theta - 15 = 1$$

and so $\langle 2\theta - 1\rangle = \langle 1\rangle$. Hence

$$\langle\theta\rangle^3 = \langle 2\rangle$$

Since 2 ramifies in $K$, so $2|\mathcal{D}_K$ and so $\mathcal{D}_K = 148$. As $disc(f) > 0$, so we have three distinct real roots. So we have $n = 3, r = 3, s = 0$.

$$c_K = \frac{3!}{3^3}\sqrt{148} < 3$$

so we only need to consider the prime $p = 2$. But $\langle 2\rangle = \langle\theta\rangle^3$. Since $\langle\theta\rangle$ is principal and so the class group is trivial.

4. The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$. The conjugates are

$$\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$$

So $n = 4, s = 2, r = 2$. Since $disc(\mathbb{Z}[\sqrt[4]{2}] = -1024 = -32^2$. So $|\mathcal{D}_K|$ is at most 1024. Thus

$$c_K = \left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4}\sqrt{|\mathcal{D}_K|} < 5$$

Consider the primes $p = 2, 3$. Write $\theta = \sqrt[4]{2}$. So it is clear that

$$\langle 2\rangle = \langle\theta\rangle^4 = P^4$$

because $\theta^4 = 2$. Also, the index must be prime to 3, so by Kummer-Dedekind, the polynomial $x^4 - 2 \bmod 3$ is irreducible and so $\langle 3\rangle$ is prime. But $\langle\theta\rangle$ is also prime. So the class group is trivial.

5. (i) Let $K = \mathbb{Q}(\sqrt{-13}$. We have $n = 2, r = 0, s = 1$ and $\mathcal{D}_K = -52$. So

$$c_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{52} < 5$$

Consider the primes $p = 2, 3$. Since $2| - 52$, so 2 ramifies in $K$,

$$\langle 2\rangle = P^2$$

where $N(P) = 2$. As $(\frac{-13}{3}) = -1$ so $\langle 3\rangle$ is prime. It is clear that $P$ is not principal because there exists no element in $\mathcal{O}_K$ with norm 2. Hence we conclude that

$$Cl(K) = \{[P], [1]\} \cong C_2$$

(ii) Let

$$\langle x + \sqrt{-13}\rangle = \prod_{i=1}^{m} P_i^{a_i}\bar{P}_i^{b_i}\prod_{j=1}^{n} Q_j^{c_j}$$

where $P_i \neq \bar{P}_i$, $Q_j = \bar{Q}_j$. If $a_i, b_i \neq 0$ for some $i$ then $P_i\bar{P}_i$ is in the factorisation and we know $P_i\bar{P}_i = \langle p_i\rangle$ for some prime $p_i$. Then

$$p_i | x + \sqrt{-13} \text{ in } \mathcal{O}_K$$

which is impossible. Hence for each $i$, either $a_i$ or $b_i = 0$. Assume $b_i = 0$, and we collect the product as

$$\prod_{i=1}^{m} P_i^{a_i}\prod_{j=1}^{n} Q_j^{c_j}$$

where the conjugate of $P_i$ never appears. Then

$$\langle x - \sqrt{-13} \rangle = \prod_{i=1}^{m} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{c_j}$$

and so

$$\langle x^2 + 13 \rangle = \prod_{i=1}^{m} P_i^{a_i} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{2c_j}$$

But this is $\langle y \rangle^3$ and so by unique factorisation we have $3|a_i, c_j$ for all $i, j$. Hence

$$\langle x + \sqrt{-13} \rangle = I^3$$

for some ideal $I$ because the exponents are all divisible by 3. Hence

$$[1] = [\langle x + \sqrt{-13} \rangle] = [I]^3.$$

But the ideal class group is $C_2$. Hence $[I] = [1]$ and $I$ is principal. It is clear that the units in $\mathcal{O}_K$ are $\pm 1$ and so

$$\langle x + \sqrt{-13} \rangle = \langle \big( \pm (a + b\sqrt{-13}) \big)^3 \rangle$$

where $a, b \in \mathbb{Z}$. We take $x + \sqrt{-13} = (a + b\sqrt{-13})^3$ first as the other case is similar. Then

$$x + \sqrt{-13} = a^3 + 3a^2 b\sqrt{-13} - 39ab^2 - 13b\sqrt{-13}.$$

Then compare the coefficient of $\sqrt{-13}$ we have

$$1 = b(3a^2 - 13)$$

Then $b = \pm 1$. (This then includes the other case.) If $b = 1$ then $3a^2 - 13 = 1$, which is impossible. If $b = -1$, then $a = \pm 2$. When $a = 2, b = -1$, we have $x = -70, y = 17$. When $a = -2, b = -1$, we have $x = 70, y = 17$. Hence $x = \pm 70, y = 17$ are the only integer solutions.

6. We firstly compute the class group of $K = \mathbb{Q}(\sqrt{-21})$. We have $n = 2, r = 0, s = 1$, and $\mathcal{D}_K = -84$. Then

$$c_K = \left( \frac{4}{\pi} \right) \frac{2!}{2^2} \sqrt{84} < 6$$

Consider the primes $p = 2, 3, 5$. Since $2, 3| - 84$ so $2, 3$ both ramify in $K$ and

$$\langle 2 \rangle = P^2, \langle 3 \rangle = Q^2$$

where $N(P) = 2, N(Q) = 3$. Since $(\frac{-84}{5}) = 1$ so

$$\langle 5 \rangle = RS$$

where $N(R) = N(S) = 5$. But

$$N(2 + \sqrt{-21}) = 25 = 5^2$$

and $5 \nmid 2 + \sqrt{-21}$ so

$$\langle 2 + \sqrt{-21} \rangle = R^s \text{ or } S^2$$

but in either case we have

$$[R] = [S]$$

Also, consider the element $\alpha = 3 + \sqrt{-21}$, $N(\alpha) = 30 = 2 \cdot 3 \cdot 5$ and so

$$\langle \alpha \rangle = PQR \text{ or } PQS$$

But since $[R] = [S]$, so we have $[P][Q] = [R]$. Hence we conclude that

$$Cl(K) = \{[P], [Q], [R] = [P][Q] = [S], [1]\} \cong C_2 \times C_2$$

and $h(K) = 4$.

Now by a similar argument as in the previous question, we have

$$\langle x + \sqrt{-21} \rangle = \prod_{i=1}^{m} P_i^{a_i} \prod_{j=1}^{n} Q_j^{c_j}$$

where the conjugate of $P_i$ does not appear in the factorisation for each $i$ and $Q_j = \bar{Q}_j$. Hence

$$\langle x^2 + 21 \rangle = \prod_{i=1}^{m} P_i^{a_i} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{2c_j}$$

But this is equal to $\langle y \rangle^3$. So each exponent is divisible by 3 and

$$\langle x + \sqrt{-21} \rangle = I^3$$

and

$$[1] = [\langle x + \sqrt{-21} \rangle] = [I]^3$$

But the class number is 4. So $[I] = [1]$ and so $[I]$ is principal. It is clear that the units in $\mathcal{O}_K$ are $\pm 1$. So set

$$x + \sqrt{-21} = (a + b\sqrt{-21})^3 = a^3 - 63ab^2 + 3a^2b\sqrt{-21} - 21b^3\sqrt{-21}$$

Then $1 = (3a^2 - 21b^2)b$. But the right hand sides is divisible by 3, which cannot be 1. Hence we conclude that there exists no integer solutions.

7. $m$ is even and so is not 1 modulo 4. We use a similar argument as above, so that

$$\langle x + \sqrt{-m} \rangle = I^3$$

Since the class number is coprime to 3, so $[I]$ has to be $[1]$ and $I$ is principal. Thus we have

$$x + \sqrt{-m} = \pm(a + b\sqrt{-m})^3$$

because the only units in $\mathcal{O}_K$ are $\pm 1$. The case when $x + \sqrt{-m} = -(a + b\sqrt{-m})^3$ is covered in the case when $x + \sqrt{-m} = (a + b\sqrt{-m})^3$ because we just simply take $-a$ and $-b$. So we have

$$x + \sqrt{-m} = a^3 - 3ab^2m + 3a^2b\sqrt{-m} - mb^3\sqrt{-m}$$

Compare the coefficients of $\sqrt{-m}$, we have

$$1 = b(3a^2 - mb^2)$$

and so $b = \pm 1$ and either

$$3a^2 - m = 1$$

or

$$3a^2 - m = -1$$

But only one of these can hold. Therefore, we have at most two pairs of $(a, b)$ which satisfies

$$1 = b(3a^2 - mb^2)$$

and hence at most two pairs of $(x, y)$ because $x$ and $y$ are determined by $a$ and $b$. So we have at most two integer solutions.

8. Since $K$ is quadratic then we have

$$\langle N(I)\rangle = I\bar{I}$$

by Proposition 15.14 and so

$$[1] = [\langle N(I)\rangle] = [I][\bar{I}] = [I]^2$$

because $I^2$ is principal. Hence $[I] = [\bar{I}]$.

9. For $d < -4$, we have $w(d) = 2$. Then by Theorem 16.28, we have

$$h(K) = \frac{-1}{|d|}\sum_{r=1}^{|d|-1} r\left(\frac{d}{r}\right)$$

As $d$ is odd,

$$\sum_{r=1}^{|d|-1} r\left(\frac{d}{r}\right) = \sum_{1\le r<\frac{|d|}{2}} \left(2r\left(\frac{d}{2r}\right) + (|d| - 2r)\left(\frac{d}{|d|-2r}\right)\right)$$

Now $(\frac{d}{2r}) = (\frac{d}{r})(\frac{d}{2})$ and since $|d| - 2r + 2r \equiv 0 \pmod{|d|}$, then

$$\left(\frac{d}{|d|-2r}\right) = -\left(\frac{d}{2r}\right)$$

by question 11 in exercise 4 because $sgn(d) = -1$. Thus,

$$\sum_{r=1}^{|d|-1} r\left(\frac{d}{r}\right) = \left(\frac{d}{2}\right)\sum_{1\le r<\frac{|d|}{2}} (4r - |d|)\left(\frac{d}{r}\right)$$

But we can also write

$$\sum_{r=1}^{|d|-1} r\left(\frac{d}{r}\right) = \sum_{1\le r<\frac{|d|}{2}} \left(r\left(\frac{d}{r}\right) + (|d| - r)\left(\frac{d}{|d|-r}\right)\right)$$

and similarly $(\frac{d}{|d|-r}) = -(\frac{d}{r})$. Hence

$$\sum_{r=1}^{|d|-1} r\left(\frac{d}{r}\right) = \sum_{1\le r<\frac{|d|}{2}} (2r - |d|)\left(\frac{d}{r}\right)$$

Let $X = \sum_{r=1}^{|d|-1} r(\frac{d}{r})$, then

$$X - 2X\left(\frac{d}{2}\right) = \left(\frac{d}{2}\right)\sum_{1\le r<\frac{|d|}{2}} |d|\left(\frac{d}{r}\right)$$

and so

$$X = \frac{1}{\left(\frac{d}{2}\right) - 2} \sum_{1 \leq r < \frac{|d|}{2}} |d| \left(\frac{d}{r}\right)$$

because $\left(\frac{d}{2}\right) = \frac{1}{\left(\frac{d}{2}\right)}$. Hence

$$h(K) = -\frac{1}{|d|} X = \frac{1}{2 - \left(\frac{d}{2}\right)} \sum_{1 \leq r < \frac{|d|}{2}} \left(\frac{d}{r}\right)$$

10. Since $p \equiv 3 \pmod 4$, so $-p \equiv 1 \pmod 4$. So the discriminant $d = -p$. Then by Dirichlet formula, we have

$$h(K) = -\frac{1}{p} \sum_{r=1}^{p-1} r \left(\frac{r}{p}\right)$$

because $\left(\frac{-p}{r}\right) = \left(\frac{r}{p}\right)$ by Theorem 4.18(i). Since $p$ is odd, so $-\frac{1}{p}$ does not change the parity, and so it suffices to show

$$X = \sum_{r=1}^{p-1} r \left(\frac{r}{p}\right)$$

is odd. But

$$X = \sum_{r=1}^{\frac{p-1}{2}} \left( r \left(\frac{r}{p}\right) + (p - r) \left(\frac{p-r}{p}\right) \right)$$

and since $p \equiv 3 \pmod 4$, so $\left(\frac{p-r}{p}\right) = -\left(\frac{r}{p}\right)$. So

$$X = \sum_{r=1}^{\frac{p-1}{2}} \left( 2r \left(\frac{r}{p}\right) \right) + \sum_{r=1}^{\frac{p-1}{2}} \left( p \left(\frac{r}{p}\right) \right)$$

The first term in the sum above is clearly even. Since $p$ is odd, so it suffices to show that

$$\sum_{r=1}^{\frac{p-1}{2}} \left(\frac{r}{p}\right)$$

is odd. But $\left(\frac{r}{p}\right)$ is either $-1$ or $1$. Let $m$ be the number of $r$ such that $\left(\frac{r}{p}\right) = 1$, and $n$ be the number of $r$ such that $\left(\frac{r}{p}\right) = -1$. Then $n + m = \frac{p-1}{2}$, which is odd because $p \equiv 3 \pmod 4$. Hence $n - m = n + m - 2m$ is also odd and so the sum

$$\sum_{r=1}^{\frac{p-1}{2}} \left(\frac{r}{p}\right)$$

is odd.

11. Consider the factorisation of $\langle 2 \rangle$. It is clear that since $p \equiv 3 \pmod 4$, so

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{p} \rangle^2$$

and so

$$[1] = [\langle 2 \rangle] = [\langle 2, 1 + \sqrt{p} \rangle]^2$$

But the class number is odd, so we have

$$[1] = [\langle 2, 1+\sqrt{p}\rangle]$$

and so $\langle 2, 1+\sqrt{p}\rangle$ is principal. So there exists $\alpha = a + b\sqrt{p}$ where $a, b \in \mathbb{Z}$ such that

$$\langle \alpha \rangle = \langle 2, 1+\sqrt{p}\rangle$$

and so

$$N(\langle \alpha \rangle) = N(\langle 2, 1+\sqrt{p}\rangle) = 2$$

So $N(\alpha) = 2$ or $-2$. So

$$a^2 - pb^2 = 2 \text{ or } a^2 - pb^2 = -2$$

But $a^2 - pb^2 = 2 \Rightarrow (\frac{2}{p}) = 1$ and $a^2 - pb^2 = -2 \Rightarrow (\frac{-2}{p}) = 1$. Since one of the above holds, and so we conclude that there exist $a, b \in \mathbb{Z}$ such that

$$a^2 - pb^2 = (-1)^{\frac{p+1}{4}} 2$$

12. The Minkowski bound $c_K \geq 1$, so

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\mathcal{D}_K|} \geq 1$$

and so

$$|\mathcal{D}_K| \geq e^{2n - \frac{\theta}{6n}} \frac{\left(\frac{\pi}{4}\right)^{2s}}{2\pi n}$$

Hence since the exponential dominates and $s < n$ and $\frac{e\pi}{4} > 1$, so the discriminant tends to infinity as $n$ tends to infinity.

13. The class number is 3 so the usual trick does not work here. We need a slight modification. If

$$x^2 + 31 = y^3$$

then

$$x^2 - 1 \equiv y^3 \pmod 4$$

Suppose $x$ is even then $y \equiv 3 \pmod 4$. Since $y^3 - 27 = (y+3)(y^2+3y+9)$, and $y^2+3y+9 \equiv 3 \pmod 4$, so there exists a prime factor $p$ of $y^2 + 3y + 9$ with $p \equiv 3 \pmod 4$. Therefore,

$$x^2 + 4 = y^3 - 27 \equiv 0 \pmod p$$

and so $-4$ is a square modulo $p$, which is impossible.

Now $x$ is odd and so $y$ is even. Then, since $-31 \equiv 1 \pmod 4$, so $\mathcal{O}_K =$ $mathbbZ[\frac{1+\sqrt{-31}}{2}]$. Hence we consider the factorisation

$$\langle \frac{x+\sqrt{-31}}{2} \rangle \langle \frac{x-\sqrt{-31}}{2} \rangle = \langle \frac{y}{2} \rangle^3 \langle 2 \rangle$$

Since $-31 \equiv 1 \pmod 8$ and so $\langle 2 \rangle = P\bar{P}$ for some prime ideal $P$. Let

$$\langle \frac{x+\sqrt{-31}}{2} \rangle = \prod_{i=1}^{m} P_i^{a_i} \bar{P}_i^{b_i} \prod_{j=1}^{n} Q_j^{c_j}$$

where $\bar{P_i} \neq P_i, \bar{Q_j} = Q_j$. Clearly for each $i$, either $a_i$ or $b_i = 0$, otherwise we have a prime which divides $\frac{x+\sqrt{-31}}{2}$. Assume $b_i = 0$ for all $i$ and recollect those prime ideals. Then

$$\langle \frac{x-\sqrt{-31}}{2} \rangle = \prod_{i=1}^{m} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{c_j}$$

and so use

$$\langle \frac{x+\sqrt{-31}}{2} \rangle \langle \frac{x-\sqrt{-31}}{2} \rangle = P\bar{P}\langle \frac{y}{2} \rangle^3$$

we have

$$\prod_{i=1}^{m} P_i^{a_i} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{2c_j} = P\bar{P}\langle \frac{y}{2} \rangle^3$$

By unique factorisation, some $P_i$ is $P$, and we may assume $P = P_1$. So we cancel $P\bar{P}$ on both sides, we have the indices

$$3|a_1 - 1, 3|a_i \text{ if } i \geq 2 \text{ and } 3|c_j$$

Then we have

$$\langle \frac{x+\sqrt{-31}}{2} \rangle = PI^3 \text{ or } \bar{P}I^3$$

for some ideal $I$. But in either case, it follows that

$$[1] = [\langle \frac{x+\sqrt{-31}}{2} \rangle] = [P][I]^3$$

Since the class number $h(K) = 3$, then $[I]^3 = [1]$, and so $P$ is principal. But this is impossible because the norm of $P$ is 2. Hence we have no integer solutions.

14. $1175 = 47 \cdot 5^2$. Hence we may consider the class group of $\sqrt{-47}$. We have $n = 2, r = 0, s = 1$ and $\mathcal{D}_K = -47$ since $-47 \equiv 1 \pmod 4$. The Minkowksi bound

$$c_K = \frac{4}{\pi} \frac{2!}{2^2} \sqrt{|\mathcal{D}_K|} < 5$$

Consider the primes $p = 2, 3$. $-47 \equiv 1 \pmod 8$ and so

$$\langle 2 \rangle = P\bar{P}$$

where $N(P) = N(\bar{P}) = 2$. $(\frac{-47}{3}) = 1$, so

$$\langle 3 \rangle = Q\bar{Q}$$

where $N(Q) = N(\bar{Q}) = 3$. Consider the element $\alpha = \frac{1+\sqrt{-47}}{2} \in \mathcal{O}_K$. The norm $N(\alpha) = 12 = 2^2 \cdot 3$. Since $2 \nmid \alpha$, so

$$\langle \alpha \rangle = P^2Q \text{ or } \bar{P}^2Q \text{ or } P^2\bar{Q} \text{ or } \bar{P}^2\bar{Q}$$

But each case gives the same result. Assume it is $P^2Q$, then we have

$$[1] = [\langle \alpha \rangle] = [P]^2[Q]$$

Hence, $[P]^2 = [\bar{Q}]$. Consider the element $\beta = \frac{9+\sqrt{-47}}{2}$, and $N(\beta) = 32 = 2^5$. Since $2 \nmid \beta$, then it is clear that

$$\langle \beta \rangle = P^5 \text{ or } \bar{P}^5$$

But in either case it gives that the order of $[P]$ is 5 since 5 is a prime number. Then $[P]^3 = [Q]$ and so the class group is

$$Cl(K) = \{[P], [P]^2 = [\bar{Q}], [P]^3 = [Q], [P]^4 = [\bar{P}], [P]^5 = [1]\} \cong C_5$$

From the equation $x^2 + 1175 = 4y^3$, it is clear that $x$ is odd. Suppose $x$ is divisible by 5, then $y$ is divisible by 5 and let $x = 5u, y = 5v$, we have

$$u^2 + 47 = 20v^3$$

and so reduce both sides modulo 4, we have

$$u^2 \equiv 1 \pmod 4$$

which is impossible. Hence $5 \nmid x$, and so we have

$$\langle \frac{x + 5\sqrt{-47}}{2} \rangle \langle \frac{x - 5\sqrt{-57}}{2} \rangle = \langle y \rangle^3$$

We may write the factorisation of $\langle \frac{5+\sqrt{-47}}{2} \rangle$ as

$$\prod_{i=1}^{m} P_i^{a_i} \prod_{j=1}^{n} Q_j^{c_j}$$

where $P_i \neq \bar{P}_i$ and $Q_j = \bar{Q}_j$. The conjugate of $P_i$ does not appear for each $i$ because if so then $P_i \bar{P}_i = \langle p_i \rangle$ for some prime $p_i$, and so

$$p_i \Big| \frac{x + 5\sqrt{-47}}{2}$$

The only possible such $p_i$ is 5, but then $5|x$, which is impossible by above. Hence

$$\langle \frac{x - 5\sqrt{-47}}{2} \rangle = \prod_{i=1}^{m} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{c_j}$$

and so

$$\prod_{i=1}^{m} P_i^{a_i} \bar{P}_i^{a_i} \prod_{j=1}^{n} Q_j^{2c_j} = \langle y \rangle^3$$

and so each index is divisible by 3. Hence

$$\langle \frac{x + 5\sqrt{-47}}{2} \rangle = I^3$$

for some $I$, and since the class number is 5, which is prime to 3, so $I$ is principal, and

$$\frac{x + 5\sqrt{-47}}{2} = \pm \left( \frac{a + b\sqrt{-47}}{2} \right)^3$$

Take the plus sign we have

$$4x + 20\sqrt{-47} = a^3 - 141ab^2 + 3ab^2\sqrt{-47} - 47b^3\sqrt{-47}$$

Compare the coefficient of $\sqrt{-47}$, we have

$$20 = b(3a^2 - 47b^2)$$

Reduce the above modulo 3, we have $b^3 \equiv 2 \pmod 3$ and so $b \equiv 2 \pmod 3$. Then check all possible such $b$ which divides 20, the only solution is given by

$$b = -1, a = \pm 3$$

Hence $4x = a^3 - 141ab^2$, and so

$$x = \pm 99, y = 14$$

are the only integer solutions.

15. (i) The first part is clear as $(\frac{p}{q}) = (\frac{q}{p})$ so at least one of them is 1 modulo 4. Since $(\frac{p}{q}) = 1$, so there exists $u$ such that

$$u^2 \equiv p \pmod q$$

If $u$ is even, then take $u + q$ so that $u + q$ is odd and

$$(u + q)^2 \equiv p \pmod q$$

and

$$(u + q)^2 \equiv 1 \pmod 4 \equiv p \pmod 4$$

Hence by Chinese Remainder Theorem, we have

$$(u + q)^2 \equiv p \pmod{4q}$$

Further, if we have some $u$ such that

$$u^2 \equiv p \pmod{4q}$$

then let $U = u + 2qk$ for some integer $k$, then

$$U^2 \equiv p \pmod{4q}$$

Then pick a suitable $k$ such that $p|U = u+2qk$, which is always possible because $(p, q) = 1$. Then such $U$ have

$$U^2 \equiv p \pmod{4q} \text{ and } p|U$$

Similarly, there exists $v$ such that

$$v^2 \equiv q \pmod p \text{ and } q|v$$

(ii) Consider firstly the map

$$f : \mathbb{Z}^3 \longmapsto \mathbb{Z}$$

by

$$f(x, y, z) = \bar{z}$$

where $\bar{z} = z \pmod 2$. Hence by the first isomorphism theorem,

$$\Lambda_1 = \{(x, y, z) \in \mathbb{Z}^3 : Z \equiv 0 \pmod 2\}$$

is a submodule of $\mathbb{Z}^3$. Now define the map

$$g : \Lambda_1 \longmapsto \mathbb{Z}$$

by

$$g(x, y, z) = \overline{x - uy - vz}$$

where $\overline{x - uy - vz} = x - uy - vz \pmod{2pq}$. Then by the first isomorphism, $\Lambda$ is a submodule of $\Lambda_1$ and hence a submodule of $\mathbb{Z}^3$. Hence there exists a $\mathbb{Z}$-basis $\{e_1, e_2, e_3\}$ for $\mathbb{Z}^3$ and $r_1, r_2, r_2 \in \mathbb{Z}$ such that $\{r_1e_1, r_2e_2, r_3e_3\}$ is a basis for $\Lambda$. So it is a lattice.
Now use (i), we may write

$$u = p(4aq + 1), v = q(bp + 1)$$

for some $a, b \in \mathbb{Z}$, and let $x = uy + vz + 2pqk$, then

$$x^2 - py^2 - qz^2 = (u^2 - p)y^2 + (v^2 - q)z^2 + 2uvyz + 4pq(kuy + kvz + pqk^2)$$

Hence

$$\begin{aligned} x^2 - py^2 - qz^2 &\equiv (u^2 - p)y^2 + (v^2 - q)z^2 + 2uvyz \bmod 4pq) \\ &\equiv 4apqy^2 + bpqz^2 + 2pqyz(4aq + 1)(bp + 1) \pmod{4pq} \\ &\equiv 0 \pmod{4pq} \end{aligned}$$

because $z$ is even and so each term is 0 modulo $4pq$.

(iii) Let $x = 2\sqrt{pq}r_1, y = 2\sqrt{p}r_2, z = 2\sqrt{p}r_3$. Then $dxdydz = 8pqdr_1dr_2dr_3$, where

$$r_1^2 + r_2^2 + r_3^2 < 1$$

Hence the volume of the ellipsoid is

$$V(X) = \frac{32\pi pq}{3} = 2^3\frac{4\pi pq}{3}$$

Consider the covolume of $\Lambda$. Let $\{e_1, e_2, e_3\}$ be a basis for $\mathbb{Z}^3$ and $r_1, r_2, r_3 \in \mathbb{Z}$ such that $\{r_1e_1, r_2e_2, r_3e_3\}$ is a basis for $\Lambda$. Then the covolume is the determinant of the matrix, whose rows are $r_1e_1, r_2e_2, r_3e_3$, which is $|r_1r_2r_3|d$, where $d$ is the determinant of the matrix whose rows are $e_1, e_2, e_3$ and hence $d = 1$. Now $|r_1r_2r_3|$ is the index of $\Lambda$ in $\mathbb{Z}^3$. The index of $\Lambda_1$ in $\mathbb{Z}^3$ is clearly 2. Now the map $g$ defined in (ii) is surjective, (simply let $y, z = 0$) and so the index of $\Lambda$ in $\Lambda_1$ is $2pq$ hence the index $|r_1r_2r_3| = 2pq \cdot 2 = 4pq$. Hence, the covolume

$$cov(\Lambda) = 4pq$$

Then since $\frac{32\pi pq}{3} > 2^3 \cdot 4pq$, by Minkowski's convex body theorem (the second case in the theorem as the $X$ in the question is not closed), there exists $(x, y, z) \in X \cap \Lambda$. We have

$$x^2 - py^2 - qz^2 \equiv 0 \pmod{4pq}$$

Suppose

$$x^2 - py^2 - qz^2 \geq 4pq$$

then $x^2 + py^2 + qz^2 \geq 4pq$, contradicting $(x, y, z) \in X$. Suppose

$$x^2 - py^2 - qz^2 \leq -4pq \iff -x^2 + py^2 + qz^2 \geq 4pq$$

then $x^2 + py^2 + qz^2 \geq 4pq$, again contradicting $(x, y, z) \in X$. Therefore,

$$-4pq < x^2 - py^2 - qz^2 < 4pq \text{ and } x^2 - py^2 - qz^2 \equiv 0 \pmod{4pq}$$

so

$$x^2 - py^2 - qz^2 = 0$$

16. We will assume $m \equiv 1 \bmod 4$, and the other case is similar. The first part is clear by direct computation, or using the theorem for quadratic fields in previous sections. For the second part we consider the following problem. Suppose that

$$[\prod_{i=1}^{k} \mathfrak{p}_i^{r_i}] = [1].$$

Since $\mathfrak{p}_i^2$ is principal so we might replace each $r_i$ by $r_i \bmod 2$ and so we can assume that $r_i \in \{0, 1\}$.

Now the above equation induces the following relation by considering the norm of the ideal

$$\prod_{i=1}^{k} p_i^{r_i} = a^2 + b^2 m \text{ for some } a, b \in \mathbb{Z}$$

since we assume $m \equiv 1 \bmod 4$.

When each $r_i = 0$ we have the trivial solution $b = 0$ and $a = \pm 1$. Clearly, if some $r_j = 0$ then the left hand side is smaller than $m$ and so we must have $b = 0$. However, the left hand side is also square free so it cannot be $a^2$ for any $a$, which is a contradiction. Therefore, we conclude that $r_i = 1$ for all $i$ and thus $a = 0$ and $b = \pm 1$ and indeed

$$\prod_{i=1}^{k} \mathfrak{p}_i = \langle \sqrt{-m} \rangle$$

is principal. So we conclude that the problem we considered has a solution if and only if $r_i$ is odd for all $i$ or $r_i$ is even for all $i$. In other words, $r_i$ have the same parity for all $i$.

Now if we look at the second part of the question, it has solution exactly when $s_i - r_i$ have the same parity for all $i$.

For the last part, consider the subgroup generated by the class of $\mathfrak{p}_i$ for $i = 1, \ldots, k-1$. Then by the above argument we know that they must be independent, viewed as $\mathbb{F}_2$ vector space multiplicatively. Therefore, this is a subgroup of order $(\mathbb{Z}/2\mathbb{Z})^{k-1}$.

17. (i) $f$ is irreducible over $\mathbb{F}_2$ and hence it is irreducible over $\mathbb{Q}$. Discrminant is 81.

(ii) $3\mathcal{O}_K = \mathfrak{p}^3$ where $\mathfrak{p} = \langle \alpha + 1 \rangle$ by direct computation so $\mathfrak{p}$ is a prime above 3 and the residue field is $\mathbb{F}_3$. It is clear that the map $\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ is surjective, by checking $0, 1, 2$ have different images. Thus for each $\alpha \in \mathcal{O}_K$, there are integers $a_i$ such that

$$\alpha \equiv a_0 + a_1(\alpha + 1) + a_2(\alpha + 1)^2 \pmod{3\mathcal{O}_K}$$

as $(\alpha + 1)^3 \mathcal{O}_K = 3\mathcal{O}_K$. This completes the second part.

(iii) From (i) the discriminant is 81 so the index of $\mathcal{O}_K$ in $\mathbb{Z}[\alpha]$ is either 1 or 3 (it cannot be 9 because if the discriminant is 1 then it is $\mathbb{Q}$). But in either case we have $3\mathcal{O}_K \subset \mathbb{Z}[\alpha]$ and hence by the second part we know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Now the discriminant is positive so it is a real field with $r = 3, s = 0$. So by calculating the Minkowski bounds we conclude that the class group is trivial.

18. The ideal class group is finite and we pick $I_1, \ldots, I_r$ be the representatives of the class group. So that for each $i$, $I_i^r$ is principal say

$$I_i^r = \langle \alpha_i \rangle.$$

Now let $L = K(\sqrt[r]{\alpha_i}, i = 1, \ldots, r)$. Then by unique factorization each $I_i\mathcal{O}_L$ becomes principal and is $\langle \sqrt[r]{\alpha_i} \rangle$. Now for any other ideal $I$, there exists $a, b \in \mathcal{O}_K$ and some $i$ such that

$$aI = bI_i.$$

Since $I_i, a, b$ are principal in $\mathcal{O}_L$, so is $I$.

19. (i) Compute the Minkowski's bound and we need to check the factorization of ideals above 2 and 3. We find that if $\omega = \frac{1}{2}(1 + \sqrt{-23})$ then

$$\langle \omega \rangle = \langle 2, \omega \rangle \langle 3, \omega \rangle.$$

(Or we just compute the norm of $\omega$ to see that it factorizes into ideals of norm 2 and 3.) We conclude that the ideal class group is cyclic of order 3.

(ii) Following the hint, if $x_i = \sum a_{ij} x_j$ for some $a_{ij} \in \mathfrak{p}$ then the matrix $(a_{ij})_{i,j}$ will be invertible which means that $\mathfrak{p}$ contains a unit which is a contradiction. One can extend this argument for any integral ideal.

Suppose $\mathfrak{a} \neq \mathfrak{b}$ but $\mathfrak{a}\mathcal{O}_L = \mathfrak{b}\mathcal{O}_L$. Then there exists a prime ideal $\mathfrak{p}$ which divides $\frac{\mathfrak{a}}{\mathfrak{b}}$ or $\frac{\mathfrak{b}}{\mathfrak{a}}$. Since $\frac{\mathfrak{a}}{\mathfrak{b}}\mathcal{O}_L = \frac{\mathfrak{b}}{\mathfrak{a}}\mathcal{O}_L = \mathcal{O}_L$, we have $\mathfrak{p}\mathcal{O}_L \supset \mathcal{O}_L$. But clearly $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Thus $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, which is a contradiction.

(iii) If $\mathfrak{p}$ is principal in $\mathcal{O}_L$ then we take the norm on both sides to get the desired equation. Then by (ii) this shows $\mathfrak{p}^{11} = N_{L/K}(x)\mathcal{O}_K$ and so $\mathfrak{p}^{11}$ is principal. But by (i) the class number is 3 and $(3, 11) = 1$ so that $\mathfrak{p}$ itself is principal, which is a contradiction to (i).

20. (i) $\mathfrak{B} \cap \mathcal{O}_K \neq \mathcal{O}_K$. If so then $1 \in \mathfrak{B}$ and so $\mathfrak{B}$ is not a prime ideal. Let $a, b \in \mathcal{O}_K$ such that $ab \in \mathfrak{p}$. Then $ab \in \mathcal{B}$ and so one of them is in $\mathfrak{B}$. So one of them is in $\mathfrak{p}$. So $\mathfrak{p}$ is a prime ideal. We have a natural map $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{B}$. The kernel is $\mathcal{O}_K \cap \mathfrak{B} = \mathfrak{p}$. So $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{B}$ is an injection and so $\mathcal{O}_L/\mathfrak{B}$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$. So $N(\mathfrak{B})$ is a power of $N(\mathfrak{p})$.

(ii) It is clear that $1, i, \frac{1+\sqrt{5}}{2}, \frac{i+i\sqrt{5}}{2}$ are algebraic integers. So they generate a sublattice of the ring of integers. The discriminant of this sublattice is 400 and so $|\mathcal{D}_L| \leq 400$.

The minimal polynomial of $\frac{1+\sqrt{5}}{2}$ is $X^2 - X - 1$ and so $\langle 2 \rangle$ is inert in $\mathbb{Q}(\sqrt{5})$. $X^2 + 1$ has no root over $\mathbb{F}_3$ and so 3 is inert in $\mathbb{Q}(i)$. The Minkowski bound is 4. Since 2 and 3 both inert in some quadratic subfield, so there is no ideal of norm 2 or 3. So the class number is 1.

(iii) Suppose $p$ is ramified in $K$, say $\mathfrak{p}^2 | p$ for some $\mathfrak{p}$. Then by question 19(ii), $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$ and so it must be a product of prime ideals and $\mathfrak{p}^2\mathcal{O}_L | p\mathcal{O}_L$. So $p$ is ramified in $L$.

If $p$ is totally ramified in $L$, then there is only one prime $\mathfrak{B} \subset \mathcal{O}_L$ above $p$. Then $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{B}$ is a prime ideal above $p$ in $\mathcal{O}_K$ and $N(\mathfrak{B})$ is a power of $N(\mathfrak{p})$ by question (ii). But $N(\mathfrak{B}) = p$ as $p$ is totally ramified so $N(\mathfrak{p}) = p$.

Suppose we have another prime $\mathfrak{q} \subset \mathcal{O}_K$ above $p$, then by question 19(ii), $\mathfrak{q}\mathcal{O}_L \neq \mathcal{O}_L$ and so it is a product of prime ideals. But there is only one prime above $p$, so $\mathfrak{q}\mathcal{O}_L = \mathfrak{B}^k$ for some $k$. Similarly, $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}^r$ for some $r$ and so

$$\mathfrak{q}^r\mathcal{O}_L = \mathfrak{p}^k\mathcal{O}_L.$$

By question 19(ii), this means that $\mathfrak{q}^r = \mathfrak{p}^k$. This contradicts the unique factorisation of ideals in $\mathcal{O}_K$. Therefore we conclude that there is only one prime ideal $\mathfrak{p}$ above $p$ in $\mathcal{O}_K$ and $N(\mathfrak{p}) = p$. So $p$ is totally ramified in $\mathcal{O}_K$.

# 17 Units in the ring of integers

In this section we are going to deduce some important properties of the units in the ring of integers.

## 17.1 Units in a quadratic field

**Lemma 17.1.** *Let $K$ be a number field. Then $u$ is a unit in $\mathcal{O}_K$ if and only if $N(u) = \pm 1$.*

*Proof.* Suppose $u$ is a unit, let $v \in \mathcal{O}_K$ such that $uv = 1$. Then $N(u)N(v) = 1$. But $N(u), N(v)$ are both integers, so $N(u) = \pm 1$. Conversely, if $N(u) = \pm 1$, then $N(\langle u \rangle) = 1$ and so

$$card(\mathcal{O}_K/\langle u \rangle) = 1$$

Thus $\langle u \rangle = \mathcal{O}_K$ and so $u$ is a unit. □

It is clear that if $K$ is a quadratic field, $K = \mathbb{Q}(\sqrt{m})$ where $m$ is square free. If $m < 0$, then the only element in $\mathcal{O}_K$ with norm $\pm 1$ are $\pm 1$. Hence the only units in $\mathcal{O}_K$ are $\pm 1$. What about the case when $m > 0$? Let $m \equiv 2$ or $3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Hence an element $\alpha = a + b\sqrt{m}$ has norm $a^2 - mb^2$. Thus, this suggests that we should look at the integer solutions to the equation

$$a^2 - mb^2 = \pm 1$$

For $a^2 - mb^2 = 1$, by Theorem 5.23, we know the solutions are

$$a + b\sqrt{m} = \pm(a_0 + b_0\sqrt{m})^n$$

where $(a_0, b_0)$ is the fundamental solution and $n \in \mathbb{Z}$. Further, the equation $a^2 - mb^2 = -1$ has integer solutions if and only if the period $k$ of the continued fraction $\sqrt{m}$ is odd, and if $(a, b)$ is a solution such that $a^2 - mb^2 = -1$, then it is clear that

$$(a', b') \text{ where } a' + b'\sqrt{d} = (a + b\sqrt{m})^2$$

is a solution for $a^2 - mb^2 = 1$. Hence the units are also of the form,

$$a + b\sqrt{m} = \pm(a_0 + b_0\sqrt{m})^n$$

where $(a_0, b_0)$ is a fundamental solution to $a^2 - mb^2 = -1$.

When $m \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Let $\alpha = a + \frac{b}{2} + \frac{b\sqrt{m}}{2}$. Then $N(\alpha) = (a + \frac{b}{2})^2 - \frac{b^2 m}{4}$. Thus we may consider the equations

$$(2a + b)^2 - mb^2 = \pm 4$$

It is clear that each solution $(x, y)$ with $x^2 - my^2 = \pm 4$ corresponds to a pair $(a, b)$ with $2a + b = x, b = y$. Thus, we shall consider

$$x^2 - my^2 = \pm 4$$

By question 9 in exercise 5, the solutions are given by

$$\frac{x + y\sqrt{m}}{2} = \pm \left( \frac{x_0 + y_0\sqrt{m}}{2} \right)^n$$

where $(x_0, y_0)$ is a fundamental solution to $x^2 - my^2 = -4$ if this is soluble, and a fundamental solution to $x^2 - my^2 = 4$ if $x^2 - my^2 = -4$ is not soluble.

Thus, in both cases, intuitively we seen that the set of units is an infinite Abelian group generated by one element together with $\pm 1$. In fact, we have

**Theorem 17.2.** *Let $K = \mathbb{Q}(\sqrt{m})$, where $m$ is square free and positive. Let $U_K$ be the set of units in $\mathcal{O}_K$. Then*

$$U_K \cong C_2 \times C_\infty$$

We shall use the algebraic method instead of the continued fraction to deduce the above result, though this seems already true from the previous discussion by continued fraction.

*Proof.* Define the map

$$L : \mathcal{O}_K \backslash \{0\} \longmapsto \mathbb{R}^2$$

by

$$L(x) = (\log |x|, \log |\sigma(x)|) = (u, v) \in \mathbb{R}^2$$

This is clearly a ring homomorphism. Restrict the map to $U_K$. Since $N(x) = \pm 1 \ \forall x \in U_K$, so the image lies in the line $W$:

$$W = \{(u, v) \in \mathbb{R}^2 : u + v = 0\}$$

Let $B$ be a compact subset in $W$ and so it is closed and bounded. Then there exists $a \in \mathbb{R}$ such that

$$\frac{1}{a} \leq |x|, |\sigma(x)| \leq a$$

for all $x \in L^{-1}(B)$. But then $|x + \sigma(x)|, |x\sigma(x)|$ are bounded and so the coefficients of the minimal polynomial of $x$ is also bounded. Hence there are only finitely many those polynomials because each coefficient is integer, and so there are only finitely many $x$. Hence $L^{-1}(B)$ is finite. Moreover, $L^{-1}(B) \cap U_K$ is finite and so $B \cap L(U_K)$ is finite. This show that $L(U_K)$ is discrete.

It is clear that $\ker L \cap U_K = \{-1, 1\}$. Since the set of units is a group under multiplication, so

$$U_K / (U_K \cap \ker L) \cong V \subseteq W$$

where $V$ is a discrete additive subgroup of $W$ and hence it is finitely generated over $\mathbb{Z}$, and has a $\mathbb{Z}$-basis which is independent over $\mathbb{R}$. So we have shown that

$$U_K / \{\pm 1\} \cong \mathbb{Z}^{\oplus m}$$

where $m = 0$ or 1 and so

$$U_K \cong C_2 \times \mathbb{Z}^{\oplus m}$$

It remains to show that $m = 1$. For each $l_1 > 0$, define $l_2$ such that

$$l_1 l_2 = \sqrt{|\mathcal{D}_K|}$$

and define the region

$$B_l = \{(y_1, y_2) : |y_i| \leq l_i\}$$

It is clear that $B$ is a convex body (a rectangle). The volume of $B$ is then

$$V(B) = 4 l_1 l_2 = 4\sqrt{|\mathcal{D}_K|} = 2^2 cov(\tau(\mathcal{O}_K))$$

where $\tau(x) = (x, \sigma(x))$. By Minkowski convex body theorem, there exists $0 \neq x_l \in B_l \cap \tau(\mathcal{O}_K)$. So

$$|x_l| \leq l_1, |\sigma(x_l)| \leq l_2 \Rightarrow |N(x_l)| \leq l_1 l_2 = \sqrt{|\mathcal{D}_K|}$$

Now move $l_1$ from a fixed point to 0. Then for each $x_l$, $N(x_l) \leq \sqrt{|\mathcal{D}_K|}$, and as $l_1 \to 0$, there are infinitely many distinct $x_l$ because $x_l \neq 0$. But by Proposition 16.20, there are only finitely many integral ideals with norm $\leq \sqrt{|\mathcal{D}_K|}$. Hence there exists $l \neq k$ such that $x_l \neq \pm x_k$ but $\langle x_l \rangle = \langle x_k \rangle$. Then $\frac{x_l}{x_k}$ is a unit other than $\pm 1$. Therefore, $m = 1$ and so

$$U_K \cong C_2 \times \mathbb{Z} \cong C_2 \times C_\infty$$

□

**Definition 17.3.** *Let $K$ be a real quadratic field. Then $U_K \cong C_2 \times C_\infty$. The* **fundamental unit** *$u$ is a positive unit $> 1$ in $\mathcal{O}_K$ which generates the infinite cyclic group of $U_K$. In other words, if $v$ is a unit in $\mathcal{O}_K$, then $v = \pm u^n$ for some $n \in \mathbb{Z}$.*

**Proposition 17.4.** *Let $K$ be a real quadratic field. Then the fundamental unit $u \in \mathcal{O}_K$ is the smallest unit of $\mathcal{O}_K > 1$.*

*Proof.* Suppose there exists a unit $\theta$ such that

$$1 < \theta < u$$

Then $\theta = u^n$ for some $n$ because both of them are positive. It is clear that $n < 0$ because $u > \theta$. But $u > 1$ and so $u^n < 1$ for $n < 0$, contradicting $\theta > 1$. □

The following theorems characterise the norm of fundamental unit in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{p})$ for an odd prime $p$.

**Theorem 17.5.** **[Hilbert]** *Let $p$ be a prime with $p \equiv 1 \pmod 4$. Then the fundamental unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ has norm $-1$.*

*Proof.* Let $u$ be the fundamental unit and let $v \in \mathcal{O}_K$ with $u\bar{u} = 1$. Then since $u, \bar{u} > 0$ then we have

$$u = \frac{1+u}{1+\bar{u}}$$

Let $m$ be the largest positive integer such that $m|1+u, 1+\bar{u}$ in $\mathcal{O}_K$. Define

$$\gamma = \frac{1+u}{m} \in \mathcal{O}_K, \bar{\gamma} = \frac{1+\bar{u}}{m} \in \mathcal{O}_K$$

so that $\gamma, \bar{\gamma}$ are coprime and $u = \frac{\gamma}{\bar{\gamma}}$. So

$$\gamma = u\bar{\gamma} \Rightarrow \langle\gamma\rangle = \langle\bar{\gamma}\rangle$$

Let $Q$ be a prime ideal which divides $\langle\gamma\rangle$. Then $Q\big|\langle\bar{\gamma}\rangle$. Let $\bar{Q}$ be the conjugate of $Q$, then

$$\bar{Q}\big|\langle\bar{\gamma}\rangle = \langle\gamma\rangle$$

Hence

$$Q, \bar{Q}\big|\langle\gamma\rangle$$

Now $Q$ is a prime ideal, and the discriminant of $\mathcal{O}_K$ is $p$, so we have either

$$Q = \bar{Q} = \langle q\rangle \text{ where } q \text{ is a prime number with } \left(\frac{p}{q}\right) = -1$$

or

$$Q \neq \bar{Q}, Q\bar{Q} = \langle q\rangle \text{ where } q \text{ is a prime number with } \left(\frac{p}{q}\right) = 1$$

or

$$Q = \bar{Q}, Q^2 = \langle q\rangle \text{ where } q \text{ is a prime number with } q|p$$

In the first case, we have $q|\gamma, \bar{\gamma}$ which is impossible.

In the second case, we have $Q$ and $\bar{Q}$ are distinct prime ideals which divide $\langle\gamma\rangle$, and so

$$\langle q\rangle = Q\bar{Q}\big|\langle\gamma\rangle = \langle\bar{\gamma}\rangle$$

and again we have $q|\gamma, \bar{\gamma}$, which is impossible.

In the third case, since $q$ is also a prime number, so $q = p$ and $Q = \langle\sqrt{p}\rangle$. Hence $\langle\sqrt{p}\rangle$ is the only prime ideal which divide $\langle\gamma\rangle$ by previous. Thus

$$\langle\gamma\rangle = \langle\sqrt{p}\rangle^j$$

If $j \geq 2$ then $p|\gamma, \bar{\gamma}$ which is impossible. Hence $j \leq 1$. If $j = 0$, then

$$\langle\gamma\rangle = \langle 1\rangle$$

and so $\gamma$ is a unit. So the norm $N(\gamma) = \gamma\bar{\gamma} = \pm 1$. Hence

$$u = \frac{\gamma}{\bar{\gamma}} = \frac{\gamma^2}{\gamma\bar{\gamma}} = \pm\gamma^2$$

which contradicts $u$ is the fundamental unit. If $j = 1$, then

$$\langle\gamma\rangle = \langle\sqrt{p}\rangle$$

and so $u = w\sqrt{p}$ for some unit $w \in \mathcal{O}_K$. Hence

$$u = \frac{\gamma}{\bar{\gamma}} = \frac{w\sqrt{p}}{-\bar{w}\sqrt{p}} = \frac{w}{-\bar{w}}$$

But $N(w) = w\bar{w} = \pm 1$, so

$$u = \frac{w^2}{-w\bar{w}} = \pm w^2$$

which again contradicts that $u$ is the fundamental unit. Hence, combine all three cases, the fundamental unit must have norm $-1$. □

**Theorem 17.6.** *Let $m$ be a positive square free integer. If there exists a prime $p \equiv 3 \pmod 4$ dividing $m$, then the fundamental unit of $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ has norm 1. In particular, the fundamental unit of $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ for $p$ a prime which is 3 mod 4 has norm 1.*

*Proof.* Let $u$ be the fundamental unit. Let $u = \frac{x+y\sqrt{m}}{2}$, where $x, y \in \mathbb{Z}$, such that

$$x \equiv y \equiv 0 \pmod 2, \text{ if } m \equiv 2, 3 \pmod 4$$

and

$$x \equiv y \pmod 2, \text{ if } m \equiv 1 \pmod 4$$

Suppose the fundamental unit $u$ has norm $-1$. Then

$$N(u) = \frac{x^2 - my^2}{4} = -1$$

and so

$$x^2 - my^2 = -4$$

Since $p|m$, we have

$$x^2 \equiv -4 \pmod p$$

But $p \equiv 3 \pmod 4$, and so $(\frac{-4}{p}) = (\frac{-1}{p}) = -1$, which is a contradiction. Hence $N(u) = 1$. □

## 17.2 Dirichlet's unit theorem

In the previous subsection we have seen that if $K$ is a quadratic field. Then

$$U_K \cong C_2 \times C_\infty$$

by Theorem 17.2 In fact, theorem 17.2 can be generalised to an arbitrary number field. The main result we are going to deduce in this subsection is

$$U_K \cong \mu_K \times (C_\infty)^m$$

where $\mu_K$ is the roots of unity in $\mathcal{O}_K$ and $m = r + s - 1$ with $r + 2s = n$.

**Lemma 17.7.** *Let $K$ be a number field. Define the map*

$$L : \mathcal{O}_K \longmapsto \mathbb{R}^{r+s}$$

*by*

$$\begin{aligned} L(x) &= (\log|\sigma_1(x)|, \ldots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \ldots, 2\log|\sigma_{r+s}(x)|) \\ &= (x_1, \ldots, x_{r+s}) \end{aligned}$$

*where, as usual for each pair of complex embeddings, only one of them appears. Then for all non-zero $\alpha \in \mathcal{O}_K$, with $L(\alpha) = (\alpha_1, \ldots, \alpha_{r+s})$, there exists a non-zero $\beta \in \mathcal{O}_K$, with $|N(\beta)| \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$ such that $\beta_i \leq \alpha_i$ for all $i \neq k$, where $k$ is a fixed index and $L(\beta) = (\beta_1, \ldots, \beta_{r+s})$*

*Proof.* Let $k$ be the fixed index, and for each $i \neq k$, choose $c_i$ such that

$$0 < c_i < e^{\alpha_i}$$

Then define $c_k$ such that

$$\prod_{i=1}^{r+s} c_i = \left(\frac{4}{\pi}\right)^s \sqrt{|\mathcal{D}_K|}$$

Define the region

$$E = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_i| \leq c_i, |z_j|^2 \leq c_{r+j}\}$$

It is clear that $E$ is a convex body and

$$V(E) = 2^r \pi^s \prod_{i=1}^{r} c_i \prod_{j=1}^{s} c_{r+j} = 2^{r+2s}\sqrt{|\mathcal{D}_K|} = 2^n cov(\sigma(\mathcal{O}_K)$$

Then, by Minkowski convex body theorem, there exists a non-zero $\beta \in \mathcal{O}_K$, such that

$$\sigma(\beta) \in E \cap \sigma(\mathcal{O}_K)$$

By construction, $N(\beta) \leq \prod_{i=1}^{r+s} c_i \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$. Let $L(\beta) = (\beta_1, \ldots, \beta_{r+s})$. If $i \neq k$, for $1 \leq i \leq r$, we have

$$\beta_i = \log|\sigma_i(\beta)| \leq \log c_i < \alpha_i$$

and for $r + 1 \leq i \leq s$, we have

$$\beta_i = 2\log|\sigma_i(\beta)| \leq 2\log\sqrt{c_i} < \alpha_i$$

□

**Lemma 17.8.** *There exists a unit $\theta$ in $\mathcal{O}_K$, if $L(\theta) = (\theta_1, \ldots, \theta_{r+s})$, then $\theta_i < 0$ for all $i \neq k$ where $k$ is a fixed index and $L$ is the map defined in Lemma 17.7.*

*Proof.* Let $k$ be a fixed index. Let $x_1$ be any non-zero element in $\mathcal{O}_K$. Define $x_n$ inductively using Lemma 17.7 such that $x_{n+1}$ is the non-zero element in $\mathcal{O}_K$ such that

$$|N(x_{n+1}| \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$$

and the $i^{th}$ coordinate of $L(x_{n+1})$ is less than the $i^{th}$ coordinate of $x_n$ for all $i \neq k$. Hence we have a sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ such that for all $i \neq k$, the $i^{th}$ coordinate of $L(x_n)$ is decreasing and $|N(x_n)|$ is bounded by $\frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$. By Proposition 16.20, there are only finitely many integral ideals with norm less than or equal to a certain bound. Hence there exists $n$ and $r > 0$ such that

$$\langle x_n \rangle = \langle x_{n+r} \rangle$$

and so $\frac{x_{n+r}}{x_n}$ is a unit. Let $\theta = \frac{x_{n+r}}{x_n}$. Let $L(x_{n+r}) = (y_1, \ldots, y_{r+s}), L(x_n) = (z_1, \ldots, z_{r+s})$ and $y_i \leq z_i$ for all $i \neq k$. Then

$$L(\theta) = (y_1 - z_1, \ldots, y_{r+s} - z_{r+s}) = (\theta_1, \ldots, \theta_{r+s})$$

and so $\theta_i < 0$ for all $i \neq k$. □

**Lemma 17.9.** *For each index $k$, $1 \leq r + s$, let $u_k$ be the units in Lemma 17.8. Let $m = r + s$ and $A$ be the $m \times m$ matrix whose $i^{th}$ row is $L(u_o)$. Then $A$ is a real matrix, and $A_{ij} < 0$ for all $i \neq j$, and $A_{ii} > 0$ for all $i$. Moreover, The sum of each row is 0 and the rank of the matrix $A$ is $m - 1$.*

*Proof.* It is clear that $A$ is real, the sum of each row, is

$$\log \prod_{i=1}^{r+s} |\sigma_i(u_k)| = \log |N(u_k)| = 0$$

and by construction and by Lemma 17.8, $A_{ij} < 0$ for $i \neq j$, and since the sum of each row is 0, so $A_{ii} > 0$ for all $i$. Also, since the sum of each row is 0, so the vector $(1, 1, \ldots, 1)^t$ is in the kernel. Hence the rank is at most $m - 1$. We show that the rank is exactly $m - 1$.

Let $V_i$ be the $i^{th}$ column. Suppose

$$t_1 V_1 + \cdots + t_{m-1} V_{m-1} = 0$$

$t_i$ not all zero. Then pick $k \in \{1, \ldots, m-1\}$ with $t_k$ maximal. We divide both sides by $t_k$, and rewrite the above as

$$t_1 V_1 + \cdots + t_{m-1} V_{m-1} = 0, t_i \leq t_t = 1$$

Now look at the $k^{th}$ row, say $(a_{k1}, \ldots, a_{km})$. Then from the above sum, we have

$$0 = \sum_{i=1}^{m-1} t_i a_{ki} \geq \sum_{i=1}^{m-1} > \sum_{i=1}^{m} a_{ki} = 0$$

using $a_{kj} < 0$ if $j \neq k$, which is a contradiction. Hence the rank is at least $m - 1$ and so the rank is $m - 1$. □

Now we shall prove the main result of the subsection.

**Theorem 17.10.** **[Dirichlet's unit theorem]** *Let $K$ be a number field. Let $U_K$ be the set of units in $\mathcal{O}_K$. Then*

$$U_K \cong \mu_K \times (C_\infty)^{r+s-1}$$

*where $\mu_K$ is the set of roots of unity in $\mathcal{O}_K$ and $n = r + 2s$ in the usual notation.*

*Proof.* The first part of the proof is identical to that in the quadratic case. Let

$$L : \mathcal{O}_K \longmapsto \mathbb{R}^{r+s}$$

by

$$L(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \ldots, 2\log|\sigma_{r+s}(x)|)$$

It is clear that $L$ is a homomorphism. Let $x$ be a unit, then $N(x) = \pm 1$. So the image of $U_K$ under $L$ lies in the hyperplane $W$, where

$$W = \left\{ (x_1, \ldots, x_r, y_1, \ldots, y_s) \in \mathbb{R}^{r+s} : \sum_{i=1}^{r} x_i + \sum_{j=1}^{s} y_j = 0 \right\}$$

Let $B$ be a compact subset in $W$, then there exists $a \in \mathbb{R}$ such that

$$\frac{1}{a} \leq |\sigma_i(x)| \leq a$$

for all $i$ and for all $x \in L^{-1}(B)$. Since $|\sigma_i(x)|$ is bounded, and so the coefficients of the minimal polynomial of $x$ are bounded, and so there are finitely many such polynomials because the coefficients are integers. Hence there are finitely many such $x$, and so $L^{-1}(B)$ is finite and so $B \cap L(U_K)$ is finite. This shows that $L(U_K)$ is a discrete additive subgroup of $W$. Also, since $\{0\}$ is a compact subset, and so $\ker L \cap U_K$ is finite, and since $U_K$ is a multiplicative group, and the kernel of $U_K$ under $L$ is $\ker L \cap U_K$, hence

$$U_K/(\ker L \cap U_K) \cong V \subseteq W$$

where $V$ is a discrete additive subgroup. Then by Lemma 16.5 $U_K/(\ker L \cap U_K)$ is finitely generated over $\mathbb{Z}$ and some $\mathbb{Z}$-basis is linearly independent over $\mathbb{R}$. So the rank of $V$ is less than or equal to the rank of $W$, which is $r + s - 1$. So we have

$$U_K/(\ker L \cap U_K) \cong \mathbb{Z}^{\oplus m}$$

where $m \leq r + s - 1$ and so

$$U_K \cong \mathbb{Z}^{\oplus m} \oplus (\ker L \cap U_K)$$

It is clear that $\ker L \cap U_K$ is a multiplicative subgroup of $K$ and we have shown it is finite. Hence any finite subgroup of $K^*$ is cyclic, where $K$ is a field. Thus, $\ker L \cap U_K$ is cyclic. Since it contains complex numbers, and so the only finite cyclic group of complex numbers is the group consisting of roots of unity. Hence, $\ker L \cap U_K = \mu_K$.

On the other hand, by Lemma 17.9, we can find $r + s - 1$ units such that the image of them under $L$ are linearly independent over $\mathbb{R}$. Hence we conclude that $m = r + s - 1$, and so

$$U_K \cong \mu_K \times \mathbb{Z}^{\oplus m} \cong \mu_K \times (C_\infty)^m$$

□

Now, we have a way to determine the units in $\mathcal{O}_K$, and so we are able to find the integer solutions to the equation

$$x^2 + k = y^3$$

for any integer $k$. We shall see many examples in the exercise.

## 17.3 Independent units

Dirichlet's unit theorem suggests that we shall define the following concept:

**Definition 17.11.** *Let $K$ be a number field. Let $e_1, \ldots, e_k$ be units of $\mathcal{O}_K$. The units $e_1, \ldots, e_k$ are said to be* **independent** *if*

$$e_1^{r_1} \cdots e_k^{r_k} = 1 \text{ where } r_1, \ldots, r_k \in \mathbb{Z} \Rightarrow r_1 = \cdots = r_k = 0$$

**Definition 17.12.** *Let $K$ be a number field with degree $n = r + 2s$. We say $\{e_1, \ldots, e_{r+s-1}\}$ is a* **fundamental system** *of units in $\mathcal{O}_K$ if $e_1, \ldots, e_{r+s-1}$ are independent and for any unit $u \in \mathcal{O}_K$, $u$ can be* **uniquely** *expressed in the form*

$$u = \zeta e_1^{k_1} \cdots e_{r+s-1}^{k_{r+s-1}}$$

*where $\zeta$ is a root of unity in $\mathcal{O}_K$ and $k_1, \ldots, k_{r+s-1}$ are integers.*

Therefore, this allows us to redefine the fundamental unit.

**Definition 17.13.** *Let $K$ be a number field with degree $n = r + 2s$. If $r + s = 2$, then by Dirichlet's unit theorem, the set of unit*

$$U_K \cong \mu \times C_\infty$$

*Then any unit $u \in \mathcal{O}_K$ such that $\{u\}$ is a fundamental system of units for $\mathcal{O}_K$ is called a* **fundamental unit**.

The Dirichlet's unit theorem gives the structure of the set of units in $\mathcal{O}_K$, but in general, it is hard to find the fundamental system of units. We shall give two examples in the exercise. Also, the fundamental system of units is not unique. For example, if $u$ is in the system, then we replace $u$ by $u^{-1}$, the new set is also a fundamental system of units.

**Definition 17.14.** *Let $K$ be a number field of degree $n = r+2s$. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \ldots, \sigma_{r+s}$ be the complex embeddings such that*

$$\sigma_{r+j} \neq \bar{\sigma}_{r+i}$$

*for any $i \neq j$. Let $\{e_1, \ldots, e_{r+s-1}\}$ be a fundamental system of units of $\mathcal{O}_K$. Let $E$ be the $(r + s - 1) \times (r + s)$ matrix with*

$$E_{ij} = \log |\sigma_i(e_j)|, \ i = 1, 2, \ldots, r + s - 1, j = 1, 2, \ldots, r + s$$

*Let $A$ be any $r + s - 1 \times r + s - 1$ minor of $E$. Then the non-negative real number*

$$R(K) = |\det A|$$

*is called the* **regulator** *of $K$.*

The first thing to check is that the regulator is independent of the $r + s - 1 \times r + s - 1$ minor we chose.

**Proposition 17.15.** *Let $E$ be the matrix above. Let $A_i$ be the matrices formed by $E$ with the $i^{th}$ column deleted. Then for any $i \neq j$,*

$$|\det A_i| = |\det A_j|$$

*Proof.* Since the norm of unit is $\pm 1$ and so the sum of each row is $E$ is $\log 1 = 0$. Let $V_1, \dots, V_{r+s}$ be the columns of $E$. Then we can write

$$V_{r+s} = -(V_1 + \cdots + V_{r+s-1})$$

Hence, the absolute value of the determinant of any $A_i$ for $i \leq r+s-1$, can be written as:

$$|\det A_i| = |\det (V_1| \cdots |V_{i-1}|V_{i+1}| \cdots | - V_i)| = |\det A_{r+s}|$$

by swapping the $i^{th}$ column and the last column because the elementary operation does not change the determinant. Hence we have shown that for any $i$,

$$|\det A_i| = |\det A_{r+s}|$$

and so

$$|\det A_i| = |\det A_j|$$

for any $i \neq j$. □

It is nature to ask whether the regulator of $K$ depends on the choice of fundamental system of units as we have seen that the fundamental system of units is not necessarily unique.

**Proposition 17.16.** *Let $K$ be a number field. The regulator $R(K)$ is independent of the choice of basis.*

*Proof.* Let $\{e_1, \dots, e_{r+s-1}\}$, and $\{f_1, \dots, f_{r+s-1}\}$ be two fundamental systems of units. Then by definition, for any $f_j$, we have $a_j, k_{ij} \in \mathbb{Z}$ any $\zeta$ a root of unity such that

$$f_j = \zeta^{a_j} e_1^{k_{1j}} \cdots e_{r+s-1}^{k_{r+s-1j}}$$

Also, we have $b_j, m_{ij} \in \mathbb{Z}$ such that

$$e_j = \zeta^{b_j} f_1^{m_{1j}} \cdots f_{r+s-1}^{m_{r+s-1j}}$$

Hence we have

$$\begin{aligned} f_j &= \zeta^{a_j} \prod_{i=1}^{r+s-1} e_i^{k_{ij}} \\ &= \zeta^{a_j} \prod_{i=1}^{r+s-1} \left( \zeta^{b_i} \prod_{l=1}^{r+s-1} f_l^{m_{li}} \right)^{k_{ij}} \\ &= \zeta^{a_j + \sum_{i=1}^{r+s-1} k_{ij} b_i} \prod_{l=1}^{r+s-1} f_l^{\sum_{i=1}^{r+s-1} m_{li} k_{ij}} \end{aligned}$$

Then, by uniqueness of the expression, we have

$$\sum_{i=1}^{r+s-1} m_{li} k_{ij} = \begin{cases} 1 & \text{if } l = j \\ 0 & \text{if } l \neq j \end{cases}$$

Now define the matrices $A$ and $B$ by

$$A_{ij} = k_{ij}, B_{ij} = m_{ij}$$

and so

$$AB = BA = I$$

Thus

$$\det A \det B = 1$$

But the matrices $A$ and $B$ have integer entries, and so

$$|\det A| = |\det B| = 1$$

Now, let $\sigma_i$ be any embeddings. Then

$$\sigma_i(f_j) = \sigma_i\left(\zeta^{a_j}\prod_{l=1}^{r+s-1} e_l^{k_{lj}}\right) = \sigma(\zeta)^{a_j}\prod_{l=1}^{r+s-1}\sigma_i(e_l)^{k_{lj}}$$

Since the conjugate of root of unity is still a root of unity, then we have

$$|\sigma_i(f_j)| = \prod_{l=1}^{r+s-1}|\sigma_i(e_l)|^{k_{lj}}$$

and so

$$\log|\sigma_i(f_j)| = \sum_{l=1}^{r+s-1} k_{lj}\log|\sigma_i(e_l)|$$

Now let $E$ and $F$ be the $(r+s-1)\times(r+s-1)$ matrices with entries $\log|\sigma_i(e_j)|$ and $\log|\sigma_i(f_j)|$ respectively. Then from above, we have

$$F = AE$$

and so

$$|\det F| = |\det AE| = |\det E|$$

Hence the determinant (regulator) is independent of the choice of fundamental system of units. □

Now, as in the proof of Dirichlet's unit theorem, let $e_1, \ldots, e_{r+s-1}$ be $r+s-1$ units. Then define the matrix $E$ by

$$E_{ij} = \log|\sigma_i(e_j)|$$

Then if any $(r+s-1)\times(r+s-1)$ minor has non-zero determinant, then $e_1, \ldots, e_{r+s-1}$ are independent. Thus, this gives an easier way to check the independence of the units. But in general, it is still hard to check whether these independent units form a fundamental system of units. One way to check this is to check whether for each $e_i$, there exists some $f_i$ such that $e_i$ is a positive power of $f_i$. If not, then the given set forms a fundamental system of units. In fact, we could use the class number formula to find the regulator and check whether the determinant of $E$ is equal to the regulator.

**Definition 17.17.** *Let $K$ be a number field. The* **Dedekind $\zeta$-function** *$\zeta_K(s)$ is defined by:*

$$\zeta_K(s) = \sum_{0\neq I\subseteq\mathcal{O}_K}\frac{1}{N(I)^s}$$

*where the summation is over all non-zero integral ideals of $\mathcal{O}_K$.*

**Theorem 17.18. [Class number formula]** *Let $K$ be a number field with discriminant $\mathcal{D}_K$. Let $R(K)$ be the regulator of $K$ and $h(K)$ be the class number. Let $n$ be the degree of $K$ over $\mathbb{Q}$ and $n = r+2s$ in the usual notation. Let $w(K)$ be the number of roots of unity in $K$. Then*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s h(K)R(K)}{\omega(K)\cdot\sqrt{|\mathcal{D}_K|}}$$

If we can approximate the left hand side well enough, then we will be able to get a decent approximation of $h(K)R(K)$. If we can also calculate the class number, then the above formula would give a good approximation of the regulator, which helps to check whether any give $r+s-1$ units form a fundamental system of units. The proof of the theorem is not elementary and we shall discuss this later.

## 17.4 The Diophantine equation: $x(x+1)(x+2) = y(y+1)$

in this subsection we use the arithmetic of the cubic field

$$K = \mathbb{Q}(\theta), \theta^3 - 4\theta + 2 = 0$$

to determine all the solutions in integers $x$ and $y$ of the equation

$$y(y+1) = x(x+1)(x+2)$$

this is, we determine all those integers that are simultaneously a product of two consecutive integers and a product of three consecutive integers. This problem was first proposed by Edgar Emerson to Burton W.Jones and was first solved by Louis.J.Mordell. By question 3 in Exercise 16, we know that the $\mathcal{O}_K$ with $K$ defined above has an integral basis $\{1, \theta, \theta^2\}$ and has class number 1 and so it is a principal ideal domain, hence a unique factorisation domain. The fundamental system of units of $\mathcal{O}_K$ is $\{u, v\}$ where $u = \theta - 1, v = 2\theta - 1$ (see question 4.) Then we start with a couple of lemmas. Throughout this subsection, let $\theta = \theta_1, \theta_2, \theta_3$ be the roots of $x^3 - 4x + 2 = 0$.

**Lemma 17.19.** *$\theta$ is a prime in $\mathcal{O}_K$. Moreover, $4\theta - 3$ is a prime.*

*Proof.* It is clear that

$$N(\langle\theta\rangle) = |N(\theta)| = \left|\prod_{i=1}^{3} \theta_i\right| = 2$$

which is a prime. Hence $\langle\theta\rangle$ is a prime ideal and hence $\theta$ is prime.

Now the conjugates of $4\theta - 3$ are

$$4\theta_1 - 3, 4\theta_2 - 3, 4\theta_3 - 3$$

and so

$$\begin{aligned} N(4\theta - 3) &= (4\theta_1 - 3)(4\theta_2 - 3)(4\theta_3 - 3) \\ &= 64\theta_1\theta_2\theta_3 - 48(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + 36(\theta_1 + \theta_2 + \theta_3) - 27 \\ &= 64(-2) - 48(-4) + 36(0) - 27 \\ &= = 37 \end{aligned}$$

which is again a prime. Hence $4\theta - 3$ is a prime. □

**Lemma 17.20.** *The factorisation of $\langle 2\rangle$ is:*

$$\langle 2\rangle = \langle\theta\rangle^3$$

*In particular, $2 = \gamma\theta^3$ where $\gamma$ is a unit in $\mathcal{O}_K$.*

*Proof.* $\theta^3 = 4\theta - 2 = 2(2\theta - 1)$, and

$$N(2\theta - 1) = N(\frac{\theta^3}{2}) = \frac{N(\theta)^3}{8} = -1$$

and hence $2\theta - 1$ is a unit. Then

$$\langle 2\rangle = \langle\theta\rangle^3$$

and so $2 = \gamma\theta^3$ for some unit $\gamma$. □

Now in the equation

$$y(y+1) = x(x+1)(x+2)$$

we set $X = 2x + 2, Y = 2y + 1$, then we have

$$2Y^2 = X^3 - 4X + 2$$

**Lemma 17.21.** *If $(X, Y)$ is a solution to $2Y^2 = X^3 - 4X + 2$, then*

$$(X - \theta)(X^2 + \theta X + (\theta^2 - 4)) = \gamma\theta^3 Y^2$$

*In particular*

$$\langle X - \theta\rangle\langle X^2 + \theta X + (\theta^2 - 4)\rangle = 2\langle Y^2\rangle$$

*Proof.* We have

$$\begin{aligned}(X - \theta)(X^2 + \theta X + (\theta^2 - 4)) &= X^3 - 4X - \theta^3 + 4\theta \\ &= X^3 - 4X + 2 \\ &= 2Y^2 \\ &= \gamma\theta^3 Y^2\end{aligned}$$

The last part follows by $\langle\theta\rangle^3 = \langle 2\rangle$. □

**Lemma 17.22.** *The only possible primes in $\mathcal{O}_K$ which divides both $X - \theta$ and $X^2 + \theta X + (\theta^2 - 4)$ are associates of $\theta$ and $4\theta - 3$.*

*Proof.* Let $\alpha$ be a prime in $\mathcal{O}_K$ which divides both $X - \theta$ and $X^2 + \theta X + (\theta^2 - 4)$. Then $\alpha$ divides

$$\begin{aligned}(X^2 + \theta X &+ (\theta^2 - 4)) - (X + 2\theta)(X - \theta) \\ &= 3\theta^2 - 4 = \frac{3\theta^2 - 4\theta}{\theta} = \frac{8\theta - 6}{\theta} \\ &= \frac{2}{\theta}(4\theta - 3) = \gamma(4\theta - 3)\theta^2\end{aligned}$$

by Lemma 17.20. Since $\gamma$ is a unit, and $4\theta - 3$ and $\theta^2$ are both irreducible because they are prime and $\mathcal{O}_K$ is a unique factorisation domain. Hence $\alpha$ can only be the associates of $4\theta - 3$ or $\theta^2$. □

**Lemma 17.23.** *$\theta$ divides both $X-\theta$ and $X^2+X\theta+(\theta^2-4)$. Further, $\theta^2 \nmid X-\theta$, $\theta^2 | X^2+X\theta+(\theta^2-4)$ but $\theta^3 \nmid X^2 + X\theta + (\theta^2 - 4)$.*

*Proof.* As $X = 2(x+1)$ so it is even, and since $\theta|2$ (as $\langle 2\rangle = \langle\theta\rangle^3$) then $\theta|X$ and so $\theta|X-\theta$. Similarly, $\theta|X^2 + X\theta + (\theta^2 - 4)$ and $\theta^2|X^2 + X\theta + (\theta^2 - 4)$. Finally, since $\theta^2|X$ and $\theta^2 \nmid \theta$, so $\theta^2 \nmid X - \theta$, and since $\theta^3 \nmid \theta^2$, $\theta^3 \nmid X^2 + X\theta + (\theta^2 - 4)$. □

**Theorem 17.24.** *The integer solutions of the equation*

$$2Y^2 = X^3 - 4X + 2$$

*are*

$$(X, Y) = (-2, \pm 1), (0, \pm 1), (2, \pm 1)(4, \pm 5), (12, \pm 29)$$

*Proof.* Let $n$ be the order of $4\theta - 3$ in $X - \theta$, namely

$$(4\theta - 3)^n | X - \theta, (4\theta - 3)^{n+1} \nmid X - \theta$$

Now let

$$X - \theta = \theta(4\theta - 3)^n \prod_{i=1}^{r} P_i^{e_i}, X^2 + X\theta + (\theta^2 - 4) = \theta^2(4\theta - 3)^m \prod_{j=1}^{t} Q_j^{f_j}$$

be the prime factorisations. By Lemma 17.22, $P_i \neq Q_j$ for all $i, j$. Then by Lemma 17.21, we have

$$\begin{aligned}(X - \theta)(X^2 + X\theta + (\theta^2 - 4)) &= \theta^3(4\theta - 3)^{m+n} \prod_{i=1}^{r} P_i^{e_i} \prod_{j=1}^{t} Q_j^{f_j} \\ &= \gamma\theta^3 Y^2\end{aligned}$$

This shows that the indices $e_i, f_i$ must all be even, and so collect all squared terms, using the fact $\mathcal{O}_K = \mathbb{Z}[\theta]$, we may write

$$X - \theta = \theta(4\theta - 3)^A u^B v^C (a + b\theta + c\theta^2)^2$$

where $a, b, c \in \mathbb{Z}$, $A, B, C \in \{0, 1\}$. Take norms of both sides, since

$$N(X - \theta) = (X - \theta_1)(X - \theta_2)(X - \theta_3) = X^4 - 4X + 2$$

and let $Z = N(a + b\theta + c\theta^2) \in \mathbb{Z}$, and the norm of unit is $\pm 1$, we have

$$X^4 - 4X + 2 = \pm 2 \cdot 37^A \cdot Z^2$$

Since $X$ is even, let $X = 2X_1$, so

$$4X_1^3 - 4X_1 + 1 = 4(X_1^2 - 1)X_1 + 1 = \pm 37^A Z^2$$

Reduce the above equation modulo 8, and for any integer $Z$,

$$Z^2 \equiv 0, 1, 4 \pmod 8$$

It is clear that $4(X_1^2 - 1)X_1 + 1 \equiv 1 \pmod 8$, and so the required $Z$ must have

$$Z^2 \equiv \pmod 8$$

Hence

$$1 \equiv \pm 5^A \pmod 8$$

This shows that $A$ is not 1 and since $A \in \{0, 1\}$, so $A = 0$. Hence,

$$X - \theta = \pm\theta u^B v^C (a + b\theta + c\theta^2)^2$$

and expand the square, we have

$$X - \theta = \pm\theta u^B v^C ((a^2 - 4bc) + (2ab + 8bc - 2c^2)\theta + (2ac + b^2 + 4c^2)\theta^2)$$

We now discuss the four cases:

$$(B, C) = (0, 0), (0, 1), (1, 0), (1, 1)$$

(i) $(B, C) = (0, 0)$. Then we equate the coefficients of $1, \theta, \theta^2$ on both sides above, we have

$$4ac + 2b^2 + 8c^2 = \pm X$$

$$a^2 - 4bc + 4b^2 + 8ac + 16c^2 = \pm 1$$

$$ab + 4bc - c^2 = 0$$

For the second equation above, reduce both sides modulo 4, then we have the plus sign holds. Thus,

$$X = 4ac + 2b^2 + 8c^2$$

$$(a + 4c)^2 + 4b^2 - 4bc = 1$$

$$b(a + 4c) = c^2$$

If $b = 0$, then $c = 0$ and then $X = 0$. This gives the solution $(0, \pm 1)$. If $b \neq 0$, then $a + 4c = \frac{c^2}{b}$ and so

$$\frac{c^4}{b^2} + 4b^2 - 4bc = 1 \iff 3b^4 + c^4 - 4b^3 c = 0$$

Now since

$$(c-b)^2((c+b)^2+2b^2) \geq 0$$

and so

$$\frac{c^4}{b^2} + 4b^2 - 4bc \geq b^2$$

this shows that $b^2 \leq 1$. Then $b = \pm 1$ and the corresponding $(a, b, c)$ are

$$(a, b, c) = (1, 1, -3) \text{ or } (-1, -1, 3)$$

This gives $X = -2$ and $Y = \pm 1$.

(ii) Now consider the case $(B, C) = (0, 1)$. We have

$$X - \theta = \pm\theta(2\theta - 1)(a + b\theta + c\theta^2)^2$$

multiply both sides by $\theta$ and collect the term $\theta^2$ into the term $(a + b\theta + c\theta^2)^2$, we have

$$(X\theta - \theta^2) = \pm(1 - 2\theta)(a^2 - 4bc + (2ab + 8bc - 2c^2)\theta + (2ac + b^2 + 4c^2)\theta^2)$$

Equate the coefficients, we have

$$0 = a^2 - 4bc + 4(2ac + b^2 + 4c^2)$$

$$\mp X = 2ab + 8bc - 2c^2 - 2(a^2 - 4bc) - 8(2ac + b^2 + 4c^2)$$

$$\pm 1 = 2ac + b^2 + 4c^2 - 2(2ab + 8bc - 2c^2)$$

From the first equation we have $a$ is even and from the last equation we have $b$ is odd. Now consider the reduction modulo 4 of the last equation, we have the plus sign holds. Hence

$$0 = (a + 4c)^2 + 4b(b - c)$$

$$1 = a(2c - b) + b^2 - 16bc + 8c^2$$

$$x = 2a^2 + 8b^2 + 34c^2 - 2ab + 16ac - 16bc$$

Suppose $c = 2b$, then we have $b^2 = 1$ from the second equation. Let $b = 1$, then $c = 2$ and $a = -6, -10$. Then we have $X = 4$ or $X = 12$ which gives the solutions

$$(4, \pm 5), (12, \pm 29)$$

Since $-a, -b, -c$ also gives the same solution, so we do not consider the case when $b = -1$.

Suppose now $c \neq 2b$, then from the second equation above, we have

$$a = \frac{b^2 - 16bc + 8c^2 - 1}{4b - 2c}$$

and so

$$a + 4c = \frac{b^2 - 1}{4b - 2c}$$

Substitute this into the first equation, we have

$$\left(\frac{b^2 - 1}{4b - 2c}\right)^2 + 4b(b - c) = 0$$

so that

$$b^2 - 2b^2 + 1 + 16b(2b - c)^2(b - c) = 0$$

which implies that $b|1$ and so $b = \pm 1$, and so $c = \pm 1$. Then $a = \mp 4$. We have

$$(X, Y) = (2, \pm 1)$$

(iii) Now consider the case $(B, C) = (1, 0)$. We have

$$\mp(X - \theta) = (\theta - \theta)^2(a^2 - 4bc + (2ab + 8bc - 2c^2)\theta + (2ac + b^2 + 4c^2)\theta^2)$$

Equating the coefficients of $\theta$ and $\theta^2$ we have

$$\pm 1 = (a^2 - 4bc) + 6(2ac + b^2 + 4c^2) - 4(2ab + 8bc - 2c^2)$$

$$0 = (2ab + 8bc - 2c^2) - (a^2 - 4bc) - 4(2ac + b^2 + 4c^2)$$

The first equation shows that $a$ is odd, and the second equation shows that $a$ is even, which is impossible.

(iv) The last case is $(B, C) = (1, 1)$. We have

$$\pm(X - \theta) = \theta(1 - \theta)(1 - 2\theta)(a + b\theta + c\theta^2)^2$$

Multiply both sides by $\theta$ and collect the term $\theta^2$ into $(a + b\theta + c\theta^2)^2$, we may write

$$\pm(X - \theta) = (1 - 3\theta + 2\theta^2)(a^2 - 4bc + (2ab + 8bc - 2c^2)\theta + (2ac + b^2 + 4c^2)\theta^2)$$

Equate the coefficients of 1 and $\theta$, we have

$$0 = (a^2 - 4bc) + 6(2ac + b^2 + 4c^2) - 4(2ab + 8bc - 2c^2)$$

$$\mp 1 = 9(2ac + b^2 + 4c^2) - 3(2ab + 8bc - 2c^2) + 2(a^2 - 4bc)$$

The first equation shows that $a$ is even and then consider the reduction modulo 4 in the first equation, we conclude that

$$2b^2 \equiv 0 \pmod 4$$

and so $b$ is even. But the second equation shows that $b$ is odd, which is impossible.

This completes the proof. □

Therefore, from the theorem above, and $X = 2x + 2, Y = 2y + 1$, we conclude that the solutions to

$$y(y + 1) = x(x + 1)(x + 2)$$

are

$$\begin{aligned}(x, y) &= (0, 0), (0, -1), (-1, 0), (-1, -1), (-2, 0), (-2, -1), (1, 2), (1, -3) \\ &\quad (5, 14), (5, -15)\end{aligned}$$

We shall see many other examples of Diophantine equations in later chapters.

## 17.5 Exercise

1. Prove that $8 + 3\sqrt{7}$ is the fundamental solution in $\mathbb{Q}(\sqrt{7})$. Hence, find all integer solutions to the equation
$$x^2 - 7y^2 = 2$$

2. By considering the factorsation of 2 and 5 in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{26})$, find all integer solutions to the equations
$$x^2 - 26y^2 = \pm 10$$
(We only need the solutions $(x, y)$ which satisfies one of the above equations.)

3. (i) For all $x \in \mathbb{R}$ and all $\theta \in \mathbb{R}$. Show that

$$\sin^2\theta(x - 2\cos\theta)^2 < x^2 + 4$$

(ii) Let $K$ be a cubic field with one real and two complex embedding. Let $u > 1$ be the fundamental unit of $\mathcal{O}_K$. If we set the conjugates of $u$ to be $re^{i\theta}$ and $re^{-i\theta}$, show that the discriminant of $\mathbb{Z}[u]$ is

$$-4\sin^2\theta(r^3 + r^{-3} - 2\cos\theta)^2$$

Show further that the absolute value of discriminant of $\mathbb{Z}[u]$ is less than

$$4(u^3 + u^{-3} + 6)$$

(iii) If $|\mathcal{D}_K| > 32$, show that

$$\left|u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right)\right| > \frac{|\mathcal{D}_K|}{8} - \frac{15}{4}$$

Hence show that

$$u^3 > \frac{|\mathcal{D}_K| - 27}{4}$$

4. Let $K = \mathbb{Q}(\theta)$ where $\theta^3 - 4\theta + 2 = 0$. Find the factorisation of primes $2, 3, 5, 7, 11, 13$ in $\mathcal{O}_K$ and hence, using question 16 of exercise 14, and the fact (which we have proved in a previous exercise) that

$$\lim_{s\to 1^+}(s-1)\zeta(s) = 1$$

estimate the limit

$$\lim_{s\to 1^+}(s-1)\zeta_K(s)$$

Hence or otherwise, prove that $\{\theta - 1, 2\theta - 1\}$ is a system of fundamental solutions in $K$. (Hint: You may use the class number formula.)

5. Use the fact that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ for $K = \mathbb{Q}(\sqrt[3]{2})$ and question 3, show that the fundamental unit of $\mathcal{O}_K$ is $1 + \sqrt[3]{2} + (\sqrt[3]{2})^2$.

6. Let $\phi$ be the Euler's totient function (Definition 2.14). Show that, if $\phi(k) \leq n$, then $k \leq 2n^2$. Hence show that $\mathcal{O}_K$ can only contains finitely many roots of unity for any number field $K$.

7. Show that if $K$ is a number field of odd degree. Then the only roots of unity in $\mathcal{O}_K$ are $\pm 1$.

8. (i) Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$. Show that $\zeta_{12} \in \mathcal{O}_K$, where $\zeta_{12}$ is the $12^{th}$ root of unity.

(ii) Further, show that 12 is the largest integer $m$ such that $\zeta_m \in \mathcal{O}_K$ with $[K : \mathbb{Q}] = 4$.

9. Show that

$$\left\{1 + \sqrt{2}, \sqrt{2} + \sqrt{3}, \frac{1}{2}\left(\sqrt{2} + \sqrt{6}\right)\right\}$$

is a fundamental system of units for $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

10. Prove that $x^3 - x^2 + x - 2$ has only one real root $\theta$. Show further that

$$1.3 < \theta < 1.4$$

and hence show that the fundamental unit is $1 + \theta^2$.

11. Let $K$ be a number field such that $U_K$ contains a non-real root of unity. Prove that $N(\alpha > 0)$ for every $\alpha \in K \backslash \{0\}$.

The following questions are examples of $x^2 + k = y^3$ using congruence relation.

12. Consider the equation

$$x^2 = y^3 + 45$$

By considering the congruence modulo 8, show that $x$ is even and $y$ is odd. Further, by considering the congruence modulo 4 and treating the case

$$y \equiv 3 \pmod 8$$

and

$$y \equiv 7 \pmod 8$$

separately, show that the equation above has no integer solutions.
(Hint: It may be useful to observe that $45 = 72 - 27 = 18 + 27$.)

13. Using a similar argument as above, show that

$$x^2 = y^3 + 46$$

has no integer solution. Further, let

$$m \equiv 4 \pmod 8 \text{ and } n \equiv 1 \pmod 2$$

and $n$ contains prime factors $p$ with

$$p \equiv 1 \text{ or } 3 \pmod 8$$

Let $k = m^3 - 2n^2$. Show that

$$x^2 = y^3 + k$$

has no integer solution.

14. (i) Classify the prime numbers $p$ such that $(\frac{3}{p}) = 1$.

(ii) Let

$$m \equiv 3 \pmod 4 \text{ and } n \equiv \pm 2 \pmod 8$$

and $n$ contains prime factors $p$ with

$$p \equiv \pm 1 \pmod{12}$$

Let $k = m^3 + 3n^2$. Show that

$$x^2 = y^3 + k$$

has no integer solution.

Finally, we give two examples of $x^2 = y^3 + k$ with no integer solutions, checked by using algebraic approach, together with congruence approach.

15. Consider the equation
$$x^2 = y^3 + 7$$
Show that the class number $h(K)$ is prime to 3, where $K = \mathbb{Q}(\sqrt{7})$. Show that if we have an integer solution $(x, y)$, then
$$x + \sqrt{7} = u^n(a + b\sqrt{7})^3$$
where $u = 8 + 3\sqrt{7}$, $n = 0, \pm 1$ and $a, b \in \mathbb{Z}$. Show that we have no integer solutions when $n = 0$. For the case $n = \pm 1$, by considering the congruence modulo 3 and 9, show that we have no integer solutions. Hence, conclude that we have no integer solutions for $x^2 = y^3 + 7$.

16. Use a similar method as above, show that the equation
$$x^2 = y^3 + 6$$
has no integer solutions.
(Hint: you may consider the congruence modulo 9 at some stage.)

⋆ 17. This question uses a different method. We are going to show the equation
$$y^3 + 51 = x^2$$
has no integer solution. Let $Y = y^3 + 54$ and $X = x^2 + 3$.

(i) Show that $2 \nmid Y$.

(ii) Show that $3 \nmid Y$.

(ii) Show that $p \nmid Y$ for any prime number $p > 3$. Hence conclude that the equation has no integer solutions.
(Hint: You may use the fact that for any prime $p$ with $p \equiv 1 \pmod 3$, and $x^3 \equiv 2 \pmod p$ is soluble if and only if there exist integers $u$ and $v$ such that $p = u^2 + 27v^2$.)

**Remark 17.25.** *The same method shows that $x^2 - 29 = y^3$ has no integer solution by observing*
$$x^2 + 3 = y^3 + 4 \cdot 2^3$$

17. Let $K = \mathbb{Q}(\zeta_8)$ and $\mathfrak{p} = \langle 1 - \zeta_8 \rangle$. Show that $N(\mathfrak{p}) = 2$ and that complex conjugation acts trivially on $\mathcal{O}_K/\mathfrak{p}^2$. Find a fundamental unit in $K$. (Hint: You may find it useful to consider the fundamental unit in the real quadratic subfield.)

## 17.6 Hint and Solutions

1. The fundamental unit in a quadratic field can be found by using the continued fraction because we have proved that any solution to
$$x^2 - my^2 = \pm 1$$
is the convergent $x = p_n, y = q_n$ for the continued fraction of $\sqrt{m}$. Thus, the first such pair of convergent gives the smallest solution, and so is the fundamental unit. Thus, $8 + 3\sqrt{7}$ is the fundamental unit.

It is a simple matter to check that the class group is a trivial group. Thus, we have

$$\langle x+\sqrt{7}y\rangle\langle x-\sqrt{7}y\rangle = \langle 2\rangle = P\bar{P}$$

where we use Kummer-Dedekind to conclude $P = \langle 2, 1+\sqrt{7}\rangle = \langle 3+\sqrt{7}\rangle$. So

$$\langle x+\sqrt{7}y\rangle = P \text{ or } P\bar{P}$$

and so

$$x+\sqrt{7}y = u(3\pm\sqrt{7})$$

Now by Dirichlet's theorem, $u = \pm(8+3\sqrt{7})^n$ and so the solutions are given by

$$x+\sqrt{-7}y = \pm(8+3\sqrt{7})^n(3\pm\sqrt{7})$$

2. It is clear that $\alpha = 5+\sqrt{26}$ is a fundamental unit. By Kummer-Dedekind, we have

$$\langle 2\rangle = \langle 2, \sqrt{26}\rangle^2 = P^2, \langle 5\rangle = \langle 5, 1+\sqrt{26}\rangle\langle 5, 1-\sqrt{-26}\rangle = Q\bar{Q}$$

Hence, from

$$\langle x+\sqrt{26}\rangle\langle x-\sqrt{26}\rangle = \langle 2\rangle\langle 5\rangle$$

we deduce that

$$\langle x+\sqrt{-26}\rangle = PQ \text{ or } P\bar{Q}$$

It is easy to check that

$$PQ = \langle \alpha+1\rangle \text{ and } P\bar{Q} = \langle \alpha-1\rangle$$

Hence the solutions are given by

$$x+\sqrt{26} = \pm\alpha^n(\alpha\pm 1)$$

3. (i) Let

$$\begin{aligned} f(x) &= x^2+4-\sin^2\theta(x-2\cos\theta)^2 \\ &= x^2\cos^2\theta + 4\sin^2\theta\cos\theta x - 4\cos^2\theta\sin^2\theta + 4 \end{aligned}$$

If $\cos\theta = 0$, then $f(x) = 4 > 0$. If not, then the at minimum point, $x = 2\frac{\sin^2\theta}{\cos\theta}$. We have the minimum,

$$4-4\cos^2\theta\sin^2\theta - 4\sin^4\theta = 4\cos^2\theta > 0$$

Hence $f(x) > 0$ for all $x \in \mathbb{R}$ and $\theta \in \mathbb{R}$.

(ii) The discriminant is

$$\begin{vmatrix} 1 & u & u^2 \\ 1 & re^{i\theta} & r^2e^{2i\theta} \\ 1 & ue^{-i\theta} & ue^{-2i\theta} \end{vmatrix}^2 \tag{1}$$

Also the norm of $u$ is $\pm 1$, and so

$$ur^2 = \pm 1$$

Since $u$ and $r > 0$, os $u = \frac{1}{r^2}$. Hence, we conclude that the discriminant is

$$-4\sin^2\theta(r^3+r^{-3}-2\cos\theta)^2$$

Now by (i), we have

$$4\sin^2\theta(r^3+r^{-3}-2\cos\theta)^2 < 4((r^3+r^{-3})^2+4) = 4(u^3+u^{-3}+6)$$

(iii) Now as $u \in \mathcal{O}_K$, so

$$|\mathcal{D}_K| \leq |D(\mathbb{Z}[u])| < 4(u^3 + u^{-3} + 6)$$

Hence,

$$u^6 - \left(\frac{|\mathcal{D}_K|}{4} - 6\right) u^3 + 1 > 0$$

Now complete the square, we have

$$\left(u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right)\right)^2 > \left(\frac{|\mathcal{D}_K|}{8} - 3\right)^2 - 1$$

Now, as $|\mathcal{D}_K| > 32$, so $\frac{|\mathcal{D}_K|}{8} - 3 > 1$, and so

$$\left(\frac{|\mathcal{D}_K|}{8} - 3\right)^2 > \left(\frac{\mathcal{D}_K}{8} - \frac{15}{4}\right)^2$$

Therefore, we have

$$\left|u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right)\right| > \frac{|\mathcal{D}_K|}{8} - \frac{15}{4}$$

If

$$u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right) < 0$$

then we end up with $u^3 < \frac{15}{4} - 3 < 1$, which is a contradiction. Hence

$$u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right) \geq 0$$

and so

$$u^3 > \frac{|\mathcal{D}_K| - 27}{4}$$

4. We have seen in the previous exercise that the ring of integers $\mathcal{O}_K = \mathbb{Z}[\theta]$, and the discriminant is $148 > 0$. Hence all roots of $x^3 - 4x + 2$ are real and so $r = 3, s = 0$ and $r + s - 1 = 2$. Thus, we may apply Kummer-Dedekind to factorises the prime numbers in $\mathcal{O}_K$. It is clear that

$$\langle 2 \rangle = \langle \theta \rangle^3$$

$$\langle 3 \rangle \text{ is prime}$$

$$\langle 5 \rangle = P_5 Q_5 \text{ where } N(P_5) = 5, N(Q_5) = 25$$

$$\langle 7 \rangle \text{ is prime}$$

$$\langle 11 \rangle \text{ is prime}$$

$$\langle 13 \rangle = P_{13} Q_{13} \text{ where } N(P_{13}) = 13, N(Q_{13}) = 169$$

Now by question 16 of exercise 14, we have

$$\zeta_K(s) = \prod_P \frac{1}{1 - (N(P))^{-s}}$$

where the product is over all prime ideals. The first few terms of the $\zeta$-function gives

$$\frac{1}{1 - 2^{-s}} \frac{1}{1 - 3^{-s}} \frac{1}{1 - 5^{-s}} \cdots$$

and the first few terms of the Dedekind $\zeta$-function is, by above

$$\frac{1}{1-2^{-s}}\frac{1}{1-27^{-s}}\frac{1}{1-5^{-s}}\frac{1}{1-25^{-s}}\cdots$$

Since the limit $(s-1)\zeta(s)$ is 1 when $s \to 1^+$ and so the limit $(s-1)\zeta_K(s)$ is the quotient of the Dedekind $\zeta$-function to the (usual) $\zeta$-function, and so it is roughly:

$$\frac{1-3^{-1}}{1-27^{-1}}\frac{1}{1-25^{-1}}\frac{1-7^{-1}}{1-343^{-1}}\frac{1-11^{-1}}{1-1331^{-1}}\frac{1}{1-169^{-1}}$$

which is roughly about 0.56736. This gives an estimate of the limit $(s-1)\zeta_K(s)$ because the later terms contain large denominator and so the quotient is very small.

Now let the matrix $E$ be:

$$E = \begin{pmatrix} \log|\theta - 1| & \log|\theta' - 1| \\ \log|2\theta - 1| & \log|2\theta' - 1| \end{pmatrix}$$

Where $\theta'$ is another root of $\theta$. Let $\theta$ be any root. Take one of the root, say $-2.2143$ and let $\theta' = 1.6751$ (worked out by computer). Then

$$|\det E| = 1.6624$$

Now use the approximation of the limit

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = 0.56736$$

and the class number is 2, the number of roots of unity is 2, we then estimate the regulator by the class number formula, which gives

$$R(K) = \frac{0.56736 \cdot 2 \cdot \sqrt{148}}{8} = 1.7255$$

Now if $\{\theta - 1, 2\theta - 1\}$ is not a fundamental system of units, then the determinant of $E$ is at least twice the regulator, which is impossible. Hence we conclude that $\{\theta - 1, 2\theta - 1\}$ is a fundamental system of units.

5. Write $\alpha = \sqrt[3]{2}$. The usual trick of these question is to use the result of question 3 and show that $1 < 1 + \alpha + \alpha^2 < u^2$ where $u$ is the fundamental unit and hence conclude that $u = 1 + \alpha + \alpha^2$. It is clear that

$$(1 + \alpha + \alpha^2)(\alpha - 1) = 1$$

so that $1 + \alpha + \alpha^2$ is a unit. Also, the discriminant is $-108$ and so we have one real roots and two non-real roots. Thus, $r + s - 1 = 1$. By question 3, we have

$$u^3 > \frac{108 - 27}{4} = \frac{81}{4} > 20$$

and so $u^2 > 20^{\frac{2}{3}}$. Since

$$1 < v = 1 + \alpha + \alpha^2 < 1 + 2 + 4 = 7 < 20^{\frac{2}{3}}$$

Hence

$$1 < v < u^2$$

But $u$ is the fundamental unit, and so $v = u^n$. Then $n = 1$ and so $u = v = 1 + \alpha + \alpha^2$.

6. Let
$$k = \prod_{i=1}^{n} p_i^{e_i} \prod_{j=1}^{m} q_j$$
where $p_i, q_j$ are distinct prime numbers and $e_i \geq 2$. Then
$$\phi(k) = \prod_{i=1}^{n} p_i^{e_i-1}(p_i - 1) \prod_{j=1}^{m} (q_j - 1)$$
and so
$$\frac{2(\phi(k))^2}{k} = \left( \prod_{i=1}^{n} p^{2e_i-3}(p_i - 1) \right) \left( \prod_{j=1}^{m} 2\frac{(q_j - 1)^2}{q_j} \right) = AB$$
It is clear that since $e_i \geq 2$, so $A \geq 1$. For $B$, if $q_j \geq 2$, then $\frac{(q_j-1)^2}{q_j} \geq 1$, and if $q_j = 1$, then $2\frac{(q_j-1)^2}{q_j} \geq 1$. Hence
$$2\phi(k)^2 \geq k$$
and since $\phi(k) \leq n$, so $k \leq 2n^2$.
Let $K$ be a number field with $[K : \mathbb{Q}] = n$. If $\zeta_k \in \mathcal{O}_K$, then $\mathbb{Q}(\zeta_k) \subseteq K$ and so
$$\phi(k) = [\mathbb{Q}(\zeta_k) : \mathbb{Q}] \leq [K : \mathbb{Q}] = n$$
and so $k \leq 2n^2$. So it contains at most $\zeta_1, \ldots, \zeta_{2n^2}$.

7. Let $K$ be a number field with $[K : \mathbb{Q}] = n$ where $n$ is odd. If $\zeta_k \in \mathcal{O}_K$, then $\mathbb{Q}(\zeta_k) \subseteq K$ and so by Tower Law:
$$n = [K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_k)][\mathbb{Q}(\zeta_k) : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_k)]\phi(k)$$
and so $\phi(k)|n$. If $k \geq 3$, let
$$k = \prod_{i=1}^{n} p_i^{e_i}$$
then
$$\phi(k) = \prod_{i=1}^{n} p_i^{e_i-1}(p_i - 1)$$
It is clear that when $k \geq 3$, $\phi(k)$ is even. Hence $\phi(k)|n$ can hold if and only if $k = 2$ because $n$ is odd and when $k = 2$, $\zeta_2 = -1$.

8. (i) $\zeta_{12}$ satisfies $x^12 - 1 = 0$ and so it lies in $\mathcal{O}_K$ if it lies in $K$. Also
$$\zeta_{12} = e^{\frac{\pi i}{6}} = \frac{1}{2} + \frac{i\sqrt{3}}{2} \in K$$
(ii) If $\zeta_k \in K$, then $\mathbb{Q}(\zeta_k) \subseteq K$ and so $\phi(k)|4$ by Tower Law. If $\phi(k) = 1$, then $k = 2$. If $\phi(k) = 2$, then let $k = 4, 6$. If $\phi(k) = 4$, then let
$$k = \prod_{i=1}^{m} p_i^{e_i}$$
and so
$$4 = \prod_{i=1}^{m} p_i^{e_i-1}(p_i - 1)$$

$p_i - 1|4$ so $p_i = 2, 3, 5$. Also we cannot have three distinct prime factors, so we conclude that $k = 5, 8, 10, 12$ and so the largest one is 12.

9. It is easy to check they are independent (either by direct argument or calculate the discriminant of the matrix which consists the logarithm of the absolute value of the conjugates). So for each of them, in this case, it might be easier to check that for each of them, it is not a positive power of some other units in $\mathcal{O}_K$. For example, if $\sqrt{2} + \sqrt{3} = u^n$ for some $n \geq 2$ and some unit $u$. Then let
$$\alpha^n = (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})^n = \sqrt{2} + \sqrt{3}$$
where $a, b, c, d \in \mathbb{Q}$. Since the minimal polynomial of $\sqrt{2} + 3$ is
$$x^4 - 10x^2 + 1 = 0$$
and so $\alpha$ satisfies the equation
$$x^{4n} - 10x^{2n} + 1 = 0$$

10. Let $f(x) = x^3 - x^2 + x - 2$. Then $f(1.3) < 0$ and $f(1.4) > 0$ so $1.3 < \theta < 1.4$. Moreover, let $y = x - \frac{1}{3}$ and so $f(y) = y^3 + \frac{2}{3}y - \frac{47}{27}$. So the discriminant is
$$disc(f) = -4(\frac{2}{3})^3 - 27(\frac{47}{27})^2 = -83 < 0$$
so it has only one real root. Then $r + s - 1 = 1$ and so we have a fundamental unit. Since $\theta^3 - \theta^2 + \theta - 2 = 0$, so we have
$$(1 + \theta^2)(\theta - 1) = 1$$
and so $1 + \theta^2$ is a unit. By question 3, if $u$ is the fundamental unit, then
$$u^3 > \frac{83 - 27}{4} = 14$$
and so $u^2 > 14^{\frac{2}{3}}$. It is clear that $1 + \theta^2 < 5$ and $5^3 < 14^2$, so
$$1 < 1 + \theta^2 < u^2$$
and hence $1 + \theta^2 = u$.

11. Consider the norm of $\alpha$, $N_{K/\mathbb{Q}}(\alpha)$. Let $f(x)$ be the minimal polynomial of $\alpha$. If $\alpha_k = a + bi$ is a non-real conjugate of $\alpha$ then $a - bi$ is also a conjugate of $\alpha$ because it is a root of $f(x)$ and hence $(a + bi)(a - bi) = a^2 + b^2 > 0$. Therefore, if $n = r + 2s$, then
$$N(\alpha) = \prod_{i=1}^{r} \alpha_i \prod_{j=1}^{s} |\alpha_j|^2$$
It is clear that each $|\alpha_j|^2 > 0$, and so we focus on the first term. Suppose we have no real conjugate, then we are done. Suppose we have one, say $\beta$, then let $L = \mathbb{Q}(\zeta_k)$ where $\zeta_k \in K$. Let $g(x)$ be the minimal polynomial of $\beta$ in $L$. If the coefficients of $g(x)$ are not real. Let $h(x) = g(x) - \overline{g(x)}$, then $h(\beta) = 0$ but $h(x) \not\equiv 0$. Hence $\beta$ satisfies a polynomial of smaller degree, which is a contradiction. Hence $g(x)$ is a real polynomial, and in particular the constant term is real. Hence
$$a = N_{K/L}(\beta) \in \mathbb{R}$$
Now
$$N_{K/\mathbb{Q}}(\beta) = N_{L/\mathbb{Q}} N_{K/L}(\beta)$$

Let $\sigma$ be an element in $Aut_{\mathbb{Q}(L)}$. Since $\sigma$ send $\zeta_k$ to $\zeta_k^j$ for some $j$ which is prime to $k$, so $\sigma$ sends $\zeta_k^{-1}$ to $\zeta_k^{-j}$. This implies that $\sigma$ fixes every real number in $L$ (in fact, we can see from this argument that $a$ must already be an integer.) and hence

$$N_{L/\mathbb{Q}}(a) = a^{\phi(k)}$$

But $\phi(k)$ is even for any $k \geq 3$ and since $N(\alpha) = N(\beta)$, we have

$$N(\alpha) = N(\beta) = a^{\phi(k)} > 0$$

12. Suppose $y$ is even, then consider the congruence modulo 8, we have

$$x^2 \equiv 5 \pmod 8$$

which is impossible. Hence $y$ is odd and $x$ is even. Then consider the congruence modulo 4, we have

$$x^2 \equiv 1 + y^3 \pmod 4$$

and so

$$y \equiv 3 \pmod 4$$

We will treat the cases $y \equiv 3 \pmod 8$ and $y \equiv 3 \pmod 8$ separately. If $y \equiv 3 \pmod 8$, then

$$x^2 - 72 = y^3 - 27 = (y-3)(y^2+3y+9)$$

It is clear that $y^2 + 3y + 9 \equiv 3 \pmod 8$ and so there exists a prime factor $p$ of $y^2 + 3y + 9$ such that

$$p \equiv \pm 3 \pmod 8$$

Hence

$$x^2 \equiv 72 \pmod p$$

and so

$$\left(\frac{72}{p}\right) = \left(\frac{2}{p}\right) = 1$$

which is impossible.

If $y \equiv 7 \pmod 8$. Then

$$x^2 - 18 = y^3 + 27 = (y+3)(y^2-3y+9)$$

Then $y^2 - 3y + 9 \equiv -3 \pmod 8$, and so there exists a prime factor $p$ of $y^2 - 3y + 9$ such that

$$p \equiv \pm 3 \pmod 8$$

Hence

$$x^2 \equiv 18 \pmod p$$

and so

$$\left(\frac{18}{p}\right) = \left(\frac{2}{p}\right) = 1$$

which is impossible. Hence we have no integer solutions.

13. If $x$ is even then $y$ is even, and so $4|x, y$, but $4 \nmid 46$ which is a contradiction. Hence $x$ is odd and $y$ is odd. Consider the congruence modulo 8, we have $y \equiv 3 \pmod 8$. Then we write

$$x^2 + 18 = y^3 + 64 = (y+4)(y^2 - 4y + 16)$$

Then (mod 8) and $y^2 - 4y + 16 \equiv -3 \pmod 8$. We have at least one of the prime factor $p$ which is 5 or 7 (mod 8). Then

$$x^2 + 18 \equiv 0 \pmod p$$

and so

$$\left(\frac{-18}{p}\right) = \left(\frac{-2}{p}\right) = 1$$

which is impossible. Hence it has no integer solutions.

We have

$$x^2 = y^3 + m^3 - 2n^2$$

If $x$ is even, then $y$ is even and so $4|x^2, y^3, m^3$, but $4 \nmid 2n^2$ because $n$ is odd. Hence $x$ and $y$ are both odd. Since $x^2 \equiv 1 \pmod 8$, $8|m^3$ and then reduce the above modulo 8, and $2n^2 \equiv 2 \pmod 8$, so we conclude that

$$y \equiv y^3 \equiv 3 \pmod 8$$

Now write

$$x^2 + 2n^2 = y^3 + m^3 = (y+m)(y^2 - my + m^2)$$

and $y^2 - my + m^2 \equiv -3 \pmod 8$, so we have some prime factor $p$ which is 5 or 7 (mod 8). Then

$$x^2 + 2n^2 \equiv 0 \pmod p$$

Since any factor dividing $n$ is 1 or 3 mod 8, so $p \nmid n$ and so

$$\left(\frac{-2n^2}{p}\right) = \left(\frac{-2}{p}\right) = 1$$

which is impossible. Hence we have no integer solutions.

14. (i) Let $(\frac{3}{p}) = 1$, then if $p \equiv 1 \pmod 4$, then $(\frac{p}{3}) = 1$ and so $p \equiv 1 \bmod 3$, which gives

$$p \equiv 1 \pmod{12}$$

If $p \equiv -1 \pmod 4$, then $(\frac{p}{3}) = -1$ and so $p \equiv -1 \bmod 3$, which gives

$$p \equiv -1 \pmod{12}$$

Hence,

$$p \equiv \pm 1 \pmod{12}$$

(ii) If $y$ is even, then $x$ is odd, since $m^3 \equiv 3 \pmod 4$, and $n^2 \equiv 0 \pmod 4$, then consider the congruence modulo 4, we have

$$1 \equiv 3 \pmod 4$$

which is impossible. Hence $y$ is odd and $x$ is even. By considering the congruence modulo 4, we have $y \equiv 1 \pmod 4$. Then write

$$x^2 = (y+m)(y^2 - my + m^2) + 3n^2$$

It is clear that $y^2 - my + m^2 \equiv 3 \pmod 4$. Now since $y^2 - my + m^2$ is symmetric in $y, m$ we consider

$$(y, m) \equiv (0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2) \pmod 3$$

and then we have $y^2 - my + m^2 \equiv 0$ or $1 \pmod 3$. But when $y^2 - my + m^2 \equiv 0 \pmod 3$, we have $(y, m) = (0, 0), (2, 1)$ which gives $3|y + m$, and so

$$9|y^3 + m^3$$

This implies that $9|x^2 - 3n^2$ and hence $3|x$ and so $9|x^2$. But the only prime factors of $n$ are $\pm 1 \pmod{12}$ and so $3 \nmid n$. Therefore, $9 \nmid x^2 - 3n^2$, which is a contradiction. Hence we conclude that

$$y^2 - my + m^2 \equiv 1 \pmod 3$$

and so

$$y^2 - my + m^2 \equiv -5 \pmod{12}$$

This shows that we must have some prime factor $p$ of $y^2 - my + m^2$ such that

$$p \equiv \pm 5 \pmod{12}$$

Hence, $p \nmid n$, and

$$x^2 \equiv 3n^2 \pmod p$$

and so

$$\left(\frac{3n^2}{p}\right) = \left(\frac{3}{p}\right) = 1$$

which is impossible by (i). Therefore we have no integer solutions.

15. We have $n = 2, r = 2, s = 0, \mathcal{D}_K = 28$ and so the Minkowski bound

$$c_K = \sqrt{7} < 3$$

Since $2|28$ so 2 ramifies and so

$$\langle 2 \rangle = P^2 = \langle 2, \sqrt{7} \rangle^2$$

So the class number is either 1 or 2, which is prime to 3. Hence, by the usual argument, we have

$$x + \sqrt{7} = \pm u^n (a + b\sqrt{7})^3$$

where $u$ is the fundamental unit and $n \in \mathbb{Z}$. It is clear that $u = 8 + 3\sqrt{7}$. Now, since $(-1) = (-1)^3$, and we absorb the cubic factors in to $(a + b\sqrt{7})^3$, so we have

$$x + \sqrt{7} = u^n (a + b\sqrt{7})^3$$

where $u = 8 + 3\sqrt{7}$ and $n = 0, \pm 1$.

When $n = 0$, compare the coefficient of $\sqrt{7}$, we have

$$1 = b(3a^2 + 7b^2)$$

which is impossible. So we have no integer solutions when $n = 0$.

When $n = \pm 1$, compare the coefficients of $\sqrt{7}$, we have

$$1 = 8b(3a^2 + 7b^2) \pm 3(a^3 + 21b^2)$$

Consider the congruence modulo 3, we have

$$1 \equiv 2b^3 \pmod 3$$

and so

$$b \equiv -1 \pmod 3$$

Then

$$b^3 \equiv -1 \pmod 9$$

Thus, consider the congruence modulo 9, we have

$$1 \equiv 3a^2 + 7 \pm 3a^3 \pmod 9$$

If $3|a$, then $9|a^2, 3a^3$, which then implies that $0 \equiv 6 \pmod 9$, and this is impossible. So $a^2 \equiv 1 \pmod 3$ and so $3a^2 \equiv 3 \pmod 9$ and $3a^3 \equiv 3a \pmod 9$, so we have

$$1 \equiv 1 \pm 3a \pmod 9$$

which is impossible.

16. We have $n = r = 2, s = 0, \mathcal{D}_K = 24$ and so the Minkowski bound

$$c_K = \frac{1}{2}\sqrt{24} = \sqrt{6} < 3$$

Since $2|24$ and so 2 ramifies. Hence the class number is either 1 or 2, which is prime to 3. The fundamental unit is $u = 5 + 2\sqrt{6}$ and so we may write

$$x + \sqrt{6} = u^n(a + b\sqrt{6})^3$$

where $n = 0, \pm 1$ and $a, b \in \mathbb{Z}$. When $n = 0$, compare the coefficient of $\sqrt{6}$, we have

$$1 = b(3a^2 + 6b^2)$$

which has no integer solution as $3|3a^2 + 6b^2$ but $3 \nmid 1$.

When $n = \pm 1$, compare the coefficient of $\sqrt{6}$, we have

$$1 = 5b(3a^2 + 6b^2) \pm 2(a^3 + 18ab^2)$$

Consider the congruence modulo 3, it is clear that $3 \nmid a$. So $a^2 \equiv 1 \pmod 3$ and $3a^2 \equiv 3 \pmod 9$. Also, if $3|b$, then consider the congruence modulo 9, we have

$$1 = \pm 2a^3 \pmod 9$$

But $a^3 \equiv 0, 1, 8 \pmod 9$ and so $\pm 2a^3$ can only be $0, 2, 7$ modulo 9, which is a contradiction. So $3 \nmid b$ and so $3b^2 \equiv 3 \pmod 9$. Therefore, reduce the above modulo 9, we have

$$1 \equiv 6b + 3b \pm 2a^3 \equiv \pm 2a^3 \ (\text{ mod}9)$$

which again is a contradiction. Therefore, the equation has no integer solutions.

17. (i) Suppose $2|Y$, then $2|y^3 + 54$ and so $2|y$. Consider the congruence modulo 8, since $8|y^3$, and $54 \equiv 6 \pmod 8$, we have

$$x^2 + 3 \equiv 6 \pmod 8 \Rightarrow x^2 \equiv 3 \pmod 8$$

which is impossible.

(ii) Suppose $3|Y$, then $3|y^3+54$ and so $3|y$. Then $27|y^3+54$ so $27|X=x^2+3$, which is impossible.

(iii) Now pick any prime number $p>3$. Suppose $p|Y=y^3+54$, then $p|x^2+3$ and so

$$\left(\frac{-3}{p}\right)=1$$

because $p>3$. This implies that

$$p\equiv 1 \pmod 3$$

Then $X=Y=y^3+54=x^2+3$ is a product of prime numbers which are congruent to 1 modulo 3. Then there exists $t$ such that

$$3t\equiv 1 \pmod p$$

Further, since $X=Y$ and so $p|x^2+3$, therefore, multiply both sides by $t^3$ we have

$$t^3y^3+54t^3=x^2t^3+3t^3$$

and since $54=2\cdot 3^3$, reduce the above modulo $p$, we have

$$(-ty)^3\equiv 2 \pmod p$$

and so by the hint we have $u$ and $v$ such that

$$p=u^2+27v^2$$

It is also clear that

$$(u_1^2+27v_1^2)(u_2^2+27v_2^2)=(u_1u_2-27v_1v_2)^2+27(u_1v_2+u_2v_1)^2$$

Hence as $X,Y$ are products of such $p$, we conclude that there exists integers $u$ and $v$ such that

$$X=Y=u^2+27v^2$$

Let $\omega$ be the third root of unit. Then since $\mathbb{Z}[\omega]$ is a unique factorisation domain, and $x^2+3=u^2+27v^2$, we have

$$\pm(x+\sqrt{-3})\omega^n=u+3v\sqrt{-3}$$

where $n=0,1,-1$ as $\omega,\omega^{-1},1$ are the only units in $\mathbb{Z}[\omega]$. (By Dirichlet's unit theorem, $r=0,s=1$ and so the only units in $\mathbb{Z}[\omega]$ are the roots of unity.) If $n=0$, then $3v=1$ which is impossible. If $n=\pm 1$, then $\omega=\frac{-1+i\sqrt{3}}{2}$ and so we have

$$\pm\frac{1}{2}\left(-x\mp 3+(\pm x-1)\sqrt{-3}\right)$$

Then compare the coefficient of $\sqrt{-3}$, we conclude that $\pm x-1$ is even and so $x+1$ is even. Then $x$ is odd and so $X=x^2+3$ is even. But $X=Y$, so $Y$ is even, which is impossible by the first part. Therefore, we have no prime factors $p$ of $Y$ such that $p>3$. Hence, combine all three parts, we conclude that we have no prime factors of $Y=y^3+54$ and so $Y=\pm 1$, but this is clearly impossible. Therefore, we have no integer solutions.

18. $[K : \mathbb{Q}] = 4$. Let $f(X) := (X - \zeta_8)(X - \zeta_8^3)(X - \zeta_8^5)(X - \zeta_8^7) = X^4 + 1$. $N(1 - \zeta_8) = (1 - \zeta_8)(1 - \zeta_8^3)(1 - \zeta_8^5)(1 - \zeta_8^7) = f(1) = 2$. So $N(\mathfrak{p}) = 2$. $\mathfrak{p}^2$ has norm 4.

Note that $0, 1, \zeta_8, 1 - \zeta_8$ are distinct elements in $\mathcal{O}_K/\mathfrak{p}^2$ (by considering the differences of them, which are not in $\mathfrak{p}^2$). So $\mathcal{O}_K/\mathfrak{p}^2 = \{0, 1, \zeta_8, 1 - \zeta_8\}$. We have $(1 - \zeta_8)^2 = (1 + i)(1 - \sqrt{2}) = \sqrt{2}\frac{1+i}{\sqrt{2}}(1 - \sqrt{2})$ where $\frac{1+i}{\sqrt{2}}(1 - \sqrt{2})$ is a unit. Since $\zeta_8 - \zeta_8^{-1} = i\sqrt{2}$ so $\zeta_8 \equiv \zeta_8^{-1} \bmod \mathfrak{p}^2$. So complex conjugation acts trivially.

We have 2 pairs of complex embeddings and so by Dirichlet's theorem the rank of the unit group of $K$ is 1, which is the same as the rank of the unit group of $\mathbb{Q}(\sqrt{2})$. The unit group of $K$ is isomorphic to $T \times \mathbb{Z}$ where $T$ is finite and in this case $T \cong \mu_8$. The unit group of $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$, generated by $1 + \sqrt{2}$. Then $1 + \sqrt{2}$ must be $\alpha^n$ for some generator $\alpha$ of the free part of the unit group of $K$, and some positive integer $n \geq 1$. We can write $\alpha = \zeta\alpha'$ where $\alpha'$ is real and $\zeta$ is some $n$th root of unity (because $\alpha^n$ is real). $\alpha'^2 = \alpha\bar{\alpha} \in K$. Suppose $n$ is odd then $\alpha'^n = \alpha^n = 1 + \sqrt{2} \in K$ and $\alpha'^2 \in K$ implies that $\alpha' \in K$. Since $\alpha'$ is a real unit so $n = 1$ and $\zeta = 1$.

Suppose $n$ is even, say $n = 2m$. Then

$$1 + \sqrt{2} = \alpha'^{2m} = (\alpha'^2)^m.$$

As $\alpha'^2$ is a real unit in $K$, so $m$ can only be 1. In this case $\alpha^2 = 1 + \sqrt{2}$ and so $\zeta = \pm 1$. So this shows that $\alpha' = \alpha/\zeta \in K$ and so $\alpha' \in \mathbb{Q}(\sqrt{2})$. Thus we cannot have $\alpha'^2 = 1 + \sqrt{2}$.

So we conclude that $n = 1$ and the units in $K$ are $\zeta_8^j(1 + \sqrt{2})^n, n \in \mathbb{Z}$.

# 18 Gauss and Jacobi sums

We have seen that if $p$ is a prime which is congruent to 1 mod 4, then there exist integers $x$ and $y$ such that

$$x^2 + y^2 = p$$

In this chapter, we are going to discuss the representation of integers as sum of squares and Gauss sum which will be defined later. Before going into the details, we shall firstly introduce the concept of some basic representation theory.

## 18.1 Representation and character

**Definition 18.1.** *Let $G$ be a finite group. Let $V$ be a finite dimensional vector space over $F$, where $F$ is a field. A* **linear representation** *$\rho$ is a group homomorphism from $G$ to $GL(V)$ where $GL(V)$ is the general linear group (consisting all non-singular endomorphism of $V$). In other words,*

$$\rho(g_1)\rho(g_2)(v) = \rho(g_1 g_2)(v) \ \forall v \in V$$

*The* **dimension** *or* **degree** *of $\rho$ is the dimension of $V$.*

**Definition 18.2.** *We say a representation $\rho$ of $G$ is faithful if the kernel is trivial.*

As far as this book is concerned, we shall assume the field $F$ above is $\mathbb{C}$ unless otherwise stated.

**Definition 18.3.** *Let $G$ be a finite group and $\rho$ is a representation of $G$. Then for each $g \in G$, $\rho(g)$ is a linear map. The* **character** *$\chi$ for $\rho$ is defined as:*

$$\chi(g) = Tr(\rho(g))$$

*where $Tr(\rho(g))$ is the trace of the linear map $\rho(g)$.*

It is clear that, if $V$ is a one-dimensional vector space over $\mathbb{C}$, then $V = \mathbb{C}$, and so the trace $\chi(g)$ is the same as $\rho(g)$. For convention, we define

**Definition 18.4.** *Let $G$ be a finite group. We say $\chi$ is a linear character of $G$ if $\chi$ is the trace of $\rho$, where $\rho$ is a one-dimensional representation of $G$. Further, we say $\chi$ is a character (mod $m$) if $\chi$ is a linear character of $G$, where $G = (\mathbb{Z}/m\mathbb{Z})^*$.*

We shall also define the Dirichlet character which we shall use later to prove the Dirichlet's theorem.

**Definition 18.5.** *A* **Dirichlet character** *(mod $m$) is a function $\chi$ mapping integers into the complex numbers such that*

*(i)* $\chi(a) \neq 0$ *if and only if* $(a, m) = 1$.

*(ii)* $a \equiv b \pmod{m} \Rightarrow \chi(a) = \chi(b)$.

*(iii)* $\chi(ab) = \chi(a)\chi(b)$.

*In particular, if we restrict the domain to a reduced residue system (mod $m$), then we obtain a linear character of $(\mathbb{Z}/m\mathbb{Z})^*$.*

**Definition 18.6.** *For any character $\chi$, define the complex conjugate $\bar{\chi}$ by*

$$\bar{\chi}(g) = \overline{\chi(g)}$$

We shall develop some basic properties of characters

**Lemma 18.7.** *Let $\chi$ be a (general) character of a finite group $G$ with identity $e$ and $\chi_m$ a character (mod $m$). Then*

*(i) $\chi(e)$ is the dimension of representation $\rho$ whose character is $\chi$. In particular, $\chi_m(1) = 1$.*

*(ii) If $(a, m) = 1$, then $\chi_m(a)$ is a $\phi(m)$ root of unity with order.*

*(iii) The conjugate $\bar{\chi}$ is also a character. In particular, the conjugate $\bar{\chi}_m$ is a character (mod $m$).*

*(iv) For any $g \in G$, $\bar{\chi}(g) = \chi(g^{-1})$.*

*Proof.* Let $\rho$ be a representation of $G$ affording the character $\chi$.

(i) Since $e$ is the identity of the group $G$ and $\rho$ is a group homomorphism, so $\rho(e)$ is the identity of the image, $GL(V)$. Hence $\rho(e)$ must be the identity map and hence the trace is just the dimension of $V$. In particular, since $\chi_m$ is a linear character, so the dimension is 1.

(ii) Each $a$ with $(a, m) = 1$ has an order in $G$, say $ord(a)$. Thus,

$$(\chi_m(a))^{ord(a)} = \chi_m(a^{ord(a)}) = \chi_m(1) = 1$$

Hence, $\chi_m(a)$ is a root of unity. Since $a^{\phi(m)} = 1$ in $(\mathbb{Z}/m\mathbb{Z})^*$, and so they are $\phi(m)$ roots of unity.

(iii) Let $\bar{\rho}$ be the representation of $G$ such that

$$\bar{\rho}(g)(v) = \overline{\rho(g)(v)} \ \forall g \in G, v \in V$$

Then it is clear that $\bar{\rho}$ is also a representation of $G$. Hence the trace $\bar{\chi}$ is a character.

(iv) Fix $g \in G$. Let $R = \rho(g) \in GL(V)$ and let $d = dim(V)$. Then, using the knowledge of Linear Algebra, we have that any $R$ which is idempotent (meaning that there exists $m$ such that $R^m = I$), is diagonalisable. Thus, we have $d$ eigenvectors, and let $\lambda_1, \ldots, \lambda_d$ be a list of them. Then

$$\chi(g) = \sum_{i=1}^{d} \lambda_i$$

Similarly, by the construction of $\bar{\chi}$, we have

$$\bar{\chi}(g) = \sum_{i=1}^{d} \bar{\lambda}_i$$

But since $R^m = I$ and for each $\lambda_i$, suppose

$$Rv_i = \lambda_i v_i$$

then

$$v_i = R^m v_i = \lambda_i^m v_i$$

and so

$$\lambda_i^m = 1$$

So each $\lambda_i$ is a root of unity and hence

$$\bar{\lambda}_i = \lambda_i^{-1}$$

Therefore, using

$$\chi(g^{-1}) = \sum_{i=1}^{d} \lambda_i^{-1}$$

we conclude that

$$\chi(g^{-1}) = \bar{\chi}(g)$$

□

**Definition 18.8.** *The* **product** *of two characters (mod $m$) $\chi_1$ and $\chi_2$ is defined by*

$$\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$$

**Lemma 18.9.** *The set of characters (mod $m$) forms a finite Abelian group under multiplication. In particular, if $\chi$ runs over the set of characters (mod $m$) then so does $\chi_1\chi$ for each fixed $\chi_1$.*

*Proof.* Since $\chi_1, \chi_2$ are both linear characters and so are identical to the group homomorphisms $\rho_1, \rho_2$ affording $\chi_1$ and $\chi_2$ respectively. Hence the composition is also a group homomorphism and the dimension is still 1. So the product $\chi_1\chi_2$ is also a character (mod $m$). Association is clear. Let $\chi_0$ be the trivial character (mod $m$). In other words, $\chi_0(a) = 1$ for any $(a, m) = 1$. Thus, the character $\chi_0$ is the identity. Finally, from Lemma 18.7(iv), we have the inverse of $\chi$ is $\bar{\chi}$. This shows that the set of characters (mod $m$) under multiplication forms a group and clearly an Abelian group.

Now we check that the group is finite. By Lemma 18.7(ii), if $(a, m) = 1$, then $\chi(a)$ is a $\phi(m)$ root of unity and hence there are only finitely many distinct characters (mod $m$) (there are at most $\phi(m)^{\phi(m)}$ of them). □

**Definition 18.10.** *Let $G$ be a group. The* **principal character** *is a* **linear** *character $\chi$ of $G$ such that $\chi(g) = 1$ for all $g \in G$.*

We are now going to focus on the characters (mod $m$) and Dirichlet's character only because those are the basic tools to this section and the proof of Dirichlet's theorem. We begin with two short lemmas.

**Lemma 18.11.** *Let $\chi_1$ be a character (mod $m$) and $\chi_2$ be a character (mod $n$). Then the function*

$$\chi(a) = \chi_1(a)\chi_2(a)$$

*defined on $(\mathbb{Z}/mn\mathbb{Z})^*$ is a character (mod $mn$).*

*Proof.* We firstly check that it is well-defined. If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m, n}$ and so $\chi_i(a) = \chi_i(b)$, $i = 1, 2$. Also, each $a$ prime to $mn$ is prime to both $m$ and $n$. Now pick $a, b \in (\mathbb{Z}/mn\mathbb{Z})^*$ and

$$\chi(ab) = \chi_1(ab)\chi_2(ab) = \chi_1(a)\chi_1(b)\chi_2(a)\chi_2(b) = \chi(a)\chi(b)$$

So the product is indeed a character (mod $mn$). □

**Lemma 18.12.** *Let $a$ be an odd integer. Fix an integer $v \geq 3$. Then*

$$\{\pm 5^t : 0 \leq t < 2^{v-2}\}$$

*is a complete residue system modulo $2^v$.*

*Proof.* Consider the order of 5 in $(\mathbb{Z}/2^v\mathbb{Z})^*$. When $v = 3$, 5 has order 2. Use induction to check that 5 has order $2^{v-2}$. Let $5^{2^{v-2}} = a_v + k_v 2^v$ where $0 \leq a_v < 2^v$ and we shall check $a_v = 1$ and $k_v$ is odd. When $v = 3$, we have $5^2 = 1 + 3 \cdot 8$, and so $a_v = 1$ and $k_v = 3$ is odd. Suppose $a_{v-1} = 1$ and $k_{v-1}$ is odd. Then

$$5^{2^{v-2}} = \left(5^{2^{v-1}}\right)^2 = \left(1 + k_{v-1}2^{v-1}\right)^2 = 1 + (k_{v-1} + k_{v-1}^2 2^{v-2})2^v$$

Hence, it is clear that $a_v = 1$ and $k_v = k_{v-1} + k_{v-1}^2 2^{v-2}$ is odd as $v \geq 3$. Therefore we have proved the claim and so we can write for a fixed $v \geq 3$,

$$5^{v-2} = 1 + k2^v$$

where $k$ is odd.

Now let $t$ be the order of 5. Then clearly $t \leq v - 2$. But clearly $t \geq 3$. If $t < v - 2$, then

$$5^t = 1 + k_t 2^{t+2}$$

where $k_t$ is odd and so $5^t \not\equiv 1 \pmod{2^v}$. Thus, $t = v - 2$. This shows that 5 has order $v - 2$. Now, we check that

$$5^a \not\equiv -5^b \pmod{2^v}$$

for any $0 \leq a, b < 2^{v-2}$. Indeed, if $5^a \equiv -5^b \pmod{2^v}$ for some $a, b$. Then $5^a \equiv -5^b \pmod 4$. But $5 \equiv 1 \pmod 4$ and so this gives $1 \equiv -1 \pmod 4$ which is impossible. Thus, $\pm 5^t, 0 \leq t < v - 2$ are all distinct modulo $2^v$. Since the group has order $2^{v-1}$ and so we have found all of them. □

**Lemma 18.13.** *Let $a > 0$, $(a, m) = 1$ and $a \not\equiv 1$ (mod $m$). Then there exists a character (mod $m$) $\chi$ such that $\chi(a) \neq 1$.*

*Proof.* The proof is basically constructing some characters which have the above property. Let

$$m = p_1^{e_1} \cdots p_n^{e_n}$$

We shall introduce firstly the following notation. If $m$ has a primitive root $g$ and $(a, m) = 1$, then let $ind_g(a)$ be the smallest positive integer such that

$$a = g^{ind_g(a)}$$

(In other words, it is the index of $a$ in $g$.) It is easy to check that

$$ind_g(ab) \equiv ind_g(a) + ind_g(b) \pmod{\phi(m)}$$

and

$$a \equiv b \pmod m \Rightarrow ind_g(a) = ind_g(b)$$

Let $e(a) = e^{2\pi i a}$ and we shall construct the following characters first. For $p_i > 2$, let $g_i$ be a primitive root (mod $p_i^{e_i}$) and let $\chi_i$ defined on $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ by:

$$\chi_{p_i}(a) = e\left(\frac{ind_{g_i}(a)}{\phi(p_i^{e_i})}\right) \text{ where } (a, p_i^{e_i}) = 1$$

Define $\chi_2$ to be the principal character (mod 2) and $\chi_4$ to be the character such that $\chi_4(1) = 1, \chi_4(3) = -1$. Further, for $v \geq 3$, define the characters

$$\chi_{2^v,1}(a) = (-1)^{\frac{a-1}{2}}$$

and

$$\chi_{2^v,2}(a) = e\left(\frac{t}{2^{v-2}}\right)$$

where $t$ is defined by $a \equiv \pm 5^t \pmod{2^v}$. (By Lemma 18.12) Suppose $m$ has an odd prime factor $p_i$ such that

$$d \not\equiv 1 \pmod{p_i^{e_i}}$$

Then we may extend the character $\chi_{p_i}$ to $\chi$ such that

$$\chi(a) = \chi_{p_i}(\bar{a}) \ \forall (a, m) = 1$$

where $\bar{a} = a \pmod{p_i^{e_i}}$. Since $d \not\equiv 1 \pmod{p_i^{e_i}}$ and so $\phi(m) \nmid ind_{g_i}(\bar{d})$, so $\chi(d) \neq 1$.

Suppose every odd prime factor of $m$ has the property that

$$d \equiv 1 \pmod{p_i^{e_i}}$$

Since $d \not\equiv 1 \pmod{m}$, so let $2^v$ be the factor of $m$ consisting the power of 2. Then $(d, m) = 1$ implies that $d$ must be odd and so $v > 1$. If $v = 2$, we extend $\chi_4$. Similarly, if $v > 2$, then if $d \equiv 1 \pmod 4$ we extend $\chi_{2^v,2}$ and if $d \equiv 3 \pmod 4$ we extend $\chi_{2^v,1}$. This is because that $(-1)^{\frac{d-1}{2}} = -1$ if $d \equiv 3 \pmod 4$ and if $d \equiv 1 \pmod 4$, the character $\chi_4(d)$ can never be equal to 1 as $t \neq 0$. □

**Theorem 18.14.** *Let $G_m$ be the group of characters (mod m) under multiplication and let $c_m = |G_m|$. Let $M$ denote the complete residue system $\{b : (b, m) = 1, 0 < b < m\}$. Then*

*(i)*

$$\sum_{\chi \in G_m} \chi(a) = \begin{cases} c_m & \text{if } a \equiv 1 \ (mod\ m) \\ 0 & \text{if } a \not\equiv 1 \ (mod\ m) \end{cases}$$

*(ii)*

$$\sum_{a \in M} \chi(a) = \begin{cases} \phi(m) & \text{if } \chi = \chi_0 \text{ is the principal character} \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$$

*(iii)* $c_m = \phi(m)$.

*(iv) When $m$ is a prime, the group $G_m$ is cyclic.*

*Proof.* (i) If $a \equiv 1 \pmod m$ then $\chi(1) = 1$ for all $\chi \in G_m$ and so

$$\sum_{\chi \in G_m} \chi(1) = c_m$$

If $a \not\equiv 1 \pmod m$ then by Lemma 18.13 choose a character $\chi'$ such that $\chi'(a) \neq 1$. Then, by Lemma 18.9, we have

$$\sum_{\chi \in G_m} \chi(a) = \sum_{\chi \in G_m} \chi(a)\chi'(a) = \chi'(a) \sum_{\chi \in G_m} \chi(a)$$

Since $\chi'(a) \neq 1$ and so

$$\sum_{\chi \in G_m} \chi(a) = 0$$

(ii) It is clear that the size of $M$ is P$\phi(m)$. So if $\chi = \chi_0$, the principal character, we have $\chi_0(a) = 1$ for any $a \in M$ and so

$$\sum_{a \in M} \chi_0(a) = \phi(m)$$

If $\chi \neq \chi_0$, then we take some $b \in M$ such that $\chi(b) \neq 1$. Thus,

$$\sum_{a \in M} \chi(a) = \sum_{a \in M} \chi(ab) = \chi(b) \sum_{a \in M} \chi(a)$$

because if $a$ runs over $M$, so does $ab$. Hence

$$\sum_{a \in M} \chi(a) = 0$$

(iii) By (i), we have

$$c_m = \sum_{a \in M} \sum_{\chi \in G_m} \chi(a)$$

because the only contribution is when $a \equiv 1 \pmod{m}$. We swap the summation, and by (ii) for each $\chi \neq \chi_0$, the contribution is 0 and so

$$c_m = \sum_{a \in M} \chi_0(a) = \phi(m)$$

(iv) Let $\chi$ be a non-principal character modulo $p$. Since $m$ is prime and so the group $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic and has a generator $g$, and the character $\chi$ is multiplicative, so the character $\chi$ is therefore determined by the image $\chi(g)$. Let $z$ be any primitive $p - 1^{th}$ root of unity. Then any element $\chi$ with $\chi(g) = z$ will generate the group $G_p$ because

$$\chi(g) = z, \chi^2(g) = z^2, \ldots, \chi^{p-1}(g) = z^{p-1} = 1$$

are all different and so $\chi, \chi^2, \ldots, \chi^{p-1}$ are different characters. But we have shown in (iii) that $|G_p| = \phi(p) = p - 1$, and so these are everything in the group. Hence, the group $G_p$ is cyclic. □

**Corollary 18.15.** *If $(t, m) = 1$, $t > 0$ and $a > 0$, then*

$$\frac{1}{\phi(m)} \sum_{\chi \in G_m} \frac{\chi(a)}{\chi(t)} = \begin{cases} 1 & \text{if } a \equiv t \pmod{m} \\ 0 & \text{if } a \not\equiv t \pmod{m} \end{cases}$$

*Proof.* Choose $u$ so that $tu \equiv 1 \pmod{m}$, then $\chi(t)\chi(u) = 1$, and so

$$\sum_{\chi \in G_m} \frac{\chi(a)}{\chi(t)} = \sum_{\chi \in G_m} \chi(au) \begin{cases} \phi(m) & \text{if } au \equiv 1 \iff a \equiv t \pmod{m} \\ 0 & \text{otherwise} \end{cases}$$

by Theorem 18.14. □

In fact, this is a special case for the more general character theory (which is known as the completeness of character) and Corollary 18.15 is sometimes known as the column orthogonality. (This is involving class function and character table, and the general version is not needed in this book.)

Now, by Corollary 18.15, the group $G_m$ can be split into three classes:

1. The principal character $\chi_0$.

2. The characters $\chi$ which take real values only. (Since the only real roots of unity are $\pm 1$, so $\chi$ can only takes values $\pm 1$ and so $\chi^2 = \chi_0$.)

3. Complex valued characters.

Here is an important property for the real characters.

**Theorem 18.16.** [**Dirichlet's lemma**] *If $\chi$ is a real character (mod $m$), then a number $h$ can be found such that*

$$\chi(a) = \left(\frac{h}{a}\right) \text{ and } h \equiv 0 \text{ or } 1 \pmod 4$$

*where $(\frac{h}{a})$ is the Kronecker symbol. In particular, if $p$ is a prime. Then there are two real characters modulo $p$, which are the principal character and the Legendre symbol.*

We shall leave it as an exercise to the reader with appropriate hint.

## 18.2 Sum of squares

We now go back to the sum of squares discussed at the beginning of this section. We have seen that for any prime $p$,

$$x^2 + y^2 = p$$

is soluble in integers if and only if $p = 2$ or $p \equiv 1 \pmod 4$. The proof we saw was using Gaussian integer. We shall introduce another important method, which is called the **infinite descent method**. Consider the equations

$$f(x_1, \ldots, x_n) = m$$

where $f$ is a quadratic form. The infinite descent method is a type of mathematical induction and gives solutions to the equation in a few important cases. For the initial step we look for a positive integer $k$ such that

$$f(x_1, \ldots, x_n) = km$$

is soluble in integers $x_1, \ldots, x_n$; This is often achieved using congruence results. Then we show that, given a solution of the above equation for some $k > 1$, we can always find another solution of this equation with $k'$ replacing $k$ and $0 < k' < k$; this is called the reduction step. Hence a solution of the initial equation can be found using the initial steps and a finite reduction steps. To illustrate the idea, we shall give the proof of

$$x^2 + y^2 = p$$

using the Euler's method.

**Theorem 18.17.** [**Euler**] *Let $p$ be a prime. Then*

$$x^2 + y^2 = p$$

*is soluble in integers $x$ and $y$ if and only if $p = 2$ or $p \equiv 1$ (mod 4).*

*Proof.* It is clear that if $p \equiv 3 \pmod 4$, then there is no solution because $x^2 + y^2$ can never be 3 (mod 4). Now $2 = 1^2 + 1^2$. If $p \equiv 1 \pmod 4$, then $-1$ is a square (mod $p$) and so there exists $0 < x < \frac{p}{2}$ such that

$$x^2 + 1 \equiv 0 \pmod p$$

Hence, the equation

$$x^2 + y^2 = kp$$

has a solution $(x_0, y_0)$ for some positive integer $k < p$ because $x^2 + 1 \leq p^2$.

Observe that

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

If $k > 1$, define $x_1$ and $y_1$ to be the absolute least residues modulo $k$ of $x_0$ and $y_0$. Thus, we have some $a, b$ such that

$$x_1 = x_0 - ak, y_1 = y_0 - bk$$

and so

$$x_1^2 + y_1^2 \equiv x_0^2 + y_0^2 \equiv 0 \pmod{k}$$

So there exists $k'$ such that

$$x_1^2 + y_1^2 = kk'$$

Since $x_1, y_1$ are the absolute least residues, so we conclude that $|x_1|, |y_1| \leq \frac{k}{2}$ and hence $x_1^2 + y_1^2 \leq 2(\frac{k}{2})^2 = \frac{k^2}{2}$. So $k' < k$.

Now we use the previous observation so that

$$(x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0x_1 + y_0y_1)^2 + (x_0y_1 - x_1y_0)^2 = x_x^2 + y_2^2 = k'k^2p$$

where $x_2 = x_0x_1 + y_0y_1$ and $y_2 = x_0y_1 - x_1y_0$. But

$$x_2 = x_0(x_0 - ak) + y_0(y_0 - bk) \equiv x_0^2 + y_0^2 \equiv 0 \pmod{k}$$

and

$$y_2 = x_0(y_0 - bk) - y_0(x_0 - ak) \equiv 0 \pmod{k}$$

Thus, if we set $x_3 = \frac{x_2}{k}, y_3 = \frac{y_2}{k}$, we have $x_3, y_3$ both integers and

$$x_3^2 + y_3^2 = k'p$$

Thus, we have found $k' < k$ such that

$$x^2 + y^2 = k'p$$

has a solution. Hence, by using the infinite decent method, we have a solution for

$$x^2 + y^2 = p$$

□

A more general result is:

**Theorem 18.18.** *The equation*

$$x^2 + y^2 = m$$

*has an integer solution if and only if each prime factor of $m$ congruent to 3 modulo 4 occurs to an even power in the prime factorisation of $m$.*

*Proof.* If the condition holds, Let

$$m = \prod_{i=1}^{k} p_i^{e_i}$$

For each prime factor $p_i = 2$ or congruent to 1 modulo 4, we use Theorem 18.17 so that we have integer solutions $x_i^2 + y_i^2 = p$. For the prime factor $p_i$ congruent to 3 modulo 4, it occurs to an even power and so $p_i^{e_i}$ is itself a square, say $q_i^2$ and $q_i^2 = q_i^2 + 0^2$. Then use the observation

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

we conclude that $m$ is a sum of squares.

Conversely, suppose $p$ is a prime factor of $m$ which occurs to an odd power, and so we may write

$$m = p^{2k+1}n$$

Suppose we have $x^2 + y^2 = m$. Then if $p|x$, then $p|y$ and so $p^2|x^2 + y^2$. Then we can divide both sides by $p^2$. So we may assume that $p \nmid x$, and so $p \nmid y$. Thus,

$$x^2 + y^2 \equiv 0 \pmod{p} \Rightarrow (xy^{-1})^2 \equiv -1 \pmod{p}$$

which implies that $-1$ is a square modulo $p$. Clearly, this is impossible. □

We shall illustrate another important example.

**Theorem 18.19.** *Let $p$ be a prime number. The equation*

$$x^2 + 3y^2 = p$$

*has an integer solution if and only if $p = 3$ or $p \equiv 1$ (mod 3).*

*Proof.* It is a simple matter to check that

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3$$

by using the Legender symbols. Thus, suppose $p \equiv 2 \pmod 3$, and $x^2 + 3y^2 = p$ has a solution, then

$$x^2 \equiv -3y^2 \pmod p$$

If $x = 0$, then $p = 3$ and $y = \pm 1$. If $x \neq 0$, then it is clear that $p \nmid x$ and $p \nmid y$. So $-3$ is a square modulo $p$. Hence $p \equiv 1 \pmod 3$ which is a contradiction.

Suppose now $p \equiv 1 \pmod 3$, we firstly observe that identity:

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac + 3bd)^2 + 3(ad - bc)^2$$

Now if $p \equiv 1 \pmod 3$ then $-3$ is a square and so $x^2 + 3 \equiv 0 \pmod p$ is soluble, and hence

$$x^2 + y^2 = kp$$

has an integer solution $(x_0, y_0)$ for some $0 < k < p$. If $k > 1$, define $x_1$ and $y_1$ to be the absolute least residue modulo $k$ of $x_0$ and $y_0$ respectively. So we have $|x_1|, |y_1| \leq \frac{k}{2}$. Suppose both equalities hold, then $k$ is even and we have $a$ and $b$ such that

$$\frac{k}{2} = x_0 - ak, \frac{k}{2} = y_0 - bk$$

and since $x_0^2 + 3y_0^2 = kp$, so we have

$$k[(1 + 2a)^2 + 3(1 + 2b)^2] = 4p$$

which is impossible because

$$4|(1 + 2a)^2 + 3(1 + 2b)^2 \Rightarrow 4t = (1 + 2a)^2 + 3(1 + 2b)^2$$

and $1 < k < p$ but

$$kt = p$$

and $p$ is a prime. Thus, we conclude that at least one of them has the strict inequality and so

$$x_1^2 + 3y_1^2 < k^2$$

and since $x_1^2 + 3y_1^2 \equiv 0 \pmod k$, we have

$$x_1^2 + 3y_1^2 = k'k$$

for some $0 < k' < k$. Now let $x_2 = x_0x_1 + 3y_0y_1$ and $y_2 = x_0y_1 - x_1y_0$ so that by the previous observation we have

$$(x_0^2 + 3y_0^2)(x_1^2 + 3y_1^2) = x_2^2 + 3y_2^2 = k^2k'p$$

It is clear that

$$x_2 = x_0(x_0 - ak) + 3y_0(y_0 - bk) \equiv x_0^2 + 3y_0^2 \equiv 0 \pmod{k}$$

and

$$y_2 = x_0(y_0 - bk) - y_0(x_0 - ak) \equiv 0 \pmod{k}$$

and hence, writing $x_3 = \frac{x_2}{k}, y_3 = \frac{y_3}{k}$, we have

$$x_3^2 + 3y_3^2 = k'p$$

for $k' < k$. Thus, by applying the infinite decent method, we conclude that

$$x^2 + 3y^2 = p$$

has an integer solution. □

By a similar argument as Theorem 18.18, we conclude that

$$x^2 + 3y^2 = m$$

has an integer solution if and only if each prime factor $p$ of $m$ congruent to 2 modulo 3 occurs to an even power in the prime factorisation of $m$. In fact, we can classify the integers $m$ represented by $x^2 + ny^2$ for $n = 1, 2, 3$ or 4 using the infinite decent method. But a different approach will be discussed later **quadratic form**.

The main result of this subsection is the famous **four squares theorem** first proved by Lagrange in 1770.

**Theorem 18.20.** *Every non-negative integer can be expressed as a sum of four squares.*

*Proof.* Observe that we have the identity:

$$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = A^2 + B^2 + C^2 + D^2$$

where

$$A = ae + bf + cg + dh, B = af - be + ch - dg, C = ag - ce + bh - df, D = ah - de + bg - fc$$

It is clear that $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$. So the idea is to check that every odd prime can be represented by a sum of four squares and so the result follows.

Let $p$ be an odd prime. Define the sets:

$$S = \left\{x^2 : x = 0, 1, \ldots, \frac{p-1}{2}\right\}, T = \left\{-1 - y^2 : y = 0, 1, \ldots, \frac{p-1}{2}\right\}$$

It is clear that $S \cap T = \varnothing$. Now for any $a \neq b \in S$, we have $a \not\equiv b \pmod{p}$. Similarly, for any $c \neq d \in T$, $c \not\equiv d \pmod{p}$. Thus, since $|S| + |T| = p + 1$, so there exists an $x \in S$ and $y \in T$ such that

$$x^2 \equiv -1 - y^2 \pmod{p}$$

and $x, y < \frac{p}{2}$. Thus, we have

$$x^2 + y^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$$

and an initial integer solution

$$x_0^2 + y_0^2 + u_0^2 + v_0^2 = kp$$

for some $1 \leq k < p$ and $0 \leq x_0, y_0, u_0, v_0$. We shall treat two different cases depending on the parity of $k$.

If $k$ is even. Then $x_0^2 + y_0^2 + y_0^2 + v_0^2 = kp$ implies that among $x_0, y_0, u_0$ and $v_0$, either none of them are even, or two of them are even or all of them are even. Relabeling if necessary, in all cases we have

$$\frac{x_0 + y_0}{2}, \frac{x_0 - y_0}{2}, \frac{u_0 + v_0}{2}, \frac{u_0 - v_0}{2}$$

all integers. Hence we have

$$\left(\frac{x_0 + y_0}{2}\right)^2 + \left(\frac{x_0 - y_0}{2}\right)^2 + \left(\frac{u_0 + v_0}{2}\right)^2 + \left(\frac{u_0 - v_0}{2}\right)^2 = \frac{k}{2}p = k'p$$

where $k' < p$ and this gives the reduction step. Hence, apply the infinite decent method, we have an integer solution for

$$x^2 + y^2 + u^2 + v^2 = p$$

If $k$ is odd. Let $x_1, y_1, u_1, v_1$ be the absolute least residue modulo $k$ of $x_0, y_0, u_0, v_0$ respectively. So it is clear that

$$x_1^2 + y_1^2 + u_1^2 + v_1^2 \equiv 0 \pmod{k}$$

and so

$$x_1^2 + y_1^2 + u_1^2 + v_1^2 = k'k$$

But $|x_1|, |y_1|, |u_1|, |v_1| < \frac{k}{2}$ because $k$ is odd and so

$$x_1^2 + y_1^2 + u_1^2 + v_1^2 < 4\left(\frac{k}{2}\right)^2 = k^2$$

and so $k' < k$. Now use the identity which we observed at the beginning, setting $A, B, C, D$ to be corresponding terms in the expression:

$$(x_0^2 + y_0^2 + u_0^2 + v_0^2)(x_1^2 + y_1^2 + u_1^2 + v_1^2) = A^2 + B^2 + C^2 + D^2$$

Let

$$x_1 = x_0 - ak, y_1 = y_0 - bk, u_1 = u_0 - ck, v_1 = v_0 - dk$$

We have

$$A = x_0x_1 + y_0y_1 + u_0u_1 + v_0v_1 \equiv x_0^2 + y_0^2 + u_0^2 + v_0^2 \equiv 0 \pmod{k}$$

$$B = x_0y_1 - x_1y_0 + u_0v_1 - u_1v_0 \equiv 0 \pmod{k}$$

$$C = x_0u_1 - u_0x_1 + y_0v_1 - y_1v_0 \equiv 0 \pmod{k}$$

and

$$D = x_0v_1 + v_0x_1 + y_0u_1 - y_1u_0 \equiv 0 \pmod{k}$$

Thus, we have

$$\left(\frac{A}{k}\right)^2 + \left(\frac{B}{k}\right)^2 + \left(\frac{C}{k}\right)^2 + \left(\frac{D}{k}\right)^2 = k'p$$

and so this gives the reduction step. Thus, by the infinite decent method, we have an integer solution for

$$x^2 + y^2 + u^2 + v^2 = p$$

This completes the proof. □

In fact, we have seen from the proof, including the several reduction steps which we have omitted, that the infinite decent method provides the explicit solutions to the two (or four) squares problem. We can use more precise argument involving the $\sigma$ and $\tau$ functions to give the formulas for the number of such representations for a fixed integer. Now what about the sum of three squares? One of the difficulty of the three square problems is that we don't have the identity such as

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$$

for three squares. For example, it is easy to check that 3 and 13 can both be represented by a sum of three squares, but 39 cannot be represented by a sum of three squares. In fact, we have some restrictions on the integer $m$ such that if $m$ satisfies some certain conditions then we are able to write $n$ as a sum of three squares. But we shall not give details in this chapter. More information and details will be discussed using the **quadratic form**.

It is nature to ask if we can represent all integers by a sum of $g$ lots of $k^{th}$ powers. This is usually know as the **Waring's problem** (Or more generally, the **Waring-Goldbach problem**). Usually, we denote the function $g(k)$ to be the least possible integer $s$ such that every natural number is the sum of **at most** $s$ $k^{th}$ power. It is postulated that $g(2) = 4, g(3) = 9, g(4) = 19$ and so on. Hilbert was the first one to show that $g(k)$ exists for all $k$. Earlier, Wieferich had shown that $g(3) = 9$ using the three square theorem (which we shall specify later). More recently, Chen proved that $g(5) = 37$. A much more difficult question, and one that leads to a much deeper understanding of the additive properties of $k^{th}$ powers, is that of estimating the function $G(k)$, defined as the least $s$ such that every **sufficiently large** positive integer $n$ is the sum of $s$ $k^{th}$ powers. This function was introduced by Hardy and Littlewood, who obtained the bound

$$G(k) \leq (k-2)2^{k-1} + 5$$

There is one aspect which distinguishes the cases $k = 2$ and $k > 2$; in the latter case there are a few exceptional integers which requires which summands than usual. For example, if $k = 3$, only 23 and 239 need nine cubes. In all probabilities, seven cubes are sufficient if $n > 454$. It is therefore more interesting and useful to find the value or bounds for $G(k)$ instead of $g(k)$ itself. It can be shown that $G(3)$ lies between 4 and 7.

## 18.3 Gauss and Jacobi sums

Throughout the subsection let $p$ be an odd prime and $\zeta$ be a $p^{th}$ primitive root of unity.

**Lemma 18.21.**

$$\sum_{i=0}^{p-1} \zeta^i = 0$$

*Proof.* It is clear because $\zeta^i$, $i = 0, 1, \ldots, p-1$ runs through every $p^{th}$ root of unity. □

**Lemma 18.22.**

$$\sum_{i=0}^{p-1} \zeta^{i^2} = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^j$$

*where* $(\frac{j}{p})$ *is the Legendre symbol.*

*Proof.* It is clear that, if $j > 0$ is a square modulo $p$, then the term $\zeta^j$ appears twice in the sum and if $j$ is not a square, then the term $\zeta^j$ does not appear. Also, for $j = 0$, the term $\zeta^0$ only appear once. Therefore, we conclude that

$$\sum_{i=0}^{p-1} \zeta^{i^2} = \sum_{j=0}^{p-1} \left(1 + \left(\frac{j}{p}\right)\right) \zeta^j$$

and by Lemma 18.21, the first term $\sum_{j=0}^{p-1} \zeta^j = 0$ and so the result follows. □

We want to further simplify the expression. As the Legendre symbol is a character (mod $p$), so this suggests that we should look at the following concept.

**Definition 18.23.** *Suppose $\chi$ is a fixed non-principal character and $\chi_0$ is a principal character, both modulo $p$. If $a \in \mathbb{Z}$, let $g_a$ be given by:*

$$g_a(\chi) = \sum_{i=0}^{p-1} \chi(i)\zeta^{ai}$$

*and*

$$g_a(\chi_0) = \sum_{i=0}^{p-1} \zeta^{ai}$$

*$g_a(\chi)$ is called a* **Gauss sum**. *We write $g(\chi)$ for $g_1(\chi)$.*

**Remark 18.24.** *By Lemma 18.21, and since $p$ is a prime we have*

$$g_a(\chi_0) = \begin{cases} p & \text{if } a \equiv 0 \ (mod\ p) \\ 0 & \text{if } a \not\equiv 0 \ (mod\ p) \end{cases}$$

*It is also clear that $g_a(\chi) = g_b(\chi)$ if $a \equiv b$ (mod $p$).*

**Theorem 18.25.** *Let $a \in \mathbb{Z}$. Let $\chi$ be a non-principal character (mod $p$). Then*

$$g_a(\chi) = \begin{cases} \chi(a^{-1})g(\chi) & \text{if } a \not\equiv 0 \ (mod\ p) \\ 0 & \text{if } a \equiv 0 \ (mod\ p) \end{cases}$$

*Proof.* If $a \not\equiv 0 \pmod{p}$, then

$$\chi(a)g_a(\chi) = \sum_{i=0}^{p-1} \chi(ai)\zeta^{ai}$$

For a fixed $a$, running through $ai$ is the same as running through every $i$ and so

$$\chi(a)g_a(\chi) = \sum_{i=0}^{p-1} \chi(i)\zeta^{i} = g(\chi)$$

Hence

$$g_a(\chi) = \chi(a^{-1})g(\chi)$$

If $a \equiv 0 \pmod{p}$, then $\zeta^{ai} = 1$ for each $i$ and so

$$g_a(\chi) = \sum_{i=0}^{p-1} \chi(i) = 0$$

by Theorem 18.14(ii) as $\chi$ is not principal. □

**Corollary 18.26.**

$$\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^{ai} = \left(\frac{a}{p}\right) \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^{i}$$

*Proof.* As the Legendre symbol is a character (mod $p$), and $(\frac{a}{p}) = (\frac{a^{-1}}{p})$, the result follows by substituting $\chi(i) = (\frac{i}{p})$ into Theorem 18.25. □

**Theorem 18.27.** *If $\chi$ is a non-principal character modulo $p$ then $|g(\chi)| = \sqrt{p}$. Further, if $\chi$ is a real character and writing $g^k(\chi) = (g(\chi))^k$, then*

$$g^2(\chi) = (-1)^{\frac{p-1}{2}} p$$

*Proof.* By Theorem 18.25, we have, for $a \not\equiv 0 \pmod{p}$,

$$g_a(\chi) = \chi(a^{-1})g(\chi)$$

Now take the conjugate of this expression, and use $\chi(a^{-1}) = \bar{\chi}(a)$, we have

$$\overline{g_a(\chi)} = \chi(a)\overline{g(\chi)}$$

Hence, we have

$$|g_a(\chi)|^2 = |g(\chi)|^2$$

for any $a \not\equiv 0 \pmod{p}$ because $\chi(1) = 1$. If $a \equiv 0 \pmod{p}$, then $g_a(\chi) = 0$. Thus,

$$T = \sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2$$

Now, evaluating the sum $T$ explicitly, we consider

$$T = \sum_{a=0}^{p-1} \left( \sum_{x=0}^{p-1} \chi(x)\zeta^{ax} \right) \left( \sum_{y=0}^{p-1} \overline{\chi(y)}\zeta^{-ay} \right)$$

Now we may switch the order of the summation and consider first the sum

$$\sum_{a=0}^{p-1} \chi(x)\overline{\chi(y)}\zeta^{a(x-y)}$$

If $x \neq y$, then the sum is 0 by Lemma 18.21. If $x = y = 0$, then $\chi(0) = 0$ and so the sum is again 0. Now if $x = y \neq 0$, then we have

$$\sum_{a=1}^{p-1} |\chi(x)|^2 = p$$

because each $\chi(x)$ is a root of unity and has modulus 1. Hence

$$T = \sum x, y = 0^{p-1} \sum a = 0^{p-1} \chi(x)\overline{\chi(y)}\zeta^{a(x-y)} = p(p-1)$$

by the above observation. Then we equate the two expressions for $T$ and so

$$(p-1)|g(\chi)|^2 = (p-1)p$$

and so

$$|g(\chi)| = \sqrt{p}$$

For the second part, we use the Dirichlet's lemma (Theorem 18.16) that the character $\chi$ is the Legendre symbol. Then

$$\begin{aligned} \overline{g(\chi)} &= \sum_{x=0}^{p-1} \left( \frac{x}{p} \right) \zeta^{-x} \\ &= \left( \frac{-1}{p} \right) \sum_{x=0}^{p-1} \left( \frac{-x}{p} \right) \zeta^{-x} \\ &= \left( \frac{-1}{p} \right) g(\chi) \end{aligned}$$

Since $p = g(\chi)\overline{g(\chi)}$ by the first part, we have

$$p = \left(\frac{-1}{p}\right)[g(\chi)]^2 = \left(\frac{-1}{p}\right)g^2(\chi)$$

The result follows by

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

□

We now introduce the Jacobi sums. Recall question 9 of exercise 4, we stated that the number of solutions to

$$x^2 - y^2 \equiv d \pmod{p}$$

is $p-1$ (about to residue system modulo $p$). We shall prove this using the Jacobi sums, which are closely related to Gauss sums.

**Definition 18.28.** *Let $\chi$ and $\psi$ be non-principal characters modulo $p$. The* **Jacobi sum** *$J = J(\chi, \psi)$, is defined as:*

$$J(\chi, \psi) = \sum_{x+y=1} \chi(x)\psi(y)$$

*where the sum is taken over all pairs $(x, y)$ such that $0 \leq x, y \leq p-1$ and $s + t \equiv 1$ (mod $p$). For the principal character $\chi_0$, we define*

$$J(\chi_0, \chi_0) = p \text{ and } J(\chi_0, \chi) = 0$$

The followings are the three important properties of the Jacobi sums.

**Theorem 18.29.** *Let $\chi$ and $\psi$ be non-principal characters modulo $p$.*

*(i)* $J(\chi, \bar{\chi}) = -\chi(-1)$.

*(ii) If $\chi\psi \neq \chi_0$, then*

$$J(\chi.\psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)} \text{ and } |J(\chi, \psi)| = \sqrt{p}$$

*(iii) If $p \equiv 1$ (mod $n$), $n > 2$ and $\chi$ is a character of order $n$ (that is $\chi^n = \chi_0$ in the character group) then*

$$g^n(\chi) = p\chi(-1)\prod_{j=1}^{n-2} J(\chi, \chi^j)$$

*Proof.* (i) Using $\bar{\chi}(y) = \chi(y^{-1})$ and $\chi(ab) = \chi(a)\chi(b)$, we have

$$J(\chi, \bar{\chi}) = \sum_{x+y=1, y\neq 0} \chi(xy^{-1})$$

because when $y = 0$ we have $\chi(0) = 0$. Now $x + y = 1 \iff xy^{-1} = y^{-1} - 1$ and so we have

$$J(\chi, \bar{\chi}) = \sum_{y=1}^{p-1} \chi(y^{-1} - 1) = \sum_{z=0}^{p-2} \chi(z)$$

because it is clear that $y^{-1} - 1$ takes values between 0 and $p-2$. By Theorem 18.14(ii), as $\chi$ is non-principal, so that

$$\sum_{z=0}^{p-2} \chi(z) = -\chi(p-1) = -\chi(-1)$$

as required.

(ii) Using the periodic properties of $\chi, \psi$ and $\zeta$, we have

$$\begin{aligned} g(\chi)g(\psi) &= \left[\sum_{x=0}^{p-1}\chi(x)\zeta^x\right]\left[\sum_{y=0}^{p-1}\chi(y)\zeta^y\right] \\ &= \sum_{t=0}^{p-1}\left[\sum_{x+y=t}\chi(x)\psi(y)\right]\zeta^t \\ &= \sum_{t=0}^{p-1}A(t)\zeta^t \end{aligned}$$

For $t = 0$, we have

$$A(0) = \sum_{x=0}^{p-1}\chi(x)\psi(-x) = \psi(-1)\sum_{x=0}^{p-1}(\chi\psi)(x) = 0$$

because $\chi\psi \neq \chi_0$. For $t \neq 0$, we may write $A(t)$ as

$$\begin{aligned} A(t) &= \sum_{xt^{-1}+yt^{-1}=1}\chi(x)\psi(y) \\ &= \sum_{u+v=1}\chi(tu)\psi(tv) \\ &= \sum_{u+v=1}(\chi\psi)(t)\chi(u)\psi(v) \\ &= (\chi\psi)(t)J(\chi,\psi) \end{aligned}$$

Hence,

$$g(\chi)g(\psi) = J(\chi,\psi)\sum_{t=0}^{p-1}(\chi\psi)(t)\zeta^t = J(\chi,\psi)g(\chi\psi)$$

and so

$$J(\chi,\psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}$$

Now apply Theorem 18.27, so

$$|J(\chi,\psi)| = \sqrt{p}$$

(iii) By (ii) we can now write (setting $\psi = \chi$)

$$g^2(\chi) = J(\chi,\chi)g(\chi^2)$$

Now multiply both sides by $g(\chi)$ and use

$$g(\chi^2)g(\chi) = J(\chi,\chi^2)g(\chi^3)$$

we have

$$g^3(\chi) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$$

Continue this and so we have

$$g^{n-1}(\chi) = \prod_{j=1}^{n-2}J(\chi,\chi^j)g(\chi^{n-1})$$

Since $\chi$ has order $n$ and so $\chi^{n-1} = \chi^{-1} = \bar{\chi}$, and

$$\begin{aligned} g(\bar{\chi}) &= \sum_{x=0}^{p-1} \bar{\chi}(x)\zeta^x \\ &= \sum_{x=0}^{p-1} \overline{\chi(x)\zeta^{-x}} \\ &= \sum_{x=0}^{p-1} \overline{\chi(-x)\zeta^{-x}} \cdot \overline{\chi(-1)} \\ &= \chi(-1)\overline{g(\chi)} \end{aligned}$$

because $(\chi(-1))^2 = \chi(1) = 1$ and so it must be real. Thus, we have

$$g(\chi)g(\bar{\chi}) = \chi(-1)|g(\chi)|^2 = \chi(-1)p$$

by Theorem 18.27. Hence the result follows.

□

How is Jacobi sums going to help for the sum of square problems? We shall reprove the theorem at the beginning of the previous subsection.

**Proposition 18.30.** *Let $p$ be a prime which is congruent to 1 modulo 4, then the equation*

$$x^2 + y^2 = p$$

*has an integer solution.*

*Proof.* By Theorem 18.14(iv), we know that the character group $G_p$ is cyclic and since the order of the group $c_p = p - 1$ is divisible by 4, hence there exists an element of order 4. Thus, $\chi$ takes values in $\{\pm 1, \pm i\}$ and hence $J(\chi, \chi) = x + yi$ for some $x, y \in \mathbb{Z}$ from the definition of $J$. Hence, by Theorem 18.29(ii),

$$|J(\chi, \chi)|^2 = x^2 + y^2 = p$$

□

Here is another example:

**Proposition 18.31.** *Let $p$ be a prime which is congruent to 1 modulo 3. Then the equation*

$$x^2 - xy + y^2 = p$$

*has an integer solution.*

*Proof.* By Theorem 18.14(iv), we have an element $\chi$ whose order is 3. So $\chi$ takes values in $\{1, z, z^2\}$ where $z = e^{\frac{2\pi i}{3}}$. Since $z^2 = -z + 1$ so we conclude that $J(\chi, \chi)$ has the form $x + yz$ and so by Theorem 18.29(ii),

$$p = |J(\chi, \chi)|^2 = x^2 + y^2 - xy$$

□

Then we give a more complicated one.

**Theorem 18.32.** *Let $p$ be a prime which is congruent to 1 modulo 3. Then the equation*

$$4p = u^2 + 27v^2$$

*has an integer solution*

*Proof.* By Theorem 18.31, we have integers $x$ and $y$ such that

$$4p = 4(x^2 - xy + y^2) = (x+y)^2 + 3(x-y)^2 + (2x-y)^2 + 3y^2 = (2y-x)^2 + 3x^2$$

Since

$$p = x^2 - xy + y^2 = x(x-y) + y^2 = x^2 + y(y-x) \equiv 1 \pmod 3$$

So at least one of $x, y, x-y$ is divisible by 3. Hence

$$4p = u^2 + 27v^2$$

by using one of the above form for $4p$. □

## 18.4 Number of solutions to $x^n + y^n \equiv 1 \pmod p$

We now go back to the question: how many solutions are there for the congruence:

$$x^n + y^n \equiv 1 \pmod p$$

For general $n$, this should require some knowledge of algebraic geometry and we shall not discuss in great details. But we shall discuss the case $n = 2, 3$ and estimate for $n > 3$. For a polynomial $f(x, y)$ we introduce the notation $N(f, p)$ to be the number of $\{x, y\}$ with $0 \le x, y \le p-1$ and $f(x, y) \equiv 0 \pmod p$.

**Theorem 18.33.** *Let $f(x, y) = x^2 + y^2 - 1$. Then*

$$N(f, p) = p - \left(\frac{-1}{p}\right)$$

*Proof.* For each $a$ and $b$ let $g_a(x) = x^2 - a$ and $h_b(y) = y^2 - b$. Then

$$N(f, p) = \sum_{a+b=1} N(g_a(x), p) N(h_b(y), p)$$

But for each $a \neq 0$, $N(g_a(x), p) = 0$ or 2, depending on whether $a$ is a quadratic residue. So we have $N(g_a(x), p) = 1 + \chi(a)$ where $\chi(a) = (\frac{a}{p})$ is a character modulo $p$. Similarly, $N(h_b(y), p) = 1 + \chi(b)$. Hence,

$$\begin{aligned} N(f,p) &= \sum_{a+b=1} (1+\chi(a))(1+\chi(b)) = \sum_{a+b=1} (1 + \chi(a)\chi(b) + \chi(a) + \chi(b)) \\ &= p + \sum_{a+b=1} \chi(a)\chi(b) + \sum_{a+b=1} \chi(a) + \sum_{a+b=1} \chi(b) \\ &= p + J(\chi, \chi) + \sum_{a=0}^{p-1} \chi(a) + \sum_{b=0}^{p-1} \chi(b) \\ &= p - \chi(-1) = p - \left(\frac{-1}{p}\right) \end{aligned}$$

by Theorem 18.29(i) since $\bar{\chi} = \chi$. □

For $x^3 + y^3 \equiv 1 \pmod p$. We need the following lemma.

**Lemma 18.34.** *If $p \equiv 1 \pmod 3$ and $\chi$ is a character of order 3 so that $J(\chi, \chi) = a + b\omega$, where $\omega = e^{\frac{2\pi i}{3}}$ and $a, b \in \mathbb{Z}$. Then $3|a+1$ and $3|b$. Moreover,*

$$4p = (2a - b)^2 + 3b^2$$

*Proof.* Consider if we work in the field $K = \mathbb{Q}(\zeta, \omega)$, then

$$g^3(\chi) = \sum t = 0^{p-1}\chi(t)^3\zeta^{3t} = \sum_{t=1}^{p-1} \zeta^{3t} \pmod 3$$

By Lemma 18.21 and $3t$ is prime to $p$, so

$$\sum_{t=1}^{p-1} \zeta^{3t} = -1$$

and so $g^3(\chi) \equiv -1 \pmod 3$. But, $\chi(-1) = \chi(-1)^3 = 1$. By Theorem 18.29(iii)

$$g^3(\chi) = p\chi(-1)J(\chi, \chi) = pJ(\chi, \chi) \equiv a + b\omega \pmod 3$$

Thus,

$$a + b\omega \equiv -1 \pmod 3$$

and take the conjugates we have

$$a + b\bar{\omega} \equiv -1 \pmod 3$$

Then we have

$$3|b(\omega - \bar{\omega})$$

and so the take the relative norm $N = N_{K/L}$ where $L = \mathbb{Q}(\zeta)$, we have $N(3) = 9$ and $N(b(\omega - \bar{\omega}) = -3b^2$. Thus, $9| - 3b^2$ and so $3|b$. Hence $b \equiv 0 \pmod 3$ and so we have $a \equiv -1 \pmod 3$.

Now by Theorem 18.29(ii), we have

$$4p = 4|J(\chi, \chi)|^2 = (2a - b)^2 + 3b^2$$

□

Now we are ready to find the number of solutions to the congruence

$$x^3 + y^3 \equiv 1 \pmod p$$

for $p \equiv 1 \pmod 3$.

**Theorem 18.35.** *Let $p \equiv 1 \pmod 3$ and $f(x, y) = x^3 + y^3 - 1$. Then $N(f, p) = p - 2 + u$, where $u$ is the solution to the equation $4p = u^2 + 27v^2$ such that $u \equiv 1 \pmod 3$.*

Note that the $u$ defined in the theorem makes sense because by Lemma 18.34, this $u$ is unique up to sign, and either $u$ or $-u$ is 1 modulo 3, and so it is uniquely determined.

*Proof.* Recall that when $p$ is a prime, the character group is cyclic. We have two characters of order 3, $\chi$ and $\chi^2$ where $\chi^3 = \chi_0$. Let $a \neq 0$. Suppose $x^3 \equiv a \pmod p$ has a solution, then the number of solutions is 3 because $x^3 - a$ is separable, since $p \neq 3$ and so $N(f, p) = 1 + \chi(a) + \chi^2(a)$ since $a$ is a cube and $\chi^3 = \chi_0$. If $x^3 \equiv a \pmod p$ has no solution, then $a \neq 1$ and so there exists a character $\psi$ such that $\psi(a) \neq 1$ by Lemma 18.13. Let $\phi = \psi^{\frac{p-1}{3}}$. Then $\phi^3 = \chi_0$. Hence,

$$1 + \chi(a) + \chi^2(a) = \phi(a) + \phi(a)\chi(a) + \phi(a)\chi^2(a) = \phi(a)(1 + \chi(a) + \chi^2(a))$$

and so $1 + \chi(a) + \chi^2(a) = 0$. Thus, in any cases, We conclude that

$$N(x^3 - a, p) = 1 + \chi(a) + \chi^2(a)$$

Using this, we have

$$\begin{aligned} N(f,p) &= \sum_{a+b=1} N(x^3-a,p)N(y^3-b,p) \\ &= \sum_{a+b=1} (1+\chi(a)+\chi^2(a))(1+\chi(b)+\chi^2(b)) \\ &= p + J(\chi,\chi) + J(\chi,\chi^2) + J(\chi^2,\chi) + J(\chi^2,\chi^2) \\ &\quad + \sum_{a=0}^{p-1}\chi(a) + \sum_{b=0}^{p-1}\chi(b) \\ &= p + J(\chi,\chi) - 2\chi(-1) + J(\bar{\chi},\bar{\chi}) \end{aligned}$$

because $\chi^2 = \bar{\chi}$ as $\chi^3 = \chi_0$. It is clear that $\chi(-1) = \chi(-1)^3 = 1$. Also, $J(\chi,\chi) + J(\bar{\chi},\bar{\chi})$ is twice the real part of $J(\chi,\chi)$. Let $J(\chi,\chi) = u + v\omega$. Then

$$J(\chi,\chi) + J(\bar{\chi},\bar{\chi}) = 2u - v$$

But by Lemma 18.34, we have $4p = (2u-v)^2 + 3v^2$. The result follows by noticing that $2u - v \equiv 1 \pmod 3$ □

## 18.5 The sign of quadratic Gauss sum

Theorem 18.27 says that if $\chi$ is real, then

$$g^2(\chi) = (-1)^{\frac{p-1}{4}} p$$

This implies that we have

$$g(\chi) = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

In fact, we always have the plus sign above. But there is no simple proof of it. We are going to deduce this result in this subsection. We firstly define the matrix $S$ to be

$$S = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta & \dots & \zeta^{p-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \zeta^{p-1} & \dots & \zeta^{(p-1)^2} \end{pmatrix}$$

so that $S_{jk} = \zeta^{jk}$ Consider each component of $S^2$. Let $G_{jk} = S_{jk}^2$, We have

$$G_{ij} = \sum l = 0^{p-1}\zeta^{jl}\zeta lk = \sum_{l=0}^{p-1} \zeta^{(j+k)l}$$

and so clearly $G_{jk} = p$ if $k \equiv -j \pmod p$, and $G_{jk} = 0$ if $k \not\equiv j \pmod p$. Thus, the matrix $G = S^2$ is:

$$G = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 0 & \dots & p \\ \vdots & \vdots & \dots & \vdots \\ 0 & p & \dots & 0 \end{pmatrix}$$

Using this, we have

**Lemma 18.36.** $\det S = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$.

*Proof.* If we swap the $k^{th}$ and $p+2-k^{th}$ column in $G$ for each $k \geq 2$, then we have $G$ diagonal. Since we have swaped $\frac{p-1}{2}$ pairs of columns, so

$$\det G = p^p(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p(p-1)}{2}}p^p$$

as $p$ is odd. Thus,

$$\det S = \pm i^{\frac{p(p-1)}{2}}p^{\frac{p}{2}}$$

We show that the plus sign holds. We can also evaluate the determinant by the Vandermonde determinant, which gives

$$\det S = \prod_{0 \leq j < k \leq p-1} (\zeta^k - \zeta^j)$$

Now, let $a = e^{\frac{\pi i}{p}}$. So that

$$\zeta^k - \zeta^j = a^{j+k}(a^{k-j} - a^{j-k}) = a^{j+k}2i\sin\left(\frac{(k-j)\pi}{p}\right)$$

Hence, using the Vandermonde determinant,

$$\det S = \prod 0 \leq j < k \leq p-1 a^{j+k} \prod_{0 \leq j < k \leq p-1} 2i\sin\left(\frac{(k-j)\pi}{p}\right)$$

Let $T = \sum_{0 \leq j < k \leq p-1} j + k$. Then

$$T = \sum_{k=1}^{p-1}\sum_{j=0}^{k-1} j + k = \sum_{k=1}^{p-1} \frac{k(k-1)}{2} + k^2 = 2p\left(\frac{p-1}{2}\right)^2$$

Thus, $T$ is divisible by $2p$ and so $a^T = 1$. Therefore,

$$\det S = \prod_{0 \leq j < k \leq p-1} 2i\sin\left(\frac{(k-j)\pi}{p}\right) = i^{\frac{p(p-1)}{2}} \prod_{0 \leq j < k \leq p-1} 2\sin\left(\frac{(k-j)\pi}{p}\right)$$

Since $\sin\left(\frac{(k-j)\pi}{p}\right) > 0$ for all $j < k$ and so the plus sign must hold. □

We give below the proof of the sign of Gauss sum by Schur.

**Theorem 18.37. [Schur]** *Let $\chi$ be a real non-principal character modulo $p$. Then*

$$g(\chi) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \ (mod\ 4) \\ 1\sqrt{p} & \text{if } p \equiv -1 \ (mod\ 4) \end{cases}$$

*Proof.* The non-principal real character modulo $p$ is the Legendre symbol (Dirichlet's lemma) and so by Lemma 18.22

$$g(\chi) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)\zeta^j = \sum_{t=0}^{p-1} \zeta^{t^2}$$

Hence, in the above notation, it is the trace of $S$. Let $\lambda_1, \ldots, \lambda_p$ be eigenvalues of $S$. It is clear that $\lambda_1^2, \ldots, \lambda_p^2$ are eigenvalues of $G = S^2$. The characteristic polynomial of $G$ is

$$\det \begin{pmatrix} p-x & 0 & \ldots & 0 \\ 0 & -x & \ldots & p \\ \vdots & \vdots & \ldots & \vdots \\ 0 & p & \ldots & -x \end{pmatrix} = -(x-p)^{\frac{p+1}{2}}(x+p)^{\frac{p-1}{2}}$$

This can be done by:
Add row $k$ by row $p+2-k$ for $2 \leq k \leq \frac{p+1}{2}$. Then subtract the column $k$ from the column $p+2-k$ for each $2 \leq k \leq \frac{p+1}{2}$. After these operations, we have a lower triangular matrix, with $\frac{p-1}{2}$ entries $x-p$, $\frac{p-1}{2}$ entries $x+p$ and the first entry $p-x$. So the set of eigenvalues $\{\lambda_1^2, \ldots, \lambda_p^2\}$ consists of $\frac{p+1}{2}$ copies of $p$ and $\frac{p-1}{2}$ copies of $-p$. Therefore, $\lambda_j = \pm\sqrt{p}$ or $\pm i\sqrt{p}$. Let $r, s, t, u$ be the multiplicity of $\sqrt{p}, -\sqrt{p}, i\sqrt{p}$ and $-i\sqrt{p}$ respectively. Then we have

$$r+s = \frac{p+1}{2}, t+u = \frac{p-1}{2}$$

As $g(\chi) = Tr(S)$, we have

$$g(\chi) = (r-s+(t-u)i)\sqrt{p}$$

Therefore, since $g(\chi)$ can take value $\pm\sqrt{p}, i \pm \sqrt{p}$ corresponding to different congruence condition for $p$, we have

$$r-s = \pm 1 \text{ and } t = u \text{ if } p \equiv 1 \pmod 4$$

$$r = s \text{ and } t-u = \pm 1 \text{ if } p \equiv 3 \pmod 4$$

Since $\det S$ is the product of eigenvalues, and by Lemma 18.36, we have

$$\det S = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}} = (-1)^s i^t (-i)^u p^{\frac{p}{2}}$$

and so

$$2s + t - u \equiv \frac{p(p-1)}{2} \pmod 4$$

Suppose first that $p \equiv 1 \pmod 4$, then $t = u$ and

$$2s \equiv \frac{p(p-1)}{2} \equiv \frac{p-1}{2} \pmod 4$$

Hence, $r-s = r+s-2s = \frac{p+1}{2} - 2s \equiv 1 \pmod 4$. But $r-s = \pm 1$, so $r-s = 1$. Hence,

$$g(\chi) = (r-s+(t-u)i)\sqrt{p} = \sqrt{p}$$

Now suppose $p \equiv 3 \pmod 4$, then we have $r = s$ and so $2s = r+s = \frac{p+1}{2}$. Then

$$t-u \equiv \frac{p(p-1)}{2} + 2s \equiv -\frac{p-1}{2} + 2s = 1 \pmod 4$$

But $t-u = \pm 1$, and so $t-u = 1$. Thus, we have

$$g(\chi) = (r-s+(t-u)i)\sqrt{p} = i\sqrt{p}$$

□

Thus, the theorem gives the evaluation of the sum $\sum_{t=0}^{p-1} \zeta^{t^2}$ In fact, the sum can be generalised to $\sum_{t=0}^{n-1} \zeta^{t^2}$ for any composite number $n$. But it is more complicated and so we shall not deduce that here.

## 18.6 Exercise

1. Let $G$ be a finite group and let $\rho : G \longmapsto GL(V)$ be a representation of $G$ of dimension $d$, affording character $\chi$. Show that $\ker \rho = \{g \in G : \chi(g) = d\}$. Show further that $|\chi(g)| \leq d$ for all $g \in G$ and equality holds if and only if $\rho(g) = \lambda I$ for some root of unity $\lambda$.

2. Let $\chi$ be a character of a representation $\rho$ of $G$ and let $g$ be an element of $G$. If $g^2 = 1$, show that $\chi(g)$ is an integer and $\chi(g) \equiv \chi(1) \pmod 2$. If $G$ is simple and $G \neq C_2$, show that $\chi(g) \equiv \chi(1) \pmod 4$. If $g^3 = 1$ and $g$ is conjugate to $g^{-1}$, show that $\chi(g) \equiv \chi(1) \pmod 3$. (Hint: You may consider the determinant of $\rho(g)$ in the second part.)

3. We have seen in Theorem 18.14(iv) that if $m$ is a prime then the character group modulo $m$ is cyclic. Hence it is isomorphic to the group $(\mathbb{Z}/m\mathbb{Z})^*$. Prove this result for general $m$.

4. Let $\{f_n\}$ be a non-increasing sequence of positive real numbers, and let $\chi$ be a non-principal character modulo $k$. Define
$$Q(x) = \sum_{n \leq x} \chi(n)$$
Use partial summation (considering $\chi(n) = Q(n) - Q(n-1)$) and Theorem 18.14, show that
$$\left| \sum_{n=r}^{s} \chi(n) f_n \right| < 2\phi(k) f_r$$

5. Recall from Theorem 5.12, that for any irrational $\alpha$, we have
$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$$
Show that if $\alpha$ and $\beta$ and real numbers with $\beta > 1$, then there exists integers $u$ and $y$ such that
$$(u, y) = 1, 0 < y \leq \beta \text{ and } \left| \alpha - \frac{u}{y} \right| < \frac{1}{y\beta}$$
Now if $n > 1$ and $z^2 \equiv -1 \pmod n$ is soluble then there exist unique integers $x$ and $y$ such that
$$(x, y) = 1, x, y > 0, x \equiv yz \pmod n \text{ and } n = x^2 + y^2$$
For uniqueness, we don't distinguish the solution $(x, y)$ and $(y, x)$.
(Hint: You may consider $\alpha = -\frac{z}{n}$ and $\beta = \sqrt{n}$.)

6. Let $v(n)$ be the number of solutions to the congruence
$$x^2 \equiv -1 \pmod n$$
(i) Show that the number of solutions to
$$n = x^2 + y^2 \text{ and } (x, y) = 1$$
is $4v(n)$. Hence, show that the number of solutions to $n = x^2 + y^2$ is
$$u(n) = 4 \sum_{d^2 | n} v\left(\frac{n}{d^2}\right)$$
(ii) Deduce that $v$ is multiplicative. Hence, show that, if $(n, m) = 1$, then
$$\frac{u(mn)}{4} = \frac{u(m)}{4} \frac{u(n)}{4}$$
Recall the character $\chi_4$ defined as:
$$\chi_4(1) = 1, \chi_4(3) = -1 \text{ and } \chi_4(a) = \chi_4(\bar{a})$$

where $\bar{a} = a \pmod 4$. Show that $\sum_{d|n} \chi_4(d)$ is multiplicative. Hence show that

$$u(n) = 4 \sum_{d|n} \chi_4(d)$$

(iii) Show further that

$$u(n) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \text{ and } p \text{ divides } n \text{ to an odd power} \\ 4\tau(n^*) & \text{otherwise} \end{cases}$$

where $n^*$ is the product of prime $p^\alpha$ for all prime $p \equiv 1 \pmod 4$.

(iv) Deduce that if $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ has only one solution in the sense that $x, y > 0$ and we don't distinguish the solution $(x, y)$ and $(y, x)$.

7. Show that if $n > 169$ then $n$ can be written as a sum of five **non-zero** squares. By direct computation show that 168 cannot be written as a sum of five non-zero squares.

8. This is a similar problem to the three square problem. Show that for any integer $n$, we have some $a, b, c \in \{\pm 1\}$ such that

$$n = ax^2 + by^2 + cz^2$$

has integer solutions. Further, show that this is not the case for

$$n^2 = ax^2 + by^2$$

where $a, b \in \{\pm 1\}$.

9. Recall the function $g(k)$ defined as the least positive $s$ such that every natural number is the sum of at most $s$ $k^{th}$ power. Using the identity

$$6\left(\sum_{i=1}^{4} x_i^2\right) = \sum_{1 \le i < j \le 4} \{(x_i + x_j)^4 + (x_i - x_j)^4\}$$

show that $g(4) \le 53$.

10. Find all solutions to $x^2 + y^2 \equiv 1 \pmod{19}$ and $x^3 + y^3 \equiv 1 \pmod{19}$.

11. Show that the number of solutions of the congruence

$$x^2 - y^2 \equiv a \pmod p$$

is $p-1$ if $p \nmid a$ and is $2p-1$ if $p|a$. This gives the result which we quote for question 9 in exercise 4.

12. In this question we shall deduce the number of solutions to

$$x^2 + y^2 + x^2y^2 \equiv 1 \pmod p$$

for $p$ a prime which is congruent to 1 modulo 4. Let $\psi$ be the Legendre symbol and $\phi$ be a character modulo $p$ which has order 4. Let $z = J(\phi, \chi)$. Show that

(i) $z = a + ib$ for some $a, b \in \mathbb{Z}$ and

$$J(\psi, \chi) + J(\psi, \chi^3) = z + \bar{z} = 2a$$

where $p = a^2 + b^2$.

(ii) By considering the sum

$$\sum_{s+t=1} (\chi(s) - 1)(\chi(t) + 1)$$

show that if $s \not\equiv 0 \pmod{p}$ then

$$\chi(s) + 1 \equiv 0 \pmod{1+i} \text{ and } z \equiv 1 \pmod{2+2i}$$

in $\mathbb{Z}[i]$.

(iii) Deduce that $a$ is odd and $b$ is even, and if $4|b$, then $4|a-1$. Also, if $4 \nmid b$, then $4|a+1$.

(iv) Let $N$ be the solution-counting function. Show that

$$N(x^2 + y^4 - 1, p) = p - 1 - 2a$$

(v) Finally, using the transformation $(x, y) \mapsto ((1 + x^2)y, x)$ show that

$$N(x^2 + y^2 + x^2y^2 - 1, p) = p - 3 - 2a$$

13. A complex number $z$ is called constructible if there exists subfield $K$ of the complex field $\mathbb{C}$ such that $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m$, $z \in K_m$ and $K_i = K_{i-1}(\sqrt{z_i})$ for some complex number $z_i \in K_{i-1}$. Note that $z$ is constructible if and only if both its real and imaginary parts are constructible.

(i) Show that $\zeta_{2^n}$ is constructible where $\zeta_t = e^{\frac{2\pi i}{t}}$.

Now let $p$ be a Fermat prime, that is a prime of the form $z^n + 1$ for some $n \in \mathbb{N}$.

(ii) If $\chi$ is a character modulo $p$, show that $g(\chi)$ is constructible.
(Hint: You may use Theorem 18.29(iii))

(iii) Deduce that $\zeta_p$ is constructible.

Readers may refer to **radical extension** in Galois theory. It is natural to think of a radical extension a field extension in terms of radical (strictly speaking, it is a succession of Kummer and cyclotomic extensions). If an element is in a radical extension of $\mathbb{Q}$, then it can be constructed geometrically using a ruler and compass. The radical extension plays an important role in Galois theory. It is true that an extension is radical if and only if it is **soluble** and that is the main idea of Galois to show that a general quintic equation (or equation of higher degree) has no general solution as the alternating group $A_5$ (or $A_n, n \geq 5$) is simple.

$^\star$ 14. In this question we are going to prove Dirichlet's Lemma. (Theorem 18.16) Consider firstly the case when $m$ is a power of odd prime number, say $m = p^n$. Let $g$ be a primitive root in $(\mathbb{Z}/m\mathbb{Z})$, show that $(\frac{a}{p}) = 1$ if and only if the index $a$ in $g$ is even. Now let $ind(a)$ be the index of $a$ in $g$.

(i) Consider the character $\chi_{p_i}$ in Lemma 18.3. Show that a general character modulo $p^n$ has the form

$$\chi(a) = \begin{cases} e\left(\frac{vind(a)}{\phi(p^n)}\right) & \text{if } (a, p^n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

where $v$ is any integer coprime to $p^n$ and $1 \leq v \leq p^n$.

(ii) Use this, show that if $\chi$ is a real character, we have

$$\chi(a) = \left(\frac{h}{a}\right)$$

where $h = p^n$ if $p^n \equiv 1 \pmod 4$ and $h = -p^n$ if $p^n \equiv -1 \pmod 4$.

(iii) Now suppose $m = 2^n p^r q^s$ where $n > 2, r, s > 0$ and $p, q$ are distinct prime numbers. Find $h$ such that $\chi(a) = (\frac{h}{a})$ for a real character $\chi$.

(iv) Combine the above results, prove Theorem 18.16.

## 18.7 Hint and Solutions

1. Suppose $g \in \ker \rho$, then $\rho(g) = I_d$ and so $\chi(g) = d$. Conversely, if $\chi(g) = d$, then since the dimension of representation is $d$ and so let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of $\rho(g)$ and so $\lambda_1 + \cdots + \lambda_d = d$. But,

$$d = |\lambda_1 + \cdots + \lambda_d| \leq \sum_{i=1}^{d} |\lambda_i| = d$$

and so the equality holds above. When equality holds, we have that $\lambda_1 = \lambda_2 = \cdots = \lambda_d$ because they are roots of unity and they are in the same direction in the complex plane. Hence $d\lambda_1 = d$ and so $\lambda_1 = \ldots = \lambda_d = 1$. So $\rho(g)$ is the identity. Therefore, $\ker \rho = \{g \in G : \chi(g) = d\}$. For the second part, we use the same argument, and the equality holds if and only if they are in the same direction and so $\lambda_1 = \ldots = \lambda_d = \lambda$. Therefore, $\rho(g) = \lambda I$.

2. Let $d$ be the dimension of the representation $\rho$ and then $\chi(1) = d$. Let $\lambda$ be an eigenvalue of $\rho(g)$ then since $g^2 = 1$ we have $\lambda^2 = 1$. Hence, $\lambda \in \{\pm 1\}$. Let $a$ be the multiplicity of 1 and $b$ be the multiplicity of $-1$. Thus, we have

$$Tr(\rho(g)) = a - b = \chi(g), a + b = d = \chi(1)$$

Hence $\chi(g) = \chi(1) - 2b$ and so they have the same parity.

The determinant of $\rho(g)$ is the product of the eigenvalues and so is equal to $(-1)^b$. Also, it is clear that the map

$$\det : G \longmapsto \mathbb{C}$$

by sending $g$ to $\det \rho(g)$ is a representation because $\rho$ is a representation. It is also clear that the kernel of the map is a normal subgroup. Since $G$ is simple, so the kernel is trivial. Thus, if $g \neq 1$, then we have the determinant of $\rho(g)$ is not equal to 1 and so

$$(-1)^b = 1 \Rightarrow b \text{ is even}$$

Thus, we have

$$\chi(g) = \chi(1) - 2b \Rightarrow \chi(g) \equiv \chi(1) \pmod 4$$

Now $g^3 = 1$ and so the eigenvalue is either 1 or $\omega$ or $\omega^2$ where $\omega = e^{\pm\frac{2\pi i}{3}}$. let $a, b, c$ be the multiplicity of 1, $\omega$ and $\omega^2$ respectively. So the trace $\chi(g) = a + b\omega + c\omega^2$. But, $g$ is conjugate

to $g^{-1}$ and let $h \in G$ such that $g^{-1} = hgh^{-1}$ and so $\chi(g^{-1}) = \chi(hgh^{-1}) = \chi(g)$ because the trace is invariant under conjugation. Also, $\omega^2 = \omega^{-1}$ and so $\chi(g^{-1}) = a + b\omega^2 + c\omega = \chi(g)$. Therefore, we conclude that $b = c$. So we may write

$$\chi(g) = a + b(\omega + \omega^2) = a - b$$

and the dimension

$$d = \chi(1) = a + b + c = a + 2b$$

So we have

$$\chi(g) = \chi(1) - 3b \Rightarrow \chi(g) \equiv \chi(1) \pmod 3$$

3. Let $m = p_1^{e_1} \cdots p_k^{e_k}$ and $\chi_{p_i}$ be the character defined in Lemma 18.13 for an odd primes $p_i$. Consider the case that $m$ is odd first. Then by Chinese Remainder Theorem,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^*$$

For each $p_i$. The functions $\chi_{p_i}^b, (b, p_i^{e_i}) = 1$ are all characters modulo $p_i^{e_i}$ and they are distinct, because $(b, p_i) = 1$. Now, there are $\phi(p_i^{e_i})$ of them and we have prove that the character group modulo $p_i^{e_i}$ has $\phi(p_i^{e_i})$ elements and so these are all of them. Now, consider the element

$$\chi_{p_1}^{b_1} \cdots \chi_{p_k}^{b_k} \text{ where } 0 \le b_i \le p_i^{e_i} \text{ for each } i \text{ and } (b_i, p_i^{e_i}) = 1$$

It is a character modulo $m$ and there are $\phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}) = \phi(m)$ of them and so every character modulo $m$ is of this form and it is clear that the structure of the character group is isomorphic to

$$G_{p_1^{e_1}} \times \cdots \times G_{p_k^{e_k}}$$

but each $G_{p_i^{e_i}}$ is isomorphic to $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ and so the result follows.

Now if $2|m$ but $4 \nmid m$, then since the only character modulo 2 is the principal one and so we use the same argument as above. If $4|m$ but $8 \nmid m$, then consider the character $\chi(4)$ defined in Lemma 18.13, then every character is of the form

$$\chi_4^b \cdots \chi_{p_1}^{b_1} \cdots \chi_{p_j}^{b_k}$$

where $b_i$ is defined as above and $b$ is 0 or 1. Again the result follows. Finally, when $8|m$, let $v$ be the exact order of 2 in $m$, then every character has the form (by counting the number of elements and compare that with the number of elements in the group)

$$\chi_{2^v,1}^b \chi_{2^v,2}^{b'} \chi_{p_1}^{b_1} \cdots \chi_{p_k}^{b_k}$$

where $b_i$ is defined as above and $b$ is 0 or 1 and $b'$ is odd and less than $2^{v-1}$. Hence the result follows. Note that the proof is implicitly using the Chinese Remainder Theorem.

4. We have

$$\begin{aligned} \sum_{n=r}^{s} \chi(n) f_n &= \sum_{n=r}^{s} (Q(n) - Q(n-1)) f_n \\ &= Q_{s+1} f_{s+1} + \sum_{n=r}^{s} Q_n (f_n - f_{n+1}) - Q_{r-1} f_r \end{aligned}$$

By Theorem 18.14, since $\chi$ is non-principal, so that

$$\sum_{a=0}^{k-1} \chi(a) = 0$$

(if $(a,k)>1$, then $\chi(a)=0$, if not, use Theorem 18.14.) Then for each $Q(n)$, let $n=qk+b$, and so

$$|Q(n)| = \left|\sum_{a=0}^{b}\chi(a)\right| < \phi(k)$$

because at most $\phi(k)$ of them are non-zero and each of them has modulus 1 since they are roots of unity. Thus, using $f_n - f_{n+1} \geq 0$, we have

$$\begin{aligned}\left|\sum_{n=r}^{s}\chi(n)f_n\right| &= \left|\left(Q_{s+1}f_{s+1}+\sum_{n=r}^{s}Q_n(f_n-f_{n+1})\right)-(Q_{r-1}f_r)\right| \\ &< \phi(k)\left(f_{s+1}+\sum_{n=r}^{s}(f_n-f_{n+1})\right)+\phi(k)f_r \\ &= \phi(k)f_r+\phi(k)f_r = 2\phi(k)f_r\end{aligned}$$

5. We have, for $\alpha$ irrational,

$$\left|\alpha-\frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}$$

and so for a fixed $\beta>1$, pick $q_n \leq \beta < q_{n+1}$. Hence the result follows by $u=p_n, y=q_n$. If $\alpha$ is rational, then clearly the result holds.

Now let $z^2 \equiv -1 \pmod{n}$ and let $\alpha = -\frac{z}{n}$, $\beta=\sqrt{n}$, so we have $u,y$ such that $(u,y)=1$, $0<y\leq\sqrt{n}$, such that

$$\left|-\frac{z}{n}-\frac{u}{y}\right| < \frac{1}{y\sqrt{n}}$$

Set $x=zy+un$ so that $x\equiv zy \pmod{n}$. From the inequality above, we have

$$x<\sqrt{n} \Rightarrow x^2<n$$

and since $y\leq\beta=\sqrt{n}$ so we have

$$0<x^2+y^2<2n$$

But $x^2+y^2 \equiv z^2y^2+y^2 \equiv 0 \pmod{n}$ and so

$$x^2+y^2=n$$

Since $x=zy+un$, so $n=(zy+un)^2+y^2$ and so

$$0=y^2(z^2+1)+n^2u^2+n(2zyu-1)$$

as $z^2+1$ is divisible by $n$, we have

$$0=y^2\frac{z^2+1}{n}+nu^2+(2zyu-1)$$

Suppose $(y,n)=d$ and then $d|-1$ by above and so $d=1$. So $(y,n)=1$. Hence, $x^2+y^2=n$ implies $(x,y)=1$.

To prove uniqueness, suppose we have

$$x_1 \equiv zy_1 \pmod{n} \text{ and } x_2 \equiv zy_2 \pmod{n}$$

both are solutions to $x^2+y^2=n$. Then we have shown that $(y_1,n)=(y_2,n)=1$, so

$$x_1y_1^{-1} \equiv x_2y_2^{-1} \equiv z \pmod{n}$$

and so

$$x_1y_2 \equiv y_1x_2 \pmod{n}$$

But $0 < x_1, x_2, y_1, y_2 \leq \sqrt{n}$ and so $0 < x_1y_2, y_2x_1 \leq n$. Thus,

$$x_1y_2 = x_2y_1$$

Now

$$x_1^2 n = x_1^2(y_2^2 + x_2^2) = x_1^2y_2^2 + x_1^2x_2^2 = x_2^2y_1^2 + x_1^2x_2^2 = x_2^2 n$$

Thus, $x_1 = x_2$ since they are both positive and so $y_1 = y_2$.

6. (i) In the previous question, we have shown that for a fixed $z$ with $z^2 \equiv -1 \pmod{n}$, there is only one solution $(x, y)$ such that $(x, y) = 1$ and $x, y > 0$. So clearly, in general, we can have $(x, y), (x, -y), (-x, y), (-x, -y)$ and so the number of solution is $4v(n)$.
Suppose now $(x, y) = d$ then $d|n$ also. Thus, for each $d^2|n$, we count the solutions to

$$\frac{n}{d^2} = a^2 + b^2$$

where $(a, b) = 1$. This gives the solution to

$$n = x^2 + y^2$$

with $(x, y) = 1$. Thus, we have

$$u(n) = 4\sum_{d^2|n} v\left(\frac{n}{d^2}\right)$$

(ii) Let $(m, n) = 1$. Then by Chinese Remainder Theorem

$$x^2 \equiv -1 \pmod{mn}$$

if and only if

$$x^2 \equiv -1 \pmod{m} \text{ and } x^2 \equiv -1 \pmod{n}$$

Thus,

$$\frac{u(mn)}{4} = \sum_{d^2|mn} v\left(\frac{mn}{d^2}\right)$$

Also, $d^2|mn$ if and only if $d = d_1d_2$ for some $d_1^2|m, d_2^2|n$. Hence

$$\begin{aligned}\frac{u(mn)}{4} &= \sum_{d_1^2|m, d_2^2|n} v\left(\frac{mn}{d_1^2d_2^2}\right) \\ &= \sum_{d_1^2|m} v\left(\frac{m}{d_1^2}\right)\sum_{d_2^2|n} v\left(\frac{n}{d_2^2}\right) \\ &= \frac{u(m)}{4}\frac{u(n)}{4}\end{aligned}$$

Let $f(n) = \sum_{d|n} \chi_4(d)$. Then, let $(m, n) = 1$. Now $d|mn$ if and only if $d = d_1d_2$ for some $d_1|m$ and $d_2|n$. It is clear that $\chi_4$ is multiplicative. So

$$f(mn) = \sum_{d|mn} \chi_4(d) = \sum_{d_1|m} \chi_4(d_1)\sum_{d_2|n} \chi_4(d_2) = f(m)f(n)$$

which is multiplicative.

Finally, consider $n$ is a power of odd prime. Let $n = p^\alpha$. Suppose $p \equiv 3 \pmod 4$, then if $\alpha$ is odd, we have no solution, and clearly $\chi_4(p) = -1$ and $\chi_4(p^2) = 1$, so

$$u(p^\alpha) = \sum_{d|p^\alpha} \chi_4(d) = 1 - 1 + 1 - \cdots = 0$$

If $\alpha$ is even, then $\sum_{d|p^\alpha} \chi_4(d) = 1$ and $v(p^\beta) = 0$ if $\beta > 1$, because if $x^2 \equiv -1 \pmod{p^\beta}$ is soluble, then $x^2 \equiv -1 \pmod p$ is soluble. Also, $v(1) = 1$. Thus, in this case, we have

$$u(p^\alpha) = 4 \sum_{d^2|p^\alpha} v\left(\frac{p^\alpha}{d^2}\right) = 4 \sum_{d|p^\alpha} \chi_4(d)$$

If $p \equiv 1 \pmod 4$, then since $p^\alpha$ is cyclic and the order is divisible by 4, so the congruence $x^2 \equiv -1 \pmod{p^\beta}$ always has two solutions. Thus, using a similar argument as above, we again conclude that

$$u(\alpha) = 4 \sum_{d^2|p^\alpha} v\left(\frac{p^\alpha}{d^2}\right) = 4 \sum_{d|p^\alpha} \chi_4(d)$$

Since $n$ is either 2 or odd, so the result follows by the multiplicative property of $\chi$ and $\frac{u(n)}{4}$.

(iii) By multiplicative property, if we have an odd prime $p$ which divides $n$ to an odd power, then $\sum_{d|p^\alpha} \chi_4(d) = 0$ and so $u(n) = 0$. Now if for every $p$ with $p \equiv 3 \pmod 4$, if $p$ divides $n$ to an even power, then $sum_{d|p^\alpha}\chi_4(d) = 1$. Finally, for any $p$ with $p \equiv 1 \pmod 4$, we have

$$\sum_{d|p^\alpha} \chi_4(d) = 1 + \alpha = \tau(p^\alpha)$$

Since $\sum_{d|n} \chi_4(d)$ and $\tau(n)$ are both multiplicative so we conclude that

$$u(n) = 4\tau(n^*)$$

(iv) Apply the above result so that we have

$$u(p) = 4\tau(p) = 8$$

But if $(x, y)$ is a solution, so are

$$(x, -y), (-x, y), (-x, -y), (y, x), (y, -x), (-y, -x), (-y, x)$$

and so we have in fact only one solution for $(x, y) > 0$ and we don't distinguish $(x, y)$ and $(y, x)$.

7. By the four square theorem (Theorem 18.20), we have for any $n > 169$,

$$n^2 - 169 = a^2 + b^2 + c^2 + d^2 \text{ where } a \geq b \geq c \geq d \geq 0 \text{ are integers}$$

If $d > 0$ then we are done as $169 = 13^2$ and so

$$n^2 = a^2 + b^2 + c^2 + d^2 + 13^2$$

If $d = 0$, $c > 0$, we have

$$n^2 = a^2 + b^2 + c^2 + 5^2 + 12^2$$

If $c = d = 0, b > 0$, we have

$$n^2 = a^2 + b^2 + 3^2 + 4^2 + 12^2$$

If $c = d = b = 0, a > 0$, we have

$$n^2 = a^2 + 10^2 + 8^2 + 2^2 + 1^2$$

Also, $a \neq 0$ since $n > 169$ and so the result follows.

8. We have for $n$ even,

$$n = 2m = (m+1)^2 - m^2 - 1^2$$

and for $n$ odd

$$n = 2m + 1 = (m+1)^2 - m^2$$

so the first part follows. Now consider $n = 6$, and clearly it is not the sum of two squares and not the difference of two squares because if

$$6 = x^2 - y^2 = (x-y)(x+y)$$

then either $x - y = 1, x + y = 6$ or $x - y = 2, x + y = 3$ but both are impossible.

9. We use the four square theorem, so that every integer can be written as a sum of four squares, say $x_1^2 + x_2^2 + x_3^2 + x_4^2$. Use the identity, so we conclude that for any integer $m$, $6m^2$ is a sum of $2 \cdot \binom{4}{2} = 12$ $4^{th}$ power. Now for any integer $n$, consider $6n$. Use the four square theorem, we can write $6n = 6(a^2 + b^2 + c^2 + d^2)$, but each $6m^2$ is a sum of 12 $4^{th}$ power. Therefore, we conclude that $6n$ is a sum of at most 48 $4^{th}$ power. We finish the proof by observing that $1^4 = 1$ and so we can write,

$$6n, 6n+1, 6n+2, 6n+3, 6n+4, 6n+5$$

as a sum of at most 53 $4^{th}$ power.

10. For $x^2 + y^2 \equiv 1 \pmod{19}$, we have

$$\begin{aligned} N(x^2 + y^2 - 1, 19) &= \sum_{a+b=1} \big(1 + N(x^2 - a, 19)\big)\big(1 + N(y^2 - b, 19)\big) \\ &= 19 - \left(\frac{-1}{19}\right) = 20 \end{aligned}$$

For $x^3 + y^3 \equiv 1 \pmod{19}$, let $\chi$ be a character of order 3. Then by Theorem 18.35, let $4 \cdot 19 = u^2 + 27v^2 = 7^2 + 27$. So $u = 7$ and so we have $19 - 2 + 7 = 24$ solutions.

11. If $p|a$ then $a = 0$ in the congruence and so it is clear that we have $x = \pm y \pmod{p}$ which gives $2p - 1$ solutions. Now if $p \nmid a$, we have the number of solutions

$$\sum_{u+v=1} \big(1 + N(x^2 - au, p)\big)\, N\, \big(1 + N(y^2 + av, p)\big) = p - \left(\frac{-1}{p}\right)^2 = p - 1$$

12. (i) $J(\phi, \chi) = \sum_{a+b=1} \phi(a)\chi(b)$, $\phi(a) = (\frac{a}{p}) \in \{\pm 1\}$ and $\chi$ has order 4 so $\chi(b) \in \{\pm 1, \pm i\}$. Therefore, $z = a + ib$ and $p = a^2 + b^2$ by Theorem 18.29(ii) because clearly $\phi\chi \neq \chi_0$. Now $\chi^3 = \chi^{-1}$ so $\chi(b) = \overline{\chi(b)}$ and so the result follows.

(ii) If $s \not\equiv 0 \pmod{p}$ then $\chi(s)+1 = 0, 2, i+1$ where $2 = -(1+i)(1-i)$ so $\chi(s)-1 \equiv 0 \pmod{1+i}$. Now we have

$$\sum_{s+t=1} (\phi(s)-1)(\chi(t)+1) = J(\phi,\chi)+p = z-p$$

Use the above observation and note that $2|(\phi(s)-1)$ for all $s$, we have $(2+2i)|(\phi(s)-1)(\chi(s)+1)$ for each $s \not\equiv 0 \pmod{p}$. When $s \equiv 0 \pmod{p}$, we have $(\chi(1)-1)(\chi(0)+1) = 0$. So we conclude that

$$z - p \equiv 0 \pmod{2+2i}$$

But $4|p-1$ and $2+2i|4$ so

$$z \equiv 1 \pmod{2+2i}$$

(iii) By (ii), $2+2i| = a-1+ib$ and so $a-1$ is even and $a$ is odd and $b$ is even. Further, let $(2+2i)(c+di) = a-1+ib$. Then $2c-2d = a-1$ and $2c+2d = b$. So if $4|b$, then $4|2c+2d$ and $4|2c-2d$ so $a \equiv 1 \pmod{4}$. The other case is similar.

(iv) Firstly, consider the number of solutions to $y^4 \equiv a \pmod{p}$. If $a \not\equiv 0 \pmod{p}$, and $y^4 \equiv a \pmod{p}$ is soluble, then $\chi(a) = \chi^4(b) = 1$ because $\chi$ has order 4. Then

$$1 + \chi(a) + \chi^2(a) + \chi^3(a) = 4$$

and the equation does have four solutions because $4|p-1$ (So if you like: $g$ is a solution would imply $g * g^{\frac{p-1}{4}}$ is a solution and so on). If $a \equiv 0 \pmod{p}$, then

$$1 + \chi(a) + \chi^2(a) + \chi^3(a) = 1$$

and the equation has only one solution. Finally, if $y^4 \equiv a \pmod{p}$ is not soluble, then $a \neq 1$ and so there exists a character $\psi$ such that $\psi(a) \neq 1$ by Lemma 18.13. Let $\psi' = \psi^{\frac{p-1}{4}}$ and so $\psi'$ has order 4. So

$$1 + \chi(a) + \chi^2(a) + \chi^3(a) = \psi'(a) + \psi'(a)\chi(a) + \psi'(a)\chi^2(a) + \psi'(a)\chi^3(a)$$

which gives $1 + \chi(a) + \chi^2(a) + \chi^3(a)$. So we have

$$\begin{aligned} N(x^2+y^4-1,p) &= \sum_{a+b=1} (1+\phi(a))\left(1+\chi(b)+\chi^2(b)+\chi^3(b)\right) \\ &= p + J(\phi,\chi) + J(\phi,\chi^2) + J(\phi,\chi^3) \\ &= p + 2a - 1 \end{aligned}$$

because $\chi^2 = \phi$ and $J(\phi,\phi) = -(\frac{-1}{p}) = -1$.

# 19 Algebraic Number Theory

We will discuss more in detail on Algebraic Number Theory. We will firstly generalise some results in general extensions of number fields (rather than focus on a specific number theory in previous sections).

## 19.1 Summary of Results of General Number Field Extensions

We will generalise the previous results to general number field extensions and give brief justifications. Recall that a number field is a field extension of $\mathbb{Q}$ of finite degree. The ring of integers $\mathcal{O}$ consists of the elements that are algebraic integers. A unit in the number field is an element in $\mathcal{O}$ with inverse in $\mathcal{O}$. Dirichlet's unit theorem tells that

$$\mathcal{O}^* \cong \Delta \times \mathbb{Z}^{r_1+r_2-1}$$

where $\Delta$ is finite and $r_1, r_2$ are real and complex pair embeddings respectively. Thus, for example, the only fields with finitely many units are $\mathbb{Q}$ and imaginary quadratic fields.

Recall that the norm of a non-zero ideal is finite. To see this, let $I$ be a non-zero ideal. Pick $\alpha \in I$ and take the minimal polynomial of $\alpha$, say

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0, a_i \in \mathbb{Z}, a_0 \neq 0.$$

Let $\beta = \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1$. Then $\alpha\beta = -a_0 \in \mathbb{Z} \notin \{0\}$. Also, $-a_0 \in I$. Therefore,

$$[\mathcal{O} : I] \leq [\mathcal{O} : \langle a_0 \rangle] = |a_0|^n < \infty$$

where $n$ is the degree of the number field.

Recall also that the norm has the property $N(IJ) = N(I)N(J)$. To see this, we have

**Lemma 19.1.** *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$, then*

*(i)* $|\mathcal{O}/\mathfrak{p}^n| = N(\mathfrak{p})^n$.

*(ii)* $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ *as an $\mathcal{O}$-module.*

*Proof.* We will prove the second statement, and the first one follows by using

$$|\mathcal{O}/\mathfrak{p}^n| = |\mathcal{O}/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^2| \cdots |\mathfrak{p}^{n-1}/\mathfrak{p}^n|.$$

By unique factorisation of Dedekind domain, we have $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$. So we can pick $\pi \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$. Thus, $\mathfrak{p}^n \big| \langle \pi \rangle$ but $\mathfrak{p}^{n+1} \nmid \langle \pi \rangle$. Now define the map

$$\psi : \mathcal{O} \longmapsto \mathcal{O}/\mathfrak{p}^{n+1} \text{ by } \psi(x) = \pi \cdot x \pmod{\mathfrak{p}^{n+1}}.$$

Then the kernel is clearly $\mathfrak{p}$. The image is $(\langle \pi \rangle \mathcal{O} + \mathfrak{p}^{n+1}\mathcal{O})/\mathfrak{p}^{n+1}\mathcal{O}$. Now recall that the sum of two ideals is the greatest common divisor of the ideals (you may refer to question 7 of Exercise 13), so

$$\langle \pi \rangle + \mathfrak{p}^{n+1} = \mathfrak{p}^n.$$

Thus the image is $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ and so the result follows by isomorphism theorem. □

**Corollary 19.2.** $N(IJ) = N(I)N(J)$.

*Proof.* $N(IJ) = |\mathcal{O}/IJ|$. Let

$$I = \prod_{i=1}^{k} \mathfrak{p}_i^{n_i}, J = \prod_{j=1}^{k} \mathfrak{p}_j^{m_j}, \max(n_i, m_i) \geq 1$$

Then by Chinese Remainder Theorem we have

$$N(IJ) = |\mathcal{O}/\mathfrak{p}^{n_1+m_1}| \cdots |\mathcal{O}/\mathfrak{p}_k^{n_k+m_k}|.$$

Then by previous lemma, this gives

$$N(\mathfrak{p}_1)^{n_1+m_1} \cdots N(\mathfrak{p}_k)^{n_k+m_k} = (N(\mathfrak{p}_1)^{n_1} \cdots N(\mathfrak{p}_k)^{n_k}) (N(\mathfrak{p}_1)^{m_1} \cdots N(\mathfrak{p}_k)^{m_k}) = N(I)N(J).$$

□

**Corollary 19.3.** *$N(I) \in I$ for any ideal $I$.*

*Proof.* It suffices to check this when $I$ is prime and then apply the previous corollary for general case. When $I$ is prime, let $p$ be the characteristic of the residue field. Then $\mathcal{O}/I$ has base field $\mathbb{F}_p$ and $\mathcal{O}/I = \mathbb{F}_{p^n}$ for some $n \geq 1$. In particular, $p \in I$ because $p$ is 0 in the residue field. Similarly, $p^n \in I$ and observe that $N(I) = p^n$. □

**Definition 19.4.** *Let $L/K$ be a extension of number fields and $I \subset \mathcal{O}_K$ be an ideal. The* **conorm** *of $I$ is the ideal $I\mathcal{O}_L$ of $\mathcal{O}_L$, the ideal generated by the elements of $I$ in $\mathcal{O}_L$. Equivalently, if $I = \langle \alpha_1, \ldots, \alpha_n \rangle$ as an $\mathcal{O}_K$-ideal, then $I\mathcal{O}_L = \langle \alpha_1, \ldots, \alpha_n \rangle$ as $\mathcal{O}_L$ ideal.*

Recall that the ideal class group of a number field is always finite. Thus we can prove

**Proposition 19.5.** *Let $L/K$ be an extension of number fields. Let $I \subset \mathcal{O}_K$ be a non-zero ideal. Then $N(I\mathcal{O}_L) = N(I)^{[L:K]}$.*

*Proof.* Let $n$ be the order of the ideal class group of $K$. Then $I^n$ is principal, and so $I^n\mathcal{O}_L = \langle \alpha \rangle$. Now, we know $N(\langle \alpha \rangle) = |N_{L/\mathbb{Q}}(\alpha)|$ and so

$$N(I^n\mathcal{O}_L) = N(\langle \alpha \rangle) = |N_{K/\mathbb{Q}} \cdot N_{L/K}(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|^{[L:K]} = N(I)^{[L:K]}.$$

□

**Definition 19.6.** *We say a prime $\mathfrak{q}$ of $L$ lies above $\mathfrak{p}$ of $K$ if $\mathfrak{q} \big| \mathfrak{p}\mathcal{O}_L$.*

**Lemma 19.7.** *Let $L/K$ be an extension of number fields. Let $\mathfrak{q}$ be a prime of $L$. Then $\mathfrak{q}$ lies above a unique prime of $K$.*

*Proof.* We claim that $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ is a prime in $K$. It is non-zero because $N(\mathfrak{q}) \in \mathfrak{q} \cap \mathcal{O}_K$. The other properties are easy to check so $\mathfrak{p}$ is prime and $\mathfrak{q}$ lies above it.

Now suppose $\mathfrak{p}'$ be another prime which $\mathfrak{q}$ lies above. Then $\mathfrak{p} + \mathfrak{p}' = \mathcal{O}_K$. Then $\mathfrak{q}$ contains $\mathcal{O}_K$ and hence contains $\mathcal{O}_L$ which is a contradiction. □

**Lemma 19.8.** *Suppose $\mathfrak{q} \subset \mathcal{O}_L$ lies above $\mathfrak{p}$. Then $\mathcal{O}_L/\mathfrak{q}$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$.*

*Proof.* Define

$$\psi : \mathcal{O}_L/\mathfrak{p} \longmapsto \mathcal{O}_L/\mathfrak{q} \text{ by } x \bmod \mathfrak{p} \mapsto x \bmod \mathfrak{q}.$$

It is well-defined because if $x \equiv y \pmod{\mathfrak{p}}$ then $x \equiv y \pmod{\mathfrak{q}}$ because $\mathfrak{q} \big| \mathfrak{p}\mathcal{O}_L$. It is clearly an homomorphism and it is injective because if $x \in \mathcal{O}_K$ and $x \in \mathfrak{q}$ then $x \in \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Hence RHS is a field extension of LHS. □

**Theorem 19.9.** *Let $L/K$ be an extension of number fields. Let $\mathfrak{p}$ be a prime of $K$.*

*(i) If $\mathfrak{p}\mathcal{O}_L$ decomposes as*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{m} \mathfrak{q}_i^{e_i}$$

*then*

$$\sum_{i=1}^{m} e_i f_i = [L:K] \text{ where } f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}].$$

*(ii) If $M/L$ is a further extension, $\mathfrak{r}$ lies above $\mathfrak{q}$ and $\mathfrak{q}$ lies above $\mathfrak{p}$ then*

$$e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{p}}, f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{p}}.$$

*Proof.* (i) Take norm of $\mathfrak{p}\mathcal{O}_L$, we have

$$N(\mathfrak{p})^{[L:K]} = \prod_{i=1}^{m} N(\mathfrak{q}_i)^{e_i} = \prod_{i=1}^{m} N(\mathfrak{p})^{e_i f_i} = N(\mathfrak{p})^{\sum_{i=1}^{m} e_i f_i}.$$

Now compare the exponent.

(ii) The tower law of ramification degree follows by the factorisation of $\mathfrak{q}_i$, for example, we can write, for each $i$,

$$\mathfrak{q}_i = \prod_{j=1}^{n_i} \mathfrak{r}_{ij}^{e_{ij}}.$$

For the residue degree, it follows by the tower law of field extension.

□

Now we are going to generalise Kummer-Dedekind theorem.

**Theorem 19.10. [Kummer-Dedekind]** *Let $L/K$ be an extension of number fields. Suppose $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$ has finite index $N$ and $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$ with minimal polynomial $f(X)$. Let $\mathfrak{p}$ be a prime in $K$, not dividing $N$. If*

$$f(x) \bmod \mathfrak{p} = \prod_{i=1}^{m} \bar{g}_i(X)^{e_i}, \bar{g}_i \text{ distinct irreducible factors },$$

*then*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{m} \mathfrak{q}_i^{e_i}, \text{ where } \mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$$

*and $g_i(X)$ is any lift of $\bar{g}_i(X)$. Further, $\mathfrak{q}_i$ are distinct primes of $L$ with $e_{\mathfrak{q}_i/\mathfrak{p}} = e_i$ and $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \bar{g}_i = f_i$.*

*Proof.* Let $A = \mathcal{O}_K[\alpha]$ and $F = \mathcal{O}_K/\mathfrak{p}$, with $\mathrm{Char}(F) = p$. Define the map

$$\psi : \mathcal{O}_K[X]/\langle f(X), \mathfrak{p}, g_i(X)\rangle \longmapsto A/\mathfrak{p}A + g_i(\alpha)A \text{ by } \psi(x) = \alpha.$$

This clearly gives an isomorphism. Also observe that

$$\mathcal{O}_K[X]/\langle f(X), \mathfrak{p}, g_i(X)\rangle \cong F[X]/\langle \bar{f}(X), \bar{g}_i(X)\rangle \cong F[X]/\langle \bar{g}_i(X)\rangle.$$

Then define the map

$$\phi : A/\mathfrak{p}A + g_i(\alpha)A \longmapsto \mathcal{O}_L/\mathfrak{q}_i \text{ by } \phi(x \bmod \mathfrak{p}A + g_i(\alpha)A) = x \bmod \mathfrak{q}_i$$

where $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_o(\alpha)\mathcal{O}_L \supset \mathfrak{p}A + g_i(\alpha)A$. So the map is well defined.

Since $p \nmid N$ so $p = \text{Char}(F) \nmid N$ and so there exists $M$ such that $NM \equiv 1 \pmod{p}$. $\phi$ is surjective if $x \in \mathcal{O}_L$ then $Nx \in A$ as $N = [\mathcal{O}_L : A]$ and so $MNx \in A$. Thus, $\phi(MNx) \equiv MNx \equiv x \pmod{\mathfrak{q}_i}$, becasue $\mathfrak{q}_i \big| \mathfrak{p}$.

Also, $\mathcal{O}_L/\mathfrak{q}_i$ is non-zero, otherwise $1 \in \mathfrak{q}_i$, and so $N \in \mathfrak{p}A + g_i(\alpha)A$. Then $MN \in \mathfrak{p}A + g_i(\alpha)A$. This implies that $MN, p \in \mathfrak{p}A + g_i(\alpha)A$. But $MN$ is prime to $p$ so that $1 \in \mathfrak{p}A + g_i(\alpha)A$ which is a contradiction.

Further, as $\mathfrak{q}_i \supset \mathfrak{p}A + g_i(\alpha)A$ so the map is injective. Together with the previous identification we conclude that

$$F[X]/\langle \bar{g}_i(X) \rangle \cong A/\mathfrak{p}A + g_i(\alpha)A \cong \mathcal{O}_L/\mathfrak{q}_i.$$

So $\mathcal{O}_L/\mathfrak{q}_i$ is a field extension of $F$ of degree $\deg \bar{g}_i$ and so $\mathfrak{q}_i$ is prime.

For $i \neq j$, since $\bar{g}_i, \bar{g}_j$ coprime, so we have $\lambda(X), \mu(X)$ such that

$$\lambda(X)g_i(X) + \mu(X)g_j(X) \equiv 1 \pmod{\mathfrak{p}}.$$

Then it is clear that $\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L$ (they both contains $\mathfrak{p}$ and use the above relation). Thus $\mathfrak{q}_i \neq \mathfrak{q}_j$ for all $i \neq j$.

Finally, we have

$$\prod_i \mathfrak{q}_i^{e_i} = \prod_i (\mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L)^{e_i} \subset \mathfrak{p}\mathcal{O}_L + \langle \prod_i g_i(\alpha)^{e_i} \rangle = \mathfrak{p}\mathcal{O}_L$$

because $\prod_i \bar{g}_i(\alpha)^{e_i} = \bar{f}(\alpha) \equiv 0 \pmod{\mathfrak{p}}$. By considering the norm,

$$N(\prod_i \mathfrak{q}_i^{e_i}) = \prod_i \left(|F|^{\deg \bar{g}_i}\right)^{e_i} = \prod_i \left(|F|^{f_i}\right)^{e_i},$$

and the fact $\sum_i e_i f_i = \deg \bar{f} = \deg f$, we conclude that

$$N\left(\prod_i \mathfrak{q}_i^{e_i}\right) = |F|^{\deg f} = |F|^{[L:K]} = N(\mathfrak{p}\mathcal{O}_L).$$

Therefore, $\prod_i \mathfrak{q}_i^{e_i} = \mathfrak{p}\mathcal{O}_L$. □

**Example 19.11.** *Let $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_5)$, and $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$. Take $\alpha = \zeta_5$ so $N = 1$ and $f(X) = X^4 + X^3 + X^2 + X + 1$.*

*(i) $f(X)$ mod 2 is irreducible so $\langle 2 \rangle$ is prime in $\mathcal{O}_L$.*

*(ii) $f(X)$ mod 3 is irreducible so $\langle 3 \rangle$ is prime.*

*(iii) $f(X)$ mod 5 gives $(X-1)^4$ so $\langle 5 \rangle = \langle 5, \zeta_5 - 1 \rangle^4$.*

*(iv) $f(X)$ mod 11 gives $(X-4)(X-9)(X-5)(X-3)$ so*

$$\langle 11 \rangle = \langle 11, \zeta_5 - 4 \rangle \langle 11, \zeta_5 - 9 \rangle \langle 11, \zeta_5 - 5 \rangle \langle 11, \zeta_5 - 3 \rangle.$$

**Example 19.12.** *Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_{p^n})$ and $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^n}]$, where $p$ is a prime. Then $f(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$.*

*(i) $f(X) = (X-1)^{p^n - p^{n-1}}$ (mod $p$) so $p$ is totally ramified in $L$.*

*(ii) If $q \neq p$ is another prime, then $X^{p^n} - 1$ mod $q$ has distinct roots, and so $f(X)$ mod $q$ is separable. So for each $i$, $e_i = 1$ and so $q$ is unramified in $L$.*

**Remark 19.13.** *We may not always find $\alpha$ with $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ but we can always find $\alpha \in \mathcal{O}_L$ with $L = K(\alpha)$. The index $N$ is always finite and so the theorem allows us to decompose all except finitely many primes (which divide $N$).*

**Corollary 19.14.** *Let $L/\mathbb{Q}$ be a finite extension, $\alpha \in \mathcal{O}_L$ with $L = \mathbb{Q}(\alpha)$ and minimal polynomial $f(X) \in \mathbb{Z}[X]$. If $f(X)$ mod $p$ has distinct roots in $\bar{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) then $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ is prime to $p$. Hence Kummer-Dedekind applies.*

*Proof.* Let $F$ be the splitting field of $f(X)$ with $f(X) = \prod_i (x - \alpha_i)$. As $f(X)$ mod $p$ has distinct roots in $\bar{\mathbb{F}}_p$ so

$$f(X) \bmod p = \prod_i (X - \bar{\alpha}_i).$$

Hence

$$\prod_{i<j} (\alpha_i - \alpha_j) \not\equiv 0 \pmod{p}.$$

Let $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$ basis for $\mathcal{O}_L$. So we have some matrix $M$ such that

$$M \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}, M \in \mathrm{Mat}_n(\mathbb{Z}).$$

Also, $|\det M| = [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. Let $\sigma_i : i = 1, \ldots, n$ be the embeddings $L \hookrightarrow F$ and write $\alpha = \alpha_1$. Then

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-1} & \sigma_2(\alpha_1)^{n-1} & \cdots & \sigma_n(\alpha_1)^{n-1} \end{vmatrix}$$

Therefore,

$$\prod_{i<j} (\alpha_i - \alpha_j) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} = \det M \det \begin{pmatrix} \beta_1 & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \beta_2 & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \cdots & \vdots \\ \beta_n & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} = \det(MB).$$

We know $p \nmid \prod_{i<j}(\alpha_i - \alpha_j)$ so $p \nmid \det(MB)$ and so $p \nmid \det M = [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. □

## 19.2 Decomposition of Primes

We will focus in this section on how a prime in the base field decomposes in the extension. Let $F/K$ be a finite Galois extension of number fields.

**Lemma 19.15.** *Let $g \in Gal(F/K)$, then*

*(i)* *If $\alpha \in \mathcal{O}_F$, then $g\alpha \in \mathcal{O}_F$.*

*(ii)* *If $I$ is an ideal in $\mathcal{O}_F$ then $g(I)$ is also an ideal in $\mathcal{O}_F$.*

*(iii)* *Let $I, J$ be ideals in $\mathcal{O}_F$, then $g(IJ) = g(I)g(J), g(I+J) = g(I) + g(J)$.*

*(iv)* *If $\mathfrak{q}$ is a prime of $F$ above $\mathfrak{p}$ where $\mathfrak{p}$ is a prime in $K$, then $g(\mathfrak{q})$ is a prime of $F$ above $\mathfrak{p}$. Further, $e_{\mathfrak{q}/\mathfrak{p}} = e_{g(\mathfrak{q})/\mathfrak{p}}, f_{\mathfrak{q}/\mathfrak{p}} = f_{g(\mathfrak{q})/\mathfrak{p}}$.*

*Proof.* The first four statements follow by elementary check. For the last statement, the ramification part follows by considering the unique factorisation of ideals.

Now for the residue degree, let $k = f_{\mathfrak{q}/\mathfrak{p}}$. Let $\{v_1, \ldots, v_k\}$ be a basis for $\mathcal{O}_F/\mathfrak{q}$, then $\{g(v_1), g(v_k)\}$ is a basis for $\mathcal{O}_F/g(\mathfrak{q})$ because $g$ is an automorphism. So $k = f_{g(\mathfrak{q})/\mathfrak{p}}$. □

**Theorem 19.16.** *Let $F/K$ be a Galois extension of number fields, $\mathfrak{p}$ is a prime of $K$. Then $Gal(F/K)$ acts transitively on the primes of $F$ above $\mathfrak{p}$.*

*Proof.* Suppose not, so without loss of generality, we cannot have $\sigma \in G$ such that $\sigma(\mathcal{P}_i) = \mathcal{P}_j$. By Chinese Remainder Theorem, pick $x \in \mathcal{O}_L$ such that

$$x \equiv 1 \pmod{\sigma(\mathcal{P}_i)\ \sigma \in G}, x \equiv 0 \pmod{\mathcal{P}_j}.$$

This is possible as $\sigma(\mathcal{P}_i) \neq \mathcal{P}_j$. Then

$$N_{F/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathcal{P}_j \cap \mathcal{O}_K = \mathfrak{p} \subset \mathcal{P}_i.$$

But $\mathcal{P}_i$ is prime, so we have $\sigma(x) \in \mathcal{P}_i$ for some $\sigma \in G$. This is the same as saying $x \in \sigma^{-1}(\mathcal{P}_i)$. Then

$$x \equiv 0 \pmod{\sigma^{-1}(\mathcal{P}_i)}$$

which is a contradiction to the choice of $x$ we had at the beginning. □

**Corollary 19.17.** *If $F/K$ is Galois, $\mathfrak{p}$ is a prime in $\mathcal{O}_K$. Then $e_1 = e_2 = \cdots = e_r = e$, $f_1 = f_2 = \cdots = f_r = f$ and so $[L : K] = ref$ where $r$ is the number of prime above $\mathfrak{p}$.*

*Proof.* Use the previous lemma and unique factorisation (note that for any $\sigma \in G$, $\sigma(\mathfrak{p}\mathcal{O}_F) = \mathfrak{p}\mathcal{O}_L$). □

**Remark 19.18.** *Let $F/K$ be a Galois extension of number fields. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ be the set of primes above $\mathfrak{p}$. Knowing the action of the Galois group on $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ allows us to easily find the number of the primes above $\mathfrak{p}$ in any intermediate extension $L$. It is the number of $Gal(F/L)$ orbits on $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ (because the Galois group $Gal(F/L)$ also permutes the $\mathfrak{q}_i$'s in the sense that $\mathfrak{q}_i$'s in the same orbit must lie above the same prime.*

**Example 19.19.** *$Gal(F/K) \cong S_4$ and there are four primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_4$ in $F$ above $\mathfrak{p}$ with $S_4$ acting in the usual way of four points. Let $H = \{id, (12)(34)\} \leq S_4$. Let $L = F^H$, then $Gal(F/L) = H$. So the number of primes in $L$ above $\mathfrak{p}$ is the number of $H$-orbits on $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_4\}$ which is 2.*

**Definition 19.20.** *Let $F/K$ be a Galois extension of number fields and $\mathfrak{q}$ a prime above $\mathfrak{p}$ of $K$. The* **decomposition group** *$D_{\mathfrak{q}} = D_{\mathfrak{q}/\mathfrak{p}}$ of $\mathfrak{q}$ is the subgroup of $Gal(F/K)$ fixing $\mathfrak{q}$, i.e.*

$$D_{\mathfrak{q}/\mathfrak{p}} = \{g \in Gal(F/K) : g(\mathfrak{q}) = \mathfrak{q}\}.$$

**Remark 19.21.** *$g \in D_\mathfrak{q}$ fixes $\mathfrak{q}$, so it acts on $\mathcal{O}_F/\mathfrak{q}$, by $x \bmod \mathfrak{q} \mapsto g(x) \bmod \mathfrak{q}$. This gives a natural map*

$$D_\mathfrak{q} \longmapsto Gal(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p}).$$

**Example 19.22.** *$K = \mathbb{Q}$, $F = \mathbb{Q}(i)$, $p = 3$. Complex conjugation acts as*

$$a + bi \bmod 3 \mapsto a - bi \bmod 3 = (a + bi)^3 \ (mod\ 3).$$

*It acts exactly as $x \mapsto x^3$ on $\mathbb{F}_3$.*

**Theorem 19.23.** *Let $F/K$ be a Galois extension of number fields. $\mathfrak{q}$ is a prime of $F$ above $\mathfrak{p}$, a prime of $K$. Then the natural map $D_\mathfrak{q} \longmapsto Gal(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$ is surjective.*

*Proof.* Let $\mathcal{O}_F/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}(\beta)$. Let $f(X) \in \mathcal{O}_K/\mathfrak{p}[X]$ be its minimal polynomial and $\beta = \beta_1, \ldots, \beta_n \in \mathcal{O}_F/\mathfrak{q}$ be its roots. As $\mathrm{Gal}(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$ is cyclic and $g(\beta)$ determines $g$, so it suffices to check that there exists $g \in \mathrm{Gal}(F/K)$ with $g(\mathfrak{q}) = \mathfrak{q}$ and $g(\beta) = \beta_2$.

Pick $\alpha \in \mathcal{O}_F$ with $\alpha \bmod \mathfrak{q} = \beta$, and $\alpha \bmod \mathfrak{q}' = 0$ for all other $\mathfrak{q}'$ above $\mathfrak{p}$. Let $F(X) \in \mathcal{O}_K[X]$ be its minimal polynomial over $K$, and $\alpha = \alpha_1, \ldots, \alpha_r \in \mathcal{O}_F$ be the roots. Then $F(X) \bmod \mathfrak{q}$ has $\beta$ as a root. So $F(X) \bmod \mathfrak{q}$ is divisible by $f(X)$ and so $\beta_i$ (in particular $\beta_2$) is a root of $F(X) \bmod \mathfrak{q}$. Then we may assume that $\alpha_2 \bmod \mathfrak{q} = \beta_2$.

Now take $g \in \mathrm{Gal}(F/K)$ such that $g(\alpha) = \alpha_2$. Then we claim that $g(\mathfrak{q}) = \mathfrak{q}$. If not, as $g$ permutes the primes above $\mathfrak{p}$, we must have $g(\mathfrak{q}') = \mathfrak{q}$ for some $\mathfrak{q}' \neq \mathfrak{q}$. Then as $\alpha \in \mathfrak{q}'$, so we have $g(\alpha) \in \mathfrak{q}$ and $g(\alpha) \equiv 0 \pmod{\mathfrak{q}}$, which implies that $\beta_2 = 0$. But this is impossible. □

**Corollary 19.24.** *Let $K$ be a number field, $F/K$ be the splitting field of a monic irreducible polynomial $f(X)$ of degree $n$. Let $\mathfrak{p}$ be a prime of $K$. Suppose*

$$f(X) \bmod \mathfrak{p} = g_1(X) \cdots g_k(X), g_i(X) \in \mathcal{O}_K/\mathfrak{p}[X], \deg g_i = d_i$$

*(Note that $g_i$'s must be distinct as the extension is separable). Then $Gal(F/K) \leq S_n$ has an element of cycle type $(d_1, \ldots, d_k)$.*

*Proof.* Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$. Let $\alpha_1, \ldots, \alpha_n \in F$ be roots of $f$. Then $\alpha_i \bmod \mathfrak{q}$ is a root of $f \bmod \mathfrak{q}$ and they are distinct because $g_i's$ are distinct. So the action of $g \in D_\mathfrak{q}$ on $\alpha_1, \ldots, \alpha_n$ are exactly the same as the action on $\alpha_1 \bmod \mathfrak{q}, \ldots, \alpha_n \bmod \mathfrak{q}$. So take $g$ which maps to the generator of $\mathrm{Gal}(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$, it has the correct cycle type on $\alpha_i \bmod \mathfrak{q}$. Such $g$ exists by surjectivity (see previous theorem). □

**Definition 19.25.** *Let $F/K$ be a Galois extension of number field. Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$. The inertia subgroup $I_\mathfrak{q} = I_{\mathfrak{q}/\mathfrak{p}}$ is the subgroup of $D_\mathfrak{q}$ such that it acts trivially on $\mathcal{O}_F/\mathfrak{q}$, i.e.*

$$I_\mathfrak{q} = \ker(D_\mathfrak{q} \longmapsto Gal(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})).$$

*Thus, by surjectivity, we have*

$$D_\mathfrak{q}/I_\mathfrak{q} \cong Gal(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p}).$$

*The latter is cyclic, generated by the Frobenius element: $\phi(x) = x^{|\mathcal{O}_K/\mathfrak{p}|}$. The* **arithmetic Frobenius element** *$Frob_{\mathfrak{q}/\mathfrak{p}}$ is the element of $D_\mathfrak{q}/I_\mathfrak{q}$ which maps to $\phi$.*

**Theorem 19.26.** *Let $F/K$ be a Galois extension of number field. Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$. Then*

*(i)* $|D_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$.

*(ii)* $|I_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}}$.

*(iii)* *The order of* $Frob_{\mathfrak{q}/\mathfrak{p}}$ *is* $f_{\mathfrak{q}/\mathfrak{p}}$.
*If* $L$ *is an intermediate field,* $\mathfrak{s}$ *is a prime below* $\mathfrak{q}$ *above* $\mathfrak{p}$*, then*

*(iv)* $D_{\mathfrak{q}/\mathfrak{s}} = D_{\mathfrak{q}/\mathfrak{p}} \cap Gal(F/L)$.

*(v)* $I_{\mathfrak{q}/\mathfrak{s}} = I_{\mathfrak{q}/\mathfrak{p}} \cap Gal(F/L)$.

*Proof.* The first part follows by orbit stabliser theorem and the fact that the Galois group acts transitively. The second part follows from (iii) and (i). For the third part, recall

$$f_{\mathfrak{q}/\mathfrak{p}} = |\mathrm{Gal}(\mathcal{O}_F/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})| = [\mathcal{O}_F/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}].$$

The rest follows from definition. □

**Example 19.27.** *Let* $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Let* $L_1 = \mathbb{Q}(\sqrt{2}), L_2 = \mathbb{Q}(\sqrt{3}), L_3 = \mathbb{Q}(\sqrt{6})$.

*Consider* $p = 2$. *We have* $\langle 2 \rangle = \langle \sqrt{2} \rangle^2$ *in* $L_1$, *and* $\langle 2 \rangle$ *ramifies in* $L_2$ *and* $L_3$ *(use Kummer-Dedekind). Then* 2 *is totally ramified in* $F$ *because for any* $\mathfrak{q}$ *in* $F$ *above* 2, *we have* $e_{\mathfrak{q}/2} \geq 2$. *Now the Galois group is* $C_2 \times C_2$, *and so* $I_{\mathfrak{q}}$ *has size* 2 *or* 4. *In either case,* $I_{\mathfrak{q}}$ *contains* $Gal(F/L_i)$ *for some* $i$. *For this* $i$, *let* $\mathfrak{s}$ *be the prime below* $\mathfrak{q}$, *then*

$$I_{\mathfrak{q}} = I_{\mathfrak{q}/\mathfrak{s}}.$$

*Therefore, the ramification degree is* 2 *in* $F/L_i$ *and so* 2 *is totally ramified.*

*Consider* $p = 3$. *Then* $\langle 3 \rangle$ *ramifies in* $L_2, L_3$ *but* $\langle 3 \rangle$ *is a prime in* $L_1$. *Let* $\mathfrak{q}$ *be a prime above* 3 *in* $F$. *Then* $f_{\mathfrak{q}} \geq 2, e_{\mathfrak{q}} \geq 2$, *and so we conclude* $e_{\mathfrak{q}} = f_{\mathfrak{q}} = 2$. *So* $I_{\mathfrak{q}} = C_2$.

**Example 19.28.** $K = \mathbb{Q}, F = \mathbb{Q}(\zeta_n)$. *Let* $p \nmid n$ *be a prime and* $\mathfrak{q}$ *a prime above* $p$. *By Kummer-Dedekind,* $p$ *is unramified. So* $I_{\mathfrak{q}/p}$ *is trivial and* $D_{\mathfrak{q}/p} = \langle Frob_{\mathfrak{q}/p} \rangle$.

$Frob_{\mathfrak{q}/p}$ *acts as* $x \mapsto x^p$ *on* $\mathcal{O}_F/\mathfrak{q}$. *So* $Frob_{\mathfrak{q}/p}(\zeta_n) = \zeta_n^p$ *mod* $\mathfrak{q}$. *But* $\zeta_n^i$ *are distinct mod* $\mathfrak{q}$ *because* $p \nmid n$. *Therefore,*

$$Frob_{\mathfrak{q}/p}(\zeta_n) = \zeta_n^p.$$

*In particular,* $f_{\mathfrak{q}/p}$ *is the order of* $Frob_{\mathfrak{q}/p}$ *in* $(\mathbb{Z}/n\mathbb{Z})^*$.

## 19.3 Counting Primes

Now we focus on how we count the number of primes in intermediate field.

**Lemma 19.29.** *Let* $F/K$ *be a Galois extension of number fields and* $G$ *be the Galois group.*

*(i)* *The primes of* $K$ *are in bijection with* $Gal(F/K)$*-orbits of primes of* $F$ *via*

$$\mathfrak{p} \longmapsto \textit{primes of } F \textit{ above } \mathfrak{p}.$$

*(ii)* *If* $\mathfrak{q}$ *is a prime of* $F$ *above* $\mathfrak{p}$*, then*

$$gD_{\mathfrak{q}} \longmapsto g(\mathfrak{q})$$

*is a* $Gal(F/K)$*-set isomorphism from* $G/D_{\mathfrak{q}}$ *to the set of primes above* $\mathfrak{p}$.

*(iii)* $D_{g(\mathfrak{q})} = gD_{\mathfrak{q}}g^{-1}, I_{g(\mathfrak{q})} = gI_{\mathfrak{q}}g^{-1}$, $Frob_{g(\mathfrak{q}/\mathfrak{p})} = gFrob_{\mathfrak{q}/\mathfrak{p}}g^{-1}$.

*Proof.* The first part follows from the fact that $G$ acts transitively. For the second part, it is easy to check that the map is well-defined. If $g_1 D_{\mathfrak{q}} = g_2 D_{\mathfrak{q}}$, then $g_2^{-1} g_1 \in D_{\mathfrak{q}}$ and so $g_2(\mathfrak{q}) = g_1(\mathfrak{q})$, so the map is injective. Surjectivity also follows from the fact $G$ acts transitively. It is clearly a homomorphism.

For the last part, see exercises. □

**Corollary 19.30.** *Let $F/K$ be a Galois extension of number fields. Let $L$ be an intermediate extension. Let $G$ be the Galois group, $H = Gal(F/L)$ and $\mathfrak{p}$ be a prime in $K$. Let $\mathfrak{q}$ be a prime of $F$ above $\mathfrak{p}$. Then we have*

$$\{ \text{ primes of } L \text{ above } \mathfrak{p}\} \longleftrightarrow H - \text{orbits on primes of } F \text{ above } \mathfrak{p} \longleftrightarrow \text{ double cosets } H\backslash G/D_{\mathfrak{q}}$$

*via*

$$\mathfrak{s} \longmapsto \text{ element that sends } \mathfrak{q} \text{ to some prime above } \mathfrak{s}$$

*is a bijection.*

*Proof.* The first correspondence is clear from the previous lemma. We shall introduce the notation of double cosets. The $H - D$ double cosets, $H\backslash G/D$ is the $H$-orbits of $G/D$. Equivalently it is the $D$-orbits of $H/G$, where $D$ acts by $d(Hg) = Hgd^{-1}$.

We shall explain the interpretation of $D_{\mathfrak{q}}$-orbits of $H\backslash G$. Let $L = K(\alpha)$, and $H$ is the stabliser of $\alpha$ because it is the group which fixes $L$ (fixing $L$ is the same as fixing $\alpha$). So the $D$-orbits on $H\backslash G$ is the $D_{\mathfrak{q}}$-orbits on the roots of the minimal polynomial of $\alpha$. Equivalently, on the embeddings $K \hookrightarrow L$.

Now each $H$-orbit on the primes above $\mathfrak{p}$ corresponds to an $H$-orbit of $G/D$, using the previous lemma ($G/D_{\mathfrak{q}}$ is isomorphic to the primes above $\mathfrak{p}$). This gives the second correspondence. □

**Proposition 19.31.** *Let $F/K$ be a Galois extension of number fields, $L = K(\alpha)$ an intermediate field. Let $G = Gal(F/K)$ and $H = Gal(F/L)$. Let $\mathfrak{p}$ be a prime of $K$ and $\mathfrak{q}$ a prime of $F$ above it. Consider the set (of size $[L : K]$)*

$$X = H\backslash G \cong \{\text{embeddings } L \hookrightarrow F\} \cong \{\text{roots of minimal polynomial of } \alpha\}.$$

*Then we have a bijection*

$$\{ \text{ primes of } L \text{ above } \mathfrak{p}\} \longleftrightarrow D_{\mathfrak{q}} - \text{orbits on } X$$

*with $e_{\mathfrak{s}/\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}} =$size of $D_{\mathfrak{q}}$-orbit, $e_{\mathfrak{s}/\mathfrak{p}} =$size of any $I_{\mathfrak{q}}$-suborbit, $f_{\mathfrak{s}/\mathfrak{p}} =$ number of $I_{\mathfrak{q}}$ suborbits, where $\mathfrak{s}$ is a prime below $\mathfrak{q}$. Explicitly, we have*

$$\mathfrak{s} \longmapsto \text{orbits of } g^{-1}(\alpha) \text{ where } g(\mathfrak{q}) \text{ lies above } \mathfrak{s}.$$

*Proof.* The bijection is clear from the proof of the previous corollary and how we introduce the action of double cosets. Let $N$ denote the size of the $D_{\mathfrak{q}}$ orbit of $g^{-1}(\alpha)$, then

$$\begin{aligned} N &= \frac{|D_{\mathfrak{q}}|}{\text{stab}_{D_{\mathfrak{q}}}(g^{-1}(\alpha))|} = \frac{|D_{\mathfrak{q}}|}{|\text{stab}_{gD_{\mathfrak{q}}g^{-1}}(\alpha)|} \\ &= \frac{|D_{\mathfrak{q}}|}{|gD_{\mathfrak{q}}g^{-1} \cap H|} = \frac{D_{\mathfrak{q}}|}{|D_{g(\mathfrak{q})} \cap H|} \end{aligned}$$

where in the second line we consider that if $h$ lies in the stabliser of $\alpha$ in $gD_{\mathfrak{q}}g^{-1}$ then $ghg^{-1} \in H$.

Now $g(\mathfrak{q})$ is a prime above $\mathfrak{s}$ and so $D_{g(\mathfrak{q})}$ gives the decomposition group of $g(\mathfrak{q})$ above $\mathfrak{s}$. Thus

$$\frac{|D_{\mathfrak{q}}|}{|D_{g(\mathfrak{q})/\mathfrak{s}}|} = \frac{e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}}{e_{g(\mathfrak{q})/\mathfrak{s}} f_{g(\mathfrak{q})/\mathfrak{s}}} = \frac{e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}}{e_{\mathfrak{q}/\mathfrak{s}} f_{\mathfrak{q}/\mathfrak{s}}} = e_{\mathfrak{s}/\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}}.$$

Similarly, the size of $I_{\mathfrak{q}}$-suborbit is

$$\frac{|I_{\mathfrak{q}}|}{|\text{stab}_{I_{\mathfrak{q}}}(g^{-1}(\alpha))|} = \frac{|I_{\mathfrak{q}}|}{|gI_{\mathfrak{q}}g^{-1} \cap H|} = \frac{|I_{\mathfrak{q}}|}{|I_{g(\mathfrak{q})/\mathfrak{s}}|} = e_{\mathfrak{s}/\mathfrak{p}}.$$

The number of $I_q$ suborbits is the size of $D_{\mathfrak{q}}$-orbit divided by the size of each $I_{\mathfrak{q}}$-suborbit, and so the result follows. □

**Example 19.32.** *Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_5, \sqrt[5]{2}), p = 73$. Let $L_1 = \mathbb{Q}(\sqrt[5]{2})$ and $L_2 = \mathbb{Q}(\zeta_5)$. Fix $\mathfrak{p}, \mathfrak{q}$ above 73 in $L_2$ and $F$ respectively.*

*Referring to Example 19.28, we have, since 73 has order 4 in $(\mathbb{Z}/5\mathbb{Z})^*$, the residue degree of $\mathfrak{p}$ is 4.*

*We claim that $\mathfrak{q}/\mathfrak{p}$ is unramified. Suppose not, then $e_{\mathfrak{q}/\mathfrak{p}} > 1$. But we know $F/L_2$ is Galois of degree 5. So $ref = 5$ implies that $e_{\mathfrak{q}/\mathfrak{p}} = 5$. But on the other hand, 73 does not ramify in $L_1$, so the ramification degree is at most 4, which gives a contradiction (it is clear that 73 is unramified in $L_1$). This shows that 73 is unramified and $f_{\mathfrak{q}/73} = 4$ or 20. But the decomposition group cannot be cyclic of order 20 and so $f_{\mathfrak{q}/73} = 4$. So $D_{\mathfrak{q}/73} = C_4$.*

*To count the number of primes in $L_1$ above 73. By previous theorem, consider the roots $\zeta_5^i \sqrt[5]{2}$, $i = 0, 1, 2, 3, 4$. $D_{\mathfrak{q}}$ permutes the roots and since it has size 4 while we have 5 roots, it must fix some root. We may assume $\sqrt[5]{2}$ is fixed. We have $D_{\mathfrak{q}} = \langle Frob_{\mathfrak{q}} \rangle$ and $Frob_{\mathfrak{q}}(\zeta_5) = \zeta_5^{73} = \zeta_5^3$. Now 3 generates $(\mathbb{Z}/5\mathbb{Z})^*$ so we have two orbits. In particular, one of them has residue degree 4 and the other has residue degree 1 by the previous Corollary.*

**Example 19.33.** *Recall that $a$ is a square mo $p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ for $p \nmid a$ (Euler's Criteria). Similarly, if $p \nmid 3a$ we claim that*

$$X^3 - a \text{ has } = \begin{cases} 3 \text{roots } mod\ p & \text{if } p \equiv 1 \ mod\ 3, a^{\frac{p-1}{3}} \equiv 1 \ mod\ p, \\ 0 \text{root } mod\ p & \text{if } p \equiv 1 \ mod\ 3, a^{\frac{p-1}{3}} \not\equiv 1 \ mod\ p, \\ 1 \text{root } mod\ p & \text{if } p \equiv 2 \ mod\ 3. \end{cases}$$

*We shall prove this. We know $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Let $g$ be a generator. If $p \equiv 2 \pmod 3$ then $X^3 - a \equiv 0 \pmod p$ is soluble if and only if $a = g^{3t}$ for some $t$. Further, we know $g^{p-1} = 1$. So let $\alpha$ be the order of $a$. Then*

$$\alpha \equiv 3t \ (mod\ p - 1).$$

*But $\alpha$ is fixed and $3 \nmid p - 1$, so $t \equiv 3^{-1}\alpha \ mod\ p - 1$, which is determined uniquely. So $X^3 - a \equiv 0$ mod $p$ has a unique solution.*

*If $p \equiv 1 \pmod 3$, then $X^3 - a \equiv 0$ is soluble if and only if $\alpha \equiv 3t \ mod\ p - 1$. Now $3 \nmid p - 1$ so $\alpha \equiv 3t \ mod\ p - 1$ is soluble if and only if $3 \big| \alpha$. Equivalently, $a = \left(g^{\frac{\alpha}{3}}\right)^3$. This is saying*

$$a^{\frac{p-1}{3}} = \left(g^{\frac{\alpha}{3}}\right)^{p-1} = 1.$$

*When it is soluble, it has three solutions for $t$, namely $t_1, t_1 + \frac{p-1}{3}, t_1 + 2\frac{p-1}{3}$.*

**Example 19.34.** *Let $f(X) = X^3 + bX + c, b, c \in \mathbb{Z}$. Let $F$ be its splitting field and $\alpha, \beta, \gamma$ be the roots of $f$. For $g \in S_3$ (permuting $\alpha, \beta, \gamma$), consider*

$$z = \alpha g(\alpha) + \beta g(\beta) + \gamma g(\gamma).$$

*It is a root of one of the followings:*

$$\Gamma_1 = X - (\alpha^2 + \beta^2 + \gamma^2) = X + 2b,$$

$$\Gamma_2 = (X - (2\alpha\beta + \gamma^2))(X - (2\alpha\gamma + \beta^2))(X - (2\beta\gamma + \alpha^2)) = X^3 - 3b^2X - b^3 - 27,$$

$$\Gamma_3 = (X - (\alpha\beta + \beta\gamma + \gamma\alpha))(X - (\alpha\gamma + \beta\alpha + \gamma\beta)) = (X - b)^2.$$

*Now take $p$ a prime and $\mathfrak{q}$ above $p$ in $F$. To determine the factorisation of $f(X)$ mod $p$, look at $Frob_{\mathfrak{q}/p}$ provided $f(X)$ mod $p$ is separable (i.e. $p \nmid 4b^3 + 27c^2$). The number of roots of $f$ mod $p$ is the number of fixed point of $Frob_{\mathfrak{q}/p}$ because $Frob_{\mathfrak{q}/p}(x) = x^p$ mod $p$, and each element in $\mathbb{F}_p$ has $x^p = x$.*

*We compute*

$$y = \alpha Frob_{\mathfrak{q}/p}(\alpha) + \beta Frob_{\mathfrak{q}/p}(\beta) + \gamma Frob_{\mathfrak{q}/p}(\gamma) \equiv \alpha^{p+1} + \beta^{p+1} + \gamma^{p+1} \ mod\ \mathfrak{q}.$$

*Consider the matrix*

$$A = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{pmatrix}$$

*has eigenvalue $\alpha, \beta, \gamma$ and so $y \equiv T = Tr(A^{p+1})$ mod $p$.*

*So if $p \nmid 3b(4b^3 + 27c^2)$, (then $\Gamma_1, \Gamma_2, \Gamma_3$ have distinct roots), then $f(X)$ has 3 distinct roots if and only if $Frob_{\mathfrak{q}/p}$ has 3 fixed points, if and only if $T \equiv -2b$ mod $p$ (as $\alpha^2 + \beta^2 + \gamma^2 = -2b$). $f(X)$ has one root if and only if $T$ is a root of $X^3 - 3b^2X - b^3 - 27$ mod $p$. Finally, $f(X)$ is irreducible if and only if $T \equiv b$ mod $p$.*

## 19.4 Representations

We will finish the section by deducing some results by using representation theory. Firstly we will introduce The permutation representation. Let $X$ be a finite $G$-set (of size $n$), the $n$-dimensional representation $\mathbb{C}[X]$ which has $\{e_x\}_{x \in X}$ as a basis with $G$-action

$$g\left(\sum \lambda_x e_x\right) = \sum \lambda_x e_{g(x)}.$$

The number of $G$-orbits on $X$ can be recovered by $\langle 1, \mathbb{C}[X] \rangle_G$, the character of $\mathbb{C}[X]$ is $\chi_{\mathbb{C}[X]}(g)$ is the number of the fixed points of $g$ on $X$.

Let $H \leq G$ of index $n$ and let $V$ be an $H$-representation. The induction is defined by:

$$\mathrm{Ind}_H^G V = \mathrm{Hom}_{\mathbb{C}[H]}(\mathbb{C}[G], V).$$

Concretely, if $g_1, \ldots, g_n$ are the left coset representatives of $H$, take Ind$V$ to be $n$ copies of $V$ with $G$-action determined by:

$$g(0, \ldots, v, 0, \ldots) = (0, \ldots, h(v), 0, \ldots)$$

where the $i^{\text{th}}$ entry $v$ gives the $j^{\text{th}}$ entry $h(v)$ when $gg_i = g_j h, (h \in H)$. Note that if $v = \not\Vdash$, then $\mathrm{Ind}_H^G V$ simply gives $\mathbb{C}[G/H]$. The character formula is

$$\chi_{\mathrm{Ind}_v}(g) = \frac{1}{|H|} \sum_{x \in G, zgz^{-1} \in H} \chi_v(zgz^{-1}).$$

The induction can be visualised by observing all the restrictions to it and read off from the picture. Say we have $S_4$ and irreducible characters, $1_G, S, T, V, W$, $H = S_3 \leq S_4$. $H = S_3 \leq S_4$, and $H$ has characters $1_H, \rho, \epsilon$. Knowing that

$$\mathrm{Res}_H^G 1_G = 1_H, \mathrm{Res}_H^G s = \epsilon, \mathrm{Res}_H^G T = \rho, \mathrm{Res}_H^G V = 1_H \oplus \rho, \mathrm{Res}_H^G W = \epsilon \oplus \rho$$

would give induction

$$\mathrm{Ind}_H^G 1_H = 1_G \oplus V, \mathrm{Ind}_H^G \epsilon = S \oplus W, \mathrm{Ind}_H^G \rho = T \oplus V \oplus W.$$

The Frobenius reciprocity says

$$\langle V, \mathrm{Res}_H^G W \rangle_H = \langle \mathrm{Ind}_H^G V, W \rangle_G.$$

Mackey's formula: Let $D, H \leq G$ and $\rho$ be an $H$-representation. Fix $X = \{x_1, \ldots, x_n\}$ a set of $H - D$ double coset representatives, and $x \in X$. Define the $x^{-1}Hx$ representation $\rho^x$ by:

$$\rho^x(x^{-1}gx) = \rho(g).$$

Then Mackey's formula says

$$\mathrm{Res}_D^G \mathrm{Ind}_H^G \rho \cong \oplus_{x \in X} \mathrm{Ind}_{x^{-1}Hx \cap D}^D \mathrm{Res}_{x^{-1}Hx \cap D}^{x^{-1}Hx} \rho^x.$$

Throughout, let $F/K$ be a Galois extension of number fields, $\mathfrak{p}$ a prime of $K$, $\mathfrak{q}$ a prime above $\mathfrak{p}$. Let $D$ be the decomposition group of $\mathfrak{q}/\mathfrak{p}$, and $I$ be its inertia group. Let Frob denote $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$, and $G =$Gal$(F/K)$.

**Remark 19.35.** *If $L$ is an intermediate field and $H = Gal(F/L)$. Then recall that the number of primes of $L$ above $\mathfrak{p}$ is the number of $H$-orbits of $G/D$. In language of representation, this is $\langle Res_H^G Ind_D^G 1_D, 1_H\rangle_H$ because $\mathbb{C}[G/D] = Ind_D^G 1_D$ and we want the $H$-orbit of it, so we take the restriction in $H$. Now by Frobenius reciprocity, we have*

$$\langle Res_H^G Ind_D^G 1_D, 1_H\rangle_H = \langle Ind_D^G 1_D, Ind_H^G 1_H\rangle_G = \langle 1_D, Res_D^G Ind_H^G 1_H\rangle_D$$

*and the latter is the number of $D$-orbits of $H\backslash G$.*

**Definition 19.36.** *If $V$ is a representation od $D$, let $V^I$ be the subspace of $I$-invariant vectors. As $I \subset D$, this is a subrepresentation. If $v \in V^I$, then so is $gv$ because for $h \in I$, $h(gv) = (hg)v$. Now $I \subset D$, so $hg = gg^{-1}hg = gh'$ as $g^{-1}hg \in I$. So $(hg)v = gh'v = g(h'v) = gv$ because $h'v = v$.*

**Lemma 19.37.** *If $V$ is an irreducible representation of $D$, then either*

*(i) $V^I = 0$.*

*(ii) Or $V$ is 1-dimensional, lifted from $D/I$ (i.e. $D \longmapsto D/I \longmapsto \mathbb{C}^*$). These kill $I$ and are determined by the action of Frob.*

*Proof.* $V^I$ is a subrepresentation, if $V$ is irreducible then $V^I = 0$ or $V^I = V$. When $V^I = V$, then every $v \in V^I$ is fixed by $I$. Then clearly if $g_1 I = g_2 I$ then $g_1 v = g_2 v$ because $g_2^{-1} g_1 \in I$. So $V$ is lifted from a representation of $D/I$. But $D/I$ is cyclic, in particular abelian, and every abelian irreducible representation is 1-dimensional. □

**Remark 19.38.** *The representation of $D$ looks like $V = A \oplus B$ by the previous lemma, where $A^I = 0$ and $B = V^I = \oplus$1-dimensional representations of $D/I$ (as we can decompose $V$ into irreducible representations). In particular, a representation with $V^I = V$ is called unramified; else ramified.*

**Definition 19.39.** *For each representation $V$, define the characteristic polynomial of Frob on $V^I$ by*

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(V, t) = det_{V^I}(t \cdot 1 - Frob_{\mathfrak{q}/\mathfrak{p}}).$$

*So we can view $Frob_{\mathfrak{q}/\mathfrak{p}}$ sa an element in the general linear set.*

**Lemma 19.40.** *Let $\psi : D \longmapsto D/I \longmapsto \mathbb{C}^*$ be a 1-dimensional representation of $D$ with $\psi$(Frob)$= \zeta$. Then $\langle \psi, V\rangle = \langle \psi, V^I\rangle$ is the multiplicity of $(t - \zeta)$ in $\Phi_{\mathfrak{q}/\mathfrak{p}}(V, t)$.*

*Proof.* It is clear that

$$\langle \psi, V\rangle = \langle \psi, A \oplus B\rangle = \langle \psi, A\rangle + \langle \psi, B\rangle$$

where $A^I = 0$. But $\psi$ is a representation which is lifted from $D/I$. Hence $\psi$ is distinct from any irreducible component of $A$ (as $A^I = 0$). So $\langle \psi, A\rangle = 0$. Now $B = V^I$ so

$$\langle \psi, V\rangle = \langle \psi, V^I\rangle.$$

But $V^I = \oplus$1-dimensional representation lifted from $D/I$, so $V^I$ looks like a diagonal matrix with entries the $|D/I|^{\text{th}}$ roots of unity. In particular, $\langle \psi, V^I\rangle$ is the number of copies of $\psi$ in $V^I$. But $\psi$(Frob)$= \zeta$ and the representation is determined by $\zeta$ because Frob generates $D/I$.

Therefore, counting the number of copies of $\psi$ in $V^I$ is the same as counting the multiplicity of $t - \zeta$ in the characteristic polynomial. □

**Remark 19.41.** *Thus $\Phi$ simply encodes the multiplicity of the 1-dimensional representations of $D/I$ in a representation of $D$.*

**Proposition 19.42.** *Let $L$ be an intermediate extension of $F/K$. $V$ is a representation of $H = Gal(F/L)$. Then*

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(Res_D^G Ind_H^G V, t) = \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(Res^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right)$$

*where $\mathfrak{s}$ runs through the primes of $L$ above $\mathfrak{p}$ and $\mathfrak{q}_i$ lies above $\mathfrak{s}$ (this is true for any $\mathfrak{q}_i$ above $\mathfrak{s}$).*

*Proof.* We must show that LHS and RHS have the same roots with the same multiplicities. Note that the roots are $f_{\mathfrak{q}/\mathfrak{p}}$ $^{\text{th}}$ root of unity. Let $\zeta$ be such a root and take $\psi : D \longmapsto D/I \longmapsto \mathbb{C}^*$ with $\psi(\text{Frob}) = \zeta$. Then the multiplicity of $t - \zeta$ in LHS, is, by previous lemma,

$$\langle \psi, \text{Res}_D^G \text{Ind}_D^G V \rangle_D.$$

Now by Mackey's formula this gives

$$\sum_{x \in H\backslash G/D} \langle \psi, \text{Ind}^D_{x^{-1}Hx \cap D} \text{Res}^{x^{-1}Hx}_{x^{-1}Hx \cap D} V^x \rangle_D.$$

Recall the set of primes above $\mathfrak{p}$ is isomorphic to the double cosets $H\backslash G/D$. So summing over the double cosets representatives are the same as summing over the set of primes in $L$ above $\mathfrak{p}$ and $\mathfrak{s}$ corresponds to some element $x$ such that $x\mathfrak{q} = \mathfrak{q}_i$ where $\mathfrak{q}_i$ above $\mathfrak{s}$ (see previous results).

Since $D_{\mathfrak{q}_i} = xD_{\mathfrak{q}}x^{-1}$ so $D_{\mathfrak{q}} = x^{-1}D_{\mathfrak{q}_i}x$. Also, the character is invariant under conjugation and by definition of $\psi^{x^{-1}}$ we have

$$\begin{aligned}
\sum_{x \in H\backslash G/D} \langle \psi, \text{Ind}^D_{x^{-1}Hx \cap D} \text{Res}^{x^{-1}Hx}_{x^{-1}Hx \cap D} V^x \rangle_D &= \sum_{\mathfrak{s}} \langle \psi^{x^{-1}}, \text{Ind}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}} \\
&= \sum_{\mathfrak{s}} \langle \text{Res}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \psi^{x^{-1}}, \text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \rangle_{D_{\mathfrak{q}_i/\mathfrak{s}}} \\
&= \sum_{\mathfrak{s}} \text{ multiplicity of } t - \zeta^{f_{\mathfrak{s}/\mathfrak{p}}} \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t)
\end{aligned}$$

where in the first line we use $\psi^{x^{-1}}(x\rho x^{-1}) = \psi(\rho)$. The second line follows by Frobenius reciprocity and the third line follows from the Lemma 19.40. Also, since $\psi(\text{Frob}) = \zeta$, but if we restrict to $D_{\mathfrak{q}_i/\mathfrak{s}}$ then it is a $f_{\mathfrak{q}_i/\mathfrak{s}}$ $^{\text{th}}$ root of unity, so we need to raise $\zeta$ to a power of $f_{\mathfrak{s}/\mathfrak{p}}$. To be more previse, we can consider $\psi(\text{Frob}_{\mathfrak{q}_i/\mathfrak{s}})$ and we restrict to $D_{\mathfrak{q}_i/\mathfrak{s}}$ and we have

$$\text{Frob}_{\mathfrak{q}_i/\mathfrak{s}} = \text{Frob}^{f_{\mathfrak{s}/\mathfrak{p}}}_{\mathfrak{q}_i/\mathfrak{p}}.$$

Further, we have the equality

$$\sum_{\mathfrak{s}} \text{ multiplicity of } t - \zeta^{f_{\mathfrak{s}/\mathfrak{p}}} \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t) = \sum_{\mathfrak{s}} \text{ multiplicity of } t - \zeta \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right)$$

and the latter gives the multiplicity of $t - \zeta$ in RHS of the statement. □

**Corollary 19.43.** *Take $\psi_n : D \longmapsto D/I \longmapsto \mathbb{C}$ which sends Frob to a primitive $n^{th}$ root of unity (so $n \big| f_{\mathfrak{q}/\mathfrak{p}}$). Then*

$$\textit{the number of primes } \mathfrak{s} \textit{ of } L \textit{ above } \mathfrak{p} \textit{ with } n \big| f_{\mathfrak{s}/\mathfrak{p}} = \langle \psi_n, Res_D^G Ind_H^G 1_H \rangle_D.$$

*Proof.* From Lemma 19.40, and the previous proposition, we have

$$\begin{aligned}
\langle \psi_n, \text{Res}_D^G \text{Ind}_H^G 1_H \rangle_D &= \text{multiplicity of } t - \zeta_n \text{ in } \Phi_{\mathfrak{q}/\mathfrak{p}}(\text{Res}_D^G \text{Ind}_D^G 1_H, t) \\
&= \text{multiplicity of } t - \zeta_n \text{ in } \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} 1_H, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right).
\end{aligned}$$

Now 1 sends Frob to 1, and so this gives the multiplicity of $t - \zeta_n$ in $\prod_{\mathfrak{s}} \left(t^{f_{\mathfrak{s}/\mathfrak{p}}} - 1\right)$. Finally, $t - \zeta_n$ is a factor of $t^{f_{\mathfrak{s}/\mathfrak{p}}} - 1$ if and only if $n \big| f_{\mathfrak{s}/\mathfrak{p}}$. □

## 19.5 Exercises

1. Let $p, q$ be two distinct prime numbers, and let $n$ be the order of $q$ in $\mathbb{F}_p^*$. Show that there are $\frac{p-1}{n}$ primes in $\mathbb{Q}(\zeta_p)$ above $q$, each unramified with residue degree $n$.

2. Determine which primes ramify in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

3. Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial. By considering the highest common factor of $f$ and its derivatives, show that there are only finitely many prime numbers $p$ such that $f$ has a repeated root modulo $p$. Deduce that there are only finitely many primes that ramify in any given extension of number fields.

4. Let $f(X)$ be a non-constant polynomial with integer coefficients. By estimating the number of solutions to $-N < f(n) < N$ for $n \in \mathbb{N}$, show that the congruence

$$f(n) \equiv 0 \pmod{p}$$

is soluble for infinitely many prime numbers $p$.

Prove that in any extension of number fields there are always infinitely many primes that splits completely. (Hint: First reduce to the case of a Galois extension of $\mathbb{Q}$.)

5*. Let $K = \mathbb{Q}(\zeta_3)$. Recall that $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ is a unique factorisation domain. Write $\lambda = 1 - \zeta_3$ so $\langle\lambda\rangle^2 = \langle 3\rangle$.

(i) Find the possible residues of $\alpha^3$ modulo 9 for $\alpha \in \mathbb{Z}[\zeta_3]$ not divisible by $\lambda$.

(ii) Suppose that $u_1, u_2$ are units of $K$ and $\alpha, \beta \in \mathbb{Z}[\zeta_3]$ are not divisible by $\lambda$. Show that if

$$u_1\alpha^3 + u_2\beta^3 \equiv 0 \pmod{\lambda^3},$$

then $u_1 = \pm u_2$ and that the congruence must also hold modulo $\lambda^4$.

(iii) Show that the equation

$$x^3 + y^3 + u\lambda^{3k}z^3 = 0, \ (k \geq 1)$$

cannot have any solutions with $x, y, z \in \mathbb{Z}[\zeta_3]$ coprime to $\lambda$ and $u$ a unit. (Assume that the equation is satisfied with some $k \geq 2$. By factorising $x^3+y^3$ find a solution to the equation with $k$ replaced by $k-1$, and hence, by induction, with $k = 1$. Obtain a contradiction by (ii).)

(iv) Prove that the equation $x^3 + y^3 = z^3$ has no integer solutions with $x, y, z > 0$.

6. Let $L_1$ and $L_2$ be two extensions of a number field $K$ inside some common extension $M/K$. Show that if a prime $\mathfrak{q}$ of $K$ splits completely both in $L_1/K$ and $L_2/K$ then it splits completely in the composition $L_1L_2/K$. (Recall that $L_1L_2$ is the smallest subfield of $M$ containing both fields).

7. Let $F/K$ be a Galois extension of number fields with Galois group $G$. Let $\mathfrak{p}$ be a prime of $K$ and $\mathfrak{q}, \mathfrak{q}'$ primes of $F$ above $\mathfrak{p}$. Prove that the decomposition groups of $\mathfrak{q}$ and of $\mathfrak{q}'$ are conjugate in $G$, as are the inertia subgroups. When the inertia groups are trivial, prove that

the Frobenius elements $\mathrm{Frob}_{\mathfrak{q}}$ and $\mathrm{Frob}_{\mathfrak{q}'}$ are also conjugate. Thus, the decomposition group of $\mathfrak{p}$, the inertia group of $\mathfrak{p}$ and when $\mathfrak{p}$ is unramified, the Frobenius element at $\mathfrak{p}$ are well-defined up to conjugacy.

8. Let $F/K$ be a Galois extension of number fields with a cyclic Galois group of order $p^n$ ($p$ is prime and $n \geq 2$) and let $L$ be the unique intermediate field of degree $p$ over $K$. Show that if a prime $\mathfrak{q}$ of $K$ does not split in $L/K$, then it cannot split in $F/K$ either. Show also that if it is ramfied in $L/K$, then it must be totally ramified in $F/K$.

9. Set $\mathfrak{q} = \langle 11, \zeta_5 - 4 \rangle$, an unramified primes of $\mathbb{Q}(\zeta_5, \sqrt[5]{5})/\mathbb{Q}$ above 11 of residue degree 5. Determine the decomposition group at $\mathfrak{q}$ and the Frobenius element $\mathrm{Frob}_{\mathfrak{q}}$.

10. Consider the equation
$$y^2 + y = x^3 - x^2.$$
It has exactly four rational solutions $(x, y) = (0, 0), (0, -1), (1, 0)$ and $(1, -1)$. Now let $K$ be a number field, let $r_1$ (resp. $r_2$) be its real (resp. conjugate pairs of complex) embeddings and let $s_{11}$ be the number of primes above 11. It is a consequence of the conjecture of Birch and Swinnerton-Dyer that if $r_1 + r_2 + s_{11}$ is odd, then the equation must have infinitely many solutions over $K$.

    (i) For which quadratic fields does this criterion force the equation to have infinitely many solutions?

    (ii) For which degree 7 extensions of $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt[7]{m})(m \in \mathbb{Z})$ does it force the equation to have infinitely many solutions?

11. Let $K$ be a number field and $F = K(\sqrt{a}, \sqrt{b})$ a biquadratic extension. Fix a prime $\mathfrak{p}$ of $K$ and let $n_L$ denote the number of primes in $L$ above $\mathfrak{p}$. Prove that
$$n_F + 2n_K = n_{K(\sqrt{a})} + n_{K(\sqrt{b})} + n_{K(\sqrt{ab})}.$$
Prove that the same formula holds when $n_L$ denotes the number of primes above $\mathfrak{p}$ with residue degree 2, but that it need not hold for the number of primes with ramification degree 2. (You may find it helpful to note that for $G = C_2 \times C_2$,
$$\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}[G] \cong \mathrm{Ind}_{C_2^{(1)}}^G 1 \oplus \mathrm{Ind}_{C_2^{(2)}}^G 1 \oplus \mathrm{Ind}_{C_2^{(3)}}^G 1,$$
where $C_2^{(1)}, C_2^{(2)}, C_2^{(3)}$ are the three subgroups of $G$ of order 2.)

12. Let $F/\mathbb{Q}$ be a Galois extension with Galois group $G = \mathrm{GL}_2(\mathbb{F}_l)$, for $l$ an odd prime, and let $K$ be the fixed field of the Borel subgroup $B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_l)$. Suppose that $\mathfrak{p}$ is a prime of $F$ above the rational prime $p$, with decomposition group $D_{\mathfrak{p}} = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ and intertia subgroup $I_{\mathfrak{p}} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Show that there are exactly two primes in $K$ above $p$, each with residue field $\mathbb{F}_p$.

13. Let $f(X)$ be a monic irreducible polynomial with integer coefficients, of degree 5. Suppose that its splitting field $F/\mathbb{Q}$ has Galois group $D_{10}$, which in its action on the five roots $\alpha_1, \ldots, \alpha_5$ is generated by the 5-cycle $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$ and the order-2 element $(\alpha_2\ \alpha_5)(\alpha_3\ \alpha_4)$. Show that

$$n = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1$$

is an integer.

Suppose $p$ is a prime such that $f(X)$ mod $p$ is irreducible. Show that it is unramified and has residue degree 5 in $F/\mathbb{Q}$, and deduce that the Frobenius element of any prime above $p$ acts as a 5-cycle on the $\alpha_i$. Show further that if $\beta$ denotes a root of $f(X)$ mod $p$ in $\mathbb{F}_{p^5}$ and $\beta_i = \beta^{p^{i-1}}$, then

$$m = \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta_5 + \beta_5\beta_1$$

lies in $\mathbb{F}_p$ and that if $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$ is the Frobenius element of some prime above $p$, then $m \equiv n \bmod p$.

Now consider $f(X) = X^5 + 2X^4 - 3X^3 + 1$. It has Galois group $D_{10}$. Its complex roots are

$$\alpha_1 = -3.01\ldots, \alpha_2 = -0.35\ldots - 0.53\ldots i, \alpha_3 = 0.85\ldots - 0.31\ldots i, \alpha_4 = \bar{\alpha}_3, \alpha_5 = \bar{\alpha}_2,$$

and the Galois group contains the 5-cycle $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$. Prove that the Frobenius element of a prime above 2 in the splitting field of $f$ has order 5 and determine its conjugacy class in the Galois group.

## 19.6 Hint and Solutions

1. $X^p - 1$ is separable over $\mathbb{F}_q$ so $q$ does not ramify in $\mathbb{Q}(\zeta_p)$ by Kummer-Dedekind. Pick any $\mathfrak{q}$ above $q$ in $\mathcal{O}_K$. Since it is unramified, the decomposition group is isomorphic to $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{q}/\mathbb{Z}/q)$ and it is cyclic, generated by $\mathrm{Frob}_\mathfrak{q}$.

   We know $\mathrm{Frob}_\mathfrak{q}(\zeta_p) = \zeta_p^q \bmod \mathfrak{q}$ and since $X^p - 1$ is separable, so we conclude that $\mathrm{Frob}_\mathfrak{q}(\zeta_p) = \zeta_p^q$. Also the order of $\mathrm{Frob}_\mathfrak{q}$ is the order of $q$ in $(\mathbb{Z}/p\mathbb{Z})^*$ and so it is $n$ by assumption.

   Since $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois, and so we have $ref = p - 1$. But $e = 1$, and $f = n$, so the number of primes is $r = \frac{p-1}{n}$.

   Alternatively, we could look at $\mathbb{F}_q(\gamma)$ where $\gamma$ is a primitive root of $X^p - 1$ and $\gamma \in \bar{\mathbb{F}}_q$. Let the minimal polynomial of $\gamma$ have degree $d$. Then we have $\mathbb{F}_q(\gamma) = \mathbb{F}_{q^d}$ and so $\gamma^{q^d} = \gamma$. But $\gamma^p = 1$ so $d$ is the least number such that $q^d - 1$ is divisible by $p$, which is $n$ by definition.

   So we know that each irreducible factor of $\frac{X^p-1}{X-1}$ over $\mathbb{F}_q$ has degree $n$. Then the result follows by Kummer-Dedekind.

2. Clearly $\langle 2\rangle = \langle \sqrt[3]{2}\rangle^3$ and so 2 ramifies. For 3, let $\alpha = 1 + \sqrt[3]{2}$, then $(\alpha - 1)^3 = 2$ and so $\alpha^3 \equiv 0 \pmod 3$. The minimal polynomial of $\alpha$ is

$$X^3 - 3X^2 + 3X - 3 = 0.$$

   The norm of $\alpha$ is then $(-1)^3(-3) = 3$. Now $3 \big| \alpha^3$ so $\langle 3\rangle I = \alpha^3$ for some ideal $I$. Now compare the norm. We know $N(\langle 3\rangle) = 27$. $N(\alpha^3) = (N(\alpha))^3 = 27$ so the norm of $I$ is 1. Therefore, $\alpha^3 = \langle 3\rangle$ and so 3 ramifies.

   For $p > 3$, the minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$ which is separable mod $p$. Then by Corollary 19.14, $p$ is unramified.

3. By Gauss's lemma, $f$ is irreducible over $\mathbb{Q}[X]$ and hence separable. There exist $\alpha(X), \beta(X) \in \mathbb{Q}[X]$ such that
$$f(X)\alpha(X) + f'(X)\beta(X) = 1.$$
Now if $p$ does not divide the denominator of the coefficients of $\alpha, \beta$, then we can reduce the above to
$$\bar{f}(X)\bar{\alpha}(X) + \bar{f}'(X)\bar{\beta}(X) = 1$$
and so $f(X), f'(X)$ have no common factor mod $p$, which implies $f(X)$ has no repeated roots mod $p$. But we only have finitely many $p$ such that $p$ divides one of the denominators of $\alpha(X), \beta(X)$. Hence there are only finitely many prime $p$ such that $f(X)$ has repeated roots mod $p$.

There are only finitely many $p$ which divides the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ where $K = \mathbb{Q}(\alpha)$ and then for $p$ does not divide the index we can apply Kummer-Dedekind, and $p$ ramifies if and only if $f(X)$ mod $p$ has repeated roots. So there are only finitely many primes which ramify.

4. For $N$ large enough we roughly have $N^{\frac{1}{d}}$ solutions where $d$ is the degree of $f$. Suppose it is only soluble for finitely many primes say $p_1, \ldots, p_k$, then $f(n)$ in $[-N, N]$ only takes value which is a product of powers of $p_i$ and so we have at most $\log_{p_1} N \cdots \log_{p_k} N \leq (\log_2 N)^k$ solutions. But $N^{\frac{1}{d}} > (\log_2 N)^k$ for $N$ large enough and so it is impossible.

Here is a more convincing method. Let $a_0$ be the constant term of $f(X)$. If $a_0 = 0$ then $x = o$ gives $f(X) \equiv 0 \pmod{p}$ for all $p$. So we may assume $a_0 \neq 0$. Consider
$$f(a_0 tX) = a_0 + a_1 a_0 tX + \cdots = a_0[1 + a_1 tX + a_2 t^2 a_0 X^2 + \cdots] = a_0 Q(X).$$
Suppose it is only soluble for finitely many $p$, say $p_1, \ldots, p_k$, let $t = p_1 \cdots p_k$. Then as $Q$ has finite degree, given such $t$, there exists $x$ such that $Q(x) \neq \pm 1, 0$ and so $Q(x)$ has a prime factor, say $p$. But
$$Q(x) = 1 + a_1 tx + a_2 t^2 a_0 x^2 + \cdots \equiv 1 \pmod{t}.$$
So the prime factor $p$ is prime to $t$ and hence $p \neq p_i$ for any $i$, which is a contradiction.

Now let $K/\mathbb{Q}$ be a Galois extension of number fields. Firstly, we eliminate a finite set of primes $s$ which contains $p$ such that $p \big| [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, where $K = \mathbb{Q}(\alpha)$. Let $f(X)$ be the minimal polynomial of $\alpha$. So for the rest of primes, we can apply Kummer-Dedekind. But we know $f(X) \equiv 0 \pmod{p}$ is soluble for infinitely many $p$ and if it is soluble, then $p$ has a prime $\mathfrak{p}$ above it such that $e_{\mathfrak{p}/p} = f_{\mathfrak{p}/p} = 1$. But $K$ is Galois over $\mathbb{Q}$ so $e = f = 1$ and so $p$ splits completely.

In general, let $L$ be the Galois closure of $K/\mathbb{Q}$. Then by above, we have infinitely many $p$ which splits completely in $L$ and hence in $K$.

5. (i) Consider $0, 1, 2, -\zeta_3, -2\zeta_3, 1 - \zeta_3, 1 - 2\zeta_3, 2 - \zeta_3, 2 - 2\zeta_3$ because for
$$(a + b\zeta_3)^3 \equiv (a - 3 + b\zeta_3)^3 \equiv (a + b\zeta_3 - 3\zeta_3)^3 \pmod{9}.$$
From above $-\zeta_3$ is a unit. So it is easy to check that $\alpha^3$ mod 9 all give $\pm 1$.

(ii) The units are $\pm 1, \pm\zeta_3, \pm\zeta_3^2$. We may assume $u_1 = 1$, otherwise we just multiply both sides by a unit, and it will not change the congruence. Now $\lambda^3 = 3(1 - \zeta_3)$ but as $\alpha^3, \beta^3 \equiv 1 \pmod{9}$ by (i), and hence is $\pm 1$ mod 3. So we must have $u_2 = \pm - 1$.
Further, $\alpha^3, \beta^3$ can only be $\pm 1$ mod 9 and so if the congruence holds for $\lambda^3$, then it holds for 3 and hence holds for 9 ($\lambda^4 = 9u$ for some unit $u$).

(iii) Let

$$x^3 + y^3 = (x + y)(x + \zeta_3 y)(x + \zeta^2 y).$$

Since $x^3 + y^3 \equiv 0 \pmod{\lambda^{3k}}$ and $\lambda$ is a prime (since it has norm 3) so $\lambda$ divides at least one of the three factors. Also, $\mathbb{Z}[\zeta_3]$ is a UFD, so $\lambda$ is irreducible.

By unique factorisation, at least one of them is divisible by $\lambda^2$, say $x + y$ (otherwise we can replace $y$ by $\zeta_3 y$ or $\zeta_3^2 y$). Consider

$$x + \zeta_3 y = x + y - (1 - \zeta_3)y = x + y - \lambda y.$$

By assumption, $\lambda \nmid y$, so $\lambda^2 \nmid \lambda y$ and as $\lambda^2 \big| x + y$, we conclude $\lambda \big| x + \zeta_3 y$ and $\lambda^2$ does not. Similarly, this holds for $x + \zeta_3^2 y$. This shows that $x + y$ is divisible by $\lambda^{3k-2}$. Now let $\pi$ be any irreducible factor dividing $x + y, x + \zeta_3 y$, then $\pi \big| y(1 - \zeta_3) = \lambda y$, and thus $\pi \big| y$ or $\pi \big| \lambda$ (recall UFD means irreducible is the same as prime). Also, $\pi \big| \zeta_3 - x = -\lambda x$ so $\pi \big| x$ or $\pi \big| \lambda$. Without loss of generality, we may assume that $x, y, z$ have no common factor. If $\pi \big| x, \pi \big| y$ then $\pi \big| z$ which is a contradiction so we conclude $\pi \big| \lambda$ and so $\pi = \lambda$. The conclusion also holds for $x + y, x + \zeta_3^2 y$. So the only pairwise common factor is $\lambda$.

Now $(x + y)(x + \zeta_3 y)(x + \zeta_3^2 y) = -u\lambda^{3k} z^3$. With the above deduction, we can set

$$x + y = \epsilon_1 \lambda^{3k-2} x'^3,$$

$$x + \zeta_3 y = \epsilon_2 \lambda y'^3,$$

$$x + \zeta_3^2 y = \epsilon_3 \lambda z'^3,$$

where $\epsilon_1, \epsilon_2, \epsilon_3$ are units. This is because $-u\lambda^{3k} z^3$ is a cube times a unit and LHS has no common factor except $\lambda$. Therefore,

$$\epsilon_1 \epsilon_2 \epsilon_3 x'^3 y'^3 z'^3 = -uz^3$$

and so

$$\epsilon_1 \epsilon_2 \epsilon_3 = -u, z = x' y' z'$$

and $x', y', z'$ have no common factor.

As $1 + \zeta_3 + \zeta_3^2 = 0$ so combine the three equations above we have

$$0 = \epsilon_1 \lambda^{3k-2} x'^3 + \epsilon_2 \lambda y'^3 \zeta_3 + \epsilon_3 \lambda z'^3 \zeta_3^2$$

and so

$$y'^3 + \frac{\epsilon_3}{\epsilon_2} \zeta_3 z'^3 + \frac{\epsilon_1}{\epsilon_2 \epsilon_3} \lambda^{3k-3} x'^3 = 0.$$

Now $\frac{\epsilon_3}{\epsilon_2} \zeta_3 \in \mathbb{Z}[\zeta_3]$. Apply division algorithm of any $a + b\zeta_3$ to $\lambda$, we have

$$\frac{\epsilon_3}{\epsilon_2} \zeta_3 \equiv \pm 1 \pmod{\lambda}.$$

Then

$$\left( \frac{\epsilon_3}{\epsilon_2} \zeta_3 \right)^3 \equiv \pm 1 \pmod{\lambda^3}.$$

By (ii), we conclude that $\frac{\epsilon_3}{\epsilon_2} \zeta_3 = \pm 1$. Assume it is 1 (if it is $-1$ then we replace this by $-\frac{\epsilon_3}{\epsilon_2} \zeta_3$ and use $-z'^3 = (-z')^3$).

Also $\frac{\epsilon_1}{\epsilon_2} \zeta_3$ is a unit, say $u'$ so

$$y'^3 + z'^3 + y' \lambda^{3k-3} x'^3 = 0.$$

So we have found a solution for $k-1$.
For the case $k=1$, if $x^3+y^3+u\lambda^3z^3=0$, then $x^3+y^3\equiv 0 \pmod{\lambda^3}$ and so by (ii)

$$x^3+y^3\equiv 0 \pmod{\lambda^4}.$$

So $\lambda\big|uz^3$ which implies $\lambda\big|z$, a contradiction to the assumption.

(iv) For $X^3+Y^3=Z^3$, consider the solutions in $\mathbb{Z}[\zeta_3]$. We may assume $(x,y,z)$ coprime. We firstly assume $\lambda\big|z$ and $\lambda\nmid x,y$ then let $z=z'\lambda^k$. Thus,

$$x^3+y^3-\lambda^{3k}z'^3=0$$

has no solution by (iii).
Then assume $\lambda\big|x$, then

$$x^3=z^3-y^3=z^3+(-y)^3$$

which has no solution by the previous case (here $x$ is $z$ in the first case).
Finally, assume $\lambda\nmid x,y,z$ (since we assume $x,y,z$ have no common factor, so $\lambda$ cannot divide more than one of them). Then $x^3+y^3\equiv \pm 1\pm 1 \pmod{\lambda^3}$, (consider the residue modulo $\lambda^3$ in $\mathbb{Z}[\zeta_3]$) which is $-2,0$ or $2$. So $z^3\equiv -2,0$ or $2 \bmod \lambda^3$. But $z^3\equiv \pm 1 \pmod{\lambda^3}$, so this gives a contradiction.
Hence it has no solutions in $\mathbb{Z}[\zeta_3]$ and hence no integer solutions.

6. Let $F$ be the Galois closure of $L_1L_2$. Let $\mathcal{P}$ be a prime of $F$ above $\mathfrak{q}$. Let $\mathfrak{p}_1,\mathfrak{p}_2$ be primes above $\mathfrak{q}$ in $L_1,L_2$ respectively. Since $\mathfrak{q}$ splits completely in both $L_1,L_2$, it is clear that

$$e(\mathfrak{p}_1/\mathfrak{q})=e(\mathfrak{p}_2/\mathfrak{q})=1, f(\mathfrak{p}_1/\mathfrak{q})=f(\mathfrak{p}_2/\mathfrak{q})=1$$

and so the decomposition group has

$$D_{\mathcal{P}/\mathfrak{q}}=D_{\mathcal{P}/\mathfrak{p}_1}=D_{\mathcal{P}/\mathfrak{p}_2}.$$

In particular, $D_{\mathcal{P}/\mathfrak{q}}\subset \mathrm{Gal}(F/L_2)$, $\mathrm{Gal}(F/L_1)$. So it fixes both $L_1$ and $L_2$ and so if fixes $L_1L_2$.
Thus, for any $\mathfrak{p}$ below $\mathcal{P}$, but above $\mathfrak{p}_1$ in $L_1L_2$, we have

$$D_{\mathcal{P}/\mathfrak{q}}=D_{\mathcal{P}/\mathfrak{p}}.$$

This shows that for any prime $\mathfrak{p}$ above $\mathfrak{p}_1$ in $L_1L_2$, we have

$$e(\mathfrak{p}/\mathfrak{p}_1)=f(\mathfrak{p}/\mathfrak{p}_1)=1$$

and similarly for prime above $\mathfrak{p}_2$. In particular, this shows that $e(\mathfrak{p}/\mathfrak{q})=f(\mathfrak{p}/\mathfrak{q})=1$ and so $\mathfrak{q}$ splits completely.

7. Let $G=\mathrm{Gal}(F/K)$. By definition

$$D_{\mathfrak{q}/\mathfrak{p}}=\{\sigma\in G:\sigma(\mathfrak{q})=\mathfrak{q}\}, D_{\mathfrak{q}'/\mathfrak{p}}=\{\sigma\in G:\sigma(\mathfrak{q}')=\mathfrak{q}'\}.$$

Let $\tau\mathfrak{q}=\mathfrak{q}'$ for some $\tau\in G$. Then

$$\tau h\tau^{-1}(\mathfrak{q}')=\tau h(\mathfrak{q})=\tau(\mathfrak{q})=\mathfrak{q}'\ \forall h\in D_{\mathfrak{q}/\mathfrak{p}}.$$

So $\tau D_{\mathfrak{q}/\mathfrak{p}}\tau^{-1}=D_{\mathfrak{q}'/\mathfrak{p}}$.

Similarly, we can show $\tau I_{\mathfrak{q}/\mathfrak{p}}\tau^{-1} = \tau I_{\mathfrak{q}'/\mathfrak{p}}\tau^{-1}$.

If the inertia group is trivial, then $\langle \text{Frob}_{\mathfrak{q}} \rangle = D_{\mathfrak{q}/\mathfrak{p}}$ and $\langle \text{Frob}_{\mathfrak{q}'} \rangle = D_{\mathfrak{q}'/\mathfrak{p}}$. Also, $\text{Frob}_{\mathfrak{q}}(x) \equiv x^f \pmod{\mathfrak{q}}$ and so

$$\tau \text{Frob}_{\mathfrak{q}} \tau^{-1}(x) \equiv \tau(\tau^{-1}(x)^f) \equiv x^f \pmod{\mathfrak{q}'}.$$

So $\tau \text{Frob}_{\mathfrak{q}} \tau^{-1}$ must be $\text{Frob}_{\mathfrak{q}'}$ as they act the same.

8. Let $L_i$ be the unique intermediate field of degree $p^i$. It is unique because $G$ is cylic of order $p^n$. We shall prove the following statement: if $\mathfrak{p}$ is a prime in $L_{i-1}$ which does not split in $L_i$, then it does not split in $L_{i+1}$. Then the result follows by induction. Note that each $L_i/L_{i-1}$ is Galois with degree $p$. So $ref = p$ and we have $r = 1$ or $p$.

   If it does not split in $L_i$ then $r = 1$. $\text{Gal}(L_{i+1}/L_i) = C_{p^2}$. Let $\amalg$ be the unique prime above $\mathfrak{p}$ in $L_i$ and let $\mathcal{P}$ be a prime above $\mathfrak{q}$ in $L_{i+1}$. Consider the decomposition group $D_{\mathcal{P}}$. Let $r', e', f'$ be the corresponding index for $L_{i+1}/L_i$. Then $r' = p$ or 1.

   Suppose $r' = p$, then in the extension $L_{i+1}/L_{i-1}$, we have $r''e''f'' = p^2$, and $r'' = p$. So $e''f'' = p$ and the decomposition group has size $p$. But it is a subgroup of $C_{p^2}$ so it has to be $C_p$. Thus, the decomposition group lies in $\text{Gal}(L_{i+1}/L_i)$. This implies that $e'f' = p$, which is a contradiction. Therefore, $r' = 1$.

   Similarly, for the ramification, we check that if it is ramified in $L_i/L_{i-1}$, with ramification degree $p$, then it also ramifies in $L_{i+1}/L_{i-1}$. This time we consider the inertia group. Let $\mathfrak{q}$ be the unique prime above $\mathfrak{p}$ in $L_i$. If $\mathfrak{q}$ is unramified, then in $L_{i+1}/L_{i-1}$ the ramification degree of $\mathfrak{p}$ is $p$ and so the inertia group is cyclic of order $p$, which again lies in $\text{Gal}(L_{i+1}/L_i)$. This implies that $\mathfrak{q}$ is ramified, which gives a contradiction.

9. Let $F = \mathbb{Q}(\zeta_5, \sqrt[5]{5}), K_1 = \mathbb{Q}(\zeta_5), K_2 = \mathbb{Q}(\sqrt[5]{5})$. Let $\mathfrak{q}$ be a prime of $F$ above 11 and so $f_{\mathfrak{q}/11} = 5$. Now $ref = 20$ so $re = 4$ (check $F/\mathbb{Q}$ has degree 20). It is easy to check 11 does not ramify so $e = 1$. Thus, $D_{\mathfrak{q}} = C_5 = \langle \text{Frob}_{\mathfrak{q}} \rangle$.

   $\text{Forb}_{\mathfrak{q}}(\zeta_5) = \zeta^1 1_5 = \zeta_5$, $\text{Frob}_{\mathfrak{q}}(\sqrt[5]{5}) \equiv 25\sqrt[5]{5} \bmod \mathfrak{q}$. So it is an element in $\text{Gal}(F/K_1)$. Let $\zeta^k \equiv 25 \pmod{\mathfrak{q}}$. We know $\zeta_5 - 4 \in \mathfrak{q}$ so $\zeta_5 \equiv 4 \pmod{\mathfrak{q}}$ and so $k = 4$. Therefore, $\text{Frob}_{\mathfrak{q}}$ corresponds to the element

$$\sigma(\sqrt{5}) = \zeta_5^4\sqrt{5}, \sigma(\zeta_5) = \zeta_5.$$

10. (i) Let $K = \mathbb{Q}(\sqrt{d})$. When $d > 0$, then $r_1 = 2, r_2 = 0$ so we need $s_{11} = 1$. So we have one prime above 11, i.e. 11 does not split. If $11 \nmid d$, then $X^2 - d$ has distinct roots mod 11 in $\bar{\mathbb{F}}_{11}$ and so Kummer-Dedekind applies. So 11 does not ramify. If $11 \big| d$ then $d = 11m$, and we have

$$\langle 11, \sqrt{d} \rangle^2 = \langle 11 \rangle \left\langle 11, \sqrt{d}, \frac{d}{11} \right\rangle.$$

    But $d$ is square free and so it is prime to 11m thus, $\langle 11 \rangle = \langle 11, \sqrt{d} \rangle^2$. When 11 inerts, we have $\left(\frac{d}{11}\right) = -1$ and so $d$ is $2, 6, 7, 8$ or 10 mod 11. Together, $d$ can be $0, 2, 6, 7, 8$ mod 11. When $d < 0$, $r_1 = 0, r_2 = 1$ so we want 11 splits. Thus, $d$ can be $1, 3, 4, 5, 9, 13$ mod 11.

    (ii) Let $K = \mathbb{Q}(\sqrt{m})$. If $11 \big| m$, then let $m = 11^a b$ where $(7, a) = 1$ because $11^7 \nmid m$ and $(11, b) = 1$. Then

$$\langle m \rangle = \langle \sqrt[7]{m} \rangle^7 = \langle 11 \rangle^a \langle b \rangle.$$

    Since $(7, a) = 1$ so $\langle 11 \rangle$ must be a $7^{\text{th}}$ power and so 11 ramifies.

When $11 \nmid m$, note that $\zeta_7 \in \mathbb{F}_{11^3}$ because $7 \big| 11^3 - 1$. Also, $m^{-21} \equiv m \pmod{11}$ so that $m^{-3}$ is a root of $f(X) = X^7 - m \bmod 11$. Now $f(X)$ mod 11 has splitting field $\mathbb{F}_{11^3}$ because $m^{-3}, \zeta_7 m^{-3}, \ldots$, are all the roots. So $f(X)$ factorises as

$$f(X) = (X - m^{-3})(X^3 + \cdots)(X^3 + \cdots)$$

because the degree of the splitting field is 3. So $s_{11} = 3$. But $r_1 = 1, r_2 = 3$ so it is always odd.

Alternatively, we can consider $F = K(\zeta_7), L = \mathbb{Q}(\zeta_7)$. If $11 \nmid m$, we can count the number of primes in $K$ by considering the $D_{\mathfrak{q}}$-orbits on the embeddings $\sqrt[7]{m}, \zeta_7\sqrt[7]{m}, \ldots, \zeta_7^6\sqrt[7]{m}$, where we fix a prime $\mathfrak{q}$ above 11 in $F$. Then in $L$, since 11 has order 3 in $(\mathbb{Z}/7\mathbb{Z})^*$, so $\frac{X^7-1}{X-1}$ has two irreducible factors modulo 11, both of which have degree 3 (see question 1). Let $\mathfrak{p}$ be a prime above 11 in $L$. Then $f_{\mathfrak{p}/11} = 3$, $e_{\mathfrak{p}/11} = 1$. Then consider $\mathfrak{q}/\mathfrak{p}$. We know

$$r_{\mathfrak{q}/\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} = 7.$$

Suppose it is ramified, then $e_{\mathfrak{q}/\mathfrak{p}} = 7$. But 11 does not ramify in $K$, and so the ramification degree is at most 6, which is a contradiction.

So $e_{\mathfrak{q}/\mathfrak{p}} = 1$ and so $I = \{id\}$. $f_{\mathfrak{q}/11} = 3$ or 21 , but the decomposition group is a subgroup of $S_7$ so it is 3.

Now we may assume that $D_{\mathfrak{q}/11}$ fixes $\sqrt[7]{m}$. Then $\mathrm{Frob}_{\mathfrak{q}}(\zeta_7\sqrt[7]{m}) = \zeta_7^4\sqrt[7]{m}$, $\mathrm{Frob}_{\mathfrak{q}}(\zeta_7^4\sqrt[7]{m}) = \zeta_7^2\sqrt[7]{m}$, and $\mathrm{Frob}_{\mathfrak{q}}(\zeta_7^2\sqrt[7]{m}) = \zeta 7\sqrt[7]{m}$. So we can see $D_{\mathfrak{q}}$ has two orbits apart from $\sqrt[7]{m}$ and it has three orbits in total so $s_{11} = 3$.

11. Let $L = K(\alpha)$ and $x_L$ be the set of roots of the minimal polynomial of $\alpha$. For a tower of extensions $F/L/K$, the number of primes above $\mathfrak{p}$ in $L$ is the number of $D_{\mathfrak{q}/\mathfrak{p}}$ orbits on $x_L$, where $\mathfrak{q}$ is a prime above $\mathfrak{p}$ in $F$. Recall that

$$\mathbb{C}[x_L] \cong \mathbb{C}[G/H] \cong \mathrm{Ind}_H^G 1_H$$

where $H =$Gal$(F/L)$.

Using the hint, we have

$$\mathbb{C}[x_K] \oplus \mathbb{C}[x_K] \oplus \mathbb{C}[x_F] \cong \mathrm{Ind}_{C_2^{(1)}}^G 1 \oplus \mathrm{Ind}_{C_2^{(2)}}^G 1 \oplus \mathrm{Ind}_{C_2^{(3)}}^G 1 \cong \mathbb{C}[x_{K(\sqrt{a})}] \oplus \mathbb{C}[x_{K(\sqrt{b})}] \oplus \mathbb{C}[x_{K(\sqrt{ab})}].$$

Let $\chi_L$ be the character of $\mathbb{C}[x_L]$. Then we have

$$2\chi_K + \chi_L = \chi_{K(\sqrt{a})} + \chi_{K(\sqrt{b})} + \chi_{K(\sqrt{ab})}.$$

Taking restriction we have

$$\mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G 2\chi_K + \mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G \chi_L = \mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G \chi_{K(\sqrt{a})} + \mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G \chi_{K(\sqrt{b})} + \mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G \chi_{K(\sqrt{ab})}.$$

Now the number of $D_{\mathfrak{q}/\mathfrak{p}}$ ortbis on $x_L$ is

$$\langle \mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}}^G \chi_L, 1 \rangle_{D_{\mathfrak{q}/\mathfrak{p}}}.$$

So use the previous equation we have

$$2n_K + n_L = n_{K(\sqrt{a})} + n_{K(\sqrt{b})} + n_{K(\sqrt{ab})}.$$

Now for the second part, it is easier to do it by checking cases (instead of using representation). For a counter example, consider $p = 2$ in $F = \mathbb{Q}(i, \sqrt{2})$. 2 is totally ramified, and so $n_F = 0, n_K = 0$. But each intermediate field gives $n_L = 1$.

12. The number of primes in $K$ is the number of double coset $B\backslash G/D$. This is the same as the number of $D\backslash G/B$. To see this, consider

$$Bg \mapsto g^{-1}H$$

which is a bijection and so $D \times \{Bg\} \mapsto D \times \{g^{-1}B\}$ is a bijection via $d(Bg) \mapsto Bgd^{-1}$.

Now we have $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ a & b \end{pmatrix}$. So for each $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$Dg = S_{a,b} = \left\{ \begin{pmatrix} * & * \\ a & b \end{pmatrix} : ab \neq 0 \right\}.$$

For $S_{a,b}B$, we have two cases: when $a = 0$, then

$$S_{a,b}B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} = B.$$

When $a \neq 0$, then

$$S_{a,b}B = \left\{ \begin{pmatrix} * & * \\ * & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_l)\backslash B \right\}$$

because $\begin{pmatrix} * & * \\ a & b \end{pmatrix}\begin{pmatrix} c & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} * & * \\ ac & * \end{pmatrix}$ and $c \neq 0$ because it is invertible.

So we have these two double cosets and hence two primes. Now the size of the inertia group is $l$ and the size of the decomposition group is $l(l-1)$ so $f_{\mathfrak{p}/p} = l - 1$. Let $\mathfrak{s}$ be the prime below $\mathfrak{p}$. We have $|B| = (l-1)^2 l$ and $|G| = (l-1)^2 l(l+1)$ so $[K : \mathbb{Q}] = l + 1$. Also by tower law $e_{\mathfrak{s}/p} = 1$ or $l$.

We know $D_{\mathfrak{p}} \subset B$ and so $D_{\mathfrak{p}} = D_{\mathfrak{p}/\mathfrak{s}}$ so $e_{\mathfrak{s}/p} = f_{\mathfrak{s}/p} = 1$. Let $\mathfrak{s}'$ be another prime in $K$ above $p$. Note that $\mathfrak{s}'$ does not necessarily lie below $\mathfrak{p}$. Then we have

$$1 + e_{\mathfrak{s}'/p} f_{\mathfrak{s}'/p} = l + 1$$

and so $e_{\mathfrak{s}'/p} f_{\mathfrak{s}'/p} = l$. But $f_{\mathfrak{s}'/p} \big| l - 1$ because $F/\mathbb{Q}$ is Galois and so for any $\mathfrak{p}'$ above $\mathfrak{s}'$ we still have $f_{\mathfrak{p}'/p} = l - 1$. So $f_{\mathfrak{s}'/p} = 1$.

13. It is easy to check that $n$ is fixed by $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha\ 5)$ and $(\alpha_2\ \alpha_5)(\alpha_3\ \alpha_4)$ and so $n$ is fixed by the Galois group so it is a rational number. But $\alpha_i \in \mathcal{O}_F$ and so $n \in \mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$.

Let $\alpha$ be a root of $f(X)$. We know $f(X)$ is irreducible mod $p$ and finite extension is always separable, so it has distinct roots in $\overline{\mathbb{F}}_p$ and so Kummer-Dedekind applies. Thus $p$ inerts in $\mathbb{Q}(\alpha)$. Now the residue degree is divisible by 5, because $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree 5. So the residue degree of $p$ in $F$ is either 5 or 10. If it is 10, then the decomposition group is isomorphic to $C_{10}$, which is impossible as $C_{10}$ does not lie in $D_{10}$. So the residue degree is 5.

The ramification degree is either 1 or 2. If it is 2, then the decomposition group is $D_{10}$ and the inertia group is $C_2$, as a normal subgroup of $D_{10}$, which is a contradiction. Hence $e = 1$, and the decomposition group is $C_5$. The Frobenius element corresponds to the 5 cycle.

Recall that the Galois group of finite extension is generated by Frobenius element. $\mathrm{Frob}_{\mathfrak{q}}(\beta) = \beta^p = \beta_2$ and similarly, we can check this for other $\beta_i$. So we conclude that the Frobenius element corresponds to the 5-cycle $(\beta_1\ \beta_2\ \beta_3\ \beta_4\ \beta_5)$. Now $m$ is fixed by this element and so it is fixed by $\mathrm{Gal}(\mathbb{F}_{p^5}/\mathbb{F}_p)$ and so it lies in $\mathbb{F}_p$.

Let $\mathfrak{q}$ be a prime above $p$ in $F$. Now $\mathrm{Frob}_{\mathfrak{q}} = (\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$. Consider the reduction

$$n \equiv \bar{\alpha}_1\bar{\alpha}_2 + \cdots + \bar{\alpha}_5\bar{\alpha}_1 \pmod{p}.$$

Each $\bar{\alpha}_i$ is a root of $f(X)$ mod $p$. So we may assume that $\bar{\alpha}_1 = \beta_1$.

Set $\alpha = \alpha_1$. Let $\bar{\alpha}^5 + a_4\bar{\alpha}^4 + \cdots + a_0 = 0$, where $a_i \in \mathbb{F}_p$. Raise both sides to the power of $p$, we have

$$\bar{\alpha}^{5p} + a_4\bar{\alpha}^{4p} + \cdots + a_0 = 0$$

using $a_i^p = a_i$. So $\bar{\alpha}^p$ is also a root and similarly $\bar{\alpha}^{p^{i-1}}$ is also a root. So we may assume that $\bar{\alpha}_i = \beta_1$ and so $m \equiv n \pmod{p}$.

Now $f(X) = X^5 + 2X^4 - 3X^3 + 1$. It is irreducible and the splitting field is $D_{10}$. It is also irreducible mod 2. So by previous part, the Frobenius element has order 5.

Wrting $\mathbb{F}_{2^5} = \mathbb{F}_2[\beta] \cong \mathbb{F}_2[X]/\langle X^5 + X^3 + 1\rangle$, via $\beta \mapsto X$. Then we have

$$m = X^3 + X^6 + X^{12} + X^{24} + X^{48} = 0 \text{ where } X^5 +^3 +1 = 0$$

and so we know $n$ must be even. Now we have two conjugacy classes:

$$\mathcal{C}_1 = \{(1\ 2\ 3\ 4\ 5), (1\ 5\ 4\ 3\ 2)\}, \mathcal{C}_2 = \{(1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3)\}.$$

Now by the previous part, $n \equiv m \bmod 2$ when the Frobenius element corresponds to $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$. So the labeling is a bit confusing. If it is (1 2 3 4 5) (i.e. the labeling which is given in the question $\alpha_1 = -3.01\ldots$ etc.) then $n$ is approximately 3, which is odd. So the Frobenius element cannot lie in this conjugacy class and so we get $\mathcal{C}_2$.

# 20 $L$-series

In this section, we are going to prove one of the most important theorems in analytic number theory: Dirichlet's theorem of primes in arithmetic progression. We are going to introduce a special series called $L$-series and prove the theorem by using it. Further, we will extend this definition to a very useful application in algebraic number theory.

## 20.1 Dirichlet's Theorem of Primes in Arithmetic Progression

We begin with the following definition:

**Definition 20.1.** *An ordinary Dirichlet series is a series* $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$.

**Lemma 20.2.** **[Abel]** *For any complex number* $a_n, b_n$ *and natural number* $N < M$, *we have*

$$\sum_{n=N}^{M} a_n b_n = \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) (b_n - b_{n+1}) + \left( \sum_{k=N}^{M} a_k \right) b_M.$$

*Proof.*

$$\begin{aligned}
\sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) (b_n - b_{n+1}) &= \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) b_n - \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) b_{n+1} \\
&= a_N b_N + \sum_{n=N+1}^{M-1} \left( \sum_{k=N}^{n} a_k \right) b_n - \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) b_{n+1} \\
&= a_N b_N + \sum_{n=N}^{M-2} \left( \sum_{k=N}^{n+1} a_k \right) b_{n+1} - \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) b_{n+1} \\
&= a_N b_N + \sum_{n=N}^{M-2} a_{n+1} b_{n+1} - \left( \sum_{k=N}^{M-1} a_k \right) b_M \\
&= \sum_{n=N}^{M-1} a_n b_n - \left( \sum_{k=N}^{M-1} a_k \right) b_M.
\end{aligned}$$

□

**Proposition 20.3.** *Let* $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ *where* $\lambda \to \infty$ *is an increasing sequence of positive reals. Then*

*(i) If the partial sums* $\sum_{n=N}^{M} a_n$ *are bounded, then the series converges locally uniformly on* $\Re(s) > 0$ *to an analytic function.*

*(ii) If the series* $f(s)$ *converges for* $s = s_0$, *then it converges locally uniformly on* $\Re(s) > \Re(s_0)$ *to an analytic function.*

*Proof.* (i) We will show it converges on the domain $D$: $-A < \arg(s) < A, \Re(s) > \delta$, and then take $A \to \frac{\pi}{2}$ and $\delta \to 0$. Let $\epsilon > 0$. As $\lambda \to \infty$, there exists $N_0$ such that for all $n > N_0$, $\left| e^{-\lambda n s} \right| < \epsilon$ in $D$.

For $M, N \geq N_0$, and $b_n = e^{-\lambda_n s}$, we have

$$\left| \sum_{n=N}^{M} a_n b_n \right| = \left| \sum_{n=N}^{M-1} \left( \sum_{k=N}^{n} a_k \right) (b_n - b_{n+1}) - \left( \sum_{N}^{M} a_k \right) b_M \right| \leq B \sum_{n=N}^{M-1} \left| e^{-\lambda_n s} - e^{-\lambda_{n+1} s} \right| + B\epsilon$$

using triangle inequality and $\sum_{k=N}^{n} a_k$ bounded and $|b_M| < \epsilon$.

Now

$$\left|e^{-\alpha s} - e^{-\beta s}\right| = \left|s\int_{\alpha}^{\beta} e^{-xs}dx\right| \leq |s|\int_{\alpha}^{\beta} e^{-x\sigma}dx = \frac{|s|}{\sigma}\left(e^{-\alpha\sigma} - e^{-\beta\sigma}\right)$$

where $\sigma = \Re(s)$. So the previous expression is

$$\leq B\frac{|s|}{\sigma}\sum_{n=N}^{M-1}\left(e^{-\lambda_n\sigma}e^{-\lambda_{n+1}\sigma}\right) + B\epsilon = B\frac{|s|}{\sigma}\left(e^{-\lambda_N\sigma} - e^{-\lambda_M\sigma}\right) + B\epsilon < \epsilon\left(B\frac{|s|}{\sigma} + B\right).$$

But $\frac{\sigma}{|s|} = \tan\theta$ where $\theta$ is the angle between $s$ and the real axis. So $\frac{|s|}{\sigma} = \sec\theta \leq K$ for some $K$ because $\arg(s)$ is bounded. So we conclude that

$$\left|\sum_{n=N}^{M} a_n b_n\right| < \epsilon(K + B).$$

Therefore, the series is cauchy and so it converges.

(ii) By assumption, let $s' = s - s_0$ and $a_0' = e^{-\lambda_n s_0}a_n$. Then $\sum a_n' e^{-\lambda_n s'}$ converges at $s' = 0$ and so $\sum a_n'$ is bounded. Then apply (i).

□

**Proposition 20.4.** *Set $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ where $\lambda_n \to \infty$ is an increasing sequence of positive reals. Suppose that $a_n > 0$, $f(s)$ converges on $\Re(s) > R$ for some $R \in \mathbb{R}$ and it has an analytic continuation to a neighborhood of $s = R$. Then $f(s)$ converges on $\Re(s) > R - \epsilon$ for some $\epsilon > 0$.*

*Proof.* We may assume $R = 0$ (then for general case, we just shift the diagram). $f$ is analytic on $\Re(s) > 0$ because it converges and has an analytic continuation at $s = 0$ (use previous proposition). On $|s| < \delta$, there exists $\epsilon$ such that $f$ is analytic on $|s - 1| \leq 1 + \epsilon$.

The Taylor series of $f$ around $s = 1$ converges on all of $|s - 1| \leq 1 + \epsilon$, in particular,

$$f(-\epsilon) = \sum_{k=0}^{\infty}\frac{1}{k!}(-1)^k(1+\epsilon)^k f^{(k)}(1)$$

converges, where we use $f(-\epsilon) = f(1 - (1 + \epsilon))$.

For $\Re(s) > 0$, $f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-\lambda_n)^k e^{-\lambda_n s}$ and so $(-1)^k f^{(k)}(1) = \sum_{n=1}^{\infty} a_n\lambda_n^k e^{-\lambda_n}$. Thus,

$$\begin{aligned} f(-\epsilon) = \sum_{k=0}^{\infty}\frac{1}{k!}(1+\epsilon)^k\sum_{n=1}^{\infty} a_n\lambda_n^k e^{-\lambda_n} &= \sum_{k,n} a_n\lambda_n^k e^{-\lambda_n}\frac{(1+\epsilon)^k}{k!} \\ &= \sum_{n=1}^{\infty} a_n e^{-\lambda_n}e^{\lambda_n(1+\epsilon)} \\ &= \sum_{n=1}^{\infty} a_n e^{\lambda_n\epsilon}. \end{aligned}$$

This shows that the series $f(s)$ converges at $s = -\epsilon$ (note that the convergence of $f$ and the convergence of the Taylor series can be different) and the result follows by the second part of previous proposition. □

**Theorem 20.5.** *(i) If $a_n$ are bounded, then $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ converges absolutely on $\Re(s) > 1$ to an analytic function.*

*(ii) If partial sums* $\sum_{n=N}^{M} a_n$ *are bounded, then* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *converges on* $\Re(s) > 0$ *to an analytic function.*

*Proof.* (i) Convergence is clear. Then apply Proposition 20.3(ii).

(i) Use Proposition 20.3(i).

□

**Proposition 20.6.** *If* $\sum a_n e^{-\lambda_n s}$ *and* $\sum b_n e^{-\lambda_n s}$ *converge on* $\Re(s) > \sigma_0$ *to the same function* $f(s)$ *then* $a_n = b_n$ *for all* $n$.

*Proof.* It suffices to check that if $\sum c_n e^{-\lambda_n s}$ converges on $\Re(s) > \sigma_0$ to a zero function then $c_n = 0$ for all $n$. Suppose not, then assume $N$ is the least number such that $c_N \neq 0$. We will prove that

$$\left|\frac{c_N}{N^s}\right| > \sum_{n=N+1} \left|\frac{a_n}{n^s}\right|$$

for some $s \in \mathbb{R}$ large enough.

Let $f(s) = \sum c_n e^{-\lambda_n s}$ then

$$\frac{f(s)N^s}{c_N} = 1 + \sum_{n \geq n+1} \frac{a_n}{a_N} \left(\frac{N}{n}\right)^s.$$

Pick $s = N^{k+1}$ for some $k$ which we will specify later. Now $(N+1)^s > N^s + sN^{s-1}$ and so for $n \geq n+1$,

$$\left(\frac{N}{n}\right)^s < \frac{N^s}{N^s + sN^{s-1}} < \frac{N^s}{N^{k+s}} = \frac{1}{N^k}$$

because $sN^{s-1} = N^{k+s}$ by the choice of $s$. Then we pick $k$ large enough, so that the sum

$$\sum_{n \geq N+1} \frac{a_n}{a_N} \left(\frac{N}{n}\right)^s$$

is bounded by a small quantity $B$, and so $1 + B$ is positive. But on the other hand, $\frac{f(s)N^s}{c_N}$ is zero because $f(s)$ converges to 0, which is a contradiction. □

Now we shall introduce Dirichlet $L$-function.

**Definition 20.7.** *Let* $N \geq 1$ *be an integer and*

$$\psi : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}^*$$

*a group homomorphism. Extend* $\psi$ *to a function on* $\mathbb{Z}$ *by*

$$\psi(n) = \begin{cases} \psi(n \bmod N) & \text{if } (n, N) = 1, \\ 0 & \text{otherwise} \end{cases}$$

*Such a function is called a* **Dirichlet character modulo** $N$. *Its L-series (or L-function) is given by*

$$L_N(\psi, s) = \sum_{n=1}^{\infty} \psi(n) n^{-s}.$$

**Lemma 20.8.** *Let $\psi$ be a Dirichlet character modulo $N$. Then*

$$\psi(a+N) = \psi(a), \psi(ab) = \psi(a)\psi(b).$$

*The L-series of $\psi$ converges absolutely on $\Re(s) > 1$ and satisfies*

$$L_N(\psi, s) = \prod_{p\in\mathbb{P}} \frac{1}{1-\psi(p)p^{-s}}.$$

*Proof.* $a + N \equiv a \pmod N$ so $\psi(a+N) = \psi(a)$. $\psi(ab) = \psi(a)\psi(b)$ because it is a homomorphism. Now $|(\psi(n)| \leq 1$ for all $n$ and so by Theorem 20.5(i), it converges absolutely to an analytic function.

For $\Re(s) > 1$, we have

$$\sum_{n=1}^{\infty} \psi(n)n^{-s} = \prod_{p\in\mathbb{P}} (1 + \psi(p)p^{-s} + \psi(p^2)p^{-2s} + \cdots) = \prod_{p\in\mathbb{P}} \frac{1}{1-\psi(p)p^{-s}}$$

by using unique factorisation of integers into prime numbers and the fact the series converges absolutely. □

**Example 20.9.** *Take $N = 10$ then $(\mathbb{Z}/10\mathbb{Z})^* \cong C_4 = \{1, 3, 7, 9\}$. Also, take $\psi$ such that $\psi(1) = 1, \psi(3) = i, \psi(7) = -i, \psi(9) = -1$. Then*

$$L_{10}(\psi, s) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{9^s} + \frac{1}{11^s} + \frac{i}{13^s} - \frac{i}{17^s} - \frac{1}{19^s} + \cdots.$$

**Remark 20.10.** *The case $\psi : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}^*$ with $\psi(n) = 1$ for all $n \in (\mathbb{Z}/N\mathbb{Z})^*$ is called the* **trivial Dirichlet character modulo** *$N$. In this case,*

$$L_N(\psi, s) = \prod_{p\nmid N, p\in\mathbb{P}} \frac{1}{1-p^{-s}} = \zeta(s) \prod_{p\Big| N, p\in\mathbb{P}} (1-p^{-s}).$$

**Theorem 20.11.** *Let $N \geq 1$, and $\psi : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}^*$ be a Dirichlet character modulo $N$.*

*(i) If $\psi$ is the trivial character, then $L_N(\psi, s)$ has an analytic continuation to $\Re(s) > 0$, except for a simple pole at $s = 1$.*

*(ii) If $\psi$ is non-trivial, then $L_N(\psi, s)$ is analytic on $\Re(s) > 0$.*

*Proof.* When $\psi$ is trivial, the result is clear by the previous remark and the property of $\zeta(s)$. When $\psi$ is non-trivial, consider

$$\sum_{n=M}^{M+N-1} \psi(n) = \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^*} \psi(n) = \langle \psi, 1\rangle = 0$$

by orthogonality of the 1-dimensional representations. So the partial sums are bounded and so the result follows from Theorem 20.5(i). □

**Theorem 20.12.** *Let $\psi$ be a non-trivial Dirichlet character modulo $N$. Then $L_N(\psi, 1) \neq 0$.*

*Proof.* Let

$$\zeta_N(s) = \prod_{\chi:(\mathbb{Z}/N\mathbb{Z})^*\mapsto\mathbb{C}^*} L_N(\chi, s).$$

Suppose $L_N(\psi,1)=0$, then $\zeta_N(s)$ has an analytic continuation to $\Re(s)>0$ because the pole for $\psi=\mathbb{1}$ is canceled by this zero (use previous theorem). On $\Re(s)>1$, $\zeta_N(s)$ has an absolutely convergent Euler product

$$\zeta_N(s)=\prod_{\chi}\prod_{p\in\mathbb{P}}\frac{1}{1-\chi(p)p^{-s}}=\prod_{p\nmid N,p\in\mathbb{P}}\prod_{\chi}\frac{1}{1-\chi(p)p^{-s}}.$$

Now consider for each $p$, the product $\prod_\chi(1-\chi(p)T)$ as a polynomial in $T$. It has degre $|(\mathbb{Z}/N\mathbb{Z})^*|$. Let $f_p$ be the order of $p$ mod $N$ and $\phi$ be the Euler totient function. Then

$$(\chi(p))^{f_p}=\chi(p^{f_p})=\chi(1)=1.$$

So $\chi(p)$ is a $f_p$ $^{\text{th}}$ root of unity. The subgroup generated by $p$ has index $\frac{\phi(N)}{f_p}$. Fix a primitive $f_p$ $^{\text{th}}$ root of unity, $\zeta$. Then $\chi(p)=\zeta^i$ for some $i$. If we run through every $\chi$, then each $\zeta^i$ occurs $\frac{\phi(N)}{f_p}$ times (refer to the structure of $\chi$ in Chapter 18) and so we have

$$\prod_{\chi}(1-\chi(p)T)=\prod_{i=0}^{f_p-1}\left(1-\zeta^iT\right)^{\frac{\phi(N)}{f_p}}=\left(1-T^{f_p}\right)^{\frac{\phi(N)}{f_p}}.$$

Thus, with $T=p^{-s}$.

$$\zeta_N(s)=\prod_{p\nmid N,p\in\mathbb{P}}\left(1+p^{-f_ps}+p^{-2f_ps}+\cdots\right)^{\frac{\phi(N)}{f_p}}.$$

But we assume that $\zeta_N(s)$ is analytic on $\Re(s)>0$ and it has positive coefficients, so it must converge on $\Re(s)>0$ by Proposition 20.4.

Now for $s>0$, the above expression dominates

$$\prod_{p\nmid N,p\in\mathbb{P}}\left(1+p^{-\phi(N)s}+p^{-2\phi(N)s}+\cdots\right)=L_N(1,\phi(N),s)$$

which diverges at $s=\frac{1}{\phi(N)}$, and this gives a contradiction. □

**Proposition 20.13.** *Let $\psi$ be a Dirichlet character modulo $N$.*

*(i) The Dirichlet series*

$$\sum_{p\in\mathbb{P},n\geq1}\frac{\psi(p)^n}{n}p^{-ns}$$

*converges absolutely on $\Re(s)>1$ to an analytic function and defines a branch of $\log L_N(\psi,s)$ there.*

*(ii) If $\psi$ is non-trivial, then $\sum_{p,n}\frac{\psi(p)^n}{n}p^{-ns}$ is bounded as $s\to1$. If $\psi$ is trivial then $\sum_{p,n}\frac{\psi(p)^n}{n}p^{-ns}\sim\log\frac{1}{s-1}$ as $s\to1$.*

*Proof.* (i) The series has the form $a_{p^n}=\frac{\psi(p)^n}{n}$ and $a_k=0$ if $k$ is not a prime power. So it has bounded coefficients and so it converges absolutely by Theorem 20.5(i).

Fix $s$ with $\Re(s)>1$, then

$$\begin{aligned}\sum_{p,n}\frac{\psi(p)^n}{n}p^{-ns}&=\sum_n\psi(p)p^{-s}+\frac{(\psi(p)p^{2s})^2}{2}+\cdots\\&=\sum_p\log\frac{1}{1-\psi(p)p^{-s}}\\&=\log\prod_p\frac{1}{1-\psi(p)p^{-s}}=\log L_N(\psi,s).\end{aligned}$$

Hence, $\prod_{p,n} \frac{\psi(p)^n}{n} p^{-ns}$ is an analytic branch of $\log L_N(\psi, s)$ on $\Re(s) > 1$.

(ii) If $\psi$ is non-trivial then by Theorem 20.11(i), $L_N(\psi, s)$ is analytic on $\Re(s) > 0$ and it is non-zero by Theorem 20.12, so by the previous part, it is bounded.

If $\psi$ is trivial, then it has a simple pole at $s = 1$ and so we can write

$$L_N(1, s) = \frac{\lambda}{s-1} + o\left(\frac{1}{s-1}\right).$$

Taking logarithm gives the result.

□

**Corollary 20.14.** *If $\psi$ is non-trivial, then $\sum_{p\in\mathbb{P}} \psi(p)p^{-s}$ is bounded as $s \to 1$. If $\psi$ is trivial, then $\sum_{p\in\mathbb{P}} \psi(p)p^{-s} \sim \log \frac{1}{s-1}$ as $s \to 1$. In particular, it tends to infinity as $s \to 1$.*

*Proof.* By Theorem 20.13,

$$\sum_{p\in\mathbb{P}} \psi(p)p^{-s} = \log L_N(\psi, s) - \sum_{p\in\mathbb{P}, n\geq 2} \frac{\psi(p)^n}{n} p^{-ns}.$$

Also, $\log L_N(\psi, s)$ is bounded as $s \to 1$ when $\psi$ is non-trivial. So it suffices to check the second term on RHS is bounded.

$$\begin{aligned}\left|\sum_{p\in\mathbb{P}, n\geq 2} \frac{\psi(n)^n}{n} p^{-ns}\right| &\leq \sum_{p\in\mathbb{P}, n\geq 2} \frac{1}{|p^s|^n} \\ &= \sum_{p\in\mathbb{P}} \frac{1}{|p^s|(|p^s|-1)} \\ &\leq \sum_{p\in\mathbb{P}} \frac{1}{p(p-1)} \leq \sum_{k=1}^{\infty} \frac{1}{k^2} < \infty\end{aligned}$$

using $\Re(s) > 1$.

Similarly, when $\psi$ is trivial, $\sum_{p,n} \frac{\psi(p)^n}{n} p^{-ns} \sim \log \frac{1}{s-1}$ as $s \to 1$ and since we have proved above that the second term on RHS is bounded, so the result follows. □

Now we can prove the main theorem:

**Theorem 20.15.** **[Dirichlet's theorem of primes in arithmetic progression]** *Let $a, N$ be coprime integers, then there exists infinitely many primes $p$ such that*

$$p \equiv a \ (mod\ N).$$

*Moreover, if $P_{a,N}$ is the set of these primes, then*

$$\sum_{p\in P_{a,N}} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1}$$

*as $s \to 1$ where $\phi$ is the Euler totient function.*

*Proof.* The first statement follows from the second one because $\log \frac{1}{s-1} \to \infty$ as $s \to 1$. Consider the class function

$$C_{a,N} : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}$$

by

$$C_{a,N}(n) = \begin{cases} 1 & \text{if } n = a, \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\langle C_{a,N}, \chi \rangle = \frac{1}{\phi(N)} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^*} C_{a,N}(n)\overline{\chi(n)} = \frac{1}{\phi(n)}\overline{\chi(a)}.$$

Since the irreducible characters form a basis so we conclude that

$$C_{a,N} = \sum_{\chi:(\mathbb{Z}/N\mathbb{Z})^* \mapsto \mathbb{C}^*} \frac{\overline{\chi(a)}}{\phi(N)}\chi.$$

Hence,

$$\sum_{p \in P_{a,N}} \frac{1}{p^s} = \sum_{p \in \mathbb{P}} C_{a,N}(p)p^{-s} = \sum_{\chi} \frac{\overline{\chi(a)}}{\phi(N)} \sum_{p \in \mathbb{P}} \frac{\chi(p)}{p^s}.$$

If $\chi$ is non-trivial, then the contribution to the above expression is bounded, by the previous corollary. So the only asymptotic contribution is from the case when $\chi$ is trivial, and so we have

$$\sum_{p \in P_{a,N}} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1}$$

as $s \to 1$. □

**Remark 20.16.** *Here is an alternative view. Note that*

$$(\mathbb{Z}/N\mathbb{Z})^* \cong Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$$

*via*

$$a \mapsto \sigma_a \text{ with } \sigma_a(\zeta_N) = \zeta_N^a.$$

*If $\mathfrak{q}$ lies above $p \nmid N$, then $\sigma_p$ is the same as $Frob_{\mathfrak{q}/p}$. So we have a correspondence*

$$\frac{1}{1-\psi(p)p^{-s}} \longleftrightarrow \frac{1}{1-\psi(Frob_{\mathfrak{q}/p})p^{-s}}.$$

**Theorem 20.17.** [**Hacke**] *Let $F/K$ be a Galois extension of number fields with $Gal(F/K)$ abelian, and*

$$\psi : Gal(F/K) \longmapsto \mathbb{C}^*$$

*a homomorphism. Then*

$$L_*(\psi, s) = \prod_{\substack{\mathfrak{p} \text{ prime of } K \\ \mathfrak{p} \text{ unramiifed}}} \frac{1}{1-\psi(Frob_{\mathfrak{p}})N(\mathfrak{p})^{-s}}$$

*has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$ when $\psi$ is trivial.*

**Remark 20.18.** *When $K = \mathbb{Q}, F = \mathbb{Q}(\zeta_N)$, this recovers Theorem 20.11.*

## 20.2 Artin $L$-function

In this section we are going to introduce Artin $L$-function. It is useful in more general number fields (not only for $\mathbb{Q}$).

**Definition 20.19.** *Let $F/K$ be a Galois extension of number fields and $\rho$ a $Gal(F/K)$ representation. Let $\mathfrak{p}$ be a prime of $K$. Choose a prime $\mathfrak{q}$ above $\mathfrak{p}$ in $F$ and an element $Frob_{\mathfrak{p}} \in D_{\mathfrak{q}/\mathfrak{p}}$ which maps to $Frob_{\mathfrak{q}/\mathfrak{p}}$ in $D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$. Then the* **local polynomial** *of $\rho$ at $\mathfrak{p}$ is*

$$P_{\mathfrak{p}}(F/K, \rho, T) = P_{\mathfrak{p}}(\rho, T) = \det\left(1 - Frob_{\mathfrak{p}} T \middle| \rho^{I_{\mathfrak{p}}}\right)$$

*where $I_{\mathfrak{p}}$ means $I_{\mathfrak{q}/\mathfrak{p}}$.*

*Recall for $I \subset D$ finite groups and $\rho$ a $D$-representation, (the notation is a bit confusing)*

$$\rho^I = \{v \in \rho : g(v) = v \ \forall g \in I\} = \{v \in V : \rho(i)v = v \ \forall i \in I\}.$$

*If $I \subset D$, then $\rho^I$ is a subrepresentation (easy to check).*

*Further, if $\lambda_i \in \mathbb{C}, g_i \in D$, write*

$$\det\left(\sum \lambda_i g_i \middle| \rho\right)$$

*for $\det_\rho(\sum \lambda_i g_i)$. Equivalently, we view $\rho$ as $\rho : D \longmapsto GL_n(\mathbb{C})$, then*

$$\det\left(\sum \lambda_i g_i \middle| \rho\right) = \det\left(\sum \lambda_i \rho(g_i)\right).$$

**Remark 20.20.** *The expression of the local polynomial is*

$$P_{\mathfrak{p}}(\rho, T) = \det\left(1 - \rho^{I_{\mathfrak{p}}}(Frob_{\mathfrak{p}})T\right).$$

*Recall from the previous chapter that*

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(\rho, T) = \det(T - \rho^{I_{\mathfrak{p}}}(Frob_{\mathfrak{q}/\mathfrak{p}})).$$

*So in fact $P_{\mathfrak{p}}(\rho, T)$ is just replacing $T^i$ by $T^{n-i}$ in $\Phi$.*

*If the representation is 1-dimensional, then*

$$P_{\mathfrak{p}}(\rho, T) = \begin{cases} 1 - \rho(Frob_{\mathfrak{p}})T & \text{if } \rho^I = \rho, \\ 1 & \text{if } \rho^I = 0. \end{cases}$$

**Lemma 20.21.** *$P_{\mathfrak{p}}(\rho, T)$ is independent of the choice of $\mathfrak{q}$ and $Frob_{\mathfrak{p}}$.*

*Proof.* For fixed $\mathfrak{q}$, another choice of $\mathrm{Frob}_{\mathfrak{p}}$ is differed by some $i \in I$, i.e.

$$\mathrm{Frob}_{\mathfrak{p}} = i\mathrm{Frob}'_{\mathfrak{p}}.$$

Then $\rho^I(\mathrm{Frob}_{\mathfrak{p}}) = \rho^I(i)\rho^I(\mathrm{Frob}'_{\mathfrak{p}}) = \rho^I(\mathrm{Frob}'_{\mathfrak{p}})$ because $\rho^I(i) = 1$.

Let $\mathfrak{q}'$ be another prime above $\mathfrak{p}$. Then $\mathfrak{q}' = g(\mathfrak{q})$ for some $g \in \mathrm{Gal}(F/K)$ and

$$\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = g\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}g^{-1}, I_{\mathfrak{q}'} = gI_{\mathfrak{q}}g^{-1}.$$

So,

$$v \in \rho^{I_{\mathfrak{q}'}} \iff hv = v \ \forall h \in I_{\mathfrak{q}'} \iff gig^{-1}v = v \ \forall i \in I_{\mathfrak{q}} \iff g^{-1}v \in \rho^{I_{\mathfrak{q}}}.$$

This shows that $\rho^{I'_{\mathfrak{q}}} = g\left(\rho^{I_{\mathfrak{q}}}\right)$.

Consider the matrix of $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$ acting on $\rho^{I_{\mathfrak{q}'}}$. Let $v' \in \rho^{I_{\mathfrak{q}'}}$ and so $v' = gv$ for some $v \in \rho^{I_{\mathfrak{q}}}$. Then

$$\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}v' = g\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}g^{-1}gv = g\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}v.$$

Let $\lambda$ be an eigenvalue of $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$, and if $\mathrm{Frob}_{\mathfrak{q}'\mathfrak{p}}v' = \lambda' v'$, then

$$g\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}v = \lambda g v.$$

$g$ is invertible, so $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}v = \lambda v$. This shows that $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$ and $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ have the same eigenvalues, so they must have the same characteristic polynomial and so by the previous remark, they have the same local polynomial. □

**Definition 20.22.** *Let $F/K$ be a Galois extension of number fields and $\rho$ a representation of $Gal(F/K)$. The* **Artin $L$-function** *of $\rho$ is defined by*

$$L(F/K,\rho,s) = L(\rho,s) = \prod_{\mathfrak{p} \text{ prime of } K} \frac{1}{P_{\mathfrak{p}}(\rho, N(\mathfrak{p})^{-s})}.$$

The polynomial $P_{\mathfrak{p}}(\rho,T)$ has the form $1-(aT+bT^2+\cdots)$ so we can write (ignoring convergence for the moment)

$$\frac{1}{P_{\mathfrak{p}}(\rho,T)} = 1+(aT+bT^2+\cdots)+(aT+bT^2+\cdots)^2+\cdots = 1+a_{\mathfrak{p}}T+a_{\mathfrak{p}^2}T^2+\cdots$$

for some coefficients $a_i$. Then

$$L(\rho,s) = \prod_{\mathfrak{p}}(1+a_{\mathfrak{p}}N(\mathfrak{p})^{-s}+a_{\mathfrak{p}^2}N(\mathfrak{p})^{-2s}+\cdots) = \sum_{\mathfrak{n} \text{ non-zero ideals}} a_{\mathfrak{n}}N(\mathfrak{n})^{-s}$$

by unique factorisation of non-zero ideals. Note that grouping ideals with equal norm yields an expression for $L(\rho,s)$ as a Dirichlet series.

**Lemma 20.23.** *The $L$-series expansion agrees with Euler product on $\Re(s)>1$ where they converge absolutely to an analytic function.*

*Proof.* It suffices to prove that

$$\prod_{\mathfrak{p}}(1+a_{\mathfrak{p}}N(\mathfrak{p})^{-s}+a_{\mathfrak{p}^2}N(\mathfrak{p})^{-2s}+\cdots)$$

converges absolutely on $\Re(s)>1$. Then we can rearrange the terms and so the expansion agrees with the definition and analyticity also follows by Proposition 4.3(ii).

Factorise $P_{\mathfrak{p}}(\rho,T)$ over $\mathbb{C}$, we have

$$P_{\mathfrak{p}}(\rho,T) = (1-\lambda_1 T)(1-\lambda_2 T)\cdots(1-\lambda_k T)$$

where $k$ is the dimension of $\rho^I$, so $k \le \dim\rho$. Also, $|\lambda_i|=1$ because the eigenvalue of the a representation of finite group must be unimodular. So the coefficient of

$$\frac{1}{P_{\mathfrak{p}}(\rho,T)} = \frac{1}{\prod_i(1-\lambda_i T)} = 1+a_{\mathfrak{p}}T+a_{\mathfrak{p}^2}T^2+\cdots$$

are bounded in absolute value by those of

$$\left(\frac{1}{1-T}\right)^{\dim\rho} = (1+T+T^2+\cdots)^{\dim\rho}.$$

Therefore,

$$\begin{aligned}
\prod_{\mathfrak{p}}\left(\sum_{n=1}^{\infty}|a_{\mathfrak{p}^n}||N(\mathfrak{p})^{-ns}|\right) &\le \prod_{\mathfrak{p}}\frac{1}{(1-|N(\mathfrak{p})^{-s}|)^{\dim\rho}} \\
&\le \prod_{\mathfrak{p}}\left(\frac{1}{1-|p|^{-s}}\right)^{\dim\rho} \\
&\le \left(\prod_{p\in\mathbb{P}}\frac{1}{1-|p^{-s}|}\right)^{\dim\rho[K:\mathbb{Q}]} \\
&= \zeta(\sigma)^{\dim\rho[K:\mathbb{Q}]} < \infty
\end{aligned}$$

where in the second inequality we use $N(\mathfrak{p}) \ge p$ and in the last line we use $\sigma = \Re(s) > 1$. □

**Example 20.24.** *(i) $K = \mathbb{Q}$,$F$ any Galois extension of $K$. If $\rho$ is trivial, then*

$$L(\mathbb{1}, s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s).$$

*(ii) More generally, let $F/K$ be arbitrary Galois extension of number fields and let $\rho$ be the trivial representation. Then*

$$L(F/K, \mathbb{1}, s) = \prod_{\mathfrak{p} \in K} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \zeta_K(s)$$

*the Dedekind $\zeta$-function.*

*(iii) Let $K = \mathbb{Q}, F = \mathbb{Q}(\zeta_N)$ and $\rho$ be a 1-dimensional representation of $Gal(F/K)$. Let*

$$\psi : (\mathbb{Z}/N\mathbb{Z})^* \longmapsto \mathbb{C}^* \text{ via } \psi(n) = \rho(\sigma_n)$$

*where $\sigma_n(\zeta_N) = \zeta_N^n$. By Remark 20.20, we know*

$$P_{\mathfrak{p}}(\rho, T) = \begin{cases} 1 - \rho(Frob_{\mathfrak{p}})T & \text{if } \rho^I = \rho, \\ 1 & \text{if } \rho^I = \rho. \end{cases}$$

*Then since $\rho(Frob_{\mathfrak{p}}) = \rho(\sigma_p) = \psi(p)$.*

$$\begin{aligned} L(F/K, \rho, s) &= \prod_{\substack{\mathfrak{p} \text{ such that} \\ \rho^{I_{\mathfrak{p}}} = \rho}} \frac{1}{1 - \rho(Frob_{\mathfrak{p}})p^{-s}} \\ &= \prod_{\substack{\mathfrak{p} \nmid N \\ \rho^{I_{\mathfrak{p}}} = \rho}} \frac{1}{1 - \psi(p)p^{-s}} \prod_{\substack{\mathfrak{p} \mid N \\ \rho^{I_{\mathfrak{p}}} = \rho}} \frac{1}{1 - \rho(Frob_{\mathfrak{p}})p^{-s}} \\ &= L_N(\psi, s) \prod_{\substack{\mathfrak{p} \mid N \\ \rho^{I_{\mathfrak{p}}} = \rho}} \frac{1}{1 - \rho(Frob_{\mathfrak{p}})p^{-s}}. \end{aligned}$$

**Lemma 20.25.** *Let $G = Gal(F/K)$, $N$ a normal subgroup of $G$, and $\mathfrak{q}/\mathfrak{s}/\mathfrak{p}$ be a tower of prime in $F/F^N/K$. Then*

*(i) $D_{\mathfrak{s}/\mathfrak{p}} = D_{\mathfrak{q}/\mathfrak{p}}N/N$.*

*(ii) $I_{\mathfrak{s}/\mathfrak{p}} = I_{\mathfrak{q}/\mathfrak{p}}N/N$.*

*(iii) If $Frob_{\mathfrak{p}} \subset D_{\mathfrak{q}/\mathfrak{p}}$ acts as the Frobenius automorphism on $\mathcal{O}_F/\mathfrak{q}$, then $Frob_{\mathfrak{p}}N \in D_{\mathfrak{s}/\mathfrak{p}}$ acts as Frobenius on $\mathcal{O}_F^N/\mathfrak{s}$.*

*Proof.* (i) $\mathfrak{s}$ is preserved by both $N$ and $D_{\mathfrak{q}/\mathfrak{p}}$ so $D_{\mathfrak{s}/\mathfrak{p}} \supset D_{\mathfrak{q}/\mathfrak{p}}N/N$. Now

$$|D_{\mathfrak{s}/\mathfrak{p}}| = e_{\mathfrak{s}/\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}} = \frac{|D_{\mathfrak{q}/\mathfrak{p}}|}{|D_{\mathfrak{q}/\mathfrak{s}}|} = \frac{|D_{\mathfrak{q}/\mathfrak{p}}|}{|D_{\mathfrak{q}/\mathfrak{p}} \cap N|} = \left|D_{\mathfrak{q}/\mathfrak{p}}N/N\right|.$$

So $D_{\mathfrak{s}/\mathfrak{p}} = D_{\mathfrak{q}/\mathfrak{p}}N/N$.

(ii) Replace the decomposition groups by inertia groups in (i).

(iii) $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{q}/\mathfrak{p}}$. Since $\mathcal{O}_F^N/\mathfrak{s}$ is a subfield of $\mathcal{O}_F/\mathfrak{q}$, so the image of $\mathrm{Frob}_{\mathfrak{p}}$ in the quotient acts as Frobenius in the field $\mathcal{O}_F^N/\mathfrak{s}$.

□

**Proposition 20.26.** *Let $F/K$ be a Galois extension of number fields, $\rho$ a $Gal(F/K)$ representation.*

*(i) If $\rho'$ is another $Gal(F/K)$ representation, then*

$$L(\rho \oplus \rho') = L(\rho, s)L(\rho', s).$$

*(ii) If $N \subset Gal(F/K)$ is a normal subgroup, which lies in $\ker \rho$, so that $\rho$ comes from a representation $\rho''$ of $Gal(F/K)/N = Gal(F^N/K)$, then*

$$L(F/K, \rho, s) = L(F^N/K, \rho'', s).$$

*(iii)* **Artin formalisation** *If $\rho = Ind_H^{Gal(F/K)} \rho'''$ for a representation $\rho'''$ of $H \subset Gal(F/K)$, then*

$$L(F/K, \rho, s) = L(F/F^H, \rho''', s).$$

*Proof.* It suffices to check the result for each prime.

(i)
$$L(\rho \oplus \rho', s) = \prod_{\mathfrak{p}} \left[\det\left(1 - (\rho \oplus \rho')^{I_{\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}})N(p)^{-s}\right)\right]^{-1}.$$

Now $(\rho \oplus \rho')^{I_{\mathfrak{p}}} = \rho^{I_{\mathfrak{p}}} \oplus \rho'^{I_{\mathfrak{p}}}$. In terms of matrix form, $(\rho \oplus \rho')^{I_{\mathfrak{p}}}$ can be viewed as a block diagonal matrix. So the discriminant can be factorised as a product.

(ii) $\rho$ comes from $\rho''$, i.e. $\rho(g) = \rho''(gN)$. For each $\mathfrak{p}$ in $K$, $I_{\mathfrak{s}/\mathfrak{p}} = I_{\mathfrak{q}/\mathfrak{p}}N/N$, Frob Therefore,

$$\rho''^{I_{\mathfrak{s}/\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}}N)N(\mathfrak{p})^{-s} = \rho^{I_{\mathfrak{q}/\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s}.$$

So they agree for each prime.

(iii) Recall from Proposition 19.42 that

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(\mathrm{Res}_D^G \mathrm{Ind}_H^G V, t) = \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(\mathrm{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right)$$

and so the same holds for the local polynomials. The result follows by the observation that the product which run through every prime $\mathfrak{s}$ of $F^H$ is the same as the double product with the first one running through $\mathfrak{p}$ for all prime in $K$ and the second one running through $\mathfrak{s}$ prime above $\mathfrak{p}$.

□

**Theorem 20.27.** *Let $F/K$ be a Galois extension of number fields and $\rho$ a 1-dimensional representation. Then*

*(i) $L(F/K, \rho, s)$ has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$ if $\rho$ is trivial.*

*(ii) If $\rho$ is non-trivial then $L(\rho, \mathbb{1}) \neq 0$.*

*Proof.* By Proposition 20.26(ii) we can reduce this to the case when $F = F^{\ker \rho}$, because

$$L(F/K, \rho, s) = L(F^{\ker \rho}/K, \rho'', s).$$

Thus we may assume that $\rho$ is faithful, and $G = \mathrm{Gal}(L/K)$ must be abelian because $\rho$ is 1-dimensional.

(i) It follows from Theorem 20.17.

(ii) We claim that

$$\zeta_F(s) = L(F/K, \mathrm{Ind}_{\{1\}}^G \mathbb{1}, s) = \prod_{\chi \in \hat{G}} L(F/K, \chi, s) = \zeta_K(s) \prod_{\chi \in \hat{G} \setminus \{1\}} L(F/K, \chi, s)$$

where $\hat{G}$ is the set of irreducible representations of $G$.

Let $H = \{1\}$ and $\rho''' = \mathbb{1}$, and $\zeta_F(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_F} \frac{1}{1 - N_F(\mathfrak{p})^{-s}}$, so Proposition 20.26(iii) implies that

$$L(F/K, \rho, s) = L(F/F, \rho''', s) \text{ where } \rho = \mathrm{Ind}_H^{\mathrm{Gal}(F/K)} \mathbb{1}.$$

Also, $\mathrm{Ind}_{\{1\}}^G \mathbb{1} = \oplus_{\chi \in \hat{G}} \chi$. Then use Proposition 20.26(i) and so we have proved the claim.

As both $\zeta$-functions have a simple pole and each $L(F/K, \chi, s)$ is analytic at $s = 1$ by (i), it follows that no $L(F/K, \chi, s)$ can have a zero there for $\chi$ non-trivial.

□

## 20.3 Applications

We are now going to apply the properties of $L$-function to give some results in number theory, among which we shall prove one of the most important applications, the **Chebotarev's Density Theorem**.

The first application is the following problem.

**Theorem 20.28.** *Let $K$ be a number field. Suppose $\alpha \in \mathcal{O}_K$ and $\alpha$ mod $\mathfrak{p}$ is a square in $\mathfrak{O}_K/\mathfrak{p}$ for all prime $\mathfrak{p}$ in $K$. Then $\alpha$ is a square in $\mathcal{O}_K$. In particular, this shows that if $x$ is a quadratic residue for all prime $p$, then $x$ is a square (you may refer to problem 8 of exercise 4).*

*Proof.* Suppose not, then $X^2 - \alpha$ is irreducible and Kummer-Dedekind applies to $\mathfrak{p}$ where $\mathfrak{p} \nmid 2\alpha N$, $N = [\mathcal{O}_F : \mathcal{O}_K[\alpha]]$. Also, $\alpha$ mod $\mathfrak{p}$ is a square so for all $\mathfrak{p} \nmid 2\alpha N$, $\mathfrak{p}$ splits. Thus,

$$\begin{aligned} \zeta_F(s) &= \prod_{\mathfrak{q} \in F} \frac{1}{1 - N(\mathfrak{q})^{-s}} = \prod_{\mathfrak{p} \nmid 2N\alpha} \left( \frac{1}{1 - N(\mathfrak{p}^{-s})} \right)^2 \prod_{\substack{\mathfrak{q} \text{ above } \mathfrak{p} \\ \mathfrak{p} \mid 2N\alpha}} \frac{1}{1 - N(\mathfrak{q})^{-s}} \\ &= \zeta_K(s)^2 \prod_{\substack{\mathfrak{q} \text{ above } \mathfrak{p} \\ \mathfrak{p} \mid 2N\alpha}} \frac{1}{1 - N(\mathfrak{q})^{-s}} \prod_{\mathfrak{p} \mid 2N\alpha} \left( \frac{1}{1 - N(\mathfrak{p}^{-s})} \right)^{-2}. \end{aligned}$$

But the last expression has a double pole at $s = 1$ but $\zeta_F(s)$ only has a simple pole. This gives a contradiction. □

By a similar argument, one can deduce

**Theorem 20.29.** *If $F/K$ is a cyclic extension of number fields with $[F:K]=p$ where $p$ is a prime, then infinitely many primes of $K$ remains prime in $F$.*

The deduction is similar by considering the Dedekind $\zeta$-functions of $F$ and $K$, and you may use the fact that only finitely many primes ramify.

**Corollary 20.30.** *Let $f(X)\in\mathbb{Z}[X]$ be a irreducible polynomial of degree $d$ where $d$ is a prime. Then $f(X)$ mod $p$ is irreducible for infinitely many prime $p$.*

*Proof.* Let $F=\mathbb{Q}(\alpha)$ where $f(\alpha)=0$. If $F/\mathbb{Q}$ is Galois, then apply the previous theorem (it must be cyclic as the degree is prime). If not, let $L$ be the Galois closure. Now $[L:\mathbb{Q}]\big|d!$ and since $[F:\mathbb{Q}]=d$, so we conclude that $[L:F]$ is prime to $p$.

For a prime $p$ in $\mathbb{Q}$, consider the index $r_pe_pf_p=[L:\mathbb{Q}]$ in $L$. Since $d\big|[L:\mathbb{Q}]$, we have $d\big|e_p$ or $d\big|f_p$ or $d\big|r_p$. If $d\big|e_p$, then by tower law of ramification degree, and the fact $[L:F]$ prime to $d$, we must have $p$ ramifies in $F/\mathbb{Q}$. Since there are only finitely many primes which ramify in $F$, so we may eliminate the case when $d\big|e_p$.

Also, we may eliminate the primes for which Kummer-Dedekind does not apply. Now for the same reason as above, $d\big|f_p$ if and only if $f(X)$ is irreducible mod $p$, and so $d\big|r_p$ means that $f(X)$ splits mod $p$. If there are only finitely many primes $p$ with $d\big|f_p$, then use the same argument as Theorem 20.28, we will get a contradiction (a simple pole against mutli-poles). So there must be infinitely many of them. □

## 20.4 Induction Theorems

**Theorem 20.31.** **[Artin's Induction Theorem]** *Let $G$ be a finite group and $\rho$ a $G$-representation. Then for some $n\geq 1$, there are cyclic subgroups $H_i,H_j'\subset G$ and 1-dimensional representations $\psi_i,\psi_j'$ of $H_i,H_j$ respectively, such that*

$$\rho^{\oplus n}\oplus\bigoplus_i Ind_{H_i}^G\psi_i\cong\bigoplus_j Ind_{H_j'}^G\psi_j.$$

*If $\langle\rho,\mathbb{1}\rangle=0$, then all $\psi_i,\psi_j'$ can be chosen to be non-trivial.*

*Proof.* Let $\chi_T$ be the character of $T$. We begin with the first statement. Let $V$ be the $\mathbb{Q}$ vector space of $\mathbb{Q}$ linear combinations of characters of $G$. Let $W$ be the subspace spanned by $\chi_{\mathrm{Ind}_H^GT}$ for all cyclic subgroups $H\subset G$ and 1-dimensional $H$-representations $T$. It will suffice to prove that $V=W$. Then

$$\chi_\rho=\sum_i\lambda_i\chi_{\mathrm{Ind}_H^GT_i},\lambda_i\in\mathbb{Q}.$$

Clear the denominators, so we have

$$n\chi_\rho=\sum_i k_i\chi_{\mathrm{Ind}_H^GT_i},n,k_i\in\mathbb{Z}$$

which gives the result.

Suppose $\psi\in W^\perp$ so $\langle\psi,\chi_{\mathrm{Ind}_H^GT}\rangle=0$ for all such $H,T$. Then by Frobenius reciprocity,

$$\langle\mathrm{Res}_H^G\psi,\chi_T\rangle_H=0\text{ for all }1-\text{dimensional representation T of }H.$$

But $H$ is cyclic, so any irreducible representation of $H$ is 1-dimensional and so $\mathrm{Res}_H^G\psi=0$. In particular, taking $H=\langle g\rangle$, we have $\psi(g)=0$. This shows that $\psi=0$ as $g$ is arbitrary so $W^\perp=0$ and so $V=W$.

Now take $W$ to be spanned by $\chi_{\mathrm{Ind}_H^GT}$ with $H$ cyclic and $T$ any non-trivial 1-dimensional representation. To prove the second part, it suffices to show that $\psi\in W^\perp$ is a multiple of the trivial character.

By Frobenius reciprocity, we have

$$\langle \mathrm{Res}^G_H \psi, \chi_T \rangle = 0$$

which implies that $\mathrm{Res}^G_H \psi$ is a multiple of $\mathbf{1}_H$. Take $H = \langle g \rangle$, then $\psi(g) = \psi(1) = \lambda$ because $1 \in H$. Then we can run through every $g \in G$ and so $\psi(g) = \lambda$ for all $g \in G$. □

**Corollary 20.32.** *Let $F/K$ be Galois and $\rho$ a $Gal(F/K)$ representation.*

*(i) For some $n \geq 1$, $L(\rho^{\oplus n}, s)$ has a meromorphic continuation to $\mathbb{C}$. If $\langle \rho, \mathbf{1} \rangle = 0$, then it is analytic and non-zero at $s = 1$.*

*(ii) If $\rho \neq \mathbf{1}$ is irreducible, then $L(\rho, s)$ has an analytic continuation to $s = 1$ where the function does not vanish.*

*Proof.* (i) By the previous theorem, we may take

$$\rho^{\oplus n} \oplus \bigoplus_i \mathrm{Ind}^G_{H_i} \psi_i \cong \bigoplus_j \mathrm{Ind}^G_{H'_j} \psi'_j$$

for some cyclic subgroups $H_i, H'_j$ and 1-dimensional representations $\psi_i, \psi'_j$. Now use Proposition 20.26(i) and (iii), we conclude

$$\begin{aligned} L(\rho^{\oplus n}, s) &= \frac{\prod_j L(F/K, \mathrm{Ind}^G_{H'_j} \psi'_j, s)}{\prod_i L(F/K, \mathrm{Ind}^G_{H_i} \psi_i, s)} \\ &= \frac{\prod_j L(F/F^{H'_j}, \psi'_j, s)}{\prod_i L(F/F^{H_i}, \psi_i, s)} \end{aligned}$$

Then by Theorem 20.27, the last expression has a meromorphic continuation to $\mathbb{C}$.

If $\langle \rho, \mathbf{1} \rangle = 0$, then $\psi_i, \psi'_j$ can be chosen to be non-trivial, and so again by Theorem 20.27, it is analytic.

(ii) $L(\rho, s)$ is an $n^{\text{th}}$ root of $L(\rho^{\oplus n}, s)$. But $L(\rho^{\oplus n}, s)$ is analytic and non-zero to $s = 1$ because $\langle \rho, \mathbf{1} \rangle = 0$. Thus we can take an analytic branch.

□

**Theorem 20.33.** **[Brauer's Induction Theorem]** *Let $G$ be a finite group and $\rho$ a $G$ representation. There are elementary subgroups (these are product of cyclic and p-groups) $H_i, H'_J \subset G$ and 1-dimensional representation $\psi_i, \psi'_j$ of $H_i, H'_j$ respectively such that*

$$\rho \oplus \bigoplus_i Ind^G_{H_i} \psi_i \cong \bigoplus_j Ind^G_{H_j} \psi'_j.$$

**Corollary 20.34.** *$L(\rho, s)$ has a meromorphic continuation to $\mathbb{C}$.*

We will omit the proof of the theorem, and the corollary follows by the same argument as the previous one.

## 20.5 Chebotarev's Density Theorem

Now we shall introduce the concept of density and use these to prove the density theorem.

**Definition 20.35.** *Let $S$ be a set of prime numbers. Then $S$ has* **Dirichlet density** $\alpha$ *if*

$$\frac{\sum_{p\in S} p^{-s}}{\log \frac{1}{s-1}} \to \alpha \text{ as } s \to 1^+.$$

**Example 20.36.** *By Dirichlet's theorem of primes in arithmetic progression and Corollary 20.14, we conclude that the set of all primes has density* 1 *and the set*

$$S_{a,N} = \{p \equiv a \bmod N\}$$

*has density* $\frac{1}{\phi(N)}$ *whenever* $(a, N) = 1$.

**Definition 20.37.** *For $F/\mathbb{Q}$ a Galois extension of number fields, $p$ a prime of $\mathbb{Q}$ which is unramified, write $Frob_p \in Gal(F/\mathbb{Q})$ for the Frobenius element $Frob_{\mathfrak{q}/p} \in Gal(F/\mathbb{Q})$ of some prime $\mathfrak{q}$ above $p$. Note that it lies in a well-defined conjugacy class of $Gal(F/\mathbb{Q})$.*

**Example 20.38.** *Let $F = \mathbb{Q}(\zeta_N)$ and $\sigma_a$ be defined by $\sigma_a(\zeta_N) = \zeta_N^a$. For $p \nmid N$, $Frob_p = \sigma_a$ if and only if $p \equiv a \pmod N$ because we know the Frobenius element sends $\zeta_N$ to $\zeta_N^p$. Then by Dirichlet's theorem, the set*

$$S_{N,\sigma} = \{p \nmid N : Frob_p = \sigma\}$$

*has Dirichlet density* $\frac{1}{|Gal(F/\mathbb{Q})|}$ *for each $\sigma \in Gal(F/\mathbb{Q})$ because $\phi(N) = |Gal(F/\mathbb{Q})|$. So $Frob_p$ are uniformly distributed in this case.*

**Theorem 20.39. [Chebotarev's Density Theorem]** *Let $F/\mathbb{Q}$ be a finite Galois extension and $\mathcal{C}$ a conjugacy class of $Gal(F/\mathbb{Q})$. Then the set*

$$S_{\mathcal{C}} = \{p \text{ unramified in } F/\mathbb{Q} \text{ such that } Frob_p \in \mathcal{C}\}$$

*has Diriclet density* $\frac{|\mathcal{C}|}{|Gal(F/\mathbb{Q})|}$.

*Proof.* For $\rho$ a representation of $\mathrm{Gal}(F/\mathbb{Q})$, let

$$L_*(\rho, s) = \prod_{p \text{ unramified}} P_p(\rho, p^{-s})^{-1}.$$

There are only finitely many primes which ramify and we conclude that

(i) $L_*(\rho, s) \neq 0, \infty$ at $s = 1$ if $\rho \neq \mathbb{1}$ and $\rho$ is irreducible, by Corollary 20.32.

(ii) $L_*(\rho, s)$ has a simple pole at $s = 1$ if $\rho$ is trivial, by the proof of Corollary 20.32 and Theorem 20.27.

Let $\chi_\rho$ be the character of $\rho$.

If $p$ is unramified, then $I_p = \{1\}$ and so $\rho^{I_p} = \rho$, and let $\lambda_i$'s be the eigenvalues (with multiplicity) of $\mathrm{Frob}_p$ on $\rho$. Then

$$\begin{aligned}
\log \frac{1}{P_p(\rho, p^{-s})} &= \log \frac{1}{\prod_i (1 - \lambda_i p^{-s})} \\
&= \sum_i \log \frac{1}{1 - \lambda_i p^{-s}} \\
&= \left(\sum_i \lambda_i\right) p^{-s} + \left(\frac{\sum_i \lambda_i^2}{2}\right) p^{-2s} + \cdots \\
&= \sum_{n\geq 1} \frac{\chi_\rho(\mathrm{Frob}_p)^n}{n} p^{-ns}.
\end{aligned}$$

The Dirichlet series

$$\sum_{p \text{ unramified}} \sum_{n \geq 1} \frac{\chi_\rho(\mathrm{Frob}_p)^n}{n} p^{-ns}$$

has bounded coefficients becaise$a_{p^n} = \frac{\chi_\rho(\mathrm{Frob}_p)^n}{n}$; $a_k = 0$ if $k \neq p^n$, and

$$|\chi_\rho(g)| \leq \dim\rho \leq |Gal(F/\mathbb{Q}|.$$

So it defines an analytic branch of $\log L_*(\rho, s)$ on $\Re(s) > 1$ by Proposition 20.13.

By the proof of Corollary 20.14, the sum

$$\sum_{p \text{ unramified}} \sum_{n \geq 2} \frac{\chi_\rho(\mathrm{Frob}_p)^n}{n} p^{-ns}$$

is bounded on $\Re(s) > 1$ (it is bounded by $\dim\rho \sum_{k=1}^{\infty} \frac{1}{k^2}$).

From the above discussion, we conclude that

(i) the term

$$f_\rho(s) = \sum_{p \text{ unramified}} \chi_\rho(\mathrm{Frob}_p) p^{-s}$$

is bounded as $s \to 1$ on $\Re(s) > 1$ if $\rho \neq \mathbb{1}$ and $\rho$ is irreducible.

(ii) the term

$$f_{\mathbb{1}}(s) = \sum_{p \text{ unramifed}} p^{-s} \sim \log \frac{1}{s-1}$$

as $s \to 1$.

Now since $\chi_\rho$ form a basis for the class function, and by defining

$$C_{\mathcal{C}}(g) = \begin{cases} 1 & \text{if } g \in \mathcal{C}, \\ 0 & \text{otherwise} \end{cases}$$

we have

$$\sum_{p \in S_{\mathcal{C}}} p^{-s} = \sum_{p \text{ unramified}} C_{\mathcal{C}}(\mathrm{Frob}_p) p^{-s} = \sum_{\rho \text{ irreducible}} \langle \chi_\rho, C_{\mathcal{C}} \rangle f_\rho(s)$$

because we can write $C_{\mathcal{C}} = \sum_\rho \langle \chi_\rho, C_{\mathcal{C}} \rangle \chi_\rho$. But this is equal to

$$\frac{|\mathcal{C}|}{|\mathrm{Gal}(F/\mathbb{Q})|} f_{\mathbb{1}}(s) + \sum_{\rho \neq \mathbb{1}} \langle \chi_\rho, C_{\mathcal{C}} \rangle f_\rho(s)$$

by definition of inner product of characters. The result follows by the previous observations. □

**Corollary 20.40.** *Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial. The set of primes $p$ such that $f(X)$ mod $p$ factorises as a product of irreducible polynomials of degree $d_1, d_2, \ldots, d_n$ has Dirichlet density $\frac{T}{|Gal(f)|}$ where $Gal(f)$ is the Galois group of the splitting field over $\mathbb{Q}$ and $T$ is the size of the set*

$$\{g \in Gal(f) : g \text{ has cycle type } (d_1, \ldots, d_n) \text{ on roots of } f\}.$$

*Proof.* $f(X)$ has repeated roots mod $p$ in $\bar{\mathbb{F}}_p$ for finitely many $p$. For the other primes, $\mathrm{Frob}_p$ acts as an element of cycle type $(d_1, \ldots, d_n)$ because when it is unramified, $\mathrm{Frob}_p$ corresponds to the generator of the extension $\mathbb{F}_p[X]/f(X)$ and so it has cycle type $(d_1, \ldots, d_n)$ (for some $d_i$, depending on the factorisation of $f(X)$ mod $p$).

So

$$\sum_{p \in S} p^{-s} \sim \sum_{\substack{p \text{unramified} \\ \mathrm{Frob}_p \text{ acts as } (d_1, \ldots, d_n)}} p^{-s}$$

and we have the required density because two elements have the same cycle type if and only if they lie in the same conjugacy class and then use the previous theorem. □

**Example 20.41.** *Let $f(X)$ be a monic irreducible polynomial of degree 5, with $Gal(f) = S_5$. Then*

*(i) The primes $p$ such that $f(X)$ splits into linear factor mod $p$ have density $\frac{1}{120}$.*

*(ii) The primes $p$ such that $f(X)$ is irreducible mod $p$ have density $\frac{24}{120} = \frac{1}{5}$.*

*(iii) The primes $p$ such that $f(X)$ mod $p$ is a product of quadratic irreducible and a cubic irreducible is $\frac{20}{120} = \frac{1}{6}$.*

**Corollary 20.42.** *If $f(X) \in \mathbb{Z}[X]$ is monic irreducible, non-linear. Then $f(X)$ mod $p$ has no roots in $\mathbb{F}_p$ for infinitely many primes $p$.*

*Proof.* It suffices to find some $g \in \mathrm{Gal}(f)$ such that it fixes no root of $f(X)$. To see this, let $S$ be the set of primes of such prime $p$, so if such $g$ exists, then $g$ has cycle type $(d_1, \ldots, d_n)$ for some $d_i > 1$. Now $f(X)$ has no root mod $p$ is equivalent of saying $f(X)$ mod $p$ splits into irreducibles as $(d_1, \ldots, d_n)$ with $d_i > 1$. But if such $g$ exists, then the set of primes $p$ with $f(X)$ mod $p$ splits as $(d_1, \ldots, d_n)$ has non-zero density by Corollary 20.40 and so we have infinitely many of such primes.

By transitivity of the action of the Galois group on the roots, we have, for any root $\alpha$,

$$|\mathrm{stab}_{\mathrm{Gal}(f)}(\alpha)| = \frac{|\mathrm{Gal}(f)|}{\deg f}.$$

But for each $\alpha$, the stabliser contains the identity, so

$$\left| \bigcup_{\alpha \text{ root of } f(X)} \mathrm{stab}_{\mathrm{Gal}(f)}(\alpha) \right| < \deg f \cdot \frac{|\mathrm{Gal}(f)|}{\deg f}$$

and so there exists $g \in G$ which does not lie in the stabliser of $\alpha$ for any $\alpha$. This completes the proof. □

## 20.6 Exercises

1. (i) For each Dirichlet character modulo 12, compute the first twenty coefficients of its Dirichlet $L$-series.

   (ii) For each irreducible representation $\rho$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$, write down the first twenty coefficients of Artin $L$-series of $L(\mathbb{Q}(\zeta_{12})/\mathbb{Q}, \rho, s)$.

2. Let $K$ be a number field and $\zeta_K(s) = \sum_{n\geq 1} a_n n^{-s}$ the expression for its Dedekind $\zeta$-function as an ordinary Dirichlet series. Show that the $n^{\text{th}}$ Dirichlet coefficient $a_n$ is the number of ideals of $\mathcal{O}_K$ with norm $n$.

3. Let $\rho$ be the the unique 2-dimensional irreducible representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{5})/\mathbb{Q})$. Compute the first ten coefficients of its Artin $L$-series.

4. Find the Galois group of the extension $\mathbb{Q}(\zeta_5, \sqrt[5]{5})/\mathbb{Q}$ and compute its character table. Determine the local polynomial at $23, 5, 7$ and 11 for the unique four-dimensional irreducible representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_5, \sqrt[5]{5})/\mathbb{Q})$. (Hint: four representations come from $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, the last is the complement to $\mathbb{1}$ in the permutation action on the $5^{\text{th}}$ roots of 5.)

5. Prove the identity between Dedekind $\zeta$-functions

$$\zeta_{\mathbb{Q}(\zeta_3, \sqrt[3]{m})}(s) \cdot \zeta_{\mathbb{Q}}(s)^2 = \zeta_{\mathbb{Q}(\sqrt[3]{m})}(s)^2 \cdot \zeta_{\mathbb{Q}(\zeta_3)}(s),$$

where $m$ is any integer that is not a perfect square.

6. Let $F/\mathbb{Q}$ be a finite Galois extension, and let $\tau$ and $\rho$ be two representations of its Galois group. Use Chebotarev's density theorem to show that if $L(\rho, s) = L(\tau, s)$ then $\rho \cong \tau$. Hence, show that if $K$ and $L$ are two finite Galois extensions of $\mathbb{Q}$ with

7. Let $F_1, F_2$ be finite Galois extensions of $\mathbb{Q}$ (inside some common extension $M/\mathbb{Q}$), and write $\mathrm{Split}(F_i)$ for the set of primes of $\mathbb{Q}$ that split completely in $F_i$. Note that

$$F_1 \subset F_2 \Rightarrow \mathrm{Split}(F_1) \supset \mathrm{Split}(F_2).$$

Use Chebotarev's density theorem to prove the converse:

$$\mathrm{Split}(F_1) \supset (F_2) \Rightarrow F_1 \subset F_2.$$

Hence, show that if $K$ and $L$ are two finite Galois extensions of $\mathbb{Q}$ with $\zeta_K(s) = \zeta_L(s)$, then $K \cong L$.

8. Find an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ whose reduction modulo every prime is reducible. Find a polynomial $g(X) \in \mathbb{Z}[X]$ which has no root in $\mathbb{Z}$, but which has a root modulo every prime.

## 20.7 Hint and Solutions

1. (i) $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. For $\chi_1 = \mathbb{1}$, we have $a_1 = a_5 = a_7 = a_{11} = a_{13} = a_{17} = a_{19} = 1$ and 0 otherwise.

   For $\chi_2$ given by $\chi_2(5) = -1, \chi_2(7) = 1, \chi_2(11) = -1$, we have $a_1 = a_7 = a_{13} = a_{19} = 1, a_5 = a_{11} = a_{17} = -1$ and 0 otherwise.

   For $\chi_3$ given by $\chi_3(5) = -1, \chi_3(7) = -1, \chi_3(11) = 1$, we have $a_1 = a_{11} = a_{13} = 1, a_5 = a_7 = a_{17} = a_{19} = -1$ and 0 otherwise.

   For $\chi_4$ given by $\chi_4(5) = 1, \chi_4(7) = -1, \chi_4(11) = -1$, we have $a_1 = a_5 = a_{17} = a_{13} = 1, a_7 = a_{11} = a_{19} = -1$ and 0 otherwise.

(ii) The Galois group is abelian and so every irreducible representation is 1-dimensional, exactly as above.

The only primes which ramify are 2 and 3. For $p \neq 2, 3$ and $\mathfrak{q}$ above $p$, $I_{\mathfrak{q}/p} = \{1\}$ and so $\rho^{I_p} = \rho$. Since $\rho$ is 1-dimensional, we conclude that the local polynomial at $p$ is $1 - \rho(\mathrm{Frob}_p)T$.

Let $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ where $\sigma_1 = id, \sigma_2(\zeta_{12}) = \zeta_{12}^5, \sigma_3(\zeta_{12}) = \zeta_{12}^7, \sigma_4(\zeta_{12}) = \zeta_{12}^{11}$. For $p = 2$, $f_{\mathfrak{q}/2} = 2$ and $I_2 = \{id, \sigma\}$. Pick $\mathrm{Frob}_p = \sigma_2$, then use the same notation as in (i), we have

$$P_2(\chi_1, T) = 1 - T, P_2(\chi_2, T) = 1 + T, P_2(\chi_3, T) = 1, P_2(\rho_4, T) = 1.$$

Similarly, for 3, we can also pick $\mathrm{Frob}_3$ to be $\sigma_2$. Then

$$P_3(\chi_1, T) = 1 - T, P_3(\chi_2, T) = 1, P_3(\chi_3, T) = 1 + T, P_3(\chi_4, T) = 1.$$

For 5, the inertia group is trivial, and the residue degree of any prime above it is 2. We can again pick $\mathrm{Frob}_5$ to be $\sigma_2$. Then

$$P_5(\chi_1, T) = 1 - T, P_5(\chi_2, T) = 1 + T, P_5(\chi_3, T) = 1 + T, P_5(\chi_4, T) = 1 - T.$$

Similarly work out the result for $7, 11$ and $17$.

2. Write

$$\zeta_K(s) = \prod_{0 \neq \mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \sum_{n \geq 1} a_n n^{-s}.$$

Expand the second term, we have

$$\prod_{0 \neq \mathfrak{p} \subset \mathcal{O}_K} (1 + N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{-2s} + \cdots) = \sum_{0 \neq I \subset \mathcal{O}_K} N(I)^{-s}$$

by unique factorisation of ideals. Then compare the coefficient and group the terms with the same norm.

3. Let $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ where $\sigma_1$ is trivial and

$$\sigma_2(\zeta_3) = \zeta_3^2, \sigma_2(\sqrt[3]{5}) = \sqrt[3]{5}, \sigma_5(\zeta_3) = \zeta_3, \sigma_5(\sqrt[3]{5}) = \zeta_3\sqrt[3]{5}, \sigma_6 = \sigma_5^2, \sigma_3 = \sigma_2\sigma_5, \sigma_4 = \sigma_2\sigma_6.$$

Writing $x = \sigma_5, y = \sigma_2$, and for the 2-dimensional representation $\rho$, let $v$ be an eigenvector of $\rho(x)$. Then some elementary calculation and choice of basis, we have

$$\rho(x) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{pmatrix}, \rho(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Now consider the primes less than 10. By using the technique in the previous chapter, we conclude that for 2, the inertia group is trivial, and can pick $\mathrm{Frob}_2 = y$, and so $P_2(\rho, T) = \det(1 - Ty) = 1 - T^2$.

For 3, the inertia group is the whole group and so $\rho^I = 0$, so $P_3(\rho, T) = 1$.

Similarly, we also get 5 totoally ramified so $P_5(\rho, T) = 1$.

For 7, the inertia group is trivial and residue degree is 3, we can pick $\mathrm{Frob}_7 = x$. Then $P_7(\rho, T) = \det(1 - Tx) = T^2 + T + 1$.

Thus, we have

$$a_1 = 1, a_2 = a_3 = a_5 = a_6 = a_8 = a_9 = a_10 = 0, a_4 = 1, a_7 = -1.$$

4. Let $S$ be the set of $5^{\text{th}}$ root of unity and $\rho_S$ be the permutation representation on $S$. Let $\chi_S$ be the character. Let $x(\zeta_5) = \zeta_5^2, x(\sqrt[5]{5}) = \sqrt[5]{5}$ and $y(\sqrt[5]{5}) = \zeta_5\sqrt[5]{5}, y(\zeta_5) = \zeta_5$. Then

$$\rho_S(x) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Similarly,

$$\rho_S(y) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $\rho_4$ be the 4-dimensional representation. Now by the hint, and Proposition 20.26 we have that

$$P_p(rho_4, s)P_p(\mathbb{1}, s) = P_p(\rho_S, s).$$

The rest is similar to what we did above, investigating the splitting behavior of the primes and pick a Frobenius. So we calculate the local polynomial for $\mathbb{1}$ and $\rho_S$ and then divide.

5. Let $F = \mathbb{Q}(\zeta_3, \sqrt[3]{m})$, $L = \mathbb{Q}(\sqrt[3]{m})$ and $K = \mathbb{Q}(\zeta_3)$. By Example 20.24 and Theorem 20.27 (the expression of $\zeta$-function in terms of $L$-series), and Proposition 20.27, it is equivalent to prove that

$$\operatorname{Ind}_{\{1\}}^G \mathbb{1} \oplus \mathbb{1}^{\oplus 2} = (\operatorname{Ind}_{H_1}^G \mathbb{1})^{\oplus 2} \oplus \operatorname{Ind}_{H_2}^G \mathbb{1}$$

where $G = \operatorname{Gal}(F/\mathbb{Q}), H_1 = \operatorname{Gal}(F/L)$ and $H_2 = \operatorname{Gal}(F/K)$. Then it suffices to check that the character holds for this as character determines the representation. The results follows by an elementary check.

6. Since it is over $\mathbb{Q}$ so there is only one prime with norm $p$, namely $p$ itself. Thus, if the $L$-series are the same then they must have the same local polynomial for each prime $p$. Now by Chebotarev's density theorem, for each conjugacy class $\mathcal{C}$, there exists at least one prime $p$ where $p$ is unramified and $\operatorname{Frob}_p$ lies in $\mathcal{C}$, because the density is positive. Therefore, for each conjugacy class $\mathcal{C}$, we take a prime $p$ for which the above holds, and for this $p$, since the local polynomials are the same, then $\rho$ and $\tau$ must have the same eigenvalues on $\operatorname{Frob}_p$ and so they have the same trace.

   Now recall that the trace is invariant under conjugate and so $\rho$ and $\tau$ have the same trace on each element in $\mathcal{C}$. But $\mathcal{C}$ is arbitrary and then $\rho$ and $\tau$ have the same character $\chi$. Recall that character determines the representation so $\rho \cong \tau$.

   For the second part, let $M = LK$ be the composition of $L$ and $K$. Since $\zeta_K(s) = \zeta_L(s)$, then setting $H_1 = \operatorname{Gal}(M/L), H_2 = \operatorname{Gal}(M/K), G = \operatorname{Gal}(M/\mathbb{Q})$ we have

$$L(M/\mathbb{Q}, \operatorname{Ind}_{H_1}^G \mathbb{1}, s) = L(M/\mathbb{Q}, \operatorname{Ind}_{H_2}^G \mathbb{1}, s).$$

   This implies that $\operatorname{Ind}_{H_1}^G \mathbb{1} = \operatorname{Ind}_{H_2}^G \mathbb{1}$.

   Let $g \in H_1$ then $\operatorname{Ind}_{H_1}^G \mathbb{1}(g) \neq 0$ and so $\operatorname{Ind}_{H_2}^G \mathbb{1}(g) \neq 0$. But this only happens when $g \in H_2$ because $K, L$ are Galois over $\mathbb{Q}$ so $H_1, H_2$ are both normal. This implies that $g \in H_1$ if and only if $g \in H_2$. Therefore, $H_1 = H_2$.

7. Let $p \in \text{Split} F_2$. Then $\text{Frob}_p$ is identity and the conjugacy class of identity has size 1. So $\text{Split}(F_2)$ has density $\frac{1}{|\text{Gal}(F_2/\mathbb{Q})|} = d_2$. Similarly, $\text{Split}(F_1)$ has density $\frac{1}{|\text{Gal}(F_1/\mathbb{Q})|} = d_1$.

   By assumption, $\text{Split}(F_2) \subset \text{Split}(F_1)$ and so $d_2 \leq d_1$. This implies that $[F_1 : \mathbb{Q}] \leq [F_2 : \mathbb{Q}]$.

   Let $M = F_1F_2$ and $S$ be the set of primes which splits completely in $M$. Then $p \in S$ if and only if $\text{Frob}_{p,M}$ is identity. This implies that (by Lemma 20.25) the Frobenius element of $p$ in $F_1, F_2$ are both identity.

   Conversely, if the Frobenius elements of $p$ in $F_1$ and $F_2$ are both identity, then again by Lemma 20.25, the Frobenius element of $p$ in $M$ must lie in both $\text{Gal}(M/F_1)$ and $\text{Gal}(M/F_2)$. If $F_1 \not\subset F_2$ then we conclude that the Frobenius element of $p$ in $M$ is identity.

   So if $F_1 \not\subset F_2$, then we conclude that $p$ splits completely in $F_1$ and $F_2$ if and only if $p$ splits completely in $M$. But $\text{Split}(F_2) \subset \text{Split}(F_1)$ and so the set $S$ is exactly $\text{Split}(F_2)$. Then again by using the density theorem, we will conclude that

$$|\text{Gal}(M/\mathbb{Q})| = |\text{Gal}(F_2/\mathbb{Q})|$$

   which gives a contradiction to our assumption so we must have $F_1 \subset F_2$.

   For the second part, we know from above that the splitting behavior determines the Galois extension. Note that $p$ splits completely in $K$ if and only if $a_p = [K : \mathbb{Q}]$ in $\zeta_K(s)$ (use question 2). So if $\zeta_K(s) = \zeta_L(s)$, then $p$ splits completely in $K$ if and only if $p$ splits completely in $F$. Then by the previous part, $L = K$.

8. Consider $(X^2 - 2)(X^2 - 3)(X^2 - 6)$. The reason is simple: for each prime $p$, either $p$ is a quadratic residue of 2 or 3, or a quadratic residue of 6.

   Consider the polynomial $f(X) = X^4 - 10X^2 + 1$. It has no root in $\mathbb{Z}$. But the extension it defines is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and so it has Galois group $C_2 \times C_2$. For any prime $p \neq 2$, if it has no root in $\mathbb{Z}$, then Kummer-Dedekind applies and so it inerts. But then decomposition group must be cyclic since it is unramified, and $C_2 \times C_2$ is not cyclic. For 2, it has a root 1.

# 21 p-adic number

In this chapter, we shall introduce the notion of p-adic numbers. We shall begin with an important theorem in number theory which involves the p-adic numbers (which we will not prove) to get readers a general idea about the importance of p-adic numbers in number theory.

**Theorem 21.1. [Hesse, Minkowski]** *Let $f$ be a homogeneous quadratic polynomial with integer square-free coefficients. $f = 0$ has a non-trivial solution in $\mathbb{Q}$ (or equivalently in $\mathbb{Z}$) if and only if it is soluble (non-trivially) in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p$.*

The $\mathbb{Q}_p$ is the p-adic numbers of the prime $p$ which we shall define soon. In fact, it can be shown that $\mathbb{R}$ and $\mathbb{Q}_p$ for $p = 2, 3, 5, \ldots$ are the only completions of $\mathbb{Q}$ and so the theorem states a very strong relation between the integer solutions and solutions in p-adic numbers of homogeneous polynomial.

## 21.1 Absolute value

Before giving the formal definition of p-adic numbers, we shall introduce the definition of absolute values.

**Definition 21.2.** *An* **absolute value** *on a field $K$ is a function*

$$|.| : K \longmapsto \mathbb{R}$$

*satisfying:*

*(i)* $|x| \geq 0$ *and* $|x| = 0 \iff x = 0$.

*(ii)* $|xy| = |x||y|$ *for all* $x, y, \in K$.

*(iii)* $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$.

**Example 21.3.** *Let $K = \mathbb{R}$ or $\mathbb{C}$ then the usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$ is an absolute value in the above definition. Usually, we shall write $|.|_\infty$ for the usual absolute value. Notice that the square of $|.|_\infty$ is not an absolute value, for*

$$4 = |2|^2 = |1 + 1|^2 \geq |1|^2 + |1|^2$$

*so the triangle inequality does not hold.*

**Definition 21.4.** *Let $K$ be any field. The* **trivial** *absolute value is define as $|x| = 1$ for all $x \in K^*$ and $|x| = 0$ if $x = 0$. It is easy to check that this is an absolute value.*

**Proposition 21.5.** *If $x^n = 1$ for some $n$, then $|x| = 1$. In particular, $|-1| = 1$ and so $|-x| = x$ for all $x \in K$*

*Proof.* If $x^n = 1$, then $|x|^n = 1$ by multiplicative property and so $|x|$ is a root of unity. But $|x|$ is real and $|x| \geq 0$ so $|x| = 1$. □

The absolute value $|.|$ induces a metric on $K$. Let $d(x, ) = |x - y|$ and so it is easy to check that $d$ is a distance function on $K$ and so it is a topological space. Open balls are of the form

$$B(x, r) = \{y \in K : |x - y| < k\}$$

**Lemma 21.6.** $|.| : K \longmapsto \mathbb{R}$ *is continuous.*

*Proof.* Since $(0, r)$ forms a basis for the metric space $\mathbb{R}$ so it suffices to check that the preimage is open in $K$. But this is just the ball $B(0, r)$ and so it is clear open. □

**Definition 21.7.** *Let $K = \mathbb{Q}$. Let $p$ be a prime and $0 < \alpha < 1$. The* **$p$-adic absolute value** *$|.|_p$ is defined as $|x|_p = 0$ if $x = 0$ and for any $x \in \mathbb{Q}^*$ write $x = p^r \frac{u}{v}$ where $u, v \in \mathbb{Z}$ and $(u, p) = (v, p) = 1$,*

$$|x|_p = \alpha^{v_p(x)}$$

*where $v_p(x) = r$. Usually we take $\alpha = \frac{1}{p}$.*

**Proposition 21.8.** *The $p$-adic absolute value is an absolute value.*

*Proof.* It is clear that $|x|_p \geq 0$ for all $x$. Now it is clear that

$$v_p(xy) = v_p(x) + v_p(y)$$

so $|xy|_p = |x|_p|y|_p$. Finally, $v_p(x + y) \geq \min(v_p(x), v_p(y))$ and since $\alpha < 1$ so

$$|x + y|_p = \alpha^{v_p(x+y)} \leq \max |x|_p, |y|_p$$

□

**Definition 21.9.** *We say an absolute value obeys the* **ultrametric law** *if*

$$|x + y| \leq \max(|x|, |y|)$$

*for all $x, y \in K$. An absolute value is called* **non-archimedean** *if it satisfies the ultrametric law. Otherwise, we say an absolute value is* **archimedean**

The following theorem is a criteria of non-archmedian absolute value.

**Theorem 21.10.** *An absolute value is non-archmedian if and only if $|n|$ is bounded for all $n \in \mathbb{Z}$.*

*Proof.* Suppose $|.|$ is non-archimedean, then since $|n| = |-n|$ so we may assume that $n \geq 1$ and so

$$|n| \leq \max(|n-1|, |1|) \leq \max(|n-2|, |1|, |1|) \ldots \leq \max(|1|, |1|, \ldots, |1|)$$

and so it is bounded.

Conversely, suppose $|n| \leq B$ for some constant $B$. Take any $x, y \in K$ and

$$|x + y|^n = \left| \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r} \right|$$

Now we have $n + 1$ terms and use the multiplicative property, for each $|\binom{n}{r}|$, it is bounded by $B$ and we take the larger term of $|x|, |y|$ in each $|x|^r |y|^{n-r}$ so we have

$$|x + y|^n \leq (n + 1)B \max(|x|^n, |y|^n)$$

and so

$$|x + y| \leq ((n + 1)B)^{\frac{1}{n}} \max(|x|, |y|)$$

Now let $n \to \infty$ and so $((n + 1)B)^{\frac{1}{n}} \to 1$, so

$$|x + y| \leq \max(|x|, |y|)$$

and $|.|$ is non-archmedian. □

**Corollary 21.11.** *If $char(k) > 0$, then all absolute values on $K$ are non-archmedian.*

*Proof.* If $char(k) > 0$, then we have only finitely many integers $n$ in the sense that $n = 1+1+\cdots+1$, say if the characteristic is $p$ then we have $p$ integers and so their values are clearly bounded and so it is non-archmedian. □

**Example 21.12.** *Let $K = \mathbb{Q}$, $p = 5$ and $|.| = |.|_5$. Let $(a_n)_{n=1}^{\infty}$ be a sequence such that $a_n = \frac{10^n-1}{3}$. Then for any $m \geq n$,*

$$|a_n - a_m|_5 = \left|\frac{10^m - 10^n}{3}\right|_5 = \frac{1}{5^n}$$

*So it is a cauchy sequence with respect to the absolute value $|.|_5$. It converges in $\frac{-1}{3}$ in $\mathbb{Q}$ because*

$$\left|a_n + \frac{1}{3}\right|_5 = \frac{1}{5^n} \to 0$$

However, not every cauchy sequence with respect to the $p$-adic absolute value converges in $\mathbb{Q}$.

**Example 21.13.** *Define a sequence $(a_n)_{n=1}^{\infty}$ by $a_1 = 2$ and*

$$a_n^2 + 1 \equiv 0 \ (mod\ 5^n) \text{ and } a_{n+1} \equiv a_n \ (mod\ 5^n)$$

*We may construct $a_n$ in this way: Let $a_{n+1} = a_n + b5^n$ and so*

$$\begin{aligned}(a_n + b5^n)^2 &= = 1 + a_n^2 + 2ba_n5^n + b^2 5^{2n} \\ &= 5^n(c + 2ba_n + b^2 5^n) \\ &\equiv 5^n(c + 2b) \ (mod\ 5^{n+1})\end{aligned}$$

*for some $c$ and so we pick $b$ such that*

$$c + 2b \equiv 0 \ (mod\ 5)$$

*and it is possible because $(2, 5) = 1$. Now, by*

$$a_{n+1} \equiv a_n \ (mod\ 5^n)$$

*we have that the sequence $(a_n)_{n=1}^{\infty}$ is cauchy. Suppose $a_n \to l$. Then*

$$|l^2 + 1|_5 \leq |a_n^2 + 1|_5 + |l^2 - a_n^2|_5$$

*and $|a_n^2 + 1|_5 \leq 5^{-n}$ and $l^2 - a_n^2$ can be arbitrarily small because $a_n^2 \to l$ and so $|l^2 + 1|_5$ can be arbitrarily small and so it must be $0$. So $l^2 + 1 = 0$ and so $l = i$ which does not lie in $\mathbb{Q}$.*

Thus, it is nature to introduce the following concept:

**Definition 21.14.** *The* **field of $p$-adic number** $\mathbb{Q}_p$ *is the completion of $\mathbb{Q}$ with respect to $|.|_p$. The* **ring of $p$-adic integers** $\mathbb{Z}_p$ *is*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

The usual addition, multiplication and the $|.|_p$ will extend on $\mathbb{Q}_p$ by continuity.

**Proposition 21.15.** *$(\mathbb{Q}_p, |.|_p)$ is a non-archmedian valued field.*

*Proof.* It is clear that the absolute value of any integer is bounded by 1. So it must be non-archmedian. □

**Lemma 21.16.** *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

*Proof.* By definition $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ and so $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Now $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$ because for any $x \in \mathbb{Z}_p$, take $y \in \mathbb{Q}_p$ such that $|x-y|_p < 1$, then

$$|y|_p \leq \max(|x|_p, |x-y|_p) \leq 1$$

and $|y| \in \mathbb{Z}_p$. So $\mathbb{Q} \cap \mathbb{Z}_p$ is dense in $\mathbb{Z}_p$ (This is a fact in metric space, which is not hard to prove.) Now

$$\begin{aligned} Q \cap \mathbb{Z}_p &= \{x \in \mathbb{Q} : |x|_p \leq 1\} \\ &= \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{(p)} \end{aligned}$$

So in some sense it can be viewed as the localisation of $\mathbb{Z}$ at the multiplicative set $S$ where $S = \mathbb{Z} \backslash \langle p \rangle$ (but do not worry if you don't understand what this means.) Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$ so $p \nmid b$. For each $n \geq 1$, pick $y_n$ such that

$$by_n \equiv 1 \pmod{p^n}$$

So it is clear that $by_n \to 1$ as $n \to \infty$ in with respect to $|.|_p$. So

$$ay_n = \frac{a}{b} by_n \to \frac{a}{b}$$

and so $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. □

Now we may generalise the definition of $p$-adic value by the following:

**Definition 21.17.** *Let $K$ be a number field and $p \subseteq \mathcal{O}_K$ be a prime ideal. Then for each non-zero $x \in K$, let $v_p(x) = ord_p(x)$. Pick $0 < \alpha < 1$ and so define*

$$|x|_p = \alpha^{v_p(x)}$$

*and $|0|_p = 0$ as usual. Then $|.|_p$ is an absolute value on $K$. Now we can pick suitable $\alpha$ so this will extend absolute value $|.|_p$ in $\mathbb{Q}$. We write $K_p$ to be the completion of $K$ with respect to $|.|_p$.*

**Lemma 21.18.** *Let $|.|_1$ and $|.|_2$ be non-trivial absolute values on $K$. Then the followings are equivalent:*

*(i) $|.|_1$ and $|.|_2$ induce the same topology.*

*(ii) $|x|_1 < 1$ if and only if $|x|_2 < 1$*

*(iii) $|x|_2 = |x|_1^c$ for some constant $c > 0$.*

*Proof.* 1. (i) ⇒ (ii): We have

$$\begin{aligned} |x|_1 < 1 &\iff x^n \to 1 \text{ with respect to } |.|_1 \\ &\iff x^n \to 1 \text{ with respect to } |.|_2 \iff |x|_2 < 1 \end{aligned}$$

because $|.|_1$ and $|.|_2$ induce the same topology so sequence converges to the same limit.

2. (ii) ⇒ (iii): Pick some $a \in K^*$ with $|a|_1 < 1$. This is possible because $|.|_1$ is non-trivial and if $|a|_1 > 1$, pick $a^{-1}$. Let $x \in K^*$, $m, n \in \mathbb{Z}$, $n > 0$ such that

$$\frac{\log |x|_1}{\log |a|_1} > \frac{m}{n}$$

Since $|a|_1 < 1$, so $\log |a|_1 < 0$ and so

$$\begin{aligned} n \log |x|_1 \quad &< \quad m \log |a|_1 \iff \left|\frac{x^n}{a^n}\right|_1 < 1 \\ \iff \quad &\left|\frac{x^n}{a^n}\right|_2 < 1 \iff \frac{\log |x|_2}{\log |a|_2} > \frac{m}{n} \end{aligned}$$

Since $\frac{m}{n} \in \mathbb{Q}$, and we have shown that for any $\frac{m}{n} \in \mathbb{Q}$,

$$\frac{\log |x|_2}{\log |a|_2} > \frac{m}{n} \iff \frac{\log |x|_1}{\log |a|_1} > \frac{m}{n}$$

and so

$$\frac{\log |x|_1}{\log |a|_1} = \frac{\log |x|_2}{\log |a|_1}$$

But as $a$ is fixed, we have that

$$\log |x|_2 = c \log |x|_1$$

for some constant $c$ and so the result follows.

3. (iii) $\Rightarrow$ (i) Let $B(x, r)$ be an open ball with respect to $|.|_1$, then it is $B(x, r^c)$ with respect to $|.|_2$ and vice versa. So open balls are the same and so they induce the same topology.

□

**Definition 21.19.** *If one of the conditions holds in Lemma 2.18, then we say $|.|_1$ and $|.|_2$ are* **equivalent**. *An equivalence class of non-trivial absolute values is called a* **place**.

**Theorem 21.20. [Ostrowski]** *Any non-trivial absolute value $|.|$ on $\mathbb{Q}$ is equivalent to either $|.|_\infty$ or $|.|_p$ for some prime $p$.*

In fact the proof will characterises when $|.|$ is equivalent to $|.|_p$ and when to $|.|_p$.

*Proof.* Suppose $|.|$ archmedian. Let $a, b > 1$ be integers and $b \geq a$. Write:

$$b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_1 a_1 + c_0, 0 \leq c_i < a$$

Then $m \leq n \log_a b$. Let $B = \max_i (c_i)$. Then by triangle inequality we have

$$|b^n| \leq (m+1) B \max (|a|^m, 1)$$

and so

$$|b| \leq ((n \log_a b + 1) B)^{\frac{1}{n}} \max (|a|^{\log_a b}, 1)$$

Therefore, let $n \to \infty$,

$$|b| \leq \max (|a|^{\log_a b}, 1)$$

Since $|.|$ is archmedian, so we have integer $b > 1$ with $|b| > 1$ by Theorem 21.10 as it is unbounded. Then by above, we have

$$|b| \leq |a|^{\log_a b}$$

Now we can repeat the above process because the above also implies $|a| > 1$ as $\log_a b > 0$. Then we would have

$$|a| \leq |b|^{\log_b a}$$

and together we have

$$\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda$$

But since $a, b$ are arbitrary, in the sense that $|b|$ is unbounded so we just increase $b$ and for any $1 < a < b$ we would have

$$|a| = |a|_\infty^\lambda$$

Now use $|-a| = |a|$ and $|\frac{1}{a}| = \frac{1}{|a|}$, and so $|.|$ is equivalent to $|.|_\infty$.

Now suppose $|.|$ is non-archmedian. Then we have seen in the proof of Theorem 21.10 that $|n| \leq 1$ for any integer $n$. Now since $|.|$ is non-trivial so there exists $n > 1$ such that $|n| < 1$. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorisation of $n$. Suppose $|p| < 1$ and $|q| < 1$ where $p, q$ are distinct primes. Then we have $r, s \in \mathbb{Z}$ such that

$$1 = rp + sq \Rightarrow 1 = |1| = |rp + sq|$$

But $|.|$ is non-archmedian, so

$$|rp + sq| \leq \max(|rp|, |sq|) \leq \max(|p|, |q|) < 1$$

because $|r|, |s| > 1$ and we have $1 < 1$ which is a contradiction. So at most one of the prime $p$ has the property that $|p| < 1$. But $|n| < 1$ and so by the multiplicative property we know that we must have some $p$ such that $|p| < 1$. So $|p| = \alpha$ for some $0 < \alpha < 1$ and $|q| = 1$ for any other prime $q$. So

$$n = p^e \prod_i p_i^{e_i} \Rightarrow |n| = \alpha^e$$

and so $|.|$ is equivalent to $|.|_p$. □

**Corollary 21.21.** *Let $\hat{K}$ be the completion of a number filed $K$ with respect to an archmedian absolute value $|.|$. Then $\hat{K} \cong \mathbb{R}$ or $\mathbb{C}$, which is an isomorphism as fields with respect to the topology. In particular, the archmedian places of $K$ corresponding to the real embeddings and the conjugate pairs of the complex embeddings.*

*Proof.* By Theorem 21.20, since $|.|$ is archmedian, so the restriction of $|.|$ to $\mathbb{Q}$ is equivalent to $|.|_\infty$ and since the completion of $\mathbb{Q}$ with respect to $|.|_\infty$ is $\mathbb{R}$, so $\mathbb{R} \subseteq \hat{K}$. Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Then inside $\hat{K}$,

$$K \subseteq \mathbb{R}(\alpha) = \mathbb{R} \text{ or } \mathbb{C}$$

depending on whether $\alpha$ is real or complex. But $\mathbb{R}$ and $\mathbb{C}$ are complete, and $\mathbb{Q}$ is dense in $\mathbb{R}$ and so $K$ is dense in $\mathbb{R}$ or $\mathbb{C}$. So

$$\hat{K} = \mathbb{R} \text{ or } \mathbb{C}$$

□

**Remark 21.22.** *(i) Check the only extension of $|.|_\infty$ on $\mathbb{R}$ to $\mathbb{C}$ is $|.|_\infty$ itself. This can be done by checking they have the same topology or just let $z = re^{i\theta}$ and use multiplicative property and $\mathbb{Q}$ is dense in $\mathbb{R}$.*

*(ii) In fact $\mathbb{R}$ and $\mathbb{C}$ are the only complete archmedian fields.*

*(iii) The non-archmedian places of number field $K$ are the $|.|_p$ for $p$ a prime ideal of $\mathcal{O}_K$. We will see this later.*

**Theorem 21.23. [Weak approximation theorem]** *Let $|.|_1, \ldots, |.|_n$ be pairwise inequivalent non-trivial absolute values on a field $K$. Given $\beta_1, \ldots, \beta_n \in K$ and $\epsilon > 0$, then there exists $\alpha \in K$ such that*

$$|\alpha - \beta_i|_i < \epsilon \forall 1 \leq i \leq n$$

*Proof.* We show by induction that there exist $y_1, \ldots, y_n \in K$ such that

$$|y_i|_i > 1 \text{ and } |y_i|_j < 1 \text{ if } i \neq j$$

For the case $n = 2$, swapping $|.|_1$ and $|.|_2$ if necessary, we have $w \in K$ such that $|w|_1 < 1$ and $|w|_2 \geq 1$. This is because if $|w|_1 < k \iff |w|_2 < 1$ for all $w$ then the two absolute values are equivalent by Lemma 21.18. Also, $|.|_2$ is non-trivial so there exists $z \in K$ such that $|z|_2 > 1$ and so let $y = w^r z$ for $r$ sufficiently large. So that $|y|_1 = |w|_1^r |z| < 1$ (using $|w|_1^r < 1$) and $|y|_2 > |w|_2^r > 1$ Now let $y_1 = \frac{1}{y}$ and $y_2 = y$ and so we are done for the case $n = 2$.

Suppose now we have $y \in K$ with $|y|_1 > 1$ and $|y|_j < 1$ for $j = 2, \ldots, n-1$. The case $n = 2$ tells that there exists $t \in K$ such that $|t|_1 > 1$ and $|t|_n < 1$. Then we define

$$y_1 = \begin{cases} y & \text{if } |y|_n < 1 \\ y^r t & \text{if } |y|_n = 1 \\ \left(\frac{y^r}{1+y^r}\right) t & \text{if } |y|_n > 1 \end{cases}$$

and pick $r$ sufficiently large. It is clear that if $|y|_n < 1$ and we pick $y_1 = y$ then $|y_1|_j < 1$ for any $j \neq 1$. If $|y|_n = 1$, then we pick $y_1 = y^r t$ for $r$ large so that $|y_1|_j < 1$ for any $j = 2, 3, \ldots, n-1$ because we don't know what the values of $|t|_j$ are. But by this construction it should be clear that $y_1$ satisfies the condition. Finally, if $|y|_n > 1$ then we pick $y_1 = (\frac{y^r}{1+y^r})t$ for $r$ large enough. Now we use triangle inequality

$$|x - y| \geq ||x| - |y||_\infty$$

Since $|y|_1 > 1$

$$|y_1|_1 \leq \frac{|y|_1^r}{|y|_1^r - 1} |t|_1 > 1$$

for $r$ large because the fractional term tends to 1. Similarly, for $j = 2, \ldots, n-1$,

$$|y_1|_j \leq \frac{|y|_j^r}{1 - |y|_j^r} |t|_j < 1$$

because the fractional term tends to 0. For $|y_1|_n$ it is similar to the case $|y_1|_1$ and so we have found such $y_1$. Now as the condition is symmetric so we can use the same method to construct $y_2, \ldots, y_n$. Now we have proved the claim. To finish the proof, let

$$\alpha = \sum_{i=1}^{n} \left(\frac{y_i^r}{1 + y_i^r}\right) \beta_i$$

and take $r$ sufficiently large. So

$$\alpha - \beta_j = \sum_{i \neq j} \left(\frac{y_i^r}{1 + y_i^r}\right) \beta_i - \left(\frac{1}{1 + y_j^r}\right) \beta_j$$

and use a similar analysis as above, the result follows. □

Now we shall prove some property for non-archmedian absolute values.

**Lemma 21.24.** *Let $(K, |.|)$ be non-archemedian, then*

*(i)* $|x| < |y| \Rightarrow |x \pm y| = |y|$.

*(ii)* $|x_1 + \cdots + x_n| \leq \max_{1 \leq i \leq n} |x_i|$ *with equality if* $|x_i| < |x_1$ *for all* $i > 1$.

*(iii) If $(K, |.|)$ is complete, then*

$$\sum_{n=1}^{\infty} a_n \text{ converges } \iff a_n \to 0$$

*Proof.* (i) Given $|x| < |y|$, by ultrametric law we have

$$|x + y| \leq \max(|x|, |y|) = |y|$$

On the other hand,

$$|y| \leq \max(|x + y|, |x|)$$

but $|y| > |x|$ so $|y| \leq |x + y|$ and hence $|x + y| = |y|$. Now replace $y$ by $-y$.

(ii) Ultrametric law and induction will give the inequality there. To prove the later part, apply (i). Let $x = x_2 + \cdots + x_n$, $y = x_1$ and so $|x_i| < |y|$ for all $i \geq 2$ by assumption and so $|x| < |y|$, then $|x + y| = |y| = \max_i |x_i|$.

(iii) One way is clear by usual analysis. Let $S_n = \sum_{i=1}^{n} a_i$. If $S_n$ converges to $l$, then $a_n = S_n - S_{n-1} \to l - l = 0$. Conversely, suppose $a_n to 0$, for $m \geq n$,

$$|S_m - S_n| = |a_{n+1} + \cdots + a_m| \leq \max_{n<i\leq m} |a_i| \to 0$$

So $(S_m)_{m=1}^{\infty}$ is cauchy hence converges as we assume $K$ is complete.

□

**Lemma 21.25.** *Let $(K, |.|)$ be non-archmedian.*

*(i) If $y \in B(x, r)$, then $B(y, r) = B(x, r)$.*

*(ii) If $y \in \overline{B(x, r)}$, then $\overline{B(y, r)} = \overline{B(x, r)}$.*

*(iii) $B(x, r)$ is both open and closed.*

*(iv) $\overline{B(x, r)}$ is both open and closed.*

*Proof.* (i) Let $z \in B(y, r)$ then $|y - z| < r$ and now by ultrametric law

$$|z - x| \leq \max(|z - y|, |y - z|) < r$$

and so $z \in B(x, r)$. So $B(y, r) \subseteq B(x, r)$ but they have the same radius so they are identical.

(ii) Replace $<$ by $\leq$ in the proof above.

(iii) (i) says that if two open balls have intersection, then they are identical. So open balls are either disjoint or identical. By definition $B(x, r)$ is open. Now if $y \notin B(x, r)$, then $B(y, r) \cap B(x, r) = \varnothing$ by the above observation and so $B(y, r) \subseteq B(x, r)^c$. Hence it is closed.

(iv) $|.|$ is continuous and so it is the preimage of $(0, r]$ and so it is closed. It is open because if $y \in \overline{B(x,r)}$ then $B(y,r) \subseteq \overline{B(y,r)} = \overline{B(x,r)}$ by (ii).

□

**Corollary 21.26.** *Let $(K, |.|)$ be non-archimedian, then $K$ is totally disconnected.*

*Proof.* If $x, y \in K$ and $x \neq y$. Let $r = \frac{1}{2}|x - y|$ then $B(x,r)$ and its complement partitions $K$ and by Lemma 21.25 we have shown that the complement of $B(x,r)$ and $x \in B(x,r)$ and $y \in B(x,r)^c$ so it is totally disconnected. □

## 21.2 Valuation

We shall introduce the concept of valuation.

**Definition 21.27.** *A valuation on $K$ is a function $v : K^* \longmapsto \mathbb{R}$ such that*

*(i)* $v(xy) = v(x) + v(y)$.

*(ii)* $v(x + y) \geq \min(v(x), v(y))$.

Fix $0 < \alpha < 1$. Then $v$ determines a non-archimedian absolute value $|x| = \alpha^{v(x)}$ for $x \neq 0$ and $|0| = 0$. Conversely, any non-archimedian absolute value determines a valuation $v(x) = \log_\alpha |x|$.

**Remark 21.28.** *Usually, we ignore the trivial valuation $v(x) = 0$ for all $x$. $v_1, v_2$ are said to be equivalent if and only if there exists $c > 0$ such that $v_1(x) = cv_2(x)$ for all $x \in K^*$. So one really should think of $v$ and $|.|$ as the same thing.*

**Definition 21.29.** *The image of the map $v(K^*)$ is a subgroup of $\mathbb{R}$ and is called the* **value group**. *If the value group is discrete (i.e. $\cong \mathbb{Z}$) then we say $v$ is a* **discrete valuation**.

We will use the following definitions and notations.

**Definition 21.30.** *Let $K$ be a field and $|.|$ be an absolute value.*
*$\mathcal{O}_v = \{x \in K : |x| \leq 1\}$ is the* **valuation ring** *of the ring of integers.*
*$\mathcal{O}_v^* = \{x \in K : |x| = 1\}$ is the* **unit group**.
*$m = \{x \in K : |x| < 1\}$ is a maximal ideal.*
*$k = \mathcal{O}_v/m$ is called the* **residue field**.

**Remark 21.31.** *(i) $m$ is the unique maximal ideal, as it consists of all non-unit elements. Thus, $\mathcal{O}_v$ is a local ring.*

*(ii) Let $x, y \in \mathcal{O}_v$, then*

$$x\mathcal{O}_v \subset y\mathcal{O}_v \iff \frac{x}{y} \in \mathcal{O}_v \iff \left|\frac{x}{y}\right| \leq 1 \iff v(x) \geq v(y).$$

*In particular, since $v(1) = 0$, so $x \in \mathcal{O}_v$ if and only if $v(x) \geq 0$.*

*(iii) If $0 \neq x \in m$, then $\mathcal{O}_v\left[\frac{1}{x}\right] = K$, because for any $y \in K$, we have some $n$ such that $v(y) \geq nv\left(\frac{1}{x}\right)$ and so by (ii) we have $y \in x^{-n}\mathcal{O}_v$. In particular, $K = Frac(\mathcal{O}_v)$.*

*(iv)* $\mathcal{O}_v$ *is integrally closed in* $K$*. Indeed, if* $x \in K^*$ *satisfies a monic polynomial say*

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = 0.$$

*Then move* $x^m$ *to the other side and take valuation we have*

$$mv(x) \geq \min\{(m-1)v(x) + v(a_{m-1}), \ldots, v(a_0)\}.$$

*But* $v(a_i) \geq 0$ *and so we deduce that* $v(x) \geq 0$ *which implies* $x \in \mathcal{O}_v$ *by definition.*

**Lemma 21.32.** *The following are equivalent:*

*(i)* $v$ *is discrete.*

*(ii)* $\mathcal{O}_v$ *is a PID.*

*(iii)* $\mathcal{O}_v$ *is Noetherian.*

*(iv)* $m$ *is principal.*

*Proof.* (i)⇒(ii) Let $I$ be a non-zero ideal in $\mathcal{O}_v$. Since the image is discrete, so there exists $x \in I$ with minimal valuation. Then for any $y \in I$, $v(y) \geq v(x)$ and so by Remark 21.31(ii), $y \in x\mathcal{O}_v$. Hence, $I = x\mathcal{O}_v$ is principal.
(ii)⇒(iii) Every PID is Noetherian.
(iii)⇒(iv) $\mathcal{O}_v$ is Noetherian so $m$ is finitely generated, say by $x_1, \ldots, x_k$. Let $x$ be $x_i$ which has minimal valuation. Then, by the same argument as above, $m = x\mathcal{O}_v$.
(iv)⇒(i) Let $m = \pi\mathcal{O}_v$ and let $c = v(\pi) > 0$. Then each $x \in \mathcal{O}_v$ has valuation 0 or valuation $\geq c$ by Remark 21.31(ii). Hence, if $y, z$ are elements in $K^*$ with $v(y) < v(z)$ then $v(y) \leq v(z) + c$ and so it is discrete. □

**Definition 21.33.** *A* **discrete valuation ring (DVR)** *is a PID with exactly one prime ideal.*

**Lemma 21.34.** *(i) If* $v$ *is discrete then* $\mathcal{O}_v$ *is a DVR.*

*(ii) If* $R$ *is a DVR, then there exists a discrete valuation* $v$ *on* $K = Frac(R)$ *such that* $R = \mathcal{O}_v$*. (Such* $v$ *is unique if we normalise it)*

*Proof.* (i) By Lemma 21.32 if $v$ is discrete then $\mathcal{O}_v$ is a PID and in PID, prime ideal is the same as maximal ideal.

(ii) Let $R$ be a DVR and let $\pi$ be a generator of the unique maximal ideal $m$. Every $x \in R\backslash\{0\}$ can be written in the form $x = u\pi^r$, where $u \in R^*$ and $r \geq 0$. (This is because every non-unit element must lie in some maximal ideal and it has to be $m$ in this case.) Hence every $x \in K^*$ may be written as $x = ux^r$, where $u \in R^*$ and $r \in \mathbb{Z}$. Finally, define $v : K^* \longmapsto \mathbb{Z}$ by $v(u\pi^r) = r$. Then

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\} = R.$$

□

We now give several examples.

**Example 21.35.** *(i)* $\mathbb{Z}_{\langle p \rangle} = \{x \in \mathbb{Q} : |x|_p \leq 1\}$ *is a DVR with field of fraction* $\mathbb{Q}$*, maximal ideal* $\langle p \rangle$ *and residue field* $\mathbb{Z}/p\mathbb{Z}$*.*

*(ii)* $\mathbb{Z}_p$ *is a DVR with field of fraction* $\mathbb{Q}_p$*, maximal ideal* $\langle p \rangle$ *and residue field* $\mathbb{Z}/p\mathbb{Z}$*. (See exercises)*

*(iii) Let* $k$ *be any field,* $K = k(t)$ *the rational functional field. Define* $v_0\left(t^n \frac{f(t)}{g(t)}\right) = n$ *where* $f(0), g(0) \neq 0$*. So* $v_0$ *can be understood as the order of vanishing at* $0$*. Then:*
$\mathcal{O} = \{f \in k(t) : f(0)$ *is defined* $\}$*.*
$\mathcal{O} = \{f \in \mathcal{O} : f(0) \neq 0\}$*.*
$m = \{f \in \mathcal{O} : f(0) = 0\}$*.*
*The residue field is* $k$ *by using the map* $\mathcal{O} \longmapsto k$ *by* $f \mapsto f(0)$*.*

*(iv) Likewise, we can define* $v_a$ *for any* $a \in \mathbb{C}$ *as the order of vanishing at* $a$*. Also, define* $v_\infty\left(\frac{f(t)}{g(t)}\right) = v_0\left(\frac{f(1/t)}{g(1/t)}\right)$*, the order of vanishing at infinity.*

*(v)* $K = k((t)) =$ *the field of Laurent series*$= \{\sum_{n \geq n_0} a_n t^n : a_n \in K\}$*, where* $n_0$ *is any integer. We define the valuation*

$$v\left(\sum a_n t^n\right) = \min\{n : a_n \neq 0\}.$$

*Then,* $\mathcal{O} = k[[t]] =$ *power series ring.*
$m = \{f \in k[[t]] : f(0) = 0\}$ *and* $\mathcal{O}/m = k$ *via* $f \mapsto f(0)$*.*

**Remark 21.36.** *In fact, one can show (see exercises) that if* $k$ *is algebraically closed, then the ones in (iv) are the only discrete valuations on* $k(t)$ *with* $v(k^*) = 0$*. Also,* $K = k(t)$ *is the function field of* $\mathbb{P}^1$*, the Riemann surface. Similar examples exist for any smooth point on an algebraic curve.*

**Lemma 21.37.** *Referring to Example 21.35*

*(i)* $k[[t]]^* = \{\sum_{n \geq 0} a_n t^n : a_0 \neq 0\}$*.*

*(ii)* $k((t))$ *is indeed a field, containing* $k(t)$*, and* $v$ *extends* $v_0$*.*

*(iii)* $k((t))$ *(resp.* $k[[t]]$*) is the completion of* $k(t)$ *(resp.* $k[t]$*) with respect to* $v_0$*.*

*Proof.* (i) Suppose $\left(\sum_{n \geq 0} a_n t^n\right)\left(\sum_{n \geq 0} b_n t^n\right) = 1$. Solve $b_n$ in terms of $a_n$ and solution exists if and only if $a_0 \neq 0$.

(ii) Take the leading term, $t^k$ for some $k$, then we may assume $f \in k((t))$ has the form $t^k\left(\sum_{n \geq 0} a_n t^n\right)$ and so by (i) we have an inverse to $f$. It contains $k[t]$ and so it contains the field of fraction. If $f(t) = t^n \frac{p(t)}{q(t)}$ with $p(0), q(0) \neq 0$. Then by (i), $p(t), q(t) \in k[[t]]^*$ and so $v(p) = v(q) = 0$. Hence, $v(f) = v(t^n) = n = v_0(t^n) = v_0(f)$ and so $v$ extends $v_0$.

(iii) It is clear that $k[t]$ is dense in $k[[t]]$ with respect to $v_0$. So it suffices to prove that $k[[t]]$ is complete with respect to $v$ by (ii). Let $(f_n)_{n=0}^\infty$ be a Cauchy sequence. Then for each $r$, there exists $N_r$ such that for all $m, n \geq N_r$, $v(f_m - f_n) \geq r$, i.e. $f_m \equiv f_n \pmod{t^r}$. Now construct an element

$$g(t) = \sum_{r \geq 0} c_r t^r, \text{ where } c_r = r^{th} \text{ coefficient in } f_{N_r}.$$

Then for each $r > 0$, we have $g \equiv f_{N_r} \pmod{t^r}$, i.e. $v(g - f_{N_r}) \geq r$, and so $f_n \to g$. (Recall that $|g - f_{N_r}| \to 0$ if $v(g - f_{N_r}) \to \infty$.)

□

Now let $v : K^* \longmapsto \mathbb{Z}$ be a normalised discrete valuation, $\mathcal{O} = \mathcal{O}_v$, pick $\pi \in m$ with $v(\pi) = 1$, we call $\pi$ a **uniformaliser**. We shall now give an important theorem in local fields.

**Theorem 21.38.** [**Hensel's Lemma Version 1**] *Assume $K$ is complete with respect to $v$. Let $f(X) \in \mathcal{O}[X]$. Suppose that the reduction $\overline{f(X)} \in k[X]$ has a simple root, i.e. there exists $a \in \mathcal{O}$ such that $f(a) \equiv 0 \pmod{\pi}$ and $f'(a) \not\equiv 0 \pmod{\pi}$, i.e. , $\overline{f(a)} = 0$ and $\overline{f'(a)} \neq 0$. Then there exists a unique $x \in \mathcal{O}$ such that $f(x) = 0$ and $x \equiv a \pmod{\pi}$.*

**Theorem 21.39.** [**Hensel's Lemma Version 2**] *Assume $K$ is complete with respect to a discrete valuation $v$ with associated absolute value $|.|$. Suppose $f(X) \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ satisfies $|f(a)| < |f'(a)|^2$. Then there exists a* **unique** *$x \in \mathcal{O}$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.*

Since version 1 is a special case of version 2, we will only prove version 2. The proof is constructive.

*Proof.* Let $r = v(f'(a))$. We will construct a sequence $(x_n)$ in $\mathcal{O}$ such that:
(i) $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$.
(ii) $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$.
In such a way, by completeness of $K$, $x_n$ converges to an element $x$ by property (ii) and $f(x) = 0$ by property (i). Let $x_1 = a$. Suppose $x_n$ has been constructed, let $x_{n+1} = x_n + b\pi^{n+r}$ for some $b \in \mathcal{O}$ so that (ii) is satisfied. By Taylor expansion, we have

$$f(x_{n+1}) = f(x_n) + b\pi^{n+r} f'(x_n) + O(\pi^{2n+2r}).$$

Let $f(x_n) = c\pi^{n+2r}$ for some $c \in \mathcal{O}$ by assumption. Then we want

$$c\pi^{n+2r} + b\pi^{n+r} f'(x_n) \equiv 0 \pmod{\pi^{n+1+2r}}.$$

But $v(f'(a)) = r$ by assumption and so by construction we conclude

$$v(f'(x_n)) = r \text{ and so } f'(x_n) = u\pi^r, \text{ where } u \in \mathcal{O}^*.$$

Thus, we need to solve $c + ub \equiv 0 \pmod{\pi}$, which is always possible. Therefore, we have obtained a sequence satisfying (i) and (ii). Now since $x_2 \equiv a \pmod{\pi^{1+r}}$ and so the resulting limit $x$ will also have $x \equiv a \pmod{\pi^{1+r}}$. Therefore,

$$|x - a| < |f'(a)|.$$

Now we prove such $x$ is unique. Suppose $x, y$ both satisfy the conditions in the theorem. Then let $\delta = y - x$. Suppose $\delta \neq 0$. Using $|x - a| < |f'(a)|$ and $|y - a| < |f'(a)|$ and the ultrametric law, we have $|\delta| < |f'(a)| = |f'(x)|$.

On the other hand, $0 = f(y) = f(x + \delta) = f(x) + \delta f'(x) + R$, where $|R| \leq |\delta^2|$. But $|0| = 0$ and so we must have $|\delta f'(x)| \leq |\delta^2|$, which gives $|f'(x)| \leq |\delta|$ which contradicts the previous paragraph and so $\delta = 0$, i.e. $x = y$. □

**Remark 21.40.** *If we write down $f(x_n)$ and $f'(x_n)$ explicitly, we will see that the proof uses the Newton-Raphson method $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.*

**Proposition 21.41.**

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \neq 2, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2. \end{cases}$$

*Proof.* Case when $p \neq 2$: Each element in $\mathbb{Q}_p^*$ can be identified by $x = up^r$ where $r \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^*$. This gives an isomorphism

$$\mathbb{Q}_p^* \cong \mathbb{Z}_p^* \times \mathbb{Z}.$$

Thus,

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \times \mathbb{Z}/2\mathbb{Z}.$$

Now let $b \in \mathbb{Z}_p^*$. Then $b$ is a square if and only if $\bar{b} \in \mathbb{F}_p^*$ is a square. One direction is clear. Now if $\bar{b}$ is a square, then consider the polynomial $X^2 - b$. Since $\mathrm{Char}(F_p) \neq 2$ so by Hensel's lemma (version 1) we conclude that $b$ is a square in $\mathbb{Z}_p^*$. But the set of quadratic residues mod $p$ forms a subgroup of index 2. Therefore,

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

and the result follows.
Case when $p = 2$. The proof is identical except that in this case, we claim that an element $b \in \mathbb{Z}_2^*$ is a square if and only if $b \equiv 1 \pmod 8$. Again, one direction is clear as the only odd square modulo 8 is 1. For the other direction, we again use Hensel's lemma on $X^2 - b$ (with Version 2) to see that if $b \equiv 1 \pmod 8$ then $b$ is a square in $\mathbb{Z}_2^*$. Thus,

$$(\mathbb{Z}_2^*/\mathbb{Z}_2^*)^2 \cong (\mathbb{Z}/8\mathbb{Z})^*/\{1\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

and the result follows from this. □

**Remark 21.42.** *If we follow the proof above, when $p \neq 2$, we can take $1, u, p, up$ as coset representatives. When $p = 2$, we can take $(-1)^s 5^t 2^r$ as coset representatives where $s, t, r \in \{0, 1\}$. (because $(-1)$ and $5$ generate $(\mathbb{Z}/8\mathbb{Z})^*$.)*

**Corollary 21.43.** *$\mathbb{Q}_p$ has exactly 3 quadratic extensions for $p \neq 2$. $\mathbb{Q}_2$ has exactly 7 quadratic extensions.*

*Proof.* Each quadratic extension is obtained by adjoining $\sqrt{\alpha}$ for some $\alpha \in \mathbb{Q}_p$. For $p \neq 2$, each non-square in $\mathbb{Q}_p^*$ is the same as one of $u, p, up$ multiplied by a square by the previous proposition, where $u$ is a non-residue. Fix some $u$, we have

$$\mathbb{Q}_p(u), \mathbb{Q}_p(p), \mathbb{Q}_p(up).$$

The case $p = 2$ is similar. □

**Proposition 21.44.**

$$\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^3 \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

*Proof.* The proof is similar to Proposition 21.41, except that we have to prove the fact that $b \in \mathbb{Q}_3$ is a cube if and only if $b \equiv \pm 1 \pmod 9$. Again this can be done by using Hensel's lemma version 2. Thus,

$$\mathbb{Z}_3^*/(\mathbb{Z}_3^*)^3 \cong (\mathbb{Z}/9\mathbb{Z})^*/\{\pm 1\} \cong \mathbb{Z}/3\mathbb{Z}.$$

□

Now let $K$ be a field, $v$ be a normalised discrete valuation, with uniformalise $\pi$, $k = \mathcal{O}/m$ the residue field.

**Lemma 21.45.** *Suppose $A \subset \mathcal{O}$ is a set of coset representatives for $k$. Then*

*(i) Every $x \in \mathcal{O}$ can be written uniquely as $x = \sum_{r=0}^{\infty} a_r \pi^r$ with $a_r \in A$.*

*(ii) $K$ is complete if and only if every $\sum_{r=0}^{\infty} a_r \pi^r$ (with $a_r \in A$) converges.*

*Proof.* (i) Take $r_0 = \bar{x}$ in the residue field. Suppose we have $r_0, \ldots, r_n$, such that $x - r_0 - \cdots - r_n\pi^n = u_{n+1}\pi^{n+1}$ where $u_{n+1} \in \mathcal{O}$. Then set $r_{n+1} = \overline{u_{n+1}}$. Thus,

$$x - r_0 - \cdots - r_{n+1}\pi^{n+1} = (u_{n+1} - r_{n+1})\pi^{n+1} = u_{n+2}\pi^{n+2}.$$

Therefore, we have obtained a sequence $(r_n)_{n=0}^{\infty}$ such that $x = \sum_{r=0}^{\infty} a_r\pi^r$.

(ii) If $K$ is complete, then the series converges if and only if the end terms tends to 0 by Lemma 21.24. Clearly the above series converges. Conversely, if the above series converges, take a Cauchy sequence $(x_n)_{n=0}^{\infty}$ in $\mathcal{O}$. Let $x_n = \sum_{r=0}^{\infty} b_{r,n}\pi^r$ for some $b_{r,n} \in A$ by (i). For each $r$, there exists an $N_r$ such that for all $m \geq N_r$, $x_{N_r} \equiv x_m \pmod{\pi^r}$. So $b_{r,N_r} = b_{r,m}$ for all $m \geq N_r$. Take $a_r = b_{n,N_r}$ for each $r$. It is then clear that $x_n \to x = \sum_{r=0}^{\infty} a_r\pi^r$. So $\mathcal{O}$ is complete.

Now take a Cauchy sequence $(x_n)_{n=0}^{\infty}$ in $K$. So there exists some $N$ such that for all $n, m \geq N$, we have $|x_n - x_m| \leq 1$. In other words, $x_n \in x_N + \mathcal{O}$ for all $n \geq N$. By previous, $x_N + \mathcal{O}$ is complete. Therefore, $x_n$ tends to a limit in $x_N + \mathcal{O} \subset K$, and so $K$ is complete.

□

## 21.3 The Techmüller map

Let $K$ be complete with respect to a discrete valuation $v$. Suppose the residue field $k$ is finite, say $|k| = q$. Put $f(X) = X^q - X \in \mathcal{O}[X]$. Each $\alpha \in k$ is a simple root of $\overline{f(X)} = X^q - X \in k[X]$. Hensel's lemma tells that there exists a unique $a \in \mathcal{O}$ such that $a^q = a$ and $a \equiv \alpha \pmod{\pi}$.

**Definition 21.46.** *$a \in \mathcal{O}$ is called the* **Teichmüller representative** *for $\alpha \in k$. Write $a = [\alpha]$.*

**Lemma 21.47.** *[.] is multiplicative.*

*Proof.* Let $a = [\alpha]$ and $b = [\beta]$. Then $(ab)^q = a^q b^q = ab$. Further, $ab \equiv \alpha\beta \pmod{\pi}$ and so $ab = [\alpha\beta]$. □

**Corollary 21.48.** *$k^* \hookrightarrow \mathcal{O}^*$. For example, $\mu_{p-1} \subseteq \mathbb{Q}_p$.*

*Proof.* The inclusion map is just given by [.] and it is a homomorphism. In particular, when $K = \mathbb{Q}_p$, the residue field is $\mathbb{Z}/p\mathbb{Z}$ and so $\mu_{p-1} \subseteq \mathbb{Q}_p$. □

**Theorem 21.49.** *Let $K$ be complete with respect to discrete valuation $v$. If Char$(K) > 0$ and $k$ is finite then $K \cong k((t))$.*

*Proof.* Let Char$(K)$ =Char$(k) = p$. Let $|k| = q = p^f$. Let $\alpha, \beta \in k$. We have

$$(|\alpha| + |\beta|)^q = |\alpha|^q + |\beta|^q = |\alpha| + |\beta|.$$

Therefore, $|\alpha + \beta| = |\alpha| + |\beta|$ and so $|.| : k \hookrightarrow K$ is a field embedding. Since $K$ is complete, so by Lemma 21.45.

$$K = \left\{ \sum_{n \geq n_0} a_r\pi^r : a_r \in k \right\} \cong k((t)) \text{ via } \pi \mapsto t.$$

□

## 21.4 Exercises

1. Prove the product formula for the absolute value on $\mathbb{Q}$: If $x \in \mathbb{Q}^*$, then
$$\prod_{\alpha} |x|_\alpha = 1$$
where $\alpha \in \{\infty, 2, 3, 5, \ldots\}$ lists all the normalised absolute values on $\mathbb{Q}$.

2. If $c \in \mathbb{Z}_p$ satisfies $|c|_p < 1$, show that $(1+c)^{-1} = 1 - c + c^2 - c^3 + \cdots$. Hence find $a \in \mathbb{Z}$ such that $|4a - 1|_5 \leq 5^{-10}$.

3. (i) Show that the inclusion $\mathbb{Z} \subset \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ for all $n \geq 1$.

   (ii) Show that $|\mathbb{Z}_p/m\mathbb{Z}_p| = |m|_p^{-1}$ for all $m \in \mathbb{Z}_p$.

   (iii) Show that a subgroup of $\mathbb{Z}_p$ is open if and only if it has finite index.

4. Suppose $a \in \mathbb{Z}$ with $(a, p) = 1$. Prove that the sequence $(a^{p^n})_{n \geq 0}$ converges in $\mathbb{Q}_p$ and its limit is a $(p-1)^{\text{th}}$ root of unity which is congruent to $a$ mod $p$.

5. Show that $\mathbb{Z}\left[\frac{1}{p}\right]$ is dense in $\mathbb{Q}_p$. Recall that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the group of all roots of unity in $\mathbb{C}$. Show that $\mathbb{Q}_p/\mathbb{Z}_p$ is isomorphic to the group of all $p$-power roots of unity.

6. (i) Prove that any $x \in \mathbb{Q}_p$ can be written uniquely in the form $x = \sum_{n=n_0}^{\infty} a_n p^n$ where $n_0 \in \mathbb{Z}$ and each $a_n \in \{0, 1, \ldots, p-1\}$.

   (ii) Show that $x \in \mathbb{Q}$ if and only if the sequence $(a_n)_n$ is eventually periodic.

   (iii) Let $s_p(n)$ denote the sum of the $p$-adic digits of $n \in \mathbb{Z}$. Prove the formula
$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

7. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in $\mathbb{Z}_7$, but has no solutions in $\mathbb{Z}_5$ or $\mathbb{Z}_3$. How many are there in $\mathbb{Z}_2$?

8. Consider the series
$$\sqrt{1+15} = 1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} 15^n$$
where $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$. Show that the series converges to 4 with respect to the 3-adic absolute value, to $-4$ with respect to the 5-adic absolute value, and diverges with respect to all other absolute values on $\mathbb{Q}$.

9. Let $K$ be a field is complete with respect to a discrete valuation $v$ and with finite residue field $k$. Show that if $\text{Char}(k) \nmid n$ then $|K^*/(K^*)^n| = n|\mu_n(K)|$ where $\mu_n(K)$ is the group of $n^{\text{th}}$ roots of unity in $K$.

10. Let $K$ be a field that is complete with respect to a non-trivial absolute value $|\cdot|$. Show that $K$ is uncountable. (Note that when $|\cdot|$ is archimedean, then $K$ contains the reals, so you may assume $|\cdot|$ is non-archimedean.)

11. Let $\bar{K}$ be the completion of a field $K$ with respect to a valuation $v$. Recall that $v$ extends to a valuation $\bar{v}$ on $\bar{K}$. Prove that the value groups of $v$ and $\bar{v}$ are the same. In particular this shows that if $v$ is discrete then $\bar{v}$ is discrete.

12. Let $k$ be an algebraically closed field and $K = k(t)$. Prove that every normalised discrete valuation on $K$ which is trivial on $k$ (i.e. $v(a) = 0$ for $a \in k^*$) is either of the form $v_a$ for some $a \in k$ (order of vanishing at $a$) or is $v_\infty(p/q) = \deg q - \deg p$.

13. Let $\mathbb{Z}[[T]]$ be the ring of formal power series over $\mathbb{Z}$. Show that there is an isomorphism of ring $\mathbb{Z}[[T]]/\langle T - p\rangle \cong \mathbb{Z}_p$ induced by the natural ring homomorphism

$$\mathbb{Z}[[T]] \longmapsto \mathbb{Z}_p \text{ via } \sum_{n=0}^{\infty} a_n T^n \mapsto \sum_{n=0}^{\infty} p^n a_n.$$

14. **(Another form of Hensel's Lemma)** Let $f_1, \ldots, f_n \in \mathbb{Z}_p[x_1, \ldots, x_d]$ with $r \leq d$. Suppose $a = (a_1, \ldots, a_d) \in \mathbb{Z}_p^d$ with $f_i(a) \equiv 0 \pmod{p}$ for all $1 \leq i \leq r$ and $\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(a) \bmod p\right) \geq r$. Show that there exists $x \in \mathbb{Z}_p^d$ with $x \equiv a \pmod{p}$ and $f_i(x) = 0$ for all $1 \leq i \leq r$. Is $x$ unique?

15. Show that the equation $x^2 - 82y^2 = 2$ has solutions in $\mathbb{Z}_p$ for every prime $p$, and yet has no solutions in $\mathbb{Z}$.

## 21.5 Hint and Solutions

1. Write the factorisation

$$x = \frac{a}{b} = \frac{\prod_{i=1}^{m} p_i^{e_i}}{\prod_{j=1}^{n} q_j^{f_j}}.$$

So

$$\prod_{\alpha} |x|_\alpha = x \cdot \prod_{i=1}^{m} p_i^{e_i} \prod_{j=1}^{n} (q_j^{f_j})^{-1} = 1.$$

2. $|c|_p < 1$ so RHS has $a_n = c^n(-1)^n$. Then $|a_n|_p = |c|_p^n \to 0$. So the series converges by Lemma 21.24.

Now let $c = -5$ then

$$-\frac{1}{4} = 1 + 5 + 5^2 + 5^3 + \cdots$$

and so

$$\frac{1}{4} = -1 - 5 - 5^2 - \cdots.$$

Take $a = -1 - 5 - 5^2 - \cdots - 5^n$ for $n$ large enough. Then $4a - 1 \to 0$ and so for $n$ large enough $|4a - 1|_5 \leq 5^{-10}$.

3. (i) Clearly the natural map is a homomorphism. If $x \in \mathbb{Z}$ and $x \in p^n\mathbb{Z}_p$, then $p^n \big| x$ and so $x \in p^n\mathbb{Z}$. So the map is injective.

   Now $\mathbb{Z} \subset \mathbb{Z}_p$ is dense and so for each $b \in \mathbb{Z}_p$, pick $a \in \mathbb{Z}$ such that $|a-b|_p < p^{-n}$ and so $a \equiv b \pmod{p^n}$. Then $a + p^n\mathbb{Z} \mapsto b + p^n\mathbb{Z}_p$, so the map is surjective.

   (ii) If $m \in \mathbb{Z}_p$, let $m = p^n u, u \in \mathbb{Z}_p^*$. Then

$$\mathbb{Z}_p/m\mathbb{Z}_p \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$$

   with cardinality $|m|_p^{-1}$.

   (iii) It is a fact (as it is profinite) that $\mathbb{Z}_p$ is compact. If $H$ is open, then we have

$$\mathbb{Z}_p = \bigcup_{g \in \mathbb{Z}_p} gH.$$

   But it is compact so it has finite index.

   Now suppose $H$ has finite index $m$. Then $m \in H$. Let $m = p^n u$ then

$$p^n\mathbb{Z}_p = m\mathbb{Z}_p \subset H.$$

   But $p^n\mathbb{Z}_p$ is open, so $H$ has non-empty interior. Write $I = p^n\mathbb{Z}_p$. Then $H = \bigcup_{h \in H} h + I$ is open.

4. $a \in \mathbb{Z}$ so $a^p \equiv a \pmod{p}$. Then

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}.$$

   So for all $n \geq m$, $a^{p^n} \equiv a^{p^m} \pmod{p^{m+1}}$, and so

$$|a^{p^n} - a^{p^m}|_p \leq p^{-(m+1)} \to 0.$$

   So it is cauchy and it tends to a limit, say $l$. Now $a^{p-1} \equiv 1 \pmod{p}$. So

$$a^{p^n(p-1)} \equiv 1 \pmod{p^n}$$

   and so $l^{p-1} \equiv 1 \pmod{p^n}$ for all $n$. So $l^{p-1} = 1$.

5. $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. It is clear that $\mathbb{Z}\left[\frac{1}{p}\right]$ is dense in $\mathbb{Q}$. Indeed, for $q \in \mathbb{Q}$, let $q = p^n\frac{a}{b}$. For each $m$, since $(a,p) = (b,p) = 1$, we can pick $c$ such that $bc \equiv a \pmod{p^n}$.

   For the second part, consider the natural map

$$\mathbb{Z}\left[\frac{1}{p}\right] \longmapsto \mathbb{Q}_p/\mathbb{Z}_p.$$

   This is surjective because $\mathbb{Z}\left[\frac{1}{p}\right]$ is dense in $\mathbb{Q}_p$. Clearly the kernel is $\mathbb{Z}\left[\frac{1}{p}\right] \cap \mathbb{Z}_p = \mathbb{Z}$. Then we have

$$\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p.$$

   But $\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ is the group of all $p^{\text{th}}$ power units.

6. (i) Let $x = p^n \frac{a}{b}$. We firstly to prove that we have a $p$-adic expansion for $\frac{a}{b}$. For $a$, consider $a_0 \in \{0, \dots, p-1\}$ such that $a \equiv a_0 \pmod{p}$. Then let $a - a_0 = u_0 p$. Then let $a_1 \in \{0, \dots, p-1\}$ such that $u_0 \equiv a_1 \pmod{p}$. Continue this, we have a $p$-adic expansion for $a$. Then, $\frac{1}{a}$ also has an expansion because $a_0 \neq 0$ (so the power series is invertible). Thus, $\frac{a}{b}$ has a $p$-adic expansion. This implies that every rational number has a $p$-adic expansion.

Now for any $x \in \mathbb{Q}_p$, it is a limit of a cauchy sequence of rational number. Then take the $p$-adic expansion of each one and we can construct a power series which is the limit of the sequence (an analogue of Lemma 21.37). Hence we have a $p$-adic expansion of $\mathbb{Q}_p$.

(ii) If the series is periodic, so there exist $k$ and $N$ such that

$$a_{N+k+m} = a_{N+m} \ \forall m \geq 0.$$

So

$$\begin{aligned} x &= x_1 + p^{N+1}(a_{N+1} + \cdots + a_{N+k}) + p^{N+k+1}(a_{N+1} + \cdots + a_{N+k}) + \cdots \\ &= x_1 + Ap^{N+1}(1 + p^k + p^{2k} + \cdots). \end{aligned}$$

This shows that $x = x_1 + \frac{Ap^{N+1}}{1-p^k}$ and hence it is rational.

Conversely, if $x$ is rational. Assume $x = \frac{a}{b}$ where $p \nmid b$. Let

$$\frac{a}{b} = \sum_{n=0}^{\infty} a_n p^n, S_n = \sum_{i=0}^{n} a_i p^i.$$

Let $u_{n+1} = \frac{a - bS_n}{p^{n+1}}$ and so

$$\frac{a}{b} = S_n + \frac{p^{n+1} u_{n+1}}{b}.$$

But $0 \leq S_n \leq p^{n+1} - 1$, so

$$-b + \frac{a+b}{p^{n+1}} = \frac{a - (p^{n+1} - 1)b}{p^{n+1}} \leq \frac{a - bS_n}{p^{n+1}} = u_{n+1} \leq \frac{a}{p^{n+1}}$$

because $u_{n+1}$ is an integer and it is bounded for all $n$. Without loss of generality, $u_{n+k} = u_n$ for some $k$, for some $n$ large enough. It is easy to check that

$$u_n \equiv a_{n+1} b \pmod{p}, u_{n+k} \equiv a_{n+k+1} b \pmod{p}.$$

But $u_n = u_{n+k}$ and $a_{n+1}, a_{n+k+1} \in \{0, \dots, p-1\}$ so $a_{n+1} = a_{n+k+1}$. Then $u_{n+1} = u_{n+k+1}$ and so $a_{n+k+m} = a_{n+m}$ for all $m \geq 0$.

For general $x$, we have $x = p^n \frac{a}{b}$ and so it is periodic since $\frac{a}{b}$ is. Alternatively, we can assume $\frac{a}{b} < 0$ and if this is true for $\frac{a}{b} < 0$, it holds for $\frac{a}{b} > 0$ (replace $a_n$ by $p - a_n$). Let $k \in \mathbb{N}$ such that

$$p^k - 1 \equiv 0 \pmod{b}.$$

So $\frac{1}{b}(1 - p^k) = z > 0$ and so $\frac{a}{b} = \frac{z}{1-p^k} = z(1 + p^k + p^{2k} + \cdots)$. But $z > 0$ is an integer, so there exists $N$ such that

$$z = \sum_{n=0}^{N} a_n p^n$$

as we know the positive integer always has a $p$-adic expansion. So

$$\frac{a}{b} = \sum_{n=0}^{N} a_n p^n (1 + p^k + p^{2k} + \cdots).$$

(iii) Induction on $n$. It is clear when $n = 1$. Suppose it is true for $\leq n$. Then if $p \big| n+1$, write $n+1 = p^k b$ and let $n+1 = p^k(a_0 + a_1 + \cdots + a_m p^m)$. Then

$$a_0 p^k - 1 = p - 1 + p(p-1) + \cdots + p^{k-1}(p-1) + (a_0 - 1)p^k \Rightarrow s_p(n) = (p-1)k - 1 + s_p(n+1).$$

By induction,

$$v_p(n!) = \frac{n - s_p(n)}{p-1} = \frac{n+1-s_p(n+1)}{p-1} - k$$

and so $v_p((n+1)!) = v_p(n!) + k = \frac{n+1-s_p(n+1)}{p-1}$.

If $p \nmid n+1$, then $v_p((n+1)!) = v_p(n) = \frac{n-s_p(n)}{p-1}$. Now $s_p(n+1) = s_p(n) + 1$ because $p \nmid n+1$. So the result follows. Therefore, it is true for $n \geq 1$. For $n \leq 1$, change the sign.

7. $x^3 - 3x + 4 \equiv (x+3)(x^2 - 3x - 1) \pmod 8$ so we have a simple root. By Hensel's lemma we have a solution equal to $-3$ mod 7. Conversely, if we have a solution then it must be congruent to $-3$ mod 7. So by Hensel's lemma, the solution is unique.

   For $\mathbb{Z}_5$, we have no solution mod 5 and hence no solution in $\mathbb{Z}_5$ (Note that any solution must be a limit of the sequence $x_n$ satisfying $f(x_n) \equiv 0 \pmod{p^n}$ so if we have no solution mod 5 then we have no solution in $\mathbb{Z}_5$).

   For $\mathbb{Z}_3$, we have no solution mod $9 = 3^2$.

   For $\mathbb{Z}_2$, by Hensel's lemma we have a solution congruent to 0 mod 2. We have no solution congruent to 1 mod 2 because we have no solution congruent to either 1 or 3 mod 4.

8. For 3,

$$\binom{\frac{1}{2}}{n} = \frac{(-1)^{n-1}}{2^{2n}(2n-1)}\binom{2n}{n}$$

   and so

$$|a_n|_3 = \left|\frac{\binom{2n}{n}}{2n-1}\right|_3 |3^n|_3 \leq |3^n|_3 \to 0.$$

   So it converges when $p = 3$. Now we have an identity

$$\left(\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}x^n\right)\left(\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}x^n\right) = \sum_{n=0}^{\infty}\binom{1}{n}x^n.$$

   Put $x = 15$, we conclude that the limit is either 4 or $-4$. In this case, $|l-1|_3 < 1$ so $l \to 4$. Similarly, the limit is $-4$ when $p = 5$.

   If it converges for any other $p$, then $15^n$ is a unit and so it still converges if we replace this by some other unit (recall that converges if and only if the $p$-adic value of the end term tends to 0). In particular, we can replace 15 by $p-1$. But

$$\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(p-1)^n = \sqrt{p}$$

   and clearly this is not in $\mathbb{Z}_p$ for any $p \neq 3, 5$.

9. Let $\pi$ be a uniformaliser and $\mathfrak{m}$ be the maximal ideal. Each $x$ can be written uniquely as $\pi^n u$ where $u \in \mathcal{O}_K^*$. Then

$$K^* \cong \mathcal{O}_K^* \times \mathbb{Z}, K^*/(K^*)^n \cong \mathcal{O}_K^*/(\mathcal{O}_K^*)^n \times \mathbb{Z}/n\mathbb{Z}.$$

It suffices to check that

$$|\mathcal{O}_K^*/(\mathcal{O}_K^*)^n| = |\mu_n(K)|.$$

We claim that for any $b \in \mathcal{O}_K^*$, $b$ is an $n^{\text{th}}$ power in $\mathcal{O}_K^*$ if and only if $b$ is an $n^{\text{th}}$ power in $k$, where $k = \mathcal{O}_K/\mathfrak{m}$.

One direction is clear. We need to check that if $b$ is an $n^{\text{th}}$ power in $k$, then it is an $n^{\text{th}}$ power in $\mathcal{O}_K$. Let $b \neq 0$. Consider the polynomial $f(x) = x^n - b$. Since $\text{Char}(k) \nmid n$ so the $f(x)$ is separable. Now $f(x)$ has a solution modulo $\pi$ because $b$ is an $n^{\text{th}}$ power in $k$. Then by Hensel's lemma, we have a lift in $\mathcal{O}_K$ and so $b$ is an $n^{\text{th}}$ power in $\mathcal{O}_K$.

Hence,

$$\mathcal{O}_K^*/(\mathcal{O}_K^*)^n \cong k^*/(k^*)^n.$$

Finally, consider the map $x \mapsto x^n$, this induces an isomorphism

$$k^*/(\mu_n(k)) \cong (k^*)^n.$$

But $\mu_n(k) = \mu_n(K)$. So $|k^*/(k^*)^n| = |\mu_n(K)|$ and so the result follows.

10. Use an analogue of question 6(i). Fix $a$ with $|a| < 1$. Then for any $x \in K^*$, we have $n_0$ such that

$$|a|^{n_0+1} \leq |x| < |a|^{n_0}.$$

Then $\left|\frac{x}{a^{n_0}}\right| < 1$ and so lies in $\mathfrak{m}$. Also, we have

$$a\mathfrak{m} = \{x \in K : |x| < |a|\}.$$

So $\frac{x}{a^{n_0}} \notin a\mathfrak{m}$. So there exists $r_0$ such that

$$\frac{x}{a^{n_0}} - r_0 \in a\mathfrak{m}, r_0 \in \mathfrak{m}/a\mathfrak{m}.$$

Let $x_1 = x - a_0 r_0$, then $\frac{x_1}{a^{n_0}} \in a\mathfrak{m}$. So

$$\left|\frac{x_1}{a^{n_0}}\right| < |a| \Rightarrow |x_1| < |a|^{n_0+1}.$$

So there exists $n_1 > n_0$ such that $|a|^{n_1+1} \leq |x_1| < |a|^{n_1}$.

Now continue the above process so we have

$$x = \sum_{n=n_0}^{\infty} r_n a^n.$$

The expansion is unique because if

$$\sum_{n=n_0}^{\infty} r_n a^n = \sum_{n=m_0}^{\infty} s_n a^n.$$

Then, $a^{n_0+1}$ divides the difference of them and hence $n_0 = m_0$, $a \big| r_{n_0} - s_{n_0}$. But we know $r_n, s_n \in \mathfrak{m}/a\mathfrak{m}$, so $r_{n_0} = s_{n_0}$ and similarly, $r_n = s_n$ for each $n$.

Therefore, we have an injection

$$K \longmapsto (\mathfrak{m}/a\mathfrak{m})^{\mathbb{Z}} \text{ via } x \mapsto (r_{n_0}, r_{n_0}+1, \ldots).$$

It is also surjective, because the series converges as $K$ is complete. So

$$|K| = |\mathfrak{m}/a\mathfrak{m}|^{\mathbb{Z}}$$

which is uncountable.

11. Let $|\cdot|$ corresponds to $v$, so $|\cdot|$ is non-archimedean. It is clear that $v(K) \subset \hat{v}(\hat{K})$. Given $a' \in \hat{v}(\hat{K})$, say $a = \hat{v}(x)$. We have a cauchy sequence $(x_n)_{n=1}^{\infty} \in K$, such that $x_n \to x$.

    Recall that $|x| < |y| \Rightarrow |x \pm y| = |y|$. Let $\widehat{|\cdot|}$ denote the corresponding absolute value of $\hat{v}$. Let $a = \widehat{|x|}$. Then $\widehat{|x_n - x|} \to 0$ and so there exists $m$ large enough such that $\widehat{|x_m - x|} < \widehat{|x|}$. Hence

    $$\widehat{|x_m|} = |(x_m \widehat{-x}) + x| = \widehat{|x|} = a.$$

    But $\widehat{|x_m|} = |x_m|$ and so $|x_m| = a$, which is the same as $v(x_m) = a'$.

12. $k$ is algebraically closed so the only irreducible polynomials are those with degree 1. Since the absolute value is non-trivial, we have $v(x-a) \neq 0$ for some $a \in k$. This is because, if $v(x-a) = 0$ for all $a \in k$ then $v(f(x)) = 0$ for any $f \in K$ by unique factorisation and the assumption $v(b) = 0$ for any $b \in k$.

    Firstly we may assume $v(x-a) > 0$ for some fixed $a$. Then for any $b \neq a$, $b-a = (x-a)-(x-b)$,

    $$0 = v(b-a) \geq \min(v(x-a), v(x-b))$$

    and so $0 \geq v(x-b)$. But $x - b = x - a + (a - b)$ so $v(x-b) \geq \min(v(x-a), v(a-b)) \geq 0$. So $v(x-b) = 0$ for any $b \neq a$. Now the valuation is normalsied, so we must have some $f(x)$ such that $v(f) = 1$. But the valuation of every polynomial is determined by the valuation of the polynomial of degree 1. So $v(x-a) = 1$, and so $v = v_a$, the order of vanishing at $a$.

    Then we assume $v(x-a) < 0$. For any $b \neq a$, we have

    $$0 > v(x-a) \geq \min(v(x-b), v(b-a)).$$

    This implies that $v(x-b) < 0$ for any $b \neq a$ and $v(x-b) \leq v(x-a)$. Also,

    $$0 > v(x-b) \geq \min(v(x-a), v(b-a)).$$

    Hence, $v(x-b) \geq v(x-a)$ and so $v(x-b) = v(x-a)$ for any $b \neq a$. This implies that $x - a$ has the same valuation for any $a \in k$. Again the valuation is normalised, so $v(x-a) = -1$ for any $a \in k$. Therefore, for any $q \in K$ we have $v(q) = -\deg q$. So $v$ is the order of vanishing at $\infty$.

13. The substitution map is clearly homomorphism. The map is surjective because for each $x \in \mathbb{Z}_p$ we have a $p$-adic expansion (see question 6). The kernel is indeed $\langle T - p \rangle$ because

    $$\sum a_n p^n = 0 \Rightarrow \sum a_n T^n = \sum a_n T^n - \sum a_n p^n$$

    and RHS is clearly divisible by $T - p$. So the kernel is contained in $\langle T - p \rangle$. It is clear that $\langle T - p \rangle$ is in the kernel. The result follows.

14. This is an analogue of the proof of Hensel's lemma, and we still apply induction on $n$. Let $x_0 = (a_1, \ldots, a_d)$. We want to pick $x_n$ such that

    $$x_n \equiv x_{n-1} \pmod{p^n}, f_i(x_n) \equiv 0 \pmod{p^n}.$$

    Suppose we have picked $x_n$, let $x_{n+1} = x_n + p^n b$, where $b \in \mathbb{Z}^d$. Then

    $$f_i(x_{n+1}) = f_i(x_n + p^n b) = f_i(x_n) + p^n b \cdot f_i'(x_n) + \cdots .$$

Note that here $f_i'(x_n)$ means $\left(\frac{\partial f_i}{\partial x_j}(x_n)\right)_{j=1}^{d}$. Assuming $f_i(x_n) \equiv 0 \pmod{p^n}$ we have $f_i(x_n) = p^n c_i$. Then

$$f_i(x_{n+1}) \equiv p^n(c_i + b \cdot f_i'(x_n)) \pmod{p^{n+1}}.$$

So we require

$$c_i + \sum_{j=1}^{d} b_j \frac{\partial f_i}{\partial t_j}(x_n) \equiv 0 \pmod{p}.$$

It is clear that $x_n \equiv a \pmod{p}$ for all $n$ by construction. So we want

$$C + Ab \equiv 0 \pmod{p} \text{ where } C = (c_i)_{i=1}^{r}, b = (b_j)_{j=1}^{d}, A = \left(\frac{\partial f_i}{\partial t_j}(x_n)\right).$$

So we need, in $\mathbb{F}_p$,

$$\bar{A}\bar{b} = -\bar{c}.$$

Also, $\bar{x_n} = a$ in $\mathbb{F}_p$ and so $f_i(x_n) = f_i(a)$ in $\mathbb{F}_p$, $f_i'(x_n) = f_i'(a)$ in $\mathbb{F}_p$. So

$$\text{rank}\bar{A} = \text{rank}\left(\frac{\partial f_i}{\partial t_j}(a) \bmod p\right) \geq r.$$

So we do have a solution $b$ such that $\bar{A}\bar{b} = -\bar{c}$. This completes the construction of $x_{n+1}$.

15. $p = 2$, $x = \frac{10}{3}, y = \frac{1}{3}$ is a solution in $\mathbb{Z}_2$. $p = 41$, since 2 is a quadratic residue in 41, so we have a solution in $\mathbb{Z}_{41}$ (pick $y = 0$ and use Hensel's lemma).

When $p \neq 2, 41$ if $\left(\frac{2}{p}\right) = 1$, pick $y = 0$. $f(x) = x^2 - 2$, which is separable. $f(x) \equiv 0 \pmod{p}$ has a solution. Apply Hensel's lemma. We have a solution for $x$.

If $\left(\frac{-41}{p}\right) = 1$, let $x = 0$. $f(y) = -2 - 82y^2$. Then

$$f(a) \equiv 0 \pmod{p} \iff 1 \equiv -41a^2 \pmod{p}.$$

But $\left(\frac{-41^{-1}}{p}\right) = \left(\frac{-41}{p}\right) = 1$. So we have $a$ such that $1 \equiv -41a^2 \pmod{p}$. Then apply Hensel's lemma.

Finally, if $\left(\frac{2}{p}\right) = \left(\frac{-41}{p}\right) = -1$, then $\left(\frac{-82}{p}\right) = 1$. Let $x = 1$, and $f(y) = -1 - 82y^2$. Now apply the same argument as in the previous case. Hence we have solution in $\mathbb{Z}_p$ for each $p$.

It has no solution in $\mathbb{Z}$. If so, we have

$$\langle x - \sqrt{82}y\rangle\langle x + \sqrt{82}y\rangle = 2.$$

Let $K = \mathbb{Q}(\sqrt{82})$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{82}]$. 2 ramifies in $K$ and so

$$\langle x - \sqrt{82}y\rangle = \langle x + \sqrt{82}y\rangle \Rightarrow x - \sqrt{82}y = \pm u^n(x + \sqrt{82}y)$$

where $u = \sqrt{82} + 9$ is a fundamental unit. Then $(x - \sqrt{82}y)^2 = \pm u^n(x^2 - 82y^2) = \pm 2u^n$. Since $u > 0$ so we have the + sign. Take the norm, we have

$$|u|^n = 1 \Rightarrow n \text{ is even because } |u| = -1.$$

So $n = 2m$ and so $(x - \sqrt{82}y)^2 = 2u^{2m}$. So

$$x - \sqrt{82}y = \pm\sqrt{2}u^m = \pm\sqrt{2}(\sqrt{82} + 9)^m.$$

The constant term has $z\sqrt{2}$ on RHS for some $z \in \mathbb{Z}$, but LHS does not have. This gives a contradiction and so we have no solution in $\mathbb{Z}$.

# 22 Dedekind Domain

In this section, we will study the Dedekind domain and the ring of integers of a number field via local method. (Study the local behavior, e.g. for each prime ideal) Some results may probably given in the previous sections, but the method will be different.

**Definition 22.1.** *A* **Dedekind domain** *is a ring $R$ such that*

*(i) $R$ is an integral domain.*

*(ii) $R$ is Noetherian.*

*(iii) $R$ is integrally closed (in its field of fraction).*

*(iv) Every non-zero prime ideal is maximal.*

**Example 22.2.** *Every PID is a Dedekind domain (every UFD is integrally clsoed).*

**Lemma 22.3.** *Let $R$ be a Noetherian ring, and $I \subset R$ a non-zero ideal. Then $I$ contains a product of non-zero prime ideals.*

*Proof.* Suppose not. Let $S$ be the set of such ideals and take $I$ to be the maximal of them. Indeed, the maximal exists because $R$ is Noetherian. Then $I$ itself cannot be a prime and so there exists $x, y \in R$ such that $xy \in I$ but $x, y \notin I$.

Now the ideal $xR+I$ strictly contains $I$ and so by maximality of $I$, $xR+I$ must contain a product of prime ideals. Let $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subset xR + I$. Similarly, we have $\mathfrak{q}_1 \cdots \mathfrak{q}_l \subset yR + I$. Therefore, we have

$$\prod_{i=1}^{k} \mathfrak{p}_i \prod_{j=1}^{l} \mathfrak{q}_j \subset (xR + I)(yR + I).$$

But $xy \in I$ and so $(xR + I)(yR + I) \subset I$, which gives a contradiction as $I$ contains a product of prime ideals. □

**Theorem 22.4.** *Let $R$ be a Dedekind domain. Then every non-zero ideal $I \subset R$ can be written uniquely as a product of prime ideals.*

**Lemma 22.5.** *Let $R$ be an integral domain, integrally closed, and $I \subset R$ a non-zero finitely generated ideal. Let $K = Frac(R)$ and $x \in K$. If $xI \subset I$, then $x \in R$.*

*Proof.* Let $I = \langle c_1, \ldots, c_k \rangle$ for some $c_i \in R$. Then $xc_j = \sum_{i=1}^{k} a_{ij} c_i$ for some $a_{ij} \in R$. Then we have

$$(xI - A) \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

where $A_{ij} = a_{ij}$. So $xI - A$ has zero determinant, which is a monic polynomial (of degree $n$) with coefficients in $a_{ij} \in R$. So $x$ is integral and hence $x \in R$. □

**Theorem 22.6.** *$R$ is a DVR if and only if $R$ is a Dedekind domain with exactly one non-zero prime ideal.*

*Proof.* Suppose firstly that $R$ is a DVR. Then it is a PID and so it is a Dedekind domain with exactly one non-zero (maximal) prime ideal.

Conversely, let $R$ be a Dedekind domain with the unique maximal ideal $m$. We claim that $m$ is principal. Let $0 \neq x \in m$, then Lemma 22.3 implies that $\langle x \rangle$ contains a product of prime ideals and the only one is $m$, so

$$m^n \subset \langle x \rangle.$$

for some $n$ large enough, and in fact we shall take the least such $n$. So $m^{n-1} \not\subset \langle x \rangle$. Pick $y \in m^{n-1} \backslash \langle x \rangle$, and let $\pi = \frac{x}{y}$. We will show $\pi$ generates $m$. We have $ym \subset m^n \subset \langle x \rangle$, and so $\pi^{-1}m \subset R$ because for any $\alpha \in m$, we have some $r \in R$ such that $y\alpha \in xr$. If $\pi^{-1}m \subset m$, then by previous lemma, we have $\pi^{-1} \in R$, which then implies that $y \in \langle x \rangle$, contradicting the assumption. Hence $\pi^{-1}m \not\subset m$, but it is an integral ideal and $m$ is maximal. Hence $\pi^{-1}m = R$, and so $m = \langle \pi \rangle$.

Now let $I$ be a non-zero ideal. Since $\pi^{-1} \supset R$ and so we have a chain

$$I \subset \pi^{-1}I \subset \pi^{-2}I \subset \dots$$

If $\pi^{-n}I = \pi^{-(n+1)}I$, then $\pi^{-1}I \subset I$ and so $pi^{-1} \in R$ by previous lemma, which is a contradiction. Then, there exists a maximal $n$ such that $\pi^{-n}I \subset R$, otherwise the chain condition does not hold. If $\pi^{-n}I \subset m = \langle \pi \rangle$, then $\pi^{-(n+1)}I \subset R$, contradicting maximality. Hence $\pi^{-n}I = R$ and so $I = \langle \pi^n \rangle$. □

We will now give a sketch that Theorem 22.4 is in fact equivalent to Theorem 22.6

*Proof.* Assume Theorem 22.4, then one direction of Theorem 22.6 is clear. For the converse, this time we can write any non-zero ideal $I$ as a power of the maximal ideal $m$. And by uniqueness, $m^{n+1} \neq m^n$ for all $n$. Pick $x \in m^n \backslash m^{n+1}$, then $\langle x \rangle$ is also a power of $m$. But by the choice of $x$, it has to be $m^n$. Therefore, $\langle x \rangle = I$ and so $R$ is a PID and hence a DVR.

Now if we assume Theorem 22.6, then for each prime ideal $\mathfrak{p}$, let $S = R \backslash \mathfrak{p}$, and let $I, J \subset R$ be ideals. We firstly quote some properties of localisation. (Details can be found later in the Commutative Algebra Section.) Let $R$ be a local Dedekind domain (with exactly one maximal ideal)

(1) $S^{-1}R$ is a local Dedekind domain with maximal ideal $S^{-1}\mathfrak{p}$.

(2) If $I \subsetneq \mathfrak{p}$, then $S^{-1}I = S^{-1}R$.

(3) $I = J \iff S^{-1}I = S^{-1}J$ for all $\mathfrak{p}$ (as $S$ depends on $\mathfrak{p}$).

So now $S^{-1}R$ is a local Dedekind domain, by Theorem 22.6 it is a DVR. Let $I$ be a non-zero ideal in $R$. Lemma 22.3 implies that we have $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k} \subset I$. Then $S^{-1}I = R$ if $\mathfrak{p} \neq \mathfrak{p}_i$ for any $i$, by property (2). If $\mathfrak{p} = \mathfrak{p}_i$ for some $i$, then $S^{-1}I = S^{-1}\mathfrak{p}_i^{\beta_i}$ for some $\beta_i \leq \alpha_i$. Then

$$I = \prod_{i=1}^{k} \mathfrak{p}_i^{\beta_i}.$$

For uniqueness, if

$$I = \prod_{i=1}^{k} \mathfrak{p}_i^{\alpha_i} = \prod_{j=1}^{l} \mathfrak{q}_j^{\beta_j}.$$

Then localise at each $\mathfrak{p}_i$ and $\mathfrak{q}_j$, we will find (after reordering) that $k = l, \mathfrak{p}_i = \mathfrak{q}_i$ for each $i$ and $\alpha_i = \beta_i$. □

Let $K$ be a field. Recall that the trace (resp. norm) of an element $x \in L/K$ is the trace (resp. determinant) of the $K-$linear map

$$x : L \longmapsto L \text{ via } x(y) = xy.$$

In the case where the extension $L/K$ is separable, $[L : K] = n$, we have

$$Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x), N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x),$$

where $\sigma_i$ are the embeddings $L \hookrightarrow \bar{K}$.

**Lemma 22.7.** *If $L/K$ is separable, then the trace form $L \times L \longmapsto K$, $(x, y) \mapsto Tr_{L/K}(xy)$ is non-degenerate.*

*Proof.* Since $L/K$ is separable, so $L = K(x)$ for some $x \in L$. So we have a $K$-basis $1, x, x^2, \ldots, x^{n-1}$, with $\sigma_1(x), \ldots, \sigma_n(x)$ are all different. Then

$$\det\left(Tr_{L/K}(x^{i+j})\right) = \det\left(\sigma_i(x^j)\right)^2 \neq 0.$$

□

**Remark 22.8.** *(1) More generally, it can be shown that for any finite dimensional commutative $K$-algebra $R$, the trace form $R \times R \longmapsto K$ is non-degenerate if and only if $R \cong L_1 \times L_2 \cdots \times L_k$ with each $L_i/K$ a separable field extension. In fact, $\Leftarrow$ follows easily from Lemma 22.7 as the determinant of a direct sum of linear map is just the product of them.*

*(2) Suppose $0 \neq x \in R$ with $x^m = 0$ for some $m$. Then $(xy)^m = 0$ for all $y \in R$, so $Tr_{L/K}(xy) = 0$ for all $y \in R$, so the trace form is degenerate.*

**Theorem 22.9.** *Let $\mathcal{O}_K$ be a Dedekind domain, $K = Frac(\mathcal{O}_K)$, $L/K$ a finite extension. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in $L$. Then $\mathcal{O}_L$ is a Dedekind domain. In particular, the ring of integer for any number field $K$ is a Dedekind domain.*

*Proof.* We will prove this for the case when $L/K$ is separable. For $L/K$ inseparable, see e.g. Janusz, Chapter I, section 6. $\mathcal{O}_L$ is a subring of a field $L$, so it must be an integral domain. By definition, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in $L$ and so it must be integrally closed. We shall check it is Noetherian and every non-zero prime ideal is maximal.

Let $x_1, \ldots, x_n$ be a $K$-basis for $L$, and multiply them by suitable elements, we have $x_i \in \mathcal{O}_K$. Let $y_1, \ldots, y_n$ be the dual basis so that $Tr_{L/K}(x_i y_j) = \delta_{ij}$. Given $z \in \mathcal{O}_L$, write $z = \sum_{i=1}^{n} \lambda_i y_i$ where $\lambda_i \in K$. Then

$$\lambda_j = Tr_{L/K}(z x_j) \in \mathcal{O}_K.$$

Then $\mathcal{O}_K \subset \mathcal{O}_K y_1 + \cdots + \mathcal{O}_L y_n$. Since $\mathcal{O}_K$ is Noetherian, so $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$ module (any submodule of Noetherian finitely generated module is again finitely generated). Thus, $\mathcal{O}_L$ is Noetherian.

Let $\mathcal{P}$ be a non-zero prime ideal in $\mathcal{O}_L$ and let $\mathfrak{p} = \mathcal{P} \bigcap \mathcal{O}_K$. Then $\mathfrak{p}$ is a prime ideal. It is also non-zero, for example, take any $0 \neq x \in \mathcal{P}$. Then $N_{L/K}(x) \neq 0$, and $N_{L/K} \in \mathcal{P} \bigcap \mathcal{O}_K = \mathfrak{p}$. Now $\mathfrak{p}$ is maximal since $\mathcal{O}_K$ is a Dedekind domain, so $k = \mathcal{O}_K/\mathfrak{p}$ is a field. $k \hookrightarrow \mathcal{O}_L/\mathcal{P}$. Since $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$ module and so $\mathcal{O}_L/\mathcal{P}$ is a finite dimensional $k$-algebra.

On the other hand, $\mathcal{P}$ is prime so $\mathcal{O}_L/\mathcal{P}$ is an integral domain. Now consider for each $x$, the map induced by multiplication by $x$. It is a linear map and injective. By rank-nullity, it is also surjective, and so it is bijective. So $x^{-1}$ exists for each $x$ and so it is a field. Therefore, $\mathcal{P}$ is maximal. □

**Definition 22.10.** *Let $\Delta(x_1, \ldots, x_n)$ denote the discriminant of volume spanned by $x_1, \ldots, x_n$. In other words, $\Delta(x_1, \ldots, x_n) = \det(Tr_{L/K}(x_i x_j))$. Note that if $y_i = \sum_{j=1}^n a_{ij} x_j$ for some $a_{ij} \in K$, let $A = (a_{ij})$, then $\Delta(x_1, \ldots, x_n) = (\det A)^2 \Delta(x_1, \ldots, x_n)$.*

For $\mathfrak{p} \in \mathcal{O}_K$, write $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$. Note that $\mathfrak{p} \subset \mathcal{P} \bigcap \mathcal{O}_K$, and since $\mathfrak{p}$ is maximal, so $\mathfrak{p} = \mathcal{P} \bigcap \mathcal{O}_K$.

**Definition 22.11.** *With the notations above, $e_i$ is called the* **ramification index**. *We say that $\mathfrak{p}$ ramifies in $L$ if $e_i > 1$ for some $i$.*

**Theorem 22.12.** *With the same setting of $L/K$ as in Theorem 22.9, $L/K$ separable, $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$, write $k = \mathcal{O}_k/\mathfrak{p}$. Then*

*(i) If $\mathfrak{p}$ ramifies in $L$ then $\mathfrak{p} \big| \Delta(x_1, \ldots, x_n)$, for every $x_1, \ldots, x_n \in K$.*

*(ii) If $\mathfrak{p}$ is unramified in $L$, then there exists $x_1, \ldots, x_n$ such that $\mathfrak{p} \nmid \Delta(x_1, \ldots, x_n)$.*

We will need several Lemmas and Theorems before we prove this.

**Definition 22.13.** *Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$. The* **residue degree** *$f$ is defined as $f = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/\mathfrak{p}]$.*

**Theorem 22.14.** *Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$ and $[L : K] = n$. Then*

$$\sum_{i=1}^{k} e_i f_i = n.$$

*Proof.* Let $k = \mathcal{O}_K/\mathfrak{p}$. By Chinese Remainder Theorem, we have

$$\mathcal{O}_L/\mathfrak{p} \cong \mathcal{O}_L/\mathcal{P}_1^{e_1} \times \cdots \times \mathcal{O}_L/\mathcal{P}_k^{e_k}.$$

We count the dimensions as $k$-vector spaces. Any $x \in \mathcal{P}^{\alpha_i} \backslash \mathcal{P}^{\alpha_{i+1}}$ generates the quotient $\mathcal{P}^{\alpha_i}/\mathcal{P}^{\alpha_{i+1}}$ as an $\mathcal{O}_L$-module. Because, for any $z \in \mathcal{P}^{\alpha_i} \backslash \mathcal{P}^{\alpha_{i+1}}$, $\langle zx^{-1} \rangle$ has no factor in $\mathcal{P}$, so let $zx^{-1} \equiv \zeta \pmod{\mathcal{P}}$. Then $zx^{-1} - \zeta \in \mathcal{P}$ and so $z - x\zeta \in \mathcal{P}^{\alpha+1}$. Thus, $z = x\zeta$ in $\mathcal{P}^{\alpha}/\mathcal{P}^{\alpha+1}$.

Thus, $dim_{\mathcal{O}_L/\mathcal{P}_i}(\mathcal{P}_i^a/\mathcal{P}_i^{a+1}) = 1$, and so $dim_k(\mathcal{P}_i^a/\mathcal{P}_i^{a+1}) = f_i$. Then we conclude that

$$dim_k\left(\frac{\mathcal{O}_L}{\mathcal{P}_i^{e_i}}\right) = dim_k\left(\frac{\mathcal{O}_L}{\mathcal{P}_i}\right) + dim_k\left(\frac{\mathcal{P}_i}{\mathcal{P}_i^2}\right) + \cdots = e_i f_i.$$

Therefore,

$$dim_k\left(\frac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L}\right) = \sum_{i=1}^{r} e_i f_i.$$

So we need to check that $dim_k(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = [L : K]$.

If $\mathcal{O}_K$ is principal ideal domain, then $\mathcal{O}_L$ is free $\mathcal{O}_K$-module of finite rank. Then by structure theorem of finitely generated module over principal ideal domain, we have

$$\mathcal{O}_L \cong \mathcal{O}_K^n, \text{ and so } \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \left(\frac{\mathcal{O}_K}{\mathfrak{p}\mathcal{O}_K}\right)^n \cong k^n.$$

But $[\mathcal{O}_L : \mathcal{O}_K] = [L : K]$ so

$$n = [L : K] = dim_k\left(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L\right).$$

In general, $S = \mathcal{O}_K/\mathfrak{p}$ is multiplicatively closed, then we consider the ring $S^{-1}\mathcal{O}_L$ and $S^{-1}\mathcal{O}_K$. Notice that, by basic knowledge of Commutative Algebra we have

(1) $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in $L$.

(2) $S^{-1}\mathfrak{p}$ and $S^{-1}\mathfrak{p}_i$ are primes in $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$ respectively.

(3) $e_i$ and $f_i$ are unchanged under localisation.

So the result follows by the previous case because $S^{-1}\mathcal{O}_K$ is principal ideal domain. □

**Lemma 22.15.** *Let $R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ and $k = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Define $\psi$(resp $\theta$) be the quotient maps from $\mathcal{O}_L$ (resp $\mathcal{O}_K$) to $R$ (resp $k$). Then we have a commutative diagram from $\mathcal{O}_L$ to $k$:*

$$\theta \circ Tr_{L/K} = Tr_{R/k} \circ \psi.$$

*Proof.* Assume $\mathcal{O}_K$ is principal ideal domain. Then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, generated by $x_1, \ldots, x_n$. Then $x_1, \ldots, x_n$ give a basis for $L$ and $\bar{x}_1, \ldots, \bar{x}_n$ give a $k$ basis for $R$.

Let $z \in \mathcal{O}_L$, and

$$zx_i = \sum_{j=1}^{n} a_{ij}x_j, a_{ij} \in \mathcal{O}_K.$$

Let $A$ be the matrix with entries $a_{ij}$. Then

$$\overline{Tr_{L/K}(z)} = \overline{Tr(A)} = Tr(\bar{A}) = Tr_{R/k}(\bar{z}).$$

Then the result follows.

In general, let $S = \mathcal{O}_K/\mathfrak{p}$ and $S^{-1}\mathcal{O}_L$ is free $S^{-1}\mathcal{O}_K$-module, and proceed as above. □

Now we prove Theorem 21.22,

*Proof.* Let

$$\mathfrak{p} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

Then by Chinese Remainder Theorem, we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathcal{P}_1^{e_1} \times \cdots \times \mathcal{O}_L/\mathcal{P}_r^{e_r}.$$

Then $\mathfrak{p}$ ramifies if and only if $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ has nilpotent elements.

(i) If $\mathfrak{p}$ ramifies in $L$ then we have nilpotent elements. So the trace degenerates and so $\Delta(\bar{x}_1, \ldots, \bar{x}_n) = 0$ for all $x_1, \ldots, x_n \in \mathcal{O}_L$. Hence, by previous lemma we have

$$\Delta(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}.$$

(ii) If $\mathfrak{p}$ is unramified, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a product of fields and each is an extension of $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, and the trace form on each of them is non-degenerate (because finite field extension is separable). Then the trace is non-degenerate on $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Hence $\Delta(\bar{x}_1, \ldots, \bar{x}_n) \neq 0$ for some $x_1, \ldots, x_n$ and so

$$\Delta(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}.$$

□

**Definition 22.16.** *The discriminant is the ideal $\mathfrak{d}_{L/K} \subset \mathcal{O}_K$ generated by $\Delta(x_1, \ldots, x_n)$ for all choices of $x_1, \ldots, x_n \in \mathcal{O}_L$.*

**Corollary 22.17.** *$\mathfrak{p}$ ramifies in $L$ if and only if $\mathfrak{p} \big| \mathfrak{d}_{L/K}$ if and only if $\mathfrak{d}_{L/K} \subset \mathfrak{p}$.*

*Proof.* Use Theorem 21.22 and the definition. □

**Remark 22.18.** *If $\mathcal{O}_K$ is principal ideal domain, we have $\mathfrak{d}_{L/K} = \langle \Delta(x_1, \ldots, x_n) \rangle$ where $x_1, \ldots, x_n$ is a basis for $\mathcal{O}_L$ as $\mathcal{O}_K$-module.*

**Lemma 22.19.** *If $L/K$ is Galois, then $G = Gal(L/K)$ acts transitively on the prime above $\mathfrak{p}$.*

*Proof.* Suppose not, so without loss of generality, we cannot have $\sigma \in G$ such that $\sigma(\mathcal{P}_i) = \mathcal{P}_j$. By Chinese Remainder Theorem, pick $x \in \mathcal{O}_L$ such that

$$x \equiv 1 \pmod{\sigma(\mathcal{P}_i)\ \sigma \in G}, x \equiv 0 \pmod{\mathcal{P}_j}.$$

This is possible as $\sigma(\mathcal{P}_i) \neq \mathcal{P}_j$. Then

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathcal{P}_j \cap \mathcal{O}_K = \mathfrak{p} \subset \mathcal{P}_i.$$

But $\mathcal{P}_i$ is prime, so we have $\sigma(x) \in \mathcal{P}_i$ for some $\sigma \in G$. This is the same as saying $x \in \sigma^{-1}(\mathcal{P}_i)$. Then

$$x \equiv 0 \pmod{\sigma^{-1}(\mathcal{P}_i)}$$

which is a contradiction to the choice of $x$ we had at the beginning. □

**Corollary 22.20.** *If $L/K$ is Galois, $\mathfrak{p}$ is a prime in $\mathcal{O}_K$. Then $e_1 = e_2 = \cdots = e_r = e$, $f_1 = f_2 = \cdots = f_r = f$ and so $[L : K] = ref$ where $r$ is the number of prime above $\mathfrak{p}$.*

*Proof.* Use the previous lemma and unique factorisation (note that for any $\sigma \in G$, $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$). □

**Definition 22.21.** *For each prime $\mathcal{P}$ above $\mathfrak{p}$, define*

$$G_{\mathcal{P}} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}.$$

## 22.1 Exercises

1. Let $R$ be a Dedekind domain containing non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$. By first treating the case $R$ is a principal ideal domain and then localising, show that $\mathfrak{a} \supset \mathfrak{b}$ if and only if $\mathfrak{a} \big| \mathfrak{b}$.

2. Prove the Chinese Remainder Theorem in the following form: Let $R$ be a ring (commutative with a 1) and let $I_1, \ldots, I_n \subset R$ be the ideals with $I_i + I_j = R$ for all $i \neq j$. Then

$$\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i = I$$

and

$$R/I \cong R/I_1 \oplus \cdots \oplus R/I_n.$$

3. Let $R$ be a Dedekind domain. Use the theorem on unique factorisation into prime ideals, and the previous exercise, to show that

   (i) If $R$ has only finitely many prime ideals then it is a principal ideal domain.

   (ii) Use(i) to prove that: If $I \subset R$ is an ideal then $I = \langle a, b \rangle$ for some $a, b \in R$.

In particular, this gives another solution of Exercise 13, question 12.

4. Let $L/K$ be a Galois extension of number fields and $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p}$ be a prime of $K$ and $\mathfrak{P}$ be a prime of $L$ dividing $\mathfrak{p}$. The **decomposition field** $E$ is the subfield of $L$ fixed by the decomposition group $G_{\mathfrak{P}} \subset G$. Let $\mathfrak{p}_E = \mathfrak{P} \cap E$. Assume that $E/K$ is also Galois. Show that $\mathfrak{p}$ splits completely in $E$ whereas $\mathfrak{P}$ is the unique prime of $L$ above $\mathfrak{p}_E$.

## 22.2 Hint and Solutions

1. If $R$ is principal ideal domain, then $\mathfrak{a} = \langle \alpha \rangle, \mathfrak{b} = \langle \beta \rangle$. Then it is clear that

$$\langle \alpha \rangle \supset \langle \beta \rangle \iff \alpha \big| \beta \iff \mathfrak{a} \big| \mathfrak{b}.$$

For general $R$, we write

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}, \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{f_i}, e_i, f_i \geq 0, \max(e_i, f_i) > 0.$$

Then localsise at each $\mathfrak{p}_i$, we know $R_{\mathfrak{p}_i}$ is DVR. Also,

$$\mathfrak{a} \supset \mathfrak{b} \iff \mathfrak{a} R_{\mathfrak{p}_i} \supset \mathfrak{b} R_{\mathfrak{p}_i}.$$

We know in $R_{\mathfrak{p}_i}$, $\mathfrak{a} R_{\mathfrak{p}_i} \supset \mathfrak{b} R_{\mathfrak{p}_i}$ if and only if $\mathfrak{a} R_{\mathfrak{p}_i} \big| \mathfrak{b} R_{\mathfrak{p}_i}$.

But

$$\mathfrak{a} R_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}, \mathfrak{b} R_{\mathfrak{p}_i} = \mathfrak{p}_i^{f_i} R_{\mathfrak{p}_i}.$$

From above we know $v_{\mathfrak{p}_i}(\mathfrak{a}) \leq v_{\mathfrak{p}_i}(\mathfrak{b})$ for all $i$ and hence $\mathfrak{a} \big| \mathfrak{b}$.

2. We check the case $n = 2$. We have $I_1 + I_2 = R$ and so we have $a \in I_1, b \in I_2$ such that $a + b = 1$. If $x \in I_1 \cap I_2$, then

$$x = x \cdot 1 = x(a + b) = xa + xb \in I_1 + I_2.$$

So $I_1 \cap I_2 \subset I_1 I_2$. Conversely, it is clear that $I_1 I_2 \subset I_1 \cap I_2$. So we have $I_1 \cap I_2 = I_1 I_2$.

Now apply induction on $n$. Suppose it is true for $n - 1$. Let $J = \bigcap_{i=1}^{n-1} I_i$. Then $J = \prod_{i=1}^{n-1} I_i$. Also, for each $i$ we have $a_i \in I_i, b_i \in I_n$ such that $a_i + b_i = 1$. Then

$$1 = \prod_{i=1}^{n-1} (a_i + b_i) \in I_j + I_n \ \forall j.$$

So $J + I_n = R$. Now apply the case when $n = 2$.

Define the map

$$f : R \longmapsto R/I_1 \oplus \cdots \oplus R/I_n$$

by

$$f(x) = (x_1, \ldots, x_n), \text{ where } x_i \equiv x \pmod{I_i}.$$

It is a homomorphism. If $x$ is in $\ker f$, then $x \equiv 0 \pmod{I_i}$ for all $i$ and so $x \in I_i \forall i$, which is equivalent to $x \in \bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$. Thus the kernel is $I$.

Let $M_j = \frac{I}{I_j}$, which is just the product of $I_i$'s without $I_j$. Then from above we can see that $M_j + I_j = R$. Then we have $a_j + b_j = 1$ for some $a_j \in M_j, b_j \in I_j$. Given $(x_1, \ldots, x_n)$, let $x = \sum_{j=1}^{n} x_j a_j$. Now fix $k$. Then for each $i \neq k$, we know $a_i \equiv 0 \pmod{I_j}$ because $I_i \big| M_i$. Also, $b_k \in I_k$ so $a_k \equiv 1 \pmod{I_k}$. Therefore, $x \equiv x_k \pmod{I_k}$. So the map is also surjective.

3. (i) Let $\mathfrak{p}_i$ be a prime ideal. Let $a \in \mathfrak{p}\backslash\mathfrak{p}^2$. Then by Chinese Remainder Theorem, since there are only finitely many primes, we can pick $x$ with

$$x \equiv a \pmod{\mathfrak{p}_i}, x \equiv 1 \pmod{\mathfrak{p}_j}\ \forall j \neq i.$$

Then consider $\langle x \rangle$. By construction, we must have $\langle x \rangle = \mathfrak{p}_i$. So each prime ideal is principal and so $R$ is a principal ideal domain.

(ii) Let $I$ be any ideal in $R$ and pick $a \in I$. There are only finitely many prime ideals containing $a$ because there are only finitely many prime ideals dividing $\langle a \rangle$. Thus, the quotient $R/\langle a \rangle$ has only finitely many prime ideals and so it is a principal ideal domain. (The quotient of a Dedekind domain is again Dedekind domain.) In particular, $I/\langle a \rangle$ is principal.

Let $I/\langle a \rangle$ be generated by $b$ and we may assume $b$ is lifted in $R$. Then it is clear that $I = \langle a, b \rangle$.

4. $\mathrm{Gal}(L/E) = [L : E]$. But $\mathrm{Gal}(L/E)$ is the decomposition group $G_{\mathfrak{P}}$. So by orbit-stabliser theorem, we have

$$|\mathrm{Gal}(L/E)| = \text{ number of primes above } \mathfrak{p}_E \cdot |G_{\mathfrak{P}}|.$$

So the number of primes is 1 and so $\mathfrak{P}$ is the unique prime above $\mathfrak{p}_E$.

Set $[L : K] = ref, [L : E] = e'f'r' = e'f'$ because $r' = 1$. Now consider the action of $G$ on $\mathfrak{P}$. We then have, by orbit-stabliser,

$$|G| = r|G_{\mathfrak{P}}| = re'f'.$$

But $|G| = [L : K] = ref$ so $ef = e'f'$. Further, $e' \big| e$ and $f' \big| f$ so $e = e', f = f'$. Thus, $e(\mathfrak{p}_E/\mathfrak{p}) = e/e' = 1$ and similarly $f' = 1$. Therefore, $\mathfrak{p}$ splits completely in $E$.

# 23 Extension of Complete Fields

In this section, we are going to discuss the extension of fields, especially the extension of $p$-adic fields.

## 23.1 Unique Extension

**Definition 23.1.** *Let $V$ be a vector space over a field $K$. A norm on $V$ is a function $\|\cdot\|$ from $V$ to $\mathbb{R}$ satisfying*

*(i)* $\|x\| \geq 0$, *equality holds if and only if* $x = 0$.

*(ii)* $\|\lambda x\| = |\lambda|\|x\|,\ \forall \lambda \in K, x \in V$.

*(iii)* $\|v + w\| \leq \|v\| + \|w\|,\ \forall v, w \in V$.

*For example, $V = K^d$ and $\|v\|_{sup} = \max_{1\leq i\leq d} |v_i|$.*

**Theorem 23.2.** *Let $(K, |\cdot|)$ be complete field with respect to the absolute value $|\cdot|$. If $dim_K V < \infty$ then any two norms on $V$ are equivalent and $V$ is complete with respect to any of the norms.*

*Proof.* We will prove that any norm on $V$ is equivalent to the supremum norm. If $d = 1$, then

$$\|v\|_\infty = |v|, \|\lambda v\| = |\lambda|\|v\|.$$

Let $\lambda = \frac{1}{v}$ because $d = 1$. Then

$$\|1\| = \frac{1}{|v|}\|v\| \text{ and so } \|v\| = |v|\|1\| = \|v\|_\infty \|1\|.$$

Use induction on $d$. Suppose this is true for $d-1$. For the case of $d$, l et $e_1, \ldots, e_d$ be the standard basis. Then

$$\|x\| = \|\sum_{i=1}^{d} x_i^{e_i}\| \leq \left(\sum_{i=1}^{d} \|e_i\|\right) \max_{1\leq i\leq d} |x_i| = c \cdot \|x\|_\infty.$$

Let $S = \{x \in V : \|x\|_\infty = 1\}$. Note that the above equation shows that $\|\cdot\|$ is continuous as a function on $S$ to $\mathbb{R}_{\geq 0}$ with respect to the supremum norm.

Now we claim that there exists $\epsilon > 0$ such that $\|x\| > \epsilon,\ \forall x \in S$. Suppose not, then we have a sequence $x^{(n)}$ in $S$ such that $\|x^{(n)}\| \to 0$ as $n \to 0$. But $\|x^{(n)}\| \to 0$ means that $x^{(n)} \to 0$ and for some $i$, $1 \leq i \leq d$ we have

$$\|x^{(n)}\|_\infty = |x_i^{(n)}| \text{ for infinitely many } n$$

because $d$ is finite. Without loss of generality, let this $i$ be $d$.

Passing to subsequence if necessary, we assume that

$$1 = \|x^{(n)}\|_\infty = \left|x_d^{(n)}\right|,\ \forall n.$$

Replacing $x^{(n)}$ by $\frac{1}{x_d^{(n)}} x^{(n)}$ for all $n$, we can assume that $x_d^{(n)} = 1$ for all $n$. So we have

$$x^{(n)} = y^{(n)} + e_d, y^{(n)} \in \langle e_1, \ldots, e_{d-1}\rangle.$$

The original $x^{(n)}$ is cauchy, and since we only divide those by $x_d^{(n)}$, and we know $\|x_d^{(n)}\|$ was 1, so the new $x^{(n)}$ is also cauchy. Thus, $y^{(n)}$ is cauchy.

By induction, we know $\|\cdot\|$ is complete on $V^{d-1}$, so $y^{(n)}$ converges to $y$ with respect to $\|\cdot\|$ for some $y \in \langle e_1, \ldots, e_{d-1}\rangle$. But

$$y^{(n)} = x^{(n)} - e_d \to -e_d \text{ as } x^{(n)} \to 0.$$

Therefore, we conclude $y = -e_d$ which is a contradiction. Thus we have proved the claim.

Now let $0 \neq x \in V$, then $\|x\|_\infty = |x_i|$ for some $1 \leq i \leq d$. Then

$$\left\| \frac{x}{x_i} \right\|_\infty = 1$$

and so it is in $S$. Therefore, by previous claim

$$\left\| \frac{x}{x_i} \right\| > \epsilon \text{ and so } \|x\| > \epsilon |x_i| = \|x\|_\infty \epsilon.$$

Thus, we conclude that $\|\cdot\|$ is equivalent to the supremum norm. Since $K$ is complete, so $V$ is complete with respect to the supremum norm. □

**Theorem 23.3.** *Let $K$ be a complete field with respect to an absolute value $|\cdot|$. Let $L$ be a finite extension of $K$. If $|\cdot|_1, |\cdot|_2$ are absolute values on $L$, extending $|\cdot|$ on $K$, then*

*(i)* $|\cdot|_1 = |\cdot|_2$.

*(ii) $L$ is complete with respect to any of them.*

*In particular, the theorem tells that the extension of absolute value of finite extension is unique.*

*Proof.* Note that $|\cdot|_1, |\cdot|_2$ are norms on $L$, so they are equivalent by the previous theorem. Then they must introduce the same topology. Recall from Lemma 21.18 that two absolute values introduce the same topology if and only if they are equivalent as absolute values. Then

$$|x|_2 = |x|_1^\alpha \text{ for some } \alpha > 0, \ \forall x \in L.$$

Take $x \in K$ and since $|\cdot|_1, |\cdot|_2$ both extend $|\cdot|$ in $K$, we have

$$|x|_2 = |x| = |x|_1.$$

This shows that $\alpha = 1$ and so $|\cdot|_2 = |\cdot|_1$. Completeness also follows from the previous theorem.

Alternatively, by equivalence of norms, we have

$$a|x|_1 \leq |x|_2 \leq b|x|_1.$$

Replace $x$ by $x^n$ and take $n \to \infty$, we also conclude that $a = b = 1$. □

## 23.2 Extension of Number Fields

**Theorem 23.4.** *Let $K$ be a complete field with respect to a discrete valuation $v$. Let $L$ be a finite extension of $K$. Then*

*(i)* $|\cdot|_K$ *extends uniquely to* $|\cdot|_L$ *on* $L$.

*(ii) $L$ is complete with respect to* $|\cdot|_L$.

*(iii) The valuation ring of $L$ is the integral closure of $\mathcal{O}_K$ in $L$.*

*Proof.* $\mathcal{O}_K = \{x \in K : |x|_K \leq 1\}$ is a DVR, let $\pi$ be the maximal ideal of $\mathcal{O}_K$. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in $L$. Then we know by previous section that $\mathcal{O}_L$ is a Dedekind domain and so

$$\pi\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

Then $|\cdot|_{\mathcal{P}_1}, \ldots, |\cdot|_{\mathcal{P}_r}$ are non-equivalent absolute values on $L$. It is clear that they are not equivalent because

$$\mathcal{P}_i + \mathcal{P}_j = \mathcal{O}_L$$

and so there exist $x \in \mathcal{P}_i, y \in \mathcal{P}_j$ such that $x + y = 1$. So $|x|_{\mathcal{P}_i} < 1$ but $|x|_{\mathcal{P}_j} = 1$, and so they are not equivalent by using Lemma 21.18. Also if $\pi\mathcal{O}_L = \mathcal{O}_L$ then $\pi\mathcal{O}_K = \mathcal{O}_K$ which is a contradiction.

Now, by previous theorem, the extension of absolute value is unique and so we conclude that $r = 1$, i.e.

$$\pi\mathcal{O}_L = \mathcal{P}^e.$$

This proves (i). The second part also follows from the previous theorem.

For the third part. Let $\mathcal{P}$ be a non-zero prime ideal in $\mathcal{O}_L$ and so $\mathcal{P} \cap \mathcal{O}_K$ is a non-zero prime ideal. Since there is only one prime ideal in $\mathcal{O}_K$ we have

$$\mathcal{P} \cap \mathcal{O}_K = \pi\mathcal{O}_K.$$

So by the above factorisation we have

$$\pi\mathcal{O}_L = \mathcal{P}^e\mathcal{O}_L.$$

This shows that there is only one prime ideal in $\mathcal{O}_L$. In particular, $\mathcal{O}_L$ is a DVR (it is a Dedekind domain with one prime ideal, use Theorem 22.6). Now the field of fraction of $\mathcal{O}_L$ is $L$ and by Lemma 21.34(ii) we know that $\mathcal{O}_L$ is the valuation ring of $L$. □

**Corollary 23.5.** *$|\cdot|_p$ on $\mathbb{Q}_p$ extends uniquely to an absolute value on $\overline{\mathbb{Q}}_p$.*

*Proof.* Let $x \in \overline{\mathbb{Q}}_p$ and $x \in K$ for some finite extension $K$ of $\overline{\mathbb{Q}}_p$. Then by previous theorem, since $|\cdot|_p$ is discrete, so by previous theorem, $|\cdot|_K$ extends $|\cdot|_p$ uniquely on $K$. Now $x \in K_1, K_2$, two different extensions of $\mathbb{Q}_p$, then we can set $|x|_{K_1} = |x|_{K_2} = |x|_{K_1 \cap K_2}$. So the absolute norm extends uniquely to $|\cdot|$ on $\overline{\mathbb{Q}}_p$. □

**Remark 23.6.** *(i) $|p|_p = \frac{1}{p}$. So $|\sqrt[n]{p}|_p = \frac{1}{\sqrt[n]{p}}$ and so $(\bar{\mathbb{Q}}_p, |\cdot|)$ is not discrete.*

*(ii) In fact, $\bar{\mathbb{Q}}_p$ is not complete with respect to $|\cdot|$, and its completion is $\mathbb{C}_p$ and $\mathbb{C}_p$ is algebraic closed.*

*(iii) Let $K/\mathbb{Q}_p$ be finite Galois extension of degree $n$. Let $|\cdot|$ be the absolute value of $K$ extending $|\cdot|_p \in \mathbb{Q}_p$. If $\sigma \in Gal(K/\mathbb{Q}_p)$, then $x \mapsto |\sigma(x)|$ is also an absolute value (not hard to check). Then by unique extension of absolute value we have*

$$|\sigma(x)| = |x| \ \forall \sigma \in G.$$

*Then*

$$|x|^n = \left|\prod_{\sigma \in G} \sigma(x)\right| = |N_{K/\mathbb{Q}_p}(x)|_p$$

*and so*

$$|x| = |N_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}}.$$

**Theorem 23.7.** *Let $\mathcal{O}_K$ be a Dedekind domain and $K$ be its field of fraction. Let $L/K$ be a finite extension and $\mathcal{O}_L$ of $\mathcal{O}_K$ in $L$. Write*

$$\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

*Then the absolute value on $L$ extending $|\cdot|_\mathfrak{p}$ are (up to equivalence) $|\cdot|_{\mathcal{P}_1}, \ldots, |\cdot|_{\mathcal{P}_r}$.*

*Proof.* For $x \in K$, $v_{\mathcal{P}_i}(x) = e_i v_\mathfrak{p}(x)$. So $|\cdot|_{\mathcal{P}_i}$ is equivalent to an absolute value extending $|\cdot|_\mathfrak{p}$. Now let $|\cdot|$ be any absolute value on $L$ extending $|\cdot|_\mathfrak{p}$ on $K$. Then

$$\mathcal{O}_K \subset \{x \in L : |x| \leq 1\} = A, \text{ where } A \text{ is the valuation ring of } L.$$

Recall from Remark 21.31(iv) that the valuation ring is integrally closed and so $\mathcal{O}_L \subset A$.

Let $\mathcal{P} = \{x \in \mathcal{O}_L : |x| < 1\}$. We can check that $\mathcal{P} \subset \mathcal{O}_L$ is a prime ideal. If $x, y \in \mathcal{P}$, so is $x + y$ by ultrametric law. If $x \in \mathcal{P}$ and $r \in \mathcal{O}_L$ then $rx \in \mathcal{P}$ because $\mathcal{O}_L \subset A$. If $xy \in \mathcal{P}$, then $|x||y| < 1$ and hence $|x| < 1$ or $|y| < 1$.

Let $S = \mathcal{O}_L \backslash \mathcal{P}$, then $S^{-1}\mathcal{O}_L$ is a DVR. In fact

$$S^{-1}\mathcal{O}_L = \{x \in L : |x|_\mathcal{P} \leq 1\}$$

because the only prime is $\mathcal{P}$. Pick $\pi \in \mathcal{P} \backslash \mathcal{P}^2$, then every $x \neq 0$ is $x = \pi^r u$, $|u|_\mathcal{P} = 1$, $r = \mathbb{Z}$.

To show $|\cdot| \sim |\cdot|_\mathcal{P}$, it suffices to show that (i) $|\pi| < 1$, (ii) $|u| = 1$ because if so then

$$|x| = |\pi^r u| = |\pi^r| < 1 \iff r \geq 1 \iff |\pi^r|_\mathcal{P} < 1 \iff |x|_\mathcal{P} < 1.$$

Now $|\pi| < 1$ because $\pi \in \mathcal{P}$ and since $\mathcal{P} = \{x \in \mathcal{O}_L : |x| < 1\}$ so $|\pi| < 1$. Also, $|u|_\mathcal{P} = 1$ and so $u \in S^{-1}\mathcal{O}_L$. Then write $u = \frac{r}{s}$ where $r \in \mathcal{O}_L$, $s \in S$ and so $s \notin \mathcal{P}$, so $|s| \geq 1$. So $|u| \leq |r| \leq 1$.

Similarly, $|u^{-1}|_\mathcal{P} = 1$ so repeat the above we have $|u| \geq 1$. So $|u| = 1$. Therefore, $|\cdot|$ extends $|\cdot|_\mathfrak{p}$ and so $|\cdot|_\mathcal{P}$ extends $|\cdot|_\mathfrak{p}$ (up to equivalence). □

**Corollary 23.8.** *The non-archmedian places of a number field $K$ are the $|\cdot|_\mathcal{P}$ for $\mathcal{P}$ prime ideal of the ring of integers.*

*Proof.* By Theorem 21.20 (Ostrowski), the non-archmedian places on $\mathbb{Q}$ are $|\cdot|_p$ for some prime $p$ and then apply the previous theorem. □

**Definition 23.9.** *For $\mathfrak{p} \subset \mathcal{O}_K$, define*

$$|x|_\mathfrak{p} = (N_\mathfrak{p})^{-v_\mathfrak{p}(x)}, N_\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|.$$

*If $\sigma$ is a real embedding then write*

$$|x|_\sigma = |\sigma(x)|.$$

*If $\sigma$ is a complex embedding we write*

$$|x|_\sigma = |\sigma(x)|^2.$$

**Definition 23.10.** *Let $L/K$ be an extension of number fields. Let $v$ be a place of $K$ and $w$ be a place of $L$. We say $w \big| v$ if $|\cdot|_w$ extends $|\cdot|_v$.*

**Definition 23.11.** *Let $L/K$ be an extension of number fields with ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ and $\mathcal{P} \big| \mathfrak{p}$ a prime of $\mathcal{O}_L$.*

*We write $K_\mathfrak{p}$ to be the completion of $K$ with respect to $|\cdot|_\mathfrak{p}$. Similarly, $L_\mathcal{P}$ means the completion of $L$ with respect to $|\cdot|_\mathcal{P}$.*

**Lemma 23.12.** *The natural map from $L \otimes_K K_\mathfrak{p} \longmapsto L_\mathcal{P}$ is surjective and $[L_\mathcal{P} : K_\mathfrak{p}] \leq [L : K]$.*

*Proof.* Let $M = LK_\mathfrak{p}$, the composition of $L$ and $K_\mathfrak{p}$ inside $L_\mathcal{P}$. Then $[M : K_\mathfrak{p}] \leq [L : K]$ and so $[M : K_\mathfrak{p}]$ is finite. $K_\mathfrak{p}$ is complete, so $M$ is complete by Theorem 23.3. Now $L \subset M \subset L_\mathcal{P}$ and $M$ is complete with respect to $|\cdot|_\mathcal{P}$, so $M = L_\mathcal{P}$. Further,

$$LK_\mathfrak{p} = L_\mathcal{P} \Rightarrow L \otimes_K K_\mathfrak{p} \longmapsto L_\mathcal{P} \text{ is surjective .}$$

□

**Theorem 23.13.** *Let $K$ be a number field and $L$ a finite extension of $K$.*

$$L \otimes_K K_\mathfrak{p} \cong \oplus_{\mathcal{P}\big|\mathfrak{p}} L_\mathcal{P}.$$

*Proof.* Write $L = K(\alpha)$. Let $f$ be the minimal polynomial of $\alpha$ over $K$. $f$ is irreducible and hence separable. So over $K_\mathfrak{p}[x]$ we have

$$f(x) = f_1(x) \cdots f_r(x), f_i(x) \in K_\mathfrak{p}[x].$$

$L = K[x]/\langle f(x)\rangle$. Then, by Chinese Remainder Theorem.

$$L \otimes_K K_\mathfrak{p} = K_\mathfrak{p}[x]/\langle f(x)\rangle \cong K_\mathfrak{p}[x]/\langle f_1(x)\rangle \oplus \cdots \oplus K_\mathfrak{p}[x]/\langle f_r(x)\rangle.$$

This is an isomorphism of $K_\mathfrak{p}$ algebra.

Let $L_i = K_\mathfrak{p}[x]/\langle f_i(x)\rangle$. This contains both $L$ and $K_\mathfrak{p}$. Indeed,

$$L = K[x]/\langle f(x)\rangle \hookrightarrow K_\mathfrak{p}[x]/\langle f_i(x)\rangle = L_i.$$

Note that $K$ is dense in $K_\mathfrak{p}$, and so $L$ is dense in $L_i$ with respect to $|\cdot|_\mathfrak{p}$.

We claim that each $L_i$ is isomorphic to $L_\mathcal{P}$ for some $\mathcal{P}\big|\mathfrak{p}$. $L_i$ is finite extension of $K_\mathfrak{p}$ and $L_i$ is complete with respect to, say $|\cdot|_i$. Then by Theorem 23.7, the restriction of $|\cdot|_i$ on $L$ is equivalent to $|\cdot|_\mathcal{P}$. Then $L$ is dense in $L_i$ with respect to $|\cdot|_\mathcal{P}$ and $L_i$ is complete with respect to $|\cdot|_i$ and so $L_i$ is also complete with respect to $|\cdot|_\mathcal{P}$. Then $L_i \cong L_\mathcal{P}$.

Then we check that each $\mathcal{P}\big|\mathfrak{p}$ appears at most once. Suppose $L_i \cong L_j$ for some $i, j$. Then by definition of $L_i$ and $L_j$, we conclude $f_i = f_j$ and so $i = j$.

Finally, we check that each $\mathcal{P}\big|\mathfrak{p}$ appears at least once. Pick any $\mathcal{P}\big|\mathfrak{p}$. By previous lemma we know that $L_\mathcal{P} = K_\mathfrak{p}(\alpha)$ because $L_\mathcal{P} = LK_\mathfrak{p}$ (notice that this notation is a bit confusing: the composite field $LK_\mathfrak{p}$ is in the composite inside $L_\mathcal{P}$ for a given $\mathcal{P}$). Let $g(x)$ be the minimal polynomial of $\alpha \in L_\mathcal{P}$ over $K_\mathfrak{p}$. Then $g(x)$ is an irreducible factor of $f(x)$. So $g(x) = f_i(x)$ for some $i$ and hence each $\mathcal{P}$ does appear at least once. □

**Corollary 23.14.** *For $x \in L$,*

$$N_{L/K}(x) = \prod_{\mathcal{P}\big|\mathfrak{p}} N_{L\mathcal{P}/K_\mathfrak{p}}(x).$$

*Proof.* Let $B_1, \ldots, B_r$ be the bases for $L_{\mathcal{P}_1}, \ldots, L_{\mathcal{P}_r}$ respectively, as $K_\mathfrak{p}$ vector spaces. Then $B = \bigcup_{i\leq r} B_i$ is a basis for $L \otimes_K K_\mathfrak{p}$ as a $K_\mathfrak{p}$ vector space by using the previous theorem. But

$$\det \begin{pmatrix} A_1 & & \\ & \cdots & \\ & & A_r \end{pmatrix} = \prod_{i=1}^{r} \det(A_i).$$

Then $\det([\cdot x]_B) = \prod_{i=1}^r \det([\cdot x]_{B_i})$ and so

$$N_{L\otimes_K K_\mathfrak{p}/K_\mathfrak{p}}(x) = \prod_{i=1}^{r} N_{L_{\mathcal{P}_i}/K_\mathfrak{p}}(x)$$

and note that

$$N_{L\otimes_K K_\mathfrak{p}/K_\mathfrak{p}}(x) = N_{L/K}(x).$$

□

**Remark 23.15.** *A similar result of trace can be deduced in a similar way.*

**Example 23.16.** $K = \mathbb{Q}$, $L = \mathbb{Q}(i)]$, $f(x) = x^2 + 1 = (x + i)(x - i)$. *Then*

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \oplus_{\mathcal{P}\big|5} L_{\mathcal{P}}.$$

*Note that* $5 = (2 + i)(2 - i)$ *and so* $f(x)$ *must split in* $\mathbb{Q}_5$. *This shows that* $i$ *is in* $\mathbb{Q}_5$.

## 23.3 Application of Techmuller Map

Now let $L/K$ be extension of number fields, complete with respect to normalised discrete valuation $v_L$ and $v_K$, with valuation rings $\mathcal{O}_L$ and $\mathcal{O}_K$, uniformaliser $\pi_L, \pi_K$, residue fields $k$ and $k_L$ respectively.

Let $\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L$. Then we have for any $x \in K$,

$$ev_K(x) = v_L(x).$$

Define the residue degree $f = f(L/K) = [k_L : k]$.

**Proposition 23.17.** *Assume either*

*(i)* $L/K$ *is finite separable, or*

*(ii)* $f_{L/K} < \infty$.

*Then* $[L : K] = ef$.

*Proof.* (i) The only prime above $\pi_K$ is $\pi_L$, and then use Theorem 22.14.

(ii) If we look back into the proof of Theorem 22.14, we only need to prove that $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. As before, we still have

$$dim_k(\mathcal{O}_L/\pi_K \mathcal{O}_L) = ef < \infty.$$

Let $x_1, \ldots, x_n$ be the coset representatives for a $k$ basis of $\mathcal{O}_L/\pi_K \mathcal{O}_L$. Given $y \in \mathcal{O}_L$, write

$$\begin{aligned} y &= \sum_{i=0}^{\infty} \left( \sum_{j=1}^{n} a_{ij} x_j \right) \pi_k^i \\ &= \sum_{j=1}^{n} \left( \sum_{i=1}^{\infty} a_{ij} \pi_k^i \right) x_j \\ &= \sum_{j=1}^{n} b_j x_j \text{ where } b_j \in \mathcal{O}_K \text{ as it converges.} \end{aligned}$$

So $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. □

**Proposition 23.18.** *Let* $L/K$ *be a Galois extension of number fields. Let* $\mathfrak{p}$ *be a prime of* $K$ *and* $\mathcal{P}\big|\mathfrak{p}$ *be a prime of* $L$. *Then* $L_{\mathcal{P}}/K_{\mathfrak{p}}$ *is Galois. Further, the restriction map*

$$Gal(L_{\mathcal{P}}/K_{\mathfrak{p}}) \longmapsto Gal(L/K)$$

*is injective and has image the decomposition group* $G_{\mathcal{P}}$.

*Proof.* Let $L = K[x]/\langle f(x)\rangle$. $L/K$ is Galois, so $L$ is the splitting field $f \in K[x]$. Then $L_{\mathcal{P}}$ is the splitting field of $f'$ over $K_{\mathfrak{p}}[x]$, for some $f'\big|f$, using the proof of Theorem 23.13. Hence $L_{\mathcal{P}}/K_{\mathfrak{p}}$ is Galois.

Now take $\sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$, we have $\sigma(L) \subset L$ because $L/K$ is Galois. By Lemma 23.12, we know $L_{\mathcal{P}} = LK_{\mathfrak{p}}$. Consider an element $\sigma$ which fixes $L$ and $K_{\mathfrak{p}}$. Then it must fix $L_{\mathcal{P}}$ and so the restriction is injective.

Finally, let $\sigma$ be an element in the image of the restriction map. Then by unique extension of absolute value, we have

$$|\sigma(x)|_{\mathcal{P}} = |x|_{\mathcal{P}} \ \forall x \in L.$$

So $\sigma\mathcal{P} = \mathcal{P}$ (otherwise it is a different absolute value). So the image lies in the decomposition group. But

$$|\mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})| = e(\mathcal{P}/\mathfrak{p})f(\mathcal{P}/\mathfrak{p}) = |G_{\mathcal{P}}|.$$

So the image is $G_{\mathcal{P}}$. □

Now let $[K : \mathbb{Q}_p] < \infty$, with valuation ring $\mathcal{O}_K$, normalised discrete valuation $v_K$, with uniformliser $\pi$ and residue field $k$. Let $e = e(K/\mathbb{Q}_p) = v_K(p)$.

**Lemma 23.19.** *If $r > \frac{e}{p-1}$, then*

$$(\pi^r\mathcal{O}_K, +) \cong (1 + \pi^r\mathcal{O}_K, *)$$

*via*

$$x \mapsto \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}.$$

*Proof.* $v_K(n!) = ev_p(n!) \leq e\frac{n-1}{p-1}$ (see Exercises). Then

$$v_K\left(\frac{x^n}{n!}\right) \geq nr - e\frac{n-1}{p-1} = r + (n-1)\left(r - \frac{e}{p-1}\right).$$

But $r - \frac{e}{p-1} > 0$, so $v_K\left(\frac{x^n}{n!}\right) \geq r \ \forall n \geq 1$ and it tends to infinity as $n \to \infty$. So the series expansion of $\exp(x)$ converges.

Similarly, consider the map

$$1 + \pi^r\mathcal{O}_K \longmapsto \pi^r\mathcal{O}_K$$

via

$$1 + x \mapsto \sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n} = \log(1+x).$$

It also converges. Then recall the identities in $\mathbb{Q}[[x, y]]$ that

$$\exp(x+y) = \exp(x)\exp(y), \log(\exp(x)) = \exp(\log(x)) = x.$$

The result follows. □

**Corollary 23.20.** *Assume $k$ is finite, then $\mathcal{O}_K^*$ has a subgroup of finite index, isomorphic to $(\mathcal{O}_K, +)$.*

*Proof.* We have

$$\mathcal{O}_K^* \supset 1 + \pi\mathcal{O}_K \supset 1 + \pi^2\mathcal{O}_K \supset \cdots \supset 1 + \pi^r\mathcal{O}_K \cong (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +).$$

Then consider the map

$$\mathcal{O}_K^* \longmapsto k^* \text{ via } x \mapsto x \pmod{\pi}$$

and

$$1+\pi^i\mathcal{O}_K \longmapsto (k,+) \text{ via } 1+\pi^i x \mapsto x \pmod{\pi}, i \geq 1.$$

These introduce the isomorphisms

$$\frac{\mathcal{O}_K^*}{1+\pi\mathcal{O}_K} \cong k^*, \frac{1+\pi^i\mathcal{O}_K}{1+\pi^{i+1}\mathcal{O}_K} \cong (k,+), i \geq 1.$$

Therefore, the index is finite as $k$ is finite. □

**Theorem 23.21.** *If $p > 2$, we have*

$$\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p.$$

*When $p = 2$, we have*

$$\mathbb{Z}_2^* \cong \{\pm 1\} \times \mathbb{Z}_2.$$

*Proof.* When $p > 2$, consider the map

$$\mathbb{Z}_p^* \longmapsto (\mathbb{Z}/p\mathbb{Z})^* \times (1+p\mathbb{Z}_p)$$

via

$$x \mapsto \left(\bar{x}, \frac{x}{[\bar{x}]}\right)$$

where $[\cdot]$ is the Techmuller map. It is clear that $\frac{x}{[\bar{x}]} \in 1+p\mathbb{Z}_p$, because $[\bar{x}] \equiv x \pmod{p}$. This is a homomorphism.

If $x \equiv 1 \pmod{p}$ and $\frac{x}{[\bar{x}]} = 1$, then $x = [\bar{x}]$, and so $x = [1] = 1$. So the kernel is trivial. It is also surjective. For instance, given $(a, b)$ in the image. Let $x = [a]b$ then it is clear that $\bar{x} = \overline{[a]} = a$, because $\bar{b} = 1$ and

$$\frac{x}{[\bar{x}]} = \frac{[a]b}{[a]} = b.$$

So we have

$$(1+p\mathbb{Z}_p, *) \cong (p\mathbb{Z}_p, +)$$

because $p > 2, e = 1$ so we only need $r = 1$ in Lemma 23.19. Therefore,

$$\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p.$$

Now let $p = 2$. It is clear that every $x \in \mathbb{Z}_2^*$ must be 1 mod 2. So in fact,

$$\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2.$$

Then it is clear that

$$(1+2\mathbb{Z}_2)/(1+4\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$$

via

$$1+2x \mapsto \bar{x}.$$

Now $p = 2$, so it is enough to take $r = 2$ such that

$$(1+4\mathbb{Z}_2, *) \cong (4\mathbb{Z}_2, +) \cong (\mathbb{Z}_2, +).$$

Therefore,

$$\mathbb{Z}_2^* \cong \{\pm 1\} \times \mathbb{Z}_2.$$

□

**Corollary 23.22.** *When $p > 2$,*

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

*When $p = 2$,*

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

*Proof.* Use the previous theorem. □

## 23.4 Exercises

1. Let $L/K$ be finite extensions of $\mathbb{Q}_p$. Let $|\cdot|_K$ and $|\cdot|_L$ be the normalised absolute values and put $n = [L : K]$.

   (i) Show that $|x|_L = |x|_K^n$ for all $x \in K$.

   (ii) Deduce that $|N_{L/K}(x)|_K = |x|_L$ for all $x \in L$.

   For the next three exercises, let $K$ be a field complete with respect to a discrete valuation, with valuation ring $\mathcal{O}$ and residue field $k$.

2. Let $f(X)$ be a polynomial in $\mathcal{O}[X]$ and suppose $\bar{f}(X) = \phi_1(X)\phi_2(X)$ where $\phi_1, \phi_2 \in k[X]$ are coprime. Show that there exist polynomials $f_1, f_2 \in \mathcal{O}[X]$ with $f(X) = f_1(X)f_2(X)$, $\deg f_1 = \deg \phi_1$, and $\bar{f}_i = \phi_i$ for $i = 1, 2$.

3. Let $f(X)$ be a monic irreducible polynomial in $K[X]$. Show that if $f(0) \in \mathcal{O}$ then $f \in \mathcal{O}[X]$.

4. Let $L/K$ be a finite extension and write $|\cdot|_K$ for the absolute value on $K$.

   (i) Let $x \in L$. Show that if $N_{L/K}(x) \in \mathcal{O}$ then $N_{L/K}(1 + x) \in \mathcal{O}$.

   (ii) Prove directly that $|x|_L = |N_{L/K}(x)|_K$ is an absolute value on $L$.

5. Prove that $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_2, \mathbb{Q}_5, \ldots$ are pairwise non-isomoprhic as fields (no topology).

6. (i) Recall the description of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ and hence find the condition for $p$ to split in the quadratic field $\mathbb{Q}(\sqrt{d})$ for $d$ a square-free integer. (Treat the case $p = 2$ and $p > 2$ separately. You may wish to compare your answer with that obtained by computing the ring of integers and then using Dedekind's criterion.)

   (ii) Let $K = \mathbb{Q}(\sqrt[3]{d})$ for $d$ a cube-free integer. Show that 3 splits in $K/\mathbb{Q}$ (i.e. there is more than one prime of $K$ above 3) if and only if $d \equiv \pm 1 \pmod 9$.

7. Let $L/K$ be an extension of number fields.

   (i) Let $v$ be a place of $K$. Show that

   $$|N_{L/K}(x)|_v = \prod_{w \mid v} |x|_w \quad \text{for all } x \in L.$$

   (ii) Deduce the product formula: If $x \in K^*$ then

   $$\prod_v |x|_v = 1 \text{ where } v \text{ runs over all places of } K.$$

8. Let $U_r = 1 + p^r\mathbb{Z}_p$. Show that for $r$ sufficiently large $U_r/U_{r+m} \cong \mathbb{Z}/p^m\mathbb{Z}$. Use this to prove that if $p$ is odd then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic. What happens when $p = 2$?

9. Let $K$ be a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. Show that if $e(K/\mathbb{Q}_p) < p - 1$ then $K$ contains exactly $q - 1$ roots of unity.

## 23.5 Hint and Solutions

1. (i) Let $\mathcal{P}$ and $\mathfrak{P}$ be the primes of $K$ and $L$ respectively. Then $|x|_L = N_{L/\mathbb{Q}_p}(\mathfrak{P})^{-v_L(x)}$, $|x|_K = N_{K/\mathbb{Q}_p}(\mathcal{P})^{-v_K(x)}$. If $x \in K$, then $v_L(x) = ev_K(x)$. Also, $N_{L/\mathbb{Q}_p}(\mathfrak{P}) = N_{K/\mathbb{Q}_p}(\mathcal{P})^f$, where $f$ is the residue degree. So

$$|x|_L = N_{K/\mathbb{Q}_p}(\mathcal{P})^{-efv_K(x)} = |x|_K^{ef}.$$

But $[L : K] = ef = n$, so $|x|_L = |x|_K^n$.

(ii) $x \mapsto |\sigma(x)|$ is an absolute value for any $\sigma \in \mathrm{Aut}_K(L)$ so $|x|_L = |\sigma(x)|_L$ by unique extension of absolute value. Then

$$|x|_L^n = \left|\prod_{i=1}^n \sigma_i(x)\right|_L = |N_{L/K}(x)|_L = |N_{L/K}(x)|_K^n$$

by (i). So $|x|_L = |N_{L/K}(x)|_K$.

2. We may assume that $\phi_1$ is monic (otherwise we just multiply this by the inverse of the leading coefficient). Let $\mathfrak{m} = \langle\pi\rangle$. We will construct the polynomials $g_n, h_n$ as follows. Let $g_1 = \phi_1, h_1 = \phi_2$. Having picked $g_n, h_n$, let

$$g_{n+1} = g_n + p\pi^n, h_{n+1} = h_n + q\pi^n$$

and we will construct $g_n, h_n$ such that they satisfy the conditions: $g_n$ is monic, $\deg g_n = \deg \phi_1$, $\deg h_n \leq \deg f - \deg \phi_1$, and $f - g_n h_n \equiv 0 \pmod{\pi^n}$. So induction on $n$, we have

$$f = g_n h_n + c\pi^n.$$

Thus,

$$f - g_{n+1}h_{n+1} = f - g_n h_n - qg_n\pi^n - ph_n\pi^n - pq\pi^{2n} \equiv \pi^n(c - qg_n - ph_n) \pmod{\pi^{n+1}}.$$

We have $g_{n+1} \equiv g_n \pmod{\pi^n}$, $h_{n+1} \equiv h_n \pmod{\pi^n}$. Also,

$$g_n \equiv \phi_1 \pmod{\pi}, h_n \equiv \phi_2 \pmod{\pi}.$$

Since $\phi_1, \phi_2$ are coprime, so there exist $\alpha, \beta$ such that

$$\alpha g_n + \beta h_n \equiv 1 \pmod{\pi} \Rightarrow \alpha g_n c + \beta h_n c \equiv c \pmod{\pi}.$$

$g_n$ is monic so apply division algorithm we have $\beta c = g_n r + p$ where $\deg p < \deg g_n$ and so $p$ is picked by this condition. Define $q$ by the following: $q = h_n r + c\alpha$ and replace all coefficients of multiple of $\pi$ by 0.

Now

$$c - qg_n - ph_n \equiv c - c\alpha g_n - c\beta h_n \equiv 0 \pmod{\pi}$$

and hence

$$f - g_{n+1}h_{n+1} \equiv 0 \pmod{\pi^{n+1}}.$$

Also, it is clear that $\deg p < \deg g_n$ so $g_{n+1} = g_n + \pi^n p$ is monic and has degree $\deg g_n = \deg \phi_1$.

It remains to check that $\deg h_{n+1} \leq \deg f - \deg \phi_1$. Suppose not, so $\deg h_{n+1} > \deg f - \deg \phi_1$. Now $h_{n+1} = h_n + q\pi^n$ and $\deg h_n \leq \deg f - \deg \phi_1$ and so $\deg q = \deg h_{n+1} > \deg f - \deg \phi_1$. Also, $c = f - g_n h_n$ so by induction $\deg c \leq \deg f$.

Now $\deg g_n = \deg \phi_1$, so $\deg(g_n q + h_n p) > \deg f$. Also,

$$f - g_{n+1}h_{n+1} = \pi^n(c - g_n q - h_n p) + \pi^{n+1}t$$

where $t$ is a polynomial. We know $\deg h_n p \leq \deg f - \deg \phi_1 + \deg p < \deg f$ and we know $\deg c \leq \deg f$. Also, $\deg g_n q > \deg f$ so the polynomial $\pi^n(c - g_n q - h_n p)$ has degree larger than $f$. This shows that $f - g_{n+1}h_{n+1} - \pi^{n+1}t$ has degree larger than $\deg f$ so the leading coefficient is divisible by $\pi^{n+1}$. But the leading coefficient is $\pi^n$ times the leading coefficient of $q$, which in turn implies that the leading coefficient of $q$ is divisible by $\pi$, contradicting the way we pick $q$. Thus, $\deg h_{n+1} \leq \deg f - \deg \phi_1$.

Now we have a sequence $g_n, h_n$ such that they satisfy the above conditions and

$$g_{n+1} \equiv g_n \pmod{\pi^n}, h_{n+1} \equiv h_n \pmod{\pi^n}$$

and

$$f - g_n h_n \equiv 0 \pmod{\pi^n}.$$

Taking the limit $g = \lim_{n\to\infty} g_n$ and $h = \lim_{n\to\infty} h_n$, we have $f = gh$. Further, $\deg g = \deg g_n = \deg \phi_1$.

3. Suppose not and let $j$ be the largest number such that $a_j \notin \mathcal{O}$, $j \geq 1$. Each $x \in K$ can be written as $x = \pi^n u$, and we multiply the equation by $\pi^N$ to clear the denominators, say we have

$$\pi^N f = b_n x^n + \cdots + b_0.$$

But $\pi \big| b_0$ because $a_0 \in \mathcal{O}$ and $N \geq 1$ because we assume that some $a_i$ does not lie in $\mathcal{O}$. So we have

$$\pi^N f(x) \equiv x^j b_j + \cdots + x b_1 \pmod{\pi}.$$

Factorise this into two coprime factors and by the previous question, we know that $\pi^N f(X)$ is reducible. Hence $f(X)$ is reducible which is a contradiction.

4. (i)

$$N_{L/K}(1+x) = \prod_{i=1}^{n} \sigma_i(1+x) = \prod_{i=1}^{n}(1+\sigma_i(x))$$

which is the sum, with each term some coefficient of $f$ where $f$ is the minimal polynomial of $x$. Since $a_0 = \prod_{i=1}^n \sigma_i(x) = N_{L/K}(x) \in \mathcal{O}$, then by the previous question $f \in \mathcal{O}[X]$ and so all coefficients are in $\mathcal{O}$ and so is $N_{L/K}(1+x)$.

(ii) The only non-trivial part we need to check is the triangle inequality. We need to show that

$$|x+y|_L \leq |x|_L + |y|_L \iff |N_{L/K}(x+y)|_K \leq |N_{L/K}(x)|_K + |N_{L/K}(y)|_K.$$

This is equivalent of showing

$$|N_{L/K}(x)|_K |N_{L/K}(1+\frac{y}{x})|_K \leq |N_{L/K}(x)|_K \cdot |1 + N_{L/K}(y)|_K$$

and then

$$|N_{L/K}(1+\alpha)|_K \leq 1 + |N_{L/K}(\alpha)|_K \ \forall \alpha \in L.$$

We have two cases. Firstly assume $N_{L/K}(x) \in \mathcal{O}$. Then by (i) $N_{L/K}(1+\alpha) \in \mathcal{O}$ and so $|N_{L/K}(1+\alpha)|_K \leq 1$.

Now if $N_{L/K}(x) \notin \mathcal{O}$. So

$$\left|\prod_{i=1}^{n} \sigma_i(\alpha)\right|_K > 1$$

and so $|\sigma_i(\alpha)|_K > 1$ for some $i$ and so $\sigma_i(\alpha)$ is not in $\mathcal{O}_L$.
Now by definition, if one of $\sigma_i$ is in $\mathcal{O}_L$, then every conjugate will be in $\mathcal{O}_L$. So we conclude that $\sigma_i(\alpha) \notin \mathcal{O}_L$ for all $i$. So $|1 + \sigma_i(\alpha)|_K \leq \max(1, |\sigma_i(\alpha)|) \leq |\sigma_i(\alpha)|$. So in this case

$$|N_{L/K}(1+\alpha)|_K = \prod_{i=1}^{n} |1 + \sigma_i(\alpha)|_K \leq \prod_{i=1}^{n} |\sigma_i(\alpha)| = |N_{L/K}(\alpha)|_K.$$

Then in both cases, we have

$$|N_{L/K}(1+\alpha)|_K \leq 1 + |N_{L/K}(\alpha)|_K$$

and so the triangle inequality holds.

5. If $p > 2$, consider $f(X) = X^2 + p - 1$. It has no root in $\mathbb{R}$ but has root in $\mathbb{Q}_p$ by Hensel's lemma. For $p = 2$, consider $f(X) = X^3 + 3$. Then it has root in $\mathbb{Z}_2$ by Hensel's Lemma but no root in $\mathbb{R}$. This shows that

$$\mathbb{R} \ncong \mathbb{Q}_p.$$

If $p, q \neq 2$, pick $a \in \mathbb{Z} > 0$ such that

$$\left(\frac{a}{p}\right) = 1, \left(\frac{a}{q}\right) = -1.$$

Let $f(X) = X^2 - a$. It has roots in $\mathbb{Z}_p$ but no root in $\mathbb{Z}_q$. Hence

$$\mathbb{Q}_p \ncong \mathbb{Q}_p.$$

Finally, when $p = 2$, $q > 2$, let $f(X) = X^{q-1} + X + 1$. It has solution in $\mathbb{Z}_q$ but no root in $\mathbb{Z}_2$ ($x = q - 2$ is a solution modulo $q$).

6. We will use the theorem

$$L \otimes_K K_{\mathfrak{p}} = \oplus_{\mathcal{P}\big|_{\mathfrak{p}}} L_{\mathcal{P}}.$$

(i) By using the theorem (and refer to its proof), $p$ splits in $L = \mathbb{Q}(\sqrt{d})$ if and only if the minimal polynomial of $\sqrt{d}$ splits in $\mathbb{Q}_p$.
When $p > 2$, we know $d \in \mathbb{Z}_p^*$ is a square if and only if $d$ is a square mod $p$. Also, $f(X) = X^2 - d$ splits in $\mathbb{Q}_p$ if and only if $d$ is a square in $\mathbb{Z}_p^*$, if and only if $\left(\frac{d}{p}\right) = 1$.
When $p = 2$, we know $d \in \mathbb{Z}_p^*$ is a square if and only if $d \equiv 1 \pmod 8$. So $p$ splits if and only if $d \equiv 1 \pmod 8$.

(ii) Let $f(X) = X^3 - d$. 3 splits in $K/\mathbb{Q}$ if and only if $f(X)$ splits in $\mathbb{Z}_3[X]$. This is equivalent of saying $d$ is a cube in $\mathbb{Z}_3^*$, which is the same as $d \equiv \pm 1 \pmod 9$.

7. (i) This is clear when $v$ is archimedean. So we may assume $v$ is non-archimedean. Then we know $v$ is equivalent to the $\mathfrak{p}$-adic value for some prime $\mathfrak{p}$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the primes of $L$ above $\mathfrak{p}$ and we know each $w$ is equivalent to the $\mathcal{P}_i$-adic value for some $i$.
Now by question 1(ii), we know that

$$|N_{L_{\mathcal{P}_i}/K_{\mathfrak{p}}}(x)|_v = |x|_{\mathcal{P}_i}.$$

Thus, by using Corollary 23.14,

$$|N_{L/K}(x)|_v = \prod_{i=1}^{r} |N_{L_{\mathcal{P}_i}/K_{\mathfrak{p}}}(x)|_v = \prod_{i=1}^{r} |x|_{\mathcal{P}_i}.$$

(ii) The infinite place gives the product

$$\prod_{v \text{ archimedean}} |x|_v = N_{K/\mathbb{Q}}(x).$$

For the finite place, we have,

$$\prod_{v \text{ non-archimedean}} |x|_v = \prod_p \prod v|p|x|_v = \prod_p |N_{K/\mathbb{Q}}(x)|_p.$$

Then by the product formula in $\mathbb{Q}$ and write $\alpha = N_{K/\mathbb{Q}}(x)$, we have

$$\prod_v |x|_v = |\alpha|_\infty \prod_p |\alpha|_p = 1.$$

8. For $r > \frac{e(K/\mathbb{Q}_p)}{p-1}$, we have

$$(1 + p^r\mathbb{Z}_p, *) \cong (p^r\mathbb{Z}_p, +).$$

So we have

$$\frac{1 + p^r\mathbb{Z}_p}{1 + p^{m+r}\mathbb{Z}_p} \cong \frac{p^r\mathbb{Z}_p}{p^{m+r}\mathbb{Z}_p} \cong \mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}.$$

Now for $\mathbb{Z}_p$, $e = 1$ and if $p > 2$ then we can pick $r = 1$. We consider the map

$$\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p\mathbb{Z}_p, *)$$

via

$$x \mapsto \left(\bar{x}, \frac{x}{[\bar{x}]}\right).$$

Consider the image of $1 + p^n\mathbb{Z}_p$, if $x \in 1 + p^n\mathbb{Z}_p$ then $x \equiv 1 \pmod{p}$. So $x \mapsto (1, x)$, and so the image is $\{1\} \times (1 + p^n\mathbb{Z}_p, *)$. Now consider the reduction map

$$\mathbb{Z}_p^* \longmapsto \mathbb{Z}_p^*/1 + p^n\mathbb{Z}_p.$$

Then we have a corresponding reduction, by previous part, that

$$\frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \cong \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Thus, we have

$$\mathbb{Z}_p^*/1 + p^n\mathbb{Z}_p \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p^{n-1}\mathbb{Z}).$$

RHS is cyclic with order $p^{n-1}(p-1)$. We check that LHS is $(\mathbb{Z}/p^n\mathbb{Z})^*$.

Indeed we have an injection

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p)^* \hookrightarrow \frac{\mathbb{Z}_p^*}{1+p^n\mathbb{Z}_p}.$$

Surjectivity follows by counting cardinality. Hence we conclude that

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p^{n-1}\mathbb{Z}).$$

When $p = 2$, we need $r = 2$ and

$$\mathbb{Z}_2^* \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_p, *).$$

Then

$$\mathbb{Z}_2^*/1 + 2^n\mathbb{Z}_2 \cong \{\pm 1\} \times (\mathbb{Z}/2^{n-2}\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

9. $\frac{e}{p-1} < 1$ so we pick $r = 1$ and we have

$$(1 + \pi\mathcal{O}_K, *) \cong (\pi\mathcal{O}_K, +).$$

Define the map

$$\mathcal{O}*_K \longmapsto k^* \times (1 + \pi\mathcal{O}_K, +) \text{ by } x \mapsto \left(\bar{x}, \frac{x}{[\bar{x}]}\right).$$

It is an isomorphism by the same argument as Theorem 23.21. The roots of unity in $K$ lies in $\mathcal{O}_K^*$ and they have finite order. So it suffices to find the elements of finite order in $k^* \times (1 + \pi\mathcal{O}_K, +)$.

Now the only element in $(1 + \pi\mathcal{O}_K, +)$ with finite order is 1 and we have $q - 1$ elements in $k^*$ with finite order. So we have $q - 1$ of them.

# 24 Inverse Limit And Local Fields

In this section, we will explain what it means by Local Fields and briefly introduce the basic properties of inverse limit.

## 24.1 Inverse Limit

**Definition 24.1.** *Suppose $A_n (n \in \mathbb{N})$ are sets (groups or rings) and*

$$\pi_n : A_{n+1} \longmapsto A_n$$

*are homomorphisms. The inverse limit of $A_n$ is*

$$\varprojlim_n A_n = \{(x_n)_{n\geq 1} : x_n \in A_n \text{ and } \pi_n(x_{n+1}) = x_n \ \forall n\}.$$

**Example 24.2.** *(i)*

$$\varprojlim_n k[t]/\langle t^n\rangle = k[[t]]$$

*where the homomorphism is given by*

$$\pi_n : k[t]/\langle t^{n+1}\rangle \longmapsto k[t]/\langle t^n\rangle, f(t) \mapsto f(t) \ (mod\ t^n).$$

*(ii)*

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

*where the homomorphism is given by*

$$\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \longmapsto \mathbb{Z}/p^n\mathbb{Z}, \alpha \mapsto \alpha \ (mod\ p^n).$$

**Definition 24.3.** *We can index by a partially ordered set $I$ such that for all $i, j \in I, i \leq j$, there exists $k \in I$ such that $i \leq k, j \leq k$ and*

$$f_{ij} : A_j \longmapsto A_i \text{ whenever } i \leq j \text{ satisfying } f_{ik} = f_{ij} \circ f_{jk} \text{ if } i \leq j \leq k$$

*and*

$$f_{ii} = id.$$

*Then define the inverse limit*

$$\varprojlim_n A_n \subset \prod_{i\in I} A_i \ni (a_i)_{i\in I}$$

*by $f_{ij}(a_j) = a_i$ for all $i \leq j$.*

**Example 24.4.** *(i) Let $K$ be a perfect field. $\bar{K}$ be its algebraic closure. Then*

$$Gal(\bar{K}/K) = \varprojlim_{L/K \text{ finite Galois}} Gal(L/K)$$

*ordered by inclusion of fields $f_{ij} : L_j \longmapsto L_i$, the restriction map.*

*(ii)*

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

*ordered by divisibility.*

If $A_n$'s have a topology, then the inverse limit topology is the weakest topology such that the projection maps

$$\pi : \lim_{\leftarrow_n} A_n \longmapsto A_i$$

are continuous. For convention, all finite groups have the discrete topology. Then, for example, the inverse limit topology of $\mathbb{Z}_p$ has basis of open sets

$$\{a + p^n\mathbb{Z}_p : n \in \mathbb{N}, a \in \mathbb{Z}/p^n\mathbb{Z}\}.$$

**Lemma 24.5.** *Let $G$ be a topological group, then the followings are equivalent:*

*(i) $G$ is the inverse limit of finite groups.*

*(ii) $G$ is Hausdorff, compact and totally disconnected.*

*In particular, condition (ii) is called* **profinite**.

*Proof.* The proof is omitted. The idea of (ii) $\Rightarrow$ (i) is to show

$$G \longmapsto \varprojlim_{N \subset G, N \text{open normal}} G/N$$

is isomorphism. □

**Proposition 24.6.** *Let $(K, |\cdot|)$ be a non-archmedian, complete field with valuation ring $\mathcal{O}$. Let $0 \neq \pi \in K$ and $|\pi| < 1$. Then we have an isomorphism*

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/\pi^n\mathcal{O} \text{ via } x \mapsto x \ (mod\ \pi^n).$$

*Proof.* $K$ is complete, so $x + \mathcal{O}$ is complete for all $x$. Hence, $\mathcal{O}$ is complete. Conversely, if $\mathcal{O}$ is complete, then $x + \mathcal{O}$ is complete for all $x$ and hence $K$ is complete, because $x + \mathcal{O}$ is a closed subset of radius 1, so for any cauchy sequence in $K$, say $(x_n)_{n=1}^{\infty}$, when $n$ gets large, the difference will be small and so the remaining term will lie in some $x + \mathcal{O}$. Thus, $K$ is complete if and only if $\mathcal{O}$ is.

Now $\mathcal{O}$ is complete if and only if whenever $(x_n)_{n=1}^{\infty}$ is cauchy in $\mathcal{O}$, i.e. $|x_n - x_{n+1}| \to 0$ as $n \to \infty$, there exists $x \in \mathcal{O}$ such that $|x_n - x| \to 0$.

Let $v$ be the corresponding valuation to $|\cdot|$, normalised such that $v(\pi) = 1$. Then the map in the proposition is an isomorphism if and only if whenever $(x_n)_{n=1}^{\infty}$ is a sequence in $\mathcal{O}$ with $v(x_{n+1} - x_n) \geq n$ for all $n$, there exists $x \in \mathcal{O}$ such that $v(x_n - x) \geq n$ (injectivity is automatic so we only need surjectivity).

Passing to subsequence if necessary, we conclude that these two conditions are the equivalent. □

## 24.2 Local Fields

**Proposition 24.7.** *Let $(K, |\cdot|)$ be complete, non-archmedian field with valuation ring $\mathcal{O}$. Then the followings are equivalent:*

*(i) $K$ is locally compact.*

*(ii) $\mathcal{O}$ is compact.*

*(iii) The valuation is discrete and the residue field $k$ is finite.*

*In particular, the field $K$ satisfying any of these is called* **local field**.

*Proof.* (i) $\Rightarrow$ (ii): Let $A$ be a compact neighbourhood of 0. Then $x\mathcal{O} \subset A$ for some $0 \neq x \in K$, closed with radius $|x|$, centered at 0. So $x\mathcal{O}$ is compact (closed subset of compact set is compact) and so $\mathcal{O}$ is compact because $\mathcal{O} = x^{-1}(x\mathcal{O})$.

(ii) $\Rightarrow$ (i): $\mathcal{O}$ is compact implies $a + \mathcal{O}$ is compact for all $a \in K$ and is a neighourhood around $a$. So $K$ is locally compact.

(ii) $\Rightarrow$ (iii) Pick any $0 \neq x \in \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal. We have

$$\mathcal{O} = \bigcup_{y \in \mathcal{O}} (y + x\mathcal{O}).$$

But $y + x\mathcal{O}$ is open and $\mathcal{O}$ is compact by assumption. So we only need a finite cover. This shows that $|\mathcal{O}/x\mathcal{O}|$ is finite. But $k = \mathcal{O}/\mathfrak{m}$ and so $k$ is finite because $x \in m$.

Suppose the valuation is not discrete, then pick $x = x_1, x_2, \ldots$ in $\mathcal{O}$ such that

$$v(x_1) > v(x_2) \cdots (> 0).$$

This shows that

$$x_1\mathcal{O} \subsetneq x_2\mathcal{O} \subsetneq \cdots \subset \mathcal{O}$$

which implies $\mathcal{O}/x\mathcal{O}$ is not finite. This gives a contradiction.

(iii) $\Rightarrow$ (ii): Let $\pi$ be a uniformliser, then

$$\frac{\pi^i \mathcal{O}}{\pi^{i+1}\mathcal{O}} \cong \mathcal{O}/\pi\mathcal{O} = k$$

which is finite. So $\mathcal{O}/\pi^n\mathcal{O}$ is finite for all $n$.

Now $K$ is complete, so by proposition 24.6, we have

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/\pi^n\mathcal{O}$$

which is profinite. Then by Lemma 24.5, $\mathcal{O}$ is compact. □

**Theorem 24.8.** *Any local field is one of the followings:*

*(i)* $\mathbb{R}$ *or* $\mathbb{C}$.

*(ii) finite extension of* $\mathbb{Q}_p$.

*(iii)* $k((t))$ *where* $k$ *is a finite field.*

*Proof.* If $K$ is archmedian then $K = \mathbb{R}$ or $\mathbb{C}$. If $K$ is non-archmedian, then by previous theorem the valuation is discrete and $k$ is finite. If $\mathrm{Char}(K) = 0$, then $\mathbb{Q} \subset K$. By Theorem 21.20 (Ostrowski), the restriction of the absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$. Then $\mathbb{Q}_p \subset K$. Now $k$ is finite so $f = [k : \mathbb{F}_p] < \infty$ and so $[K : \mathbb{Q}_p] = ef < \infty$

If $\mathrm{Char}(K) > 0$ then apply Theorem 21.49. □

## 24.3 Exercises

1. Show that $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ where the product is over all primes $p$.

2. Show that $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ and $\mathrm{Gal}(\mathbb{Q}(\bigcup_{n\geq 1}\mu_n)/\mathbb{Q}) \cong \hat{\mathbb{Z}}^*$.

3. For an integer $M > 1$ define $\mathbb{Z}_M = \varprojlim \mathbb{Z}/M^n\mathbb{Z}$ with respect to the natural surjections $\mathbb{Z}/M^{n+1}\mathbb{Z} \mapsto \mathbb{Z}/M^n\mathbb{Z}$. Prove that $\mathbb{Z}_M \cong \prod_{p\big|M} \mathbb{Z}_p$. In particular, $\mathbb{Z}_M$ is an integral domain if and only if $M$ is a prime power, and $\mathbb{Z}_{p^k} \cong \mathbb{Z}_p$ for $k \geq 1$.

4. Give a direct proof that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is sequentially compact.

5 Let $G$ be a profinite group. Show that every open subgroup of $G$ has finite index and that every closed subgroup of finite index is open.

## 24.4 Hint and Solutions

1. By Chinese Remainder Theorem, we have

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

Define the map

$$f : \hat{\mathbb{Z}} \longmapsto \prod_p \mathbb{Z}_p \text{ by } f(a_1, a_2, \ldots) = (b_1, b_2, \ldots)$$

where each element in the inverse limit is represented by $(a_1, a_2, \ldots)$, $a_i \in A_i$, $\pi_{ij}(a_j) = a_i$ and $b_i$ is a sequence obtained by $(a_1^{(1)}, a_2^{(2)}, \ldots)$ mod $p_i^j$, where $p_i$ is the $i^{\text{th}}$ prime.

So the map defined above is homomorphism (as modulo arithmetic is) and is bijective by Chinese Remainder Theorem.

2. $L/\mathbb{F}_q$ is finite Galois, $L = \mathbb{F}_{q^n}$ and $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. So

$$\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Then,

$$\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

So

$$\mathrm{Gal}(\mathbb{Q}(\bigcup_{n\geq 1}\mu_n)/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^* = \hat{\mathbb{Z}}^*.$$

3 $\mathbb{Z}_M = \varprojlim \mathbb{Z}/M^n\mathbb{Z}$. Let $M = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. Then

$$\mathbb{Z}/M^n\mathbb{Z} \cong \mathbb{Z}/(p_1^n)^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k^n)^{e_k}\mathbb{Z}.$$

So $\mathbb{Z}_M \cong \prod_{p\big|M} \mathbb{Z}_{p^e}$.

Now we claim that $\mathbb{Z}_{p^e} \cong \mathbb{Z}$ because we have

$$f : \mathbb{Z}_{p^e} \longmapsto \mathbb{Z}_p \text{ by } (a_1, a_2, \ldots) \mapsto (b_1, b_2, \ldots)$$

where $b_1 \equiv a_1 \pmod{p}$, $b_2 \equiv a_1 \pmod{p^2}$, $\ldots$, $b_e \equiv a_1 \pmod{p^e}$ and $b_{e+1} \equiv a_2 \pmod{p^{e+1}}$ and so on. It is clearly bijective.

Finally, if we have $p_1 \neq p_2$, $p_i \big| M$, then $(a, 0) \cdot (0, b) = (0, 0)$ and so it is a domain if and only if $M$ is a power of $p$.

4. We use a two pass method. Each element in $\mathbb{Z}_p$ is a sequence $(a_1, a_2, \ldots)$ where $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ and $a_i \equiv a_j \pmod{p^i}$ if $j \geq i$. Now $\mathbb{Z}/p^i\mathbb{Z}$ is finite for all $i$. So we have infinitely many elements whose first coordinate are the same say the set of those elements is $A_1$. Then for the elements in $A_2$, there are infinitely many of them which have the same second coordinate, and call the set of those $A_2$.

   Continue this so we have sets $A_1, A_2, \ldots$ and now we have a convergent subsequence because for any $x, y \in A_n$ we have $|x - y|_p \leq p^{-n}$ and so they converge.

5. Let $H$ be an open subgroup. Then $gH$ is open for all $g \in G$. But

$$G = \bigcup_{g \in G} gH.$$

   $G$ is compact and so we have a finite subcover $G = \bigcup_{i=1}^{n} g_i H$ so $[G : H] < \infty$.

   Now let $H$ be a closed subgroup with finite index. Then every coset $g_i H$ is closed. Hence, the complement of $H$ is a union of finitely many cosets, which is again closed, so $H$ is open.

# 25 Ramification Theory

Throughout the section, $[K : \mathbb{Q}_p] < \infty$ with valuation ring $\mathcal{O}_K$, normalised discrete valuation $v_K$, with uniformliser $\pi_K$, residue field $K$.

## 25.1 Unramified Extensions

**Definition 25.1.** *Let $L$ be a finite extension of $K$. We say $L/K$ is unramified if $e(L/K) = 1$, $L/K$ is ramified if $e(L/K)$ and $L/K$ is totally ramified if $e(L/K) = [L : K]$.*

**Lemma 25.2.** *Let $n \geq 1$, then there exists $L/K$ unramified with $[L : K] = n$.*

*Proof.* Write $k = \mathbb{F}_q$. Then $\mathbb{F}_{q^n} = \mathbb{F}_q(\bar{\alpha})$ for some $\bar{\alpha} \in \mathbb{F}_{q^n}$. Let $g \in \mathcal{O}_K[x]$ be the minimal polynomial of any lift $\alpha$ of $\bar{\alpha}$. Let $L = K(\alpha)$. Now $\bar{g}$ has $\bar{\alpha}$ as a root and has degree $n$. So $\bar{g}$ must be irreducible because the minimal polynomial of $\bar{\alpha}$ has degree $n$. So $g$ must be irreducible.

$[L : K] = \deg g = n$ and $f(L/K) \geq [\mathbb{F}_q(\bar{\alpha}) : \mathbb{F}_q]$ because $\bar{\alpha}$ is in the residue field of $L$. Hence $f(L/K) \geq n$ which implies $f(L/K) = n$ and $e(L/K) = 1$. So $L/K$ is unramified. □

**Theorem 25.3.** *Let $L/K$ be a finite extension. Let $\mathbb{F}_q$ be the residue field of $k$ and $\mathbb{F}_{q^n}$ be the residue field of $L$. Write $m = q^n - 1$. Then the extension $K(\zeta_m)/K$ is unramified, contained in $L$ and the extension $L/K(\zeta_m)$ is totally ramified.*

*Proof.* Consider the Techmuller map

$$[\cdot] : \mathbb{F}_{q^n}^* \longmapsto L.$$

Let $\alpha$ be a generator of $\mathbb{F}_{q^n}^*$, then $\alpha^m = 1$. Then we claim that $\zeta_m = [\alpha]$. Indeed, we have

$$[\alpha] \equiv \alpha \pmod{\pi_k}, [\alpha]^m = 1.$$

So $[\alpha]$ is a primitive root and without loss of generality, we may assume $[\alpha] = \zeta_m$. This shows that $K(\zeta_m) \subset L$.

Now $\bar{\zeta_m} \in \mathbb{F}_{q^n}$ is a primitive root and the residue field of $K(\zeta_m)$ is then $\mathbb{F}_q(\bar{\zeta_m}) = \mathbb{F}_{q^n}$. Hence $f(K(\zeta_m)/k) = n$. Now by assumption, $f(L/K) = n$ so $f(L/K(\zeta_m)) = 1$. Therefore, $L/K(\zeta_m)$ is totally ramified.

The natural map $\mathrm{Gal}(K(\zeta_m)/K) \longmapsto \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is injective becasue if $\sigma(\zeta_m) \equiv \zeta_m \pmod{\pi_L}$, and we also have $\sigma(\zeta_m)^{m+1} = \sigma(\zeta_m)$, using that

$$\sigma(\zeta_m)^{m+1} = \sigma(\zeta_m^{m+1}) = \sigma(\zeta_m).$$

So $\sigma(\zeta_m)$ also satisfies the properties

$$a^{m+1} = a, \bar{a} \equiv \zeta_m \pmod{\pi_L}.$$

But we know $\zeta_m$ also satisfies these properties, then by uniqueness of Techmuller map, we conclude that $\sigma(\zeta_m) = \zeta_m$ and so the map is injective.

Therefore, $[K(\zeta_m) : K] \leq [\mathbb{F}_{q^n} : \mathbb{F}_q] = n = f(K(\zeta_m)/K)$ and so the equality must hold. So $K(\zeta_m)/K$ is unramified of degree $n$. □

**Corollary 25.4.** *Let $[K : \mathbb{Q}_p] < \infty$ with residue field $\mathbb{F}_q$ and set $m = q^n - 1$. Then $L/K$ is unramified of degree $n$ if and only if $L = K(\zeta_m)$.*

*Proof.* It is clear by the proof of previous theorem that $K(\zeta_m)/K$ is unramified of degree $n$. Conversely, let $L/K$ be unramified of degree $n$. Then $L$ has residue field $\mathbb{F}_{q^n}$. Now apply the previous theorem, we know that $L/K(\zeta_m)$ is totally ramified. But $L/K$ is unramified, so $L = K(\zeta_m)$. □

**Corollary 25.5.** *For each $n \geq 1$, there is a unique unramified extension $L/K$ of degree $n$. Moreover, $L/K$ is Galois, and the natural map $Gal(L/K) \longmapsto Gal(k_L/k)$ is an isomorphism. In particular, $Gal(L/K)$ is cyclic, generated by $Frob_{L/K}$, where*

$$Frob_{L/K}(x) \equiv x^q \ (mod\ \pi_L),\ \forall x \in L.$$

*Proof.* The first part follows from the previous corollary, and it is clear that every cyclotomic extension is Galois. We have seen in the proof of Theorem 25.3 that the natural map is injective. Further,

$$[L : K] = f(L/K) = [k_L : k]$$

and so the natural map is surjective. Finally, let $Frob_{L/K}$ correspond to a generator say $\sigma$ of $\mathrm{Gal}(k_L/k)$, which sends $x$ to $x^q$. So the rest follows. □

**Corollary 25.6.** *If $L/K$ is Galois, then the natural map $Gal(L/K) \longmapsto Gal(k_L/K)$ is surjective.*

*Proof.* The natural map factors as

$$\mathrm{Gal}(L/K) \longmapsto \mathrm{Gal}(K(\zeta_m)/K) \longmapsto \mathrm{Gal}(k_L/K)$$

where the first map is restriction. But restriction is always surjective and we know the second one is isomorphism, so the composition is surjective. □

**Definition 25.7.** *The* **inertia group** $I = \ker(Gal(L/K) \longmapsto Gal(k_L/k))$. *Since $[L : K] = e(L/K)f(L/K)$ and $|Gal(k_L/k)| = f(L/K)$, it is easy to see $|I| = e(L/K)$.*

## 25.2 Totally Ramified Extension And Eisenstein Polynomial

**Definition 25.8.** *We say a polynomial $g = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathcal{O}_K[x]$ is an Eisenstein polynomial if $v_K(a_i) \geq 1$ for all $i \geq 1$ and $v_K(a_0) = 1$.*

**Theorem 25.9.** *(i) If $L/K$ is totally ramified, then the minimal polynomial of $\pi_L$ is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.*

*(ii) Conversely, if $g \in \mathcal{O}_K[x]$ is Eisenstein, $L = K(\alpha)$ where $\alpha$ is a root of $g$. Then $L/K$ is totally ramified and $\alpha$ is a uniformliser of $L$.*

*Proof.* (i) $[L : K] = e$. Let

$$g(x) = x^m + \sum_{i=0}^{m-1} a_i x^i$$

be the minimal polynomial of $\pi_L$, where $a_i \in \mathcal{O}_K, m \leq e$. So we have

$$\pi_L^m = -\sum_{i=1}^{m-1} a_i \pi_L^i$$

and so

$$v_L(a_i\pi_L^i) = v_L(a_i) + i = ev_K(a_i) + i \equiv i \ (\mathrm{mod}\ e).$$

So all these terms are distinct, for different $i$ because $0 \leq i \leq m-1 \leq e-1$. Now by ultrametric law, we have

$$m = v_L(\pi_L^m) = \min_{0 \leq i \leq m-1}(i + ev_K(a_i))$$

and so $v_K(a_i) \geq 1$ for all $i \geq 1$. Also, when $i = 0$ we have $v_K(a_i) = 1$ becasue $m \leq e$. Therefore, the minimum is achieved at $i = 0$, and so $m = e$. So the extension is totally ramified.

Now $L = K(\pi_L)$. For each $y \in L$, let

$$y = \sum_{i=0}^{e-1} b_i \pi_L^i, b_i \in K.$$

$v_L(y) = \min_{0 \le i \le e-1}(ev_K(b_i) + i)$. Therefore,

$$y \in \mathcal{O}_L \iff v_L(y) \ge 0 \iff v_K(b_i) \ge 0 \ \forall i.$$

The last condition is equivalent to $b_i \in \mathcal{O}_K$, which is the same as saying $y \in \mathcal{O}_K[\pi_L]$. So we have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

(ii) If $g \in \mathcal{O}_K[x]$ is Eisenstein, let $L = K(\alpha)$ where $g(\alpha) = 0$. Write $g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, and $e = e(L/K)$. We know that $v_K(a_i) \ge 1$ and so $v_L(a_i) \ge e$ and $v_L(a_0) = e$.

Since $g(\alpha) = 0$, we have

$$\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i \Rightarrow n v_L(\alpha) \ge \min_{0 \le i \le n-1}(i v_L(\alpha) + v_L(a_i)).$$

We may assume the minimum is achieved at $j$. Then

$$v_L(\alpha)(n-j) \ge v_L(a_j) \ge e.$$

So $v_L(\alpha) > 0$.

Now for $i \ne 0$, we have

$$v_L(a_i \alpha^i) > v_L(a_i) \ge e = v_L(a_0).$$

So the minimum is achieved at $i = 0$ and so $n v_L(\alpha) = v_L(a_0) = e$. Therefore,

$$v_L(\alpha) = \frac{e}{n}.$$

But $v_L$ is discrete so we must have $e = n$ (because $e \le n$) and $v_L(\alpha) = 1$. So $\alpha$ is a uniformlsier. □

**Remark 25.10.** *Recall from the previous exercise that*

$$|N_{L/K}(x)|_K = |x|_L \ \forall x \in L.$$

*This is equivalent to*

$$v_K(N_{L/K}(x)) = f(L/K) v_L(x) \ \forall x \in L.$$

*We will use this condition later.*

## 25.3 The Norm Map

**Definition 25.11.** *Let $L/K$ be an extension of number fields and $I_L, I_K$ be groups of fractional ideals of $L$ and $K$ respectively. The* **norm map** *is defined as,*

$$N_{L/K} : I_L \longmapsto I_K$$

*via, for each prime $\mathcal{P} \subset \mathcal{O}_L$ and $\mathfrak{p} \subset \mathcal{O}_K$,*

$$\mathcal{P} \mapsto \mathfrak{p}^f$$

*where $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$ and $f = f(\mathcal{P}/\mathfrak{p})$. Extend this to a group homomorphism as $I_L$ is a free abelian group, generated by prime ideals.*

**Lemma 25.12.** *Let $x \in L^*$ and $N_{L/K}(x)^*$ is an element in $K$. Then we have a commutative diagram:*

$$N_{L/K}(x)\mathcal{O}_K = N_{L/K}(x\mathcal{O}_L).$$

*Proof.* Let $\mathfrak{p}$ be a prime of $K$. For $x \in L^*$, recall from Corollary 23.14, we have

$$N_{L/K}(x) = \prod_{\mathcal{P}\Big|\mathfrak{p}} N_{L_\mathcal{P}/K_\mathfrak{p}}(x).$$

So we have

$$v_\mathfrak{p}(N_{L/K})(x) = \sum_{\mathcal{P}\Big|\mathfrak{p}} v_\mathfrak{p}(N_{L_\mathcal{P}/K_\mathfrak{p}}(x)).$$

Then by Remark 25.10, we have

$$\sum_{\mathcal{P}\Big|\mathfrak{p}} v_\mathfrak{p}(N_{L_\mathcal{P}/K_\mathfrak{p}}(x)) = \sum_{\mathcal{P}\Big|\mathfrak{p}} v_\mathfrak{p}(x) f(\mathcal{P}/\mathfrak{p}) = v_\mathfrak{p}(N_{L/K}(x\mathcal{O}_L)).$$

This is because, say $x\mathcal{O}_L = \mathfrak{p}^\alpha \cdot Q$, where $Q$ is prime to $\mathfrak{p}$. Then

$$N_{L/K}(x\mathcal{O}_L) = N_{L/K}(\mathfrak{p}^\alpha) N_{L/K}(Q).$$

Let

$$\mathfrak{p} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}, N_{L/K}(\mathfrak{p}) = N_{L/K}(\mathcal{P}_1)^{e_1} \cdots N_{L/K}(P_r)^{e_r}.$$

Also, $v_{\mathcal{P}_i}(x) = \alpha e_i$. Therefore,

$$\sum_{\mathcal{P}\Big|\mathfrak{p}} v_\mathcal{P}(x) f(\mathcal{P}/\mathfrak{p}) = \sum_{i=1}^{r} \alpha e_i f_i = \alpha[L:K].$$

But by definition of the norm map, we have the $\mathfrak{p}$-part of $N_{L/K}(x\mathcal{O}_L)$ is:

$$\mathfrak{p}^{\alpha e_1 f_1 + \cdots + \alpha e_r f_r}$$

and so $v_\mathfrak{p}(N_{L/K}(x\mathcal{O}_L)) = \alpha \sum e_i f_i = \alpha[L:K]$. Hence we have proved that

$$v_\mathfrak{p}(N_{L/K}(x)) = \sum_{\mathcal{P}\Big|\mathfrak{p}} v_\mathfrak{p}(N_{L_\mathcal{P}/K_\mathfrak{p}}(x)) = v_\mathfrak{p}(N_{L/K}(x\mathcal{O}_L)).$$

Since $\mathfrak{p}$ is arbitrary, so we have

$$N_{L/K}(x)\mathcal{O}_K = N_{L/K}(x\mathcal{O}_L).$$

□

**Remark 25.13.** *If $\mathfrak{a} \subset \mathcal{O}_K$, then $N_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.*

## 25.4 Different And Inverse Different

**Definition 25.14.** *The inverse different is*

$$\mathcal{D}_{L/K}^{-1} = \{y \in L : \pi_{L/K}(xy) \in \mathcal{O}_K \ \forall x \in \mathcal{O}_L\}.$$

*This is an $\mathcal{O}_L$-submodule of $L$ and it contains $\mathcal{O}_L$.*

Let $x_1, \ldots, x_n \in \mathcal{O}_L$ be a basis for $L$ over $K$ and $d = \Delta(x_1, \ldots, x_n)$. If $x \in \mathcal{D}_{L/K}^{-1}$, $x = \sum \lambda i x_i$, $\lambda_i \in K$. Then

$$\sum_{i=1}^{n} \lambda_i Tr_{L/K}(x_j x_j) = Tr_{L/K}(x x_j) \in \mathcal{O}_K$$

and so we have a matrix

$$T\lambda = a \text{ where } a \in \mathcal{O}_K.$$

So $\lambda = T^{-1}a$ and $T^{-1} = \frac{1}{d}T^{adj}$. But $T^{adj}$ has entries in $\mathcal{O}_K$, so $\lambda \in \frac{1}{d}\mathcal{O}_K^d$ and so $\lambda_i \in \frac{1}{d}\mathcal{O}_K$. Thus we conclude that

$$x \in \frac{1}{d}\mathcal{O}_L, d\mathcal{D}_{L/K}^{-1} \subset \mathcal{O}_L.$$

The inverse of $\mathcal{D}_{L/K}^{-1}$, $\mathcal{D}_{L/K}$ is therefore an ideal in $\mathcal{O}_L$.

**Theorem 25.15.** *(i) If $M/L/K$ is a tower of number fields, then*

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$$

*as an ideal in $\mathcal{O}_M$.*

*(ii) If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and $\alpha$ has minimal polynomial $g(x)$ in $\mathcal{O}_K[x]$, then $\mathcal{D}_{L/K} = \langle g'(\alpha) \rangle$.*

*(iii) $N_{L/K}(\mathcal{D}_{L/K}) = \mathfrak{d}_{L/K}$, the discriminant.*

*Proof.* (i)

$$\begin{aligned}
x \in \mathcal{D}_{M/K}^{-1} &\iff Tr_{M/k}(xy) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_M \\
&\iff Tr_{M/K}(xyz) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_M, \forall z \in \mathcal{O}_L \\
&\iff Tr_{L/K}(Tr_{M/L}(xyz)) = Tr_{L/K}(zTr_{M/L}(xy)) \in \mathcal{O}_K, \ \forall y \in \mathcal{O}_M, \forall z \in \mathcal{O}_L \\
&\iff Tr_{M/L}(xy) \in \mathcal{D}_{L/K}^{-1}, \forall y \in \mathcal{O}_M \\
&\iff Tr_{M/L}(rxy) \in \mathcal{O}_L, \forall y \in \mathcal{O}_M, r \in \mathcal{D}_{L/K} \text{ because } r \in \mathcal{D}_{L/K} \subset \mathcal{O}_L \\
&\iff rx \in \mathcal{D}_{M/L}^{-1} \iff x \in \mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1}.
\end{aligned}$$

So $\mathcal{D}_{M/K}^{-1} = \mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1}$.

(ii) Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be roots of $g$. Let

$$\frac{g(x)}{x - \alpha} = \beta_{n-1}x^{n-1} + \cdots \beta_1 x + \beta_0, \beta_i \in \mathcal{O}_L, \beta_{n-1} = 1.$$

Claim

$$\sum_{i=1}^{n} \frac{g(x)}{x - \alpha_i} \frac{\alpha_i^r}{g'(\alpha_i)} = x^r \text{ for } 0 \leq r \leq n-1.$$

Indeed, the difference of both sides is a polynomial of degree ¡ $n$, which vanishes at $x = \alpha_i$ for $i = 1, \ldots, n$. So the difference has to be identically zero.

Now equate the coefficient of both sides of $x^s$, we have

$$Tr_{L/K}\left(\frac{\beta_s \alpha^r}{g'(\alpha)}\right) = \delta_{rs}.$$

By assumption, $\mathcal{O}_L$ has $\mathcal{O}_K$ basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ and so the above equation gives a dual basis. So $\mathcal{D}_{L/K}^{-1}$ has basis

$$\frac{\beta_0}{g'(\alpha)}, \frac{\beta_1}{g'(\alpha)}, \ldots, \frac{1}{g'(\alpha)}$$

as $\beta_{n-1} = 1$. But this is an ideal so we conclude that

$$\mathcal{D}_{L/k}^{-1} = \left\langle \frac{1}{g'(\alpha)} \right\rangle, \mathcal{D}_{L/K} = \langle g'(\alpha) \rangle.$$

(iii) Suppose for simplicity that $\mathcal{O}_L$ and $\mathcal{O}_K$ are principal ideal domain (the general case can be done by localisation). Let $\mathcal{O}_L$ have $\mathcal{O}_K$ basis $x_1, \ldots, x_n$ and let $y_1, \ldots, y_n$ be the dual basis such that

$$Tr_{L/K}(x_i y_j) = \delta_{ij}.$$

$L/K$ is separable so we have $n$ embeddings.

$$\sum_{i=1}^{n} \sigma_i(x_j)\sigma_i(y_k) = Tr_{L/K}(x_j y_k) = \delta_{jk}.$$

Recall that $\Delta(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2$. So we have

$$\Delta(x_1, \ldots, x_n)\Delta(y_1, \ldots, y_n) = 1.$$

Write $\mathcal{D}_{L/K}^{-1} = B\mathcal{O}_L$ for some $B \in L$, as we assume it is principal ideal domain. Then

$$\mathfrak{d}_{L/K}^{-1} = \langle \Delta(x_1, \ldots, x_n) \rangle^{-1} = \langle \Delta(y_1, \ldots, y_n) \rangle = \langle \Delta(Bx_1, \ldots, Bx_n) \rangle$$

because $y_1, \ldots, y_n$ and $Bx_1, \ldots, Bx_n$ are $\mathcal{O}_K$ basis for $\mathcal{D}_{L/K}^{-1}$, and the discriminant is invariant under a change of basis. But

$$\langle \Delta(Bx_1, \ldots, Bx_n) \rangle = (N_{L/K}(B))^2 \langle \Delta(x_1, \ldots, x_n) \rangle.$$

So

$$\mathfrak{d}_{L/K}^{-1} = N_{L/K}(B) = N_{L/K}(\mathcal{D}_{L/K}^{-1}), \mathfrak{d}_{L/K} = N_{L/K}(\mathcal{D}_{L/K}).$$

In general, let $S = \mathcal{O}_K \backslash \mathfrak{p}$ and replace $\mathcal{P}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K, S^{-1}\mathcal{O}_L$.

□

**Remark 25.16.** *The definition of $\mathcal{D}_{L/K}$ and its properties carry over to the case whenever $K$ is an extension of $\mathbb{Q}_p$. We identify the local different $\mathcal{D}_{L_\mathcal{P}/K_\mathfrak{p}}$ with a power of $\mathfrak{p}$.*

**Theorem 25.17.** *The global different is the product of the local differents. In other words,*

$$\mathcal{D}_{L/K} = \prod_{\mathfrak{p}} \prod_{\mathcal{P}\big|\mathfrak{p}} \mathcal{D}_{L_\mathcal{P}/K_\mathfrak{p}}.$$

*Proof.* By an analogue of Corollary 23.14, we have

$$Tr_{L/K}(x) = \sum_{\mathcal{P}\big|\mathfrak{p}} Tr_{L_\mathcal{P}/K_\mathfrak{p}}(x).$$

Write $\mathcal{D}_{L_\mathcal{P}/K_\mathfrak{p}} = \mathcal{P}^{\delta(\mathcal{P}/\mathfrak{p})}$.

We firstly show that the LHS divides RHS. Suppose $x \in L$, with $v_{\mathfrak{p}}(x) \geq -\delta(\mathcal{P}/\mathfrak{p})$ so in $L_{\mathcal{P}}$, we have $\mathcal{D}^{-1}_{L_{\mathcal{P}}/K_{\mathfrak{p}}} \big| \langle x \rangle$. Then $Tr_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathfrak{p}}, \forall y \in \mathcal{P}, \forall \mathcal{P}, \forall \mathfrak{p}$. Since $\mathcal{O}_L \subset \mathcal{O}_{\mathfrak{p}}$, we have

$$Tr_{L/K}(xy) \in \mathcal{O}_{\mathfrak{p}} \ \forall y \in \mathcal{O}_L, \forall \mathfrak{p}.$$

Therefore, $Tr_{L/K}(xy) \in \mathcal{O}_K$ as $\bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} = \mathcal{O}_K$, and so $x \in \mathcal{D}^{-1}_{L/K}$. We conclude that

$$\prod_{\mathcal{P}} \mathcal{P} \big| \mathfrak{p} \mathcal{D}^{-1}_{L_{\mathcal{P}}/K_{\mathfrak{p}}} \subset \mathcal{D}^{-1}_{L/K}.$$

Hence, LHS divides RHS.

Now conversely, fix $\mathcal{P}$ a prime of $L$ and let $r = v_{\mathcal{P}}(\mathcal{D}_{L/K})$. Pick $x \in \mathcal{P}^{-r} \backslash \mathcal{P}^{-(r-1)}$. Then $v_{\mathfrak{p}}(x) = -r, v_{\mathcal{P}'}(x) \geq 0 \ \forall \mathcal{P}' \neq \mathcal{P}$. This shows that $x \in \mathcal{D}^{-1}_{L/K}$.

Now we again use the equation

$$Tr_{L/K}(x) = \sum_{\mathcal{P} \big| \mathfrak{p}} Tr_{L_{\mathcal{P}}/K_{\mathfrak{p}}}.$$

For any $y \in \mathcal{O}_L$, we know $Tr_{L/K}(xy) \in \mathcal{O}_L$ as $x \in \mathcal{D}^{-1}_{L/K}$. Since $v_{\mathcal{P}'}(x) \geq 0$ for any $\mathcal{P}' \neq \mathcal{P}$, we have $xy \in \mathcal{O}_{\mathcal{P}'}$ and hence $Tr_{L_{\mathcal{P}'}/K_{\mathfrak{p}}}(x) \in \mathcal{O}_{\mathfrak{p}}$ for any $\mathcal{P}' \neq \mathcal{P}$. Then, by using the equation above, we have

$$Tr_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathfrak{p}} \ \forall y \in \mathcal{O}_L.$$

By continuity, we have

$$Tr_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathfrak{p}} \ \forall y \in \mathcal{O}_{\mathfrak{p}}.$$

This implies that $x \in \mathcal{D}^{-1}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$ for all $\mathfrak{p}$. Then

$$-r = v_{\mathcal{P}}(x) \geq -\delta(\mathcal{P}/\mathfrak{p}) = v_{\mathcal{P}}(\mathcal{D}^{-1}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}).$$

Then,

$$v_{\mathcal{P}}(\mathcal{D}_{L/K}) = r \leq v_{\mathcal{P}}(\mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}) \ \forall \mathfrak{p}.$$

Therefore,

$$\mathcal{D}_{L/K} \big| \prod_{p} \prod_{P} \mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}.$$

□

**Corollary 25.18.**

$$\mathfrak{d}_{L/K} = \prod_{\mathfrak{p}} \prod_{\mathcal{P}} \mathfrak{d}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}.$$

*Proof.* Take norm in the previous theorem. □

**Lemma 25.19.** *Let $[K : \mathbb{Q}_p] < \infty$ and $L$ be a finite extension of $K$. Let $\alpha \in \mathcal{O}_L$ have $k(\bar{\alpha}) = k_L$ and $g \in \mathcal{O}_K[x]$ be any monic lift of the minimal polynomial of $\bar{\alpha}$ over $k$. Then*

*(i) $g(\alpha) \equiv 0 \ (mod \ \pi)$ and $g'(\alpha) \not\equiv 0 \ (mod \ \pi_L)$.*

*(ii) $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ if and only if there exists $\beta \in \mathcal{O}_K[\alpha]$ with $v_L(\beta) = 1$.*

*(iii) Either $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ or $\mathcal{O}_L = \mathcal{O}_K[\alpha + \pi_L]$.*

*Proof.* (i) $\bar{g}$ is irreducible and so it is separable. Then $g'(\bar{\alpha}) \neq 0$ and so

$$g'(\alpha) \not\equiv 0 \pmod{\pi}.$$

(ii) $\mathcal{O}_K[\alpha]$ is the image of the continuous map

$$\mathcal{O}_K^n \longmapsto L \text{ via } (x_0, \ldots, x_{n-1}) \mapsto to \sum_{i=0}^{n-1} x_i \alpha^i$$

where $n = [K(\alpha) : K]$. But $\mathcal{O}_K$ is compact, so $\mathcal{O}_K[\alpha]$ is closed in $L$.

Clearly, if $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ then pick $\beta$ to be the uniformliser. Conversely, since $k_L = k(\bar{\alpha})$ and so $\mathcal{O}_K[\alpha]$ contains coset representatives for $k_L$. But $k_L = \mathcal{O}_L/\pi_L\mathcal{O}_L = \mathcal{O}_L/\beta\mathcal{O}_L$ by assumption. So given $y \in \mathcal{O}_L.$, we have

$$y = \sum_{i=0}^{\infty} \lambda_i \beta^i, \lambda_i \in \mathcal{O}_K[\alpha]$$

because $\mathcal{O}_K[\alpha]$ is closed and so it is complete. Thus, $\beta \in \mathcal{O}_K[\alpha]$ and so $y \in \mathcal{O}_K[\alpha]$.

(iii) By Taylor expansion,

$$g(\alpha + \pi_L) = g(\alpha) + \pi_L g'(\alpha) \pmod{\pi_L^2}.$$

By (i), $g'(\alpha) \not\equiv 0 \pmod{\pi_L}$ so it is a unit. The valuation of $\pi_L$ is 1. $v_L(\pi_L g'(\alpha)) = 1$. Now consider the valuation of the above equation, we conclude that either $v_L(g(\alpha + \pi_L) = 1$ or $v_L(g(\alpha)) = 1$. For example, if $v_L(g(\alpha)) > 1$ then $g(\alpha + \pi_L) = 1$ by ultrametric law. Also by (i), $v_L(g(\alpha)) \geq 1$.

Now $g(\alpha) \in \mathcal{O}_K[\alpha]$ and $g(\alpha) \in \mathcal{O}_K[\alpha]$ and $g(\alpha + \pi_L) \in \mathcal{O}_K[\alpha + \pi_L]$. Now use part (ii).

□

**Definition 25.20.** *Let $K$ be a finite extension of $\mathbb{Q}_p$ and $L$ be a finite extension of $K$. We say $L/K$ is tamely ramified if $p \nmid e(L/K)$ and $L/K$ is wildly ramified if $p \big| e(L/K)$.*

**Theorem 25.21.** *Let $K$ be a finite extension of $\mathbb{Q}_p$ and $L$ be a finite extension of $K$. Let $\mathcal{D}_{L/K} = \pi_L^{\delta(L/K)}\mathcal{O}_L$. Then $\delta(L/K) \geq e(L/K) - 1$, with equality if and only if $L/K$ is tamely ramified. In particular, $L/K$ is unramified if and only if $\mathcal{D}_{L/K} = \mathcal{O}_L$.*

*Proof.* We check the case when $L/K$ is totally ramified or unramified. When $L/K$ is totally ramified. we have $[L : K] = e$ and by Theorem 25.9 we know $\mathcal{O}_L = \mathcal{O}_K[\pi]$. The minimal polynomial of $\pi_L$, say $g$, is Eisenstein. Write

$$g(x) = x^e + \sum_{i=0}^{e-1} a_i \pi_L^i.$$

Then

$$g'(\pi_L) = e\pi_L^{e-1} + \sum_{i=0}^{e-1} i a_i \pi_L^{i-1}.$$

Now $v_L(e\pi_L^{e-1}) = e-1+v_L(e) \geq e-1$ and $v_L(ia_i\pi_L^{i-1}) = v_L(i)+v_L(a_i)+i-1 \geq e$. So $v_L(g'(\pi_L)) \geq e-1$, with equality if and only if $e$ is a unit.

By Theorem 25.15(ii), $\mathcal{D}_{L/K} = \langle g'(\pi_L) \rangle$ and $v_L(\mathcal{D}_{L/K}) = \delta(L/K)$. Thus, $\delta(L/K) \geq e - 1$, with equality if and only if $e$ is a unit, which is equivalent of saying $L/K$ is tamely ramified (as $p \nmid e$).

Now let $L/K$ be unramified. By Lemma 25.19 (ii), since $\pi_L = \pi_K$, so if we take any $\alpha \in \mathcal{O}_L$ with $k(\bar{\alpha}) = k_L$, we will have $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Further, by (i) of Lemma 25.19, we know $g'(\alpha)$ is a unit. Then again we apply Theorem 25.15(ii) and so

$$\mathcal{D}_{L/K} = \langle g'(\alpha) \rangle = \mathcal{O}_L.$$

Hence, $\delta(L/K) = 1$.

In general, use Theorem 25.3, so we have a tower $L/K(\zeta_m)/K$. Then use Theorem 25.15(i) we have

$$\mathcal{D}_{L/K} = \mathcal{D}_{L/K(\zeta_m)}\mathcal{D}_{K(\zeta_m)/K}.$$

So we have, by the previous work that

$$\mathcal{D}_{L/K(\zeta_m)} = \pi_{L/K(\zeta_m)}^{\delta(L/K(\zeta_m))}\mathcal{O}_{K(\zeta_m)},\ \mathcal{D}_{K(\zeta_m)/K} = \mathcal{O}_K.$$

Thus, $\delta(L/K) = \delta(L/K(\zeta_m))$. Also, $e(L/K(\zeta_m)) = e(L/K)$. So the result follows. □

## 25.5 Krasner's Lemma And Application

**Lemma 25.22. [Krasner's Lemma]** *$[K : \mathbb{Q}_p] < \infty$. Let $f \in \mathcal{O}_K[x]$ be irreducible, monic with roots $\alpha = \alpha_1, \ldots, \alpha_n$ in $\bar{K}$. Suppose $\beta \in \bar{K}$, with $|\beta - \alpha| < |\beta - \alpha_i|$ for all $2 \leq i \leq n$. Then $\alpha \in K(\beta)$.*

*Proof.* Let $L = K(\beta)$ and $L' = L(\alpha_1, \ldots, \alpha_n)$ so $L'/L$ is Galois. If $\sigma \in \mathrm{Gal}(L'/L)$, then $|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha|$ by unique extension of absolute values. So by assumption $\sigma(\alpha) = \alpha$ and so $\alpha \in L = K(\beta)$. □

**Corollary 25.23.** *$[K : \mathbb{Q}_p] < \infty$. Let $f \in \mathcal{O}_K[x]$ be irreducible, monic with roots $\alpha = \alpha_1, \ldots, \alpha_n$ in $\bar{K}$. Suppose $\beta \in \bar{K}$ with $|\beta - \alpha| < |\alpha - \alpha_j|$ for all $2 \leq j \leq n$. Then $\alpha \in K(\beta)$.*

*Proof.* $|\beta - \alpha| < |\alpha - \alpha_j|$. So

$$|\beta - \alpha_j| = |\beta - \alpha + \alpha - \alpha_j| = |\alpha - \alpha_j|$$

by ultrametric law. So $|\beta - \alpha| < |\beta - \alpha_j|$ for $2 \leq j \leq n$. Now apply the previous theorem. □

**Theorem 25.24.** *$[K : \mathbb{Q}_p] < \infty$. Let $f = \sum_{i=0}^n b_i x^i \in \mathcal{O}_K[x]$ be an irreducible monic polynomial. Let $\alpha \in \bar{K}$ be a root of $f$. Then there exists $\epsilon > 0$ such that whenever $g = \sum_{i=0}^n b_i x^i \in \mathcal{O}_K[x]$ is a monic polynomial with $|a_i - b_i| < \epsilon$ for all $i$, then $g$ is irreducible. Further, if $g(\beta) = 0$, then $K(\alpha) = K(\beta)$.*

*Proof.* $f$ is irreducible and so separable. Thus, $f'(\alpha) \neq 0$. For $\epsilon$ small enough, we have

$$|g(\alpha)| < |f'(\alpha)|^2,\ |g'(\alpha) - f'(\alpha)| < |f'(\alpha)|.$$

There are possible because $f'(\alpha) \neq 0$ and $f(\alpha) = 0$, so $|a_i - b_i| < \epsilon$ means that $g$ is very close to $f$ and $g(\alpha)$ is close to 0.

Now by ultrametric law,

$$|g'(\alpha)| = |g'(\alpha) - f'(\alpha) + f'(\alpha)| = |f'(\alpha)|$$

and so $|g(\alpha)| < |f'(\alpha)|^2 = |g'(\alpha)|^2$. Then by Hensel's lemma, $g$ has a root $\beta \in K(\alpha)$ such that $|\beta - \alpha| < |g'(\alpha)|$. But

$$|g'(\alpha)| = |f'(\alpha)| = \left|\prod_{i=2}^n (\alpha - \alpha_i)\right| \leq |\alpha - \alpha_j|,\ \forall 2 \leq j \leq n.$$

This is because

$$|\alpha|^n = \left|\prod_{i=1}^n \sigma_i(\alpha)\right| = |a_0| \leq 1$$

and so $|\alpha| \leq 1$, and similarly $|\alpha_i| \leq 1$. Then $|\alpha - \alpha_i| \leq 1$. Hence

$$|\beta - \alpha| < |g'(\alpha)| \leq |\alpha - \alpha_j|\ \forall 2 \leq j \leq n.$$

Then apply the previous corollary, and so $\alpha \in K(\beta)$. This shows that $K(\alpha) = K(\beta)$ and so $g$ is irreducible. □

**Corollary 25.25.** *Let $[K:\mathbb{Q}_p]<\infty$. Then $K$ is the completion of some number field.*

*Proof.* Let $K=\mathbb{Q}_p(\alpha)$ and assume $\alpha\in\mathcal{O}_K$ (by clearing denominator). Let $f\in\mathbb{Z}_[x]$ be the minimal polynomial of $\alpha$. Then by the previous theorem, we have $g\in\mathbb{Z}[x]$ which is monic and irreducible such that $\mathbb{Q}_p(\alpha)=\mathbb{Q}_p(\beta)$, where $g(\beta)=0$, using $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Then, $K=\mathbb{Q}_p(\beta)$, the completion of $\mathbb{Q}(\beta)$. □

**Corollary 25.26.** *Let $[K:\mathbb{Q}_p]<\infty$. There are only finitely many extensions of $K$ of a given degree.*

*Proof.* By Corollary 25.4, we know the unramified extension of given degree is unique and so we only need to check the totally ramified extension and then use Theorem 25.3 for a general extension. But the totally ramified extension corresponds to Eisenstein polynomial by Theorem 25.9. Also we have a 1-1 correspondence

$$\{\text{Eisenstein polynomial of degree}n\}\longleftrightarrow\{(a_0,\dots,a_{n-1})\in\mathcal{O}_K^n, v_K(a_i)\geq 1, i\geq 2, v_K(a_0)=1\}.$$

Now RHS is a compact set as it is a closed subset of a compact set.

By Theorem 25.24 we know that the subset defining a given field $L$ is open because if two polynomials are close then they define the same field. Then by compactness, there are only finitely many such fields. This shows that there are finitely many totally ramified extension of a given degree. □

**Corollary 25.27.** *Let $K$ be a number field and $n\geq 1$, $S$ a finite set of primes of $K$. Then there are only finitely many extensions $L/K$ of degree $n$, unramified outside $S$.*

*Proof.* For each $\mathfrak{p}\in S$. The previous corollary says there are finitely many possibilities for the extension $L_{\mathcal{P}}/K_{\mathfrak{p}}$, because $[L_{\mathcal{P}}:K_{\mathfrak{p}}]\leq[L:K]$ and for each degree there are only finitely many extensions. Thus, there are only finitely many possibilities for the discriminant $\mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$.

By Corollary 25.18,

$$\mathfrak{d}_{L/K}=\prod_{\mathfrak{p}}\prod_{\mathcal{P}\mid\mathfrak{p}}\mathfrak{d}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}.$$

Also, by Theorem 25.21, if $\mathfrak{p}\notin S$ is unramified, then

$$\mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}=\mathcal{O}_{L_{\mathcal{P}}}.$$

So in fact we have

$$\mathfrak{d}_{L/K}=\prod_{\mathfrak{p}\in S}\prod_{\mathcal{P}\mid\mathfrak{p}}\mathfrak{d}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}.$$

Since $S$ is finite, then there are only finitely many possibilities for $\mathfrak{d}_{L/K}$.

Taking norm, and since

$$\mathcal{D}_{L/\mathbb{Q}}=\mathcal{D}_{L/K}\mathcal{D}_{K/\mathbb{Q}}$$

we have

$$\mathfrak{d}_{L/\mathbb{Q}}=N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})\mathfrak{d}_{K/\mathbb{Q}}.$$

Since $\mathfrak{d}_{K/\mathbb{Q}}$ is fixed, so there are only finitely many possibilities for $\mathfrak{d}_{L/\mathbb{Q}}$.

Recall from Hermit's Theorem that there are only finitely many number fields with bounded discriminant (see Theorem 16.24). Then the result follows by applying Hermit's Theorem. □

## 25.6 Ramification Group

Let $[K : \mathbb{Q}_p] < \infty$, $L/K$ be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Let $K' = K(\zeta_m)$.

**Definition 25.28.** *The inertia group is*

$$I = \{\sigma \in G : \sigma(x) \equiv x \ (mod\ \pi_L)\ \forall x \in \mathcal{O}_L\}.$$

*Note that $I \subset G$ and $|I| = e(L/K)$. The $n^{th}$* **ramification group** *is*

$$G_n = \{\sigma \in G : \sigma(x) \equiv x \ (mod\ \pi_L^{n+1}\ \forall x \in \mathcal{O}_L\}.$$

*Note that $G_i \subset G_{i+1}$ and $G_0 = I$.*

**Remark 25.29.** *Note that*

$$G_n = \ker\left(G \longmapsto Aut(\mathcal{O}_L/\pi_L^{n+1}\mathcal{O}_L)\right)$$

*the kernel of the restriction map. So $G_n$ is a normal subgroup of $G$.*

**Theorem 25.30.** *(i)* $G_n = \{\sigma \in I : v_L(\sigma(\pi_L) - \pi_L) > n\}$.

*(ii)* $\bigcap_{n\geq 0} G_n = \{1\}$.

*(iii)* $G_0/G_1 \hookrightarrow k_L^*$ *and* $G_n/G_{n+1} \hookrightarrow (k_L, +)$ *for all* $n \geq 1$.

*Proof.* Since $K'/K$ is unramified, so $I(L/K) = I(L/K')$. Then we can replace $K$ by $K'$. In other words, we only need to check the result holds for totally ramified extension because $k_{K'} = k_L$.

(i) Since we assume $L/K$ is totally ramified, so we have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Therefore,

$$\sigma(\pi_L) \equiv \pi_L \ (\mathrm{mod}\ \pi_L^{n+1}) \iff \sigma(x) \equiv x \ (\mathrm{mod}\ \pi_L^{n+1})\ \forall x \in \mathcal{O}_L.$$

Hence, $G_n = \{\sigma \in I : v_L(\sigma(\pi_L) - \pi_L) > n\}$.

(ii) If $\sigma \neq 1$, then $\sigma(\pi_L) \neq \pi_L$ because $L = K(\pi_L)$ and so $\sigma(\pi_L) - \pi_L \neq 0$. Then $v_L(\sigma(\pi_L) - \pi_L) < \infty$. Apply (i) and so we have $\sigma \notin G_n$ for $n$ large enough. Since $G$ is finite, so the largest such $n$ exists and so $\bigcap_{n\geq 0} G_n = \{1\}$.

(iii) For $\sigma \in G_0$, let $\sigma(\pi_L) = a_\sigma \pi_L$ if $\sigma \in G_0$. Consider the map

$$G_0 \longmapsto k_L^* \text{ by } \sigma \mapsto a_\sigma \ (\mathrm{mod}\ \pi_L).$$

The map has the correct image because by unique extension of absolute value, $\sigma(\pi)$ also has valuation 1 and so $a_\sigma \in k_L^*$.

Let $\sigma, \tau \in G_0$. Then

$$\sigma(\tau(\pi_L)) = \sigma(a_\tau)\sigma(\pi_L) = \sigma(a_\tau)a_\sigma\pi_L$$

and so

$$a_{\sigma\tau} = \sigma(a_\tau)a_\sigma \ (\mathrm{mod}\ \pi).$$

But $\sigma \in G_0$ and so $\sigma(a_\tau) - a_\tau \equiv 0 \ (\mathrm{mod}\ \pi_L)$. Therefore,

$$a_{\sigma\tau} \equiv a_\tau a_\sigma \ (\mathrm{mod}\ \pi_L)$$

and so the map is a homomorphism. The kernel is clearly $G_1$.

For $n \geq 1$, $\sigma \in G_n$, we have

$$\sigma(\pi_L) = \pi_L + a_\sigma \pi_L^{n+1}$$

by using (i) and unique extension. Then define the map

$$G_n \longmapsto (k_L, +) \text{ by } \sigma \mapsto a_\sigma \pmod{\pi_L}.$$

The map has the correct image by (i).

Now for $\sigma, \tau \in G_n$, we have

$$\sigma(\tau(\pi_L)) \equiv \pi_L + a_\sigma \pi_L^{n+1} + \sigma(a_\tau)\pi_L^{n+1} \pmod{\pi_L^{n+2}}$$

and so $a_{\sigma\tau} = a_\sigma + \sigma(a_\tau) \pmod{\pi_L}$. But $\sigma(a_\tau) \equiv a_\tau \pmod{\pi_L}$ so

$$a_{\sigma\tau} \equiv a_\sigma + a_\tau \pmod{\pi_L}$$

and so the map is a homomorphism. It is clear that the kernel is $G_{n+1}$.

□

**Corollary 25.31.** *$G_1$ is the unique Sylow $p$-subgroup of $G_0$.*

*Proof.* By the previous theorem, $G_n/G_{n+1}$ is a subgroup of $(k_L, +)$, which is a $p$-group. Also, let $N$ be the smallest number such that $G_N = \{1\}$. Then $G_{N-1}/G_n$ is a $p$-group. Hence $G_{N-2}$ is a $p$-group and so we conclude by induction that $G_1$ is a $p$-group.

Uniqueness is clear as $G_1$ is a normal subgroup of $G_0$ by the previous theorem. Also, by the previous theorem, $G_0/G_1$ has order prime to $p$ (as it is a subgroup of $k_L^*$) so $G_1$ is the largest $p$-group inside $G_0$. □

$K'$ is the fixed field of $G_0$, and set $K''$ to be the fixed field of $G_1$. Then by previous theorem, $K'/K''$ is tamely ramified and $L/K''$ is wild ramified.

**Corollary 25.32.** *$Gal(L/K)$ is soluable.*

*Proof.* It is clear as $G_{n+1}$ is normal in $G_n$. □

## 25.7 Exercises

1. Let $K = \mathbb{Q}_p(\zeta_p)$. Show that $(1 - \zeta_p^i)/(1 - \zeta_p) \equiv i \pmod{\pi_K}$ for all $1 \leq i \leq p-1$ and that $(1 - \zeta_p)^{p-1} = -pu$ for some $u \in 1 + \pi_K \mathcal{O}_K$. Deduce that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$.

2. Let $K$ be a $p$-adic field and $L = K(\zeta_m)$ where $m$ is an integer coprime to $p$. Let $g(X)$ be the minimal polynomial of $\zeta_m$ over $K$. Use a version of Hensel's lemma (see question 2 of section 23) to show that $\bar{g} \in k[X]$ is irreducible. Deduce that $L/K$ is unramified.

3. Let $K$ be a number field and $L = K(\sqrt[n]{a})$ for some $a \in \mathcal{O}_K$. Show that if $\mathfrak{p} \nmid na$ then $\mathfrak{p}$ is unramified in $L$.

4. Let $L/K$ and $M/K$ be extensions of $p$-adic fields. Show that if $L/K$ is unramified then the natural map

$$\{K - \text{embeddings} L \hookrightarrow M\} \longmapsto \{k - \text{embeddings} k_L \hookrightarrow k_M\}$$

is a bijection.

5. (i) Let $L_1/K$ and $L_2/K$ be extension of $p$-adic fields, at least one of which is Galois, with ramifications indices $e_1$ and $e_2$. Suppose that $(e_1, e_2) = 1$. Show that $L_1L_2/K$ has ramification index $e_1e_2$. In particular, the composite of any two unramified extensions is unramified.

   (ii) Compute the valuation rings of $\mathbb{Q}_p(\zeta_p, \sqrt[p]{p})$ and $\mathbb{Q}_p(\zeta_p, \sqrt[2p-1]{p})$.

6. Let $L/K$ be a Galois be a Galois extension of number fields. Suppose that $\mathrm{Gal}(L/K)$ is not cyclic. Show that no primes of $K$ are inert in $L$. (A prime $\mathfrak{p}$ of $K$ is inert in $L$ if $\mathfrak{p}\mathcal{O}_L$ is prime.)

7. Let $K = \mathbb{Q}(\sqrt[3]{m})$ where $m \geq 2$ is a square-free integer with $m \not\equiv 0 \pmod 3$. Show (using the results about the different) that $K$ has discriminant

$$\mathfrak{d}_K = \begin{cases} -3m^2 & \text{if } m \equiv \pm 1 \pmod 9, \\ -27m^2 & \text{otherwise .} \end{cases}$$

8. Let $L/K$ and $E/K$ be extensions of number fields. Let $\mathfrak{p}_E \big| \mathfrak{p}$ be primes of $E$ and $K$. Show that if $\mathfrak{p}$ is unramified in $L/K$ then $\mathfrak{p}_E$ is unramified in $LE/E$. Give an example to show the converse is false.

9. (i) Show there are no finite extensions of $\mathbb{Q}$ that are unramified at all primes.

   (ii) Show that if $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(\sqrt{-1})$ then $L/K$ is unramified at all primes.

   (iii) Let $L$ be the splitting field of $f(X) = X^3 - X - 1$ over $\mathbb{Q}$. Since $f(X)$ has discriminant $-23$ the unique quadratic subfield is $K = \mathbb{Q}(\sqrt{-23})$. Show that $L/K$ is unramified at all primes.

10. Compute the ramification groups of $\mathbb{Q}_3(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_3$.

11. Prove that $\mathbb{Q}_2$ has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. Compute its ramification groups.

12. Prove that there is at most one prime $p$ for which $\mathbb{Q}_p$ has a Galois extension with Galois group $S_4$.

13. Prove that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified Galois extension, determine its degree, its Galois group and all ramification groups $G_i$. (Hint: $1 - \zeta$ is a uniformlsier.)

14. Suppose $L/K$ is Galois, totoally and tamely ramified extension of degree $n$. Prove that $\mu_n \subset K$ and $L = K(\sqrt[n]{\pi_K})$. How many totally and tamely ramified Galois extensions does $\mathbb{Q}_5$ have? (Hint: Use Kummer's theorem.)

15. Let $L/K$ be a finite Galois extensions that is totally ramified. Let $G = \mathrm{Gal}(L/K)$ and for $\sigma \in G$ put $i_{L/K} = v_L(\sigma(\pi_L) - \pi_L)$. Let $\delta(L/K) = v_L(\mathcal{D}_{L/K})$. Show that

$$\delta(L/K) = \sum_{1 \neq \sigma \in G} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1)$$

where $G_i \subset G$ is the $i^{\text{th}}$ higher ramification group.

## 25.8 Hint and Solutions

1. Adjoining the root of $f(X) = 1 + X + \cdots + X^{p-1}$ is the same as adjoining the root of $f(X+1)$. But

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$$

which is Eisenstein. So by theorem, the root $\zeta_p - 1$ is a uniformliser. So we may assume $\pi_K = 1 - \zeta_p$.

Now

$$\frac{1 - \zeta_p^i}{1 - \zeta_p} - i = (1 - 1) + (\zeta_p - 1) + \cdots + (\zeta_p^{i-1} - 1) \equiv 0 \pmod{1 - \zeta_p}$$

and so $(1 - \zeta_p^i)/(1 - \zeta_p) \equiv i \pmod{\pi_K}$. Further, we have

$$\prod_{i=1}^{p-1} \frac{1 - \zeta_p^i}{1 - \zeta_p} \equiv (p-1)! \pmod{\pi_K}.$$

But $(p-1)! \equiv -1 \pmod{p}$ and so is $-1 \pmod{\pi_K}$. Also, $\prod_{i=1}^{p-1}(1 - \zeta_p) = f(1) = p$. Thus, we have

$$\frac{p}{(1 - \zeta_p)^{p-1}} \equiv -1 \pmod{p}.$$

Then it can be written as $-1 + ap$, for some $a \in \mathcal{O}_K$. Thus,

$$p = -(1 - \zeta_p)^{p-1} + a(1 - \zeta_p)^{p-1} p$$

and so

$$(1 - \zeta_p)^{p-1} = -p(1 - a(1 - \zeta_p)^{p-1}) = -pu$$

where $u = 1 - a(1 - \zeta_p)^{p-1} \in 1 + \pi_K \mathcal{O}_K$.

Thus $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(1 - \zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-pu})$. But $u \in 1 + \pi_K \mathcal{O}_K$ is a unit. So we consider the polynomial $X^{p-1} - u = 0$. Reduce modulo $\pi_K$, we have $X^{p-1} - 1 \equiv 0 \pmod{\pi_K}$. Thus, by Hensel's lemma, we have a solution to the equation $X^{p-1} - u = 0$. Hence

$$\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-pu}) = \mathbb{Q}_p(\sqrt[p-1]{-p}).$$

2. If $\bar{g}$ is reducible then by question 2 of section 23, $g$ is reducible. Also $\bar{g} \big| X^m - 1$ and $p \nmid m$ so $\bar{g}$ is separable. Then

$$ef = [L : K] = \deg g = \deg \bar{g} \leq [k_L : k] = f$$

and so equality holds so $e = 1$.

3. Localise at $\mathfrak{p}$. Since $\mathfrak{p} \nmid na$ so $X^n - a$ is separable. Pick any $\mathcal{P}$ above $\mathfrak{p}$. Then $L_{\mathcal{P}} = K_{\mathfrak{p}}(\beta)$ where the minimal polynomial of $\beta$ is an irreducible factor of $X^n - a$ over $\mathbb{K}_p[X]$, say $g$. Then by question 2 of section 23, $\bar{g}$ is irreducible. Then we have

$$e(\mathcal{P}/\mathfrak{p})f(\mathcal{P}/\mathfrak{p}) = [L_{\mathcal{P}} : K_{\mathfrak{p}}] = \deg g = \deg \bar{g} \leq [k_L : k] = f(\mathcal{P}/\mathfrak{p}).$$

So equality holds and so $e(\mathcal{P}/\mathfrak{p}) = 1$.

4. We know when $L/K$ is unramified then $L = K(\zeta_m)$ and $k_L = k(\zeta_m)$. Then any $K$-embeddings $L \hookrightarrow M$ is determined by the image of $\zeta_m$, and any $k$-embeddings $k_L \hookrightarrow k_M$ is also determined by the image of $\zeta_m$. So the result follows.

5. (i) It is clear that the ramification degree is at least $e_1e_2$ by tower law. Let $e_1'$ be the ramification degree of $L_1L_2/L_2$. Since $L_1/K$ is Galois, so $L_1L_2/L_2$ is Galois. Now consider the restriction map

$$\mathrm{Gal}(L_1L_2/L_2) \longmapsto \mathrm{Gal}(L_1/K).$$

If $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$ fixes $L_1$ and $L_2$, then it fixes $L_1L_2$. So the restriction map is an injection. In particular, the inertia subgroup of LHS injects into the inertia group of RHS. So $e(L_1L_2/L_2)\big|e(L_1/K)$, i.e. $e_1'\big|e_1$. Then $e(L_1L_2/K) = e_1'e_2\big|e_1e_2$. So $e(L_1L_2/K) \leq e_1e_2$.

(ii) $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$. By theorem (Eisenstein polynomial), the valuation ring is $\mathbb{Z}_p[1-\zeta_p]$. Now the minimal polynomial for $\sqrt[p]{p}$ in $\mathbb{Q}_p(\zeta_p)$ is $X^p - p$. By earlier question we know

$$(1-\zeta_p)^{p-1} = -pu.$$

So the valuation of $p$ in $\mathbb{Q}_p(\zeta_p)$ is $p-1$ and since $p$ is totally ramified in $\mathbb{Q}_p(\sqrt[p]{p})$, so the valuation of $\sqrt[p]{p}$ in $\mathbb{Q}_p(\zeta_p, \sqrt[p]{p})$ is $p-1$.
In $\mathbb{Q}(\zeta_p, \sqrt[p]{p})$, the valuation of $1-\zeta_p$ is $p$ again by using the equation

$$(1-\zeta_p)^{p-1} = -pu = -(\sqrt[p]{p})^p u.$$

So $\frac{1-\zeta_p}{\sqrt[p]{p}}$ is a uniformliser and so by theorem (Lemma 25.19), $\mathcal{O} = \mathbb{Z}_p\left[\frac{1-\zeta_p}{\sqrt[p]{p}}\right]$.

Similarly, we can check $\frac{1-\zeta_p}{\sqrt[2p-1]{p^2}}$ is a uniformliser in $\mathbb{Q}_p(\zeta_p, \sqrt[2p-1]{p})$ so $\mathcal{O} = \mathbb{Z}_p\left[\frac{1-\zeta_p}{\sqrt[2p-1]{p^2}}\right]$.

6. Suppose $p$ inerts in $L$. Let $\mathcal{P}$ be a prime above $\mathfrak{p}$. Then $L_{\mathcal{P}}/K_{\mathfrak{p}}$ is Galois and the decomposition group is $\mathrm{Gal}(L/K)$ (because we assume there is only one prime above $\mathfrak{p}$). But it is unramified, so the decomposition group is cyclic, which is a contradiction.

7. We know if $p$ is unramified, then $\mathcal{D}_{K_{\mathcal{P}}/\mathbb{Q}_p}$ is trivial. So we only need to consider those $p$ which ramify in $K$. The discriminant of $\sqrt[3]{m}$ is $-27m^2$, and we know the discriminant of $K$ only differs $-27m^2$ by a square. Also, it is clear that $m$ ramifies.

Let $p$ be a prime and $p \neq 3$. Then $p$ must be tamely ramified and so by Theorem, for any prime $\mathcal{P}$ above $p$,

$$\delta(K_{\mathcal{P}}/\mathbb{Q}_p) = e(\mathcal{P}/p) - 1.$$

Further, we can check that $\langle p \rangle = \langle p, \sqrt[3]{m} \rangle$ so $p$ is totally ramified and so $e(\mathcal{P}/p) = 3$. Thus, we have

$$\prod_{p\big|m}\prod_{\mathcal{P}\big|m} \mathfrak{d}_{K_{\mathcal{P}}/\mathbb{Q}_p} = \prod_{p\big|m} p^2 = m^2.$$

So the discriminant is $-3m^2$ or $-27m^2$, depending on the ramification of 3. When $m \equiv 1 \pmod 9$, we know by earlier theorem that $m$ is a cube in $\mathbb{Z}_3$ (you can also refer to question 6 in section 23). Thus, if $\mathcal{P}$ is any prime above 3, we must have $e(\mathcal{P}/3) \leq 2$, and so $\delta(\mathcal{P}/3) \leq 1$. Thus, we have $-3m^2$.

When $m \not\equiv 1 \pmod 9$, we know $m$ is not a cube in $\mathbb{Z}_3$. Hence, $X^3 - m$ is irreducible over $\mathbb{Q}_3$. Thus, $e(\mathcal{P}/3) = 3$ and so we have $-27m^2$ (recall when it is 3, it is not tamely ramified, so $\delta > e - 1$).

8. Localise at $\mathfrak{p}$. $\mathfrak{p}$ is unramified in $L/K$ so for any $\mathcal{P}$ above $\mathfrak{p}$, $L_{\mathcal{P}}/K_{\mathfrak{p}}$ is unramified and so it is Galois. Then by question 5 the (local) ramification degree is

$$e(LE/K) = e(L/K)e(E/K) = e(LE/E)e(E/K).$$

Thus, since $e(L/K) = 1$ so $e(LE/E) = 1$.

Let $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{-3})$ and $E = \mathbb{Q}(\sqrt{3})$. Then $LE = \mathbb{Q}(\sqrt{3}, i)$. Let $p = 3$ then $p$ is ramified in $L, E$. Also, $\mathfrak{p}_E = \sqrt{3}$. But $\sqrt{3}$ does not ramify in $LE$.

9. (i) Let $[K : \mathbb{Q}] < \infty$. If $K$ is unramified at all primes, then the discriminant must be a unit in $\mathbb{Z}$, which is $\pm 1$, and this is impossible.

(ii) By the previous question, if $p$ is unramified in $\mathbb{Q}(\sqrt{-1})$, then $\mathfrak{p}$ is unramified in $L$, where $\mathfrak{p}$ is a prime above $p$. So the only primes which could possibly ramify are the primes in $K$ above 2.

The discriminant of $\mathbb{Q}(\sqrt{5})$ is 5 and so 2 is unramified in $\mathbb{Q}(\sqrt{5})$. Thus, the ramification degree of 2 in $L$ is 2 and the residue degree is 2. But 2 already ramifies in $\mathbb{Q}(\sqrt{-5})$ and so if $\mathfrak{p}$ is a prime above 2 in $K$, then $\mathfrak{p}$ must be unramified in $L/K$.

(iii) Since $-23$ is not a square so $L/\mathbb{Q}$ is not cyclic and hence $[L : \mathbb{Q}] = 6$, with Galois group $S_3$. Let $E = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $f$. Then the discriminant of $E$ must be $-23$ as it is square free. So the only prime which ramifies in $E/\mathbb{Q}$ is 23. By the previous question, we know that the only primes which can ramify in $L/K$ are the primes above 23 in $K$.

Let $\mathfrak{p}$ be a prime above 23 in $E$. We know that

$$\delta(E_{\mathfrak{p}}/\mathbb{Q}_2 3) \geq e(\mathfrak{p}/23) - 1$$

with equality holds if and only if 23 is tamely ramified. We pick the $\mathfrak{p}$ such that $e(\mathfrak{p}/23) \geq 2$ because we know 23 ramifies. Then it could not be 3 because otherwise the discriminant will have a factor of $23^2$. Hence, we conclude that

$$23 = \mathfrak{p}^2\mathfrak{p}'$$

in $E/\mathbb{Q}$. This shows that we have at least two primes in $L$ above 23, i.e. $r \geq 2$.

Since $ref = [L : \mathbb{Q}] = 6$, and $2 \big| e$, $r \geq 2$ we must have $e = 2$, $r = 3$. Finally, 23 already ramifies in $K/\mathbb{Q}$ so the ramification degree in $L/K$ is 1. Thus, there is no prime which ramifies in $L/K$.

10. Let $\alpha = \sqrt[3]{2}$ and so $F = \mathbb{Q}_3(\zeta_3, \alpha)$ is the splitting field of $\alpha$. So $F/\mathbb{Q}_3$ is Galois. It is clear that $\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3$ is ramified. Also, the minimal polynomial of $\alpha + 1$ over $\mathbb{Q}_3$ is $X^3 - 3X^2 + 3X - 3$, which is Eisenstien. So it is totally ramified. Hence we conclude that $e(F/\mathbb{Q}_3) = 6$.

Now $G = G_0$ is clear as $e = 6$. Also, $G_1$ is the Sylow 3 subgroup so $G_1$ is cyclic of order 3. We know $1 - \zeta_3$ is a uniformliser in $\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3$. So the valuation $v_F(1 - \zeta_3) = 3$ and similarly $v_F(1 + \alpha) = 2$. Then we know that $\frac{1-\zeta_3}{1+\alpha}$ is a uniformliser in $F$.

Now let $\sigma : \sqrt[3]{2} \mapsto \zeta_3\sqrt{3}[2]$ and so $G_1 = \langle\sigma\rangle$. Then $\sigma(\pi_L) - \pi_L = \frac{(1-\zeta_3)^2}{(1+\zeta_3\alpha)(1+\alpha)}$ which has valuation 2. So by theorem $G_n = \{1\}$ for all $n \geq 2$.

11. Since $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 = \{1, -1, 2, 5\}$ so we only have 3 non-trivial quadratic extensions. Hence the composition of these gives the unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$.

    Let $F = \mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{5})$. We know that $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified, and the quotient of $G/I$ is cyclic so the inertia group is $(\mathbb{Z}/2\mathbb{Z})^2$.

    Let $L = \mathbb{Q}_2(\sqrt{-1}, \sqrt{2})$. Let $\sigma : \sqrt{-1} \mapsto -\sqrt{-1}$ and $\tau : \sqrt{2} \mapsto -\sqrt{2}$. Note that $\mathbb{Q}_2(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}_2(\zeta_8)$ where $\zeta_8 = \sqrt{1 + i\sqrt{2}}$. We can check that $\zeta_8 - 1$ is a uniformliser. So let $\pi_L = \frac{1+i}{\sqrt{2}} - 1$.

    Now $\sigma(\pi_L) = \frac{1-i}{\sqrt{2}} - 1$ and then $\sigma(\pi_L) - \pi_L = -\sqrt{2}i$ which has valuation 2. Similarly, $\tau(\pi_L) - \pi_L = -\sqrt{2}(1 + i)$ which has valuation 4.

    Therefore, we have $G_1 = G_0$, $G_2 = G_3 = \langle\tau\rangle$ and $G_n = \{1\}$ for all $n \geq 4$.

12. Let $I$ be the inertia group and $I$ is normal. But $S_4/I$ must be cyclic, so $I = S_4$ or $A_4$. Now $G_1$ is the $p$-subgroup of $G_0$, and $G_1$ is a normal subgroup of $S_4/I$. So $p = 2$ is the only possible prime.

13. Consider the polynomial $\frac{(X+1)^{p^n}-1}{(X+1)^{p^{n-1}}-1}$, this is $p$-Eisenstein and hence irreducible. Further this shows that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified with degree $p^{n-1}(p-1)$. The Galois group is $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

    Let $\alpha = \zeta - 1$ which is a uniformliser. Let $\sigma(\zeta) = \zeta^i$ for some $i$ prime to $p$ and $i$ generates the group $(\mathbb{Z}/p^n\mathbb{Z})^*$. $\sigma^k(\alpha) - \alpha = \zeta^{i^k} - \zeta = \zeta(\zeta^{i^k-1} - 1)$.

    It is clear that $i^{(p-1)p^m} \equiv 1 \pmod{p^{m+1}}$ for $m \leq n - 1$ and by choice the $i$ (the generator) we have $i^{(p-1)p^m} - 1 = bp^{m+1}$ where $(b, p) = 1$. Thus, for each $m$, $\zeta^{i^{(p-1)p^m-1}}$ is a primitive $p^{n-m-1}$-th root and so $\zeta^{i^{(p-1)p^m-1}} - 1$ is a uniformliser in $\mathbb{Q}_p(\zeta_{p^{n-m-1}})/\mathbb{Q}_p$. So the valuation of it is $p^{m+1}$. Thus, we have $G_0 = G, G_1 = \cdots = G_{p-1} = \langle\sigma^{p-1}\rangle$.

    Similarly, for each $m$, $G_{p^m} = \cdots = G_{p^{m+1}-1} = \langle\sigma^{(p-1)p^m}\rangle$.

14. It is tamely ramified so $(n, p) = 1$. Also, it is totally ramified so $G = G_0$. $G_1$ is the $p$-subgroup, and so $G_1 = \{1\}$. Now $G_0/G_1 \hookrightarrow k_l^* = k*$. So we conclude that $G = G_0$ is a subgroup of $k^*$.

    Let $k^* = \mathbb{F}_{p^r}^*$, $r \geq 1$. Now $G_0 = G$ has order $n$ so $n \big| p^r - 1$. We have $n^{\text{th}}$ root of unity in the residue field and $(n, p) = 1$ so we have those in $K$ by using Hensel's Lemma.

    By Kummer Theory, $L = K(\sqrt[n]{\alpha})$ where $\alpha \in K$ and $\alpha$ is not an $n^{\text{th}}$ power. Consider the valuation of $\sqrt[n]{\alpha}$. If the valuation is prime to $n$, say it is $a$, then there exists $b$ such that $ab \equiv 1 \pmod{n}$. Then since $K = (\sqrt[n]{\alpha}) = K(\sqrt[n]{\alpha^b})$ we have $L = K(\sqrt[n]{\pi_K})$.

    Now suppose the valuation is not prime to $n$. Then there exists $b > n$ such that the valuation of $\sqrt[n]{\alpha^b}$ is a multiple of $n$, say $cn$. So $\beta = \frac{\sqrt[n]{\alpha^b}}{\pi_K^c}$ is a unit. Then consider the extension $K(\beta)/K$. The minimal polynomial is a factor of

$$X^n - \frac{\alpha^b}{\pi_K^c} = 0.$$

Then by question 3, ($\beta$ is a unit so it is in $\mathcal{O}_K$) we know this is unramified. But $K(\beta)$ is a subextension of $K(\sqrt[n]{\alpha})$ so this gives a contradiction.

Finally, we know by the first part we must have $\mu_n \subset \mathbb{Q}_5$. But $\mathbb{Q}_5$ only contains $\zeta_4$. So $n = 2, 4$. The ramified quadratic extensions are $\mathbb{Q}_5(\sqrt{5})$ and $\mathbb{Q}_5(\sqrt{10})$.

Then for $n = 4$. It is easy to show that $b$ is a fourth power in $\mathbb{Z}_5$ if and only if $\bar{b}$ is a fourth power in $\mathbb{F}_5$, by using Hensel's Lemma. Let $k = \mathbb{F}_5$. The map $k^* \longmapsto (k^*)^4$ by $x \mapsto x^4$ induces an isomorphism

$$k^*/(\mathbb{Z}/4\mathbb{Z}) \cong (k^*)^4$$

because $\mu_4 \subset \mathbb{Q}_5$. Hence

$$\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^4 \cong (\mathbb{Z}/4\mathbb{Z})^2.$$

For representatives, it is generated by the product $ab$ where $a$ is $1, 2, 3, 4$ and $b$ is $1, 5, 15, 125$. But we need $L = \mathbb{Q}_5(\sqrt[4]{\pi_K})$ so among those, we have uniformlisers $5, 10, 15, 20$. Therefore, we have 4 extensions of degree 4 which is tamely and totally ramified.

Therefore, we have 6 in total.

15. For the equation

$$\sum_{1 \neq \sigma \in G} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1),$$

we have $|G_i| - 1 = card\{\sigma \neq 1, \sigma \in G : v_L(\sigma(\pi_L) - \pi_L) \geq i + 1\} = card\{\sigma \neq 1, \sigma \in G : i_{L/K}(\sigma) \geq i + 1\}$. So if we set $\sigma_j$, for $j = 1, \ldots, n$ and $i_{L/K}(\sigma_j) = a_j$, then $\sigma_j$ is counted $a_j$ times expect we don't count $\sigma_1 = id$ (RHS). This is the same as summing over $j$ for each $a_j$ (LHS).

Now for the equality $\delta(L/K) = \sum_{1 \neq \sigma \in G} i_{L/K}(\sigma)$, we have

$$\mathcal{D}_{L/K} = \mathcal{P}^{\delta(L/K)}\mathcal{O}_L = \langle \pi_L \rangle^{\delta(L/K)}\mathcal{O}_L.$$

It is totally ramified so $\mathcal{D}_{L/K} = \langle g'(\pi_L) \rangle$. So

$$\delta(L/K) = v_L\langle g'(\pi_L) \rangle = v_L(\prod_{i \neq 1}^{n} (\pi_L - \sigma(\pi_L))) = \sum_{1 \neq \sigma \in G} v_L(\pi_L - \sigma(\pi_L)).$$

# 26 Introduction to Elliptic Curves

In this section we will give an introduction to elliptic curves. Elliptic curves play an important role in modern number theory. For example, each Modell's equation is a special form of elliptic curves.

## 26.1 Basic Properties

**Definition 26.1.** *An* **elliptic curve** *over a field $K$ is a* **non-singular** *projective curve of genus 1 over $K$, together with a $K$-rational point $\mathcal{O}$. By using method of algebraic geometry, we can simplify the curve to the following equation:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, a_i \in K.$$

*For ease of notation, we will work in the* **Affine space**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*In this case, the given point $\mathcal{O}$ is the infinity.*

**Example 26.2.** *$y^2 = x^3 - x$ is an elliptic curve. Further if we work in the projective case, then the infinity corresponds to the point where $z = 0$, so for $y^2z = x^3 - xz^2$, the point $\mathcal{O}$ is $[0 : 1 : 0]$.*

**Definition 26.3.** *We will denote $E(K)$ for the set*

$$\{\mathcal{O}\} \cup \{(x, y) : x, y \in K \text{ and } (x, y) \text{ satisfies } E\}.$$

**Theorem 26.4.** *Let $E$ be an elliptic curve over $K$. Then there exists an isomorphism (in the sense of projective geometry) from $E$ to the projective curve defined by*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K$$

*and maps the given point to $[0 : 1 : 0]$.*

**Example 26.5.** *Let $E$: $y^2 = x^4 - 1$, $\mathcal{O} = (1, 0)$. Given that this is an elliptic curve. We can use the following steps:*

*(1) $x_2 = x - 1$. Then we have $y^2 = x_2(x_2 + 2)(x_2^2 + 2x_2 + 2)$.*

*(2) $x_3 = \frac{1}{x_2}$. Then $y^2 = x_3^{-1}(x_3^{-1} + 2)(x_3^{-2} + 2x_3^{-1} + 2)$.*

*(3) $y_2 = yx_3$. Then $y_2^2 = 4x_3^3 + 6x_3^2 + 4x_3 + 1$.*

*(4) $y_3 = \frac{y_2}{2}$. Then $y_3^2 = x_3^3 + \frac{3}{2}x_3^2 + x_3 + \frac{1}{4}$.*

*It is easy to check that $p$ goes to infinity.*

**Remark 26.6.** *This must be a reversable process because it is an isomorphism and the rational points of $E$ go bijectively to those of the resulting curve.*

**Proposition 26.7.** *(1) We can further simplify the equation to $E : y^2 = x^3 + a_2x^2 + a_4 + a_6$, if $Char(K) \neq 2$. Further, when $Char(K) \neq 2, 3$ then we can reduce it to $y^2 = x^3 + Ax + B$.*

(2) *Two curves given by the given equations $E, E'$ are isomorphic over $K$ if and only if they are related by a change of variables of the form:*

$$x = u^2x' + r, y = u^3y' + u^2sx' + t, u, r, s, t \in K.$$

(3) *$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$, $Char(K) \neq 2$ is non-singular if and only if the right hand side has no repeated roots in $\bar{K}$, the algebraic closure of $K$.*

The proof for (1) is straightforward by completing square or cube. We shall omit the proof of (2) and (3) here because we need some knowledge in algebraic geometry.

**Definition 26.8.** *Let $P, Q \in E(K)$. Define the sum $P \oplus Q$ in the following rule. Let the line through $P$ and $Q$ intersects $E$ at $R$. There must be a third point on the intersection by Bezout's theorem. Repeat this for $R$ and $\mathcal{O}$, and say the third point on the intersection of the line through $R$ and $\mathcal{O}$ and $E$ is $T$. Then define*

$$P \oplus Q = T.$$

**Theorem 26.9.** *$E(K)$ is an abelian group under $\oplus$, with $\mathcal{O}$ the identity. So $P \oplus Q \in E(K)$.*

The group law $\oplus$ is clearly commutative. Also, by definition, it is easy to check that $\mathcal{O}$ is the identity. The inverse of $P$ is just the third point on the intersection of the line through $P$ and $\mathcal{O}$ and $E$. The hard bit is associativity and we will prove this later.

**Remark 26.10.** *If $F/E$ is a field extension, then $E(K) \subset E(F)$ as a subgroup.*

## 26.2 Elliptic Curves over $\mathbb{C}$

We will discuss the property of elliptic curve over $\mathbb{C}$.

**Definition 26.11.** *We say that a function $f : \mathbb{C} \longmapsto \mathbb{C}$ is meromorphic if at each $a \in \mathbb{C}$, it has a Laurent expansion*

$$f(z) = \sum_{n=n_0}^{\infty} C_n(z-a)^n, n_0 \in \mathbb{C}, C_{n_0} \neq 0 \text{ unless } f \equiv 0.$$

*Write the order of $f$ at $a$, $ord_a(f) = n_0$. Also, define the residue, $res_a(f) = C_{-1}$.*

**Definition 26.12.** *A lattice $\Lambda$ in $\mathbb{C}$ is a discrete rank 2 subgroup. In other words, $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where $\omega_1, \omega_2$ are independent over $\mathbb{R}$. We call $\pi$ the fundamental parallelogram which is the region*

$$\{a\omega_1 + b\omega_2 : a, b \in [0, 1)\}.$$

**Definition 26.13.** *An* **elliptic function** *(with respect to $\Lambda$) is a meromorphic function on $\mathbb{C}$ such that*

$$f(z + \omega) = f(z), \ \forall z \in \mathbb{C}, \omega \in \Lambda.$$

*In other words, it is doubly periodic.*

Another way to understand elliptic functions is that they are precisely meromorphic functions on $\mathbb{C}/\Lambda = \pi$. They form a field $\mathbb{C}(\pi)$.

**Lemma 26.14.** *Let $f$ be a non-zero elliptic function. Then*

(1) *If $f$ is analytic, then $f$ is constant.*

(2) *$ord_\omega(f) \neq 0$ for only finitely many $\omega \in \mathbb{C}/\Lambda$.*

*(3) We have the following identities:*

$$\sum_{\omega\in\mathbb{C}/\Lambda} res_\omega f = 0 \text{ and } \sum_{\omega\in\mathbb{C}/\Lambda} ord_\omega f = 0.$$

*(4) We also have*

$$\sum_{\omega\in\mathbb{C}/\Lambda} \omega ord_\omega f \in \Lambda.$$

*Proof.* (1) $f$ is analytic and so $f$ is bounded on the closure of $\pi$. But $f$ is periodic and hence $f$ is bounded everywhere. Then by complex analysis, we know that an entire bounded function must be constant.

(2) Suppose we have infinitely many $\omega$ such that $ord_\omega f \neq 0$, then since the closure of $\pi$ is compact and so we can take a convergent subsequence. In other words, we have $(\omega_n)_{n=1}^\infty \to \omega \in \bar{\pi}$, such that $ord_{\omega_n} f \neq 0$, then we must have $ord_\omega f \neq 0$. Also we may assume that $ord_{\omega_n} f$ have the same sign.

Now if the sign is positive, then we have an accumulation of zeros of $f$, then by isolation of zeros, we must have $f \equiv 0$. If the sign is negative, then we have an accumulation of poles of $f$, then $f$ is singular, and so is not meromorphic. Therefore, we only have finitely many such $\omega$.

(3) By residue theorem, we have

$$\sum_{\omega\in\mathbb{C}/\Lambda} res_\omega f = \frac{1}{2\pi i}\oint_{\partial\pi} f(z)dz.$$

We may split the integral into four line integrals, say $L_1, L_2, L_3$ and $L_4$, in the sense that $L_1, L_2, L_3, L_4$ are the boundaries of $\pi$, counted anticlockwise. Then it is clear that the value of the integral on $L_1$ cancels with that on $L_3$, because $f$ is periodic. Similarly, $L_2$ cancels with $L_4$. Hence the sum is zero.

For the second identity, by argument principal of complex analysis we have

$$\sum_{\omega\in\mathbb{C}/\Lambda} = \frac{1}{2\pi i}\oint_{\partial\pi} \frac{f'(z)}{f(z)}dz.$$

Hence it is 0 by a similar argument as above.

(4) Writing $f(z) = (z-\omega)^{ord_\omega f} g(z)$. It is easy to check this has residue $\omega ord_\omega f$ at $\omega$. Hence the integral

$$\oint_{\partial\pi} \frac{zf'(z)}{f(z)}dz = \sum_{\omega\in\mathbb{C}/\Lambda} \omega ord_\omega f.$$

Again we split the integral into four line integrals in the same notation as above. Then on $L_3$, we use the substitution $z = z' + \omega_2$ and the fact that

$$\int_{L_1} \frac{f'(z)}{f(z)}dz$$

is a multiple of $2\pi i$ (because $f(z)$ takes the same value at the end points by periodicity and so the logarithm differs by a multiple of $2\pi i$). Hence the whole expression is in $\Lambda$.

□

**Definition 26.15.** *The Weistress $\wp$ function with respect to $\Lambda$ is given by*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

**Proposition 26.16.** *This expression converges locally uniformly on $\mathbb{C}/\Lambda$ to an elliptic function. So $\wp(z)$ is analytic on $\mathbb{C}/\Lambda$. It has double poles for any $z \in \Lambda$.*

*Proof.* For $|\omega| > 2|z|$, we have

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \frac{|z|}{|\omega|^2} \left| \frac{2\omega - z}{(z-\omega)^2} \right| \leq \frac{10|z|}{|\omega|^3}.$$

Then

$$\sum_{|\omega|>2|z|} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq 10|z| \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{|\omega|^3} < \infty.$$

So the sum converges uniformly on compact subset of $\mathbb{C}/\Lambda$ and converges locally uniformly to an analytic function on $\mathbb{C}/\Lambda$. It is clear that $\wp(z)$ has a double pole for $z \in \Lambda$.

To check $\wp(z)$ is elliptic, consider the derivative

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

So it is clear that $\wp'(z)$ is elliptic. Hence, for any $\omega \in \Lambda$, we have

$$\frac{d}{dz}(\wp(z+\omega) - \wp(z)) = 0.$$

So $\wp(z+\omega) = \wp(z) + c$ for some constant $c$, which map depends on $\omega$. But by definition, it is clear that $\wp(z) = \wp(-z)$, and so

$$\wp(\frac{\omega}{2}) = \wp(-\frac{\omega}{2}).$$

Then pick $z = \frac{\omega}{2}$ in the above expression, and so we find $c = 0$. Hence, for any $\omega \in \Lambda$, we have $\wp(z+\omega) = \wp(z)$. □

**Definition 26.17.** *The Eisenstein series of weight $2k$ is*

$$G_{2k} = G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}, k \geq 2.$$

**Example 26.18.** *For $\Lambda = \mathbb{Z}[i]$, we have $i\Lambda = \Lambda$. Then we can find that $G_6 = 0$. This is because the sum is unchanged if we summing over $i\omega$ instead of $\omega$, by using $i\Lambda = \Lambda$, and so we have $G_6 = -G_6$ which in turn gives $G_6 = 0$.*

**Lemma 26.19.** *We have the following identity:*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

*Proof.* Consider that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2} \left( \frac{1}{(1-\frac{z}{\omega})^2} - 1 \right) = \sum_{k=1}^{\infty} \frac{(2k+1) z^{2k}}{\omega^{2k+2}}.$$

Now sum this over $\omega \in \Lambda \setminus \{0\}$, and since the sum converges absolutely, so we can swap the order of the sum and the result follows. □

**Theorem 26.20.** *We have the following identity:*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

*Proof.* By previous lemma, we have

$$\wp(z) = z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots,$$

and so

$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots, \text{ and } \wp'(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots.$$

Then,

$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_4 + \cdots.$$

So we have

$$4\wp(z)^4 3 - 60G_4\wp(z) - 140G_6 - \wp'(z)^2 = O(z^2).$$

But the left hand side above is an elliptic function and has no poles. So by Lemma 26.14(1), it is constant. Put $z = 0$ we see that the constant is 0. Hence the result follows. □

**Remark 26.21.** *We now get a map:*

$$\theta : \mathbb{C}/\Lambda \longmapsto E_\Lambda : y^2 = 4x^3 - 60G_4x - 140G_6,$$

*by*

$$f(z) = (\wp(z), wp'(z)).$$

**Lemma 26.22.** *$\wp(z)$ is even and $\wp'(z)$ is odd. Further, $\wp(z) - \wp(\alpha)$ has a double pole at $z \in \Lambda$, and has a zero at $\alpha$ and it has a double zero at $\alpha$ if $2\alpha \in \Lambda, \alpha \notin \Lambda$, and no other zeros or poles.*

*Proof.* Clearly, $\wp(z)$ is even as $\wp(z) = \wp(-z)$. Then differentiate both sides we have $\wp'(z) = -\wp'(-z)$. Also, $\wp(z) - \wp(\alpha)$ has double poles for $z \in \Lambda$.

Now we may assume that, given any $\alpha$, we can shift $\omega$ properly so that $\omega - \alpha \in \pi$; Otherwise we will work in a shifted fundamental parallelogram. Also, $\wp(\alpha) = \wp(\omega - \alpha)$. If $2\alpha \notin \Lambda$, then $\alpha$ and $\omega - \alpha$ are distinct. But we only have a double pole in $\pi$, and the number of poles must be equal to the number of zeros, so we only have single zeros at $\alpha$ and $\omega - \alpha$ in $\pi$. If $2\alpha \in \Lambda$, then we must have a double zero. □

**Theorem 26.23.** *Let $\Lambda \subset \mathbb{C}$ be a lattice and $X = \mathbb{C}/\Lambda$. Then $\mathbb{C}(X) = \mathbb{C}(\wp(z), \wp'(z))$. And every even elliptic function lies in $\mathbb{C}(\wp(z))$.*

*Proof.* Recall that $\mathbb{C}(X)$ consists of all elliptic functions. We will check that the later statement implies the first one. Indeed, for each $f$ we have

$$f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}(f(z) - f(-z)) = g_1(z) + g_2(z),$$

where the first part is even and the second part is odd. Then assuming the second statement, we have $g_1(z) \in \mathbb{C}(\wp(z))$. Now let $g$ be an odd elliptic function, then $g(z) = \wp'(z)h(z)$ where $h$ is an even function. Hence $h \in \mathbb{C}(\wp(z))$ and so $g \in \mathbb{C}(\wp(z), \wp'(z))$. Therefore, each function $f \in \mathbb{C}(\wp(z), \wp'(z))$.

To prove the second statement, we may assume that $f(z) \neq 0, \infty$ for $z = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Otherwise, we can replace the given function $f(z)$ by some $a + \frac{1}{f(z)+b}$ which is again elliptic such that $f(z) \neq 0$ at the above points, and the result will be the same as $a, b$ are just constants.

Suppose now $f(z) = 0$ or $\infty$ at $\pm z_i$ (as it is even) and let $h_i = ord_{z_i} f$. Set

$$g(z) = \prod_i (\wp(z) - \wp(z_i))^{n_i}.$$

Notice that $\wp(z)-\wp(z_i)$ has simple zero $z_i$. Then we claim $\frac{f(z)}{g(z)}$ has no zeros or poles on $\mathbb{C}/\Lambda$. Indeed, it clearly has no zeros. For poles, we use the fact that $\sum_i n_i = 0$, using Lemma 26.14(3) and so the double poles introduced by each $\wp(z) - \wp(z_i)$ will be canceled out. But the function $\frac{f(z)}{g(z)}$ is again elliptic and so it has no zeros or poles in $\mathbb{C}$. So it is analytic, and hence it is constant by Lemma 26.14(1). So $f(z) \in \mathbb{C}(g(z)) \subset \mathbb{C}(\wp(z))$. □

**Theorem 26.24.** *Let $\Lambda$ be a lattice in $\mathbb{C}$. Then*

$$E_\Lambda : y^2 = 4x^3 - 60G_4x - 140G_6$$

*defines an elliptic curve over $\mathbb{C}$ and the map*

$$\theta : \mathbb{C}/\Lambda \longmapsto E_\Lambda(\mathbb{C})$$

*via*

$$\theta(z) = (\wp(z), \wp'(z)), \theta(0) = \mathcal{O}$$

*is an isomorphism.*

*Proof.* By earlier remark, the map has the correct image. Suppose $x = \wp(z_0)$ for some $z_0 \in \mathbb{C}$. Then we have shown that $\wp(z) - \wp(z_0)$ only have double poles at 0 in $\mathbb{C}/\Lambda$, and so it has two zeros in $\mathbb{C}/\Lambda$, say $z_0$ and $z_1$ where they are not necessarily distinct. But clearly $-z_0$ goes to $(\wp(z_0), -\wp'(z_0))$ in the image. We shall discuss the cases $\wp'(z_0) = 0$ and $\wp'(z_0) \neq 0$ separately.

Recall $\wp'(z)$ is an odd function and it is also periodic, thus

$$\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(\frac{\omega_1}{2} - \omega_1\right) = \wp'\left(-\frac{\omega_1}{2}\right) = -\wp'\left(\frac{\omega_1}{2}\right).$$

So $\wp'\left(\frac{\omega_1}{2}\right) = 0$. Similarly, $\frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ are also zeros of $\wp'(z)$. But the value of $\wp$ at these three points are all distinct, because if not, say

$$\wp\left(\frac{\omega_1}{2}\right) = \wp\left(\frac{\omega_2}{2}\right).$$

Then $\wp(z) - \wp\left(\frac{\omega_1}{2}\right)$ has a double zero at $\frac{\omega_1}{2}$ and also a zero at $\frac{\omega_2}{2}$, which is impossible. Also, notice that $\wp'(z)$ has a triple pole at 0 in $\mathbb{C}/\Lambda$ and hence these are the only zeros of $\wp'(z)$.

Now if $\wp'(z_0) \neq 0$. Then we see $z_0$ and $-z_0$ give different images. Therefore, the map is injective. But by Theorem 26.20, the map is surjective as each point $(x, y)$ has a preimage (as the identity holds for each $z$). So it is bijective.

To check it is homomorphism, it is clear that $\wp(0) = \mathcal{O}$. Given $\alpha_1, \alpha_2$ and images $P_1, P_2$. Let $P_3 = \ominus(P_1 \oplus P_2)$, and let $\alpha_3$ be the preimage of $P_3$. In other words, there is a line through $P_1, P_2$ and $P_3$. Let $L$ have equation $ax + by + c = 0$. Then

$$a\wp(z) + b\wp'(z) + c = 0.$$

has zeros at $\alpha_1, \alpha_2, \alpha_3$ and it has triple poles at $z = 0$. So each zero is simple, and by Lemma 26.14(4) we have $\alpha_1 + \alpha_2 + \alpha_3 \in \Lambda$. Hence, in $\mathbb{C}/\Lambda$, $\alpha_1 + \alpha_2 + \alpha_3 = 0$. So in fact, the map from $E_\Lambda$ to $\mathbb{C}/\Lambda$ is a homomorphism, and since it is bijective so it is isomorphism. □

**Remark 26.25.** *The result shows that $(E_\Lambda, \oplus)$ is a group. In particular, $\oplus$ is associative because clearly $+$ is associative in $\mathbb{C}/\Lambda$.*

**Theorem 26.26.** **[Uniformlisation Theorem]** *Every elliptic curve over $\mathbb{C}$ is isomorphic to $E_\Lambda$ for some $\Lambda$. In other words, given*

$$y^2 = 4x^3 - 60ax - 140b,$$

*non-singular, there is a lattice $\Lambda$ such that $G_4(\Lambda) = a, G_6(\Lambda) = b$. Further, for each elliptic curve of the form $E : y^2 = x^3 + Ax + B$, there exists a lattice $\Lambda$ and the map*

$$\theta(z) = \left(\wp(z), \frac{\wp'(z)}{2}\right),$$

*is an isomorphism from $\mathbb{C}/\Lambda$ to $E$.*

We are not going to prove this theorem here.

**Corollary 26.27.** *Let $K$ be a number field and $E/K$ is an elliptic curve over $K$. Then*

$$E(K)[n] \leq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

*where for any abelian group $A[n]$ means the subgroup of $A$ consisting of elements of order dividing $n$.*

*Proof.* $E(\mathbb{C}] \cong E_\Lambda(\mathbb{C}) \cong \mathbb{C}/\Lambda$ by uniformalisation theorem and the previous theorem. Then in $\mathbb{C}/\Lambda$, the subgroup of elements of order dividing $n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since $K$ is a number field, and so $K \subset \mathbb{C}$. Thus, $E(K) \leq E(\mathbb{C})$ and so the result follows. □

**Corollary 26.28.** *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over a field $K$ such that Char$(K) = 0$. Then $(E(K), \oplus)$ is a group.*

*Proof.* The only part we have not checked is associativity. Let $P_i = (x_i, y_i), i = 1, 2, 3$. Let $F = \mathbb{Q}(a_1, a_2, a_3, a_4, a_6, x_1, x_2, x_3, y_1, y_2, y_3) \subset K$. Then (see Exercises) we have an embedding $F \hookrightarrow \mathbb{C}$. So we can regard $E$ as an elliptic curve over $F \subset \mathbb{C}$ and we know

$$P_1 \oplus (P_2 \oplus P_3) = (P_1 \oplus P_2) \oplus P_3$$

over $\mathbb{C}$ and hence true in $F$. □

## 26.3 Height

**Definition 26.29.** *For $\alpha \in \mathbb{Q}$, write $\alpha = \frac{p}{q}$, where $(p, q) = 1$. Define $H(\alpha) = \max(|p|, |q|)$. Then the* **height** *of $\alpha$ is defined to be $h(\alpha) = \log H(\alpha)$. For convention, define $H(0) = 1$ and $h(0) = 0$.*

**Proposition 26.30.** *(1) $h(\alpha) \geq 0$ for all $\alpha \in \mathbb{Q}$, with equality if and only if $\alpha = 0, \pm 1$.*

*(2) $h(\alpha^d) = dh(\alpha)$.*

*(3) If*

$$f(x) = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \in \mathbb{Q}(X)$$

*has degree $d$, where we define $d = \max m, n$. Then $h(f(\alpha)) = dh(\alpha) + O(1)$, where the constant $O(1)$ does not depend on $\alpha$. In other words, there exists $C$ such that*

$$dh(\alpha) - C \leq h(f(\alpha)) \leq d(h(\alpha)) + C.$$

*(4) The set $\{\alpha \in \mathbb{Q} : h(\alpha) \leq C\}$ is finite for all $C > 0$.*

*Proof.* (1) Clear.

(2) If $|m| > |n|$ then $|m|^d > |n|^d$. Also, use $\log n^d = d \log n$.

(3) Assume $n \geq m$. If $n < m$ then we can consider the function $g(x) = f(x^{-1})$ and the argument is then similar. We have

$$f\left(\frac{S}{T}\right) = \frac{a_n S^n + \cdots + a_0 T^n}{(b_m S^m + \cdots + b_0 T^m) T^{n-m}} = \frac{A(S,T)}{B(S,T)}.$$

Then

$$\begin{aligned} H(\alpha) &\leq \max\left(|A(p,q)|, |B(p,q)|\right) \leq (n+1) \max_i(|a_i|, |b_i|) \max(|p|^n, |q|^n) \\ &\leq (n+1) \max_i(|a_i|, |b_i|) H(\alpha)^d. \end{aligned}$$

Hence $h(\alpha) \leq C + dh(\alpha)$, where $C$ only depends on the degree of $f$ and the coefficients.

Conversely, $A(S,1)$ and $B(S,1)$ are coprime in $\mathbb{Z}[S]$. Then there exists $\psi(S), \phi(S)$ such that

$$A(S,1)\psi(S) + B(S,1)\phi(S) = d_1 \in \mathbb{Z}.$$

(The easiest way to see this is by Gauss's lemma so $A(S,1)$ and $B(S,1)$ are coprime over $\mathbb{Q}[S]$, then apply Euclidean algorithm and clear denominator.) Now homogenize, so we have $\psi_1(S,T)$ and $\phi_1(S,T)$ such that

$$A(S,T)\psi_1(S,T) + B(S,T)\phi_1(S,T) = d_1 T^N$$

for some $N$. Similarly, there exist $\psi_2(S,T)$ and $\phi_2(S,T)$ such that

$$A(S,T)\psi_2(S,T) + B(S,T)\phi_2(S,T) = d_2 S^M$$

for some $M$. Now for $\alpha = \frac{p}{q}$ where $(p,q) = 1$. From above we see that the common divisor of $A(p,q)$ and $B(p,q)$ must divide $d_1 q^N$ and $d_2 p^M$. Hence it must divide $d_1 d_2$ as $(p,q) = 1$. Then let $d = (A(p,q), B(p,q))$, we have

$$H(f(\alpha)) = \frac{\max(|A(p,q)|, |B(p,q)|)}{d(p,q)} \geq \frac{\max(|A(p,q)|, |B(p,q)|)}{d_1 d_2}.$$

For $|p|, |q|$ large enough we have

$$|A(p,q)|, |B(p,q)| \geq \max\left(\left|\frac{p}{2}\right|, \left|\frac{q}{2}\right|\right)^n.$$

For $|p|, |q|$ small we can use a constant multiple to correct the error, hence we conclude that

$$H(\alpha) \geq \frac{C'}{d_1 d_2} \max\left(\left|\frac{p}{2}\right|, \left|\frac{q}{2}\right|\right)^n.$$

Hence, $H(f(\alpha)) \geq C' H(\alpha)^d$ for some constant $C'$ and so

$$h(\alpha) \geq C + h(\alpha).$$

Also from the above, we see that again the constant $C$ depends only on the degree of $f$ and also $d_1 d_2$ is independent of $\alpha$.

(4) $h(\alpha) \leq C$ if and only if $H(\alpha) \leq C'$ for some $C'$ and so the number of such $\alpha$ is finite.

□

We shall now extend the definition of height.

**Definition 26.31.** *Let $K$ be a number field. The set $\Sigma_K$ of normalised absolute values of $K$ consists of*

*(i)* $|\cdot|_{\mathfrak{p}} = \frac{1}{N(\mathfrak{p})}^{v_{\mathfrak{p}}(\cdot)}$, *where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$.*

*(ii)* $|\cdot|_\sigma = |\sigma(\cdot)|$ *for each real embedding $\sigma : K \hookrightarrow \mathbb{R}$.*

*(iii)* $|\cdot|_\sigma = |\sigma(\cdot)|^2$ *for each pair of complex mbedding $\sigma : K \hookrightarrow \mathbb{R}$.*

**Definition 26.32.** *For $\alpha \in K$. Define*

$$H_K(\alpha) = \prod_{v \in \Sigma_K} \max(1, |\alpha|_v),$$

*and $h_K(\alpha) = \log H(\alpha)$. Again for convention, let $H_K(0) = 1, h_K(0) = 0$.*

**Proposition 26.33.** *Let $K$ be a number field.*

*(1)* $h_K(\alpha) \geq 0$, *with equality if and only if $\alpha = 0$ or $\alpha$ is a root of unity in $K$.*

*(2)* $h_K(\alpha^d) = dh_K(\alpha)$.

*(3) Let $f \in K(X)$ of degree $d$. Then $h_K(f(\alpha) = d(h(\alpha)) + O(1)$, where the constant $O(1)$ is independent of $\alpha$.*

*(4) The set $\{\alpha \in K : h_K(\alpha) < C\}$ is finite.*

*Proof.* (1) $h(\alpha) \geq 0$ is clear. $h(\alpha) = 0$ if and only if $H(\alpha) = 1$. If $\alpha \neq 0$, then $H(\alpha) = 1$ if and only if the valuation of $\alpha$ is less than or equal to 1 for all $v \in \Sigma_K$. Then $\alpha \in \mathcal{O}_K$. Hence the norm $N(\alpha)$ is an integer. In particular this means that $|\prod_i \sigma_i(\alpha)|$ is an integer. But each $|\sigma_i(\alpha)| \leq 1$ and $N(\alpha) \neq 0$. So we must have each $|\sigma_i(\alpha)| = 1$ and $N(\alpha) = 1$. Now $\mathcal{O}_K$ is a lattice and so the intersection of $\mathcal{O}_K$ with $\{z \in \mathbb{C} : |z| = 1\}$ is finite. So each of them must be root of unity.

(2) Clear.

(3) This is similar to the case in $\mathbb{Q}$. We need the identity from local fields, that

$$\prod_v |x|_v = 1, \ \forall x \in K^*.$$

Then if we write $\alpha = \frac{x}{y}$ where $x, y \in \mathcal{O}_K$, and we have no prime ideal dividing both $x$ and $y$. Then it is clear that the part of product which runs through finite places (i.e. primes) is

$$\prod_{\mathfrak{p}} |y|_{\mathfrak{p}}^{-1} = N(y).$$

So in fact,

$$H(\alpha) = N(y) \prod_{\sigma_i} \max(1, |\sigma_i(\alpha)|).$$

By suitable relabeling we may assume that $|\sigma_i(x)| \geq |\sigma_i(y)|$ for $i = 1, \ldots, r$ and $|\sigma_i(x)| < |\sigma_i(y)|$ for $i > r$. Then we have

$$H(\alpha) = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{i>r} |\sigma_i(y)| = \prod_i \max(|\sigma_i(x)|, |\sigma_i(y)|).$$

Since $\sigma_i(f(\alpha)) = f(\sigma_i(\alpha))$, then writing

$$f(S,T) = \frac{A(S,T)}{B(S,T)}, x_i = \sigma_i(x), y_i = \sigma_i(y)$$

we have

$$H\left(f\left(\frac{x}{y}\right)\right) = \prod_i \max(|A(x_i, y_i)|, |B(x_i, y_i)|).$$

Then the first inequality follows in the same way as before. For the second inequality, note that this time we get $d_1$ and $d_2 \in \mathcal{O}_K$. The rest is just similar, apart from that this time we need to take the product.

(4) Notice that if $H_K(\alpha) \leq C'$, then there are only finitely many units $u$ such that $H_K(u\alpha) \leq C'$. Indeed, by Dirichlet's unit theorem, we may write $u$ as a product of fundamental units. Suppose $u_i$ is a fundamental unit, then there exists $N$ large enough such that we have a conjugate of $u_i^N$ which is greater than $C'$. Hence, we only have finitely many units $u$ such that every conjugate of $u$ is less than or equal to $C'$. Then, to prove there are only finitely many such $\alpha$, it is equivalent to prove there are finitely many such $\alpha$ modulo units.

By previous discussion, if $\alpha = \frac{x}{y}$, then $N(y) \leq H(\alpha) \leq C'$. But since we can ignore the units now, so it is the same as finding how many principal ideals $\langle y \rangle$ there are, whose norm is less than or equal to $C'$. But we only have finitely many integral principal ideal $I$ such that $N(I) \leq C'$ by Proposition 16.20. Therefore, we conclude that there are only finitely many such $\alpha$.

□

**Definition 26.34.** *Let $K$ be a number field and $E : y^2 = x^3 + Ax + B$ where $A, B \in K$ be an elliptic curve over $K$. For $P = (a, b) \in E(K)$, the height of $P$, written $h_E(P)$ is defined by*

$$h_E(P) = h_K(a),$$

*and for convention define $h_E(\mathcal{O}) = 0$.*

**Remark 26.35.** *The height of $P$ only depends on the $x$-coordinate of $P$.*

**Lemma 26.36.** *The set $\{P \in E(K) : h_E(P) < C\}$ is finite for all $C > 0$.*

*Proof.* We only have finitely many choices for the $x$-coordinate of $P$ and hence finitely many choices for $P$. □

**Lemma 26.37.** *Let $E$ be an elliptic curve over a field $K$ of Char$(K) = 0$. Then*

$$h_E(mP) = m^2 h_E(P) + O(1),$$

*where the constant $O(1)$ is independent of $P$, but it depends on $m$.*

*Proof.* We claim that there exists $f(x) \in K(X)$ of degree $m^2$ such that, if $P = (a, b)$, then $mP = (f(a), *)$. Since the height of a point only depends on $x$-coordinate so we don't care about the $y$-coordinate.

Firstly, apply the group law $m$ times we have $mP = (F(a, b), *)$. Let

$$F(x, y) = g_1(x, y^2) + yg_2(x, y^2),$$

as $\{1, y\}$ is a basis for $K(x, y)/K(x, y^2)$. But on $E$,

$$y^2 = x^3 + Ax + B.$$

So if we replace $y^2$ by a $x^3 + Ax + B$, and so $g_1$ and $g_2$ are both functions in $x$, and rewrite

$$F(x, y) = g_1(x) + yg_2(y).$$

By using uniformlisation theorem, and embedding $K$ into $\mathbb{C}$, we have that if $P = (a, b) = \left(\wp(z), \frac{\wp'(z)}{2}\right)$, then

$$mP = \left(\wp(mz), \frac{\wp'(mz)}{2}\right).$$

Then in the above notation, we have

$$\wp(mz) = g_1(\wp(z)) + \frac{\wp'(z)}{2} g_2(\wp(z)).$$

But $\wp(z)$ is even and $\wp'(z)$ is odd, so replace $z$ by $-z$ above, we see that $g_2(\wp(z)) = 0$. Hence, $\wp(mz) = g_1(\wp(z))$, i.e. $F(x, y) = g_1(x)$ which is a function of $x$.

Finally, to check that $g_1(x)$ has degree $m^2$, we count the number of poles. It is clear that $\wp(mz)$ has $m^2$ poles and so the degree of $g$ is $m^2$. Thus we have proved the claim. The results follows by applying Proposition 26.30(3). □

**Theorem 26.38.** [**Parallelogram Law**] *With the same setting as above, we have*

$$h(P \oplus Q) + h(P \ominus Q) = 2h(P) + 2h(Q) + O(1),$$

*where the constant is independent of $P$ and $Q$.*

*Proof.* We only need to prove that

$$h(R_1 \oplus R_2) + h(R_1 \ominus R_2) \leq 2h(R_1) + 2h(R_2) + C,$$

because then for the other inequality we pick $R_1 = P \oplus Q$ and $R_2 = P \ominus Q$, then

$$h(2P) + h(2Q) \leq 2h(P \oplus Q) + 2h(P \ominus Q).$$

But $h(2P) = 4h(P) + O(1)$ where the constant is independent of $P$ and similarly for $h(2Q)$. Hence,

$$h(P \oplus Q) + h(P \ominus Q) \leq 2h(P) + 2h(Q) + C'.$$

We shall prove this for $\mathbb{Q}$. (For general number fields, it takes some computation of algebra.) But even in $\mathbb{Q}$, we need a long (but elementary) calculation, to conclude that, if $\alpha + \beta = \frac{m}{t}$ and $\alpha\beta = \frac{n}{t}$, then

$$h(\alpha) + b(\beta) = \log(\max(|m|, |n|, |t|)) + O(1),$$

where the constant is independent of $m, n, t$. Then let $x_{R_i}$ be the $x$-coordinate of $R_i$. Let $x_{R_1} + x_{R_2} = \frac{u_1}{u_3}, x_{R_1} x_{R_2} = \frac{u_2}{u_3}$, and we find that

$$x_{R_1 \oplus R_2} + x_{R_1 \ominus R_2} = \frac{v_1}{v_3}, x_{R_1 \oplus R_2} x_{R_1 \ominus R_2} = \frac{v_2}{v_3},$$

where

$$v_1 = 2Au_1u_3 + 2u_1u_3 + 4Bu_3^2,$$
$$v_2 = u_2^2 - 2Au_2u_3 - 4Bu_1u_3 + A^2u_3^2,$$
$$v_3 = u_1^2 - 4u_2u_3.$$

So we conclude

$$\begin{aligned} h(R_1 \oplus R_2) + h(R_1 \ominus R_2) &= \log(\max(|v_1|, |v_2|, |v_3|)) + C \\ &= \log(\max(|u_1^2|, |u_2^2|, |u_3^2|)) + C' \\ &= 2h(R_1) + 2h(R_2) + C'', \end{aligned}$$

where in the second line we use the fact that $v_i$'s are quadratic in $u_i$'s and we can see the constants are independent of $u_i$. □

**Theorem 26.39. [Canonical Height]** *There exists a unique function $\hat{h} : E(K) \longmapsto \mathbb{R}$, such that*

*(i)* $\hat{h}(P) = h(P) + O(1)$, *where the constant is independent of the point $P$.*

*(ii)* $\hat{h}(mP) = m^2\hat{h}(P)$.

*It also satisfies the following:*

*(iii)* $\{P \in E(K) : \hat{h}(P) < C\}$ *is finite for all $C > 0$.*

*(iv)* $\hat{h}(P \oplus Q) + \hat{h}(P \ominus q) = 2\hat{h}(P) + 2\hat{h}(Q)$.

*(v)* $\hat{h}(P) \geq 0$ *for all $P$ and $\hat{h}(P) = 0$ if and only if $P$ has finite order.*

*(vi) The height pairing defined by*

$$\langle P, Q\rangle = \hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q)$$

*is bilinear. So $\hat{h}$ is a quadratic form.*

*Proof.* Set $\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}$ for each $P$. We have for $n < m$

$$|4^{-n}h(2^nP) - 4^{-m}h(2^mP)| \leq \sum_{j=n}^{m-1} |4^{-j}h(2^jP) - 4^{-(j+1)}h(2^{j+1}P)|.$$

Now, we have $h(2^{n+j}P) = 4h(2^{n+j-1}P) + C$, where $C$ is independent of $P$ and $n, j$, so we conclude that

$$|4^{-n}h(2^nP) - 4^{-m}h(2^mP)| \leq \sum_{j=n}^{m-1} \frac{C}{4^j} \to 0$$

as $n \to \infty$. So $4^{-n}h(2^nP)$ is a cauchy sequence in $\mathbb{R}$ and hence the sequence converges. So the limit is well-defined.

Now we have $h(2^nP) = 4^nh(P) + O(1)$ where $O(1)$ depends on $n$, but not $P$. Since the limit exsits, so we know that $\hat{h}(P) - h(P)$ is just a constant. In fact we could set

$$h_n(P) = 4^{-n}h(2^nP) - h(P),$$

and we know the limit exists, so the difference is a constant which is independent of $P$. Also, $h(2^n mP) = m^2 h(2^n P) + O(1)$, where $O(1)$ only depends on $m$. So let $n \to \infty$, we have $4^{-n}O(1) \to 0$ because $m$ is fixed. Thus, we have

$$\hat{h}(mP) = \lim_{n \to infty} 4^{-n} h(2^n mP) = \lim_{n \to \infty} 4^{-n}(m^2 h(2^n P) + O(1)) = m^2 \hat{h}(P).$$

It is also unique, because, say $h_1, h_2$ are functions which also satisfies properties (i) and (ii). Then by (i), we have

$$h_1(P) - h_2(P) = O(1), \ \forall P$$

where the constant is independent of $P$. In particular, $|h_1(P) - h_2(P)| \leq C$ for some constant $C$. Then

$$|h_1(mP) - h_2(mP)| \leq C, \ \forall m, P.$$

But by (ii), this implies that

$$|h_1(P) - h_2(P)| \leq \frac{C}{m^2}, \ \forall m, P.$$

Hence, $|h_1(P) - h_2(P)| = 0$ for all $P$ and so $h_1 = h_2$.

Then we check it satisfies other properties. (iii) is clear by using (i) and Lemma 26.36. For (iv), consider

$$4^{-n}[h(2^n(P \oplus Q)) + h(2^n(P \ominus Q))] = 4^{-n}[2h(2^n P) + 2h(2^n Q) + O(1)],$$

where the constant $O(1)$ is independent of $P, Q$ and $n$. Then as $n \to \infty$, we have $4^{-n}O(1) \to 0$. Therefore (iv) is also clear.

For (v), we know that $h(P) \geq 0$ for all $P$. Hence $4^{-n}h(2^n P) \geq 0$, for all $n, P$. Then by elementary analysis, we know that the limit of a sequence of non-negative numbers cannot be negative. So $\hat{h}(P) \geq 0$. Suppose $P$ has finite order, say $mP = \mathcal{O}$, then by (ii) we have

$$0 = \hat{h}(\mathcal{O}) = m^2 \hat{h}(P),$$

and so $\hat{h}(P) = 0$. Conversely, suppose $\hat{P} = 0$. Then $\hat{h}(mP) = 0$ for all $m$. By (iii), we only have finitely many $Q \in E(K)$ such that $h(\hat{Q}) = 0$, so there exists some $m$ such that $mP = \mathcal{O}$.

For (vi), clearly the form is symmetric, so it suffices to check it is linear in one component. We want to check

$$\langle P \oplus Q, R \rangle = \langle P, R \rangle + \langle Q, R \rangle.$$

In other words, we need

$$\hat{h}(P \oplus R) + \hat{h}(Q \oplus R) - \hat{h}(P) - \hat{h}(Q) - 2\hat{h}(R) = \hat{h}(P \oplus Q \oplus R) - \hat{h}(P \oplus Q) - \hat{h}(R).$$

Consider the difference of the above, which is

$$\hat{h}(P \oplus Q \oplus R) - \hat{h}(P \oplus Q) - \hat{h}(P \oplus R) - \hat{h}(Q \oplus R) + \hat{h}(P) + \hat{h}(R) + \hat{h}(Q).$$

We want to use (iv). For simplicity, we use $(P, Q)$ to mean that we apply (iv) to the points $P$ and $Q$. Then, we have the following identities,

$$(P \oplus Q, R) \Rightarrow \hat{h}(P \oplus Q \oplus R) + \hat{h}(P \oplus Q \ominus R) = 2\hat{h}(P \oplus Q) + 2\hat{h}(R).$$

$$(P, R \oplus Q) \Rightarrow \hat{h}(P \oplus Q \oplus Q) + \hat{h}(P \ominus R \ominus Q) = 2\hat{h}(P) + 2\hat{h}(R \oplus Q).$$

$$(P \ominus R, Q) \Rightarrow \hat{h}(P \oplus Q \ominus R) + \hat{h}(P \ominus R \ominus Q) = 2\hat{h}(P \ominus R) + 2\hat{h}(Q).$$

Then take the sum of the first two identities and subtract the third one, we have

$$2\hat{h}(P \oplus Q \oplus R) = 2\hat{h}(P \oplus Q) + 2\hat{h}(R) - 2\hat{h}(P \ominus R) - 2\hat{h}(Q) + 2\hat{h}(P) + 2\hat{h}(R \oplus Q).$$

Then use $\hat{h}(P \ominus R) = 2\hat{h}(P) + 2\hat{h}(R) - \hat{h}(P \oplus R)$ on right hand side and the result follows. $\square$

**Corollary 26.40.** *Let $E/K$ be an elliptic curve of number field. Then $E(K)$ has finitely many points of finite order.*

*Proof.* By previous theorem $P$ has finite order if and only if $\hat{h}(P) = 0$. But there are only finitely many such $P$, again by previous theorem. □

**Remark 26.41.** *All the $O(1)$ constants can be made explicitly and $\hat{h}$ can be computed to desired accuracy.*

## 26.4 Exercises

1. Let $E$ be the elliptic curve given by

$$y^2 - y = x^3 - x^2.$$

Verify that the point $P = (0, 0)$ has order 5.

2. Find all points of order 2 on the elliptic curve

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma).$$

3. Determine the group $E(\mathbb{F}_3)$ for the elliptic curves

$$E : y^2 = x^3 - x \quad \text{and} \quad E : y^2 = x^3 + x.$$

4. Let $E$ and $E'$ be two elliptic curves over a field $K$ given by Weierstrass equations. Show that if the elliptic curves $E$ and $E'$ are isomorphic, then so are the groups $E(K)$ and $E'(K)$.

5. Let $E$ be the elliptic curves given by $y^2 = x^3 + Ax + B$ with $A, B \in K$, a field of characteristic zero. Prove the duplication formula: if $P = (x_1, y_1) \in E(K)$, then $P \oplus P = (\lambda^2 - 2x_1, \lambda^3 - 3\lambda x_1 + y_1)$, where $\lambda = \frac{3x_1^2 + A}{2y_1}$.

6. Let $E/\mathbb{Q}$ be an elliptic curve that has a rational point of order 3. Show that $E$ is isomorphic to one of the form

$$y^2 = x^3 + a^2(x - b)^2.$$

7. Find all elliptic curves over $\mathbb{F}_3$ up to isomorphism.

8. Let $E/\mathbb{C}$ be an elliptic curve given by

$$y^2 = x^3 + Ax + B,$$

and let $m \geq 1$ be an integer. Show that there is some rational function $f$ such that for every point $P = (x_1, y_1) \in E(\mathbb{C})$, the $y$-coordinate of $mP$ is $y_1 f(x_1)$.

9. Let $E/K$ be an elliptic curve over a field of characteristic zero. Prove that

$$E(\bar{K})_{\text{tors}} \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

10. Let $E$ be an elliptic curve over $\mathbb{F}_p$ given by a Weierstrass equation. Prove that the operation $\oplus$ is associative. (Hint: Write $E$ as the reduction mod $p$ of a suitable elliptic curve with coefficients in $\mathbb{Z}_p$. You will need Hensel's Lemma to life points from $\mathbb{F}_p$ to $\mathbb{Z}_p$.)

11. Prove that every finitely generated field extension of $\mathbb{Q}$ can be embedded into $\mathbb{C}$.

12. Prove that the definitions of height on $\mathbb{Q}$ agree, i.e. that for $x = \frac{n}{m}$ with $n, m \in \mathbb{Z}\backslash\{0\}$ copirme,

$$\max(|n|, |m|) = \max(1, |x|) \cdot \prod_p \max(1, |x|_p)$$

where $\left|p^r \frac{a}{b}\right|_p = p^{-r}$ for $p \nmid a, b$.

13. Let $E/\mathbb{Q}$ be an elliptic curve given by $E : y^2 = x^3 + Ax + B$, and let $P \in E(\mathbb{Q})$. For each $n \geq 1$ write $nP = (x_n, y_n)$. Prove that

$$h_{\mathbb{Q}}(x_n) = n^2 a + O(1) \text{ and } h_{\mathbb{Q}}(y_n) = \frac{3}{2} n^2 a + O(1),$$

where the constant $a \in \mathbb{R}$ and the error terms $O(1)$ may depends on $E$ and $P$, but not on $n$.

## 26.5 Hint and Solutions

1. $\frac{dy}{dx} = \frac{3x^2-2x}{2y-1} = 0$ at $(0,0)$. So the tangent is $y = 0$. Then we have $x = 0$ or 1. Thus $-(P \oplus P) = (1,0)$. When $x = 1$, $y = 0$ or 1 so $P \oplus P = (1,1)$. Similarly we have $\ominus 4P = (0,0) = P$. Thus $5P = \mathcal{O}$.

2. $P$ has order two if and only if $P = \ominus P$. If $P = (x,y)$ then $\ominus P = (x,-y)$ and so we need $(x,y) = (x,-y)$ which implies that $y = 0$. Then $x = \alpha, \beta$ or $\gamma$.

3. For the first one, $y^2 = x(x-1)(x-2)$, the set of points of order 2 is $\{\mathcal{O}, (0,0), (1,0), (2,0)\}$. Note that we have at most 7 points, and we have $(\mathbb{Z}/2\mathbb{Z})^2$ inside the group so it must be $(\mathbb{Z}/2\mathbb{Z})^2$.

   In $\mathbb{F}_3$, we know $x^3 = x$ and so $y^2 = x^3 + x = 2x$. So the only points are $\mathcal{O}, (0,0), (2, \pm 1)$. Now the point $P = (2,1)$ has order 4 so the group is $\mathbb{Z}/4\mathbb{Z}$.

4. The substitution $x' = u^2 x + r, y' = u^3 y + u^2 s x + t$ will take each line to another line. Then by construction of $P \oplus Q$, we could get the corresponding point in the image, say $\phi(P) \oplus \phi(Q)$. Also, the map will preserve the multiplicity (as it preserves tangents).

   Alternatively we can just use direct computation to find the equation of the resulting curve and corresponding points.

5. $P = (x_1, y_1) \in E(K)$. Then $\frac{dy}{dx} = \frac{3x^2+A}{2y} = \lambda$ at $P$. So $y - y_1 = \lambda(x - x_1)$ and so the line is $y = \lambda(x - x_1) + y_1$. Then substitute this into the equation

$$y^2 = \lambda^2 (x - x_1)^2 + y_1^2 + 2\lambda y_1 (x - x_1) = x^3 + Ax + B.$$

   We know $x_1$ is a double root, and so we will find the last root is $x = \lambda^2 - 2x_1$. Then $y = \lambda^3 - 3\lambda x_1 + y_1$.

6. Without loss of generality we may assume $P = (0, b)$. Let $y^2 = x^3 + Ax^2 + Bx + C$, then $C = b^2$. $\frac{dy}{dx} = \frac{3x^2+2Ax+B}{2y} = \frac{B}{2b^2}$ at $P$. Since $P$ has order 3, so $P \oplus P = \ominus P$. Thus, by definition, the tangent of $P$ intersects $E$ at $P$ only.

   Then $y^2 = \frac{B^2}{4b^2}x^2 + b + Bx = x^3 + Ax^2 + Bx + C$. This has solution at 0 only because the line only intersects the curve at $P$. Thus, it has to be $x^3$. Then we compare the coefficient, we have $A = \frac{B^2}{4b^2} = a^2$ and so $B = 2ab$. We have $y^2 = x^3 + a^2\left(x + \frac{b}{a}\right)^2$.

7. The only transforms are linear ones, i.e. $x = x' + r, y = uy'$, using $u^2 = 1$ in $\mathbb{F}_3$. We have

$$y^2 = x^3 + ax^2 + c, y^2 = x^3 + x + 1, y^2 = x^3 - x + c$$

   where $a, b, c$ are variables in $\mathbb{F}_3$ such that the curve is not singular.

8. Induction on $m$. The $x$-coordinate is a rational function of $x$ (which we have proved but we will give another proof by induction). This is true when $m = 1$. Suppose it is true for $m$, say $mP = (f(x_1), y_1 g(x_1))$. Then the line through $P, mP$ is $y - y_1 = \lambda(x - x_1)$, where $\lambda = \frac{y_1 g(x_1) - y_1}{f(x_1) - x_1} = y_1 h(x_1)$ where $h$ is a rational function. Then $y = y_1 x - y_1(x_1 h(x_1) + 1) = y_1 x - y_1 k(x_1)$ where $k$ is a rational function.

   Now $y^2 = y_1^2(x - k(x_1))^2 = x^3 + Ax + B$. We know $y_1^2 = x_1^3 + Ax_1 + B = u(x_1)$. So

$$u(x_1)(x - k(x_1))^2 = x^3 + Ax + B$$

   has roots $x = x_1, x = f(x_1)$. So we divide this by $(x - x_1)(x - f(x_1))$, we still have a rational function. Thus, $y = y_1(x - x_1 h(x_1) - 1) = y_1 G(x_1)$ for some rational function $G_1$.

9. $\mathrm{Char}(K) = 0$ so $\mathbb{Q} \subset K$. Let $F_m = \mathbb{Q}(a_1, a_2, a_3, a_4, a_6, x_{m,1}, \ldots, y_{m,1}, \ldots)$ where $(x_{m,i}, y_{m,i})$'s are the coordinates of the $m$-torsions. The number of $m$-torsions is finite. Suppose $mP = \mathcal{O}$, by the previous question, if $P = (x, y)$, then $mP = (f(x), g(x)y)$. Further, we know $f(x)$ has degree $m^2$. So there are finitely many $x$ such that $f(x)$ is infinity. So $F_m$ is a subfield of $\mathbb{C}$ (see the last question).

   Now in $\mathbb{C}$, in the lattice $\Lambda$, we have $m^2$ points such that $m\alpha = 0$. Then apply uniformlisation theorem, we have $m^2$ points in $\bar{F}_m$ such that $mP = \mathcal{O}$. Then

$$E(\bar{F}_m)[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

   Now take the union of these we have the torsion subgroup

$$E(\bar{K})_{\mathrm{tors}} \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

   Alternatively, let $F = \bigcup_{n=1}^{\infty} F_m$ and so $\bar{F} \subset \bar{K}$. So $F \subset \mathbb{C}$. Now work in $\bar{F}$.

10. For any point $(a, b) \in E$, since the curve is smooth so

$$\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}\right)_{(a,b)} \neq 0.$$

    Thus by Hensels' Lemma, we have $(x, y) \in \mathbb{Z}_p^2$ such that $(x, y)$ gives the solution if the curve. In other words, we can lift the curve in $\mathbb{Z}_p$. Then $\mathrm{Char}(\mathbb{Q}_p) = 0$ so the result follows by the theorem.

11. Since all finite extensions are algebraic so it suffices to show that we can do it for infinite extension. The extension is separable so it is $\mathbb{Q}(x_1, \ldots, x_m)$. Further, we may assume that none of $x_i$ satisfies any algebraic relation, because we are done with the finite extensions. Now it is clear that $\mathbb{Q}(x_1, \ldots, x_m)$ is countable, because each element can be written as a polynomial in $x_1, \ldots, x_m$, with coefficients in $\mathbb{Q}$.

    The set of transcendental numbers is uncountable. So we can send $x_1$ to some transcendental number. Then for $x_2$, we may assume $x_2$ is algebraically independent of $x_1$, otherwise it is a finite extension. Then we can send $x_2$ to a transcendental number and so on. Therefore, we can embed $\mathbb{Q}(x_1, \ldots, x_m)$ into $\mathbb{C}$.

12. If $|n| \geq |m|$ then $|x| \geq 1$. Then

$$\prod_p \max(1, |x|_p) = \prod_p \max\left(1, \left|\frac{n}{m}\right|_p\right).$$

    $\left|\frac{n}{n}\right|_p > 1$ if and only if $p \big| m$. So the above gives $\prod_p \left|\frac{1}{m}\right|_p = |m|$. A similar deduction holds when $|n| \leq |m|$.

13. Recall that the height of a point is the height of the $x$-coordinate. Let $a = \hat{h}(P)$ where $\hat{h}$ is the canonical height. Then $\hat{h}(nP) = n^2 a$. Since $h = \hat{h} + O(1)$ so $h_{\mathbb{Q}}(x_n) = n^2 a + O(1)$.

    $h_{\mathbb{Q}}(y_n^2) = h_{\mathbb{Q}}(x_n^3 + 3Ax_n + B) = 3h_{\mathbb{Q}}(x_n) + O(1)$. On the other hand, $h_{\mathbb{Q}}(y_n^2) = 2h_{\mathbb{Q}}(y_n) + O(1)$. Then $h_{\mathbb{Q}}(y_n) = \frac{3}{2}n^2 a + O(1)$.

# 27 Modell-Weil Theorem and Rank of Elliptic Curves

Following the previous chapter, we will discuss the main problem in studying elliptic curve, the rank.

## 27.1 Rank of Elliptic Curves

We have shown that $E(K)$ is a group for an elliptic curve $E$ over a field $K$ and it is an abelian group. So it is natural to ask whether it is finitely generated. We begin with the following lemma

**Lemma 27.1.** *If $A$ is a countable abelian group with no element of finite order and $h : A \longmapsto \mathbb{R}$ is a positive definite quadratic form such that for any $C > 0$ the set*

$$\{g \in A : h(g) < C\}$$

*is finite. Then $A \cong \mathbb{Z}^n$ or $A \cong Z^\infty = \bigoplus_{k=1}^{\infty} \mathbb{Z}$.*

*Proof.* Since $A$ is countable, so we can enumerate $A$ as $\{v_1, v_2, \ldots\}$. Inductively construct a basis for $A$ as follows. We may assume $v_1 \neq 0$ (if so interchange $v_1$ and $v_2$). Pick $\omega_1 \in A$ such that $N\omega_1 = v_1$ for some $N \in \mathbb{Z}$ maximal. Indeed, such $N$ exists because $h(v_1) = h(N\omega_1) = N^2 h(\omega_1)$. Since $v_1 \neq 0$ so $h(v_1) \neq 0$, and so it is some constant. Then if $N\omega_1 = v_1$ then we have $h(\omega_1) \leq h(v_1)$ and by assumption we only have finitely many such $\omega$. So the maximal $N$ exists. Then proceed to $v_2$.

Suppose we have picked $v_1, \ldots, v_{kj-1}$ and $\omega_i$ for $i \in I \subset \{1, \ldots, k-1\}$, such that

(1) $\omega_i$'s are linearly independent over $\mathbb{Z}$, (Recall that any abelian group is automatically a $\mathbb{Z}$-module).

(2) $v_1, \ldots, v_{k-1} \in \langle \omega_i : i \in I \rangle$.

(3) If $Nz \in \langle \omega_i : i \in I \rangle$, then $z \in \langle \omega_i : i \in I \rangle$.

Any lattice satisfying (3) is called a **saturated** lattice.

Now either $v_k \in \langle \omega_i : i \in I \rangle$, then we proceed to $v_{k+1}$; Or $v_k$ is not in the the span. We want to find $\omega_k$ such that (1),(2) and (3) hold for $k$. Define the set

$$\Lambda = \{v \in A : Nv \in \langle \omega_i : i \in I : v_k \rangle \text{ for some } N \in \mathbb{N}\}.$$

Then take any $v \in \Lambda$, divide the coefficient of $v$, we have

$$v = \sum_{i \in I} \lambda_i \omega_i + \lambda_k v_k, \lambda_j \in \mathbb{Q} \ \forall j.$$

(Think of the representation as a sequence $\lambda_i, i \in I, \lambda_k$ as it has no meanning in $A$.) Note that such representation is unique. Indeed, for each $v \in \Lambda$ we have a minimal $N$ such that $Nv \in \langle \omega_i, i \in I, v_k \rangle$. So for other $Mv$ in the set, we must have $N|M$, otherwise we have a contradiction for the minimality. For the minimal $N$, the expression of $Nv$ is unique. Indeed, if we have two expressions, with coefficients $a_i$ and $b_i$ respectively, then

$$\sum_{i \in I} (a_i - b_i)\omega_i + (a_k - b_k)v_k = 0.$$

If $a_k - b_k \neq 0$, then either $(a_k - b_k)v_k = 0$, which is impossible as $A$ has no element of finite orders, or $(a_k - b_k)v_k \in \langle \omega_i : i \in I \rangle$ which in turn gives $v_k \in \langle \omega_i : i \in I \rangle$ by (3). Hence $a_k = b_k$ and thus $a_i = b_i$ for all $i \in I$ by (1).

Consider the homomorphism $\Phi : \Lambda \longmapsto \mathbb{R}$ by $\Phi(v) = \lambda_k$. Consider the set $\pi = \{\sum_{i\in I} \mu_i\omega_i + \mu_k\omega_k : \mu \in [0,1]\}$. Then $\pi$ is a compact set and $h$ is continuous, so $h$ is bounded on the set $\pi$ and so $\pi \cap A$ is finite. Also $\pi \cap \Lambda$ is non-empty because we can replace $\lambda_i$ by $\lambda_i - [\lambda_i]$ for each $i$ and the resulting element is again in $\Lambda$. Now, pick $\omega_k \in \pi \cap \Lambda$ such that $\Phi(\omega_k) > 0$ is minimal and claim this is the one we want.

For (1), since $\Phi(\omega_k) > 0$, and the expression is unique so we know $\omega_k$ is not in $\langle \omega_i : i \in I\rangle$ and hence the set $\omega_i : i \in I, \omega_k$ are linearly independent, again by using (3) for $k-1$.

For (2), we have $\omega_k = \sum_{i\in I} \lambda_i\omega_i + \lambda_k v_k$ and $\Phi(\omega_k) = \lambda_k$. Also $\Phi(v_k) = 1$. Observe that if $v, v' \in \Lambda$ then so is $av + bv'$ for all $a, b \in \mathbb{Z}$. Then let $r$ be the largest integer such that $r\lambda_k \leq 1$ In other words, $(r+1)\lambda_k > 1$, and so $\lambda_k > 1 - r\lambda_k$. Then we have

$$\Phi(\omega_k) > \Phi(v_k - r\omega_k) = \Phi(\omega_k').$$

But $1 - r\lambda_k \geq 0$, so by the choice of $\omega_k$, this is only possible when $\Phi(\omega_k') = 0$. In other words, we have $r\lambda_k = 1$. Thus, $v_k = r\lambda_k$ and so we have (2).

For (3), if $Nz \in \langle \omega_i : i \in I, \omega_k\rangle$, then we can pick $N$ to be the minimal one and $N \neq 0$. Write $Nz = \sum_{i\in I} a_i\omega_i + a_k\omega_k$, and we can assume $a_k \neq 0$, otherwise it is just the case for $k-1$. Then clearly $z \in \Lambda$ and

$$\Phi(z) = \frac{a_k}{N}\Phi(\omega_k).$$

Let $r$ be the largest integer such that $a_k - rN \geq 0$. Then it is clear that $z - r\omega_k$ is also in $\Lambda$, and

$$\Phi(z - r\omega_k) = \frac{a_k - rN}{N}\Phi(\omega_k).$$

Now by choice of $r$, $0 \leq \frac{a_k - rN}{N} < 1$, so by minimality of $\Phi(\omega_k)$, we must have $a_k - rN = 0$. Thus, $N \big| a_k$, and so $N(z - r\omega_k) \in \langle \omega_i : i \in I\rangle$. Hence, $z - r\omega_k \in \langle \omega_i : i \in I\rangle$ and so $z \in \langle \omega_i : i \in I : \omega_k\rangle$.

Thus, we have checked that we can have such construction of basis. We have a sequence $\omega_i$, which is linearly independent and spans $A$. So $A \cong \mathbb{Z}^n$ or $A \cong \mathbb{Z}^\infty$, depending on whether the set $I$ is finite. □

**Theorem 27.2.** *Let $E/K$ be an elliptic curve over a number field $K$. Then*

$$E(K) \cong \Delta \times \mathbb{Z}^n \text{ or } E(K) \cong \Delta \times \mathbb{Z}^\infty,$$

*where $\Delta$ consists of the points of finite order in $E(K)$.*

*Proof.* Let $\Delta$ be the set of points of finite order. Then $E(K)/\Delta$ is a countable abelian group. Indeed, it is countable because each pair $(a, b)$ on $E(K)$ is a solution of the equation, with coefficients in $K$, and since $K$ is a number field, so $K$ is countable. Hence $E(K)$ is countable as it is a countable union of countable sets. Also, we have a positive definite quadratic form $\hat{h}$ on $E(K)/\Delta$. Therefore, the result follows from the previous lemma. □

**Definition 27.3.** *With the same notation as in the previous theorem, we call $n$ the rank of $E$ when $E \cong \Delta \times \mathbb{Z}^n$ and we say $E$ has infinite rank otherwise.*

**Remark 27.4.** *In fact $\hat{h}$ and the pairing $\langle , \rangle$ can be used to get a lower bound on the rank of $E(K)$. For example, if $P$ and $Q$ are linearly independent if and only if*

$$\det \begin{pmatrix} \langle P, P\rangle & \langle Q, P\rangle \\ \langle P, Q\rangle & \langle Q, Q\rangle \end{pmatrix} \neq 0.$$

*Indeed, they are linearly independent if and only if*

$$\langle P, \lambda P - \mu Q\rangle \neq 0, \langle Q, \lambda Q - \mu Q\rangle \neq 0,$$

*for all $\lambda, \mu \in \mathbb{Z}$.*

## 27.2 Modell-Weil Theorem

The main purpose of this section is to prove that the rank of $E$ is always finite. Let $F/K$ be a field extension and $E/K$ an elliptic curve over $K$. We shall introduce the following notations:

(1) For each point $P = (a, b) \in E(F)$, write $K(P) = K(a, b)$.

(2) When $F/K$ is Galois, write $\sigma(P) = (\sigma(a), \sigma(b))$, for $\sigma \in \mathrm{Gal}(F/K)$. Clearly $\sigma(P) \in E(F)$.

**Lemma 27.5.** *Let $E/K$ be an elliptic curve over $K$ and $K \subset \mathbb{C}$. Let $P \in E(K)$, and $n$ be a natural number. Then*

*(i) There are $n^2$ points on $Q \in E(\mathbb{C})$ with $nQ = P$.*

*(ii) $K(Q)/K$ is algebraic.*

*(iii) If $E(K)[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$, then $K(Q_i) = K(Q_j)$ for any $nQ_i = nQ_j = P$. If $nQ = P$, then $K(Q)/K$ is Galois, and*

$$Gal(K(Q)/K) \leq \mathbb{Z}/n \times \mathbb{Z}/n.$$

*Proof.* (i) is clear by uniformlisation theorem. For (ii), recall that in the proof of Lemma 26.37, if $Q = (a, b)$ then $P = nQ = (f(a), *)$ where $f(x)$ has degree $m^2$. Suppose $a$ is transcendental over $K$. Then $f(a)$ is again transcendental. But $f(a) \in K$ as $P \in E(K)$. So $a$ is algebraic. Also, $b^2 = a^3 + Aa + B$ and so $b$ is also algebraic. Hence $K(Q) = K(a, b)$ is algebraic.

For (iii), if $nQ_1 = nQ_2 = P$, then we have $Q_1 = Q_2 + T$ for some $T$ such that $nT = \mathcal{O}$. But $E(K)[n] = E(\mathbb{C})[n]$, so $T$ with $nT = \mathcal{O}$ lies in $E(K)$. Then, $K(Q_1) = K(Q_2)$. Let $F$ be the Galois closure of $K(Q)/K$. Pick any $\sigma \in \mathrm{Gal}(F/K)$. Observe that

$$n\sigma(Q) = \sigma(nQ) = \sigma(P) = P.$$

Hence $\sigma(Q) - Q$ is also an element $T$ such that $nT = \mathcal{O}$. Thus,

$$\sigma(K(Q)) = K(\sigma(Q)) = K(Q).$$

So the extension $K(Q)/K$ is normal. But it is also separable. So $K(Q)/K$ is Galois. Finally, since each $\sigma$ can only send $Q$ to some other points with $n\sigma(Q) = P$, say $\sigma(Q) = Q + T_\sigma$. Then we have a homomorphism

$$\psi : \mathrm{Gal}(K(Q)/K) \longmapsto E(K)[n], \psi(\sigma) = T_\sigma.$$

It is clearly injective and so the result follows. □

We shall briefly recall some knowledge in algebraic number theory. Let $F/K$ be an extension of number fields, $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, and write

$$\mathfrak{p}\mathcal{O}_F = \prod_i \mathfrak{q}_i^{e_i}.$$

Then

(1) $\mathcal{O}_F/\mathfrak{q}_i$ is a finite field and is an extension of $\mathcal{O}_K/\mathfrak{p}$ of degree $f_i$.

(2) $\sum_i e_i f_i = [F : K]$.

(3) If $\mathfrak{p} \neq \mathfrak{p}'$, then they have different prime factorisation.

(4) When $F/K$ is Galois, then the action of $\mathrm{Gal}(F/K)$ on the set of primes above $\mathfrak{p}$ is transitive. Moreover, if $g(\mathfrak{q}_i) = \mathfrak{q}_i$, then $g$ induces an action on $\mathcal{O}_F/\mathfrak{q}_i$.

**Lemma 27.6.** *Let $K$ be a number field, and $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ an elliptic curve over $K$. Further, assume $\alpha, \beta, \gamma \in \mathcal{O}_K$ and they are distinct. Let $Q \in E(\bar{K})$ such that $2Q \in E(K)$. Then the extension $K(Q)/K$ can only ramify at primes dividing $2D$, where $D = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$.*

*Proof.* Clearly, $\alpha, \beta, \gamma \in E(K)[2]$, and together with $\mathcal{O}$, we have $E(K)[2] \cong C_2 \times C_2$. Let $F = K(Q)$ and $\mathfrak{p} \nmid 2D$. Now we can extend $E$ to an elliptic curve over $F$. Further, let $\mathfrak{q}$ be a prime above $\mathfrak{p}$ with residue degree $f$ and ramification degree $e$. Reduce $E$ modulo $\mathfrak{q}$ we get an elliptic curve over $\mathcal{O}_F/\mathfrak{q}$. Also the curve must have distinct roots over this field. Indeed, since $\mathfrak{p} \nmid 2D$ so we have $\alpha, \beta, \gamma$ distinct over $\mathcal{O}_K/\mathfrak{p}$. Also $\mathcal{O}_F/\mathfrak{q}$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$.

By previous lemma we know $F/K$ is Galois and let $\sigma \in \mathrm{Gal}(F/K)$. Then $\sigma(Q) = Q + T$, where $T \in E(\bar{K})[2] = E(K)[2]$. Suppose $\sigma$ is not identity and $\sigma(\mathfrak{q}) = \mathfrak{q}$. Then it induces an automorphism on $\mathcal{O}_F/\mathfrak{q}$. Also, it is non-trivial, because, say $\sigma(Q) = Q + T$ where $T \neq \mathcal{O}$, so it is one of $(\alpha, 0), (\beta, 0), (\gamma, 0)$ and we know they are also distinct over $\mathcal{O}_F/\mathfrak{q}$. Thus, each $\sigma$ gives an automorphism of $\mathcal{O}/\mathfrak{q}$, and so

$$f \geq card\{\sigma : \sigma(\mathfrak{q}) = \sigma(\mathfrak{q})\} = \frac{[F:K]}{\text{the number of primes above } \mathfrak{p}}$$

by orbit-stabliser theorem. This implies that $\sum_i f_i \geq [F:K]$. But we also have

$$\sum_i e_i f_i = [F:K].$$

Therefore, $e_i = 1$ for all $i$ and so $\mathfrak{p}$ is unramified. □

**Lemma 27.7.** *Let $K$ be a number field and let $a$ be a non-zero element in $\mathcal{O}_K$. Write*

$$\langle a \rangle = \prod_i \mathfrak{p}_i^{n_i}.$$

*Then $K(\sqrt{a})$ ramifies at all $\mathfrak{p}_i$ with $n_i$ odd.*

*Proof.* Let $F = K(\sqrt{a})$. Then we have

$$\langle a \rangle = \langle \sqrt{a} \rangle^2 = \prod_i \mathfrak{p}_i^{n_i}.$$

But the left hand side is a square, so the right hand side must also be a square, by unique factorisation. Thus, if $n_i$ is odd, then $\mathfrak{p}$ must be a square in $K(\sqrt{a})$ and is therefore ramified. □

**Lemma 27.8.** *Let $K$ be a number field and $S$ be a finite set of primes. Then there are only finitely many quadratic extension of $K$ that only ramify at primes inside $S$.*

*Proof.* By Dirichlet's unit theorem, $\mathcal{O}_K^* \cong \Delta \times \mathbb{Z}^{r+s-1}$ and so

$$\mathcal{O}_K^*/(\mathcal{O}_K^*)^2 \cong \text{ finite } \times (\mathbb{Z}/2\mathbb{Z})^{r+s-1}.$$

So we can find a finite set $I$ and $u_i, i \in I$ which are representatives for the quotient. Also take $c_j, j \in J$ as ideal representatives for the ideal class group, so $J$ is also finite. Finally, let $x_k, k \in R$ be generators for all principal ideals of the form

$$\langle x_k \rangle = c_j^2 \prod_{\mathfrak{p}_i \in T} \mathfrak{p}_i,$$

where $T \subset S$. We only have finitely many possibilities for $T$ and since $J$ is finite, so $R$ is also finite.

Let $F$ be a quadratic extension of $K$ so $F = K(\sqrt{a})$ for some $a \in K$. We may assume $a \in \mathcal{O}_K$. Let

$$\langle a \rangle = c^2 \prod_i \mathfrak{p}_i,$$

where we took out the squared factor in the factorisation and denote it by $c^2$. By previous lemma, we want primes ramify inside $S$. So suppose we have some $\mathfrak{p}_i$ above which is not in $S$, then by previous lemma $\mathfrak{p}_i$ also ramifies. Therefore, $\mathfrak{p}_i \in T \subset S$. Now pick $c_j$ such that $c_j = c$ in the ideal class group. Then we have some $\alpha \in K^*$ such that

$$\langle \alpha \rangle c_j = c.$$

So

$$\langle a \rangle = \langle \alpha \rangle^2 c_j^2 \prod_{\mathfrak{p}_i \in T} \mathfrak{p}_i = \langle \alpha \rangle^2 \langle x_k \rangle,$$

for some $x_k$. So $a = \alpha^2 x_k u$ where $u \in \mathcal{O}_K^*$ and so

$$a = \alpha^2 \beta^2 x_k u_i \text{ for some } i \in I.$$

Then $F = K(\sqrt{a}) = K(\sqrt{x_k u_i})$ for some $k \in R, i \in I$. Since $R$ and $I$ are both finite, so we only have finitely many such $F$. □

**Lemma 27.9.** *Let $K$ be a number field and $E/K$ and elliptic curve over $K$. Assume that $E(K)[2] \cong C_2 \times C_2$. Then the map*

$$E(K)/2E(K) \longmapsto F \quad \textit{with } Gal(F/K) \leq C_2 \times C_2,$$

*by $P \mapsto K(Q)$ where $Q \in E(\bar{K}), 2Q = P$ is well-defined and finite to one. In other words, the preimage of each element in the image is finite.*

*Proof.* By Lemma 27.5 we have the correct Galois group. We check it is well-defined. Firstly, if $2Q = 2Q' = P$, then $Q = Q' + T$ where $T \in E(K)$ as $E(K)[2] = E(\bar{K})[2]$, so $K(Q) = K(Q')$. Now if we have $P = P' + 2R$ for some $R \in E(K)$ and write $2Q = P, 2Q' = P'$, then

$$2(Q - Q' - R) = \mathcal{O} \Rightarrow Q = Q' + R + T, \text{ for some } T \in E(K)[2].$$

Then we again have $K(Q) = K(Q')$. Hence the map is well-defined.

To check it is finite to one, let $P_1, \ldots, P_r \in E(K)$ with $P_i = 2Q_i$ for some $Q_i$ and suppose we have $K(Q_i) = F$. Let $\mathrm{Gal}(F/K) \subset \{\sigma_i : i = 1, 2, 3, 4\} = C_2 \times C_2$. Then we know

$$2\sigma_i(Q_j) = \sigma_i(P_j) = P_j.$$

So $\sigma_i(Q_j) = Q_j \oplus T$ for some $T \in E(K)[2]$. Let $E(K)[2] = \{T_1, T_2, T_3, T_4\}$. Further, let $\sigma_1, \sigma_2$ generate $C_2 \times C_2$. By relabeling suppose

$$\sigma_1(Q_1) = Q_1 \oplus T_i, \sigma_1(Q_2) = Q_2 \oplus T_j, \sigma_2(Q_1) = T_k, \sigma_2(Q_2) = T_l.$$

If $T_i = T_j$ and $T_k = T_l$ then $Q_1 \ominus Q_2$ is fixed by $\sigma_1, \sigma_2$ and hence fixed by $\mathrm{Gal}(F/K)$. This implies that $Q_1 \ominus Q_2 \in E(K)$ and so $P_1 - P_2 \in 2E(K)$. Therefore $P_1 = P_2$ in $E(K)/2E(K)$. Hence, $P_1 \neq P_2$ in $E(K)/2(K)$ only when

$$T_i \neq T_j \text{ or } T_k \neq T_l.$$

Based on this observation, in general let $\sigma_1(Q_i) = Q_1 + T_i$ and $\sigma_2(Q_i) = Q_1 + T_k$. Then we have at most 16 possibilities, and if we have one more, say $Q_{17}$, then we must have some $i$ such that

$$\sigma_1(Q_i) = \sigma_1(Q_{17}), \sigma_2(Q_i) = \sigma_2(Q_{17}),$$

which implies $P_1 = P_{17}$ in $E(K)/2E(K)$. Thus, we have at most 16 preimages. □

**Theorem 27.10.** [**Weak Modell-Weil Theorem**] *Let $E/K$ be an elliptic curve over $K$ where $K$ is a number field, $E(K)[2] \cong C_2 \times C_2$. Then $E(K)/2E(K)$ is finite.*

*Proof.* Assume that

$$E : y^2 = (x-\alpha)(x-\beta)(x-\gamma), \alpha, \beta, \gamma \in K.$$

But recall that $K = Frac(\mathcal{O}_K)$, so we may write $\alpha$ as a quotient in $\mathcal{O}_K$ and similarly for $\beta$ and $\gamma$. Then clear the denominator and by using an isomorphism of the form $x' = r^2x, y' = r^3y$ we may assume that $\alpha, \beta, \gamma \in \mathcal{O}_K$. Consider the map from $E(K)/2E(K)$ to $K(Q)$ as in the previous lemma.

Let $K(Q) = F$ and we know $\mathrm{Gal}(F/K) \leq C_2 \times C_2$. Hence $F$ is biquadratic (or quadratic) and so $F = K(\sqrt{a}, \sqrt{b})$. Lemma 27.6 implies that the only prime which can ramify in $F$ are those diving $2D$ where $D = (\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2$. So the number of such prime is finite and let $S$ be the set of primes which ramify in $F/K$. This means by tower law that the only prime which can ramify in $K(\sqrt{a})$ and $K(\sqrt{b})$ are those in $S$. But we only have finitely many such quadratic fields by Lemma 27.8. In particular, the number of such $K(Q)$ is finite.

Finally, use the previous lemma so that the set $E(K)/2E(K)$ is finite because each $K(Q)$ only has at most 16 preimages. □

**Theorem 27.11.** [**Modell-Weil Theorem**] *Let $E/K$ be an elliptic curve over a number field $K$. Then the rank of $E(K)$ is finite.*

*Proof.* Let $F = K(T_1, T_2, T_3)$ where $2T_1 = 2T_2 = 2T_3 = \mathcal{O}$. Then $E(F)[2] \cong C_2 \times C_2$. Further, if $E(F) \cong \Delta \times \mathbb{Z}^\infty$, then $E(F)/2E(F)$ would be infinite, which is a contradiction to the previous theorem. Hence, $E(F)$ has finite rank. Now it is an easy exercise (see Exercises 27) that if $E(F)$ is finitely generated, so is $E(K)$. □

**Example 27.12.** *Consider $E : y^2 = x^3 - x$ over $\mathbb{Q}$. Note that $E(\mathbb{Q})[2] = C_2 \times C_2$. Let $E(\mathbb{Q}) \cong \Delta \times \mathbb{Z}^r$ and we proved that (via uniformlisation theorem) that*

$$\Delta \leq \mathbb{Z}/k \times \mathbb{Z}/k.$$

*Let $\Delta = \mathbb{Z}/m \times \mathbb{Z}/n$. Since $C_2 \times C_2$ is in $\Delta$ so we have $2 \big| m, n$. Follow the proof we know that $\mathbb{Q}(Q) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ where $2Q = P \in E(\mathbb{Q})$. Now we have $\alpha = 1, \beta = -1, \gamma = 0$, so the only prime which can ramify is $p \big| 8$ which is 2. So the only possible biquadratic one is $\mathbb{Q}(\sqrt{2}, i)$. Then followed by our previous proof we have at most 16 points in $E(\mathbb{Q})/2E(\mathbb{Q})$. Since $m, n$ are both even, so we will have $C_2 \times C_2$ from $\Delta$. Therefore, we conclude that*

$$C_2 \times C_2 \times (\mathbb{Z}/2)^r \leq 16.$$

*Hence $r \leq 2$.*

**Example 27.13.** *Let $E : y^2 = x^3 - 3x$ be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is generated by $C_2 \times \mathbb{Z}$, with generators $(0,0)$ and $(-1,-1)$.*

**Example 27.14.** *Let's now construct a curve with rank $\geq 5$. Take*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*and insist the following points on $E$: $(0,0), (1,1), (-\frac{1}{2}, 0), (2,-2), (-1, -\frac{1}{2})$. Then compute the height pairing and use Remark 27.4 to show they are linearly independent. Hence the rank is at most 5.*

**Remark 27.15.** *It is still a big mystery whether we can construct elliptic curve over $\mathbb{Q}$ arbitrary large rank.*

## 27.3 Elliptic Curve Over $p$-adic field

Now we have proved that each elliptic curve over $\mathbb{Q}$ has finite rank. The task is to get a lower bound and an upper bound for those. In order to do so, we will consider the curve over $p$-adic field.

**Definition 27.16.** *Let $E/K$ be an elliptic curve over a number field $K$, where $E$ is given by:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*The* **discriminant** *of $E$ is defined by:*

$$\Delta_E = -b_2^2b_8 - 8b_4^2 - 2b_6^2 + 9b_2b_4b_6,$$

*where*

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, b_8 = b_2b_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

*When $a_1, a_3 = 0$ we have $E : y^2 = f(x)$. Then $\Delta_E = 16disc(f(x))$ where $disc(f(x)) = -4A^3 - 27B^2$ when $f(x) = x^3 + Ax + B$.*

**Proposition 27.17.** *$E$ is non-singular if and only if $\Delta_E \neq 0$.*

We will omit the proof because it is going it is going to use some geometric technique.

**Remark 27.18.** *If $E$ and $E'$ are isomorphic, related by $y' = u^3y + rx + t, x' = u^2x + r, u \neq 0$. Then $\Delta'_{E'} = u^{12}\Delta$. So it differs by a $12^{th}$ power.*

**Definition 27.19.** *When $K = \mathbb{Q}$, we say an equation of $E$ is* **minimal** *at $p$ or a* **minimal model** *for $p$ (where $p$ is a prime) if it is integral (which means the $\mathfrak{p}$-adic valuation of each coefficient is non-negative) and $ord_p(\Delta_E)$ is as small as possible among all such equations defining the same elliptic curve, up to isomorphism.*

*The reduced curve is:*

$$\bar{E}/\mathbb{F}_p : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6,$$

*where $\bar{a_i} \equiv a_i \pmod p$ for any minimal model.*

**Remark 27.20.** *The minimal model at $p$ is unique up to isomorphism of the form*

$$y = u^3y' + t, x = u^2x' + sx' + r, u, s, r, t \in \mathbb{Q} \text{ with non-negative } p - \text{valuation.}$$

*This induces an isomorphism on reduced curves and so $\bar{E}/\mathbb{F}_p$ is well-defined up to isomorphism. Then by Remark 27.18 if the equation is integral and $ord_p(\Delta_E) < 12$ then it must be minimal.*
**WARNING***: $\bar{E}$ might be singular.*

**Definition 27.21.** *We say $E$ has a* **good reduction** *at $p$ if $\bar{E}/\mathbb{F}_p$ is non-singular (and hence an elliptic curve over $\mathbb{F}_p$) and* **bad reduction** *if it is singular. We shall also define the set*

$$\bar{E}_{ns}(\mathbb{F}_p) = \bar{E}(\mathbb{F}_p)\backslash\{\text{singular points if there exists}\}.$$

**Remark 27.22.** *$\bar{E}_{ns}(\mathbb{F}_p)$ is an abelian group (even $\bar{E}$ is singular) with identity $\mathcal{O}$ and $P \oplus Q \oplus R = \mathcal{O}$ if $P, Q, R$ line on the same line in $\mathbb{F}_p$. This just follows that a line in $\mathbb{Q}$ will be reduced to a line in $\mathbb{F}_p$.*

**Remark 27.23.** *Reduction types are the following:*

*(1) Good reduction.*

*(2) Split multiplicative (which means bad reduction and $\bar{E}_{ns}(\mathbb{F}_p) = \mathbb{F}_p^*$).*

*(3) Non-split multiplicative (which means bad reduction and $\bar{E}_{ns}(\mathbb{F}_p) = \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \cong C_{p+1}$.*

*(4) Additive reduction (bad reduction and $\bar{E}_{ns}(\mathbb{F}_p) = (\mathbb{F}_p, +) = C_p$.*

*When $p \neq 2$, there is a minimal model of the form*

$$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6.$$

*Then the type depends on the roots of $f(x)$ mod $p$. It has good reduction if we have distinct roots. It has multiplicative reduction if we have repeated roots. So we can shift by constant so that*

$$\bar{E} : y^2 = x(x + \eta).$$

*In particular, it is split multiplicative if and only if $\eta \in \mathbb{F}_p^{*2}$. It has non-split multiplicative reduction if $\eta \notin \mathbb{F}_p^{*2}$. Then $\bar{E}_{ns}(\mathbb{F}_p) = \mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*/\mathbb{F}_p^*$ via $(x, y) \mapsto x^{-1}y$. Finally, it has additive reduction if it has triple roots. Then we may assume that $\bar{E} : y^2 = x^3$ and $\bar{E}_{ns}(\mathbb{F}_p) \cong (\mathbb{F}_p, +)$ via $(x, y) \mapsto x^{-1}y$.*

*Alternatively we may think split multiplicative reduction as that $\bar{E}$ can be rearranged as*

$$[y - \alpha x][y + \alpha x] = x^3, \text{ where } \alpha^2 = \eta.$$

**Example 27.24.** *Consider $E : y^2 = x^3 - 3 \cdot 5^4x - 3 \cdot 5^6$. Then $\Delta_E = -2^4 3^3 5^1 3$. It is integral, but it is not minimal, because if we set $x \mapsto 5^2x, y \mapsto 5^3y$, we then have*

$$y^2 = x^3 - 3x - 3, \Delta \mapsto 5^{-12}\Delta.$$

*The this equation is minimal at 5.*

*Now reduce the curve over $\mathbb{F}_5$ we have*

$$\bar{E} : y^2 = x^3 + 2x + 2 = (x - 1)^2(x + 2).$$

*By a suitable linear transformation we have $y^2 = x^2(x + 3)$. It is singular, and it is non-split multiplicative because 3 is not a square in $\mathbb{F}_5^*$. Finally, we have*

$$\bar{E}(\mathbb{F}_5) = \{(1, 0)\} \cup \{(2, \pm 2), (3, 0), (4, \pm 2), \mathcal{O}\},$$

*where the second set is $\bar{E}_{ns}(\mathbb{F}_p)$.*

**Definition 27.25.** *For $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$, find $\alpha \in \mathbb{Q}^*$, so that $\alpha x_i$ have $ord_p(\alpha x_i) \geq 0$ and at least one of them is not divisible by $p$. Then $\bar{P} = [\overline{\alpha x_0} : \cdots : \overline{\alpha x_n}] \in \mathbb{P}^n(\mathbb{F}_p)$. For an elliptic curve $\mathbb{E}/\mathbb{Q}$ with a minimal model, this gives*

$$E(\mathbb{Q}) \longmapsto \bar{E}(\mathbb{F}_p)$$

*via reduction modulo $p$, provided that $p \nmid$ the denominator of $x$ or $y$. This is just some terminology in projective space.*

We recall some basic definition and properties of metric space. We can define $d(0, x) = p^{-n}$ where $x = \frac{a}{b}p^n, p \nmid a, b$ and $d(x, y) = d(0, x - y)$. So $x$ is close to $y$ if they look like the same modulo $p$. Recall that $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to this metric. We may also write

$$\mathbb{Z}_p = \left\{ \sum n = 0^{\infty} a_n p^n : 0 \leq a_n \leq p - 1 \right\}$$

and

$$\mathbb{Q}_p = Frac(\mathbb{Z}_p) = \left\{ \sum_{n=n_0}^{\infty} a_n p^n : 0 \leq a_n \leq p - 1, n_0 \in \mathbb{Z} \right\}.$$

**Remark 27.26.** *(i) Recall that $\mathbb{Z}_p$ is a local ring, with unique maximal ideal $\langle p \rangle$. $\frac{1}{n} \in \mathbb{Z}_p$*

*(ii) $\frac{1}{n} \in \mathbb{Z}_p$ for all $p \nmid n$.*

*(iii) $\forall x \in \mathbb{Z}_p$ we can define $\bar{x} \equiv x \bmod p$. So if we have $x = \sum_{n=0}^{\infty} a_n p^n$, then $\bar{x} = a_0$.*

*(iv) Recall that Hensel's lemma says suppose $f(x) \in \mathbb{Z}_p[X], \bar{f}(x) = f(x) \bmod p$. So $\bar{f}(x) \in \mathbb{F}_p[X]$. If $\bar{\alpha} \in \mathbb{F}_p$ such that $\bar{f}(\bar{\alpha}) = 0$, and $\bar{f}'(\bar{\alpha}) \neq 0$ for some $\bar{\alpha}$ then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \bar{\alpha} \bmod p$.*

**Example 27.27.** *$p = 7$, $\frac{1}{2} = 4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + \cdots$. Indeed, multiply both sides by 2, and notice that*

$$\sum_{n=0}^{\infty} 6 \cdot 7^n = -1$$

*so the right hand side is indeed just 1.*

**Definition 27.28.** *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weistress equation. Define*

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : P \text{ reduces to some point in } \bar{E}_{ns}(\mathbb{F}_p)\},$$

*and*

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : P \text{ reduces to } \mathcal{O}\}.$$

**Lemma 27.29.** *$E_1(\mathbb{Q}_p) \leq E_0(\mathbb{Q}_p) \leq E(\mathbb{Q}_p)$ as subgroup and the reduction modulo $p$ is a homomorphism from $E_0(\mathbb{Q}_p)$ to $\bar{E}_{ns}(\mathbb{F}_p)$.*

*Proof.* Let $P, Q, R$ lie on a line in $\mathbb{Q}_p$ and $\bar{P}, \bar{Q}, \bar{R} \in \bar{E}_{ns}(\mathbb{F}_p)$, then $\bar{P}, \bar{Q}, \bar{R}$ lie on a line in $\mathbb{F}_p$. It follows that $E_0(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$. Then it is clear that reduction modulo $p$ is a homomorphism with kernel $E_1(\mathbb{Q}_p)$ and so $E_1(\mathbb{Q}_p)$ is a subgroup of $E_0(\mathbb{Q}_p)$. □

We then give a theorem which gives the property of the quotient $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ in different cases. We will omit the proof.

**Theorem 27.30.** *The group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is finite and is*

*(i) trivial if $E$ has good reduction.*

*(ii) $\cong \mathbb{Z}/n\mathbb{Z}$ if $E$ has split multiplicative reduction.*

*(iii) $\{1\}$ if $ord_p(\Delta_E)$ is odd and $E$ has non-split multiplicative reduction.*

*(iv) $\mathbb{Z}/4\mathbb{Z}$ if $ord_p(\Delta_E)$ is even if $E$ has non-split multiplicative reduction.*

*(v) of order $\leq 4$ if $E$ has additive reduction. where $n = ord_p(\Delta E)$ of a minimal model.*

**Remark 27.31.** *There is an algorithm (Tate's algorithm) that determines this quotient group completely. The order of the group is called local number $E$.*

**Theorem 27.32.** *Reduction modulo $p$ induces an isomorphism*

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \bar{E}_{ns}(\mathbb{F}_p).$$

*Proof.* We have checked that we have the correct kernel so it suffices to check the map is surjective. We will do it by Hensel's lemma. We can write $E$ as $g(x,y) = 0$, where

$$g(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

Let $\bar{P} = (\bar{a}, \bar{b}) \in \bar{E}_{ns}(\mathbb{F}_p)\backslash\{\mathcal{O}\}$. It is not a singular point, hence if $\bar{g}$ is the the reduced equation, then

$$\frac{\partial \bar{g}}{\partial x}\Big|_{\bar{P}} \neq 0 \text{ or } \frac{\partial \bar{g}}{\partial y}\Big|_{\bar{P}} \neq 0.$$

If we are in the first case, then let $b \in \mathbb{Z}_p$ such that $b \equiv \bar{b} \bmod p$. Then solve the equation $g(x,b) = 0$ for $x$, using Hensel's lemma. If we are in the second case, then pick $a \in \mathbb{Z}_p$ such that $a \equiv \bar{a} \bmod p$ and solve for $b$. Hence the map is surjective. □

**Proposition 27.33.** *The map $E_1(\mathbb{Q}_p) \longmapsto p\mathbb{Z}_p$ defined by $(x,y) \mapsto -\frac{x}{y}$ and $\mathcal{O} \mapsto 0$ is a bijection.*

*Proof.* Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be minimal at $p$, where $a_i \in \mathbb{Z}_p$. Let $\omega = -\frac{1}{y}$ and $t = -\frac{x}{y}$. So the equation becomes

$$\omega = t^3 + a_1t\omega + a_2t^2\omega + a_3\omega^2 + a_4t\omega^2 + a_6\omega^3,$$

and the point $\mathcal{O}$ goes to $(0,0)$ and $E_1(\mathbb{Q}_p)$ is the set of points with $\omega, t \in p\mathbb{Z}_p$ because $P \in E_1(\mathbb{Q}_p)$ if $P$ reduces to $\mathcal{O}$. If $P = (x,y)$ then $\bar{P} = (\bar{x}, \bar{y}) = \mathcal{O}$ if and only if $x, y$ both have denominators divisible by $p$. Then we will have $\omega \in p\mathbb{Z}_p$. Now $ord_p(\omega) \geq 1$, and use the above equation, we conclude that $t \in \mathbb{Z}_p$. For each $t \in p\mathbb{Z}_p$, we have 0 is a solution to

$$\omega \equiv a_3\omega^2 + a_5\omega^3 \pmod{p}.$$

Further if we differentiate with respect to $\omega$, we have

$$1 - a_1t - a_2t^2 - 2a_3\omega - 2a_4t\omega - 3a_5\omega^2,$$

and this is 1 modulo $p$ when we put $\omega = 0$. Hence, by Hensel's lemma, we have a unique $\omega \in \mathbb{Z}_p$ which is 0 mod $p$ and $(t,\omega)$ satisfies the given equation and $\omega \equiv 0 \pmod{p}$ is the same as $\omega \in p\mathbb{Z}_p$. Therefore, for each $t \in p\mathbb{Z}_p$ there is a unique $\omega \in p\mathbb{Z}_p$ such that

$$\omega = t^3 + a_1t\omega + a_2t^2\omega + a_3\omega^2 + a_4t\omega^2 + a_6\omega^3.$$

Then we can set $x = t\omega^{-1}$ and $y = -\omega^{-1}$. It is easy to check this map is inverse to the map $(x,y) \mapsto -xy^{-1}$. Hence the map is bijective. □

**Remark 27.34.** *Doing Hensel's lemma explicitly produces a unique power series for $\omega$ in terms of $t$. We have (using Newton-Raphson to calculate $\omega_n$)*

$$\omega(t) = t^3 + (a_1^2 + a_2)t^4 + (a_1^3 + 2a_1a_2 + a_3)t^3 + \cdots.$$

*This gives*

$$x(t) = \frac{t}{\omega(t)} = \frac{1}{t^2} - \frac{a_1}{t} - a_2 - a_3t - (a_4 + a_1a_3)t^2 + \cdots.$$

$$y(t) = -\frac{1}{\omega(t)} = \frac{1}{t^3} + \frac{a_1}{t} + \frac{a_2}{t^2} + a_3 + (a_4 + a_1a_3)t^2 + \cdots.$$

**Proposition 27.35.** *(i) There is a power series*

$$F_E(t_1, t3) = t_1 + t_2 - a_1 t_1 t_2 - a_2(t_1^2 t_2 + t_1 t_2^2) + \cdots .$$

*where $F_E(t_1, t_2) \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ such that for $t_3 = F_E(t_1, t_2)$ we have*

$$(x(t_1), y(t_1)) \oplus (x(t_2), y(t_2)) = (x(t_3), y(t_3)) \in E(K),$$

*where $K = \mathbb{Q}(a_1, \ldots, a_6)((t_1, t_2))$.*

*(ii) There is a unique power series $i_E(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that*

$$\ominus(x(t), y(t)) = (x(i_E(t)), y(i_E(t))).$$

*(iii) These describe the elliptic curves addition law on $p\mathbb{Z}_p$. Let*

$$\psi : E_1((Q)_p) \times E_1(\mathbb{Q}_p) \text{ via } \psi(P, Q) = P \oplus (Q),$$

*and*

$$\phi : E_1(\mathbb{Q}_p) \to p\mathbb{Z}_p \text{ via } \phi((x, y)) = -\frac{x}{y},$$

*and let $\phi$ send $E_1((Q)_p) \times E_1(\mathbb{Q}_p)$ to $p\mathbb{Z}_p \times p\mathbb{Z}_p$ componentwise. Then we have*

$$F_E(t_1, t_2) = \phi(\psi(P, Q)), \text{ where } t_1 = \phi(P), t_2 = \phi(Q).$$

*Also, if we set $\chi(P) = \ominus(P)$ for each $P$ then*

$$i_E(\phi(P)) = \phi(\chi(Q)).$$

*Proof.* (i) Let $P_i = (x(t_i), y(t_i))$ for $i = 1, 2$ and let $P_1 \oplus P_2 = (x(t_3), y(t_3))$. Then we have

$$t_3 = -\frac{x_{P_1 \oplus P_2}}{y_{P_1 \oplus P_2}}.$$

Let $t_3 = F_E(t_1, t_2)$ and then explicit computation we will find $t_3$ has the desired form.

(ii) It is easy to check that $\ominus(x(t), y(t)) = (x(t), y(t) - a_1 x(t) - a_3)$. Hence

$$i_E(t) = \frac{-x(t)}{-y(t) - a_1 x(t) - a_3} = \frac{-t - a_1 t^2 + \cdots}{1 + 2a_1 + \cdots}.$$

So the denominator is invertible and so it is in $\mathbb{Z}[a_1, \ldots, a_6][[t]]$.

(iii) Obvious by the expression of $F_E(t_1, t_2)$ and $i_E(t)$ above in (i) and (ii).

□

**Definition 27.36.** *A (one parameter commutative) formal group over some ring $R$ is simply a power series $F \in R[[x, y]]$ such that*

*(i) $F(x, y) = x + y +$terms of degree $\geq 2$, and sometimes we write this as $x \oplus_F y$.*

*(ii)* $F(x,y) = F(y,x)$.

*(iii)* $F(x, F(y,z)) = F(F(x,y), z)$.

*(iv) There is a unique* $i(T) \in R[[T]]$ *such that* $F(T, i(T)) = 0$.

*(v)* $F(x,0) = x$.

**Corollary 27.37.** *$F_E$ defined in Proposition 27.35 is a formal group over any ring $R$ which contains $\mathbb{Z}[a_1, \ldots, a_6]$.*

*Proof.* We check it satisfies the above property. (i) is clear as $F_E(t_1, t_2) = t_1 + t_2 +$higher order terms. (ii) follows from the fact $P \oplus Q = Q \oplus P$. (iii) follows from the associativity of the group law of $\oplus$. Now by Proposition 27.35(ii), there is a unique $i_E(t)$ such that

$$\ominus(x(t), y(t)) = (x(i_E(t)), y(i_E(t))).$$

So $F_E(t, i_E(t))$ is the parameter for $\mathcal{O}$. But recall from Proposition 27.33 that $\mathcal{O}$ goes to 0 and so $F_E(t, i_E(t)) = 0$. Finally, since 0 corresponds to $\mathcal{O}$, so $F_E(t, 0) = t$ as $P \oplus \mathcal{O} = P$. □

**Definition 27.38.** *we will write $F(p\mathbb{Z}_p)$ for the formal group $(p\mathbb{Z}_p, \oplus_F)$, and $F(p^n\mathbb{Z}_p)$ for $(p^n\mathbb{Z}_p, \oplus_F)$, where $\oplus_F$ is to be specified.*

**Example 27.39.** *We call define $\oplus_F$ to be the usual addition. Then $F(p\mathbb{Z}_p)$ is just a group under addition. Also, we could define*

$$F(x,y) = x + y + xy.$$

*Then properties (i) and (ii) are immediate. For (iii),*

$$F(x, F(y,z)) = x + F(y,z) + xF(y,z) = x + y + z + xy + xz + yz + xyz = F(F(x,y), z).$$

*Now since $x \in p\mathbb{Z}_p$ so $1 + x$ is a unit in $\mathbb{Z}_p$. Hence, if $y = -(1+x)^{-1}x$, then $F(x,y) = x - x(1+x)^{-1} - x^2(1+x)^{-1} = 0$ and it is unique. Finally, $F(x,0) = x + 0 + 0 = x$. So it defines a formal group. In fact, we have*

$$F(\mathbb{Z}_p) \cong (1 + \mathbb{Z}_p, *) \text{ via } \theta(x) = 1 + x,$$

*because $\theta(F(x,y)) = 1 + F(x,y) = (1+x)(1+y) = \theta(x)\theta(y)$.*

**Theorem 27.40.** *Let $E$ be an elliptic curve over $\mathbb{Q}_p$, where the equation $E$ is minimal at $p$. Then*

$$\bar{E}(p\mathbb{Z}_p) \cong E_1(\mathbb{Q}_p),$$

*where $\bar{E}(p\mathbb{Z}_p) = F_E(p\mathbb{Z}_p)$ is the formal group associated to $E$ with respect to $\oplus$.*

*Proof.* By Proposition 27.33 we have a bijection between $E_1(\mathbb{Q}_p)$ and $p\mathbb{Z}_p$. Moreover, by definition of $F_E(t_1, t_2)$ it is immediate that the map is a group homomorphism. □

**Lemma 27.41.** *Let $F$ be a formal group over $R$ and let $[n]$ denote the multiplication by $n$. In other words, $[n](T) = T \oplus_F T \cdots \oplus_F T$, with addition $n$ times. Then*

$$[n](T) = nT + O(T^2) \in R[[T]].$$

*Proof.* We will prove this by induction. When $n = 1$ the result is obvious. Suppose it is true for $n-1$, then $[n](T) = [n-1](T) \oplus_F T$. By inductive hypothesis, we have

$$[n](T) = ((n-1)T + aT^2) \oplus T = (n-1)T + T + bT^2 = nT + bT^2 = nT + O(T^2),$$

by property (i) of formal group. Hence it is true for all $n$. □

**Lemma 27.42.** *Let $f(T) = aT + O(T^2) \in R[[T]]$ with $a \in R^*$. Then there exists $g(T) \in R[[T]]$ such that $g(T) = a^{-1}T + O(T^2)$ and $f(g(T)) = T$. Moreover, $g(f(T)) = T$.*

*Proof.* Let $g_1(T) = a^{-1}T$ then $f(g_1(T)) = a(b_1T) + O(T^2) = T + O(T^2)$. Suppose we have $g_n(T) = b_1T + \cdots + b_nT^n$ such that $f(g_n(T)) = T + cT^{n+1} + O(T^{n+1})$. Then consider,

$$g_{n+1}(T) = g_n(T) - ca^{-1}T^{n+1}.$$

It is easy to check that $f(g_{n+1}(T)) = T + O(T^{n+2})$. Hence we have a sequence $g_n(T)$ such that $f(g_n(T)) = T + O(T^{n+1})$ for all $n$ and $g_{n+1}(T) - g_n(T) = O(T^{n+1})$. So we can define $g(T) = \lim_{n\to\infty} g_n(T)$ which is a power series in $R[[T]]$ and $f(g(T)) = T$. Moreover the leading coefficient of $g(T)$ is $a^{-1}$, by $g_1(T)$.

Now since $a^{-1} \in R^*$ so again we can use the above procedure to construct $h(T)$ such that $g(h(T)) = T$. Apply $f$ on both side so $f(g(h(T))) = f(T)$. But $f(g(T)) = T$ so we have $h(T) = f(T)$. In other words, $g(f(T)) = T$. □

**Corollary 27.43.** *For $p \nmid n$, the map $[n]$ is an automorphism of $E_1(\mathbb{Q}_p)$. In particular, $E_1(\mathbb{Q})[n] = \{\mathcal{O}\}$.*

*Proof.* It is clear an homomorphism. Now $n \in \mathbb{Z}_p^*$ as $p \nmid n$. We also know that $E_1(\mathbb{Q}_p) \cong \bar{E}(p\mathbb{Z}_p)$. Then in $\bar{E}(p\mathbb{Z}_p)$, the corresponding map of $[n]$ is just $[n]$ defined Lemma 27.41 and we know

$$[n](T) = nT + O(T^2).$$

Then by Lemma 27.42, we have some $g(T)$ such that $[n](g(T)) = T$. Also $g([n](T)) = T$. To check $[n]$ is bijective in $E_1(\mathbb{Q}_p)$ it is now equivalent to check it is bijective in $\bar{E}(p\mathbb{Z}_p)$. Given $h(T) \in \bar{E}(p\mathbb{Z}_p)$ we have $[n](g(h(T))) = h(T)$ and hence it is surjective. If $[n](h(T)) = 0$ then apply $g$ on both sides we conclude that $h(T) = 0$. Therefore $[n]$ is bijective and so an isomorphism. □

**Theorem 27.44.** *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Z}_p$ is minimal at $p$. Further when $p = 2$ we assume that $a_1 \equiv 0 \pmod 2$. Then $E_1(\mathbb{Q}_p)$ has no element of order $p$.*

*Proof.* Assume $a_1 = 0$, otherwise we can set $y' = y + \frac{a_1x}{2}$ and $x' = x$. In the case when $p = 2$ we already have $a_1 \equiv 0 \pmod 2$ by assumption. Note that the translation preserves the minimality. Recall that

$$F_E(t_1, t_2) = t_1 + t_2 - a_1t_1t_2 - a_2(t_1^2t_2 + t_2^2t_1) + \cdots .$$

But $a_1 = 0$ so $F_E(t, t) = 2t + O(T^3)$ and by induction it is easy to prove that $[n](T) = nT + O(T^3)$ when $p \neq 2$. Let $\alpha \in \mathbb{Z}_p\backslash\{0\}$, and $ord_p(\alpha) = k \geq 1$. Then

$$[p](\alpha) = p\alpha + O(p^{3k}).$$

For the case $p = 2$, we have $ord_2(a_1t^2) \geq 3$. In either case, $ord_p(p\alpha) = k + 1 < 3k$. Hence, $ord_p([p]\alpha) = k + 1$. Therefore, $[p](\alpha) \neq 0$ (because 0 does not have finite valuation). The rest just follows by using the isomorphism $\bar{E}(p\mathbb{Z}_p) \cong E_1(\mathbb{Q}_p)$. □

**Theorem 27.45.** *Let $F$ be a formal group over $\mathbb{Z}_p$. Then*

*(i)* $F(p^n\mathbb{Z}_p) \leq F(p\mathbb{Z}_p)$.

*(ii)* $F(p^n\mathbb{Z}_p)/F(p^{n+1}\mathbb{Z}_p) \cong \mathbb{F}_p$.

*(iii) For sufficiently large $n$,* $F(p^n\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$.

*Proof.* (i) It is clear as $p^n\mathbb{Z}_p \subset p\mathbb{Z}_p$.

(ii) $p^n\mathbb{Z}_p$ has element $a_np^n + a_{n+1}p^{n+1} + \cdots$. Let

$$\chi : F(p^n\mathbb{Z}_p) \longmapsto \mathbb{F}_p \text{ via } \phi(\sum_{k=n}^{\infty} a_kp^k) = a_n.$$

It is well-defined and it is a homomorphism because

$$\phi(\sum_{k=n} a_np^n \oplus_F \sum_{k=n}^{\infty} b_np^n) = a_n + b_n$$

as $A \oplus B = A + B$+higher order terms. Also, the kernel of the map is just $p^{n+1}\mathbb{Z}_p$.

(iii) We will omit this part of the proof but the idea is the same as what we did in Local Fields to prove $(1 + p\mathbb{Z}_p, *) \cong (\mathbb{Z}_p, +)$.

□

**Theorem 27.46.** *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}_p$ be a minimal model at $p$. Then the reduction*

$$E_0(\mathbb{Q}_p) \longmapsto \bar{E}_{ns}(\mathbb{F}_p)$$

*is injective on the torsion part provided $p$ is odd or $2\big|a_1$ if $p = 2$.*

*Proof.* By Corollary 27.43 and Theorem 27.44, we conclude that $E_1(\mathbb{Q}_p)$ has no points of finite order other than $\mathcal{O}$. Let $P$ be a point of finite order in $E_0(\mathbb{Q}_p)$ and $E_1(\mathbb{Q}_p)$ is the kernel of the map. But $\bar{E}_{ns}(\mathbb{F}_p)$ is a finite set with order at most $2p^2$.

Suppose $P, Q$ are both torsion points and if $P, Q$ reduce to the same point in the image, then $P \ominus Q$ is also torsion and it reduces to $\mathcal{O}$. So $P \ominus Q$ comes from $E_1(\mathbb{Q}_p)$ and hence $P \ominus Q = \mathcal{O}$ which proves the result. □

**Example 27.47.** *Let $E : y^2 + y = x^3 - x$. $\Delta_E = -11$ so it is a global minimal model. We have $(0,0), (0,-1), (1,0), (1,1), \mathcal{O}$ which are torsion points. Reduce mod 2, we have (as $a_1 = 0$)*

$$E(\mathbb{Q})_{tors} \leq E(\mathbb{Q}_2)_{tors} \leq \bar{E}(\mathbb{F}_2) \leq C_5,$$

*because it is easy to check that we have good reduction so $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$. But we have 5 distinct points already in $\bar{E}(\mathbb{F}_2)$ and hence it is $C_5$. So $E(\mathbb{Q})_{tors}$ is a subgroup of $C_5$ and we have 5 points so it is $C_5$.*

## 27.4 Decent

The last part of the section is on discussion of decent. Recall that the trick we used to prove Modell-Weil theorem is to prove $E(K)/2E(K)$ is finite first. This method is, in particular, called the 2-decent of elliptic curve. We will study further by using this method.

**Lemma 27.48.** *Let $E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$, $\alpha, \beta, \gamma$ distinct be an elliptic curve over $\mathbb{Q}$. Let $F$ be the maximal extension of the form $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots)$ which only ramifies at $p\big|2\Delta_E$. In other words, $a_i$ is either $-1$, 2 or prime factor of $\Delta_E$. Then*

*(i) For $P \in E(\mathbb{Q})$, we have $\mathbb{Q}(R) \subset F$, where $2R = P$.*

*(ii) The map*

$$\phi_P : Gal(F/\mathbb{Q}) \longmapsto E(\mathbb{Q})[2] \text{ via } \phi_P(\sigma) = \sigma(R) \ominus R$$

*is well-defined and is homomorphism.*

*(iii) The map*

$$\psi : E(\mathbb{Q})/2E(\mathbb{Q}) \longmapsto Hom(Gal(F/\mathbb{Q}), E(\mathbb{Q})[2]) \text{ via } \psi(P) = \phi_P$$

*is well-defined and is an injective homomorphism.*

*(iv)* $\ker \phi_P = Gal(F/\mathbb{Q}(R))$.

*Proof.* (i) Since $(\alpha, 0), (\beta, 0), (\gamma, 0), \mathcal{O}$ are the 2-torsion points and they lie in $E(\mathbb{Q})$ so we have $\mathrm{Gal}(\mathbb{Q}(R)/\mathbb{Q}) \leq C_2 \times C_2$ and $\mathbb{Q}(R) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. But Lemma 27.6 implies that $\mathbb{Q}(R)/\mathbb{Q}$ only ramifies at primes dividing $2\Delta_E$. Thus, we conclude

$$a, b \in \{-1, 2, p_i : p_i \big| \Delta_E\}.$$

Hence $\mathbb{Q}(R) \subset F$.

(ii) We firstly check it is well-defined. Suppose $R'$ is another point with $2R' = P$. Then $R \ominus R' = T \in E(K)[2]$ and so

$$\sigma(R) \ominus R = \sigma(R') \oplus \sigma(T) \ominus R' \ominus T = \sigma(R') \ominus R'$$

because $T \in E(K)[2]$ is fixed. Let $\sigma, \tau \in \mathrm{Gal}(F/\mathbb{Q})$. Then,

$$\phi(\sigma\tau) = \sigma(\tau(R)) \ominus R = \sigma(\tau(R)) \ominus \sigma(R) \oplus \sigma(R) \ominus R.$$

But $\tau(R) \ominus R \in E[K](2)$ and hence is fixed by $\sigma$. So the above gives

$$\phi(\sigma\tau) = \sigma(\tau(R) \ominus R) \oplus (\sigma(R) \ominus R) = \phi(\tau) \oplus \phi(\sigma).$$

(iii) Let $P = P'$ in $E(\mathbb{Q})/2E(\mathbb{Q})$, then $P' = P \oplus 2T$ for some $T \in E(K)$. Now $R + T$ is a choice such that $2R \oplus 2T = P'$, so

$$\phi_{P \oplus 2T}(\sigma) = \sigma(R + T) \ominus (R \oplus T) = \sigma(R) \ominus R.$$

Hence, the map is well-defined.

Given $P, P' \in E(K)/2E(K)$ and let $2R = P, 2R' = P'$. Then

$$\phi_{P \oplus P'}(\sigma) = \sigma(R \oplus R') \ominus (R \oplus R') = \phi_P \oplus \phi_{P'}.$$

So it is a homomorphism. Finally, if $\phi_P$ is a zero map, in other words, $\phi_P(\sigma) = \mathcal{O}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, then $R$ is fixed by the Galois group and hence $R \in E(\mathbb{Q})$. This shows that $P = 2R \in 2E(K)$. Hence the map is injective.

(iv) $\sigma \in \ker \phi_P$ if and only if $\sigma(R) = R$. But $\sigma(R) = R$ if and only if $\sigma(\mathbb{Q}(R)) = \mathbb{Q}(R)$. Then by Galois theory, this happens when $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(R))$.

□

**Remark 27.49.** *The lemma above implies that $P \in E(\mathbb{Q})/2E(\mathbb{Q})$ gives a biquadratic extension $\mathbb{Q}(R)/\mathbb{Q}$ independent of the choice of $R$ such that $2R = P$ and we have an associated homomorphism*

$$\phi_P : Gal(F/\mathbb{Q}) \longmapsto E(\mathbb{Q})[2] \cong C_2 \times C_2.$$

*Further by (iii) we can get an upper bound for $E(K)/2E(K)$ by computing $Hom(Gal(F/\mathbb{Q}), E(\mathbb{Q})[2])$.*

**Lemma 27.50.** *Let $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ be an elliptic curve over $\mathbb{Q}$, and set*

$$E(\mathbb{Q})[2] = \{\mathcal{O}, T_1, T_2, T_3\}.$$

*Let $P \in E(\mathbb{Q})$, $2R = P$ and $F = \mathbb{Q}(R)$. Then*

*(i) $Gal(F/\mathbb{Q})$ acts on the sets $S_i$ where*

$$S_{i,P} = \{\{R, R \oplus T_i\}, \{R \oplus T_j, R \oplus T_k\}\},$$

*where $i, j, k$ is any permutation of $1, 2, 3$. The kernel of the action on $S_{i,P}$ is*

$$H_{P,T_i} = \ker\left(Gal(F/\mathbb{Q}) \longmapsto E(\mathbb{Q})[2] \longmapsto E(\mathbb{Q}[2]/\{\mathcal{O}, T_i\})\right),$$

*where the map $Gal(F/\mathbb{Q}) \longmapsto E(\mathbb{Q})[2]$ is $\phi_P$ defined in previous lemma.*

*(ii) Let $F^{H_{P,T_i}} = \mathbb{Q}(\sqrt{a_{P,T_i}})$, $a_{P,T_i} \in \mathbb{Q}^*$. Then the map sending $P$ to $a_{P,T_i}$ is a homomorphism from $E(K)$ to $\mathbb{Q}^*$.*

*(iii) Let the map defined in (iii) be $\chi_i$ for each $i$. Then the map*

$$\chi : E(\mathbb{Q})/2E(\mathbb{Q}) \longmapsto \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$$

*defined by*

$$P \mapsto (\chi_1(P), \chi_2(P), \chi_3(P)) = (a_{P,T_1}, a_{P,T_2}, a_{P,T_3})$$

*is an injective homomorphism.*

*(iv) $\mathbb{Q}(R) = \mathbb{Q}(\sqrt{a_{P,T_1}}, \sqrt{a_{P,T_2}})$ with subfields $\mathbb{Q}(\sqrt{a_{P,T_i}})$, $i = 1, 2, 3$.*

*Proof.* We will prove the first two parts for $(i, j, k) = (1, 2, 3)$ as the rest is similar.

(i) It clearly defines an action because $T_i \oplus T_j = T_k$ for $i \neq j \neq k$. $\sigma \in H_{P,T_1}$ if and only if $\sigma$ sends $R$ to $R$ or to $R \oplus T_1$. Equivalently $\phi_P(\sigma) = \mathcal{O}$ or $T_1$, so the result follows.

(ii) Let $P'$ be another point and let $2R' = P'$. Note that the kernel has order 1 or 2 by (i). Then consider the action on the set

$$S = \{\{R \oplus R', R \oplus R' \oplus T_1\}, \{R \oplus R' \oplus T_2, R \oplus R' \oplus T_3\}\}.$$

Take $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\sigma(\sqrt{a_{P,T_1}}) = \pm\sqrt{a_{P,T_1}}$ and similarly for $P'$. $\sigma$ also acts on the sets $S_{i,P}, S_{i,P'}$ and $S$. Further, $\sigma$ fixes $\{R \oplus R', R \oplus R' \oplus T_1\}$ if and only if $\sigma$ either fixes both $\{R, R + T_1\}$ and $\{R', R' \oplus T_1\}$ or it fixes neither of them (using $T_2 \oplus T_3 = T_1$).

Moreover, by definition of $\sqrt{a_{P,T_1}}$, $\sigma$ fixes it if and only if $\sigma$ is in the kernel $H_{P,T_1}$ and $\sigma(\sqrt{a_{P,T_1}}) = -\sqrt{a_{P,T_1}}$ if and only if it is not in the kernel. Hence, by the above discussion, $\sigma$ is in the kernel of the action on $S$, if and only if $\sigma$ fixes $\sqrt{a_{P,T_1}a_{P',T_1}}$. Thus,

$$F^{H_{P\oplus P',T_1}} = \mathbb{Q}(\sqrt{a_{P,T_1}a_{P',T_1}})$$

and so it is a homomorphism.

(iii) Each $\chi_i$ is a homomorphism and so it is clear that $\chi$ is a homomorphism. Let $\chi(P) = (1,1,1)$ in the image. Equivalently, $a_{P,T_i}$ is a square for each $i$, and so the kernel of the action is the whole group for each $i$. If $\sigma(R) = R \oplus T_i$ then $\sigma$ cannot be in the kernel of the action on $S_{j,P}$ for $j \neq i$. Hence, $\sigma(R) = R$ for all $\sigma$. This implies that $R \in E(K)$ and so $P \in 2E(K)$. So the map is injective.

(iv) It is clearly that $\mathbb{Q}(\sqrt{a_{P,T_i}}) \subset F$ for each $i$. Recall that we have a homomorphism, if $\sigma(R) = R \oplus T_i$ then $\psi(\sigma) = T_i$ is an injective homomorphism (Lemma 27.5(iii)). So in fact $\mathbb{Q}(R)$ is biquadratic if and only if for each $T_i$ there exists $\sigma$ such that $\sigma(R) = R \oplus T_i$. This is the same as saying that each $H_{P,T_i}$ is a proper subgroup (take $\sigma$ which sends $R$ to $R \oplus T_j$ so the set is not fixed) and equivalently this says that none of $a_{P,T_i}$ is a square in $\mathbb{Q}$.

Further, $\mathbb{Q}(R)$ is quadratic if and only if there exists $T_i$ such that we have no $\sigma$ such that $\sigma(R) = R \oplus T_i$, but there exists $\sigma$ such that $\sigma(R) = R \oplus T_j$. Hence we also have no element such that $\sigma(R) = R \oplus T_k$. Thus, $H_{P,T_j}$ must be the same as the whole group. Also, $H_{P,T_i} = H_{P,T_k}$ and so $a_{P,T_i} = a_{P,T_k}$ in $\mathbb{Q}/\mathbb{Q}^{*2}$.

Finally, $\mathbb{Q}(R) = \mathbb{Q}$ if and only if $H_{P,T_i}$ is the whole group for each $i$ and so each $a_{P,T_i}$ is a square. Thus, from each given triple in the image $a_{P,T_i}$, $i = 1,2,3$, we can recover the field $\mathbb{Q}(R)$ as we know the degree of the extension and we know all the subfields.

□

**Remark 27.51.** *To each $P \in E(\mathbb{Q})/2E(\mathbb{Q})$, we associate $\mathbb{Q}(R), \phi_P$, and for each $T_i$ we have a corresponding quadratic (or trivial) extension characterised by $a_{P,T_i}$. Notice that the product of $a_{P,T_i}$ is a rational square because they together define a biquadratic extension.*

**Lemma 27.52.** *Let $E : y^2 = x^3 + Ax^2 + Bx$ be an elliptic curve over $K$, where Char$(K) \neq 2$. Then*

*(i) If $R = (x_0, y_0) \in E(K)$ then $2Q = \mathcal{O}$ or*

$$2Q = \left( \left( \frac{x_0 - \beta}{2y_0} \right)^2, \cdots \right).$$

*(ii) If $P = (x_0, y_0) \neq \mathcal{O}, P \in E(K)$ and take any $R$ with $2R = P$, then $K(\sqrt{x_0}) \subset K(R)$.*

*(iii) For $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, if $P = (x_0, y_0)$ and $2R = P$, then*

$$K(\sqrt{x_0 - \alpha}, \sqrt{x_0 - \beta}, \sqrt{x_0 - \gamma}) \subset K(R).$$

*Proof.* (i) is clear by direct computation. For (ii), let $R = (x_1, y_1)$ then by (i), we have $x_0 = \left(\frac{x_1 - \beta}{y_1}\right)^2$ and so $x_0 = 2\sqrt{x_0}y_1 + \beta$. Thus, $\sqrt{x_0} = \frac{x_1 - \beta}{2y_1}$ and so $\sqrt{x_0} \in K(R)$.

For (iii), shift $x$ by $-\alpha$, we have $y^2 = x(x + \alpha - \beta)(x + \alpha - \gamma)$ and $P = (x_0 - \alpha, y_0)$ in the new coordinate and hence $\sqrt{x_0 - \alpha} \in K(R)$ by (ii). Similarly, shift $x$ by $-\beta$ (resp. $-\gamma$), we have $\sqrt{x_0 - \beta}$ (resp $\sqrt{x_0 - \gamma}$) $\subset K(R)$. □

**Lemma 27.53.** *Let $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ be an elliptic curve over $\mathbb{Q}$. If $P = (x_0, y_0)$, then*

$$a_{P,(\alpha,0)} = x_0 - \alpha \text{ if } P \neq (\alpha, 0),$$

$$a_{P,(\beta,0)} = x_0 - \beta \text{ if } P \neq (\beta, 0),$$

$$a_{P,(\gamma,0)} = x_0 - \gamma \text{ if } P \neq (\gamma, 0).$$

*Proof.* We give a sketch of the proof. We can compute $R$ where $2R = P$ and compute $R \oplus (\alpha, 0)$, $R \oplus (\beta, 0)$ and $R \oplus (\gamma, 0)$, in terms of $(x_0, y_0)$. Then we can check that

$$\mathbb{Q}(R) = \mathbb{Q}(\sqrt{x_0 - \alpha}, \sqrt{x_0 - \beta}, \sqrt{x_0 - \gamma}),$$

and $\mathrm{Gal}(\mathbb{Q}(R)/\mathbb{Q})$ fixes $\sqrt{x_0 - \alpha}$ if it preserves the pair $\{R, R \oplus (\alpha, 0)\}$ etc. so that $a_{P,(\alpha,0)} = x_0 - \alpha$. (Follow the proof of Lemma 27.50)

Alternatively, we can consider $E : y^2 = (x - t_1)(x - t_2)(x - t_3)$ over

$$K = \mathbb{Q}(t_1, t_2, t_3, X)[Y]/\langle Y^2 - X^3 - \cdots \rangle.$$

It is a field of characteristic 0. Note that $P = (X, Y) \in E(K)$ and $E(K)[2] = \{\mathcal{O}, (t_1, 0), (t_2, 0), (t_3, 0)\}$. Also, if $2R = P$ then $\mathrm{Gal}(K(R)/K) \leq C_2 \times C_2$. Then by the previous lemma (iii) we know $K(\sqrt{x - t_i}) \subset K(R)$. So we conclude that

$$K(R) = K(\sqrt{x - t_1}, \sqrt{x - t_2}, \sqrt{x - t_3}) \text{ and } \prod_i \sqrt{x - t_i} = Y.$$

So we may assume that

$$R = (a + b\sqrt{x - t_1} + c\sqrt{x - t_2} + d\sqrt{x - t_3}, e + f\sqrt{x - t_1} + g\sqrt{x - t_2} + h\sqrt{x - t_3}), a, b, c, d, e, f, g, h \in K.$$

Also, since the Galois element permutes the half points of $P$, and they only switch the sign of $\sqrt{x - t_i}$ thus the other half points of $P$ are obtained by switching signs properly. But we have picked $t_1, t_2, t_3$ in any order and so we can assume that $t_2, t_3$ are symmetric. Also the product must be preserved by Galois and hence each Galois element must switch precisely two signs.

On the other hand, the half points of $P$ are $R, R \oplus (t_i, 0)$. Use the fact that $t_2, t_3$ are symmetric, we have

$$R \oplus (t_1, 0) = (a + b\sqrt{x - t_1} - c\sqrt{x - t_2} - d\sqrt{x - t_3}, e + f\sqrt{x - t_1} - g\sqrt{x - t_2} - h\sqrt{x - t_3}).$$

These are purely algebraic statement. Now we can set $X = x_0, Y = y_0, \alpha = t_1, \beta = t_2, \gamma = t_3$ and $K = \mathbb{Q}$. Thus we have shown that $\mathbb{Q}(\sqrt{x_0 - \alpha}, \sqrt{x_0 - \beta}, \sqrt{x_0 - \gamma})$ is the field we want. Now that $\{R, R \oplus (\alpha, 0)\}$ is preserved by $\mathrm{Gal}(\mathbb{Q}(R)/\mathbb{Q}(\sqrt{x_0 - \alpha}))$ by above as it does not switch the sign of $\sqrt{x_0 - \alpha}$. So $a_{P,(\alpha,0)} = x_0 - \alpha$ and similarly for others. Note that when $P = (\alpha, 0)$ the argument does not work simply because 0 is not in the image of the map defined in Lemma 27.50 (ii). □

We shall give some worked examples.

**Example 27.54.** *$E : y^2 = (x - 1)x(x + 1)$. For $P \in E(\mathbb{Q})$, $\mathbb{Q}(R)$ only ramifies at 2 and so $\mathbb{Q}(R) \leq \mathbb{Q}(i, \sqrt{2})$ (where $2R = P$). We have shown the rank is $\leq 2$ in Example 27.12.*

*Let $P = (x_0, y_0)$. If $P$ is not the two torsion points, then by previous theorem we have, under the homomorphism $\chi$, $\chi(P) = (x_0, x_0 - 1, x_0 + 1)$. But $\mathbb{Q}(R) = \mathbb{Q}(\sqrt{x_0}, \sqrt{x_0 - 1})$ and so we must have $x_0, x_0 - 1, x_0 + 1 = \pm 1, \pm 2$ up to rational square. We shall list all the possibilities.*

*Since $x_0(x_0 - 1)(x_0 + 1)$ is a rational square, so the third one is determined by the previous two. Also, note that when $P = (\alpha, 0)$ we just work out $x_0 - \beta, x_0 - \gamma$ and then obtain $x_0 - \alpha$ by the above fact. Thus, we can have at most 16 possibilities for $x_0$ and $x_0 - 1$. We shall use the pair $[a, b]$ to denote the value of $(x_0, x_0 - 1)$ modulo a rational square.*

*$\mathcal{O}$ must be mapped to the identity, which is $[1, 1]$. For $P = (0, 0)$, $x_0 = 0$ so we can work out $x_0 - 1 = -1, x_0 + 1 = 1$ and so $x_0$ must be $-1$ as the product is a rational square. So this gives $[-1, -1]$. Similarly, the other two torsion points give $[1, 2], [-1, -2]$.*

*Now if $x_0 - 1 > 0$ then $x_0 > 0$ because any rational square times a positive integer is again positive, and if we add 1 we shall again get a positive number. So we can rule out $[-1, 1], [-1, 2].[-2, 1], [-2, 2]$. Also, the map is a homomorphism, so if $[x, y]$ is in the image but $[u, v]$ is not, then $[xu, yv]$ cannot be in the image. Hence, we can also rule out, $[1, -1], [1, -2], [2, -2], [-2, -2]$.*

*Further, we shall rule out* $[2,1]$. *Suppose* $x_0 = 2A^2, x_0 - 1 = B^2, x_0 + 1 = C^2$. *Then*

$$2A^2 - 1 = B^2, 2A^2 + 1 = 2C^2.$$

*Setting* $A = \frac{a}{z}$ *we have,*

$$2a^2 - z^2 = (Bz)^2, 2a^2 + z^2 = 2(Cz)^2.$$

*Clearly,* $a, z, Bz, Cz$ *must be integers. Reduce modulo* 8, *we have, if* $2 \big| a$, *then* $-1$ *is a square modulo* 8, *which is impossible; If* $2 \nmid a$, *then* $a^2 \equiv 1 \pmod 8$ *and so* $2 - z^2$ *is a square modulo* 8 *and* $2 + 2z^2$ *is twice a square modulo* 8 *and this cannot happen. Hence* $[2,1]$ *is not in the image.*

*Therefore, we have at most* 7 *points in* $E(K)/2E(K)$ *(recall that the map* $\chi$ *is injective) and since* $C_2 \times C_2$ *lives inside* $E(K)/2E(K)$, *so we have* $|E(K)/2E(K)| = 4$. *Therefore the rank is* 0.

**Theorem 27.55.** **[2-descent]** *Let* $K$ *be a field of characteristic* 0 *and* $E/K$ *an elliptic curve given by the equation* $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$. *Then*

*(i) If* $P = (x_0, y_0)$, *then the map sending* $P$ *to* $(x_0 - \alpha, x_0 - \beta, x_0 - \gamma)$ *(where we replace* $x_0 - \alpha$ *by* $(x_0 - \beta)(x_0 - \gamma)$ *if* $P = (\alpha, 0)$ *and similarly for the other two cases) is an injective homomorphism from* $E(K)/2E(K)$ *to* $K^*/K^{*2} \times K^*/K^{*2} \times K^*/K^{*2}$.

*(ii) A triple* $(a, b, c)$ *that lies in the image satisfies* $abc \in K^{*2}$. *It lies in the image if and only if:*
*It is either the image of* $\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)$;
*Or the equations*

$$cz_3^2 - \alpha + \gamma = az_1^2, az_3^2 - \beta + \gamma = bz_2^2$$

*are soluble simultaneously with* $z_i \in K^*$, *in which case,* $P = (az_1^2 + \alpha, \sqrt{abc} z_1 z_2 z_3)$ *maps to* $(a, b, c)$.

*(iii) For* $K = \mathbb{Q}$, *pick any triple* $(a, b, c)$ *and we can pick* $a, b, c$ *square free. Then* $a, b, c$ *only has prime factors dividing* $2(\alpha - \beta)(\beta - \gamma)(\gamma - \beta)$.

*Proof.* (i) is an analogue of Lemma 27.53. The proof works the same because $\mathrm{Char}(K) = 0$. For (ii), if it is not any of the 2-torsion points, then by (i) we have some $x_0$ and $z_i$ such that

$$x_0 - \alpha = az_1^2, x_0 - \beta = bz_2^2, x_0 - \gamma = cz_3^2.$$

Then the solvability of these two equations is the same condition as in (ii). When it is soluble, we set $az_1^2 + \alpha = x_0$, and $y_0^2 = (x_0 - \alpha, x_0 - \beta, x_0 - \gamma)$. Finally for (iii), let $2R = P$. Recall that $\mathbb{Q}(R) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with intermediate subfields $\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{b}), \mathbb{Q}(\sqrt{c})$ by Lemma 27.50(iv) and we know $\mathbb{Q}(R)$ only ramifies at prime dividing $2\Delta_E$ and since we pick $a, bc$ square free, so they can only have prime factor dividing $2(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$. □

**Remark 27.56.** *To get the rank of* $E\mathbb{Q}$ *we study the triples in the image. We can get a lower bound for* $E(\mathbb{Q})/2E(\mathbb{Q})$ *by finding different points. We can get an upper bound by counting the number of triples in the image. Condition (ii) above can be discussed in more detail. For example, if one has an equation which is not soluble over* $\mathbb{Q}_p$ *then it is definitely not soluble over* $\mathbb{Q}$. *In fact, by Minkowski's theorem, any quadratic equations is soluble over* $\mathbb{Q}$ *if and only if it is soluble over* $\mathbb{Q}_p$ *for all* $p$ *and* $\mathbb{R}$. *So we can rule out some possibilities by considering the curve over* $\mathbb{Q}_p$ *or over* $\mathbb{R}$.

**Proposition 27.57.** *Let* $E/\mathbb{Q}$ *be an elliptic curve* $E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$, *where* $\alpha, \beta, \gamma$ *are distinct and* $E$ *is a global minimal model. Then*

*(i) If* $p$ *is odd then the size of* $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ *is 4.*

*(ii) If $p \nmid 2\Delta_E$ then $\mathbb{Q}(R)$ is unramified at $p$, where $2R = P \in E(\mathbb{Q}_p)$.*

*(iii) For $p \nmid 2\Delta_E$, $(a_1, a_2, a_3)$ lies in the image of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ if and only if $ord_p(a_i)$ is even for all $i$.*

*Proof.* Recall that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{p, 1, j, jp\}$ where $j$ is not a quadratic residue mod $p$.

(i) Recall that $E_1(\mathbb{Q}_p) \subset E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ and the indices are finite. We have an exact sequence

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \to 0.$$

Define the maps $f, g, h$ to be the multiplication by 2 on $E_1(\mathbb{Q}_p), E(\mathbb{Q}_p)$ and $E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ respectively. Then apply snake's lemma (which you may refer to some theory in commutative algebra), we have a long exact sequence

$$0 \to \ker f \to \ker g \to \ker h \to \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0.$$

When $p$ is odd we have $p \nmid 2$ and so $[2]$ is and isomorphism on $E_1(\mathbb{Q}_p)$. So $\ker f = 0$ and $\mathrm{coker} f = 0$. Thus,

$$\ker g \cong \ker h, \mathrm{coker} g \cong \mathrm{coker} h.$$

Therefore,

$$|E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)| = |\mathrm{coker} g| = |\mathrm{coker} h| = |\ker h| = |\ker g| = |E(\mathbb{Q}_p)[2]| = 4.$$

We should briefly justify why $|\mathrm{coker} h| = |\ker h|$. Let $h$ be an endomorphism of finite group $G$. Then

$$G/\ker h \cong \mathrm{Im} h.$$

Then $|G| = |\ker h||\mathrm{Im} h|$. But $|G| = |\mathrm{Im} h||\mathrm{coker} h|$ so they have the same size.

(ii) This is just an analogue of the case $\mathbb{Q}$. The proof is identical.

(iii) $\mathbb{Q}_p$ also has characteristic 0 and so $\mathbb{Q}_p = \mathbb{Q}_p(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$. By (ii) it is unramified at $p$. Also, $a_i$ can be chosen to be one of $1, p, j, jp$. Hence, if it is $p$ or $jp$, then it must ramify at $p$. So each $a_i$ is either 1 or $j$ and so $ord_p(a_i)$ is even.

□

**Example 27.58.** *$E : y^2 = x(x-5)(x+5)$. Note that $P = (-4, 6) \in E(\mathbb{Q})$ and $\Delta_E = 2^6 \cdot 5^6$. We have four points in the image, given by the 2-torsion points, which are $[1, 1], [-1, -5], [5, 2], [-5, -10]$, where $[a, b]$ denotes the pair of the value of $(x_0, x_0 - 5)$ in the image. Also, $[4, 6]$ gives $[-1, -1]$. As the map is a homomorphism, we conclude that $[1, 5], [-5, -2], [5, 10]$ are also in the image. So we have 8 points already.*

*Now if $x_0 > 0$ then $x_0 + 5 > 0$. If $x_0 < 0$ then $x_0 - 5 < 0$. So the sign of the triple is either $+, +, +$ or $-, -, +$.*

*Finally, we consider $E(\mathbb{Q}_5)$. We know $|E(\mathbb{Q}_5)/2E(\mathbb{Q}_5)| = 4$ and we have $\mathbb{Q}_5^*/\mathbb{Q}_5^{*2} = \{1, 2, 5, 10\}$. Also note that $-1$ is a square in $\mathbb{Q}_5$. The torsion points give $(1, 5, 5), (5, 2, 10), (5, 10, 2), (1, 1, 1)$ and these four points are representatives for $E(\mathbb{Q}_5)/2E(\mathbb{Q}_5)$. So we need to find all associated points to these. In other word, say $(1, 5, 5)$, we have $(-1, -5, -5)$ is the same as $(1, 5, 5)$ modulo $\mathbb{Q}_5^{*2}$. Hence it is possible that in the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ we have $(-1, -5, -5)$. Therefore, we list all the possible associated points, which gives*

$$[\pm 1, \pm 5], [\pm 5, \pm 2], [\pm 5, \pm 10], [\pm 1, \pm 1].$$

*But according to the sign discussion above we can only have*

$$[1,5],[-1,-5],[5,2],[-5,-2],[5,10],[-5,-10],[1,1],[-1,-1].$$

*So there are at most* 8 *points. Combine this with the result in the first paragraph, we conclude that*

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 8.$$

*Hence the rank is precisely* 1.

## 27.5 Exercises

1. Suppose $A$ is an abelian group with $A/2A$ finite that admits a function $h : A \longmapsto \mathbb{R}_{\geq 0}$ satisfying

   (i) For every $C \in \mathbb{R}$ there are only finitely many $x \in A$ with $h(x) < C$, and

   (ii) $h(x+y) + h(x-y) = 2h(x) + 2h(y) + O(1)$, where the implied constant is independent of $x, y \in A$.

   By expressing $x \in A$ as $x = a_1 + 2a_2 + \cdots + 2^n a_n + 2^{n+1}y$, where $a_i$ are fixed representatives $A/2A$, prove that $A$ must be finitely generated.

2. Let $E/K$ be an elliptic curve over a number field, and $F/K$ a finite extension. Prove that $\mathrm{rk}E/F \geq \mathrm{rk}E/K$.

3. Let $E/\mathbb{Q}$ be an elliptic curve given by

   $$y^2 = (x-\alpha)(x-\beta)(x-\gamma), \alpha, \beta, \gamma \in \mathbb{Z}.$$

   Find a very crude but completely explicit bound on the rank of $E/\mathbb{Q}$ in terms of $\alpha, \beta, \gamma$.

4. Let $E/K$ be an elliptic curve over a number field, such that $E(K)[2] \cong C_2 \times C_2$. Fix representatives $P_1, \ldots, P_k$ for $E(K)/2E(K)$ and let $Q_i \in E(\bar{K})$ satisfy $2Q_i = P_i$. Show that the number field $F = K(Q_1, \ldots, Q_k)$ generated by the $x$ and $y$ coordinates of the $Q_i$ has Galois group of the form $G = \mathrm{Gal}(F/K) \cong C_2 \times \cdots \times C_2$. By considering the injective homomorphism from $E(K)/2E(K)$ to $\mathrm{Hom}(G, E(K)[2])$ given by $P_i \mapsto f_{P_i}$, where $f_{P_i} : \sigma \to \sigma(Q_i) \ominus Q_i$, deduce that the rank of $E/K$ is at most $2n-2$, where $G \cong C_2 \times \cdots \times C_2$ ($n$ times).

5. Let $E/K$ be an elliptic curve over a number field given by $y^2 = x^3 + ax^2 + bx + c$. For $d \in K^*$, the **quadratic twist** of $E$ by $d$ is the elliptic curve given by

   $$E_d : dy^2 = x^3 + ax^2 + bx + c.$$

   Prove that $E$ and $E_d$ are isomorphic over $K(\sqrt{d})$ and that (for $\sqrt{d} \notin K$)

   $$\mathrm{rk}E/K(\sqrt{d}) = \mathrm{rk}E/K + \mathrm{rk}E_d/K.$$

6. Let $E/\mathbb{Q}$ be an elliptic curve and write $K = \mathbb{Q}(E[p])$ for the number field generated by the $x$ and $y$ coordinates of the points in $E(\mathbb{C})$ of order $p$. Show that $\mathrm{Gal}(K/\mathbb{Q}) \leq \mathrm{GL}_2(\mathbb{F}_p)$.

7. Prove that the rank of elliptic curves over number fields can be arbitrarily large.

8. Show that $E : y^2 + y = x^3 + x^2 + x$ has three points of finite order.

9. Show that $E : y^2 + y = x^3 - x^2$ has discriminant $-11$ and that it has split multiplicative reduction at 11. By looking at $E/\mathbb{Q}_{11}$ show that $E(\mathbb{Q})_{\text{tors}} \cong C_5$. (Hint: Observe that $(0, 0)$ has order 5).

10. Show that if $E$ does not have multiplicative reduction at $2, 3$ or 5, then $|E(\mathbb{Q})_{\text{tors}}| \leq 6$.

11. Let $E : y^2 = x(x+5)(x-5)$. Show that the equation is minimal at 5 and that $E(\mathbb{Q}_5)/E_0(\mathbb{Q}_5) \cong C_2 \times C_2$ and $E_0(\mathbb{Q}_5)/E_1(\mathbb{Q}_5) \cong C_5$.

12. Let $p$ be an odd prime and $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weierstrass equation. Show that the $x$-coordinate of any given point in $E_1(\mathbb{Q}_p)$ is a perfect square.

13. Compute the rank of $E : y^2 = x(x + 3)(x - 6)$ over $\mathbb{Q}$. (Hint: $(-2, 4) \in E(\mathbb{Q})$.)

14. Compute the rank of $E : y^2 = x^3 - 49x$ over $\mathbb{Q}$. (Hint: $(25, 120) \in E(\mathbb{Q})$.)

15. Let $E : y^2 = x(x + 5)(x - 5)$. Note that the discriminant is $2^6 5^6$ and $(-4, 6) \in E(\mathbb{Q})$.
    (i) List the primes of all bad reduction for $E$.
    (ii) Prove that the torsion group is $C_2 \times C_2$.
    (iii) Show that $E(\mathbb{Q}_5)/2E(\mathbb{Q}_5) \cong C_2 \times C_2$, all coming from $E/E_0$.

16. Let $E : y^2 = x(x - 6)(x + 6)$. Note that $(-3, 9) \in E(\mathbb{Q})$. You may assume that the torsion group is $C_2 \times C_2$.
    (i) Find all primes where $E$ has bad reduction.
    (ii) Show that $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2) \cong C_2 \times C_2$, all coming from the 2-torsions of $E$.
    (iii) Show that $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \cong C_2 \times C_2 \times C_2$.
    (iv) Deduce that $E$ has rank 1.

## 27.6 Hint and Solutions

1. We obtain $a_i$ as follows: For any $x$, let $a_i \in A$ such that $x - a_1 \in 2A$. Then let $2x_1 = x - a_1$. Let $x_1 - a_2 \in 2A$, and so on. Thus we can write, for any $n$ that

$$x = a_1 + 2a_2 + 4a_3 + \cdots + 2^n a_{n+1} 2^{n+1} y, a_i \in A/2A.$$

Now plug in $x = y = 2^n a$ in the second condition we have

$$h(2^{n+1}a) + h(0) = 4h(2^n a) + O(1).$$

Writing the constant explicitly, we have $h(2^{n+1}a) = 4h(2^n a) + c - h(0)$. Thus, we have

$$h(a) = \frac{h(2^n a)}{4^n} + \frac{4^n - 1}{3 \cdot 4^n}(c - h(0)).$$

Thus for large $n$, $h(a)$ is roughly $\frac{h(2^n a)}{4^n} + \frac{1}{3}(c - h(0))$.

Also, we know $h$ only takes positive value so $h(a+b) + h(a-b) = 2h(a) + 2h(b) + c$ and so $h(a+b) \leq 2h(a) + 2h(b) + c$. Then

$$h(a_1 + \cdots + 2^n a_{n+1}) \leq 2h(a_1 + \cdots + 2^{n-1} a_n) + 2h(2^n a_{n+1}) + c.$$

Proceed this estimate we conclude that

$$h(a_1 + \cdots + 2^n a_{n+1}) \leq 4\frac{4^n d}{3} + \left(\frac{4^n}{3} + \frac{(n-1)n}{2}\right) c$$

where $d = \min_i h(a_i)$ which exists as $A/2A$ is finite.

Now use $2^{n+1}y = x - a_1 - 2a_2 - \cdots$, we have

$$h(2^{n+1}y) \leq 2h(x) + 2h(a_1 + \cdots + 2^n a_{n+1}) + c \leq 2h(x) + 2\frac{4^{n+1}d}{3} + 2\left(\frac{4^n}{3} + \frac{(n-1)n}{2}\right) c.$$

But for $n$ large, $h(2^{n+1}y)$ is roughly $4^{n+1}h(y) + \frac{c}{3}$, so $h(y) \leq \frac{2h(x)}{4^{n+1}} + \frac{1}{3}d + a$ for some constant $a$, for $n$ large. So we pick $n$ large such that $\frac{2h(x)}{4^{n+1}} + a \leq C$ for a fixed constant $C$. Then we only have finitely many such $y$ by assumption, say $y_1, \ldots, y_k$. Thus $A$ is generated by $A/2A$ and $y_1, \ldots, y_k$.

Note that what we have done above is just approximate the height and try to pick $n$ large so that $h(y)$ is below a certain bound. There might be a better way to approximate this.

2. Let $E(F) \cong \Delta' \times \mathbb{Z}^m$ and $f_1, \ldots, f_m$ be the generator of $\mathbb{Z}^m$. Since $E(K) \subset E(F)$ so each $e_i$ can be written as

$$e_i = b_i \prod_{j=1}^{m} f_j^{\alpha_{ij}}, b_i \in \Delta'.$$

Each $b_i$ has finite order, say $n_i$ and so

$$e_i^{n_i} = \prod_{j=1}^{m} f_j^{\beta_{ij}}$$

where $\beta_{ij} = n_i \alpha_{ij}$. If $m < n$, then we have $n$ equations with $m$ variables for $f_j$. So we have a non-trivial relation, say

$$\prod_{i=1}^{n} \prod_{j=1}^{m} f_j^{k_i \beta_{ij}} = 1.$$

Then this implies that

$$\prod_{i=1}^{n} e_i^{n_i k_i} = 1.$$

But $\{e_1, \ldots, e_n\}$ is a basis so we have $n_i k_i = 0$ for each $i$. But $n_i \neq 0$ for all $i$, and not all $k_i$ are zero as the relation is non-trivial. This gives a contradiction. So $m \geq n$.

3. Note that by theorem the map $P \mapsto \mathbb{Q}(\frac{1}{2}P)$ is at most 16-to-1. Also, we know $\mathbb{Q}(\frac{1}{2}P)$ ramifies only at primes dividing $2(\alpha-\beta)(\beta-\gamma)(\alpha-\gamma) = 2d$. Thus we can only have $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ where $a, b \big| 2d$.

   The number of possible factors of $N$ is at most $N$ and so the number of possible fields is at most $(2d)^2$. So

   $$|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 16 \cdot (2d)^2.$$

   Then the rank is at most $\log_2(16(2d)^2) - 2$ as we have $C_2 \times C_2$ the torsion group inside $E(\mathbb{Q})/2E(\mathbb{Q})$. So the rank is at most $2 + 2\log_2(2d)$.

4. We know $K(Q_i) = K(\sqrt{a_i}, \sqrt{b_i})$ and so $F = K(\sqrt{a_1}, \sqrt{b_1}, \sqrt{a_2}, \sqrt{b_2}, \ldots)$. Then the Galois group is a product of $C_2$.

   The map is an injective homomorphism by using an analogue of Lemma 27.48(iii). For the rank, we have all the 2-torsion points, and since the map is injective, we have

   $$|E(K)/2E(K)| \leq |\mathrm{Hom}(G, E(K)[2])|.$$

   But $G \cong (\mathbb{Z}/2\mathbb{Z})^n$. So we have $n$ generators for $G$ and each of them can be sent to any of the four points in the image, in $\mathrm{Hom}(G, E(K)[2])$. Thus, we have at most $4^n$ points in $E(K)/2E(K)$ and so the rank is at most $2n - 2$.

5. Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle\sigma\rangle$ and so $\sigma(\sqrt{d}) = -\sqrt{d}$. For any $P \in E(\mathbb{Q}(\sqrt{d}))$, we have

   $$2P = (\sigma+1)P \oplus (1-\sigma)P = Q \oplus R.$$

   where $(\sigma+1)P$ means $\sigma(P) \oplus P$ and $(1-\sigma)P$ means $P \ominus \sigma(P)$. Further, $\sigma(Q) = Q$ and $\sigma(R) = \ominus R$.

   We claim that

   $$2E(\mathbb{Q}(\sqrt{d})) \cong E(K) + E_d(K).$$

   Indeed, if $R$ has coordinate $(x, y)$ then $\ominus R$ has coordinate $(x, -y)$ and so if $\sigma(R) = \ominus R$ then $\sigma(x) = x, \sigma(y) = -y$. Then $x \in \mathbb{Q}$ and we set $y = a + b\sqrt{d}$, then $\sigma(y) = -y$ implies that $a = 0$ and so $y = b\sqrt{d}$. But consider the equation of $E_d$,

   $$dy^2 = x^3 + ax^2 + bx + c \iff y'^2 = x'^3 + ax'^2 + bx' + c$$

   via $y' = \sqrt{d}y, x' = x$. So these two are isomorphic and hence we have proved the claim. For the intersections, let $(\sigma+1)P = (1-\sigma)P$, then we have $2\sigma(P) = \mathcal{O}$ and so we have 4 intersections.

   Now by previous claim, and the fact that $E(K)$ and $E_d(K)$ have finite intersections, we conclude that the rank of $E(\mathbb{Q}(\sqrt{d}))$ is the sum of the rank of $E(\mathbb{Q})$ and $E_d(\mathbb{Q})$.

6. The points of order $p$ together with $\mathcal{O}$ forms a group $(\mathbb{Z}/p\mathbb{Z})^2$. Suppose the group is generated by two points, say $Q_1$ and $Q_2$. Then any other points can be written as $aQ_1 \oplus bQ_2, a, b \in \{0, 1, \ldots, p-1\}$. Thus, $K = \mathbb{Q}(Q_1, Q_2)$ and the Galois group will permute these points. Each element is determined by the image of $Q_1$ and $Q_2$.

   Now for any $\sigma$ in the Galois group, it corresponds to a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

   where $\sigma(Q_1) = aQ_1 \oplus bQ_2, \sigma(Q_2) = cQ_1 \oplus dQ_2$ and it is invertible because $\sigma$ is an automorphism. Therefore,

$$\mathrm{Gal}(K/\mathbb{Q}) \leq \mathrm{GL}_2(\mathbb{F}_p).$$

7. Consider $E : y^2 = x^3 - x$. The twist $E_d : dy^2 = x^3 - x$ is isomorphic to $y^2 = x^3 - d^2x$. Then by question 5, we have

$$\mathrm{rk}E(K(\sqrt{d})) = \mathrm{rk}E/K + \mathrm{rk}E_d/K.$$

   Thus, we can use an inductive argument, so that for any $r$ we have an elliptic curve over some number field with rank $r$. But we need to make sure that we can always pick $d$ so that $\mathrm{rk}E_d/K \neq 0$ for a given number field $K$. This can be done by showing we have some non-torsion points on $E_d$.

   Pick $d \equiv 1 \pmod 5$ and $\sqrt{d}$ is not in the given number field. (By Dirichlet's theorem, there are infinitely many prime which is congruent to 1 modulo 5). Reduce $E_d$ mod 5 we have $y^2 = x^3 - x$ which is non-singular and so we have good reduction. We have injection from torsion points on $E_d$ to $E_d(\mathbb{F}_p)$. So for this curve, the torsion points on $y^2 = x^3 - x$ over $\mathbb{F}_5$ are fixed, say $n$. Thus, if we have an element of order greater than $a$, it cannot be torsion. For these $n$ points, the canonical height $\hat{h}$ is 0, and so the height is below some certain constant. So we only need to find some element $P = (x, y)$ on $E_d$ such that $h(P) = h(x)$ (recall that the height only depends on the $x$-coordinate) is large.

   We have an alternative method. Pick $x = N$ and solve $y = \sqrt{N^3 - N}$ for the given number field $K$. Let $F = K(\sqrt{N^3 - N})$. If $\sqrt{N^3 - N} \in K$, then we replace $N$ by $Nq$ such that $\sqrt{q} \notin K$. This is possible because there is no number field with $\sqrt{q} \in K$ for all prime. Also $(Nq)^3 - Nq$ has a factor $q$ so $\sqrt{(Nq)^3 - Nq} \notin K$.

   Let $x = N$. The height $\hat{h}$ only depends on $x$. So over $F$, we have got a new point $P = (N, \sqrt{N^3 - n})$ and pick $N$ large enough so that $h(N)$ is large and so $\hat{h}(N) \neq 0$. This gives a point of infinite order. Also, we need to make sure that this is a point which is not a quotient of some point in the field $K$, i.e. we don't want $nP \in E(K)$ for some $n$.

   But we now that $nP = (f(N), \sqrt{N^3 - N}g(N))$, where $f, g$ are rational functions (see question 8 of Exercise 26). But $\sqrt{N^3 - N} \notin K$ and $g(N) \in K$, so $nP \notin K$ for all $n$.

   Therefore, the point $P$ introduce another generator (possibly a quotient of $P$) and so

$$\mathrm{rk}E/F \geq \mathrm{rk}E/K + 1.$$

   Continue this construction.

8. $a_1 = 0$ and the discriminant is $-19$. So it is a minimal model at 2. It has good reduction at 2. So we have

$$E(\mathbb{Q})_{\mathrm{tors}} = E_0(\mathbb{Q})_{\mathrm{tors}} \leq E_0(\mathbb{Q}_2)_{\mathrm{tors}} = \bar{E}(\mathbb{F}_2) \leq \mathbb{Z}/3\mathbb{Z}.$$

   But $(0, 0)$ has order 3 and so the torsion group is cyclic of order 3.

9. By a shift,
$$\left(y+\frac{1}{2}\right)^2=\left(x-\frac{1}{3}\right)^3-\frac{1}{3}\left(x-\frac{1}{3}\right)-\frac{2}{27}+\frac{1}{4}$$
we conclude that $\Delta f(x)=-\frac{11}{16}$ and so $\Delta E=-11$.

Consider the curve mod 11 and complete the square, we have
$$y^2=x^3-x^3+4^{-1}=x^3-x^2+3=(x-7)(x+3)^2.$$
The only singular point is $(-3,0)$. Then put in the required form, we have
$$y^2=x^2(x-10)$$
where $-10=1$ is a square, so it has split multiplicative reduction at 11.

$(0,0)$ has order 5 and $ord_{11}(-11)=1$ so $E_0(\mathbb{Q}_{11})=E(\mathbb{Q}_{11})$. Thus, the torsion points inject into $\bar{E}(\mathbb{F}_{11})=\mathbb{Z}/10\mathbb{Z}$ because it has split multiplicative reduction. Further, by considering reduction at 2, it has at most 5 torsion points and so it is $\mathbb{Z}/5\mathbb{Z}$.

10. Let $c_p$ be the size of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. It has no multiplicative reduction so $c_p\leq 4$.

Let $P$ be a torsion point and it has order $l$ with $l$ prime. Suppose $l>5$, then $P\notin E_1(\mathbb{Q}_2)$ and $P$ has order $l$ in $E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)$. But
$$|E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)|=|E(\mathbb{Q}_2/E_0(\mathbb{Q}_2)|\cdot|E_0(\mathbb{Q}_2/E_1(\mathbb{Q}_2)|=c_2\cdot\alpha$$
where $\alpha\leq 5$, and it is not divisible by $l$, which gives a contradiction.

Thus we can only have $2^n,3^n$ or $5^n$ torsion points. For $3^n$, consider the size of $E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)$ we conclude $n\leq 1$. For $5^n$, consider $E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)$ we conclude $n\leq 1$. For $2^n$, consider $E(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$, and recall that $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)\cong\bar{E}(\mathbb{F}_3)$. If it has good reduction at 3, then it has at most 7 points so $n\leq 2$. If it has additive reduction, then $c_3\leq 4$, and $\bar{E}(\mathbb{F}_3)$ has 3 points so we again have $n\leq 2$.

If we have 5-torsion, then we must have good reduction at 2 and so we have at most 5 torsion points. If we have no 5-torsion, but 3-torsion, then if we have good reduction at 5, then we have at most 2 lots of 2-torsions (because it has at most 11 points, if we have 4 lots of 2-torsions, we will have 12 points). If we have additive reduction at 5 then we have no 2-torsion because $c_5$ must be 3. So we have 3 points. Finally, if we have no 5-torsion or 3-torsion, then we have at most 4 points, all coming from $2^n$-torsions, $n\leq 2$.

11. The discriminant is $5^62^6$ and so it is minimal at 5. It has additive reduction at 5. Consider the 2-torsions, they give different representatives in $E(\mathbb{Q}_5)/E_0(\mathbb{Q}_5)$ because if not, then the difference is another 2-torsion, which lies in $E_0(\mathbb{Q}_5)$. But all the 2-torsion reduces to singular points, which is a contradiction. The other result follows because it has additive reduction at 5.

12. Consider the bijection
$$E_1(\mathbb{Q}_p)\longmapsto p\mathbb{Z}_p \text{ via } (x,y)\mapsto -\frac{x}{y}$$
and the inverse is given by $t\mapsto(x(t),y(t))$. The expression of $x(t)$ is
$$\frac{1}{t^2}-\frac{a_1}{t}-a_2-a_3t+\cdots=\frac{1}{t^2}(1-a_1t-a_2t^2+\cdots)=\frac{1}{t^2}f(t)$$

where $f(t) \equiv 1 \pmod{p}$. So it is a square mod $p$. Thus, it must be a square in $\mathbb{Z}_p$ by Hensel's Lemma. So

$$x = \left(\frac{1}{t}\sqrt{f(t)}\right)^2.$$

13. Consider the Kummer image $(x, x+3, x-6) = (a_1, a_2, a_3)$. Discriminant has prime factors $2, 3$ so $a_i \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. We have at least 5 points in the image. Over $\mathbb{R}$, the sign is $+, +, +$ or $-, +, -$.

    Over $\mathbb{Q}_3$, we know $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2 = \{1, 2, 3, 6\}$. Also, we know that $-1$ is the same as 2. The two torsions give $(1,1,1), (-2,3,6), (-3,3,1), (6,1,6)$. Then use $-1 \sim 2$ and the sign check, we have at most 8 points, which are

    $$(1,1,1), (-2,1,2), (-2,3,-6), (1,3,3), (-3,3,-1), (6,3,2), (6,1,6), (-3,1,-3).$$

    So there are 8 points and so the rank is 1.

14. Use the same argument as above, and consider $\mathbb{Q}_7^*/(\mathbb{Q}_7^*)^2$, with the sign check $(+,+,+)$ or $(-,-,+)$ we have 16 possibilities. Now consider the equations

    $$a_3 z_3^2 + 7 = a_1 z_1^2, a_1 z_3^2 - 7 = a_2 z_2^2.$$

    Let $(a_1, a_2, a_3) = (2, 2, 1)$. Clear $z_3$ and so we have

    $$21 = 4z_1^2 - z_2^2.$$

    Now reduce the equation modulo 8, we have $5 \equiv 4z_1^2 - z_2^2 \pmod{8}$, which is impossible. Therefore we have at most 15 points, and so in fact we have 8 points. So the rank is 1.

15. (i) Bad reduction occurs when the polynomial is not separable. So the primes when we have bad reduction are exactly those dividing the discriminant of the polynomial and in this case, we have $p = 2, 5$.

    (ii) Consider reduction at 3. $\bar{E}(\mathbb{F}_3) \cong C_2 \times C_2$ and we have good reduction at 3.

    (iii) The size of the group is 4 by Proposition 27.57. Now consider the 2-torsions. They clearly give all the representatives of $E/E_0$. Also, $E_0(\mathbb{Q}_5)/E_1(\mathbb{Q}_5) \cong C_5$. Recall from Proposition 27.57 that we have an exact sequence

    $$0 \to E_1(\mathbb{Q}_5) \to E(\mathbb{Q}_5) \to E(\mathbb{Q}_5)/E_1(\mathbb{Q}_5) \to 0$$

    and if we let $f, g, h$ denote the multiplication by 2 map on $E_1, E, E/E_1$ respectively, then

    $$\mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0$$

    is exact. But we know $\mathrm{coker} f = 0$. Thus, $E(\mathbb{Q}_5)/2E(\mathbb{Q}_5) \cong \mathrm{coker} h$. But $E/E_1$ is again abelian, since $E/E_0 \cong C_2 \times C_2$, $E_0/E_1 \cong C_5$ so

    $$E(\mathbb{Q}_5)/E_1(\mathbb{Q}_5) \cong C_2 \times C_2 \times C_5$$

    and so coker $h \cong C_2 \times C_2$.

16. (i) $p = 2, 3$ (For detail see previous question).

(ii) Same argument as question 11.

(iii) Use Lemma 27.41 and look back into the proof of Corollary 24.43, we conclude that $E_1(\mathbb{Q}_2)/2E_1(\mathbb{Q}_2) \cong C_2$. Now recall from Proposition 27.57, with the same notation, we have

$$0 \to \ker f \to C_2 \times C_2 \to \ker h \to C_2 \to \text{coker} g \to \text{coker} h \to 0.$$

It is clear that $E_0(\mathbb{Q}_2)/E_1(\mathbb{Q}_2) \cong C_2$ and observe that

$$E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2) = \langle (0,0), (6,0), (-3,9) \to \cong C_2 \times C_2 \times C_2$$

and so $\ker h = \text{coker } h \cong C_2 \times C_2 \times C_2$. Also, $C_2 \times C_2$ injects into $\ker h$ in the above sequence (because the 2-torsions injects into $\ker h$) and so in fact we can split the sequence so that

$$0 \to C_2 \times C_2 \to C_2 \times C_2 \times C_2 \to C_2 \to \text{coker} g \to C_2 \times C_2 \times C_2 \to 0.$$

Chasing the diagram we conclude that coker $g = C_2 \times C_2 \times C_2$.

(iv) Consider the curve over $\mathbb{Q}_2$. We have $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
Since $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ has size 8, so we have 8 points in the image over $\mathbb{Q}_2$. But among these, only 1 is a square and so we only have 8 points (unlike many other cases where we possibly have $-1$ a square etc.). Therefore, the rank is 1.

# 28 Introduction To Class Field Theory

Class field theory is probably one of the most important theories in algebraic number theory which classifies the abelian extensions of number fields. The theory takes its name from the fact that it provides a one-to-one correspondence between finite abelian extensions of a fixed global field and appropriate classes of ideals of the field or open subgroups of the idele class group of the field. One of the important examples is Hilbert class field, which is the maximal unramified abelian extension of the given field. The existence and finiteness of such extension is a result of class field theory. Another example is the extension of quadratic reciprocity in earlier chapter. For example, in one of our earlier problems (Problem 17 of Exercise 17) we assumed that for a prime $p \equiv 1 \pmod 3$,

$$x^3 \equiv 2 \pmod 2$$

is soluble if and only if $p$ can be written as $u^2 + 27v^2$. This is one of the important applications of Hilbert class field.

In this chapter, we are going to introduce the concept of global class field. Local class field theory will be given in the next Chapter. We will not go through the proof of the main theorem (Takagi-Artin).

## 28.1 Cyclotomic Extensions

An extension $F/K$ is abelian if it is Galois and the Galois group is abelian. Let $F/K$ be abelian and $\mathfrak{p}$ a prime of $K$ unramified in $F/K$. Write

$$\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{p}}(F/K) = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$$

for any $\mathfrak{q}$ above $\mathfrak{p}$. Note that this is well-defined because the Galois group is abelian.

**Remark 28.1.** *Note that $\mathfrak{p}$ splits completely if and only if $Frob_{\mathfrak{p}} = id$. Also if $F/L/K$ is a tower of number fields, then $Frob_{\mathfrak{p}}(L/K)$ is the image of $Frob_{\mathfrak{p}}(F/K)$ under the projection*

$$Gal(L/K) \longmapsto Gal(L/K).$$

*In particular, $\mathfrak{p}$ splits completely in $L$ if and only if $Frob_{\mathfrak{p}}(L/K) = id$, if and only if $Frob_{\mathfrak{p}} \in Gal(F/L)$.*

**Definition 28.2.** *$F/K$ is called a cyclotomic extension if $F \subset K(\mu_N)$ for some $N \geq 1$, where $\zeta_N$ is a primitive $N^{th}$ root of unity and $\mu_N = \langle \zeta_N \rangle$. Note that, the cyclotomic extensions are abelian, as the Galois group is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$.*

**Lemma 28.3.** *Let $F = K(\zeta_N)$ and $\mathfrak{p} \nmid N$ be a prime of $K$. Then $\mathfrak{p}$ is unramified in $F$ and $Frob_{\mathfrak{p}}$ is the unique element with $Frob_{\mathfrak{p}}(\zeta_N) = \zeta_N^{N(\mathfrak{p})}$.*

*Proof.* $X^N - 1$ has distinct root in characteristic $p \nmid N$. Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$ in $F$. Then $I_{\mathfrak{q}/\mathfrak{p}}$ fixes each $\zeta_N$ mod $\mathfrak{q}$ by definition and so can only contain the identity element because $I_{\mathfrak{q}/\mathfrak{p}}$ sends $\zeta_N$ mod $\mathfrak{q}$ to another root of unity mod $\mathfrak{q}$. But we know they are distinct modulo $\mathfrak{q}$ so it must be $\zeta_N$. This shows that $\mathfrak{p}$ is unramified.

$\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \equiv \zeta_N^{N(\mathfrak{p})} \bmod \mathfrak{q}$ by definition (recall that the Frobenius element of finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is given by $x \mapsto x^q$). But the roots are distinct modulo $\mathfrak{q}$ and so $\mathrm{Frob}_{\mathfrak{p}}(\zeta_N) = \zeta_N^{N(p)}$. This is unique because each element is determined by the image of $\zeta_N$. □

**Lemma 28.4.** *Let $F = \mathbb{Q}(\zeta_N)$. Then*

*(i) $p$ ramifies in $F/\mathbb{Q}$ if and only if $p \big| N$.*

*(ii)* *$p$ splits completely in $F/\mathbb{Q}$ if and only if $p \equiv 1$ (mod $N$).*

*(iii)* *$Frob_{p_1} = Frob_{p_2}$ if and only if $p_1 \equiv p_2$ mod $N$.*

*(iv)* *$\prod_i Frob_{p_i} = \prod_j Frob_{p'_j}$ if and only if $\prod_i p_i \equiv \prod_j p'_j$ mod $N$ (for $p_i, p'_j \nmid N$).*

*(v)* *The map*

$$\phi : \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, (a, N) = (b, N) = 1, a, b > 0 \right\} \longmapsto Gal(F/\mathbb{Q})$$

*via*

$$\phi\left(\frac{\prod_i p_i}{\prod_j p'_j}\right) \mapsto \prod_i Frob_{p_i} (\prod_j Frob_{p'_j})^{-1}$$

*is a surjective homomorphism with kernel $\left\{ \frac{a}{b} \in \mathbb{Q} : a \equiv b \text{ mod } N \right\}$.*

*Proof.* (i) If $p \nmid N$, then it is unramified by taking $K = \mathbb{Q}$ in the previous lemma. Conversely, we know that $\mathcal{O}_F = \mathbb{Z}[\zeta_N]$ and consider that if $p \big| N$, then $X^N - 1 \equiv (x-1)^N \bmod p$ and let $d$ be the degree of the minimal polynomial of $\zeta_N$. Then the minimal polynomial is congruent to $(x-1)^d \bmod p$ and use Kummer-Dedekind.

(ii) $p$ splits completely if and only if $p \nmid N$ with $\text{Frob}_p = id$. Then by previous lemma, this is equivalent of saying $p \nmid N$ and $\zeta_N^p = \zeta_N$, which is the same as $p \equiv 1 \bmod N$.

(iii) See (iv) with $i = j = 1$.

(iv) $(\prod_i \text{Frob}_{p_i})(\zeta_N) = \zeta^{\prod_i p_i}$. Thus,

$$\prod_i \text{Frob}_{p_i} = \prod_j \text{Frob}_{p'_j} \iff (\prod_i \text{Frob}_{p_i})(\zeta_N) = (\prod_j \text{Frob}_{p'_j})(\zeta_N) \iff \prod_i p_i \equiv \prod_j p'_j \bmod N.$$

(v) Write $a$ and $b$ into product of primes. Clearly it is a well-defined homomorphism. Consider $\text{Frob}_p(\zeta_N) = \zeta_N^p$. Given any $c \in (\mathbb{Z}/N\mathbb{Z})^*$, there exists prime $p$ such that $p \equiv c \bmod N$ by Dirichlet's theorem of primes in arithmetic progression. Therefore, given a map $\psi$ in the image, and suppose $\psi(\zeta_N) = \zeta_N^c$, then we can pick $p \equiv c \bmod N$ and so $\phi(p) = \psi$. So it is surjective.

For the kernel,

$$\phi\left(\frac{\prod_i p_i}{\prod_j p'_j}\right)(\zeta_N) = \zeta_N \iff \prod_i \text{Frob}_{p_i} = \prod_j \text{Frob}_{p'_j} \iff a \equiv b \bmod N$$

□

**Theorem 28.5.** *Let $F/\mathbb{Q}$ be cyclotomic.*

*(i)* *There exists $N \geq 1$ and $H \subset (\mathbb{Z}/N\mathbb{Z})^*$ such that*

*(a)* *$p$ splits completely in $F$ if and only if $p \bmod N \in H$ for $(p \nmid N)$.*

*(b)* *$\prod_i Frob_{p_i} = \prod_j Frob_{p'_j}$ if and only if $\frac{\prod_i p_i}{\prod_j p'_j} \in H (p_i, p'_j \nmid N)$.*

*(c) The map*

$$\phi : \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}_{>0},\ \textit{coprime to } N \right\} \longmapsto Gal(F/\mathbb{Q})$$

*via*

$$\phi\left(\frac{\prod_i p_i}{\prod_j p'_j}\right) = (\prod_i Frob_{p_i})(\prod_j Frob_{p'_j})$$

*is a surjective homomorphism with kernel* $\left\{\frac{a}{b} \bmod N \in H\right\}$.

*(ii) There exists a least $N$ such that the above works in the sense that any other $N'$ has $N \big| N'$. For this $N$, $p \big| N$ if and only if $p$ ramifies in $F/\mathbb{Q}$.*

*(iii) For every $N \geq 1$ and $H \subset (\mathbb{Z}/N\mathbb{Z})^*$ there is a unique cyclotomic field giving rise to $(N, H)$ as in (i).*

*Proof.* (i) We know $F \subset \mathbb{Q}(\zeta_N)$ for some $N$. Then $F = \mathbb{Q}(\zeta_N)^H$. Take such $N$ and $H$. Then:

(a) $F/\mathbb{Q}$ is an abelian extension, so it make sense to talk about $\mathrm{Frob}_p$. $p$ splits completely in $F$ if and only if $\mathrm{Frob}_p = id$. By Remark 28.1, $\mathrm{Frob}_p(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/F) = H$. So the map $\zeta_N \mapsto \zeta_N^p$ lies in $H$ if and only if $p \bmod N \in H$.

(b)

$$\prod_i \mathrm{Frob}_{p_i}(F/\mathbb{Q}) = \prod_j \mathrm{Frob}_{p'_j}(F/\mathbb{Q})$$

if and only if

$$\prod_i \mathrm{Frob}_{p_i}(\mathbb{Q}(\zeta_N)/\mathbb{Q})(\prod_j \mathrm{Frob}_{p'_j})(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{-1} \in H.$$

This is equivalent of saying $\frac{\prod_i p_i}{\prod_j p'_j} \in H$.

(c) Surjectivity follows from Dirichlet's theorem of primes in arithmetic progression. It has the correct kernel by (b).

(ii) Suppose $N_1, N_2$ both works, then take the corresponding $H_i$ and so we have $F = \mathbb{Q}(\zeta_{N_i})^{H_i}, i = 1, 2$. Let $N = (N_1, N_2)$.

We will firstly show that $\mathbb{Q}(\zeta_{N_1}) \cap \mathbb{Q}(\zeta_{N_2}) = \mathbb{Q}(\zeta_N)$. It is clear that

$$\mathbb{Q}(\zeta_{N_1})\mathbb{Q}(\zeta_{N_2}) = \mathbb{Q}(\zeta_L)$$

where $L$ is the least common multiple of $N_1$ and $N_2$. It is also clear that $\mathbb{Q}(\zeta_N) \subset \mathbb{Q}(\zeta_{N_1}) \cap \mathbb{Q}(\zeta_{N_2})$. Then

$$[\mathbb{Q}(\zeta_{N_1}) : \mathbb{Q}(\zeta_{N_1} \cap \mathbb{Q}(\zeta_{N_2}))] = [\mathbb{Q}(\zeta_L) : \mathbb{Q}(\zeta_{N_2})] = \frac{\phi(L)}{\phi(N_2)} = \frac{\phi(N_1)}{\phi(N)}.$$

by a calculation using Euler totient function. This shows that

$$[\mathbb{Q}(\zeta_{N_1}) \cap \mathbb{Q}(\zeta_{N_2}) : \mathbb{Q}] = \phi(N) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$$

and so they are the same. Then $N$ also works by the argument in (i) and hence the least such $N$ exists.

Now for this $N$ we know that we can set $F = \mathbb{Q}(\zeta_N)$ by (i) (or assuming (iii)) because we know for the least $N$ we have $F \subset \mathbb{Q}(\zeta_N)$ and so we can take such $N$ and $H$. One direction is clear, if $p \nmid |N$ then $p$ is unramified in $\mathbb{Q}(\zeta_N)$ (Kummer-Dedekind) and so $p$ must be unramified in $F$. Conversely, if $p \big| N$, then let $N = p^r m$ where $(m, p) = 1$. Suppose $p$ is unramified in $F$. Then

$$\{1\} = I_p(F/\mathbb{Q}) = \frac{I_p(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/F) \cap I_p(\mathbb{Q}(\zeta_{p^r} m)/\mathbb{Q})}$$

so we have that

$$I_p(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/F).$$

But $\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is unramified at $p$. So

$$I_p(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}) = I_p(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_m)).$$

Also, any prime above $p$ is totally ramified in $\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_m)$ by considering the ramification degrees. Therefore,

$$I_p(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_m)) = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_m))$$

Then combine the above observation, we conclude that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_m)) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/F)$$

and so $F \subset \mathbb{Q}(\zeta_m)$. Therefore, $m$ also works, which contradicts the minimality of $N$.

(iii) Take $F = \mathbb{Q}(\zeta_N)^H$. We need to check it is unique. Suppose $F_1 \neq F_2$, both work for $N, H$ and let $F_1, F_2 \subset \mathbb{Q}(\zeta_N)$. Let $F_i = \mathbb{Q}(\zeta_N)^{H_i}$ and so $(F_i, N, H_i)$ works in (i). Since $F_1 \neq F_2$, then they have different set of primes which split completely, (because $N_i, H_i$ are different) i.e. there exists $p$ splits completely in $F_1$, but not in $F_2$. Then by the conditions in (i), $p \bmod N \in H$ (for $F_1$) but $p \bmod N \notin H$ (for $F_2$) which is a contradiction.

□

**Example 28.6.** *(i) $F = \mathbb{Q}(\zeta_7), N = 7$ and $(\mathbb{Z}/N\mathbb{Z})^* \cong C_6$. Let $H = \{1\}$. Then $p$ splits completely in $F$ if and only if $p \equiv 1$ mod 7. The only prime which ramifies is 7. Also,*

$$Frob_2 = Frob_{23} = Frob_{37} = (Frob_3)^2.$$

*(ii) $F = \mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(\zeta_7)^H$ where $N = 7, H = \{1, 2, 4\} \cong C_2$. Then $p$ splits completely in $F$ if and only if $p$ mod $N$ is $1, 2$ or $4$ mod 7, which is the same as $\left(\frac{p}{7}\right) = 1$.*

*The only prime which ramifies is 7. We also have*

$$Frob_2 = Frob_{11} = Frob_{29} = Frob_3 Frob_5 = id, Frob_3 = Frob_5 = (Frob_3)^3 = \text{complex conjugation.}$$

**Proposition 28.7.** *Let $F = K(\mu_N)$.*

*(i) If $\mathfrak{p} = \langle \alpha \rangle$ is a prime of $K$ with $\alpha \equiv 1$ mod $N$, and $\sigma(\alpha) > 0$, for each embedding $\sigma : K \hookrightarrow \mathbb{R}$, then $p$ splits completely in $F/K$.*

*(ii) Define*

$$\psi : \oplus_{\mathfrak{p} \nmid N} \mathfrak{p}^{\mathbb{Z}} \longmapsto Gal(F/K) \text{ by } \psi(\mathfrak{p}) = Frob_{\mathfrak{p}}.$$

*This gives a homomorphism whose kernel contains*

$$P_N^1 = \text{principal fractional ideals generated by } \alpha \equiv 1 \text{ mod } N, \sigma(\alpha) > 0 \forall \sigma : K \hookrightarrow \mathbb{R}.$$

*In other words,*

$$P_N^1 = \left\{ \langle\alpha\rangle\langle\beta\rangle^{-1} : \alpha \equiv \beta \ mod\ N, \sigma\left(\frac{\alpha}{\beta}\right) > 0,\ \forall\sigma : K \hookrightarrow \mathbb{R} \right\}.$$

*Equivalently, if* $\langle\alpha\rangle\mathfrak{a} = \langle\beta\rangle\mathfrak{b}$ *with* $\alpha \equiv \beta \ mod\ N$ *and* $\sigma\left(\frac{\alpha}{\beta}\right) > 0$ *for all embeddings* $\sigma$ *then* $\psi(\mathfrak{a}) = \psi(\mathfrak{b})$.

*Proof.* If $\alpha = 1 + Nt$, $t \in \mathcal{O}_K$, i.e. $\alpha \equiv 1 \bmod N$, then

$$N(\alpha) = \prod_{\sigma:K\hookrightarrow\mathbb{C}} \sigma(\alpha) = \prod_{\sigma:K\hookrightarrow\mathbb{C}} (1 + N\sigma(t)) = 1 + N\lambda, \text{ where } \lambda \in \mathbb{Z}$$

because it is an algebraic integer, (as the sum or product of $\sigma(t)$ is) and it is also fixed by any embedding $\tau$ so it must be an integer. Also, $\sigma(\alpha) > 0$ for all real embedding, and $\sigma(\alpha)\overline{\sigma(\alpha)} > 0$ for each complex embedding, so $N(\alpha) > 0$. Thus

$$N(\langle\alpha\rangle) = |N(\alpha)| = N(\alpha) = 1 + N\lambda \equiv 1 \ (\text{mod } N).$$

(i) $\text{Frob}_{\mathfrak{p}}(\zeta_N) = \zeta_N^{N(\mathfrak{p})} = \zeta_N^{N(\langle\alpha\rangle)} = \zeta_N$. So $\text{Frob}_{\mathfrak{p}}$ has order 1 (it is unramified because $\mathfrak{p} \nmid N$ by Theorem 28.5) so $\mathfrak{p}$ splits completely.

(ii) Similarly, if $\alpha \equiv k \bmod N$, i.e. $\alpha = k + Nt$, $t \in \mathcal{O}_K$. Then $N(\alpha) = N(k) + N\lambda, \lambda \in \mathbb{Z}$. So

$$\alpha \equiv \beta \bmod N \Rightarrow N(\alpha) \equiv N(\beta) \bmod N.$$

Now $\mathfrak{p} \nmid N$, so $\mathfrak{p}$ is unramified in $F$. So $\psi(\mathfrak{p}) = id$ if and only if $\text{Frob}_{\mathfrak{p}}(\zeta_N) = \zeta_N$, if and only if $N(\mathfrak{p}) \equiv 1 \bmod N$.

Pick any element $\langle\alpha\rangle\langle\beta\rangle^{-1} \in P_N^1$, then $\alpha \equiv \beta \bmod N$ and so $N(\alpha) \equiv N(\beta) \bmod N$.

Also, if $\sigma\left(\frac{\alpha}{\beta}\right) > 0\ \forall\sigma : K \hookrightarrow \mathbb{R}$, then $N\left(\frac{\alpha}{\beta}\right) > 0$. Thus,

$$\zeta_N^{N(\langle\alpha\rangle)} = \zeta_N^{N(\langle\beta\rangle)}$$

i.e. $\zeta_N^{N(\langle\alpha\rangle\langle\beta\rangle^{-1})} = \zeta_N$. So $\langle\alpha\rangle\langle\beta\rangle^{-1} \in \ker\psi$.

□

**Example 28.8.** $K = \mathbb{Q}(i), F = K(\zeta_3)$. *If* $\mathfrak{a} = \langle\alpha\rangle$ *with* $a = 1 + 3t$, $t \in \mathbb{Z}[i]$. *Then*

$$N(\alpha) = 1 + 3(t + \bar{t}) + 9t\bar{t} = 1 + 3[t + \bar{t} + 3t\bar{t}] = 1 + 3\lambda, \lambda \in \mathbb{Z}.$$

*So* $N(\alpha) > 0$, *(check that* $1 + 3(t + \bar{t} + t\bar{t}) > 0$, *and so*

$$\zeta_3^{N(\langle\alpha\rangle)} = \zeta_3^{N(\alpha)} = \zeta_3.$$

*Generally,*

$$N(2 + 3t) \equiv 1 \ mod\ 3, N(i + 3t) \equiv 1 \ mod\ 3, N(2i + 3t) \equiv 1 \ mod\ 3.$$

*So if* $\mathfrak{p} = \langle\alpha\rangle$ *with* $\alpha \equiv \pm 1, \pm i \ mod\ 3$, *then* $Frob_{\mathfrak{p}} = id$.

*Also,*

$$N(1+i+3t) \equiv 2 \ mod\ 3, N(1+2i+3t) \equiv 2 \ mod\ 3, N(2+i+3t) \equiv 2 \ mod\ 3, N(2+2i+3t) \equiv 2 \ mod\ 3.$$

*So if* $\mathfrak{p} = \langle\alpha\rangle, \alpha \equiv 1 \pm i, 2 \pm i \ mod\ 3$ *then* $Frob_{\mathfrak{p}}$ *sends* $\zeta_3$ *to* $\zeta_3^{-1}$.

*If* $\mathfrak{a} = \prod_i \mathfrak{p}_i = \langle\alpha\rangle$ *with* $\alpha \equiv \pm 1, \pm i \ mod\ 3$, *then* $\prod_i Frob_{\mathfrak{p}_i} = id$. *If* $\alpha \equiv 1 \pm 1, 2 \pm i$ *then* $Frob_{\mathfrak{p}_i}$ *sends* $\zeta_3$ *to* $\zeta_3^{-1}$.

*Note that* $\langle\alpha\rangle = \langle-\alpha\rangle = \langle i\alpha\rangle = \langle -i\alpha\rangle$. *So* $\pm 1, \pm i$ *must give the same* $Frob_{\mathfrak{p}}$. *Similarly this is true for* $1 \pm i, 2 \pm i$.

**Example 28.9.** *$K = \mathbb{Q}(\sqrt{-5}), \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $F = K(\zeta_3)$. Residues mod 3 are $0, \pm\sqrt{-5}, 1, 1 \pm \sqrt{-5}, 2, 2 \pm \sqrt{-5}$. Among these, $1 \pm \sqrt{-5}$ and $2 \pm \sqrt{-5}$ are not prime to $\langle 3 \rangle$.*

*$N(\pm 1 + 3t) \equiv 1$ mod 3. $N(\pm\sqrt{-5} + 3t) \equiv (\sqrt{-5})(-\sqrt{-5}) \equiv 2$ mod 3. So if $\mathfrak{p} = \langle \alpha \rangle$ is a prime, and $\alpha \equiv \pm 1$ mod 3 then $Frob_\mathfrak{p}$ is identity. If $\alpha \equiv \pm\sqrt{-5}$ mod 3 then $Frob_\mathfrak{p} : \zeta_3 \mapsto \zeta_3^{-1}$.*

*What about non-principal ideals? Take $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-5} \rangle$, which is a prime above 2. The norm is 2 so it takes $\zeta_3$ to $\zeta_3^{-1}$.*

*If $\mathfrak{p}$ is non-principal, then $\mathfrak{p}\mathfrak{p}_2$ must be principal because the ideal class group is $C_2$. So let $\mathfrak{p}\mathfrak{p}_2 = \langle \alpha \rangle$. Then*

$$Frob_\mathfrak{p} = \begin{cases} id & \text{if } \alpha \equiv \pm\sqrt{-5} \text{ mod } 3, \\ \zeta_3 \mapsto \zeta_3^{-1} & \text{if } \alpha \equiv \pm 1 \text{ mod } 3. \end{cases}$$

*In other words, $Frob_\mathfrak{p}$ is determined by the image of $\mathfrak{p}$ in the ideals modulo prime ideals that are congruent to 1 modulo 3.*

## 28.2 Class Field

**Definition 28.10.** *A* **modulus** $\mathfrak{m}$ *is a formal product of an ideal of $\mathcal{O}_K$ and some real embeddings of $K$. In other words, it has the form*

$$\mathfrak{m} = \prod_i \mathfrak{p}_i^{n_i} \prod_j \sigma_j^{n_j} = \mathfrak{m}_0 \mathfrak{m}_\infty.$$

*Write $I_m = \oplus_{\mathfrak{p} \nmid m_0} \mathfrak{p}^\mathbb{Z}$, the group of fractional ideals coprime to $\mathfrak{m}$. Define $P_{\mathfrak{m}_0}$ to be the principal fractional ideals coprime to $\mathfrak{m}_0$, the subgroup generated by principal ideals in $I_m$. Let $P_\mathfrak{m}$ be the subgroup of $P_{\mathfrak{m}_0}$ with $\sigma\left(\frac{\alpha}{\beta}\right) > 0$ for all $\sigma \big| \mathfrak{m}_\infty$. Finally, define $P_\mathfrak{m}^1$ to be a subgroup of $P_\mathfrak{m}$ which contains ideals of the form*

$$\langle \alpha \rangle \langle \beta \rangle^{-1}, \alpha \equiv \beta \text{ mod } \mathfrak{m}_0 \text{ and } \sigma\left(\frac{\alpha}{\beta}\right) > 0 \ \forall \sigma \big| \mathfrak{m}_\infty.$$

**Remark 28.11.** *Write $P_1$ to be the group of principal (fractional) ideals and recall that $cl_K = \frac{I_K}{P_1}$. Then*

$$I_\mathfrak{m}/P_\mathfrak{m} = \frac{I_\mathfrak{m}}{P_1 \cap I_\mathfrak{m}} \cong \frac{I_\mathfrak{m} P_1}{P_1} \subset cl_K.$$

*So $|I_\mathfrak{m}/P_\mathfrak{m}|$ is finite.*

*Moreover, $P_{\mathfrak{m}_0}/P_\mathfrak{m}$ is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^T$ where $T$ is the size of $\{\sigma \text{ real embedding} : \sigma \big| \mathfrak{m}_\infty\}$.*

*Now we claim that*

$$P_\mathfrak{m}/P_\mathfrak{m}^1 \cong (\mathcal{O}_K/\mathfrak{m}_0)^*/\mathcal{O}_K^*$$

*via the map*

$$\phi : P_\mathfrak{m}/P_\mathfrak{m}^1 \longmapsto (\mathcal{O}_K^*/\mathfrak{m}_0)^*/\mathcal{O}_K^*$$

*defined by*

$$\phi(\langle \alpha \rangle) = \alpha \text{ mod } \mathfrak{m}_0.$$

*The map is well-defined, as if we have $\langle \alpha \rangle = \langle \beta \rangle$ in $P_\mathfrak{m}/P_\mathfrak{m}^1$, then this means that*

$$\langle \alpha \rangle \langle \beta^{-1} \rangle \in P_\mathfrak{m}^1 \Rightarrow \alpha \equiv \beta \text{ mod } \mathfrak{m}_0.$$

*Also, $\langle \alpha \rangle$ is identified with $\alpha$ modulo a unit*

*It is injective because if $\alpha \equiv 1$ mod $\mathfrak{m}_0$, then $\langle \alpha \rangle \in P_\mathfrak{m}^1$ by definition. Surjectivity is clear. Therefore, we have proved the claim. This shows that $I_\mathfrak{m}/P_\mathfrak{m}^1$ is finite.*

**Definition 28.12.** *A* **congruence subgroup** *$H$ for $\mathfrak{m}$ is a subgroup of $I_\mathfrak{m}$ containing $P_\mathfrak{m}^1$. An extension $F/K$ is a* **class field** *of $(\mathfrak{m}, H)$ if a prime $\mathfrak{p} \nmid \mathfrak{m}$ of $K$ that splits completely in $F$ are exactly those lie in $H$.*

**Example 28.13.** *$K = \mathbb{Q}$. So $\mathcal{O}_K$ is a principal ideal domain.*

*(i)* $\mathfrak{m} = N \cdot \infty$, *where $\infty$ is the real embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. So*

$$\begin{aligned} I_{\mathfrak{m}} &\cong \left\{ \frac{\prod_i p_i}{\prod_j p'_j} : p_i, p'_j < 0, \text{ prime to } N \right\} \\ &= \left\{ \frac{a}{b} : a, b \in \mathbb{N} \text{ prime to } N \right\}. \end{aligned}$$

$$P^1_{\mathfrak{m}} \text{ is the subgroup generated by } \frac{\langle a \rangle}{\langle b \rangle} \text{ with } a \equiv b \bmod N, \frac{a}{b} > 0.$$

*So $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}/N\mathbb{Z})^*$.*

*(ii)* $\mathfrak{m} = N$. *Then $I_{\mathfrak{m}}$ will be the same but*

$$P^1_{\mathfrak{m}} \text{ is the subgroup generated by } \frac{\langle a \rangle}{\langle b \rangle} \text{ with } a \equiv b \bmod N.$$

*So $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$.*

*(iii)* $\mathfrak{m} = 5 \cdot \infty$. *Let $H = P^1_{\mathfrak{m}}$. We can check that $\mathbb{Q}(\zeta_5)$ is a class field of $\mathbb{Q}$ for $(\mathfrak{m}, H)$. Let $p \nmid 5$ and $p$ splits completely in $\mathbb{Q}(\zeta_5)$. Then by Lemma 28.4, $\mathfrak{p} \equiv 1 \bmod 5$.*

*Now let $H \subset I_{\mathfrak{m}}$ of index 2, we have $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}/5\mathbb{Z})^* = C_4$. So $H/P^1_{\mathfrak{m}} = \{1, 4\}$, so $H$ is generated by those congruent to 1 or 4 mod 5.*

*Consider $F = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5)^{H'}$, where $H' = \{1, 4\}$. Then by Theorem 28.5(i), $p$ splits completely in $F$ if and only if $p$ mod 5 in $H'$ and this is saying $p \in H$. So it is a class field.*

**Example 28.14.** *(i) $K = \mathbb{Q}, \mathfrak{m} = 3$. Then $I_{\mathfrak{m}}$ is the group of ideals which are prime to 3. $P^1_{\mathfrak{m}}$ are those generated by 1 mod 3. So*

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}[i]/\langle 3 \rangle)^*/\{\pm 1, \pm i\} \cong C_2.$$

*(Remember that we need to quotient out the units in the ring of integers.)*

*(ii) $K = \mathbb{Q}(\sqrt{-5}), \mathfrak{m} = \langle 3 \rangle = \mathfrak{p}_3\mathfrak{p}'_3$. Then*

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong C_2 \times C_2 = \langle [\mathfrak{p}_2], [\sqrt{-5}] \rangle$$

*where $\mathfrak{p}_2$ is a prime above 2 becasue*

$$(\mathbb{Z}[\sqrt{-5}]/\langle 3 \rangle)^* \cong \{\pm\sqrt{-5}, \pm 1 \bmod 3\}.$$

*This shows that*

$$P_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathcal{O}^*_K/\mathfrak{m}_0)^*/\mathcal{O}^*_K \cong C_2 = \{\pm\sqrt{-5}\}.$$

*Then by previous argument,*

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong cl_K \times P_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong C_2 \times C_2 = \langle [\mathfrak{p}], [\sqrt{-5}] \rangle.$$

*Let $H/P^1_{\mathfrak{m}} = \{id, [\mathfrak{p}_2\langle\sqrt{-5}\rangle]\}$ and let $F = K(\zeta_3)$. The primes which split completely in $F$ are (by Example 28.9):*

$$\begin{aligned} &\mathfrak{p} = \langle \alpha \rangle \quad \text{if } \mathfrak{p} \text{ is principal}, \alpha \equiv \pm 1 \bmod 3, \\ &\mathfrak{p}\mathfrak{p}_2 = \langle \alpha \rangle \quad \text{if } \alpha \equiv \pm\sqrt{-5} \bmod 3. \end{aligned}$$

*But in the quotient, say $\alpha \equiv -1 \bmod 3$, we will have $\langle -\alpha \rangle \in P^1_{\mathfrak{m}}$ and so is $\langle \alpha \rangle$. This shows that $\{\mathfrak{p} = \langle \alpha \rangle, \alpha \equiv \pm 1\} \subset H$. Similarly, we can show that the other set is also in $H$. Therefore, $F = K(\zeta_3)$ is a class field.*

## 28.3 Main Theorem of Class Field Theory

Now we state the main theorem of class field theory:

**Theorem 28.15.** [**Takagi-Artin**] *Let $K$ be a number field.*

*(i) Every abaelian extension $F/K$ is a class field for some $(\mathfrak{m}, H)$.*

*(ii) Every $(\mathfrak{m}, H)$ has a unique class field $F$. Moreover, $F$ is abelian over $K$.*

*(iii) Among $(\mathfrak{m}, H)$ in (i), there is a minimal one in the sense that other $(\mathfrak{m}', H')$ have $\mathfrak{m}\big|\mathfrak{m}'$. The minimal modulus is called the* **conductor** *of $F/K$. The primes that ramify in $F/K$ are precisely those dividing the conductor. Moreover, the real embeddings in the conductors are precisely those that extend to complex embeddings of $F$.*

*(iv)* [**Artin Reciprocity Law**] *If $F/K$ is a class field for $(\mathfrak{m}, H)$ then the Artin map*

$$\phi : (I_{\mathfrak{m}}/P^1_{\mathfrak{m}}) \longmapsto Gal(F/K)$$

*determined by $\phi(\mathfrak{p}) = Frob_{\mathfrak{p}}$ is a surjective homomorphism with kernel $H$.*

**Corollary 28.16.** [**Kronecker Weber Theorem**] *Every abelian extension of $\mathbb{Q}$ is cyclotomic.*

*Proof.* Let $F/\mathbb{Q}$ be an abelian extension. By Theorem 28.5, cyclotomic fields are class fields for all possible moduli $m = N \cdot \infty$ and congruence subgroups $H$. Now over $\mathbb{Q}$, $\mathfrak{m}$ is either $N$ or $N \cdot \infty$ for some $N$. We know $F/\mathbb{Q}$ is a class field for some $(\mathfrak{m}, H)$. If $\mathfrak{m} = N \cdot \infty$, then by uniqueness (Theorem 28.15(ii)) we must have $F$ cyclotomic. Also, by (iii), $F$ cannot be real because the real embedding extends to complex embedding. This shows that every non-real abelian extension is cyclotomic.

If $F$ is real, then let $F' = F(i)$ and so $F'$ is non-real, and $F'/\mathbb{Q}$ is also abelian (easy to check that the Galois actions commute). Then $F'$ is cyclotomic and so $F$ is cyclotomic. □

**Lemma 28.17.** *Let $\mathfrak{m} = \mathfrak{m}_0 = \prod_i \mathfrak{p}_i^{n_i}$ be an ideal of $\mathcal{O}_K$ with $\mathfrak{p}_i$ distinct primes.*

*(i) We have an isomorphism*

$$(\mathcal{O}_K/\mathfrak{m})^*/\mathcal{O}_K^* \cong P_{\mathfrak{m}}/P^1_{\mathfrak{m}}, \alpha \mapsto \langle\alpha\rangle,$$

*where $P_{\mathfrak{m}}$ is the subgroup of $I_{\mathfrak{m}}$ generated by principal ideals.*

*(ii) We have an isomorphism*

$$(\mathcal{O}_K/\mathfrak{m})^* \cong \prod_i (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^*, x \mapsto (x \ mod\ \mathfrak{p}_1^{n_1}, \ldots, x \ mod\ \mathfrak{p}_r^{n_r}).$$

*(iii) If $\mathfrak{p}$ is a prime then $(\mathcal{O}_K/\mathfrak{p}^n) \cong C_{p^k-1} \times A$, where $p^k = N(\mathfrak{p})$ and $A$ is an abelian group of order $p^{k(n-1)}$.*

*Proof.* (i) See Remark 28.11.

(ii) Use Chinese Remainder Theorem.

(iii) By unique factorisation the only ideals containing $\mathfrak{p}^n$ are $\mathfrak{p}^l, l \leq n$ and so the maximal ideal among those is $\mathfrak{p}$. Thus $\mathfrak{p}/\mathfrak{p}^n$ is the unique maximal ideal of $\mathcal{O}_K/\mathfrak{p}^n$. So each $x \in \mathfrak{p}\backslash\mathfrak{p}^n$ is invertible (it is a local ring and so every element not in the maximal ideal is invertible). Thus,

$$|(\mathcal{O}_K/\mathfrak{p}^n)^*| = (p^k - 1)p^{k(n-1)}.$$

Now $(\mathcal{O}_K/\mathfrak{p}^n)^*$ projects onto $(\mathcal{O}_K/\mathfrak{p})^* \cong C_{p^k-1}$, and so $(\mathcal{O}_K/\mathfrak{p}^n)^* \cong C_{p^k-1} \times A$.

□

**Example 28.18.** *Let $K = Q(i)$. If $\mathfrak{m} = \langle 1\rangle$ then $I_\mathfrak{m}/P^1_\mathfrak{m} = 1$ as $|cl_K| = 1$. The class field of $(m, P^1_\mathfrak{m})$ is $K$ itself (as we need every ideal splits completely). If $F/K$ is an abelian extension unramified at all primes, it is a class field of $(\langle 1\rangle, H)$ (Theorem 28.15(iii). Hence there are no such extensions of $\mathbb{Q}(i)$ (except for $\mathbb{Q}(i)$ itself).*

**Example 28.19.** *Let $K = \mathbb{Q}(i)$ so $I_\mathfrak{m} = P_\mathfrak{m}$. If $\mathfrak{m} = \langle 7\rangle$ then by previous lemma we have*

$$I_\mathfrak{m}/P^1_\mathfrak{m} \cong (\mathbb{Z}[i]/\langle 7\rangle)^*/\{\pm 1, \pm i\} \cong C_{12}.$$

*Take a subgroup $H$ such that $I_\mathfrak{m}/H \cong C_4$. Explicitly it is given by the classes of $1, \ldots, 6, i, \ldots, 6i \in (\mathbb{Z}[i]/\langle 7\rangle)^*$. Then by Theorem 28.15(iv), the class field of $(\mathfrak{m}, H)$ has Galois group $C_4$ and is ramified at 7 only (note that 7 is prime in $K$).*

*Let it be $F$ and by Kummer Theory we have $F = K(\sqrt[4]{\alpha})$ for some $\alpha \in K$. By scaling and absorbing powers we may assume that $\alpha \in \mathcal{O}_K$ and $\alpha = i^a 7^b$ because it only ramifies at 7 and $0 \leq a, b \leq 3$. If $b = 0$ or 2 then $K(\sqrt{\alpha})/K$ is unramified at 7 and thus unramified everywhere. But this is impossible by the previous example. Therefore, we may assume that $b = 1$ (when $b = 3$, we take $7^b \frac{1}{\alpha}$. Now we can either work out the ramification to find that $F = K(\sqrt[4]{-7})$ (the others ramify at $\langle 1 + i\rangle$). Alternatively, we can compute $Frob_\mathfrak{p}$. For example, if $\mathfrak{p} = \langle x\rangle$ with $x \in H$ then by definition of class field $Frob_\mathfrak{p} = id$. Take $x = 7 + 2i$. This is a prime above 53. If $\mathfrak{p} = \langle x\rangle$ then $Frob_\mathfrak{p} = id$. Then we have*

$$\begin{aligned} \sqrt[4]{\alpha} &\equiv Frob_\mathfrak{p}(\sqrt[4]{\alpha}) \equiv (\sqrt[4]{\alpha})^{53} \equiv (i^a 7)^{13} \sqrt[4]{\alpha} \ mod\ \mathfrak{p} \\ &\equiv i^a(-2i)^{13}\sqrt[4]{\alpha} \equiv i^{a-1}30\sqrt[4]{\alpha} \equiv -i^a\sqrt[4]{\alpha} \ mod\ \mathfrak{p}. \end{aligned}$$

*Note that $2^{13} \equiv 30$ mod 53 and $30 - i = (7 + 2i)(4 - i)$. Hence $a = 2$.*

## 28.4 Ray Class Field

**Note the abuse of notation $H$ for $H/P^1_\mathfrak{m}$ in many cases.**

**Definition 28.20.** *Let $\mathfrak{m}$ be a modulus of $K$. Its* **ray class group** *is $I_\mathfrak{m}/P^1_\mathfrak{m}$. Its* **ray class field** *$K_\mathfrak{m}$ is the class field of $(\mathfrak{m}, P^1_\mathfrak{m})$.*

**Remark 28.21.** *When $\mathfrak{m} = \langle 1\rangle$ the ray class group is $cl_K$. The corresponding field $K_{\langle 1\rangle}$ is called the* **Hilbert class field**.

**Example 28.22.** *Let $K = \mathbb{Q}$ and $\mathfrak{m} = N \cdot \infty$. Then $K_\mathfrak{m} = \mathbb{Q}(\zeta_N)$.*

**Lemma 28.23.** *Let $K$ be a number field and $\mathfrak{m}$ a modulus*

*(i) $Gal(K_\mathfrak{m}/K) \cong I_\mathfrak{m}/P^1_\mathfrak{m}$.*

*(ii) The class field $F$ of $(\mathfrak{m}, H)$ lies inside $K_\mathfrak{m}$ and $Gal(F/K) \cong I_\mathfrak{m}/H$, i.e. $F = K^H_\mathfrak{m}$.*

*(iii) If $\mathfrak{m}\big|\mathfrak{m}'$ then $K_\mathfrak{m} \subset K_{\mathfrak{m}'}$.*

*Proof.* (i) Theorem 28.15(iv).

(ii) By Remark 28.1, $\text{Frob}_{\mathfrak{p}}(K_{\mathfrak{m}}^H/K) = id$ if and only if $\mathfrak{p} \in H$. Therefore, $K_{\mathfrak{m}}^H$ is a class field of $(\mathfrak{m}, H)$. Then by uniqueness, it is the class field for $(\mathfrak{m}, H)$.

(iii) $K_{\mathfrak{m}}$ is also a class field for $(\mathfrak{m}', H')$ for some $H'$ because $\mathfrak{m} \big| \mathfrak{m}'$ (Theorem 28.15(iii)). Now by (ii), $K_{\mathfrak{m}} \subset K_{\mathfrak{m}'}$.

□

**Lemma 28.24.** *Let $K$ be a number field and $F = K_{\langle 1 \rangle}$ be its Hilbert class field.*

*(i) $cl_K \cong Gal(F/K)$ (via the Artin map $\prod \mathfrak{p} \mapsto \prod Frob_{\mathfrak{p}}$).*

*(ii) A prime $\mathfrak{p}$ of $K$ is principal if and only if $p$ splits completely in $F/K$.*

*(iii) The order of $\mathfrak{p}$ in $cl_K$ is equal to the order of $Frob_{\mathfrak{p}}$ in $Gal(F/K)$ and $f_{\mathfrak{p}}$, the residue degree of $\mathfrak{p}$ in $F/K$.*

*(iv) $F/K$ is unramified at all primes and all embeddings $K \hookrightarrow \mathbb{R}$ extend to $F \hookrightarrow \mathbb{R}$. If $L/K$ is another abelian extension with this property, then $L \subset F$.*

*Proof.* (i) When $\mathfrak{m} = \langle 1 \rangle$, we have $P_{\mathfrak{m}} = P_{\mathfrak{m}}^1$ and we know that $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ is isomorphic to the class group.

(ii) A prime $\mathfrak{p}$ is principal if and only if $\mathfrak{p} \in P_{\mathfrak{m}}^1$ with $\mathfrak{m} = \langle 1 \rangle$ if and only if $\text{Frob}_{\mathfrak{p}} = id$.

(iii) This follows from (i) and the definition of the Artin map.

(iv) Clearly $F/K$ is unramified because the conductor is $\langle 1 \rangle$ and so all real embeddings from of $K$ must extend to real embeddings of $F$. If $L$ is another such extension, then $L$ must have conductor $\langle 1 \rangle$ and $L/K$ is abelian, so $L$ is a class field of $(\langle 1 \rangle, H)$ for some $H$. Then $L \subset F$ by previous Lemma 28.23(ii).

□

**Example 28.25.** *Let $K = \mathbb{Q}(\sqrt{-5})$ so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the class group is $C_2$. We claim that the Hilbert class field is $F = K(i)$. Firstly, only 2 and 5 ramifies in $F/\mathbb{Q}$. They also ramify in $K$. But it is easy to see that they are not totally ramified and so $F/K$ is unramified everywhere. Further $K$ has no real embeddings. Then by Lemma 28.24(iv), $F$ lies in the Hilbert class field $L$. But the class group has order 2 so the degree of $L/K$ is 2 and so $F = L$.*

**Proposition 28.26.** *Let $K/k$ be a Galois extension of number fields and $\mathfrak{m}$ a modulus of $K$ with $\mathfrak{m} = g\mathfrak{m}$ for all $g \in Gal(K/k)$. Then:*

*(i) $K_{\mathfrak{m}}$ is Galois over $k$.*

*(ii) If $\mathfrak{n} \big| \mathfrak{m}$ then $K_{g\mathfrak{n}} = \bar{g}K_{\mathfrak{n}}$ for any $\bar{g} \in Gal(K_{\mathfrak{m}}/k)$ that projects to $g \in Gal(K/k)$.*

*(iii)* $\psi(g\mathfrak{a}) = \bar{g}\psi(\mathfrak{a})\bar{g}^{-1}$, *where* $\psi : I_\mathfrak{m} \longmapsto Gal(K_\mathfrak{m}/K)$ *is the Artin map and* $g, \bar{g}$ *as in (ii).*

*Proof.* Let $F/k$ be the Galois closure of $K_\mathfrak{m} = k$, and $\mathfrak{q}$ a prime of $F$ above $\mathfrak{p}$, where $\mathfrak{p}$ is a prime of $K$. Observe that

$$\sigma \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\sigma^{-1} = \mathrm{Frob}_{\sigma(\mathfrak{q})/\sigma(\mathfrak{p})}$$

(i) $\mathfrak{p}$ splits completely in $\sigma K_\mathfrak{m}$ if and only if $\sigma^{-1}\mathfrak{p}$ splits completely in $K_\mathfrak{m}$ if and only if $\mathfrak{p}$ splits completely in $K_\mathfrak{m}$ as the definition of $K_\mathfrak{m}$ is $\mathrm{Gal}(F/k)$-invariant. (consider $\mathfrak{p}$ splits completely if and only if $\mathfrak{p} \in P^1_\mathfrak{m}$).

Thus $\sigma K_\mathfrak{m}$ is also a class field for $\mathfrak{m}$ and so $\sigma K_\mathfrak{m} = K_\mathfrak{m}$ by uniqueness. Hence $K_\mathfrak{m}/k$ is Galois.

(ii) $\mathfrak{n}$ is invariant as $\mathfrak{n}\big|\mathfrak{m}$. $\mathfrak{p}$ splits completely in $\sigma K_\mathfrak{n}$ if and only if $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathrm{Gal}(F/K_\mathfrak{n})$ if and only if $\sigma\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\sigma^{-1} \in \mathrm{Gal}(F/\sigma K_\mathfrak{n})$ if and only if $\mathrm{Frob}_{\sigma(\mathfrak{q})/\sigma(\mathfrak{p})} \in \mathrm{Gal}(F/\sigma K_\mathfrak{n})$ if and only if $\sigma(\mathfrak{p})$ splits completely in $\sigma K_\mathfrak{n}$ if and only if $\mathfrak{p}$ splits completely in $K_\mathfrak{n}$.

The last one is the same as $\mathfrak{p} \equiv 1 \bmod \mathfrak{n}$ and hence mod $\sigma\mathfrak{n}$ because $\sigma\mathfrak{n} = \mathfrak{n}$. This is equivalent to $\mathfrak{p} \in P^1_{\sigma\mathfrak{n}}$. Hence $K_\mathfrak{n}$ is a ray class field for $\sigma\mathfrak{n}$ and so $\sigma K_\mathfrak{n} = K_{\sigma\mathfrak{n}}$ by uniqueness.

(iii) The result follows from the observation at the beginning.

□

**Remark 28.27.** *For the Hilbert class field we have:* $\mathfrak{p}$ *is principal if and only if* $\mathfrak{p}$ *splits completely. For* $\mathfrak{p}$ *non-principal Hilbert conjectured that* $\mathfrak{p}\mathcal{O}_F$ *is principal, which turned out to be true.*

## 28.5 Principal Ideal Theorem

**Definition 28.28.** *Let* $F/K$ *be a Galois extension and* $K^{ab}$ *the maximal abelian extension of* $K$ *in* $F$*, so if* $Gal(F/K) = G$ *then* $Gal(F/K^{ab}) = G'$ *and* $Gal(K^{ab}/K) = G/G'$*, where*

$$G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$$

*is the commutator subgroup. The Artin map is defined by*

$$\psi_{F/K} : I_\mathfrak{m} \longmapsto Gal(K^{ab}/K) = G/G', \mathfrak{p} \mapsto Frob_\mathfrak{p} G'.$$

**Definition 28.29.** *Let* $F/K$ *be a Galois extension of number fields and* $G = Gal(F/K)$*. The* **relative norm** *of an ideal* $\mathfrak{a} \subset \mathcal{O}_F$ *is an ideal* $N_{F/K}(\mathfrak{a}) \subset \mathcal{O}_K$ *with*

$$N_{F/K}(\mathfrak{a})\mathcal{O}_F = \prod_{g \in G} g(\mathfrak{a}).$$

**Remark 28.30.** *(i)* $N_{F/K}(\langle\alpha\rangle) = \langle N_{F/K}(\alpha)\rangle$ *straight from the definition.*

*(ii) If* $\mathfrak{q}$ *is a prime above* $\mathfrak{p}$*, and* $\mathfrak{q}_i$ *are the primes above* $\mathfrak{p}$*, then*

$$\prod_{g \in G} g(\mathfrak{q}) = (\mathfrak{q}_1 \cdots \mathfrak{q}_k)^{ef} = \mathfrak{p}^f.$$

**Lemma 28.31.** *Let* $F$ *and* $L$ *be Galois extensions of* $K$ *with* $FL/L$ *abelian,* $\mathfrak{a}$ *an ideal of* $\mathcal{O}_L$*, and* $\mathfrak{m}$ *a suitable modulus (i.e. the conorm of the conductor of* $K^{ab} = K$*). Then*

$$\psi_{F/K}(N_{L/K}(\mathfrak{a}) = \psi_{FL/L}(\mathfrak{a})G'$$

*for* $(\mathfrak{a}, \mathfrak{m}) = 1$*, where* $G'$ *is the commutator of* $G$

*Proof.* Clearly the relative norm is multiplicative so it suffices to check this holds for primes. Let $\mathfrak{q}$ be a prime of $L$ above $\mathfrak{p}$ (where $\mathfrak{p}$ is unramified in $F/K$). Then by previous remark, we have

$$\psi_{F/K}(N_{L/K}(\mathfrak{q})) = \psi_{F/K}(\mathfrak{p}^{f_\mathfrak{p}}) = \mathrm{Frob}_\mathfrak{p}^{f_\mathfrak{p}}(F/K)G'.$$

Recall that if $L/K$ is finite, then $\mathrm{Gal}(FL/L)$ is isomorphic to a subgroup of $\mathrm{Gal}(F/K)$ via the restriction map. Then $\mathrm{Frob}_\mathfrak{q}(FL/L)$ sends to $\mathrm{Frob}_\mathfrak{p}(F/K)$ because $N(\mathfrak{q}) = N(\mathfrak{p})^{f_\mathfrak{p}}$. This completes the proof as $\psi_{FL/L}(\mathfrak{q}) = \mathrm{Frob}_\mathfrak{q}$. □

**Corollary 28.32.** *Suppose $F/K$ is abelian. If $\mathfrak{p} = N_{F/K}(\mathfrak{q})$, then $Frob_\mathfrak{p} = id$, for $\mathfrak{p}$ unramified in $F/K$.*

*Proof.* Take $L = F$ in the previous lemma and so

$$\mathrm{Frob}_\mathfrak{p} = \psi_{F/K}(\mathfrak{p}) = \psi_{F/F}(\mathfrak{q}) = id.$$

□

**Definition 28.33.** *Let $H \subset G$ be finite groups. The transfer map (or Verlagerung) $Ver : G/G' \mapsto H/H'$ is defined as follows: Let $Hr_1, \ldots, Hr_k$ be the right cosets of $H$ in $G$. If $g \in G$, let $Hr_i g = Hr_\sigma(i)$ (so $\sigma$ is a fixed permutation for $g$). Then*

$$Ver(g) = \prod_i r_i g r_{\sigma(i)}^{-1} \cdot H'.$$

*It is a fact that Ver is a well-defined homomorphism.*

**Remark 28.34.** *Rearrange the product, we have*

$$Ver(g) = r_1 g r_{\sigma(1)}^{-1} \left(r_{\sigma(1)} g r_{\sigma^2(1)}^{-1}\right) \left(r_{\sigma^2(1)} g r_{\sigma^3(1)}^{-1}\right) = \prod_{s \in \Sigma} s g^{f(s)} s^{-1},$$

*where $H_s\langle g\rangle$ are the $H\backslash G/\langle g\rangle$ double cosets, equivalently the $\langle g\rangle$-orbits on the $Hr_i$, and $f(s) = |H_s\langle g\rangle|/|H|$ is the length of the orbit of $Hs$ (think of the definition of $\sigma$).*

**Lemma 28.35.** *Let $F/K$ be a Galois extension of number fields, $L/K$ finite and $\mathfrak{m}$ the conductor of the maximal abelian extension of $K$ in $F$. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_F$. Then for $H = Gal(FL/L)$,*

$$\psi_{FL/L}(\mathfrak{a}\mathcal{O}_L) = Ver\psi_{F/K}(\mathfrak{a})$$

*for $(\mathfrak{a}, \mathfrak{m}) = 1$.*

*Proof.* Again we only need to check this holds for prime. With the same notation as in the remark above, and $g = \mathrm{Frob}_\mathfrak{p}$, we have

$$\begin{aligned} \mathrm{Ver}\psi_{F/K}(\mathfrak{a}) &= \mathrm{VerFrob}_\mathfrak{p} = \prod_{s\in\Sigma} s\mathrm{Frob}_\mathfrak{p}^{f(s)}s^{-1} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{Frob}_\mathfrak{q} \\ &= \prod_{\mathfrak{q}\mid\mathfrak{p}} \psi_{FL/L}(\mathfrak{q}) = \psi_{FL/L}(\mathfrak{p}\mathcal{O}_L), \end{aligned}$$

where the last equality in the first line comes from Corollary 19.30 and Proposition 19.31, because $\mathfrak{p}$ prime to the conductor means $\mathfrak{p}$ is unramified and so $\langle \mathrm{Frob}_\mathfrak{p}\rangle$ gives the decomposition group. □

**Theorem 28.36.** **[Furtwangler]** *Let $G$ be a finite group and $H = G'$. The transfer map Ver from $G$ to $H$ is trivial, i.e. $Ver(\mathfrak{q}) = id$.*

The proof is hard but we will use this to deduce the main theorem of this section.

**Corollary 28.37.** [**Principal Ideal Theorem**] *All ideals in a number field $K$ become principal in its Hilbert class field, i.e. $\mathfrak{a}\mathcal{O}_{K_{\langle 1\rangle}} = \langle\alpha\rangle$ for some $\alpha \in \mathcal{O}_{K_{\langle 1\rangle}}$.*

*Proof.* Let $F$ be the Hilbert class field of $K$ and we know by Proposition 28.26 that $F_{\langle 1\rangle}/K$ is Galois. Let $G = \mathrm{Gal}(F_{\langle 1\rangle}/K)$ and $H = \mathrm{Gal}(F_{\langle 1\rangle}/F)$. Note that all subfields $L$ of $F_{\langle 1\rangle}$ are unramified at all primes of $K$, and all $K \hookrightarrow \mathbb{R}$ extends to $L \hookrightarrow \mathbb{R}$. As $F$ is the maximal abelian such field we have $H = G'$. If $\mathfrak{p}$ is a prime of $K$, we have by previous theorem and lemma,

$$\psi_{F_{\langle 1\rangle}/F}(\mathfrak{p}\mathcal{O}_F) = \mathrm{Ver}_{G\mapsto H}(\mathrm{Frob}_{\mathfrak{p}}) = id.$$

Hence $\mathrm{Frob}_{\mathfrak{p}}(F/K)$ is also trivial. Then by Lemma 28.24(ii), we conclude that $\mathfrak{p}\mathcal{O}_F$ is principal. Therefore every ideal is principal. □

## 28.6 Exercises

1. Let $p$ be an odd prime number, $K$ be a number filed, and $\mathfrak{q}\big|p$ a prime of $K$. Prove that if the class number of $K$ is prime to $p$ then $K$ has at most one cyclic extension of degree $p$ which is unramified at all primes other than $\mathfrak{q}$.

2. Prove that $\mathbb{Q}(i)$ has only one quadratic extension and no $C_4$-extension, that is unramified outside 11. Find the quadratic one.

3. Let $K = \mathbb{Q}(i)$ and $\mathfrak{m} = \langle 4 + i\rangle$. Show that $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong C_4$ and find the ray class field of $\mathfrak{m}$.

4. Let $K = \mathbb{Q}(\zeta_3)$ and $\mathfrak{m} = \langle 7\rangle = (3 + 2\zeta_3)(1 - 2\zeta_3)$. Show that there is a unique congruence subgroup $H$ for $\mathfrak{m}$ with $I_{\mathfrak{m}}/H \cong C_3$ and hence describe this subgroup in terms of congruence classes of $\mathbb{Z}[\zeta_3]$ modulo $\langle 7\rangle$. Find the class field of $(\mathfrak{m}, H)$.

5. Let $K = \mathbb{Q}(\sqrt{2})$ and let $\sigma_1, \sigma_2$ denote its two real embeddings. Compute $I_{\mathfrak{m}}/P^1_{\mathfrak{m}}$ for $\mathfrak{m} = \langle 3\rangle, \langle 3\rangle\sigma_1, \langle 3\rangle\sigma_1\sigma_2$, and determine the corresponding ray class fields. (Note that $K$ has trivial class group).

6. Prove that for odd prime $p$, the quadratic subfield $\mathbb{Q}(\sqrt{\pm p})$ of $\mathbb{Q}(\zeta_p)$ (so that $\pm p \equiv 1 \bmod 4$) has odd class number.

7. Show that if $\mathbb{Q}(\sqrt{d})$ has ideal class group $C_4$, then its Hilbert class field has Galois group $D_8$ over $\mathbb{Q}$.

8. Find a number field whose class number is divisible by 11.

9. Let $K/k$ be a Galois extension of number fields with Galois group $G$, let $\mathfrak{m}$ be a modulus of $K$ which is invariant under $G$ and let $H$ be a congruence subgroup for $\mathfrak{m}$. Prove that the class field of $(\mathfrak{m}, H)$ is Galois over $k$ if and only if $G(H) = H$.

10. Take $\mathfrak{m} = \langle 41\rangle = \langle 5 + 4i\rangle\langle 5 - 4i\rangle$, a modulus of $\mathbb{Q}(i)$. Prove that its ray class field contains two subfields which are Galois over $\mathbb{Q}$ of degree 10 and that one of the Galois groups is $C_{10}$ while the other is $D_{10}$.

## 28.7 Hint and Solutions

1. The only prime which can ramify is $\mathfrak{q}$ and so $\mathfrak{m} = \mathfrak{q}^n$ for some $n \geq 0$. Let $k = \mathbb{F}_{\mathfrak{q}}^*$ and by Lemma 28.17,

$$P_{\mathfrak{m}}/P^1_{\mathfrak{m}_0} \cong \frac{C_{p^k-1} \times A}{\mathcal{O}_K^*}$$

where $A$ is abelian of order $p^{k(n-1)}$. Further,

$$|P^1_{\mathfrak{m}_0}/P^1_{\mathfrak{m}}| = 2^r$$

for some $r \geq 0$. Let $h_K$ be the class number of $K$. Then

$$|I_{\mathfrak{m}}/P^1_{\mathfrak{m}}| = h_k 2^r (p^k - 1)\frac{p^{k(n-1)}}{|\mathcal{O}_K^*|}.$$

Suppose we have a required extension as in the question, say $L$, then it is cyclic and hence abelian. So it is a class field of $K$ for $(\mathfrak{m}, H)$ for some $H$. $[L : K] = p$ and so $H/P^1_{\mathfrak{m}}$ is the subgroup which has quotient of order $p$ (because $I_{\mathfrak{m}}/H$ is isomorphic to the Galois group) and further the quotient is cyclic of order $p$.

Now look at the expression above for $|I_{\mathfrak{m}}/P^1_{\mathfrak{m}}|$, there is only one possible group (as $I_{\mathfrak{m}}/P^1_{\mathfrak{m}}$ is abelian) which satisfies the above, as $(2, p) = (h_K, p) = 1$. So we have at most one such extension.

2. Let $F/K$ be abelian which is unramified outside 11. $K$ has no real embeddings, so the conductor $\mathfrak{m} = \langle 11\rangle^n$ for some $n \geq 0$. Since the class number is 1 and the units $\pm 1, \pm i$ are distinct modulo 11, so

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = P_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong \frac{C_{120} \times A}{C_4} \cong C_{30} \times A$$

where $A$ is abelian of order $11^{2(n-1)}$.

This has no $C_4$ quotient and so there is no $C_4$-extension. It has only one $C_2$-quotient and so there is a unique $C_2$-extension. Let it be $\mathbb{Q}(i)(\sqrt{\alpha})$. Then 11 is ramified (we know the Hilbert class field of $\mathbb{Q}(i)$ is itself so if 11 is unramified then the extension is trivial).

In this case, $11\big|\alpha$ and no other primes ramified so we can try $\alpha = -11$. The only possible primes which ramify in $\mathbb{Q}(i)(\sqrt{-11})$ are 2 or 11. But 2 is unramified in $\mathbb{Q}(\sqrt{-11})$ and it is ramified in $\mathbb{Q}(i)$. Hence, $\mathbb{Q}(i)(\sqrt{-11})/\mathbb{Q}(i)$ is unramified outside 11 and by uniqueness it is the required one.

3. $K$ is a principal ideal domain so $I_{\mathfrak{m}} = P_{\mathfrak{m}}$ and so

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = P_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong \frac{(\mathcal{O}_K/\langle 4+i\rangle)^*}{\mathcal{O}_K^*} = \frac{C_{16}}{C_4} = C_4$$

because we have no real embeddings in $K$ and $\pm 1, \pm i$ are distinct modulo $4 + i$.

By Kummer theory, let $F$ be the ray class field and $F = K(\sqrt[4]{\alpha})$. $\mathfrak{m}$ is a prime and so it must be the conductor and so $\langle 4 + i\rangle$ ramifies and no other prime ramifies. So $\alpha$ is a power of $4 + i$ modulo unit. We may assume that $\alpha = i^a(4+i)^b, a, b = 0, 1, 2, 3$. If $b = 0$ or 2, then $K(\sqrt{\alpha})/K$ is unramified at $4 + i$ and hence unramified everywhere, but we know $K$ has no non-trivial Hilbert class field, so $b = 1$ or 3. Again we can assume that $b = 1$ so $\alpha = i^a(4+i), a = 0, 1, 2, 3$.

Take $x = 6 + i$ which is not a prime in $P^1_{\mathfrak{m}}$ and so the Frobenius element should not be trivial. $x$ is a prime above 37. Let $\mathfrak{p} = \langle 6 + i\rangle$. Then

$$\mathrm{Frob}_{\mathfrak{p}}(\sqrt[4]{\alpha}) \equiv -i^{a+1}\sqrt[4]{\alpha} \bmod x$$

and so $a \neq 1$ because the Frobenius cannot be trivial (note that $4+i \equiv -2 \bmod x$ and $2^9 \equiv -6 \bmod 37$).

Now consider $x = 4+5i$ which is a prime in $P^1_{\mathfrak{m}}$. Then the Frobenius element should be trivial. Repeat the same as above, we get

$$\sqrt[4]{\alpha} \equiv (-1)^{a+1}\sqrt[4]{\alpha} \bmod x$$

and so $a = 1$ or 3. But $a \neq 1$ so $a = 3$ and so $F = K(\sqrt[4]{1-4i})$.

4. The class group is trivial and so $I_{\mathfrak{m}} = P_{\mathfrak{m}}$. Then

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong \frac{C_6 \times C_6}{C_6} = C_6$$

as 7 splits as a product of primes. If $I_{\mathfrak{m}}/H \cong C_3$ then $H/P^1_{\mathfrak{m}}$ is the unique one with quotient $C_3$ of above and so $H$ is unique.

It is clear that $\{1,2,4\} = C_3 \subset C_6$ and $1,2,4$ are distinct modulo 7 and distinct modulo units. So we need a generator of the form $a+b\zeta_3$ whose square is 2 mod 7 (in this way we can find a representative class for $H$). Certainly one can deduce this by looking at the isomorphisms but I think this way is easier. Consider

$$a^2 - 2 - b^2 + (2ab - b^2)\zeta_3 \equiv 0 \bmod 7.$$

Take $a = 2$ and $b = 4$ and $2+4\zeta_3$ is not congruent to $1,2,4$ modulo the units. Thus, we have

$$H/P^1_{\mathfrak{m}} = \{1, 4+\zeta_3\} \text{ as } (2+4\zeta_3)^3 \equiv 4+\zeta_3 \bmod 7.$$

Then $H$ corresponds to the congruence classes of

$$\{\pm 1, \pm\zeta_3, \pm\bar{\zeta_3}, \pm\alpha, \pm\zeta_3\alpha, \pm\bar{\zeta_3}\alpha\} \text{ where } \alpha = 4+\zeta_3.$$

For the class field, consider that $F$ is the cubic extension contained in $\mathbb{Q}(\zeta_7)$ then $FK$ is a cubic extension of $K$ which is unramified outside 7 and $FK/K$ is abelian. Then by uniqueness of the class field, we know that $FK$ must be the class field of $(\mathfrak{m}, H)$.

5. Let $\sigma_1(\sqrt{2}) = \sqrt{2}, \sigma_2(\sqrt{2}) = -\sqrt{2}$. The class group is trivial.

For the first case,

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = P_{\mathfrak{m}}/P^1_{\mathfrak{m}} = (\mathcal{O}_K/\langle 3\rangle)^*/\mathcal{O}_K^* = C_8/\mathcal{O}_K^*.$$

But $\mathcal{O}_K^* = \{\pm e^n\}$ where $e = \sqrt{2}+1$. Now $(\mathcal{O}_K/\langle 3\rangle)^*$ has representatives

$$\pm 1, \pm\sqrt{2}, 1\pm\sqrt{2}, -1\pm\sqrt{2}.$$

Then by direct computing we see that $e^2 \equiv -\sqrt{2} \bmod 3$ and $e^3 \equiv -\sqrt{2}+1 \bmod 3$ and so the units cover everything in $(\mathcal{O}_K/\langle 3\rangle)^*$ because the above list is

$$\pm 1, \pm e, \pm e^2, \pm e^3.$$

So $(\mathcal{O}_K/\langle 3\rangle)^*/\mathcal{O}_K^*$ is trivial.

For $\mathfrak{m} = \langle 3\rangle\sigma_1$, we only quotient out the units which are positive under $\sigma_1$, i.e. $\{e^n : n \in \mathbb{Z}\}$. Notice that $e^4 \equiv -1 \bmod 3$ and so $1, e, \ldots, e^7$ also gives the above representatives and so we again have the trivial group.

Similarly, for $\mathfrak{m} = \langle 3\rangle\sigma_1\sigma_2$, we only quotient out the units which are positive under both $\sigma_1$ and $\sigma_2$. The units which are positive under $\sigma_2$ are $\bar{e}^n = (-e)^n$ where $\bar{e} = -\sqrt{2}+1$. So the intersection gives

$$\{e^{2n} : n \in \mathbb{Z}\}.$$

Therefore, $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = C_2$ (because we only have $1, e^2, e^4, e^6$).

For the ray class field, clearly if $\mathfrak{m} = \langle 3\rangle$ or $\mathfrak{m} = \langle 3\rangle\sigma_1$, then since $I_{\mathfrak{m}}/P^1_{\mathfrak{m}}$ is trivial so the ray class field is itself.

When $\mathfrak{m} = \langle 3\rangle\sigma_1\sigma_2$, the ray class field has degree 2 over $K$ and the only prime which ramifies is 3. Moreover by Theorem 28.15(iii), the real embedding extends to the complex embedding and so we consider $F = \mathbb{Q}(\sqrt{2}, \zeta_3)$ because $F$ must be inside a cyclotomic extension, and among those only $F$ is the one which only ramifies at 3 (or use Kummer theory).

6. Let $p \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{p})$. To check the class number is odd, it suffices to check (by property of Hilbert class field) that it has no quadratic extension which is unramified everywhere.

   Suppose $F/K$ is a quadratic extension which is unramified everywhere. If $F/\mathbb{Q}$ is Galois, then it is $C_4$ or $C_2 \times C_2$. So $F$ is a class field for some $(\mathfrak{m}, H)$ where $\mathfrak{m} = p^n$ for some $n$ and $F$ is a subfield of $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$ because if $\mathfrak{m} = p$ then the ray class field is $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$ and we apply Lemma 28.23. Extensions of these are totally ramified at $p$, but $F/K$ is unramified at $p$, which is a contradiction.

   If $F/\mathbb{Q}$ is not Galois, let $L/\mathbb{Q}$ be the Galois closure and $\mathrm{Gal}(L/\mathbb{Q}) \subset S_4$. Let $F = K(\sqrt{\alpha})$. Now we can write $\alpha = a + b\sqrt{p}$ and so $F = \mathbb{Q}(\sqrt{a+b\sqrt{p}})$. The conjugates are $\pm\sqrt{a \pm b\sqrt{p}}$. Since it is not Galois, and observe that $\sqrt{a-b\sqrt{p}} = \frac{\sqrt{a^2-b^2p}}{\sqrt{a+b\sqrt{p}}}$ we conclude that $L = F(\sqrt{a^2-b^2p})$ and so $[L:\mathbb{Q}] = 8$. Since $F/\mathbb{Q}$ is not Galois, and so $\mathrm{Gal}(L/\mathbb{Q})$ can only be $D_8$ or $\mathbb{Q}_8$ where

   $$\mathbb{Q}_8 = \langle i, j, k : i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j\rangle.$$

   Since $F/\mathbb{Q}$ only ramifies at $p$ so $L/\mathbb{Q}$ only ramifies at $p$. If $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8 = \langle x, y : x^4 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$, and $\langle x^2, y\rangle, \langle x\rangle$ are subgroups of index 2, so they give rises to different quadratic extensions, only ramified at $p$. But we only have one such extension for $p \equiv 1 \bmod 4$, which is a contradiction. Similarly, for $\mathbb{Q}_8$ we can consider $\{\pm 1, \pm i\}, \{\pm 1, \pm j\}$. This completes the proof.

   For $-p \equiv 1 \bmod 4$, run through the above argument for $-p$.

7. Let $K = \mathbb{Q}(\sqrt{d})$ and $F$ be the its Hilbert class field. Then $\mathrm{Gal}(F/K) = C_4$ and further we know that $F/\mathbb{Q}$ is Galois. Let $\mathfrak{p}$ be a prime in $K$, the order of $[\mathfrak{p}]$ in $\mathrm{cl}_K$ is the same as the order of $\mathrm{Frob}_{\mathfrak{p}}$ in $\mathrm{Gal}(F/K)$ (Lemma 28.24). Fix a prime $\mathfrak{p}$ such that $[\mathfrak{p}]$ has order 4 and so $\mathrm{Frob}_{\mathfrak{p}}$ has order 4.

   Let $G = \{1, \sigma\}$ where $\sigma$ sends $\sqrt{d}$ to $-\sqrt{d}$. It is clear that for any prime $\mathfrak{p}$, $\mathfrak{p}\sigma(\mathfrak{p})$ is principal (equal to the prime below $\mathfrak{p}$) and so $\sigma$ acts as $-1$ in $\mathrm{cl}_K$.

   If $p$ ramifies in $K/\mathbb{Q}$ then $e_p(F/\mathbb{Q}) = 2$ because $F/K$ is unramified everywhere. Take $y$ to be a generator of $I_p$. We claim that $y$ gives a lift of $\sigma$. Suppose not, then $y$ fixes $K$, and so $y \in \mathrm{Gal}(F/K)$. But $I_p(F/K) \cap \mathrm{Gal}(F/K) = \{1\}$, which is a contradiction. So $y$ is a lift of $\sigma$.

   Now we can set $\mathrm{Gal}(F/\mathbb{Q}) = \langle x, y\rangle$ where $\langle x\rangle = \mathrm{Gal}(F/K)$. We have $x^4 = y^2 = 1$. Also take the prime $\mathfrak{p}$ for which $\mathrm{Frob}_{\mathfrak{p}}$ has order 4. Then $\mathrm{Frob}_{\mathfrak{p}} = x$ or $x^3$ and we may assume it is $x$. Then if we write $\mathrm{cl}_K = \{0, 1, 2, 3\}$, the action of $y$ is sending $a$ to $-a$ and the action of $x$ is

sending $a$ to $a+1$ for $a \in \mathrm{cl}_K$ (via the Artin map, the action of $x$ on $\mathrm{cl}_K$ is compatible with the order of $x$). Now consider $yxy^{-1}$,

$$yxy^{-1}(a) = yx(-a) = y(1-a) = a - 1 = x^{-1}(a).$$

This shows that $yxy^{-1} = x^{-1}$ and hence the Galois group is $D_8$.

8. We can find a $C_t$ extension of a number field $K$ which is unramified everywhere with $t$ a multiple of 11 (then this extension must lie in the Hilbert class field of $K$ and hence the class number of $K$ is divisible by 11).

   For any number field $K$, $K(\zeta_{23})/K$ can only ramify at 23. Pick a prime which splits completely in $\mathbb{Q}(\zeta_{23})$, say $q = 47$. Let $f(X)$ be $q$-Eisenstien such that $f(X) = \Phi_{23}(X) \bmod (23)^N$ for some $N$ large enough and it is always possible. Pick $N$ large enough so that

   $$\mathbb{Q}_{23}[X]/\langle f(X)\rangle \cong \mathbb{Q}_{23}[X]/\Phi_{23}(X)$$

   by using Theorem 25.24.

   Pick $\alpha$ a root of $f$. Let $K = \mathbb{Q}(\alpha)$. Then by Kummer-Dedekind, $q$ is totally ramified, But $q$ splits completely in $\mathbb{Q}(\zeta_{23})$ so $K(\zeta_{23})/K$ has degree 22. Now if $\mathfrak{p}$ is a prime of $K$ above 23, then $K_{\mathfrak{p}} = \mathbb{Q}_{23}(\alpha) = \mathbb{Q}_{23}(\zeta_{23})$.

   Now apply Theorem 23.13. We know

   $$K_{\mathfrak{p}} = \mathbb{Q}_{23}[X]/\langle f(X)\rangle = \mathbb{Q}_{23}[X]/\Phi_{23}(X)$$

   and Theorem 23.13 says the splitting behavior of $\mathfrak{p}$ in $K(\zeta_{23})/K$ depends on the factoirsation of $\Phi_{23}(X)$ in $K_{\mathfrak{p}}[X] = \mathbb{Q}_{23}(\zeta_{23})(X)$. But this clearly splits completely and so we claim that $\mathfrak{p}$ splits completely in $K(\zeta_{23})/K$.

   Thus, $K(\zeta_{23})/K$ is an extension of degree 22, unramified everywhere and so the class number of $K$ is divisible by 22.

9. Let $F$ be the class field of $(\mathfrak{m}, H)$ and $X = \mathrm{Gal}(F/K)$. Note that We can introduce the $G$ action on $X$ by $\sigma x = \tilde{\sigma} x \tilde{\sigma}^{-1}$ where $\tilde{\sigma}$ is a lift of $\sigma$.

   Let $L$ be the Galois closure of $F/k$ and $\mathfrak{q}$ a prime of $L$ above $\mathfrak{p}$, a prime of $K$. Let $\tilde{G} = \mathrm{Gal}(L/k)$ and so $\tilde{G}$ acts on $\mathfrak{p}$. We know $\mathfrak{p} \in H$ if and only if $\mathfrak{p}$ splits completely in $F$ and $F/k$ is Galois if and only if $\sigma F = F$ for all $\sigma \in \tilde{G}$. The action of $\sigma$ on $K$ is the same as $\sigma|_K \in G$.

   By uniqueness $\sigma F = F$ if and only if $\sigma F$ is also a class field for $(\mathfrak{m}, H)$, if and only if the following condition holds: $\mathfrak{p} \in H$ if and only if $\mathfrak{p}$ splits completely in $\sigma F$.

   But $\mathfrak{p}$ splits completely in $\sigma F$ if and only if $\sigma^{-1}\mathfrak{p} \in H$, if and only if $\mathfrak{p} \in \sigma H$. Therefore, $\sigma F = F$ if and only if we have the condition that $\mathfrak{p} \in H$ if and only if $\mathfrak{p} \in \sigma H$, where the later is the same as $H = \sigma H$.

   Hence $F/k$ is Galois if and only if $\sigma F = F$ for all $\sigma \in \tilde{G}$, if and only if $G(H) = H$ (as the action of $\tilde{G}$ on $H$ is the same as $G$ on $H$).

10. $K = \mathbb{Q}(i)$ is a principal ideal domain. Then

    $$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = P_{\mathfrak{m}}/P^1_{\mathfrak{m}} = \frac{C_{40} \times C_{40}}{C_4} = C_{10} \times C_{40}.$$

The ray class field has Galois group $C_{10} \times C_{40}$ and so we only have two subgroups with index 5 (so that it has degree 10 over $\mathbb{Q}$) namely $C_2 \times C_{40}$ and $C_{10} \times C_8$. By fundamental theorem of Galois, we know that these two subfields must be different. Further, let $F = K(\alpha)$ be any of these two, then $F = \mathbb{Q}(\alpha, i)$ must be Galois over $\mathbb{Q}$ because it has every conjugate inside $F$ (as $F/K$ is Galois).

Finally, the only groups of degree 10 are isomorphic to either $C_{10}$ or $D_{10}$. But since the two subfields are not isomorphic to each other (otherwise we are saying that $C_2 \times C_{40}$ is isomorphic to $C_{10} \times C_8$) so the Galois group of these two over $\mathbb{Q}$ must also be distinct. Therefore, one of them is $C_{10}$ and the other one is $D_{10}$.

# 29 Isogeny and The Weil Pairing

We will discuss some more topics on elliptic curves in this and next several sections. Some basic algebraic geometry is required in some topics. Throughout the section, $K$ will be a number field and $\bar{K}$ its algebraic closure. This is based on Silverman's book, with my own solution to the collection of exercises at the end of the section.

## 29.1 Isogeny

We have seen isomorphisms between elliptic curves (in the sense they are isomorphism viewed as projective varieties). Recall that the set of (rational) points on elliptic curves has a natural group structure, and we would like to investigate the maps between different elliptic curves which preserve the group structure, i.e. homomorphisms.

**Definition 29.1.** *Let $E$ and $F$ be elliptic curves. An* **isogeny** *from $E$ to $F$ is a morphism*

$$\phi : E \to F \text{ satisfying } \phi(O) = O.$$

*Two elliptic curves $E$ and $F$ are said to be* **isogenous** *if there is a non-trivial isogeny from $E$ to $F$. Later we will see this is an equivalence relation and in particular a symmetric relation.*

It will be shown later (Proposition 29.3) that any morphism between two elliptic curves which preserve the origin is indeed a group homomorphism between the two curves with the natural group structure. Also, it is known that a morphism between curves is either constant or surjective. Therefore, except for the trivial isogeny, we have

$$\phi(E) = F.$$

The morphism induces an injection of the function fields

$$\phi^* \bar{K}(F) \to \bar{K}(E).$$

The degree of the map $\phi$ is the degree of the finite extension $\bar{K}(E)/\phi^*\bar{K}(F)$. We say the map is separable, inseparable or purely inseparable if the corresponding field extension has the same property. By convention the trivial isogeny has degree 0. Then it is clear that

$$\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi) \text{ for any chain of isogenies.}$$

We denote the sum of isogenies by the taking the pointwise sum. Under this operation, the set of isogenies from $E$ to $F$ form a group, denoted by $\mathrm{Hom}(E, F)$. If $F = E$ then we denote the set by $\mathrm{End}(E)$, the set of endomorphisms of $E$ and we define the multiplication of two endomorphisms to be the composition. We will see later this forms a ring structure.

**Example 29.2.** *For each integer $m$ we have seen the multiplication-by-$m$ map on $E$ itself. This is clearly an isogeny (endomorphism) by definition. The degree of the map is $m^2$.*

**Proposition 29.3.** *(i) Let $E/K$, $F/K$ be elliptic curves. Then $Hom(E, F)$ is a torsion-free $\mathbb{Z}$-module.*

*(ii) For any elliptic curve $E/K$, $End(E)$ is an integral domain (hence a ring )of characteristic 0. Note $End(E)$ is not necessarily commutative (although we will show later this is the case when $K$ is a number field).*

*Proof.* Assuming that the multiplication is distributive in $\mathrm{End}(E)$ then it is clearly a ring by checking the basic definitions. Also, by the first part we see that $\mathrm{End}(E)$ has characteristic 0 as it is torsion-free. Finally, since the degree is multiplicative so if the composition of two endomorphisms gives the trivial isogeny then one of them must be trivial because one of them must have degree 0.

So it remains to check the first part of the proposition and show that multiplication in $\mathrm{End}(E)$ is distributive. It is clear that multiplication by $m$ is surjective by showing it is nonconstant. (As we are working over number fields $K$ so this is clearly true. In fact this is true even for $K$ with non-zero characteristic.) So the degree of $[m]$ is non-zero and hence if we have some isogeny $\phi$ in $\mathrm{Hom}(E, F)$ then by considering the degree we conclude that $\phi$ has degree 0 and hence the trivial isogeny.

To prove that multiplication is distributive, we need to show that for all $P, Q \in E$,

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

In fact we prove something stronger, for any isogeny $\phi$ from $E$ to $F$ we prove the above relation. This is certainly true for the trivial isogeny so assume $\phi$ non-trivial. We require some knowledge of algebraic geometry here. The morphism between the varieties induces a homomorphism between the Picard groups

$$\phi_* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(F).$$

defined by

$$\phi_*([\sum_i n_i(P_i)]) = [\sum_i n_i(\phi P_i)]$$

where the square bracket denotes the class (of the divisor).

We also have the isomorphism (which identifies an elliptic curve with its Jacobian) given by

$$j_E : E \to \mathrm{Pic}^0(E),\ P \mapsto [(P) - (O)].$$

Then since $\phi(O) = O$ we have a commutative diagram given by the following equation

$$\phi_*(j_E(P)) = j_F(\phi(P))$$

because both sides gives the class $[\phi(P) - O]$.

Now since $j_E, j_F$ are isomorphisms and $\phi_*$ is a group homomorphism, so $\phi$ is a group homomorphism. This proves the required identity. □

The proof above for the second part shows that any isogeny is indeed a group homomorphism. Also note that

**Corollary 29.4.** *The kernel of any isogeny is finite.*

*Proof.* The size of the kernel is at most the degree of the isogeny by some basic algebraic geometry. □

**Example 29.5.** *Usually we will find that the multiplication by $m$ map is the whole endomorphism ring. However, there are some exceptions and when the endomorphism ring is strictly bigger than $\mathbb{Z}$ (the multiplications) we say the curve $E$ has* **complex multiplication**. *For instance consider the curve*

$$E : y^2 = x^3 - x,$$

*it has an endomorphism, denoted by $[i]$, that*

$$[i] : (x, y) \mapsto (-x, iy),$$

*which is not given by any multiplication by $m$ map. Thus $E$ has complex multiplication. Notice that $[i] \circ [i]$ is the inverse map $[-1]$. Another example is*

$$E : y^2 = x^3 + 1$$

*where we have an endormorphism*

$$[\zeta_3] : (x, y) \mapsto (\zeta_3 x, y).$$

**Definition 29.6.** *Let $E/K$ be an elliptic curve and $Q \in E$ a fixed point. Then we define the translation-by-$Q$ map*

$$\tau_Q : E \to E,\ P \mapsto P + Q.$$

*The map $\tau_Q$ is clearly an isomorphism of curves but not an isogeny.*

**Remark 29.7.** *Let $E/K, F/K$ be elliptic curves and $\phi$ a morphism. Then the compossition*

$$\psi = \tau_{-\phi(O)} \circ \phi$$

*is an isogeny because it is a morphism preserving the origin.*

Our goal in this subsection is to prove that given an elliptic curve $E$ and a finite subgroup $H$ of $E$, there exists a unique elliptic curve $F$ and a separable isogeny with kernel equal to $H$. We first establish the following lemmas.

**Lemma 29.8.** *Let $\phi : E \to F$ be a non-trivial isogeny. Then for each $Q \in F$ the number of fibers of $Q$ is equal to the separable degree, $|\phi^{-1}(Q)| = \deg_s \phi$ where $\deg_s \phi$ is the separable degree.*

*Further for each $P \in E$, we have*

$$e_\phi(P) = \deg_i \phi$$

*where $e_\phi(P)$ is the ramification degree and $\deg_i \phi$ is the inseparable degree of $\phi$.*

*Proof.* By some result of algebraic geometry, for all but finitely many $Q$ we have $|\phi^{-1}(Q)| = \deg_s \phi$. For any $Q_1, Q_2 \in F$ , let $R \in E$ such that $\phi(R) = Q_1 - Q_2$. Since $\phi$ is a homomorphism, so that for each $S_1$ in the preimage of $Q_1$, the point $S_2 = S_1 + R$ is in the preimage of $Q_2$. Hence we have a 1-1 correspondence between the fibers of different points.

Now let $P_1, P_2 \in E$ with the same image. Let $R = P_2 - P_1$ so $\phi(R) = O$. So the map $\phi \circ \tau_R$ is the same as $\phi$. It is a fact of algebraic geometry that ramification degree is unchanged under translation so

$$e_\phi(P_1) = e_{\phi\circ\tau_R}(P_1) = e_\phi(\tau_R(P_1))e_{\tau_R}(P) = e_\phi(P_2)$$

because the translation map is unramified. So each point has the same ramification index. Thus

$$\deg \phi = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = |\phi^{-1}(Q)| e_\phi(P) = (\deg_s \phi) e_\phi(P)$$

from the previous part. □

**Lemma 29.9.** *Let $\phi : E \to F$ be a non-trivial isogeny. The map*

$$\ker \phi \to Aut(\bar{K}(E)/\phi^* \bar{K}(F)),\ T \mapsto \tau_T^*$$

*is an isomorphism, where $\tau_T^*$ is the induced map of the function field by $\tau_T$.*

*Proof.* Firstly we check the map is well-defined, which means that $\tau_T^*$ lives in the correct image. Take $f \in \bar{K}(F)$ and $T \in \ker \phi$ we have

$$\tau_T^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f$$

because $\phi \circ \tau_T = \phi$. This shows that $\tau_T^*$ fixes any element in the base field so it is in the image.

It is clear that the map is a homomorphism because

$$\tau_{S+T} = \tau_s \circ \tau_T = \tau_T \circ \tau_S.$$

Finally by the previous lemma we know the size of the kernel is exactly the separable degree. Now by Galois theory, we know that the number of automorphism is at most the separable degree, so this

shows that the size of the image is at most the size of $\ker \phi$. Since both sets are finite so to show it is bijective, it suffices to show it is injective.

Suppose $\tau_T^*$ fixes $\bar{K}(E)$. Since

$$\tau_T^* \circ f(P) = (f \circ \tau_T)(P) = f(T+P)$$

by definition then every rational function on $E$ takes the same value at $T$ and $O$. By considering the function $f(P) = x(P)$ we conclude that $T = O$ and so it is injective. □

**Corollary 29.10.** *Let $\phi : E \to F$ be a non-trivial, separable isogeny. Then $\phi$ is unramified and $|\ker \phi| = \deg \phi$, and $\bar{K}(E)$ is a Galois extension of $\phi^* \bar{K}(F)$.*

*Proof.* By the previous two lemmas, we see that if $\phi$ is separable then the degree of $\phi$ is the separable degree so for each $Q \in F$, $|\phi^{-1}(Q)| = \deg \phi$. Also,

$$\deg \phi = \sum_{P \in \phi^{-1} Q} e_\phi(P)$$

we conclude that $e_\phi(P) = 1$ for all $P$ in the preimage so it is unramified and the size of the kernel is by taking $Q = O$. Combining the previous proposition we see that the degree of extension is the same as the size of the automorphism group so it is a Galois extension. □

**Corollary 29.11.** *Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be non-trivial isogenies and assume that $\phi$ is separable. If $\ker \phi \subset \ker \psi$ then there exists a unique isogeny $\lambda$ from $E_2$ to $E_3$ such that $\psi = \lambda \circ \phi$.*

*Proof.* $\phi$ is separable so by previous Corollary the extension of function field is Galois. Further, since $\ker \phi \subset \ker \psi$ and by the identification in Lemma 29.9 we conclude that the map $\tau_T^*$ induced by translation of any point $T$ in $\ker \phi$ must fix the field $\psi^* \bar{K}(E_3)$ and we have a tower of fields

$$\psi^* \bar{K}(E_3) \subset \phi^* \bar{K}(E_2) \subset \bar{K}(E_1).$$

By algebraic geometry an injection of function field induces a morphism between the curves so there exists a morphism $\lambda : E_2 \to E_3$ such that

$$\phi^*(\lambda^* \bar{K}(E_3)) = \psi^* \bar{K}(E_3)$$

which is equivalent of saying $\lambda \circ \phi = \psi$. Since both $\phi$ and $\psi$ fix the origin so does $\lambda$ and it is an isogeny. □

Now we are ready to prove the main theorem.

**Theorem 29.12.** *Let $E$ be an elliptic curve and $H$ a finite subgroup of $E$. Then there is a unique elliptic curve $C$ together with a separable isogeny $\phi : E \to C$ such that $\ker \phi = H$. Often we denote the curve $C$ by $E/H$ (in general the quotient of a variety b a finite group of automorphism is again a variety).*

*Proof.* Let $\bar{K}(E)^H$ be the subfield fixed by the action of $H$, where we identify each element $T$ in $H$ in the sense that given $T \in H$, the induced map $\tau_T^*$ is an automorphism on $\bar{K}(E)$. Then $\bar{K}(E)/\bar{K}(E)^H$ is a Galois extension with Galois group $H$.

The field $\bar{K}(E)^H$ has transcendence degree one (since $\bar{K}(E)$ has transcendence degree one) over $K$ so by algebraic geometry we know there is a unique smooth curve $C/K$ and a finite morphism

$$\phi : E \to C \text{ satisfying } \phi^* \bar{K}(C) = \bar{K}(E)^H.$$

We next show that $\phi$ is unramified. Let $P \in E$ and $T \in H$. Let $f \in \bar{K}(C)$, then

$$f(\phi(P+T)) = (\tau_T^* \circ \phi *) f(P) = (\phi^* f)(P) = f(\phi(P))$$

because by definition for every element $T \in H$ the induced map $\tau_T^*$ fixes the function field $\phi^*\bar{K}(C) = \bar{K}(E)^H$. Thus $\phi(P+T) = \phi(P)$. Now let $Q \in C$ and pick any $P \in E$ with $\phi(P) = Q$. Since $\phi(P+T) = \phi(P) = Q$ for all $T \in H$ so the preimage of $Q$ contains the coset $P + H$. But $|\phi^{-1}(Q)| \leq \deg \phi$ with equality if and only if the map $\phi$ is unramified. Since

$$\deg \phi = [\bar{K}(E) : \phi^*\bar{K}(C)] = [\bar{K}(E) : \bar{K}(E)^H] = |H|$$

and the size of $P + H$ is the same as $|H|$ we conclude that $\phi$ is unramified

By Riemann-Hurwitz formula and since $\phi$ is unramified we have

$$2\text{genus}(E) - 2 = (\deg \phi)(\text{genus}(C) - 2)$$

and so $C$ has genus one. Since we work over the algebraic closure so $C$ has a rational point and so it becomes an elliptic curve and $\phi$ is an isogeny by taking $\phi(O)$ to be $O_C$. From this construction we see that the kernel is exactly $H$. □

## 29.2 Invariant Differential

In this subsection we will introduce the invariant differential and the main goal is to prove that for number field $K$ (or more generally any field with characteristic 0) the ring $\text{End}(E)$ is commutative.

**Definition 29.13.** *Let $E/K$ be an elliptic curve with standard Weierstrass form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*The* **invariant differential** $\omega$ *is defined to be*

$$\omega = \frac{dx}{2y + a_1x + a3} \in \Omega_E.$$

*It has neither zero or poles.*

The following proposition justifies the name of invariant differential.

**Proposition 29.14.** *$\omega$ is invariant under translation. In other words,*

$$\tau_Q^*\omega = \omega$$

*for all $Q \in E$.*

*Proof.* Either one check this directly (probably by using Sage or MAGMA) or here is an alternative way to prove this. Since $E$ has genus one so $\Omega_E$ is a one-dimensional $\bar{K}(E)$-vector space, and so there is a function $a_Q \in \bar{K}(E)^*$ such that

$$\tau_Q^*\omega = a_Q\omega.$$

Then we see the divisor of $a_Q$ is the difference of divisor of $\tau_Q^*\omega$ and divisor of $\omega$. But we know that $\omega$ has neither zero of poles so this implies that $a_Q$ has neither zero or poles. Hence $a_Q$ is a constant. Now consider the map

$$f : E \to \mathbb{P}^1,\ Q \mapsto [a_Q : 1].$$

It is clear that this is a rational function (because roughly speaking it can be written in terms of $x(Q)$ and $y(Q)$) and it is not surjective because $[1 : 0]$ is not in the image. Therefore it is a constant map and so $a_Q$ is independent of $Q$. So evaluating at $Q = O$ we conclude that $a_Q = 1$ for all $Q$. □

We then prove the distributive law in the following sense

**Theorem 29.15.** *Let $E$ and $F$ be elliptic curves and $\omega$ be invariant differential of $E$. Let $\phi, \psi$ be isogenies from $F$ to $E$. Then*

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega.$$

*Here the $+$ on left hand side is the operation in $Hom(E, F)$ while the $+$ on the right hand side is the addition in the vector space $\Omega_E$.*

*Proof.* The idea of the proof is essentially to check some calculations. There is nothing to prove when $\phi$ or $\psi$ is trivial. Also if $\phi + \psi$ is trivial then

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*$$

and it suffices to check $[-1]^* \omega = -\omega$. This is immediate if we plug in the formulae for $-(x, y)$ in terms of $(x, y)$. So we may assume that none of $\phi, \psi, \phi + \psi$ is trivial.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be independent points on $E$ (in the sense that there are no algebraic relations between the coordinates). Let $R = (x_3, y_3) = P + Q$. Let $\omega(x, y)$ denote the invariant differential at $(x, y)$. By writing $R$ explicitly in terms of $x_1, x_2, y_1, y_2$ we have

$$\omega(x_3, y_3) = f(x_1, x_2, y_1, y_2)\omega(x_1, y_1) + g(x_1, x_2, y_1, y_2)\omega(x_2, y_2).$$

We check $f$ and $g$ are both 1. Fix some $Q \in E$ such that $x_2 = x(Q)$ and $y_2 = y(Q)$ so that $dx_2 = 0$ and $\omega(x_2, y_2) = 0$. Then by previous lemma we have

$$\omega(x_3, y_3) = \tau_Q^* \omega(x_1, y_1) = \omega(x_1, y_1).$$

Substitute this into the above equation we get $f(x_1, y_1, x(Q), y(Q)) = 1$ and so $f$ does not depend on $x_1, y_1$. Similarly we can repeat to conclude that $f$ is also independent of $x_2, y_2$ and hence $f = 1$ is a constant. Repeat this for $g$ we conclude that $g = 1$.

Now we have shown

$$R = P + Q \Rightarrow \omega(R) = \omega(P) + \omega(Q).$$

Let $S$ be a point on $F$ and let

$$P = \phi(S), Q = \psi(S), R = (\phi + \psi)(S) = \phi(S) + \psi(S).$$

Thus we have $\omega(R) = \omega(P) + \omega(Q)$ which means

$$(\omega \circ (\phi + \psi))S = (\omega \circ \phi)S + (\omega \circ \psi)S$$

and this gives the required identity. □

**Corollary 29.16.** *Let $E$ be an elliptic curve and $\omega$ the invariant differential. Then for all $m \in \mathbb{Z}$,*

$$[m]^* \omega = m\omega.$$

*Proof.* This is clearly true for $m = 0$ and 1. Now apply induction and use the theorem for the inductive step with $\phi = [m]$ and $\psi = [1]$. □

The second application of the theorem is on elliptic curve over finite fields.

**Corollary 29.17.** *Let $E$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $p$. Let $\phi : E \to E$ be the $q^{th}$-power Frobenius morphism and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

*is separable if and only if $p \nmid m$. In particular the map $1 - \phi$ is separable.*

*The Frobenius morphism is the map which sends $(x, y)$ to $(x^q, y^q)$. We do not tend to discuss elliptic curves over finite fields in detail in this chapter but later on we will probably give a chapter for that.*

*Proof.* Let $\omega$ be the invariant differential on $E$. By algebraic geometry, the map $\phi$ is separable if and only if $\phi^* : \Omega_E \to \Omega_E$ is injective. But $\Omega_E$ is a one-dimensional vector space so injective basically means that the map $\phi^*$ is not trivial. Then $m + n\phi$ is separable if and only if

$$(m + n\phi)^*\omega = m\omega + n\phi^*\omega \neq 0$$

using the theorem and the previous corollary.

$\phi$ is the Frobenius morphism so it is easy to check directly that

$$\phi^*\omega = \left(\frac{d(x^q)}{2y^q + a_1x^q + a_3}\right) = 0$$

because $q = 0$ in $\mathbb{F}_q$. Hence the map $m + n\phi^*$ is separable if and only if $m\omega \neq 0$, which is the same as $p \nmid m$. In particular, $1 - \phi$ is separable by setting $m = 1$ and $n = -1$. □

We now prove the main theorem.

**Theorem 29.18.** *Let $E/K$ be an elliptic curve and let $\omega$ be the invariant differential. Define a map from $End(E)$ to $\bar{K}$ in the following way:*

$$End(E) \to \bar{K} \ , \phi \mapsto a_\phi \text{ such that } \phi^*\omega = a_\phi\omega.$$

*Then this map is a ring homomorphism with kernel the set of inseparable endomorphisms of $E$. In particular, when $K$ is a field of characteristic zero, $End(E)$ is a commutative ring.*

*Proof.* We check the map has the correct image. Since $\Omega_E$ is a one-dimensional $\bar{K}(E)$-vector space so $\phi^*\omega = a_\phi\omega$ for some $a_\phi \in \bar{K}(E)$. We see the divisor of $a_\phi$ is trivial in the proof of previous theorem so $a_\phi$ is constant.

The map is clearly a ring homomorphism where the addition law follows from Theorem 29.15 and multiplication follows directly by definition. To find the kernel we have

$$a_\phi = 0 \iff \phi^*\omega = 0 \iff \phi \text{ is inseparable}$$

by algebraic geometry (same statement in the last corollary. Therefore, when $K$ has characteristic zero, every endomorphism is separable so $\mathrm{End}(K)$ is isomorphic to a subring of $\bar{K}$ which is commutative. □

## 29.3 The Dual Isogeny

The purpose of this subsection is to prove that for every non-trivial isogeny $\phi : E \to F$ there exists a unique isogeny $\hat{\phi} : F \to E$ such that the composition is multiplication-by-$m$ where $m = \deg\phi$ and discuss some important properties of this map.

Intuitively, we may consider the following maps: Let $\phi : E \to F$ be a non-trivial isogeny, then it induces a map $\phi^*$ between the Jacobians (Picard groups)

$$\phi^* : \mathrm{Pic}^0(F) \to \mathrm{Pic}^0(E).$$

Recall we also have the map which identifies elliptic curve with its Jacobian

$$j_E : E \to \mathrm{Pic}^0(E), \ P \mapsto [(P) - (O)].$$

Then the composition $j_E^{-1} \circ \phi^* \circ j_F$ gives a map from $E_2$ to $E_1$. Later we will verify that this map actually sends a point $Q$ to $[\deg\phi](P)$ where $P$ is any point such that $\phi(P) = Q$.

**Theorem 29.19.** *Let $\phi : E \to F$ be a non-trivial isogeny of degree $m$. Then there exists a unique isogeny*

$$\hat{\phi} : F \to E \text{ satisfying } \hat{\phi} \circ \phi = [m].$$

*Moreover, the map $\hat{\phi}$ can be computed by using the composition of the following maps. For any point $Q$ in $F$, send $Q$ to $(Q) - (O)$ in the degree zero divisor group. Write*

$$\phi^*((Q) - (O)) = \sum_P n_P(P).$$

*Then the map $\hat{\phi}(Q) = \sum_P |n_P|P$ where the sum is taken in the group $E$. $\hat{\phi}$ is called the* **dual isogeny**.

*Proof.* Since we are mainly interested in the case when $E/K$ is defined over a number field, so we will only prove this for number field (or characteristic zero case). The general case is also true and can be found in one of the references.

Since $K$ has characteristic zero so $\phi$ is separable and so by Corollary 29.10, we conclude that the size of the kernel is the same as the degree, $m$. Thus, every element of $\ker \phi$ has order dividing $m$. Now apply Corollary 29.11 with $E_3 = E$, $E_2 = F$ and $\psi = [m]$.

Suppose $\hat{\phi}_1, \hat{\phi}_2$ are isogenies satisfying

$$\hat{\phi}_i \circ \phi = [m].$$

Then let $\hat{\phi} = \hat{\phi}_1 - \hat{\phi}_2$ so we get $\hat{\phi} \circ \phi = [0]$. By considering the degree we see that $\hat{\phi}$ must itself be the trivial isogeny.

Since we have proved such map is unique, it suffices to check that the given construction satisfies the property. Let $Q \in E_2$. By Corollary 29.10, every separable isogeny is unramified so

$$\sum \phi^*((Q) - (O)) = \sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}O} T.$$

Fix any $P \in \phi^{-1}(Q)$ then any other point sent to $Q$ is of the form $P + T$ for some $T \in \phi^{-1}(O)$ and so the above sum is $|\phi^{-1}(Q)|P$. Since $P$ is arbitrary so this is valid for any such $P$ and so we get $|\deg \phi|P$ because the size of the kernel is the same as degree.

Let the map constructed be $\psi$ then

$$\psi \circ \phi(P) = [\deg \phi]P$$

and this is true for all $P$ so by uniqueness $\psi = \hat{\phi}$. □

The next theorem gives some useful properties of the dual isogeny.

**Theorem 29.20.** *Let $\phi : E_1 \to E_2$ be a non-trivial isogeny.*

*(i) Let $m = \deg \phi$ then*

$$\hat{\phi} \circ \phi = [m] \text{ on } E_1 \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \text{ on } E_2.$$

*(ii) Let $\lambda : E_2 \to E_3$ be another isogeny. Then*

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

*(iii) Let $\psi : E_1 \to E_2$ be another isogeny, then*

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

*(iv) For all $m \in \mathbb{Z}$,*

$$\widehat{[m]} = [m], \text{ and } \deg[m] = m^2.$$

*(v)* $\deg \hat{\phi} = \deg \phi$.

*(vi)* $\hat{\hat{\phi}} = \phi$.

*Proof.* (i) The first identity is by definition of $\hat{\phi}$. For the second one we consider

$$\hat{\phi} \circ (\phi \circ \hat{\phi}) = [m] \circ \hat{\phi} = \hat{\phi} \circ [m]$$

because $\mathrm{End}(E)$ is commutative for characteristic zero field and so $\phi \circ \hat{\phi} = [m]$.

(ii) Let $n = \deg \lambda$. We consider

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = [nm].$$

The result follows by uniqueness of the dual isogeny.

(iii) Let $(x_1, y_1) \in E_1$ and $(x_2, y_2) \in E_2$. We can view $E_2$ as an elliptic curve defined over the function field of $E_1$. Then for any isogeny $\phi$ we can view $\phi(x_1, y_1) \in E_2(K(x_1, y_1))$. Consider the divisor

$$D = \mathrm{div}((\phi + \psi)(x_1, y_1)) - \mathrm{div}(\phi(x_1, y_1)) + \mathrm{div}(\psi(x_1, y_1)) + (O).$$

It sums to $O$ so we know that $D$ is a principal divisor. Then there exists a function

$$f \in K(x_1, y_1)(E_2) = K(x_1, x_2, y_1, y_2)$$

such that $\mathrm{div} f = D$.

Now we consider $f$ as a function of $x_1$ and $y_1$ (so we consider $f$ as a function in $K(x_2, y_2)(E_1)$). Suppose $P_1 \in E_1(\overline{K(x_2, y_2)})$ is a point such that $\phi(P_1) = (x_2, y_2)$. From definition of $D$, we see $f$ has a pole at $P_1$ (by investigating the term $\mathrm{div}(\phi(x_1, y_1))$ in $D$). Further

$$\mathrm{ord}_{P_1}(f) = e_\phi(P_1).$$

Similarly, $f$ has a pole at $P_1$ if $(x_2, y_2) = \psi(P_1)$ and it has a zero at $P_1$ if $(x_2, y_2) = (\phi + \psi)(P_1)$. It follows that as a function of $x_1$ and $y_1$, the divisor of $f$ has the form

$$(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum_i n_i(P_i)$$

where the $P_i$'s are in $E_1(\bar{K})$. The divisor of a function must sum up to $O$ and use the construction of the dual isogeny in the previous theorem, we conclude that

$$\widehat{(\phi + \psi)}(x_2, y_2) - \hat{\phi}(x_2, y_2) - \hat{\psi}(x_2, y_2)$$

does not depend on $(x_2, y_2)$, i.e. it is in $E_1(\bar{K})$. So we can evaluate this at $(x_2, y_2) = O$ which shows that the point is $O$. This completes the proof.

(iv) It is clearly true for $m = 0, 1$. Now apply induction on $m$ and use

$$\widehat{[m+1]} = \widehat{[m]} + \hat{[1]}.$$

Let $d = \deg[m]$ so that

$$[d] = \widehat{[m]}[m] = [m^2]$$

which shows that $d = m^2$.

(v) Let $m = \deg \phi$ then $\deg[m] = m^2 = \deg \hat{\phi} m$ and so $\deg \hat{\phi} = m$.

(vi) Let $\deg \phi = m$ then by (v)

$$\hat{\hat{\phi}}\hat{\phi} = [m]$$

and so $\hat{\hat{\phi}} = \phi$ by uniqueness.

□

**Corollary 29.21.** *Let $E$ and $F$ be elliptic curves. The degree map*

$$\deg : Hom(E, F) \to \mathbb{Z}$$

*is a positive definite quadratic form.*

*Proof.* Clearly it is quadratic because $[-1]$ has degree 1. It is clear that the degree map is positive definite so we check hat

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear. Consider

$$\begin{aligned} [\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)] \\ &= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi}\psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \end{aligned}$$

using the previous theorem. It is clear, again by the theorem, that the last line is linear in both components. □

## 29.4 The Tate Module

This is a short subsection introducing the Tate module as a preliminary knowledge to later sections. The basic idea is consider the action of the absolute Galois group $G_{\bar{K}/K}$ on the torsion subgroups. It is clear that element of the Galois group can only permute the $m$-torsions for any given $m$ because

$$[m](\sigma(P)) = \sigma([m]P) = \sigma(O) = O \ \forall P \in E[m].$$

Thus we obtain a representation

$$G_{\bar{K}/K} \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

where the later isomorphism depends on a choice of basis for $E[m]$. By taking the inverse limit we have the following

**Definition 29.22.** *Let $E$ be an elliptic curve and $p \in \mathbb{Z}$ a prime. The $p$-adic Tate module of $E$ is*

$$T_p(E) = \varprojlim_n E[p^n]$$

*the inverse limit with the projection map*

$$E[p^{n+1}] \to E[p^n], \ Q \mapsto [p]Q.$$

Since each $E[p^n]$ is a $\mathbb{Z}/p^n\mathbb{Z}$-module we see that the Tate module has a natural structure as a $\mathbb{Z}_p$ module. Further since the multiplication-by-$p$ maps are surjective the inverse limit topology on the Tate module is equivalent to the $p$-adic topology it gains by being a $\mathbb{Z}_p$-module.

**Remark 29.23.** *As a $\mathbb{Z}_p$ module, the Tate module $T_p(E) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, simply by the structure of $E[p^n]$ for each $n$.*

**Definition 29.24.** *The p-adic representation (of $G_{\bar{K}/K}$ associated to $E$) is the homomorphism*

$$\rho_p : G_{\bar{K}/K} \to Aut(T_p(E))$$

*induced by the action of $G_{\bar{K}/K}$ on the $E[p^n]$.*

**Remark 29.25.** *If we fix a $\mathbb{Z}_p$-basis for $T_p(E)$ we obtain a representation*

$$G_{\bar{K}/K} \to GL_2(\mathbb{Z}_p),$$

*and then from the natural injection $\mathbb{Z}_p \subset \mathbb{Q}_p$ gives a representation*

$$G_{\bar{K}/K} \to GL_2(\mathbb{Q}_p).$$

*In this way we obtain a two-dimensional representation of $G_{\bar{K}/K}$ and we can avoid choosing a basis by using the natural map*

$$\rho_p : G_{\bar{K}/K} \to Aut(T_p(E)) \hookrightarrow Aut(T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

*In fact, this is analogous to the following construction which is more familiar to us. Recall we can identify the p-adic integer by the inverse system*

$$\mathbb{Z}_p \cong T_p(\mu) = \varprojlim_n \mu_{p^n}$$

*where the projection map is given by*

$$\mu_{p^{n+1}} \to \mu_{p^n},\ \zeta \mapsto \zeta^p.$$

*Further, the natural action of $G_{\bar{K}/K}$ on $\mu_{p^n}$ induces an action on $T_p(\mu)$, so we obtain a one-dimensional representation*

$$G_{\bar{K}/K} \to Aut(T_p(\mu)) \cong \mathbb{Z}_p^*.$$

Now consider elliptic curves $E$ and $F$ and an isogeny

$$\phi : E \to F$$

then $\phi$ induces maps of the $p^n$-torsions for each $n$ and hence induces a map

$$\phi_p : T_p(E) \to T_p(F).$$

Thus we obtain a natural homomorphism

$$\mathrm{Hom}(E, F) \to \mathrm{Hom}(T_p(E), T_p(F)).$$

Further if $E = F$ then this induces a map from the endomorphism ring to the ring of endomorphism of the Tate module.

**Theorem 29.26.** *Let $E$ and $F$ be elliptic curves. Then the natural map*

$$Hom(E, F) \otimes \mathbb{Z}_p \to Hom(T_p(E), T_p(F)),\ \phi \mapsto \phi_p,$$

*is injective.*

*Proof.* The idea of the proof is to work in a finitely generated subgroup of $\mathrm{Hom}(E,F)$ such that if $\phi_p$ is trivial then we can fit $\phi$ into $M \otimes \mathbb{Z}_p$. Let $M$ be the subgroup such that $\phi \in M \otimes \mathbb{Z}_p$ and define

$$N = \{\phi \in \mathrm{Hom}(E,F) : [m] \circ \phi \in M \text{ for some integer } m \geq 1\}.$$

We prove that $N$ is also finitely generated. But this is clear if we extend the degree map over $\mathbb{Q}$.

Let

$$U = \{\phi \in M \otimes \mathbb{Q} : \deg \phi < 1\}$$

be an open neighbourhood of 0. Further since $\mathrm{Hom}(E,F)$ is a torsion-free $\mathbb{Z}$-module by Proposition 29.3, there is a natural inclusion

$$N \subset M \otimes \mathbb{Q}.$$

Further, it is clear that

$$N \cap U = \{0\}$$

because every non-trivial isogeny has degree at least 1. Hence $N$ is a discrete subgroup of the finite-dimensional vector space of $M \otimes \mathbb{Q}$ so it is finitely generated. (Intuitively we might just think $N$ as $M \otimes \mathbb{Q}$ so it is finitely generated by tensoring the basis but the above is a more detailed proof).

Now suppose $\phi_p = 0$ and pick $M$ finitely generated (as we can always do because the group of homomorphism is abelian) so that $\phi \in M \otimes \mathbb{Z}_p$. Take $N$ as above and $N$ is finitely generated so it is free as $\mathrm{Hom}(E,F)$ is $\mathbb{Z}$-torsion free. Let $\psi_1, \ldots, \psi_r$ be a basis for $N$, and by definition of $N$ we can write

$$\phi = \alpha_1\psi_1 + \cdots + \alpha_r\psi_r \text{ with } \alpha_1, \ldots, \alpha_r \in \mathbb{Z}_p$$

because $N \otimes \mathbb{Z}_p = M \otimes \mathbb{Z}_p$.

By density of $\mathbb{Z}$ in $\mathbb{Z}_p$ so fix some $n \geq 1$ and pick

$$a_i \equiv \alpha \ (\mathrm{mod} p^n).$$

Then $\phi_p = 0$ implies that the isogeny

$$\psi = [a_1] \circ \psi_1 + \cdots + [a_r]\psi_r \in \mathrm{Hom}(E,F)$$

annihilates $E[p^n]$ and so $\ker([p^n]) \subset \ker(\psi)$ and then by Corollary 29.11 there exists an isogeny $\lambda$ such that

$$\psi = \lambda \circ [p^n] = [p^n] \circ \lambda.$$

Then $\lambda \in N$ by definition and so we have integers $b_i \in \mathbb{Z}$ such that

$$\lambda = [b_1] \circ \psi_1 + \cdots + [b_r] \circ \psi_r.$$

Since $\psi = [p^n] \circ \lambda$ so by comparing the coefficients of the basis we conclude that

$$a_i = p^n b_i \ \forall i$$

and hence

$$\alpha_i \equiv 0 \ (\mathrm{mod}\ p^n).$$

Since $n$ is arbitrary so we conclude that this is true for all $n$ and hence

$$\alpha_i \equiv 0 \ (\mathrm{mod}\ p^n), \forall n$$

and so $\alpha_i = 0$. This completes the proof. □

**Corollary 29.27.** *Let $E$ and $F$ be elliptic curves. Then the group $\mathrm{Hom}(E,F)$ is a free $\mathbb{Z}$-module of rank at most 4.*

*Proof.* We know that the group is torsion-free. This implies that the $\mathbb{Z}$-rank of the module is the same as

$$\text{rank}_{\mathbb{Z}_p}\text{Hom}(E,F)\otimes\mathbb{Z}_p.$$

By the previous theorem, we have

$$\text{rank}_{\mathbb{Z}_p}\text{Hom}(E,F)\otimes\mathbb{Z}_p \leq \text{rank}_{\mathbb{Z}_p}\text{Hom}(T_p(E),T_p(F)).$$

Then pick bases for $T_p(E)$ and $T_p(F)$ we see that

$$\text{Hom}(T_p(E),T_p(F)) = M2(\mathbb{Z}_p)$$

is the additive group of $2\times 2$ matrices with entries in $\mathbb{Z}_p$. The result follows from this. □

**Remark 29.28.** *We define the group $Hom_K(T_p(E),T_p(F))$ to be the group of $\mathbb{Z}_p$-linear maps from $T_p(E)$ to $T_p(F)$ which commute with the action of $G_{\bar{K}/K}$ as given by the p-adic representation. Thus we have a homomorphism*

$$Hom_K(E,F)\otimes\mathbb{Z}_p \to Hom_K(T_p(E),T_p(F)).$$

*In fact, a deep theorem by Faultings shows that this is an isomorphism when $K$ is a number field.*

## 29.5 The Weil Pairing

In this subsection, we will introduce one of the important pairings on elliptic curve, the Weil-pairing. The construction of the pairing requires some terminology of algebraic geometry (actually there are several equivalent definitions and the one we give here will not require too much knowledge in algebraic geometry). But the key thing in this subsection is the list of properties we will see, of the Weil pairing.

We start with one of the simple pairing one can think of

**Definition 29.29.** *Let $E$ be an elliptic curve Fix a basis $T_1,T_2$ for $E[m]$. Then the discriminant pairing is given by*

$$\det : E[m]\to\mathbb{Z}/\mathbb{Z}/m\mathbb{Z},\ \det(aT_1+bT_2,cT_1+dT_2) = ad-bc.$$

However, a drawback of the determinant pairing is that it is not Galois equivariant, which means that the values of $\det(\sigma(P),\sigma(Q))$ and $\sigma(\det(P,Q))$ may not be the same (for example, if one of the 3-torsion $T_1$ is in the base field and the other one $T_2$, independent of $T_1$ is not in the base field and let $\sigma(T_2)=2T_2$).

**Definition 29.30. [The Weil Pairing]** *Let $T\in E[m]$. Then there is a function $f\in K(E)$ satisfying*

$$div(f) = m(T)-m(O).$$

*Then pick $T'\in E$ to be a point with $[m]T'=T$. Then there is a similarly function $g\in\bar{K}(E$ satisfying*

$$div(g) = [m]^*(T)-[m]^*(O) = \sum_{R\in E[m]}(T'+R)-(R).$$

*Then it is clear that $f\circ[m]$ and $g^m$ have the same divisor so they differ by a constant and by rescaling $f$ by a suitable constant in $\bar{K}$ we may assume that*

$$f\circ[m] = g^m.$$

*Now let $S \in E[m]$ be another $m$-torsion point where we allow $S = T$. Then for any point $X \in E$ we have*

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

*Thus as a function of $X$, the function $g(X+S)/g(X)$ takes values in the $m$-th root of unity. In particular, the morphism*

$$E \to \mathbb{P}^1,\ S \mapsto g(X+S)/g(X)$$

*is not surjective and hence constant. Thus we define the* **Weil pairing** $e_m$ *by*

$$e_m : E[m] \times E[m] \to \mu_m,\ e_m(S,T) = g(X+S)/g(X).$$

*where $X \in E$ is any point such that $g(X+S)$ and $g(X)$ are both defined and nonzero. Note that $g$ is defined up to a constant and so the pairing is well-defined as the constant is canceled out by the quotient.*

We will give another definition in the exercise. Next we list some properties of the Weil pairing.

**Proposition 29.31.** *The Weil pairing has the following properties:*

*(i) It is bilinear.*

$$e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T),\ e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2).$$

*(ii) It is alternating.*

$$e_m(T,T) = 1$$

*and in particular, $e_m(S,T) = e_m(T,S)^{-1}$.*

*(iii) It is non-degenerate:*

$$e_m(S,T) = 1, \forall S \in E[m] \Rightarrow T = O.$$

*(iv) It is Galois invariant:*

$$\sigma(e_m(S,T)) = e_m(\sigma(S),\sigma(T))\ \forall \sigma \in Gal_{\bar{K}/K}.$$

*(v) It is compatible,*

$$e_{mm'}(S,T) = e_m([m']S,T)\ \forall S \in E[mm']\ \textit{and}\ T \in E[m].$$

*Proof.* (i)

$$\begin{aligned} e_m(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X)} = \frac{g((X+S_1)+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)} \\ &= e_m(S_2,T)e_m(S_1,T). \end{aligned}$$

. So we need to check it is linear in the second factor. Let $T_3 = T_1 + T_2$ and $f_1, f_2, f_3, g_1, g_2, g_3$ be the corresponding functions as in the definition. Take a function

$$\mathrm{div}(h) = (T_3) - (T_1) - (T_2) + (O).$$

Then

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = m\mathrm{div}(h),$$

so $f_3 = cf_1f_2h^m$ for some $c \in \bar{K}^*$. Now compose with $[m]$ we have

$$g_3 = c'g_1g_2(h \circ [m]) \text{ for some } c' \in \bar{K}^*.$$

This allows us to compute

$$\begin{aligned} e_m(S, T_1 + T_2) &= \frac{g_3(X+S)/g_3(X)}{=} \frac{g_1(X+S)g_2(X+S)h([m]X + [m]S)}{g_1(X)g_2(X)h([m]X)} \\ &= e_m(S, T_1)e_m(S, T_2) \end{aligned}$$

as $[m]S = O$.

(ii) Fix $T \in E[m]$ and $f$ the function as in the definition of the Weil pairing. Let $\tau_P$ be the translation-by-$P$ map. We compute

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\sum_{i=0}^{m-1}([1-i]T) - ([-i]T) = 0.$$

It follows that $\prod_{i=0}^{m-1} f \circ \tau_{[i]T}$ is constant and since $f \circ [m] = g^m$ so the function

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$$

is also constant for $[m]T' = T$. Therefore we obtain the identity

$$\prod_{i=0}^{m-1} g(X + [i]T') = \prod_{i=0}^{m-1} g(X + T' + [i]T') = \prod_{i=0}^{m-1} g(X + [i+1]T').$$

Canceling like terms from each side gives

$$g(X) = g(X + [m]T') = g(X + T),$$

and hence

$$e_m(T, T) = \frac{g(X+T)}{g(X)} = 1.$$

Now from (i) we have

$$e_m(S+T, S+T) = e_m(S, S)e_m(S, T)e_m(T, S)e_m(T, T)$$

and so $e_m(S, T) = e_m(T, S)^{-1}$.

(iii) If $e_m(S, T) = 1$ for all $S \in E[m]$, then $g(X + S) = g(X)$ for all $S \in E[m]$. This implies that

$$\tau_S^* \circ g = g \ \forall S \in E[m].$$

Then by the identification of Lemma 29.9, this means that $g$ as an element in $\bar{K}(E)/[m]^*\bar{K}(E)$ must live in the base field as it is fixed by the automorphism group. Thus there exists $h$ (which is the pull back of $[m]$) such that

$$g = h \circ [m], h \in \bar{K}(E).$$

Thus,

$$(h \circ [m])^m = g^m = f \circ [m]$$

and so $h^m = f$. Thus

$$m\text{div}(h) = \text{div}(f) = m(T) - m(O)$$

and so $\text{div}(h) = (T) - (O)$. But as we know the principal divisor must sum up to $O$ and so $T = O$.

(iv) Let $\sigma \in \text{Gal}_{\bar{K}/K}$. Take $f, g$ the functions as in the definition of Weil pairing for a point $T \in E[m]$. Then $\sigma(f)$ and $\sigma(g)$ will be the corresponding functions for $\sigma(T)$. Then

$$e_m(\sigma(S), \sigma(T)) = \frac{\sigma(g)(\sigma(X) + \sigma(S))}{\sigma(g)(\sigma(X))} = \sigma\left(\frac{g(X+S)}{g(X)}\right) = \sigma(e_m(S,T)).$$

(v) Taking $f$ and $g$ as usual then

$$\text{div}(f^{m'}) = mm'(T) - mm'(O)$$

and

$$(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}.$$

Thus, the corresponding functions for $T$ and $mm'$ are $f^{m'}$ and $g \circ [m']$. Then directly from the definition of $e_{mm'}$ and $e_m$ we have

$$e_{mm'}(S,T) = \frac{g \circ [m'](X+S)}{g \circ [m'](X)} = \frac{g(Y + [m']S)}{g(Y)} = e_m([m']S, T).$$

□

**Corollary 29.32.** *There exists $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive $m$-th root of unity. In particular, if $E[m] \subset E(K)$ then $\mu_m \subset K^*$.*

*Proof.* Let $d$ be an integer $d|m$ such that $\mu_d$ is the image of $e_m(S,T), S, T \in E[m]$. Then

$$1 = e_m(S,T)^d = e_m([d]S, T) \ \forall S, T \in E[m].$$

By non-degeneracy of $e_m$ we conclude that $[d]S = O$. Since $S$ is arbitrary, we must have $d = m$. Thus if $E[m] \subset E(K)$, by Galois invariance of $e_m$ we conclude that $e_m(S,T) \in K^*$ for all $S, T \in E[m]$ and therefore, $K$ contains a primitive $m$-th root of unity. □

The next proposition relates the isogenies and Weil pairing.

**Proposition 29.33.** *Let $\phi : E \to F$ be a non-trivial isogeny. Then for all $P \in E[m]$ and $T \in F[m]$,*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

*Proof.* Take $f, g$ be the corresponding functions for $T$. Then

$$e_m(\phi(S), T) = \frac{g(X + \phi(S))}{g(X)}.$$

Pick a function $h \in \bar{K}(E)$ satisfying

$$\text{div}(h) = \phi^*((T)) - \phi^*((O)) - (\hat{\phi}T) + (O).$$

Such $h$ exists because this is a degree zero divisor and the above sums up to $O$. To see this, the sum is actually $|\deg\phi|Q$ where $\phi(Q)=T$, where the sum is independent of which $Q$ we pick. Composing the image of this under $\phi$ we get $|\deg\phi|T$ and since the sum is independent of $Q$ so this is exactly $\hat{\phi}T$.

Now we observe that

$$\mathrm{div}\left(\frac{f\circ\phi}{h^m}\right)=\phi^*\mathrm{div}(f)-m\mathrm{div}(h)=m(\hat{\phi}T)-m(O).$$

and

$$\left(\frac{g\circ\phi}{h\circ[m]}\right)^m=\frac{f\circ[m]\circ\phi}{(h\circ[m])^m}=\left(\frac{f\circ\phi}{h^m}\right)\circ[m].$$

Then by definition,

$$\begin{aligned} e_m(S,\hat{\phi}T) &= \frac{(g\circ\phi/h\circ[m])(X+S)}{(g\circ\phi/h\circ[m])(X)} \\ &= \frac{g(\phi X+\phi S)}{g(\phi X)}\frac{h([m]X)}{h([m]X+[m]S)} \\ &= e_m(\phi(S),T) \end{aligned}$$

because $[m]S=O$. □

Recall from the last subsection, we constructed the Tate module by taking the inverse limit of the $p^n$-th torsion. Now we are going to extend the Weil pairing for $p^n$ torsion to a pairing on the Tate module. We simply do this by taking the inverse limit of the system

$$e_{p^n}: E[p^n]\times E[p^n]\to\mu_{p^n}$$

together with the projection maps

$$E[p^{n+1}]\to E[p^n], Q\mapsto[p]Q \text{ and } \mu_{p^{n+1}}\to\mu_{p^n}, \zeta\mapsto\zeta^p.$$

The resulting pairing is denoted by

$$e: T_p(E)\times T_p(E)\to T_p(\mu).$$

To see the pairings $e_{p^n}$ are compatible with taking the inverse limits, we must show that

$$e_{p^{n+1}}(S,T)^p=e_{p^n}([p]S,[p]T),\ \forall S,T\in E[p^{n+1}].$$

But this is clear by using (i) and (v) of Proposition 29.31. Further it inherits all the properties described in Proposition 29.31 and Proposition 29.33.

Recall the representation

$$\mathrm{End}(E)\to\mathrm{End}(T_p(E)),\ \phi\mapsto\phi_p.$$

Let $tr(\phi_p)$ and $\det(\phi_p)$ be the trace and determinant of the linear map $\phi_p$. Then we have

**Proposition 29.34.** *Let $\phi\in End(E)$ and let $\phi_p: T_p(E)\to T_p(E)$ be the map that $\phi$ induces on the Tate moduel. Then*

$$\det(\phi_p)=\deg(\phi)\quad and\quad tr(\phi_p)=1+\deg(\phi)-\deg(1-\phi).$$

*In particular,* $\deg(\phi_p)$ *and* $tr(\phi_p)$ *are in* $\mathbb{Z}$ *and are independent of* $p$.

*Proof.* Pick a $\mathbb{Z}_p$-basis $\{v_1, v_2\}$ for $T_p(E)$ and interpret the map $\phi_p$ in terms of the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$\begin{aligned} e(v_1, v_2)^{\deg \phi} &= e([\deg \phi]v_1, v_2) = e(\hat{\phi}_p \phi_p v_1, v_2) \\ &= e(\phi_p v_1, \phi_p v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) = e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det \phi_p} \end{aligned}$$

using bilinearity and compatibility.

Since $e$ is non-degenerate so we conclude that $\deg \phi = \det \phi_p$. Finally, for any $2 \times 2$ matrix, we can write the trace in terms of the determinant, given by

$$tr(A) = 1 + \det(A) - \det(1 - A).$$

□

## 29.6 Exercises

1. Let $E/\bar{K}$ be a smooth curve, and let $H$ be a finite group of isomorphism from $C$ to itself. Recall that an element $\alpha \in H$ acts on the function field by

$$\alpha^* : \bar{K}(C) \to \bar{K}(C),\ \alpha^*(f) = f \circ \alpha.$$

   (i) Prove that there exist a unique smooth curve $C'/\bar{K}$ and a finite separable morphism $\phi : C \to C'$ such that $\phi^* \bar{K}(C') = \bar{K}(C)^H$.

   (ii) Let $P \in C$. Prove that the ramification index

$$e_\phi(P) = |\{\alpha \in H : \alpha P = P\}|.$$

   (iii) Prove that $\phi$ is unramified if and only if every non-trivial element of $H$ has no fixed points.

   (iv) Express the genus of $C'$ in terms of the genus of $C$, $|H|$ and the number of fixed points of elements of $H$.

   (v) Suppose that $C$ is defined over $K$ and that $H$ is $G_{\bar{K}/K}$-invariant which means that for all $\alpha \in H$, we have $\sigma(\alpha) \in H$. Prove that it is possible to find $C'$ and $\phi$ in (i) such that $C'$ and $\phi$ are defined over $K$. Prove further that $C'$ is unique up to isomorphism over $K$.

   This is a generalization of Theorem 29.12.

2. Prove directly that the natural map

$$\mathrm{Hom}(E, F) \to \mathrm{Hom}(T_p(E), T_p(F))$$

   is injective. (Hint: If $\phi : E \to F$ satisfies $\phi_p = 0$ then $E[p^n] \subset \ker \phi$ for all $n \geq 1$.)

3. This is a definition of the generalized Weil pairing. Let $E/K$ and $F/K$ be elliptic curves, and let $\phi : E \to F$ be an isogeny of degree $m$ defined over $K$.

(i) Construct a pairing

$$e_\phi : \ker \phi \times \ker \hat{\phi} \to \mu_m$$

in a analogous way to the construction of the Weil pairing.

(ii) Prove that $e_\phi$ is bilinear, non-degenerate, and Galois invariant.

(iii) Prove that $e_\phi$ is compatible in the sense that if $\psi : E_2 \to E_3$ is another isogeny, then

$$e_{\psi\circ\phi}(P, Q) = e_\psi(\phi P, Q) \ \forall P \in \ker(\psi \circ \phi) \text{ and } Q \in \ker \hat{\psi}.$$

4. This is an alternative definition of Weil pairing. Let $E$ be an elliptic curve. We define a pairing

$$e'_m : E[m] \times E[m] \to \mu_m$$

as follows: Let $P, Q \in E[m]$ and choose divisors $D_p$ and $D_Q$ in $\mathrm{Div}^0(E)$ that add to $P$ and $Q$ respectively. Assume further that $D_P$ and $D_Q$ are chosen with disjoint support (meaning they have disjoint points as components). Since $P$ and $Q$ have order $m$, there are functions $f_P, f_Q \in \bar{K}(E)$ such that

$$\mathrm{div}(f_P) = mD_P \text{ and } \mathrm{div}(f_Q) = mD_Q.$$

We define

$$e'_m = \frac{f_P(D_Q)}{f_Q(D_P)}$$

where for a divisor $D = \sum n_P(P)$, we write $f(D) = \prod_P f(P)^{n_P}$.

(i) Prove that this is a well-defined pairing in the sense that its value depends only on $P, Q$, independent the choice of $D_P, D_Q, f_P$ and $f_Q$. You may assume the Weil reciprocity, which says for any functions $f, g$ in the function field, we have

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

(ii) Prove that $e'_m(P, Q) \in \mu_m$.

(iii)* Prove that $1/e'_m$ is the same as $e_m$.

5. Let $E/K$ be an elliptic curve over $K$ with complex multiplication, which means that $\mathrm{End}_K(E)$ is strictly bigger than $\mathbb{Z}$. (Assuming $K$ is a number field) Prove that the action of $G_{\bar{K}/K}$ on the Tate module $T_p(E)$ is abelian. You may assume that when $E$ has complex multiplication, the endomorphism ring is an order in an imaginary quadratic field, i.e.

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = F, \quad \text{for some imaginary quadratic field } F.$$

6. Let $E$ be an elliptic curve $y^2 = x^3 + x$ with complex multiplication by $\mathbb{Z}[i]$. Let $m \geq 2$ be an integer and $T \in E[m]$ be a point of exact order $m$. Then prove $\{T, [i]T\}$ is a basis for $E[m]$ if $m \equiv 3 \pmod 4$ or $m$ is an odd prime, $K$ is a field with $i \notin K$ and $T \in E(K)$.

7. Let $\phi \in \mathrm{End}(E)$ be an endomorphism, and let

$$d = \deg \phi \text{ and } a = 1 + \deg \phi - \deg(1 - \phi).$$

(i) Prove that $\phi^2 - [a] \circ \phi + [d] = [0]$ in $\mathrm{End}(E)$.

(ii) Let $\alpha, \beta \in \mathbb{C}$ be the complex roots of the polynomial $t^2 - at + d$. Prove that

$$|\alpha| = |\beta| = \sqrt{d}.$$

Hint: Use the fact that $\deg([m] + [n] \circ \phi) \geq 0$ for all $m, n \in \mathbb{Z}$.

(iii) Prove that $\deg(1 - \phi^n) = 1 + d^n - \alpha^n - \beta^n$ for all $n \geq 1$ and deduce that

$$|\deg(1 - \phi^n) - 1 - d^n| \leq 2d^{n/2}.$$

(iv) Prove that

$$\exp\left(\sum_{n=1}^{\infty} \frac{\deg(1 - \phi^n)}{n} X^n\right) = \frac{1 - aX + dX^2}{(1 - X)(1 - dX)},$$

where the power series converges for $|X| < d^{-1}$.

## 29.7 Hint and Solutions

1. (i) This is identical to the proof of Theorem 29.12 because the transcendence degree of $\bar{K}(C)^H$ over $\bar{K}$ is one. Thus there is a unique curve $C'$ and a morphism

$$\phi : C \to C', \ \phi^* \bar{K}(C') = \bar{K}(C)^H.$$

$\phi$ is separable as we assume $K$ is a number field in this section (the general case is still true if we follow the proof of Theorem 29.12).

(ii) Firstly we check that each element in the Galois group acts on the fibre. Let $\alpha \in H$ and let $P \in \phi^{-1}(Q)$ for some $Q$ in $C'$. Then for all $f \in \bar{K}(C')$,

$$f\phi(\alpha(\phi^{-1}(Q))) = \alpha^*(\phi^* f)(\phi^{-1}(Q)) = \phi^* f(\phi^{-1}(Q)) = f(Q).$$

This implies that $\phi(\alpha(\phi^{-1}(Q))) = Q$ and so $\alpha(\phi^{-1}(Q))$ is also a preimage of $Q$ and this completes the proof of our assertion.

Next we show that action is transitive. This follows from the fact that each point corresponds to a maximal (hence prime) ideal and since the Galois group acts transitively on the prime ideals above so we conclude that the action is transitive.

Now given any $P_1, P_2$ with $\phi(P_1) = \phi(P_2)$ then there exists some $\alpha \in H$ such that $\alpha(P_1) = P_2$. Since isomorphism has trivial ramification index everywhere we have

$$e_\phi(P_1) = e_{\phi \circ \alpha}(P_1) = e_\phi(\alpha(P_1)) e_\alpha(P_1) = e_\phi(P_2).$$

This shows every point has the same ramification.

Finally we used the formula $\deg \phi = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$, $\deg \phi = |H|$ and transitivity of the action so that $|\deg^{-1}(Q)| = |\mathrm{Orbit}(P) : P \in \phi^{-1}(Q)|$, we conclude that

$$e_\phi(P) = |\{\alpha \in H : \alpha P = P\}|$$

by Orbit-Stablizer theorem.

(iii) Immediate from (ii).

(iv) By Riemann-Hurwitz we have

$$2Genus(C) - 2 = (\deg \phi)(2Genus(C') - 2) + \sum_{P \in C}(e_\phi(P) - 1).$$

Replace $\deg \phi$ by $|H|$ and $e_\phi(P)$ by the size of elements which fix $P$ we can write genus of $C'$ in terms of the required terms.

(v) Let $P \in C(K)$ and $\alpha \in H$ so

$$\sigma(\alpha(P)) = \sigma(\alpha)(\sigma(P)) = \alpha(P)$$

because $\sigma(\alpha) = \alpha$ so this shows that each

$$\alpha^* : K(C) \to K(C)$$

is well-defined so we can replace $\bar{K}$ by $K$ at each stage of the proof in (i) and so we can find $C'$ and $\phi$ defined over $K$. $C'$ is unique up to isomorphism because the function field of $C'$ is determined.

2. Following the hint, let $\phi_p = 0$ then $E[p^n] \in \ker \phi$ for all $n \geq 1$. Then by taking the dual isogeny, we see that the kernel of $[m] = \hat{\phi}\phi$ contains $E[p^n]$ for all $n \geq 1$. Then clearly this can only happen when $m = 0$.

3. (i) Let $S \in \ker \phi$ and $T \in \ker \hat{\phi}$. Pick a function $f \in \bar{K}(F)$ satisfying

$$\mathrm{div}(f) = m(T) - m(O).$$

Let $T' \in E$ such that $\phi T' = T$. Then there is a similarly a function $g \in \bar{K}(F)$ such that

$$\mathrm{div}(g) = \phi^*(T) - \phi^*(O) = \sum_{R \in \ker \phi} (T' + R) - (R).$$

Then we can assume that $f \circ \phi = g^m$ because they have the same divisor. Now if $S \in \ker \phi$ then we have

$$g(X + S)^m = f(\phi X + \phi S) = f(\phi X) = g(X)^m.$$

Thus, we define

$$e_\phi(S, T) = \frac{g(X + S)}{g(X)}.$$

(ii) It is easy to check that

$$e_\phi(S_1 + S_2, T) = \frac{g(X + S_1 + S_2)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} = e_m(S_1, T) e_m(S_2, T).$$

To check it is linear in second component, let $T_3 = T_1 + T_2$ and let $f_1, f_2, f_3, g_1, g_2, g_3$ be the corresponding functions. Let

$$\mathrm{div}(h) = (T_3) - (T_1) - (T_2) + (O).$$

Then

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = m\mathrm{div}(h),$$

so $f_3 = cf_1f_2h^m$ for some constant $c$ and thus by using the fact $f_i \circ \phi = g_i^m$ we conclude that

$$g_3 = c'g_1g_2(h \circ \phi).$$

Therefore,

$$e_\phi(S, T_3) = \frac{g_1(X+S)g_2(X+S)h(\phi X + \phi S)}{g_1(X)g_2(X)h(\phi X)} = e_m(S, T_1)e_m(S, T_2).$$

This is essentially an identical proof to the original one.

Similarly, to prove this is non-degenerate. We just repeat the original proof except that we take $T'$ with $\phi T' = T$, instead of $[m]T' = T$ in the original proof. Finally it is clear that it is Galois invariant.

(iii) Let $\mathrm{div}(f) = m(T) - m(O)$ and $f \circ \psi = g^m$ where $m = \deg \psi$. Then

$$e_\psi(\phi P, Q) = \frac{g(\phi X + \phi P)}{g(\phi X)}.$$

Let $n$ be the degree of $\psi$ and pick a function $h$ satisfying

$$\mathrm{div}(h) = mn(Q) - mn(O).$$

Then up to a constant we have $f^n = h$ and so

$$h \circ \psi \circ \phi = f^n \circ \psi \circ \phi = g^{mn} \circ \phi.$$

So the corresponding $g$ function for $\psi \circ \phi$ is $g \circ \phi$. Thus,

$$e_{\psi\circ\phi}(P, Q) = \frac{g(\phi X + \phi P)}{g(\phi X)} = e_\psi(\phi P, Q).$$

4. (i) If we replace $f_P$ by $cf_P$, where $c$ is a constant then clearly $e'_m$ is unchanged because essentially

$$cf_P(D_Q) = c^{\deg D_Q} f_P(D_Q) = f_P(D_Q)$$

because $D_Q$ is a degree zero divisor. Similar argument applies to $f_Q$. Now if we replace $D_Q$ by another $D'_Q$ which still sums up to $Q$, so we must have

$$D'_Q = D_Q + \mathrm{div}(h)$$

for some principal divisor $\mathrm{div}(h)$. Then

$$\mathrm{div}(f'_Q) = mD_Q + m\mathrm{div}h$$

and since we showed that the constant of $f_Q$ does not change the result so that we may assume that

$$f'_Q = f_Q h^m.$$

Now the the pairing is

$$\frac{f_P(D'_Q)}{f'_Q(D_P)} = \frac{f_P(D_Q)f_P(\mathrm{div}h)}{f_Q(D_P)h^m(D_P)}.$$

To prove this is unchanged it suffices to show that

$$\frac{f_P(\mathrm{div}h)}{h^m(D_P)} = 1.$$

But this is clear by using Weil reciprocity and the fact $h^m(D_P) = h(mD_P)$.

(ii) This is again by Weil reciprocity as follows:

$$e'^m_m = \frac{f_P^m(D_Q)}{f_Q^m(D_P)} = \frac{f_P(mD_Q)}{f_Q(mD_P)} = 1.$$

(iii) Fix $S, T \in E[m]$ and $f, g$ be the usual notation as in the construction of $e_m(S,T)$. The key idea to is construct a divisor of the form

$$\mathrm{div}h = D = (m-1)(S'+X) + (S'-S+X) - m(X)$$

where $[m]S' = S$, $X$ is a point such that $D$ and $\mathrm{div}(g)$ have different support. Also such $h$ exists because the $D$ has degree 0 and $D$ sums up to $O$.
We will apply Weil reciprocity to compare $g(\mathrm{div}h)$ and $h(\mathrm{div}g)$. Now

$$\begin{aligned} g(\mathrm{div}h) &= \frac{g(S'+X)^{m-1}g(S'-S+X)}{g(X)^m} = \frac{g(S'+X)^m}{g(X)^m}\frac{g(S'-S+X)}{g(S'+X)} \\ &= \frac{f([m]S'+[m]X)}{f([m]X)}\frac{g((S'+X)-S)}{g(S'+X)} \\ &= \frac{f(S+[m]X)}{f([m]X)}\frac{1}{e_m(S,T)} \end{aligned}$$

where we use $g^m = f \circ [m]$.
Now we have

$$h(\mathrm{div}g) = \prod_{R\in E[m]} \frac{h(T'+R)}{h(R)}, \text{ since } \mathrm{div}(g) = \sum_{R\in E[m]} (T'+R) - (R)$$

where $[m]T' = T$. Then define a function $H$ such that

$$H(P) = \prod_{R\in E[m]} h(P+R) = \prod_{R\in E[m]} h \circ \tau_R(P).$$

Then

$$\begin{aligned} \mathrm{div}(H) &= \sum_{R\in E[m]} ((m-1)(S'+X-R) + (S'-S+X-R) - m(X-R)) \\ &= \sum_{R\in E[m]} ((m-1)(S'+X+R) + (S'+X+R) - m(X+R)) \\ &= m\sum_{R\in E[m]} (S'+X+R) - (X+R) \\ &= m(\mathrm{div}g_S \circ \tau_{-X}) = \mathrm{div}g_S^m \circ \tau_{-X} \end{aligned}$$

where in the third line we use the fact that $S \in E[m]$ so summing over $S+R, R \in E[m]$ is the same as summing over $R, R \in E[m]$ and in the last line we write $g_S$ the corresponding pull back function for $f_S$ and $f_S$ is the one with divisor $(S) - (O)$.
Hence up to a constant we have

$$H = g_S^m \circ \tau_{-X} = f_S \circ [m] \circ \tau_{-X}.$$

Evaluating at $T'$ where $[m]T' = T$ we have

$$\prod_{R\in E[m]} h(T'+R) = H(T') = f_S(T - [m]X).$$

Finally, evaluating at $O$ we have

$$\prod_{R\in E[m]} h(R) = H(O) = f_S(-[m]X).$$

Combine the above two we conclude that

$$h(\mathrm{div} g) = \prod_{R\in E[m]} \frac{h(T'+R)}{h(R)} = \frac{f_S(T-[m]X)}{f_S(-[m]X)}.$$

Now Weil reciprocity implies that

$$\frac{f(S+[m]X)}{f([m]X)}\frac{1}{e_m(S,T)} = \frac{f_S(T-[m]X)}{f_S(-[m]X)}.$$

Thus,

$$e_m(S,T) = \frac{f_S(-[m]X)}{f_S(T-[m]X)}\frac{f(S+[m]X)}{f([m]X)} = \frac{f'_S(O)}{f'_S(T)}\frac{f(S+[m]X}{f([m]X)}$$

where $f'_S(P) = f_S(P-[m]X)$. Finally, we pick $D_S = (S+[m]X)-([m]X)$ and $D_T = (T)-(O)$. Then $\mathrm{div}(f) = (T)-(O)$ and $\mathrm{div}(f'_S) = (S+[m]X)-[m]X$. So by definition the last term in the above equation is $1/e'_m(S,T)$.

5. By definition the elements in $\mathrm{End}_K(E)$ commute with the action of $G_{\bar{K}/K}$ on $T_p(E)$. To prove the action of $G_{\bar{K}/K}$ on $T_p(E)$ is abelian, it is equivalent to prove that the image of $G_{\bar{K}/K}$ under $p$-adic representation $\rho_p$ is abelian. Let

$$V_p = T_p(E)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p.$$

Then $V_p$ is a two-dimensional $\mathbb{Q}_p$ vector space. Let $E$ has complex multiplication by a quadratic field $F$, and let $F_p = F\otimes_{\mathbb{Q}}\mathbb{Q}_p$. This is also a two-dimensional vector space over $\mathbb{Q}_p$ and since $V_p$ is contained in $F_p$, we conclude that $V_p$ has dimension one over $F_p$ and clearly it is free. Since the action of Galois commute with the endomorphism ring so the action of Galois is $F_p$ linear on $V_p$.

Now for each Galois element, we have an induced $F_p$-linear map between $V_p$ and itself, with rank 1 over $F_p$ so it is given by a $1\times 1$ matrix with entries in $F_p$. Since the collection (the group) of $1\times 1$ matrix group is always abelian so the result follows.

6. Since $[m][i]T = [i][m]T = O$ so $[i]T$ is also an element of order $m$. Further, if $[a][i][T] = O$ for some integer $a$ then $[i][a][T] = O$ and so $[a][T] = O$ because $[i]$ is an isomorphism. Thus $[i]T$ has exact order $m$.

Firstly let $m\equiv 3 \bmod 4$. Suppose we have some integer $a$ such that $[a]T = [i]T$ then

$$([a^2+1])T = ([a]+[i])([a]-[i])T = ([a]+[i])O = O.$$

Thus $m|a^2+1$ and so $a^2\equiv -1 \bmod m$ so $a^2\equiv -1 \bmod p$ for all prime $p|m$. However, as $m\equiv 3 \bmod 4$ there must exist $p|m$ with $p\equiv 3 \bmod 4$. Then $a^2\equiv -1 \bmod p$, which is a contradiction because $-1$ is not a square mod $p$ when $p\equiv 3 \bmod 4$.

Then we assume $m$ is a prime, $K$ is a field with $i\notin K$ and $T\in E(K)$. Recall that for each $a$ the coordinate of $[a]T$ can be written in terms of the coordinate of $T$. So the fact $E(K)[m]$ is non-trivial implies that $E(K)$ contains a cyclic subgroup of order $m$ because $m$ is prime. If $T\in K$, then $[i]T\notin K$ because $i\notin K$ and hence they must be independent, since each element in the subgroup generated by $T$ will also be in $K$.

7. (i) Recall that for each $p$, we have

$$\det(\phi_p) = \deg(\phi), tr(\phi_p) = 1 + \deg(\phi) - \deg(1-\phi)$$

so that for each $p$,

$$\phi_p^2 - [a] \circ \phi_p + [d] = \phi_p^2 - tr(\phi_p) \circ \phi_p + \det(\phi_p) = 0$$

where the second equality holds for any $2 \times 2$ matrix.
Recall from Theorem 29.26 that the map $\psi \to \psi_p$ is an injection from $\mathrm{End}(E) \otimes \mathbb{Z}_p \to \mathrm{End}(T_p(E))$. Thus, this implies that for each $p$, the image of the map

$$\phi^2 - [a] \circ \phi + [d]$$

in $\mathrm{End}(E) \otimes \mathbb{Z}_p$ is trivial and hence itself must be trivial.

(ii) We should check $a^2 - 4d \leq 0$ then it is direct calculation from $|\alpha| = |\beta|$ and $\alpha\beta = d$. Consider the map $[-a] + [2]\phi$. For any $p$, we have

$$\deg([-a] + [2]\phi) = \det([-a] + [2]\phi_p).$$

Now pick a basis for $\phi_p$ or for simplicity we may assume it is diagonal because determinant is invariant under a change of basis. Let $\phi_p$ have diagonal entries $u, v$. Then

$$\det([-1] + 2\phi_p) = (-a)^2 - 2(tr(\phi_p))a + 4uv = -a^2 + 4d$$

using $tr(\phi_p) = a$ and $uv = \det(\phi_p) = d$. Since the degree must be non-negative, this shows that $4d - a^2 \geq 0$ and hence completes the proof.

(iii) By Theorem 29.34, for any $p$,

$$\deg(1 - \phi^n) = 1 + \deg(\phi^n) - tr(\phi_p^n) = 1 + d^n - tr(\phi_p^n).$$

Since the trace form is independent of the choice of basis we may assume the matrix is diagonal with entries $\alpha$ and $\beta$ and hence they satisfy the equation in (ii). Further, $tr(\phi_p) = \alpha + \beta$ and so $tr(\phi_p^n) = \alpha^n + \beta^n$. This completes the first part.
The term on the left hand side is essentially $|\alpha^n + \beta^n|$ and the inequality follows from (ii) and triangle inequality.

(iv) Recall the identity

$$\sum_{n=1}^{\infty} \frac{T^n}{n} = -\log(1-T)$$

which converges for all $|T| < 1$. Thus,

$$\exp\left(\sum_{n=1}^{\infty} \frac{X^n}{n}\right) = \frac{1}{1-X}, \exp\left(\sum_{n=1}^{\infty} \frac{d^n X^n}{n}\right) = \frac{1}{1-dX}$$

converging for $|X| < d^{-1}$ and

$$\exp\left(\sum_{n=1}^{\infty} \frac{\alpha^n X^n}{n}\right) = \frac{1}{1-\alpha X}, \exp\left(\sum_{n=1}^{\infty} \frac{\beta^n X^n}{n}\right) = \frac{1}{1-\beta X}$$

converging for $|X| < \alpha^{-1}, \beta^{-1}$.
Combine these together and $(1-\alpha X)(1-\beta X) = 1 - aX + dX^2$ and the fact $|\alpha| = |\beta| = \sqrt{d}$, the result follows.

# 30 Computation of Mordell-Weil Group

In this section, we will explain the general (possible) procedure on computing the Mordell-Weil group. We have seen one of the method before, which we called 2-descent. We will explain the general descent procedure systematically. Further, we will introduce the Selmer group and the Tate-Shafarevich group which are closely related to the computation and briefly introduce the idea of **visibility**, which gives a suitable motivation for what my own research is doing. A good reference is Silverman's book of Arithmetic of Elliptic Curves, as well as several papers written by my supervisor, Dr.T.A.Fisher (available on his webpage).

## 30.1 Cohomology Group

In this subsection we will briefly introduce the basic concept and theorems of group cohomology. We begin the cohomology of finite groups.

**Definition 30.1.** *Let $G$ be a finite group. We say $M$ is a $G$-module if $M$ is an abelian group together with an action of $G$ on $M$. Define*

$$H^0(G,M) = M^G = \{m \in M : \sigma m = m \ \forall \sigma \in G\}.$$

**Example 30.2.** *Let $L/K$ be a finite Galois extension and $G = Gal(L/K)$. Let $E/K$ be an elliptic curve defined over $K$ and let $M = E(L)$ be the group of points of $E$ in $L$. Then $M$ is a $G$ module with the natural action induced by action of Galois. In particular,*

$$H^0(G, E(L)) = M^G = E(K).$$

**Definition 30.3.** *A map $f : G \to M$ is said to be a* **crossed homomorphism** *if*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

*It is clear that*

$$f(1) = f(1 \cdot 1) = f(1) + f(1) \Rightarrow f(1) = 0.$$

*A crossed homomorphism $f$ is said to be* **principal** *if it has the form*

$$f(\sigma) = \sigma m - m, \sigma \in G$$

*for some $m \in M$. The sum and difference of crossed homomorphism is again a crossed homomorphism and so the collection of crossed homomorphism with addition is a group. Similarly, since the sum and difference of principal crossed homomorphism is again principal, so we can define the following:*

$$H^1(G,M) = \frac{\{crossed\ homomorphism\}}{\{principal\ crossed\ homomorphism\}}.$$

*There are also cohomology groups $H^n(G,M)$ for $n \geq 2$ but for the purpose of this section we only need $H^0$ and $H^1$.*

*For non-abelian group (non-abelian cohomology) any two elements lie in the same class if they satisfy the following relation*

$$m\phi_\sigma = \psi_\sigma \sigma(m)$$

*for some $m \in M$.*

**Proposition 30.4.** *Let $L$ be a finite Galois extension of $K$ with Galois group $G$, then $H^1(G, L^*) = 0$, i.e., every crossed homomorphism $G \to L^*$ is principal. This is sometimes referred as Hilbert 90 for cohomology group.*

*Proof.* Take any crossed homomorphism $f : G \to L^*$ so we have

$$f(\sigma\tau) = f(\sigma)\sigma f(\tau), \forall \sigma, \tau \in G.$$

Recall Dedekind Theorem (Theorem 12.26) says that the elements in Galois group are linearly independent and since $f(\tau) \in L^*$ is non-zero so the map $\sum_{\tau \in G} f(\tau)\tau$ is non-zero. Thus there exists $\alpha \in L$ such that

$$\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0.$$

Now for all $\sigma \in G$ we have

$$\begin{aligned} \sigma\beta &= \sum_{\tau \in G} \sigma f(\tau)\sigma\tau(\alpha) \\ &= \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\alpha) \\ &= \sum_{\delta \in G} f(\sigma)^{-1} f(\delta)\delta(\alpha) \\ &= f(\sigma)^{-1}\beta. \end{aligned}$$

Since $\sigma\beta$ is non-zero so we have $f(\sigma) = \beta/\sigma\beta = \sigma(\beta^{-1})/\beta^{-1}$. □

**Corollary 30.5.** *With same notation as above, a point $P = [x_0 : x_1 : \ldots : x_n] \in \mathbb{P}^n(L)$ is fixed by $G$ if and only if it is represented by an $n+1$-tuple in $K$.*

*Proof.* If every coordinate is in $K$ then it is clearly fixed by $G$. Now let $\sigma P = P$ for all $\sigma \in G$. Then

$$\sigma[x_0 : \ldots : x_n] = c(\sigma)[x_0 : \ldots : x_n]$$

for some $c(\sigma) \in L^*$. It is easy to check that the map $\sigma \mapsto c(\sigma)$ is a crossed homomorphism from $G$ to $L^*$ and so by previous proposition there exists $c \in L$ such that

$$c(\sigma) = \sigma(c)/c.$$

Thus the above equation implies that

$$\sigma[cx_0 : \ldots : cx_n] = [cx_0 : \ldots : cx_n]$$

and so the point $P = [x_0 : \ldots : x_n] = [cx_0 : \ldots : cx_n]$ can be represented by $n+1$-tuple in $K$. □

**Proposition 30.6.** *Let $G$ be a finite group and given any short exact sequence of $G$-module*

$$0 \to M \to N \to P \to 0$$

*there exists a canonical long exact sequence*

$$0 \to H^0(G, M) \to H^0(G, N) \to H^0(G, P) \to H^1(G, M) \to H^1(G, N) \to H^1(G, P)$$

*where we call $\delta : H^0(G, P) \to H^1(G, M)$ above the* **boundary map**.

*Proof.* It is essentially just diagram chasing and we give the construction of the boundary map here. Let $p \in H^0(G, P)$, by short exactness, we have $n \in N$ which maps to $p$. Since $\sigma P = P$, so if we call $f : N \to P$ the map in the short exact sequence then $\sigma n - n$ is in the kernel of $f$ and hence is in the image of $M \to N$. Since $M \to N$ is injective so there is a unique $m \in M$ corresponding to this point.

The map $\sigma \mapsto m$ where $m$ corresponds to $\sigma n - n$ is a crossed homomorphism and define $\delta(p)$ to be the class of this crossed homomorphism. Then one checks this is well-defined in the sense that if we pick another $n'$ in the preimage of $p$, and the class of $\sigma \mapsto m'$ where $m'$ corresponds to $\sigma n' - n'$ differs the above by a crossed homomorphism $\sigma \mapsto m''$ where $m''$ corresponds to $\sigma(n - n') - (n - n')$. But $n - n'$ maps to 0 in $P$ so it is in the image of $M \to N$ and by injectivity of $M \to N$ we conclude that this map is principal. Hence the two crossed homomorphism lie in the same class. □

**Definition 30.7.** *The restriction map is defined as follows. Let $H$ be a subgroup of $G$. The restriction map $f \to f|_H$ defines a homomorphism*

$$Res : H^1(G, M) \to H^1(H, M).$$

*There is a* **corestriction map** *(which we are not going to prove)*

$$Cor : H^1(H, M) \to H^1(G, M)$$

*such that $Cor \circ Res = m$ where $m$ is the index $[G : H]$.*

**Proposition 30.8.** *If $G$ has order $m$ then $mH^1(G, M) = 0$.*

*Proof.* Apply the property of corestriction map above with $H = 1$. □

**Definition 30.9.** *We define the* **inflation** *map as follows. Let $H$ be a normal subgroup of $G$ then $M^H$ is a $G/H$-module. Each crossed homomorphism $f : G/H \to M^H$ extends to a crossed homomorphism $g : G \to M$ in the sense that for each $\sigma \in G$, reduce $\sigma$ to $G/H$ and take the image of $\sigma$ under $f$ then use the inclusion $M^H \hookrightarrow M$. Thus we obtain a map*

$$Inf : H^1(G/H, M^H) \to H^1(G, M),$$

*and a short exact sequence*

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)$$

*where the maps above are given by the inflation map and restriction map respectively.*

Now we extend the concept for $G$ an infinite Galois group. Let $K$ be a perfect field. The absolute Galois group $G = \mathrm{Gal}(\bar{K}/K)$ has a natural topology where the open subgroups are exactly those which fix some finite extensions of $K$. Note that $G$ is a compact group and so any open subgroup has finite index. The usual fundamental theorem of Galois extends in the sense that any intermediate field corresponds to a closed subgroup of $G$. Now let $M$ be a $G$-module.

**Definition 30.10.** *We say $M$ is discrete if the action of Galois is continuous with respect to the natural topology described above. Equivalently,*

$$M = \bigcup_{H \, open} M^H.$$

*In other words, every element of $M$ is fixed by the subgroup of $G$ fixing some finite extension of $K$.*

*When $M$ is discrete, a crossed homomorphism $f$ is continuous if and only if $f$ is constant on the cosets of some some open normal subgroup $H$ of $G$, so that $f$ arises by inflation from a crossed homomorphism $G/H \to M^H$. Thus, every principal crossed homomorphism is continuous because every element of $M$ is fixed by some open normal subgroup of $G$.*

*Finally, for $M$ discrete we define $H^1(G, M)$ to be the group of continuous crossed homomorphisms $f : G \to M$ modulo the subgroup of principal crossed homomorphisms. In other words,*

$$H^1(G, M) = \lim_{\to H} H^1(G/H, H^M)$$

*where $H$ runs through the open normal subgroups of $G$. This means that $H^1(G, M)$ is the union of the images of the inflation maps.*

**Proposition 30.11.** *For $G$ infinite Galois group and $M$ discrete, $H^1(G, M)$ is torsion.*

*Proof.* $G/H$ is finite as $H$ is open normal. By definition each element $\alpha$ can be think of some element in $H^1(G/H, M^H)$ and this is torsion by Proposition 30.8. □

We give some examples.

**Example 30.12.** *(i) By Hilbert 90 (Proposition 30.4) we conclude that*

$$H^1(G, \bar{K}^*) = \lim_{\to H}(G/H, (K^*)^H) = \lim_{\to L}(Gal(L/K), L^*) = 0.$$

*(ii) Take the long exact sequence of cohomology from*

$$1 \to \mu_n(\bar{K}) \to \bar{K}^* \to \bar{K}^* \to 1$$

*where the later map is given by $\alpha \mapsto \alpha^n$, we have a long exact sequence*

$$1 \to \mu_n(K) \to K^* \to K^* \to H^1(G, \mu_n(\bar{K})) \to 1$$

*because by (i) $H^1(G, \bar{K}^*)$ is trivial. Thus, we have*

$$H^1(G, \mu_n(\bar{K})) \cong K^*/(K^*)^n.$$

*(iii) When the action of $G$ is trivial, the group $H^1(G, M)$ becomes the set of continuous homomorphism $\alpha : G \to M$. Since $M$ is discrete, the kernel is open (also normal) so $\alpha$ induces an injective homomorphism $Gal(\bar{K}/L) \to M$.*

*(iv) Let $E/\mathbb{Q}$ be an elliptic curve. Pick an embedding $\mathbb{Q}_p \hookrightarrow \bar{\mathbb{Q}}_p$. The action of $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\bar{\mathbb{Q}}$ defines a homomorphism*

$$Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to Gal(\bar{\mathbb{Q}}/\mathbb{Q}).$$

*Hence a crossed homomorphism $Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to E(\bar{\mathbb{Q}})$ defines (by composition) a crossed homomorphism $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to E(\bar{\mathbb{Q}}_p)$. In this way, we obtain a homomorphism*

$$H^1(Gal(\bar{\mathbb{Q}}/\mathbb{Q}), E(\bar{\mathbb{Q}})) \to H^1(Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), E(\bar{\mathbb{Q}}_p)).$$

*which is independent of the choice of the embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$.*

## 30.2 Revisit of Two Descent

In this subsection we briefly recall the procedure of (general) 2-descent, in a more formal language. Write $G_{\bar{K}/K}$ for $\mathrm{Gal}(\bar{K}/K)$.

**Theorem 30.13.** *Assume $E[m] \subset E(K)$.*

*(i) There exists a bilinear pairing*

$$b : E(K)/mE(K) \times E[m] \to K^*/(K^*)^m$$

*satisfying*

$$e_m(\delta(P)(\sigma), T) = \delta_K(b(P, T))(\sigma) \ \forall \sigma \in G_{\bar{K}/K}$$

*where*

$$\delta_E : E(K)/mE(K) \to Hom(G_{\bar{K}/K}, E[m]), \delta_E(P)(\sigma) = \sigma(Q) - Q \text{ for any } [m]Q = P$$

*and*

$$\delta_K : K^*/(K^*)^m \to Hom(G_{\bar{K}/K}, \mu_m), \delta_K(a)(\sigma) = \sigma(\alpha)/\alpha \text{ for any } \alpha^m = a.$$

*One check $\delta_E$ is well-defined by a similar argument to Lemma 27.48, and $\delta_K$ is well-defined by using Hilbert 90.*

*(ii) The pairing in (i) is non-degenerate on the left.*

*(iii) Let $S \subset M_K$ be the union of the set of infinite places, the set of finite primes at which $E$ has bad reduction and the set of finite primes dividing $m$. Then the image of the pairing in (i) lies in the set*

$$K(S,m) = \{a \in K^*/(K^*)^m : ord_v(a) \equiv 0 \ (mod\ m)\ \forall v \notin S\}.$$

*(iv) The pairing (i) can be computed as follows. For each $T \in E[m]$ pick $f_T, g_T \in K(E)$ by*

$$divf_T = m(T) - m(O), f_T \circ [m] = g_T^m$$

*(as in the construction of the Weil pairing). Then for any point $P \neq T$,*

$$b(P,T) \equiv f_T(P)\ (mod (K^*)^m).$$

*For $P = T$ we can compute $b(T,T)$ using linearity. Let $Q \in E(K)$ be any point with $Q \neq T$ then $b(T,T) = f_T(T+Q)f_T(Q)^{-1}$.*

*Proof.* By Hilbert 90, the map $\delta_K$ is actually an isomorphism. Thus, we can define $b(P,T)$ by considering the preimage of $e_m(\delta_E(P)(\sigma), T)$ for each $\sigma \in G_{\bar{K}/K}$ and so the relation in (i) is automatic. Now the Weil-pairing is bilinear and so by how we define $b$ above $b$ is bilinear.

(ii) follows from the non-degeneracy of the Weil-pairing. Precisely, it means if $b(P,T) = 1$ for all $T \in E[m]$ then we have $P \in mE(K)$. But $b(P,T) = 1$ implies that

$$e_m(\sigma(Q) - Q, T) = 1\ \forall \sigma \in G_{\bar{K}/K}.$$

Then by non-degeneracy of the Weil pairing this shows that $\sigma(Q) - Q = O$ for all $\sigma$ and hence $Q \in E(K)$ and $P \in mE(K)$.

For any $v \notin S$, let $\delta_K(b(P,T))(\sigma) = \sigma(\alpha)/\alpha$ and then the image $a = \alpha^m$. Now for any $\alpha$ by definition (the relation of (i)) we have

$$e_m(\sigma(Q) - Q, T) = \sigma(\alpha)/\alpha.$$

Let $v \in S$ be a prime. Then since $\alpha^m = a$, the extension $K(\alpha)/K$ is unramified at $v$, if and only if $\text{ord}_v(a) \equiv 0 \pmod m$. We briefly explain how this works. One direction is clear, namely if the extension is unramified at $v$, then by transitivity of the action of Galois, $\alpha$ lies in some prime above $v$ if and only if it lies in all primes above $v$. This proves that the extended valuation of $v$ at $\alpha$ is an integer, and hence the valuation at $a$ is a multiple of $m$. Now conversely, if the valuation is a multiple of $m$, then localise at $v$ and pick a uniformliser $\pi$ of $v$ then

$$a = \pi^k u, k \geq m, u \text{ is a unit }.$$

Hence $K_v(\alpha) = K_v(\sqrt[m]{a}) = K_v(\sqrt[m]{u})$. By basic knowledge of local fields we know this is unramified. Thus, this shows that $a \in K(S,m)$.

Finally, for $P \neq T$, we compute the functions $f_T, g_T$ as in the theorem. Now since $f_T \circ [m] = g^m$, we have (by extend the function to $\bar{K}(E)$

$$f_T(P) = f_T([m]Q) = g_T^m(Q).$$

Further

$$\delta_K(g_T^m(Q))(\sigma) = \sigma(g_T(Q))/g_T(Q) = g_T(\sigma Q)/g_T(Q)$$

by definition of $Q$ and this is the same as $g_T(\sigma(Q) - Q + X)/g_T(X)$ by picking $X = Q$. This shows that $b(P,T)$ and $f_T(P)$ are the same for some choice of $g_T$ (remember when we construct $f_T$ there is a choice of constant $c$) and from the proof above we only care about $c^m$ (as we need $g^m$) so

$$b(P,T) \equiv f_T(P) \pmod{(K^*)^m}.$$

□

The proof of weak Mordell Weil theorem based on the following fact.

**Proposition 30.14.** *The set $K(S,m)$ is finite (where $S$ is the set introduced in the previous theorem)*

*Proof.* Let $R_S = \{a \in K : \mathrm{ord}_v(a) \geq 0 \text{ for all } v \notin S\}$ which is the $S$-integer in $T$. Consider the natural map

$$f : R_S^* \to K(S,m).$$

For each $a \in K^*$ considered as a lift of element in $K(S,m)$ (note we can assume $a$ has positive valuation by multiplying $a$ by suitable elements), the ideal $aR_s$ is an $m$-th power of some ideal in $R_S$. To see this, the prime ideal in $R_S$ corresponds to the prime ideal of $\mathcal{O}_K$ not in $S$ and for any $v \in S$, we have $vR_S = R_S$.

Let $I_1, \ldots, I_h$ be the representatives for the ideal class group of $K$. Note if $v \in S$ for all $v$ such that $\mathrm{ord}_v(I_j) \geq 1$ for some $j$, then $I_i R_S = R_S$ for all $i$ and so the ideal class group for $R_S$ will be trivial and thus $R_S$ is principal ideal domain. Thus, enlarge $S$ if necessary (and note that if $S \subset S'$ then $K(S,m) \subset K(S',m)$ and so we may prove $K(S',m)$ is finite), we may assume that $R_S$ is principal ideal domain. Then we can assume that $aR_s = b^m R_S$ for some $b \in R_S$ and so there exists a unit $u \in R_S^*$ such that

$$a = ub^m.$$

This shows that $a$ and $u$ have the same image in $K(S,m)$ and hence the map $f$ is surjective. Now the kernel contains $(R_S^*)^m$ and so

$$(R_S^*)/(R_S^*)^m \to K(S,m)$$

is surjective. Now the left hand side is finite by Dirichlet's unit theorem and hence the result follows. □

Now we study the special case when $m = 2$ (2-descent). Under the assumption $E[m] \subset E(K)$ we may assume

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3), e_i \in K.$$

Let $T_i = (e_i, 0)$ be the non-trivial 2-torsions. Let $T = (e, 0)$ be any of these points. We want to study the map $f_T$ in the previous theorem and hence compute the map $b$.

**Proposition 30.15** (2-descent)**.** *With the above setting, and let $S \subset M_K$ be a finite set of places of $K$ including all infinite (archimedean) places, all places dividing 2 and all places at which $E$ has bad reduction. Let $K(S,2)$ be defined as in Theorem 30.13 in the case $m = 2$. Then there is an injective homomorphism*

$$E(K)/2E(K) \to K(S,2) \times K(S,2)$$

*defined by*

$$P = (x,y) \mapsto = \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_1, e_2, \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right) & \text{if } x = e_1, \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right) & \text{if } x = e_2, \\ (1,1) & \text{if } P = O. \end{cases}$$

*Let $(b_1, b_2) \in K(S,2) \times K(S,2)$ be a point which is not the image of $O, T_1, T_2$. Then $(b_1, b_2)$ is the image of a point*

$$P = (x,y) \in E(K)/2E(K)$$

*if and only if the following equations*

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1,$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1,$$

*have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then we can take*

$$P = (x,y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

*Proof.* Consider if $T \neq T_1, T_2$ then $f_T = x - e$ because the divisor

$$\operatorname{div}(x - e) = 2(T) - 2(O)$$

and a direct calculation shows

$$x \circ [2] = \left( \frac{x^2 - 2ex - 2e^2 + 2(e_1 + e_2 + e_3)e - (e_1e_2 + e_1e_3 + e_2e_3)}{2y} \right)^2,$$

and so it satisfies both properties of $f_T$.

Now we consider the map $E(K)/2E(K) \to K(S,2) \times K(S,2)$ by

$$P \mapsto (b(P, T_1), b(P, T_2))$$

where $b$ is the pairing in Theorem 30.13 and we compute the pairing $b$ by computing $f_T$. So for $x \neq e_1, e_2$ the image is $(x - e_1, x - e_2)$ (remember in Theorem 30.13 we cannot use $f_T(P)$ to compute $b(P,T)$ when $P = T$). If $P = T_1$, i.e., $x = e_1$, we use linearity (as in the remark of Theorem 30.13(iv)) to compute

$$b(T_1, T_1) = b(T_1, T_1 + T_2)b(T_1, T_2)^{-1} = b(T_1, T_3)b(T_1, T_2)^{-1} = \frac{e_1 - e_3}{e_1 - e_2}$$

and similarly,

$$b(T_2, T_2) = \frac{e_2 - e_3}{e_2 - e_1}.$$

Finally, the image $b(O, T_i) = 1$ is clear. Therefore, since $b$ is left-non-degenerate, so the map

$$P \mapsto (b(P, T_1), b(P, T_2))$$

is injective and has the correct image stated in the theorem.

Now let $(b_1, b_2) \in K(S,2) \times K(S,2)$ which is not the image of $O, T_1, T_2$ and by above we have

$$b(P, T_1) = b_1, b(P, T_2) = b_2, P \neq O, T_1, T_2.$$

Let $P = (x, y)$. By definition of $K(S,2)$ such a point lies in the image if and only if there is a solution

$$(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$$

to the system of equations

$$y^2 = (x - e_1)(x - e_2)(x - e_3), b_1 z_1^2 = x - e_1, b_2 z_2^2 = x - e_2.$$

Define $z_3$ by the relation $y = b_1 b_2 z_1 z_2 z_3$ and thus the above is equivalent to

$$b_1 b_2 z_3^2 = x - e_3, b_1 z_1^2 = x - e_1, b_2 z_2^2 = x - e_2.$$

Eliminating $x$ we have

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1, b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1.$$

Finally, if such solution exists, we can recover the point $P$ by

$$x = b_1 z_1^2 + e_1, y = b_1 b_2 z_1 z_2 z_3.$$

This completes the final part of the proposition. □

Note that this is basically the same as what we did before, but in a different and probably more formal language.

## 30.3 Twisting

In this subsection we explain the basic theory of twists of curves. Intuitively, it gives a tool to measure the Galois conjugate of isomorphism between different curves.

**Definition 30.16.** *Let $C/K$ be a smooth projective curve. The isomorphism group of $C$ denoted by $Isom(C)$ is the group of $\bar{K}$-isomorphism from $C$ to itself. We denote the subgroup of $Isom(C)$ consisting of isomorphism defined over $K$ by $Isom_K(C)$.*

The reason we use the notation $\mathrm{Isom}(C)$ instead of $\mathrm{Aut}(C)$ is because for $C$ an elliptic curve, $\mathrm{Aut}(C)$ means the isomorphism which fixes the origin.

**Definition 30.17.** *A twist of $C/K$ is a smooth curve $C'/K$ which is isomorphic to $C$ over $\bar{K}$. For $C', C''$ twists of $C$, we say $C'$ is equivalent to $C''$ if $C'$ is isomorphic to $C''$ over $K$. The set of twists of $C/K$, quotient out by the equivalence is denoted by $Tiwst(C/K)$.*

Now we establish the relation between the twists and the group cohomology.

**Theorem 30.18.** *Let $C/K$ be a smooth projective curve. For each twist $C'/K$ of $C/K$, choose a $\bar{K}$-isomorphism $\phi : C \to C'$ and define a map $\xi_\sigma = \phi^{-1}\sigma(\phi) \in Isom(C)$ where the map $\sigma(\phi)$ is defined as $\sigma \circ \phi \circ \sigma^{-1}$. Then*

*(i) The map $\xi$ is a 1-cocycle, i.e.*

$$\xi_{\sigma\tau} = \xi_\sigma \sigma(\xi_\tau),\ \forall \sigma, \tau \in G_{\bar{K}/K}.$$

*The associated cohomology class in $H^1(G_{\bar{K}/K}, Isom(C))$ is denoted by $\{\xi\}$.*

*(ii) The cohomology class $\{\xi\}$ is determined by the $K$-isomorphism class $C'$ and is independent of the choice of $\phi$. We thus obtain a natural map*

$$Twist(C/K) \to H^1(G_{\bar{K}/K}, Isom(C)).$$

*(iii) The map in (ii) is a bijection. Hence the twists of $C/K$ up to $K$-isomorphism are in 1-1 correspondence with the elements of cohomology set $H^1(G_{\bar{K}/K}, Isom(C))$.*

*Proof.* Note that by definition $\sigma(\phi\psi) = \sigma(\phi)\sigma(\psi)$.

The first part is clear as

$$\xi_{\sigma\tau} = \phi^{-1}\sigma\tau(\phi) = (\phi^{-1}\sigma(\phi))\sigma(\phi^{-1}\tau(\phi)) = \xi_\sigma\sigma(\xi_t au).$$

For the second part, we want to show the map is well-defined. In other words, let $C''$ be another twist of $C/K$ and let $\psi : C \to C''$ be $\bar{K}$-isomorphism. We want to show $\phi^{-1}\sigma(\phi)$ and $\psi^{-1}\sigma(\psi)$ lies in the same cohomology class. Let $\theta : C' \to C''$ be isomorphism over $\bar{K}$ as they are both isomorphic to $C$. Assume $C'$ is equivalent to $C''$ so $\theta$ is defined over $K$.

Let $\alpha = \phi^{-1}\theta\psi \in \mathrm{Isom}(C)$. Then

$$\begin{aligned} \alpha(\psi^{-1}\sigma(\psi)) &= \phi^{-1}\theta\sigma(\psi) = \phi^{-1}\sigma(\theta\psi) \\ &= \phi^{-1}\sigma(\phi)\sigma(\phi^{-1}\theta\psi) = (\phi^{-1}\sigma(\phi))\sigma(\alpha). \end{aligned}$$

Thus they lie in the same class.

Finally, we develop several steps to prove the last statement. We show the map in (ii) is injective first. Suppose $C'/K$ and $C''/K$ are twist of $C/K$ which give the same cohomology class. This means

if we pick $\bar{K}$-isomorphisms $\phi : C \to C'$ and $\psi : C \to C''$ then there exists a map $\alpha \in \text{Isom}(C)$ such that

$$\alpha(\psi^{-1}\sigma(\psi)) = (\phi^{-1}\sigma(\phi))\sigma(\alpha) \ \forall \sigma \in G_{\bar{K}/K}.$$

Now consider the map $\theta = \phi\alpha\psi^{-1}$. It is a $\bar{K}$-isomorphism and we check it is defined over $K$. Indeed,

$$\sigma(\theta) = (\sigma(\phi))\sigma(\alpha)\sigma(\psi^{-1}) = \phi\alpha(\psi^{-1}\sigma(\psi))\sigma(\psi^{-1}) = \theta$$

by using the relation above. Thus, $C'$ and $C''$ are equivalent so they have the same class in $\text{Twist}(C/K)$. This shows the map is injective.

To prove surjectivity, we introduce the twisted action. For any $f \in \bar{K}(C)$, let $\sigma(f)$ denote the usual action of $\sigma \in G_{\bar{K}/K}$ on $f$ and define the twisted action

$$\sigma^*(f) = \sigma(f)\xi_\sigma$$

where $\xi_\sigma \in \text{Isom}(C)$ is the one introduced in (i). Now we consider the subfield $F \subset \bar{K}(C)$ fixed by $\sigma^*$. Intuitively, $F$ is the function field of the twisted curve and now we check this is the case.

Clearly, $F \cap \bar{K} = K$ because for any constant function $f$, $\xi_\sigma(f) = f$ and since $f \in F$ we conclude that $\sigma(f) = f$ for all $\sigma \in G_{\bar{K}/K}$. This shows that $f \in K$. Further, $\bar{K}F = \bar{K}(C)$ (here $\bar{K}(C)$ is considered as the function field with the twisted action). We leave this as an exercise. Thus, $F$ has transcendence degree one over $K$ and hence a function field of some smooth curve $C'$. Thus, the isomorphism of function field induces (a geometric fact) an isomorphism between $C'$ and $C$ over $\bar{K}$. This shows that $C'$ is a twist of $C$.

Finally, we show that the image of $C'/K$ corresponds to the class $\{\xi\}$. Let $\phi : C \to C'$ be a $\bar{K}$-isomorphism, for which $\phi^*$ is the isomorphism of function fields

$$\phi^* : \bar{K}(C') \to \bar{K}(C).$$

In fact, the above notation is a bit confusing because $\bar{K}(C') = \bar{K}(C)$, viewed under different action of Galois so we may identify $(\phi^*)^{-1}$ in terms of $\sigma^*$. This means if $\psi = \phi^{-1}$, then the Galois action is compatible in the following sense:

$$\sigma(f\psi) = \sigma^*(\psi^* f) = \sigma(f)\xi_\sigma\psi.$$

This is true for all $f \in \bar{K}(C)$ (although again it might be confusing because $\bar{K}(C)$ is the same as $\bar{K}(C')$ endowed with different action). Thus, this shows that

$$\sigma(\psi) = \xi_\sigma\psi \Rightarrow \xi_\sigma = \phi^{-1}\sigma(\phi)$$

using $\psi = \phi^{-1}$. □

We finish this subsection by giving a very simple example.

**Example 30.19.** *Let $E/K$ be an elliptic curve and let $d$ be a non-square in $K$. Let*

$$\chi : G_{\bar{K}/K} \to \{\pm 1\}, \chi(\sigma) = \sigma(\sqrt{d})/\sqrt{d}.$$

*Define a 1-cocycle by*

$$\xi : G_{\bar{K}/K} \to Isom(E), \xi_\sigma = [\chi(\sigma)]$$

*where $[\cdot]$ is the multiplication by $\cdot$ map.*

*Let $E/K$ be given by $y^2 = f(x)$ and $\bar{K}(E) = \bar{K}(x, y)$. We want to find the twist $C/K$ associated to the cohomology class of $\xi_\sigma$. We firstly find the twisted action:*

$$\sigma^*(\sqrt{d}) = \chi(\sigma)\sqrt{d}, \sigma^*(x) = x, \sigma^*(y) = \chi(\sigma)y$$

*by using* $[-1](x,y) = (x,-y)$ *and* $\sqrt{d}$ *is a constant function. Now let* $x' = x$ *and* $y' = y/\sqrt{d}$*, then it is clear that* $x'$ *and* $y'$ *are fixed by* $\sigma^*$ *and we have*

$$dy'^2 = f(x').$$

*To see these generate the function field, note that the action only depends on the action of* $Gal(K(\sqrt{d})/K)$ *and by fundamental theorem of Galoois, we expect that the function field of the twist has degree* 2 *over the base field* $K$*, which is clear as* $y' = y/\sqrt{d}$*.*

*Thus, we have found the twist and the isomorphism* $(x,y) \mapsto (x, y/\sqrt{d})$ *over* $K(\sqrt{d})$*. We will give a more complicated example later.*

We now introduce a special class of twists, associated to elliptic curves.

**Definition 30.20.** *Let* $E/K$ *be an elliptic curve. A (principal)* **homogenous space** *(sometimes called* **torsor***) for* $E/K$ *is a smooth curve* $C/K$ *together with a simply transitive algebraic group action of* $E$ *on* $C$ *defined over* $K$*. In other words, a homogenous space for* $E/K$ *consists of a pair* $(C,\mu)$ *where* $C/K$ *is a smooth curve and*

$$\mu : C \times E \to C$$

*is a morphism defined over* $K$ *having the following properties:*

*(i)* $\mu(p,O) = p$ *for all* $p \in C$*.*

*(ii)* $\mu(\mu(p,P),Q) = \mu(p,P+Q)$ *for all* $p \in C$ *and* $P,Q \in E$*.*

*(iii) For all* $p,q \in C$ *there is a unique* $P \in E$ *satisfying* $\mu(p,P) = q$*.*

*We will often replace* $\mu(p,P)$ *with the more intuitive notation* $p+P$ *and similarly a* **subtraction map** *on* $C$ *is defined by*

$$\nu : C \times C \to E, \nu(q,p) = (P \in E : \mu(p,P) = q).$$

*We will often replace* $\mu(q,p)$ *by the more intuitive notation* $q-p$*.* $\nu$ *is well-defined by (iii).*

We now prove some immediate properties from the definition:

**Lemma 30.21.** *Let* $C/K$ *be a homogenous space for* $E/K$*. Then for all* $p,q \in C$ *and* $P,Q \in E$ *we have*

*(i)* $p+O = p, p-p = O$*,*

*(ii)* $p+(q-p) = q, (p+P)-p = P$*,*

*(iii)* $(q+Q)-(p+P) = (q-p)+Q-P$*,*

*where we use the notation* $\mu(p,P) = p+P$ *and* $\nu(q,p) = q-p$*.*

*Proof.* (i) $p+O = p$ is definition and thus $p-p = O$ is clear by definition.

(ii) Let $q - p = P$ and so $P$ is the unique point such that $p + P = q$ by definition of $\nu$. Thus, $p + (q - p) = q$. Now let $q = p + P$ and so $q - p = P$ so $(p + P) - p = P$.

(iii) Let $p + P = t \in C$, $P, Q \in E$ and we have

$$\begin{aligned} t + ((q-p) + (Q-P)) &= (t + (q-p)) + (Q-P) = ((p+P) + (q-p)) + (Q-P) \\ &= (p + (P + (q-p))) + (Q-P) = (p + ((q-p) + P)) + (Q-P) \\ &= ((p + (q-p)) + P) + (Q-P) = (q+P) + (Q-P) \\ &= q + (P + Q - P) = q + Q \end{aligned}$$

where each line we use property (ii) of the property of $\mu$ (the proof is essentially by repeated use of property (ii)).

□

Now we prove that the subtraction map is a morphism.

**Proposition 30.22.** *Let $E/K$ be an elliptic curve and $C/K$ a homogenous space for $E/K$. Fix a point $p_0 \in C$ and define*

$$\theta : E \to C, \theta(P) = p_0 + P.$$

*(i) The map $\theta$ is an isomorphism defined over $K(p_0)$. In particular, $C/K$ is a twist of $E/K$.*

*(ii) For all $p \in C$ and $P \in E$,*

$$p + P = \theta(\theta^{-1}(p) + P)$$

*where the addition on the left hand side is given by $\mu$ and the one on the right hand side is the usual addition on elliptic curve.*

*(iii) For all $p, q \in C$,*

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

*(iv) The subtraction map*

$$\mu : C \times C \to E, \mu(q, p) = q - p,$$

*is a morphism and is defined over $K$.*

*Proof.* (i) Let $\sigma \in G_{\bar{K}/K}$ which fixes $p_0$, then for any $P \in E$,

$$\sigma(\theta)(P) = \sigma(\theta(\sigma^{-1}P)) = \sigma(p_0 + \sigma^{-1}P) = p_0 + P = \theta(P)$$

and hence the map $\sigma(\theta)$ is invariant under $\sigma \in G_{\bar{K}/K}$ which fixes $p_0$ (note in the equation above $\sigma(\theta)$ is the map twisted by $\sigma$). Since $\mu$ is a morphism and hence $\theta$ is a morphism. The action of $\mu$ is transitive so $\theta$ has degree 1 and hence it is an isomorphism.

(ii) It is clear that if we start from the right hand side then

$$p_0 + ((p - p_0) + P) = (p_0 + (p - p_0)) + P = p + P$$

using property (ii) of $\mu$.

(iii) Again we start from the right hand side,

$$\theta^{-1}(q) - \theta^{-1}(p) = (p_0 + \theta^{-1}(q)) + (p_0 + \theta^{-1}(p)) = q - p$$

by using (iii) of the previous lemma.

(iv) Since subtraction on $E$ is a morphism and so by (iii) the map $\nu$ is a morphism. Finally, to check $\nu$ is defined over $K$ we need $\sigma(q-p) = \sigma q - \sigma p$. This follows from (iii) by

$$\begin{aligned} \sigma(q-p) &= \sigma(\theta^{-1}q - \theta^{-1}p) = \sigma(\theta^{-1}q) - \sigma(\theta^{-1}p) \\ &= \sigma(q - p_0) - \sigma(p - p_0) = \sigma(q) - \sigma(p) \end{aligned}$$

where we use the subtraction map on $E$ is defined over $K$.

□

**Definition 30.23.** *Let $C/K$,$C'/K$ be homogenous space for $E/K$. We say $C/K, C'/K$ are equivalent if there is an isomorphism $\theta : C \to C'$ defined over $K$ that is compatible with the action of $E$ on $C$ and $C'$. In other words,*

$$\theta(p + P) = \theta(p) + P \ \forall p \in C, P \in E.$$

*The equivalence class containing $E/K$ acting on itself by translation is called the trivial class. The collection of equivalence classes of homogenous spaces for $E/K$ is called the* **Weil-Chatelet group** *for $E/K$ and is denoted by $WC(E/K)$.*

The following proposition gives a criteria of when $C/K$ is in the trivial class.

**Proposition 30.24.** *Let $C/K$ be a homogenous space for $E/K$. Then $C/K$ is in the trivial class if and only if $C(K)$ is not the empty set.*

*Proof.* Suppose $C/K$ is in the trivial class. Then there is a $K$-isomorphism $\theta : E \to C$ and thus $\theta(O) \in C(K)$.

Conversely, suppose $p_0 \in C(K)$ then construct the map

$$\theta : E \to C, \theta(P) = p_0 + P,$$

is an isomorphism defined over $K(p_0) = K$ (by previous proposition). The required compatibility condition follows directly from property (ii) of $\mu$:

$$\theta(P + Q) = p + (P + Q) = (p + P) + Q = \theta(P) + Q.$$

□