

# Logic and Set Theory

Zexiang Chen

August 15, 2011

This is an introduction to Logic and Set Theory based on Prof. Leader's Notes and Prof. Johnstone's book. You may find hints and solutions to the questions on Tripos paper in previous years at the end of the booklet. All errors are happily received (zc231@cam.ac.uk) and are my responsibility, not the lecturers. Please do not redistribute this booklet or photocopy them without my permission.

I would like to thank Dr.T.Forster for hints and discussion on some questions and Zhenlin Low for final check of the article.

## Contents

<b>1</b>	<b>Propositional Logic</b>	<b>2</b>
<b>2</b>	<b>Well-orderings</b>	<b>8</b>
<b>3</b>	<b>Ordinals</b>	<b>13</b>
<b>4</b>	<b>Posets and Zorn's Lemma</b>	<b>19</b>
<b>5</b>	<b>Predicate Logic</b>	<b>24</b>
<b>6</b>	<b>Set Theory</b>	<b>34</b>
<b>7</b>	<b>Cardinal</b>	<b>40</b>
<b>8</b>	<b>Brief Discussion on Example Sheet 2011</b>	<b>42</b>
8.1	Example sheet 1 . . . . .	42
8.2	Example sheet 2 . . . . .	45
8.3	Example sheet 3 . . . . .	50
8.4	Example sheet 4 . . . . .	54

<b>9</b>	<b>Discussion on Triplos Paper</b>	<b>57</b>
9.1	2004 . . . . .	57
9.2	2005 . . . . .	59
9.3	2006 . . . . .	60
9.4	2007 . . . . .	61
9.5	2008 . . . . .	64
9.6	2009 . . . . .	65
9.7	2010 . . . . .	67

# 1 Propositional Logic

Let  $P$  be a set of primitive language (specified later), unless otherwise stated,  $P = \{p_1, p_2 \dots\}$ . i.e.  $P$  is countable.

The set of propositions, written  $L$  or  $L(P)$ , is defined inductively by:

1. If  $p \in P$ , then  $p \in L$ .
2.  $\perp \in L$  ( $\perp$  reads as 'False').
3. If  $p, q \in L$ , then  $(p \Rightarrow q) \in L$ .

**Remark 1.1.** 1. Propositions are finite strings of symbols from the alphabet, e.g.  $\perp, \Rightarrow, (, ) \dots$

2. ' $L$  defined inductively' means that we set  $L_0 = P, L_1 = P \cup \{\perp\}$  and for  $n \geq 2, L_{n+1} = L_n \cup \{(p \Rightarrow q) : p, q \in L_n\}$ .  $L = \bigcup_{n \in \mathbb{N}} L_n$ .

3. Each proposition is built up from 1&2 using 3 above, and is in a unique way. For example,  $((p_1 \Rightarrow p_2) \Rightarrow (p_1 \Rightarrow p_3))$  came from  $(p_1 \Rightarrow p_2)$  and  $(p_1 \Rightarrow p_3)$

We can now define e.g.  $\neg p$  (reads as 'not  $p$ '),  $p \vee q$  (reads as ' $p$  or  $q$ '),  $p \wedge q$  (reads as ' $p$  and  $q$ '). In particular we can write  $p \vee q$  as  $((\neg p) \Rightarrow q)$  and  $p \wedge q$  as  $\neg(p \Rightarrow (\neg q))$

## Symmantic implication

**Definition 1.2.** A valuation on  $L$  is a function  $v : L \rightarrow \{0, 1\}$  s.t.  $v(\perp) = 0$  and

$$v(p \Rightarrow q) = \begin{cases} 0 & \text{if } v(p) = 1, v(q) = 0, \\ 1 & \text{otherwise} \end{cases}$$

The valuation is precisely a map from  $L$  to  $\{0, 1\}$  that preserves the structure ( $\perp$  and  $\Rightarrow$ ) i.e. a homomorphism.

**Proposition 1.3.**

1. If  $v, v'$  are valuations with  $v(p) = v'(p) \forall p \in P$ , then  $v = v'$
2. For any function  $w : P \rightarrow \{0, 1\} \exists$  valuation  $v$  with  $v(p) = w(p) \forall p \in P$

*Proof.*

1.  $v(p) = v'(p) \forall p \in L_1$  because  $v(\perp) = v'(\perp) = 0$ . If  $v(p) = v'(p)$  and  $v(q) = v'(q)$ , then  $v(p \Rightarrow q) = v'(p \Rightarrow q)$  and hence  $v(p) = v'(p) \forall p \in L_2$ . Continue this inductively,  $\forall n, v(p) = v'(p) \forall p \in L_n$  and hence  $v = v'$  (Remember we assume the primitive language to be countable)
2. Set  $v(p) = w(p) \forall p \in P$  and set  $v(\perp) = 0$ . this defines a valuation  $v$  on  $L_1$ . Then we define  $v$  inductively on  $L_n$ . Having defined  $L_n$ , use Definition 1.2 to define  $v$  on  $L_{n+1}$ . Hence  $v$  is a valuation on  $L$

□

**Example 1.4.** Let  $v$  be given by  $v(p_1) = v(p_2) = 1$   $v(p_n) = 0 \forall n \geq 3$ . Then  $v((p_1 \Rightarrow p_2) \Rightarrow p_3) = 0$

**Definition 1.5.**  $p$  is a tautology, written ' $\models p$ ', if  $v(p) = 1 \forall v$ .

Table 1: Truth table

$v(p)$	$v(q)$	$v(q \Rightarrow p)$	$v(p \Rightarrow (q \Rightarrow p))$
1	1	1	1
1	0	1	1
0	1	0	1
0	0	1	1

**Example 1.6.**

1.  $p \Rightarrow (q \Rightarrow p)$  is a tautology.

*We can use the truth table (see table 1 above):*

2.  $(\neg\neg p) \Rightarrow p$  i.e.  $((p \Rightarrow \perp) \Rightarrow \perp) \Rightarrow p$

3.  $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$

*It's tedious to check the truth table in this case. Instead, we could use the following trick:*

*Suppose not, then we have some valuation  $v$  s.t. the value of  $v$  is 0 on this proposition. Then  $v(p \Rightarrow (q \Rightarrow r)) = 1, v((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) = 0$ . Therefore,  $v(p \Rightarrow q) = 1, v(p \Rightarrow r) = 0$  and so  $v(p) = 1, v(q) = 1, v(r) = 0$ . But then  $v(p \Rightarrow (q \Rightarrow r)) = 0 \neq 1$ , which is a contradiction.*

**Definition 1.7.** For  $S \subset L$  and  $t \in L$ , we say that  $S$  entails  $t$  or semantically implies  $t$ , written  $S \models t$ , if  $\forall v$  with  $v(s) = 1, \forall s \in S$  then  $v(t) = 1$ .

**Example 1.8.**  $\{p \Rightarrow q, q \Rightarrow r\} \Rightarrow \{p \Rightarrow r\}$

*Because if  $v(p \Rightarrow r) = 0$ , then  $v(p) = 1, v(r) = 0$ . This is impossible for  $v(p \Rightarrow q), v(q \Rightarrow r) = 1$ . Therefore, if both  $v(p \Rightarrow q), v(q \Rightarrow r) = 1$  then  $v(p \Rightarrow r) = 1$*

**Definition 1.9.** Given  $t \in L$ ,  $v$  valuation, we say  $t$  is true in  $v$  or  $v$  is a model of  $t$  if  $v(t) = 1$ . For  $S \subset L$ , a model of  $S$  is a valuation  $v$  s.t.  $v(s) = 1 \forall s \in S$ . So  $S \models t$  says that every model of  $S$  is a model of  $t$ .

Note:  $\models t$  is the same as  $\emptyset \models t$ .

## Syntactic implication

For a notion of *proof*, we will need axioms and deduction rule. We have the following axioms:

$$A_1 \quad p \Rightarrow (q \Rightarrow p)$$

$$A_2 \quad (p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$$

$$A_3 \quad (\neg\neg p) \Rightarrow p$$

**Remark 1.10.** We checked before that all of these are tautologies. And usually we call them Axiom-Schemes

For rules of deduction, we will only use Modus Ponens (MP) (which means that from  $p, p \Rightarrow q$  we can deduce  $q$ ).

**Definition 1.11.** For  $S \subset L, t \in L$ , a proof of  $t$  from  $S$  consists of finite sequence  $t_1 \dots t_n$  of propositions, written  $t_n = t$  s.t. for each  $i$ ,  $t_i$  is either:

1. Axioms
2. an element of  $S$
3. or  $\exists j, k < i$  with  $t_k = (t_j \Rightarrow t_i)$

If there is a proof of  $t$  from  $S$ , we say that  $S$  syntactically implies  $t$  or  $S$  proves  $t$ , or  $t$  is a theorem of  $S$ , written  $S \vdash t$ .

If  $\emptyset \vdash t$ , we write  $\vdash t$  for shorthand, and it means ‘ $t$  is a theorem’. In a proof of  $t$  from  $S$ ,  $t$  is the conclusion and  $S$  is the set of hypothesis or premises.

**Example 1.12.**  $\vdash (p \Rightarrow p)$

1.  $[A_2] (p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$

2.  $[A_1] p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$

3.  $[MP] (p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$

4.  $[A_1] p \Rightarrow (p \Rightarrow p)$

5.  $[MP] p \Rightarrow p$

**Proposition 1.13. [Deduction theorem]:** *Let  $S \subset L$  and  $p, q \in L$  then  $S \vdash (p \Rightarrow q)$  if and only if  $S \cup \{p\} \vdash q$ .*

*Proof.*

‘ $\Rightarrow$ ’: Given a proof of  $p \Rightarrow q$  from  $S$ , write down  $p$  (hypothesis), and by MP, we can deduce  $q$  from  $p$  and  $p \Rightarrow q$ .

‘ $\Leftarrow$ ’: Conversely, given a proof of  $t_1 \dots t_n$  of  $q$  from  $S \cup \{p\}$ , we will show that  $S \vdash (p \Rightarrow t_i) \forall i$ .

If  $t_i$  is axiom or  $t_i \in S$ , then  $A_1$  implies  $t_i \Rightarrow (p \Rightarrow t_i)$  and so  $p \Rightarrow t_i$  by MP.

If  $t_i$  is  $p$  then we have shown that  $\vdash p \Rightarrow p$ .

If  $t_i$  is obtained by MP, i.e. we have earlier lines  $t_j, t_j \Rightarrow t_i$ . We use an inductive argument. Assume that  $S \vdash (p \Rightarrow t_j)$  and  $S \vdash (p \Rightarrow (t_j \Rightarrow t_i))$ . We can write down, by  $A_2$ :

$(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$ . Use MP, we have  $S \vdash (p \Rightarrow t_i)$  □

How are  $\vdash$  and  $\models$  related?

**Theorem 1.14. [Completeness theorem]:**  *$S \vdash t$  if and only if  $S \models t$*

We split the proof into two parts.

**Proposition 1.15. [Soundness]** *If  $S \vdash t$  then  $S \models t$ .*

*Proof.* Let  $v$  be any valuation s.t.  $v(p) = 1 \forall p \in S$  and  $v(p) = 1 \forall p$  axioms. Also if  $v(p) = 1$  and  $v(p \Rightarrow q) = 1$  then by definition  $v(q) = 1$ . Hence each line  $p$  of proof of  $t$  from  $S$  has  $v(p) = 1$ . And as  $t$  is the last line of the proof so  $v(t) = 1$  as required. □

**Definition 1.16.** *We say  $S \subset L$  is consistent if  $S \not\vdash \perp$*

**Theorem 1.17. [Adequacy]** *Let  $S \subset L$  be consistent. Then  $S$  has a model.*

*Proof.* Claim: for any  $S \subset L$  consistent and  $p \in L$ , at least one of  $S \cup \{p\}$  and  $S \cup \{\neg p\}$  is consistent.

Proof of the claim: Suppose not, then both of them are inconsistent. Then  $S \cup \{p\} \vdash \perp$  and  $S \cup \{\neg p\} \vdash \perp$ . Then by Deduction theorem,  $S \vdash (p \Rightarrow \perp)$  and  $S \vdash p$  so  $S \vdash \perp$ , which is a contradiction.

Now, as we assume that  $L$  is countable so we may enumerate it as  $\{t_1, t_2, \dots\}$  and let  $S_0 = S$ . Let  $S_1 = S_0 \cup \{t_1\}$  or  $S_0 \cup \{\neg t_1\}$  s.t.  $S_1$  is consistent.

And similarly, suppose we have  $S_n$ , define  $S_{n+1}$  inductively by  $S_{n+1} = S_n \cup \{t_n\}$  or  $S_n \cup \{\neg t_n\}$  s.t. it is consistent.

Let  $\mathfrak{S} = \bigcup_{n=0}^{\infty} S_n$ . Then  $S \subset \mathfrak{S}$  and  $\forall p \in L$  either  $p \in \mathfrak{S}$  or  $\neg p \in \mathfrak{S}$ . Also  $\mathfrak{S}$  is consistent, for if not, as proof is finite, and by construction of  $\mathfrak{S}$ , we must have  $S_n$  inconsistent for some  $n$ . And  $\mathfrak{S}$  is deductively closed, meaning that if  $\mathfrak{S} \vdash t$  then  $t \in \mathfrak{S}$ . Because, if not, then as one of  $t$  or  $\neg t$  lies in  $\mathfrak{S}$  so  $\neg t$  is in  $\mathfrak{S}$ . But  $\mathfrak{S} \vdash t$ , and so by MP,  $\mathfrak{S} \vdash \perp$ , contradiction.

Now define  $v : L \rightarrow \{0, 1\}$  by:

$$v(p) = \begin{cases} 1 & \text{if } p \in \mathfrak{S} \\ 0 & \text{if } \neg p \in \mathfrak{S} \end{cases}$$

As  $S \subset \mathfrak{S}$  it remains to check that  $v$  is indeed a valuation and hence a model of  $S$ . As  $\mathfrak{S}$  is consistent so that  $\perp \notin \mathfrak{S}$  and so  $v(\perp) = 0$

If  $v(q) = 1$  then  $q \in \mathfrak{S}$  and use  $A_1, q \Rightarrow (p \Rightarrow q)$  so that by MP,  $p \Rightarrow q \in \mathfrak{S}$  and as it is deductively closed,  $v(p \Rightarrow q) = 1$ .

Similarly, if  $v(p) = 0$ , so  $p \notin \mathfrak{S}$  and so  $\neg p \in \mathfrak{S}$ . We check that  $\vdash \perp \Rightarrow q$ .

By  $A_1, \perp \Rightarrow (\neg q \Rightarrow \perp)$ , and then by  $A_3, \neg \neg q \Rightarrow q$  so by MP,  $\perp \Rightarrow q$ . Therefore, by MP,  $\mathfrak{S} \vdash p \Rightarrow q$  and so  $v(p \Rightarrow q) = 1$ .

Finally, if  $v(p) = 1, v(q) = 0$ , so  $p, \neg q \in \mathfrak{S}$ . We cannot have  $p \Rightarrow q \in \mathfrak{S}$  as  $\mathfrak{S}$  is deductively closed. If  $p \Rightarrow q \in \mathfrak{S}$ , then  $q \in \mathfrak{S}$ , but  $\neg q \in \mathfrak{S}$ , contradiction. Hence  $v$  is a valuation and so it is a model for  $S$ .  $\square$

**Remark 1.18.** *In fact, theorem 1.17 holds when  $L$  is not countable.(see later)*

Now we can prove the other part of ‘Completeness Theorem’.

*Proof.* Let  $S \subset L, t \in L$  and assume  $S \models t$ , then,  $S \cup \{\neg t\} \models \perp$ . (they cannot both have valuation 1). If  $S \cup \{\neg t\} \not\models \perp$ , by Adequacy, then  $S \cup \{\neg t\}$  has a model, contradiction. And so  $S \cup \{\neg t\} \vdash \perp$ , then by Deduction theorem, and  $A_3$  we have  $S \vdash t$ .  $\square$

**Corollary 1.19. [Compactness Theorem]** *Let  $S \subset L, t \in L$  with  $S \models t$ , then we have some finite subset  $S'$  of  $S$  s.t.  $S' \models t$ .*

*Proof.* This is trivial if we replace ' $\models$ ' by ' $\vdash$ ', because proof is finite so we must have only used a finite subset of it.  $\square$

**Remark 1.20.** *The case  $t = \perp$  says if every finite subset has a model, then  $S$  itself has a model. This is a very useful consequence.*

**Corollary 1.21.** *There is an algorithm to decide in finite time whether or not  $S \vdash t$  for any given  $S$  and  $t$*

Note: This seems highly unlikely to do but it is possible.

*Proof.* Trivial if we replace  $\vdash$  by  $\models$  and use the truth table.  $\square$

## 2 Well-orderings

**Definition 2.1.** *A linear order or total order is a pair  $(X, <)$  where  $X$  is a set and  $<$  is a relation on  $X$  satisfying:*

1. *Irreflexive: Not  $x < x \forall x \in X$*
2. *Transitivity:  $x < y, y < z \Rightarrow x < z \forall x, y, z \in X$*
3. *Trichotomous:  $x < y$  or  $y < x$  or  $x = y \forall x, y \in X$*

Notation: We write  $x > y$  to mean  $y < x$  and  $x \leq y$  to mean  $x < y$  or  $x = y$

In terms of  $\leq$ , a total order would be:

1. Reflexive:  $x \leq x$
2. Transitivity:  $x \leq y, y \leq z \Rightarrow x \leq z$
3. Antisymmetric:  $x \leq y$  and  $y \leq x \Rightarrow x = y$
4. Trichotomous:  $x \leq y$  or  $y \leq x$

**Example 2.2.**



1.  $(\mathbb{N}, <)$ , where  $<$  is the usual ordering.
2.  $(\mathbb{Z}, <)$ , again  $<$  is the usual ordering.
3.  $\mathbb{R}, \mathbb{Q}$  with usual ordering.
4.  $(\mathbb{N}, <)$  where  $x < y$  if  $x|y$  and  $x \neq y$ . This is not a total ordering as it does not satisfy Trichotomous. e.g.  $x=3, y=5$ .
5.  $\mathbb{P}(S)$  The power set of some set  $S$ , where  $x < y$  if  $x \subset y$ . This is not total ordering as it again does not satisfy Trichotomous.

A total ordering is called *Well-Ordering* if every **non-empty** subset has a least element. i.e.  $\forall S \subset X, S \neq \emptyset \Rightarrow \exists x \in S, \text{ s.t. } x \leq y \forall y \in S$ .

**Example 2.3.**

1.  $(\mathbb{N}, <)$
2.  $(\mathbb{Z}, <)$  is not as it does not have a least element.
3.  $\{x \in \mathbb{Q}, x \geq 0\}$  is not as it does not have a least element.
4.  $\{\frac{1}{2}, \frac{2}{3}, \dots\}$  as a subset of  $\mathbb{R}$
5.  $\{1 - \frac{1}{n} : n = 1, 2, \dots\} \cup \{1\}$
6.  $\{1 - \frac{1}{n} : n = 2, 3, \dots\} \cup \{2\}$
7.  $\{1 - \frac{1}{n} : n = 2, 3, \dots\} \cup \{2 - \frac{1}{n} : n = 2, 3, \dots\}$

**Remark 2.4.** A total ordering is a well-ordering if and only if it does not contain an infinite strictly decreasing sequence  $x_1, x_2 \dots$  because if we have such, then the subset  $\{x_1, x_2 \dots\}$  has no least element. Conversely, if  $S \subset X$  has no least element then surely we can have an infinite decreasing sequence, with Axiom of Choice (see later).

**Definition 2.5.** Given two total orderings  $X, Y$  we say  $X$  is **isomorphic** to  $Y$  if there is a bijection from  $X$  to  $Y$  which preserves ordering, i.e.  $f(x) < f(y)$  if and only if  $x < y \forall x, y \in X$ .

**Proposition 2.6. [Proof by Induction]** Let  $(X, <)$  be a well-ordering and let  $S \subset X$  s.t.  $\forall x \in X$ , if  $y \in S \forall y < x \Rightarrow x \in S$ . Then  $S = X$ . (Equivalently: for a property  $P(X)$ , if  $P(y)$  holds  $\forall y < x \Rightarrow P(x)$ , then  $P(x)$  holds  $\forall x$ ).

*Proof.* Suppose  $S \neq X$ , so that  $X \setminus S$  is non-empty. As  $X$  is a well-ordering, so we have a least element  $x \in X \setminus S$ , i.e.  $x \notin S$ . Then for any  $y < x, y \in S$ . But by assumption, if  $\forall y < x, y \in S$  then  $x \in S$ , which is a contradiction. Hence  $S = X$ .  $\square$

**Proposition 2.7.** Let  $X$  and  $Y$  be isomorphic well-orderings. Then there is a unique isomorphism from  $X$  to  $Y$ .

*Proof.* Let  $f, g : X \rightarrow Y$  be isomorphisms. We shall show that  $f(x) = g(x) \forall x \in X$ .

We prove this by induction. Given  $x \in X$ , with  $f(y) = g(y) \forall y < x$ , we want  $f(x) = g(x)$ . Clearly,  $f(x)$  is not in the set  $\{f(y) : y < x\}$  as  $f$  is bijective, and so  $f(x) \in Y \setminus \{f(y) : y < x\}$  i.e. the set  $Y \setminus \{f(y) : y < x\}$  is non-empty. As  $Y$  is well-ordering, let  $a$  be the least element of  $Y \setminus \{f(y) : y < x\}$ .

Claim:  $f(x) = a$ . If not, then  $f(x) > a$  by the choice of  $a$ , but as  $f$  is bijective, we have some  $x'$  s.t.  $f(x') = a$ . And  $x' > x$  because if not,  $x' < x$  and so  $f(x') \in Y \setminus \{f(y) : y < x\}$ . Now we have  $f(x') = a < f(x)$  but  $x' > x$ , which is a contradiction.

Hence  $f(x) = a$ . Similarly,  $g(x) = a$  by the same argument. Therefore  $f(x) = g(x)$  and so by induction,  $f(x) = g(x) \forall x \in X$ .  $\square$

**Definition 2.8.** A subset  $I$  of a total ordering  $X$  is an **initial segment** if  $x \in I, y < x \Rightarrow y \in I$ . For example, for any  $x \in X$ ,  $I_x = \{y \in X : y < x\}$ .

Note that every initial segment is of the above form. e.g. in  $\mathbb{R}$  we have something like  $\{x \leq 3\}$ . In  $\mathbb{Q}$  we can have  $\{x < \sqrt{2}\}$ .

**Remark 2.9.** In a well-ordering  $X$ , every proper initial segment  $I$  is of the form  $I_x$  for some  $x \in X$ . Indeed, let  $x = \min(X \setminus I)$  Then  $y < x \Rightarrow y \in I$ . Conversely,  $y \in I \Rightarrow y < x$  because  $y \neq x$ , and if  $x < y$  then  $x \in I$ , but by the choice of  $x$ ,  $x \notin I$ .

Aim: Every subset of a well-ordering is isomorphic to some initial segment.

Notation: For  $f : A \rightarrow B, A' \subset A$ , the restriction of  $f$  to  $A'$  is the function  $f|_{A'} : A' \rightarrow B$  given by  $f|_{A'} = \{(a, f(a)) : a \in A'\}$ .

**Theorem 2.10. [Definition by recursion]** *Let  $X$  be a well-ordering, and  $Y$  is any set. Then for any  $G : \mathbb{P}(X \times Y) \rightarrow Y, \exists f : X \rightarrow Y$  s.t.  $f(x) = G(f|_{I_x}) \forall x \in X$ . Moreover,  $f$  is unique.*

*Proof.*

Existence: The clever idea is to say 'h is an attempt' to mean  $h : I \rightarrow Y$ , some initial segment of  $X$  and  $\forall x \in I, h(x) = G(h|_{I_x})$  where  $h|_{I_x} = \{(y, h(y)) : y < x\}$ .

Firstly we show that if  $h, h'$  both attempts defined at  $x$  and at  $y \forall y < x$ , then  $h(x) = h'(x)$ . Because if  $h(y) = h'(y) \forall y < x$ , then  $h|_{I_x} = h'|_{I_x}$  and so by definition  $h(x) = h'(x)$ . Then use induction, we conclude that every two attempts defined at  $x$  are the same.

Then we check that  $\forall x \in X$  there is an attempt defined at  $x$ . Again we use induction, by the first observation, we know if there is an attempt at  $x$ , then it must be unique. For every  $y < x$ , there is a unique attempt defined at  $\{z : z < y\}$ . Let  $h = \bigcup_{y < x} h_y$ . This is an attempt defined on  $I_x$ . Thus let  $h' = h \cup \{(x, G(h))\}$  is an attempt defined at  $x$ . Then we define  $f : X \rightarrow Y$  by  $f(x) = y$  if there is an attempt defined at  $x$  with  $h(x) = y$ .

Uniqueness: This is clear as we have shown above that at each  $x$ , we have a unique attempt.  $\square$

**Proposition 2.11. [Subset Collapse]**  *$X$  is a well-ordering,  $Y \subset X$ , then  $Y$  is isomorphic to an initial segment of  $X$ . Moreover, it is unique.*

*Proof.* To obtain  $f : Y \rightarrow X$  an isomorphism with an initial segment of  $X$ , we need precisely that  $f(x) = \min X \setminus \{f(y) : y < x\} \forall x \in Y$ . Thus by proposition 2.10, this function is well-defined and is unique. Note that  $\{f(y) : y < x\} \neq X$ , because  $f(y) \leq y \forall y \in Y$  which can be easily checked by induction. So  $x \notin \{f(y) : y < x\}$ , hence the set  $X \setminus \{f(y) : y < x\}$  is non-empty.  $\square$

**Remark 2.12.** *In particular, a well-ordering  $X$  cannot be isomorphic to proper initial segment of itself.*

**Definition 2.13.** *For any two well-orderings  $X, Y$ , write  $X \leq Y$  if  $X$  is isomorphic to an initial segment of  $Y$ .*

**Example 2.14.**  $X = \mathbb{N}, Y = \{\frac{1}{2}, \frac{2}{3}, \dots\} \cup \{2\}$  then  $X \leq Y$ .

We write  $X < Y$  if  $X \leq Y$  but  $X$  is not isomorphic to  $Y$ .

**Proposition 2.15.** *Let  $X, Y$  be well-orderings, then either  $X \leq Y$  or  $Y \leq X$ .*

*Proof.* Suppose  $Y \not\leq X$ , for  $f : X \rightarrow Y$  isomorphism from  $X$  to an initial segment of  $Y$  we need precisely that  $f(x) = \min Y \setminus \{f(y) : y \leq x\} \forall x \in X$ , and this is well-defined by 2.10 provided that  $Y \setminus \{f(y) : y \leq x\}$  is non-empty. But if  $Y = \{f(y) : y \leq x\}$ , then  $Y$  is isomorphic to an initial segment of  $X$ .  $\square$

**Proposition 2.16.** *Let  $X, Y$  be well-orderings. If  $X \leq Y$  and  $Y \leq X$  then  $X$  is isomorphic to  $Y$ .*

*Proof.* Let  $f$  be isomorphism from  $X$  to an initial segment of  $Y$  and  $g$  be an isomorphism from  $Y$  to an initial segment of  $X$ . Hence,  $g \circ f$  is an isomorphism from  $X$  to an initial segment of  $X$ , which can only be  $X$  itself. Hence it is an identity of  $X$ . Similarly  $f \circ g$  is identity of  $Y$ . Therefore,  $f, g$  are both bijective.  $\square$

Given a well-ordering  $X$  choose  $x \notin X$ , and let  $y < x, \forall y \in X$ . Then this is a well-ordering on the set  $X \cup \{x\}$ , called the successor of  $X$ , written  $X^+$ , and clearly  $X < X^+$ .

Putting things together: given set  $\{X_i : i \in I\}$  of well-orderings, we look for a well-ordering  $X$  with  $X \geq X_i \forall i$ .

**Definition 2.17.** *Given two sets  $X, Y$ . Let  $<_x, <_y$  be orderings on  $X, Y$  respectively. We say  $X$  extends  $Y$  if  $Y < X$ , and  $<_x, <_y$  agree on  $Y$  and  $Y$  is an initial segment of  $X$ .*

**Definition 2.18.** *We say  $\{X_i : i \in I\}$  is nested if  $\forall i, j$ , either  $X_i$  extends  $X_j$  or  $X_j$  extends  $X_i$ .*

**Proposition 2.19.** *Let  $\{X_i : i \in I\}$  be a nested set of well-orderings, then there exists a well-ordering  $X$  with  $X \geq X_i \forall i$ .*

*Proof.* Let  $X = \bigcup_{i \in I} X_i$  with  $x < y$  if  $x <_i y$  for some  $i$ , where  $<_i$  is the ordering on  $X_i$ . This is well-defined because  $\{X_i : i \in I\}$  is nested (and  $x, y$  must both be in some  $X_i$ ).

$X$  is total order, and each  $X_i$  is an initial segment of  $X$  by construction (as  $\{X_i : i \in I\}$  is nested). Now given  $S \subset X$  where  $S$  is non-empty. We have  $S \cap X_i \neq \emptyset$  for some  $i$ . Let  $x$  be the least element in  $S \cap X_i$ , and it exists because  $X_i$  is a well-ordering and  $S \cap X_i$  is a non-empty subset. We check that  $x$  is the least element in  $S$ .

Take any  $y$  in  $S$ , suppose  $y < x$  then as  $X_i$  is an initial segment of  $X$  so we have that  $y \in X_i$  and hence  $y \in S \cap X_i$ , which contradicts  $x$  being least. Hence we have a least element for every non-empty subset of  $X$  and so  $X$  is a well-ordering.  $\square$

**Remark 2.20.** *The above proposition is also true even if  $\{X_i : i \in I\}$  is not nested.*

### 3 Ordinals

Is the collection of well-orderings itself well-ordered?

**Definition 3.1.** *An ordinal is a well-ordering with two well-orderings regarded as the same if they are isomorphic. (Informally, ordinal measures the size of well-ordering).*

**Definition 3.2.** *For a well-ordering  $X$  corresponding ordinal  $\alpha$ , we say that  $X$  has order type  $\alpha$ .*

**Example 3.3.** 1. *For any  $k \in \mathbb{N}$ , write  $k$  for the order type of a set with  $k$  elements. e.g.  $\{1, 3, 4, 8\}$  has order type 4*

2. *We write  $\omega$  for the order type of  $\mathbb{N}$ .*

3. *Similarly,  $\{\frac{1}{2}, \frac{2}{3}, \dots\}$  has order type  $\omega$ .*

**Definition 3.4.** *For  $\alpha, \beta$  ordinals, we say  $\alpha \leq \beta$  if  $\exists X$  with order type  $\alpha$  and  $Y$  with order type  $\beta$ , s.t.  $X \leq Y$ . And we define  $\alpha < \beta, \alpha^+$  in a similar way.*

**Proposition 3.5.** *Let  $\alpha$  be an ordinal, then the set of ordinals  $< \alpha$  form a well-ordering of order type  $\alpha$ .*

*Proof.* Let  $X$  be a set of order type  $\alpha$ . Then the well-orderings  $< X$  are precisely (up to isomorphism) the proper initial segment of  $X$ . But by previous remark we know they are of the form  $I_x, x \in X$ . So for each ordinal  $< \alpha$  there is an initial segment of  $X$  corresponding to this ordinal, and so the set of ordinals  $< \alpha$  has order type  $\alpha$ .  $\square$

Notation: write  $I_\alpha$  to mean  $\{\beta : \beta < \alpha\}$ .

**Proposition 3.6.** *Let  $S$  be non-empty set of ordinals, then  $S$  has a least element.*

*Proof.*  $S \neq \emptyset$ , so pick  $\alpha \in S$ , if  $\alpha$  is least, then we are done. If not, then  $S \cap I_\alpha \neq \emptyset$ , and so by previous proposition,  $S \cap I_\alpha$  has a least element as it is a well-ordering. This element must also be the least element in  $S$  by the same argument as in proposition 2.19.  $\square$

**Theorem 3.7. [Burali-Forti paradox]** *The class of ordinals do not form a set.*

*Proof.* Suppose  $X$  is a set containing every ordinal, then  $X$  itself is a well-ordering, and it has an order type, say  $\alpha$ . But then  $X$  is isomorphic to a proper initial segment of itself, i.e.  $X$  is isomorphic to  $I_\alpha$ .  $\square$

**Definition 3.8.** *Let  $S = \{\alpha_i : i \in I\}$  be a set of ordinals, then  $S$  has an upper bound  $\alpha$  s.t.  $\alpha > \alpha_i \forall i$ . By proposition 3.6, we have a least upper bound, called  $\text{Sup } S$ .*

Before next section, we may count the ordinals, starting from 0.  $0, 1, 2 \dots \omega, \omega + 1 \dots \omega + \omega = \omega \cdot 2$ ,  
 $\omega \cdot 2 + 1 \dots \omega \cdot 3 \dots \omega^2 + 1 \dots \omega^2 + \omega \dots \omega^3 \dots \omega^\omega \dots \omega^{\omega^\omega} \dots$  Note:  $\omega \cdot 2$  is not the same as  $2 \cdot \omega$  (see later).

All the above ordinals are countable, is there an uncountable one?

**Theorem 3.9.** *There is an uncountable ordinal.*

More generally, we have:

**Theorem 3.10. [Hartog's Lemma]** *Given any set  $X$ , there is an ordinal which does not inject into  $X$ .*

As the previous theorem is a consequence of Hartog's Lemma, by choosing the set to be  $\mathbb{N}$ , so we only need to prove Hartog's Lemma.

*Proof.* The typical way of doing this is to consider the set  $A$  which consists of every well-ordering of subsets of  $X$  and then let  $B$  be the set which is a collection of order type of those. Then set  $\gamma$  to be the sup of the set  $B$  hence the result. Here is another way. Suppose every ordinal can be injected into the set  $X$  then  $X$  itself is a well-ordering containing every ordinal, which contradicts Burali-Forti.  $\square$

**Remark 3.11.** *We call  $\omega_1$  to be the least uncountable ordinal. Moreover, for any  $X$ , the least ordinal which does not inject into  $X$  is denoted by  $\gamma(X)$ .*

# successor and limit

Let  $\alpha$  be an ordinal, does it have a greatest element?

If it does, say the greatest element is  $\beta$  then  $\gamma \in I_\alpha \Rightarrow \gamma = \beta$  or  $\gamma < \beta$ . So  $\alpha = \beta^+$  called a successor.

If not, then  $\forall \beta < \alpha, \exists \gamma < \alpha$  s.t.  $\beta < \gamma$ . So  $\alpha = \text{Sup} \{\beta : \beta < \alpha\}$ , we call such  $\alpha$  limit.

**Example 3.12.**  $5$  is a successor.  $\omega^+$  is a successor.  $\omega$  is a limit.  $0$  is a limit as  $0 = \text{Sup} \emptyset$ .

# ordinal arithmetic

Inductive definition.

**Definition 3.13.** We define '+' inductively by:

1.  $\alpha + 0 = \alpha$

2.  $\alpha + \beta^+ = (\alpha + \beta)^+$

3.  $\alpha + \lambda = \text{Sup}\{\alpha + \beta : \beta < \lambda\}$  for  $\lambda$  a non-zero limit

**Remark 3.14.** The definition is defined on the right, and more importantly, it is different from the usual addition. For example,  $1 + \omega \neq \omega + 1$  and in particular  $1 + \omega = \omega$  as it is  $\text{Sup} \{1 + \beta : \beta < \omega\} = \omega$ .

**Exercise 3.15.** 1. If  $\beta \leq \gamma$ , then  $\alpha + \beta \leq \alpha + \gamma$  (hint: induction on  $\gamma$ )

2. If  $\beta < \gamma$ , then  $\alpha + \beta < \alpha + \gamma$  (hint: use previous and observe that  $\beta < \gamma \Rightarrow \beta^+ \leq \gamma$ ).

**Proposition 3.16.**  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \forall \alpha, \beta, \gamma$ .

*Proof.* Induction on  $\gamma$ .

1. (i) When  $\gamma = 0$ , both sides are  $\alpha + \beta$ .

2. (ii) For successor  $\gamma^+$ , if  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ , we have

$$\begin{aligned}\alpha + (\beta + \gamma^+) &= \alpha + (\beta + \gamma)^+ \\ &= (\alpha + (\beta + \gamma))^+ \\ &= ((\alpha + \beta) + \gamma)^+ \\ &= (\alpha + \beta) + \gamma^+\end{aligned}$$

3. (iii) For non-zero limit  $\lambda$ ,  $(\alpha + \beta) + \lambda = \text{Sup} \{(\alpha + \beta) + \gamma : \gamma < \lambda\}$ , and this is  $\text{Sup} \{\alpha + (\beta + \gamma) : \gamma < \lambda\}$  by induction. Then we need to check firstly that  $\beta + \gamma$  is a limit, as it is  $\text{Sup} \{\beta + \gamma : \gamma < \lambda\}$ . Fix  $\beta$ .,  $\forall \gamma < \lambda$ ,  $\exists \gamma' < \lambda$  s.t.  $\gamma < \gamma'$  so  $\beta + \gamma < \beta + \gamma'$  and so it is a limit.(as it has no maximal element.

Then we have, in one direction,  $\text{Sup} \{\alpha + (\beta + \gamma) : \gamma < \lambda\} \leq \text{Sup} \{\alpha + \delta : \delta < \beta + \lambda\}$  as for each  $\gamma < \lambda$ ,  $\alpha + (\beta + \gamma) \in \{\alpha + \delta : \delta < \beta + \lambda\}$ . On the other hand,  $\text{Sup} \{\alpha + (\beta + \gamma) : \gamma < \lambda\} \geq \text{Sup} \{\alpha + \delta : \delta > \beta + \lambda\}$  as  $\forall \delta < \beta + \lambda$  we have  $\delta \leq \beta + \gamma$  for some  $\gamma < \lambda$ . So  $\alpha + \delta \leq \alpha + (\beta + \gamma)$  Hence,  $\text{Sup} \{\alpha + (\beta + \gamma) : \gamma < \lambda\} = \text{Sup} \{\alpha + \delta : \delta < \beta + \lambda\}$

□

Another viewpoint: Synthetic definition. We can also define addition synthetically as follows:

$\alpha + \beta$  is the order type of disjoint union of  $X$  and  $Y$ , where  $X$  has order type  $\alpha$  and  $Y$  has order type  $\beta$ . Usually, we take the set  $\{(a, b) : a \in X, b = 0 \text{ or } a \in Y, b = 1\}$  with  $(a, b) < (a', b')$  if either  $b = b', a < a'$  or  $b < b'$ .

**Example 3.17.**  $\omega + 1$  has order type  $\mathbb{N} \times \{0\} \cup \{1\} \times \{1\}$ . It is sometimes useful to have a picture in mind:  $\underbrace{X}_{\omega} \sqcup \underbrace{Y}_1$ .

**Proposition 3.18.** *The inductive and synthetic definition of addition coincides.*

*Proof.* Write  $+$  for inductive addition and  $+'$  for synthetic addition. The proof is again using induction on the right, i.e. on  $\beta$

1.  $\beta = 0$  we have  $\alpha + 0 = \alpha$  and  $\alpha +' 0 = \alpha$  because 0 measures the size of empty set.



2. For successor, if  $\alpha + \beta = \alpha +' \beta$  then  $\alpha + \beta^+ = (\alpha + \beta)^+ = (\alpha +' \beta)^+$ . Now consider that  $(\alpha +' \beta)^+$  is the same as  $\alpha +' \beta^+$ . Clearly we have an order isomorphism between them, and we might use the picture:  

$$\underbrace{(\alpha)} \cdot \underbrace{(\beta \cdot 1)} = \underbrace{(\alpha \cdot \beta)} \cdot \underbrace{(1)}.$$

3. For limit,  $\alpha + \lambda = \text{Sup} \{ \alpha + \beta : \beta < \lambda \} = \text{Sup} \{ \alpha +' \beta : \beta < \lambda \}$ . And the later is just  $\alpha +' \lambda$  because the well-orderings  $\alpha +' \beta, \beta < \lambda$  are nested and taking the Sup is the same as taking union of those, which is just  $\alpha +' \lambda$ . To be more precise, it is the union of all initial segments of the form  $I_{\alpha+\beta}, \beta < \lambda$ , which we know exists by previous result.

□

For precise order isomorphism, see the solutions to questions on Tripas paper.

**Remark 3.19.** *As we have shown both definition coincide, sometimes it is much easier to use synthetic definition, e.g. to show  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$  it is much easier to use synthetic definition and the ‘picture’:*

$$\underbrace{(\alpha \cdot \beta)} \underbrace{(\gamma)} = \underbrace{(\alpha)} \underbrace{(\beta \cdot \gamma)}.$$

*To be more precise, consider that  $\alpha + (\beta + \gamma) = \{(a, b) : a \in \alpha, b = 0 \text{ or } a \in \beta + \gamma, b = 1\}$  and  $(\alpha + \beta) + \gamma = \{(a, b) : a \in \alpha + \beta, b = 0 \text{ or } a \in \gamma, b = 1\}$ . And it is easy to check that the map:*

$$f(a, b) = \begin{cases} (a, b) & \text{if } a \in \alpha, b = 0 \text{ or } a \in \gamma, b = 1 \\ (a, 0) & \text{if } a \in \beta, b = 1 \end{cases}$$

*is an order isomorphism.*

### Ordinal multiplication:

**Definition 3.20.** *The inductive ordinal definition is as follows:*

1.  $\alpha \cdot 0 = 0$
2.  $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$
3.  $\alpha \cdot \lambda = \text{Sup} \{ \alpha \cdot \gamma : \gamma < \lambda \}$  where  $\lambda$  is non-zero limit

**Example 3.21.**  $\omega \cdot 2 = \omega \cdot 1 + \omega = \omega + \omega$ . But  $2 \cdot \omega = \text{Sup} \{2 \cdot \beta : \beta < \omega\} = \omega$  and so the ordinal multiplication is Not commutative.

**Definition 3.22.** The synthetic definition of  $\alpha \cdot \beta$  is order type of  $X \times Y$ ,  $X$  with order type  $\alpha$ ,  $Y$  with order type  $\beta$  s.t.  $(a, b) < (c, d)$  if  $b < d$  or  $a < c, b = d$ . Informally, we can consider the picture:  $\uparrow^\beta \alpha$  meaning,  $\beta$  lots of  $\alpha$ .

**Exercise 3.23.** Check the inductive and synthetic definition of multiplication coincide. (hint: induction on  $\beta$ ).

We can similarly define ordinal exponential

**Definition 3.24.** We define  $\alpha^\beta$  as follows:

1.  $\alpha^0 = 1$
2.  $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$
3.  $\alpha^\lambda = \text{Sup} \{\alpha^\beta : \beta < \lambda\}$ ,  $\lambda$  non-zero limit.

Note:  $2^\omega = \text{Sup} \{2^\beta : \beta < \omega\} = \omega$  and so it is countable. (different from usual exponentiation).

The following concept is not in the syllabus but is extremely useful:

**Definition 3.25.** \* A function  $f : ON \rightarrow ON$  is called normal if it is continuous in limit and it is increasing ( $ON$  means the class of ordinals). To be more precise, it is normal if:

1.  $f(\alpha) \leq f(\beta)$  if  $\alpha \leq \beta$ .
2.  $f(\bigcup_{\alpha < \lambda} \alpha) = \bigcup_{\alpha < \lambda} f(\alpha)$  \*.

We will see the use of normal function later.

**Exercise 3.26.** Check that  $f(\alpha) = \alpha + \omega$ ,  $f(\alpha) = \alpha \cdot \omega$ ,  $f(\alpha) = \alpha^\omega$  are all normal functions.

## 4 Posets and Zorn's Lemma

**Definition 4.1.** A partial ordinal set or poset is a pair  $(X, \leq)$  where  $\leq$  is a binary relation on  $X$  satisfying:

1. Reflexive:  $x \leq x \forall x \in X$ .
2. Transitivity:  $x \leq y, y \leq z \Rightarrow x \leq z \forall x, y, z \in X$ .
3. Antisymmetry:  $x \leq y, y \leq x \Rightarrow x = y$ .

Write  $x < y$  if  $x \leq y$  but  $x \neq y$ , and  $x \geq y$  if  $y \leq x$ .

**Example 4.2.**

1. Any total order is poset.
2.  $(\mathbb{N}, |)$  where  $|$  means divides, i.e.  $x \leq y$  if  $x|y$ .
3. For any set  $S$ , take  $X = \mathbb{P}(S)$  and  $A \leq B$  if  $A \subset B$ .
4. Take  $X \subset \mathbb{P}(S)$  and take  $\leq$  as above.
5. Hasse diagram (very useful): It is a graph (c.f. Part II Graph Theory) with vertices satisfying  $a < b$  if  $a$  is adjacent to  $b$  and  $b$  is drawn above  $a$ , and any non-adjacent vertices are unrelated. For example:  
 $\begin{array}{c} a \\ b \end{array} | \begin{array}{c} d \\ c \end{array}$ . We have  $b < a, c < d$  and  $a \& d, b \& c$  are not related.

**Remark 4.3.** In partial ordering, we do not require Trichotomous.

**Definition 4.4.** A subset  $S$  of a poset is a chain if it is total ordered i.e.  $\forall x, y, x \leq y$  or  $y \leq x$ . So in a total order, every subset is a chain.

Note: chain can be uncountable. For example, consider  $(\mathbb{R}, \leq)$ .

**Definition 4.5.** For  $S \subset X$ , an upper bound for  $S$  is  $x \in X$  with  $y \leq x \forall y \in S$ . A least upper bound is in addition  $x \leq z \forall z$  upper bound.

If  $S$  has a least upper bound, we write it to be  $\text{Sup } S$  or  $\vee S$  (sometimes called join of  $S$ ).

**Example 4.6.**

1. In  $(\mathbb{R}, \leq)$ ,  $\mathbb{N}$  has no upper bound.
2. In  $(\mathbb{R}, \leq)$ ,  $\{x : x^2 \leq 2\}$  has an upper bound and a least upper bound  $\sqrt{2}$ .
3. In  $(\mathbb{Q}, \leq)$ ,  $\{x : x^2 \leq 2\}$  has an upper bound but has no least upper bound.
4. In the Hasse diagram above,  $\{a, b, c\}$  has no upper bound as  $b, c$  are unrelated.

**Remark 4.7.**  $\text{Sup}$  may not belong to  $S$ . For example  $\text{Sup } (0, 1) = 1$  but  $1$  is not in  $(0, 1)$ .

**Definition 4.8.** A poset is complete if every subset has a  $\text{Sup}$  which lies in the poset.

**Example 4.9.**

1.  $(\mathbb{R}, \leq)$  is not complete.
2.  $[0, 1]$  is complete.
3.  $[0, 1)$  is not complete.
4.  $\mathbb{P}(S)$  is always complete, as we just take the unions of any given subsets of  $\mathbb{P}(S)$ .

**Remark 4.10.** If  $X$  is complete, then  $X$  has a greatest element. Also it has a least element because the least element is the  $\text{Sup}$  of the empty set in  $X$ .

**Definition 4.11.** For a poset  $X$ , a function  $f : X \rightarrow X$  is order-preserving if  $f(x) \leq f(y)$  whenever  $x \leq y$ .

**Example 4.12.**

1.  $f(x) = x + 1$  on  $\mathbb{N}$ .

2.  $f(x) = \frac{x}{2}$  on  $(0, 1)$ .

3.  $f(x) = \frac{1+x}{2}$  on  $(0, 1)$ .

4.  $f(A) = A \cup \{i\}, i \in S$ , where  $X = \mathbb{P}(S)$ .

**Theorem 4.13. [Knaster-Tarski Fixed Point Theorem]** Let  $X$  be a complete poset, then any order-preserving function has a fixed point.

*Proof.*  $S = \{x \in X : x \leq f(x)\}$  Let  $c = \text{Sup}S$ , and  $c \in X$  because  $X$  is complete We check that  $c$  is the fixed point, and we do it in two steps.

Step(i):  $c \leq f(c)$ , and to show this, as  $c$  is the least upper bound, it is enough to show that  $f(c)$  is an upper bound. Indeed, take any  $x \in S, x \leq c$  so  $f(x) \leq f(c)$ . But  $x \leq f(x)$  in  $S$  and so  $x \leq f(c)$ . Hence  $f(c)$  is an upper bound.

Step(ii):  $f(c) \geq c$ . To show this, it suffices to show that  $f(c) \in S$ .  $c \leq f(c)$  and so  $f(c) \leq f(f(c))$  as  $f$  is order-preserving. Therefore,  $f(c) \in S$ .

Combining both steps, we conclude that  $c = f(c)$ . □

We have some immediate consequences and applications of the theorem:

**Corollary 4.14. [Cantor-Berstein]** Let  $A, B$  be sets s.t.  $\exists f : A \rightarrow B, g : B \rightarrow A$ , where  $f, g$  both injections. Then there is a bijection from  $A$  to  $B$ .

*Proof.* We want to write  $A = P \sqcup Q$ , and let  $R = f(P), S = g^{-1}(Q)$  and define a function:

$$h(A) = \begin{cases} f(A) & \text{on } P \\ g^{-1}(A) & \text{on } Q \end{cases}$$

and as  $f, g$  both injections, so the function  $h$  defined above is a bijection if  $R \sqcup S = B$ , and it is enough to find some  $P \subset A$  s.t.  $A \setminus g(B \setminus f(P)) = P$ .

Let  $\theta : \mathbb{P}(A) \rightarrow \mathbb{P}(A)$  by  $\theta(P) = A \setminus g(B \setminus f(P))$ , we check  $\theta$  is order-preserving and as  $\mathbb{P}(A)$  is complete, use the theorem, we can find a fixed point. Let

$P \subset Q$ , then  $f(P) \subset f(Q)$  and so  $g(B \setminus f(Q)) \subset g(B \setminus f(P))$ . And hence  $A \setminus g(B \setminus f(P)) \subset A \setminus g(B \setminus f(Q))$  and so it is order-preserving. Hence  $P$  is fixed and let  $Q = A \setminus P$ .  $\square$

## Zorn's Lemma

**Definition 4.15.** *An element  $x$  of a poset  $P$  is maximal if there does not exist  $y \in P$  s.t.  $x < y$ .*

Many posets have no maximal elements, e.g.  $\mathbb{N}, \mathbb{R}, \mathbb{Q}$ .

**Theorem 4.16. [Zorn's Lemma]** *Let  $X$  be a non-empty poset s.t. every chain has an upper bound. Then there exists a maximal element.*

*Proof.* Suppose  $X$  has no maximal element. Then for each  $x \in X$  we have some  $x' > x$ . And we also assume that each chain  $C$  has an upper bound, say  $u(C)$ .

By Hartog's Lemma, let  $\gamma = \gamma(X)$ .

Fix  $x \in X$ . Define  $x_\alpha, \alpha < \gamma$  inductively as:

$$x_0 = x.$$

$$x_{\alpha+} = x'_\alpha. \text{ (for some } x'_\alpha > x_\alpha \text{)}$$

$$x_\lambda = u(\{x_\alpha : \alpha < \lambda\}) \text{ for } \lambda \text{ a non-zero limit.}$$

Then we have an injection from  $\gamma$  to  $X$ , which is a contradiction.  $\square$

Note: The proof seems easy but it does require a lot of knowledge of Chapter 3, including Hartog's Lemma. Applications:

**Theorem 4.17.** *Every vector space has a basis.*

*Proof.* Let  $V$  be a vector space. We want to apply Zorn's Lemma. Let  $X = \{\text{linearly independent sets}\}$  ordered by inclusions. So  $X$  is a poset. Given any chain  $\{A_i : i \in I\}$ , take  $A = \bigcup_{i \in I} A_i$ . We check that  $A$  is an upper bound. Firstly, we check  $A \in X$ . Suppose not, i.e.  $A$  is linearly dependent, then as linearly dependence is a finite concept, we must have  $\exists \lambda_i, \sum_{i=1}^n \lambda_i x_i = 0$  for some  $x_i \in A$ , where  $\lambda_i \neq 0$ . WLOG, let  $x_j \in A_{i_j}$  and let  $i_k = \max\{i_j\}$ . So the set  $A_{i_k}$  is linearly dependent, which is a contradiction. And also as we take  $A$  to be the union, so it is clearly an upper bound. Hence by Zorn's Lemma, we have a maximal element in  $X$ , say  $P$ . Suppose  $P$  does not span  $X$ , then  $\exists x \in V$ , s.t.  $P \cup \{x\}$  is linearly independent, which contradicts  $P$  being maximal. Therefore,  $P$  is a basis.  $\square$

**Theorem 4.18.** *Let  $S \subset L(P)$  for any  $P$ . Then  $S \not\vdash \perp \Rightarrow S \not\equiv \perp$ .*

*Proof.* Seek consistent  $\bar{S} \supset S$  s.t.  $\forall t \in L, t \in \bar{S}$  or  $\neg t \in \bar{S}$ .

Then we set:

$$v(t) = \begin{cases} 1 & \text{if } t \in S \\ 0 & \text{if } t \notin S \end{cases}$$

We will find a maximal consistent  $\bar{S} \supset S$ , and then we are done, because if  $t \notin \bar{S}$ , then  $S \cup \{t\} \vdash \perp$  because  $\bar{S}$  is maximal.

By Deduction theorem  $\bar{S} \vdash \neg t$  and  $\neg t \in S$ , because if not, then  $\bar{S} \cup \neg t$  is still consistent.

Now let  $X = \{T \subset L(P) \text{ s.t. } T \not\vdash \perp, T \supset S\}$  ordered by inclusion. Given a chain  $\{T_i : i \in I\}$ , let  $T = \bigcup_{i \in I} T_i$ .

Suppose  $T \vdash \perp$  then by as proof is finite, so some  $T_k \vdash \perp$ , which is a contradiction. And as we take the union,  $T$  is an upper bound. Therefore, by Zorn's Lemma, we have a maximal element.  $\square$

**Theorem 4.19. [Well-ordering Theorem]** *Every set  $S$  can be well-ordered.*

*Proof.*  $X = \{(A, R) : A \subset S, R \text{ is a well-ordering of } A\}$

It is ordered by:  $(A, R) \leq (A', R')$  if  $(A', R')$  extends  $(A, R)$ .

Then  $X \neq \emptyset$  because  $(\emptyset, \emptyset) \in X$ .

Given a chain  $\{(A_i, R_i) : i \in I\}$ , we have that  $(A_i, R_i)$  are nested, which is same as in Chapter 2. So  $(\bigcup_{i \in I} A_i, \bigcup_{i \in I} R_i)$  is a well-ordering extending  $(A_i, R_i)$ , and so it is an upper bound.

Hence by Zorn's Lemma, it has a maximal element, say  $(A, R)$ . If  $A \neq S$ , then let  $x \in S \setminus A$ , define  $(A \cup \{x\}, R')$  as  $(A, R)$  plus  $y < x \forall y \in A$ , which contradicts  $(A, R)$  being maximal. So  $A = S$ .  $\square$

**Remark 4.20.** *Surprisingly,  $\mathbb{R}$  can be well-ordered.*

## Zorn's Lemma and Axiom of Choice

In the proof of Zorn's Lemma, we used that for each  $x \in X, \exists x' > x$ .

There might be infinitely many choices. We did the same thing in the proof of countable union of countable set being countable.

Axiom of Choice says that we can pick an element for each of a family  $\{A_i : i \in I\}$  of non-empty sets. More precisely, it states: every family  $\{A_i : i \in I\}$  of non-empty sets has a choice function, meaning a function

$$f : I \rightarrow \bigcup_{i \in I} A_i \quad f(i) \in A_i \quad \forall i.$$

This is a different nature of the other set-building rules in that the object whose existence is being asserted is NOT specified uniquely by its properties. So it is often in interest, to know whether a proof uses AC or not. Note: AC is trivial if we have only one set  $A_1$  and similarly, for  $A_1 \cup A_2$ , choose  $x \in A_1, y \in A_2$ , and hence for any finite  $I$ .

But it turns out that for general  $I$ , we cannot deduce AC from the other set-building rules. And we DID use AC to prove Zorn's Lemma. But conversely, we can also deduce AC from Zorn's Lemma, because the Well-Ordering Theorem implies AC (pick the least element in each set).

**Remark 4.21.** *Usually given a counter intuitive consequence of Zorn's Lemma or Well-Ordering Theorem or Axiom of Choice, one finds that either it is not counter intuitive or one can prove that at least as counter intuitive statement without using these.*

A notation related to completeness:

**Definition 4.22.** *A poset  $X$  is chain-complete if  $X \neq \emptyset$ , and every chain has a Sup.*

**Theorem 4.23.** *Any inflationary function in a chain-complete  $X$  has a fixed point.*

It follows immediately from Zorn's Lemma, pick the maximal element. But, in fact we can prove it without using AC (and hence no Zorn's Lemma). Because this time, we don't need to 'choose'  $x' > x$ , we have instead that  $f(x) \geq x$  and so  $x_0, f(x_0), f(f(x_0)) \dots$  for a fixed  $x_0$ . We can deduce Zorn's Lemma by this and AC, and so this is a AC free version of Zorn's Lemma.

## 5 Predicate Logic

Recall a group, consisting of a set  $A$  and some functions  $M_A$  of arity 2 ( $M_A : A^2 \rightarrow A$ ),  $i_A$  of arity 1,  $i_A : A \rightarrow A$ , and a constant  $e_A$  of arity 0.  $e_A : A^0 \rightarrow A$ . These functions satisfy the followings:

1.  $\forall x, y, z \in A, M_A(x, M_A(y, z)) = M_A(M_A(x, y), z)$ .
2.  $\forall x, M_A(e_A, x) = x$ .
3.  $\forall x, M_A(i_A(x), x) = e_A$ .



A poset is a set  $A$  equipped with a relation  $\leq_A$  of arity 2, meaning  $\leq_A$  is a relation on two things, satisfying some rules.

Overview of the set up:

Language: e.g. Language of groups, things like 1,2,3 above.

Valuation: A set equipped with functions and the relations of given arities.

Models of  $S$ : A structure in which all of  $S$  is true.

$S \models t$ : e.g.  $\{1, 2, 3\} \models M_A(e_A, e_A) = e_A$ .

$S \vdash t$ : see later.

Let  $\Omega$  and  $\Pi$  be disjoint sets and let  $\alpha : \Omega \sqcup \Pi \rightarrow \mathbb{N}$  the language  $L : L(\Omega, \Pi, \alpha)$  consists of formulae defined by variables.

terms: defined inductively by:

1. every variable is a term.
2. for  $f \in \Omega$ , say  $\alpha(f) = n$  and terms  $t_1 \dots t_n$ , then  $ft_1 \dots t_n$  is a term. e.g. Language of groups  $\Omega = (M, i, e), \Pi = \emptyset, \alpha(M) = 2, \alpha(i) = 1, \alpha(e) = 0$ .  $M(x_1, x_2), M(e, M(e, e)), M(x, e)$  are terms.

Atomic formulae:

1.  $\perp$  is an atomic formulae.
2.  $(s = t)$  is an atomic formulae for any terms  $s, t$ .
3. For  $\emptyset \in \Pi$ , say  $\alpha(\emptyset) = n$ , and terms  $t_1 \dots t_n$  have atomic formulae  $\emptyset t_1 \dots t_n$ .

**Example 5.1.** *Language of Posets.*  $\Omega = \phi, \Pi = \{\leq\}, \leq$  has arity 2.

$(x_1 = x_2), (x_1 \leq x_2)$  are atomic formulae.

Formally, we shall write  $\leq x_1 x_2$  instead of  $x_1 \leq x_2$ .

Formulae: it is defined inductively by:

1. Every atomic formulae is a formulae.
2. If  $p, q$  are formulaes, so is  $(p \Rightarrow q)$ .
3. If  $p$  is a formulae,  $x$  is variable, then  $(\forall x)p$  is a formulae.

**Example 5.2.** *Language of groups:*

$$(\forall x_1)(\forall x_2)(M(x_1, x_2) = M(x_2, x_1)).$$

$$(\exists y)(M(y, y) = x).$$

$$(\forall x)(M(x, x) = e) \Rightarrow (\exists y)(M(y, y) = x).$$

**Remark 5.3.**

1. A formulae is a string of symbols.

2. We write  $\neg p$  for  $p \vdash \perp$  and similarly for  $p \vee q, p \wedge q$ , and  $(\exists x)p$  for  $\neg(\forall x)(\neg p)$ .

**Definition 5.4.** *We say a term is closed if it contains no variables*

e.g. In language of groups,  $e, M(e, M(e, e))$  are closed but  $M(x_1, i(x_1))$  is not.

Note: we just consider the symbols, we don't know  $M(x, i(x)) = e$  yet.

**Definition 5.5.** *An occurrence of a variable in formulae  $p$  is called a bound if it is within the bracket of a  $\forall x$  quantifier, otherwise, it is called free.*

**Example 5.6.**

1.  $(\forall x)(M(x, x) = e)$  is bound.

2.  $(\exists y)(M(y, y) = e)$  is bound. (Remember the definition of  $\exists$ ).

3.  $\underbrace{(M(x, x) = e)}_{\text{free}} \Rightarrow \underbrace{(\forall x)(\forall y)(M(x, y) = M(y, x))}_{\text{bound}}$ .

**Definition 5.7.** *A sentence is a formulae with no free variable.*

**Example 5.8.**  $(\forall x)(M(x, x) = e) \Rightarrow (\exists y)(M(y, y) = x)$ .

$(\forall x)(M(x, e) = x)$ .

**Definition 5.9.** *For a formulae  $p$ , a variable  $x$  and a term  $t$ , we write  $p[t/x]$  for the substitution obtained by  $t$  replacing each free occurrence of  $x$  with  $t$ .*

e.g. If  $p$  is  $(\exists y)(M(y, y) = x)$   $p[e/x]$  is  $(\exists y)(M(y, y) = e)$ .

## Semantic entailment

For language,  $L = (\Omega, \Pi, \alpha)$ , an  $L$ -structure is a non-empty set  $A$ , equipped with:

1. For each  $f \in \Omega$ , say  $\alpha(f) = n$ , a function  $f_A : A^n \rightarrow A$ .
2. For each  $\phi \in \Pi$ , say  $\alpha(\phi) = n$ , a subset  $\phi_A \subset A^n$ .

e.g.  $L$ =language of groups, an  $L$ -structure is non-empty set  $A$ , with functions  $M_A : A^2 \rightarrow A, i_A : A \rightarrow A, e_A : A^0 \rightarrow A$ .

For a sentence in  $p$ , we want to define what  $p$  holds in  $A$ . e.g.  $(\forall x)(M(x, x) = e)$  holds in  $A$  if and only if for every  $a \in A$ ,  $M_A(a, a) = e_A$ . So insert  $\in A$  after each  $\forall x$  and for subscript  $A$  to each function symbol and relation symbol.

Formally, define  $t_A$  for each closed term  $t$  inductively by for  $f \in \Omega$  say arity  $\alpha(f) = n$  and closed terms  $t_1 \dots t_n$ ,  $(ft_1 \dots t_n)_A = f_A(t_{1A} \dots t_{nA})$ . e.g.:  $M(e, M(e, e))_A = M_A(e_A, M_A(e_A, e_A))$ .

Note: For  $c$  a constant,  $c_A$  is already defined.

Now define the interpretation  $p_A$  of a sentence  $p$  inductively by:

1.  $\perp_A = 0$ .
2. For closed terms  $s, t$ ,

$$(s = t)_A = \begin{cases} 1 & \text{if } s_A = t_A \\ 0 & \text{otherwise} \end{cases}$$

- 3.

$$(p \Rightarrow q) = \begin{cases} 0 & \text{if } p_A = 1, q_A = 0 \\ 1 & \text{otherwise} \end{cases}$$

4. For  $\phi \in \Pi$ ,  $\alpha(\phi) = n$  closed terms  $t_1 \dots t_n$ ,

$$(\phi t_1 \dots t_n)_A = \begin{cases} 1 & \text{if } (t_{1A} \dots t_{nA}) \in \phi_A \\ 0 & \text{otherwise} \end{cases}$$

5.

$$((\forall x)p)_A = \begin{cases} 1 & \text{if } p(\bar{a}/x)_A = 1 \text{ for each } a \in A \\ 0 & \text{otherwise} \end{cases}$$

where for a given  $a \in A$ , we add a constant to  $L$ , called  $\bar{a}$ , and make  $L$  into an  $L'$  structure by setting  $\bar{a}_A = a$ . The reason for that is we don't want free variables in  $p$ , but constant is free.

We can also define  $p_A$  for  $p$  having free variables. e.g. If  $p$  is  $M(x, x) = e$  then  $p_A = \{a \in A : M_A(a, a) = e_A\}$ . If  $p_A = 1$ , say  $p$  holds in  $A$  or  $p$  is true in  $A$  or  $A$  is a model of  $P$ . For a theory (set of sentences)  $S \subset L$ , say that  $A$  is a model of  $S$  if  $p_A = 1 \forall p \in S$ . Say  $S$  entails  $p$  (some theory  $S$  and some sentence  $p$ ), written  $S \models p$  if every model of  $S$  is a model of  $p$ . We have a look at some concrete examples below:

**Example 5.10.**

1. *Groups:  $L$ =Language of groups.*

*Let  $T$  be the theory, which is:*

$$(i) (\forall x)(\forall y)(\forall z)M(x, (M(y, z))) = M(M(x, y), z).$$

$$(ii) (\forall x)(M(x, e) = X \wedge M(e, x) = X).$$

$$(iii) : (\forall x)(m(x, i(x)) = e \wedge m(i(e), e) = e).$$

*Then an  $L$ -structure is a model of  $T$  if and only if it is a group in usual sense.*

2. *Fields:  $L$ =Language of field. We have  $+$ ,  $\cdot$ ,  $0$ ,  $1$ ,  $-$  with arities  $2, 2, 0, 0, 1$  respectively.*

*Let  $T$  be the theory, which is:*

(i) Abelian group under  $+$ , with identity  $0$ .

(ii) distributive over  $+$ .

(iii) commutative.

(iv)  $(\forall x)(1 \cdot x = x)$ .

(v)  $\neg(0 = 1)$ .

(vi)  $(\forall x)(\neg(x = 0)) \Rightarrow ((\exists y)(x \cdot y = 1))$ .

Then an  $L$ -structure is a model of  $T$  if and only if it is a field.

3. Theory of Graph:  $L =$  One predicate symbol, with a single function  $a$  of arity 2.

Let  $T$  be the theory, which is:

(i)  $\neg a(x, x)$ .

(ii)  $(\forall x)(\forall y)(a(x, y) \Rightarrow a(y, x))$ .

$a$  means adjacent, and so this is a theory of graph. (c.f. Part II Graph Theory).

Note: In the second one, we have  $T \models$  'inverse is unique'. i.e.  $(\forall x)(\neg(x = 0)) \Rightarrow ((\forall y)(\forall z)((x \cdot y = 1 \wedge x \cdot z = 1) \Rightarrow (y = z)))$ .

## Syntactic entailment

We have the following axioms:

1.  $p \Rightarrow (q \Rightarrow p)$ .

2.  $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ .

3.  $\neg\neg p \Rightarrow p$ .

4.  $(\forall x)(x = x)$  for any variable  $x$ .
5.  $(\forall x)(\forall y)((x = y) \Rightarrow (p \Rightarrow p[y/x]))$  for any  $p, x, y$  with  $y$  not bound in  $p$ .
6.  $(\forall x)p \Rightarrow p[t/x]$  for any formulae  $p$ , variable  $x$ , term  $t$  with no free variable of  $t$  bound in  $p$ .
7.  $[(\forall x)(p \Rightarrow q)] \Rightarrow [p \Rightarrow (\forall x)q]$  for any formulae  $p, q$ , variable  $x$  not occurring free in  $p$ .

deduction rules:

1. MP: From  $p, p \Rightarrow q$ , we can deduce  $q$ .
2. Generalisation(Gen): From  $p$  we can deduce  $(\forall x)p$  provided that  $x$  does not occur free in any premises used.

**Definition 5.11.** *A proof of  $p$  from  $S$  ( $p$  any formulae,  $S$  any set of formulae) is a finite sequence of a member of  $S$  or a logic axiom or obtained by earlier lines by deduction rules. If such proof exists, we say  $S$  proves  $p$ , written  $S \vdash p$ .*

**Remark 5.12.** *Each axiom is a tautology (i.e. True in every  $L$ -structure).*

Note of  $\emptyset$ : Suppose we allow the empty set as a structure (for a language with no constant). Then in that structure,  $(\forall x)\perp$  holds. But  $\perp$  does not hold. Then we have  $((\forall x)\perp) \models \perp$  does not hold, but this is an instant of axiom 6.

**Example 5.13.**  $\{x = y, x = z\} \vdash y = z$ .

1.  $(\forall x)(\forall y)(x = y) \Rightarrow ((x = z) \Rightarrow (y = z))$  by  $A_5$ .
2.  $(\forall x)(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z))) \Rightarrow ((\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z))))$  by  $A_6$ .
3.  $(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$  by MP.

4.  $(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z))) \Rightarrow ((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$  by  $A_6$ .

5.  $(x = y) \Rightarrow ((x = z) \Rightarrow (y = z))$  by MP.

6.  $(x = z) \Rightarrow (y = z)$  by MP.

7.  $y = z$  by MP.

**Proposition 5.14. [Deduction rule]**  $S \subset L, p, q \in L. S \vdash (p \Rightarrow q)$  if and only if  $S \cup \{p\} \vdash q$ .

*Proof.*  $\Rightarrow$  As for propositional logic, we have  $S \cup \{p\} \vdash p$  and  $S \cup \{p\} \vdash (p \Rightarrow q)$ . So  $S \cup \{p\} \vdash q$ .

$\Leftarrow$  As for propositional logic, the only new case is that in proof of  $q$  from  $S \cup \{p\}$  we have possibly  $(\forall x)r(\text{Gen})$ . and have a proof of  $p \Rightarrow r$  from  $S$ .

We again use induction, suppose we have seen a proof of  $p \Rightarrow (\forall x)r$  from  $S$ , and so in proof of  $r$  from  $S \cup \{p\}$ , no hypothesis used had  $x$  free and hence also in our proof of  $p \Rightarrow r$  from  $S$ , no hypothesis used had  $x$  free. Thus  $S \vdash (\forall x)(p \Rightarrow r)(\text{Gen})$ . If  $x$  is not free in  $p$ , get  $S \vdash (p \Rightarrow (\forall x)r)$  by  $A_7$ . If  $x$  is free in  $p$ , the proof of  $r$  from  $S \cup \{p\}$  cannot use  $p$  and so  $S \vdash r$  hence  $S \vdash (\forall x)r(\text{Gen})$  and so  $S \vdash (p \Rightarrow (\forall x)r)$  by  $A_1$  and use MP.

□

**Theorem 5.15. [Completeness Theorem]**  $S \models p$  if and only if  $S \vdash p$ .

Again we do it in two steps:

**Proposition 5.16. [Soundness]** Let  $S$  be a set of sentences,  $p$  a sentence, then if  $S \vdash p, S \models p$ .

*Proof.* We want to show any models of  $S$  is a model of  $p$ . This is an easy induction on the lines of proof of  $p$  from  $S$  and details are left as an exercise.

□

**Theorem 5.17. [Adequacy]** Let  $S \subset L$  be consistent, then  $S$  has a model.

Before we prove this, we need the following concept:

**Definition 5.18. [Witness]** For each sentence in  $S$ , add a new constant  $c$  and add to  $S$  the sentence  $p[c/x]$ , we call this Witness.

*Proof.*  $S$  is consistent  $L = L(\Omega, \Pi)$ . Extend  $S$  to  $S_1$  maximal consistent by Zorn's Lemma. Then  $S_1$  is complete, i.e. for  $p \in L$ ,  $S_1 \vdash p$  or  $S_1 \vdash \neg p$ . For each  $(\exists x)p \in S_1$ , add a constant to  $L$ , and sentence  $p[c/x]$  to  $S_1$ , we obtain a set  $T_1$  in language  $L_1 = L(\Omega \cup c_1, \Pi)$ . It is easy to check that  $T_1$  is consistent. Now extend  $T_1$  to maximal consistent, get  $S_2$  and add witness to  $S_2$  to obtain  $T_2$ , and get corresponding  $L_2$ . Continue this inductively as above and let  $\mathcal{S} = S_1 \cup S_2 \cup \dots$ , and  $\mathcal{L} = L(\Omega \cup c_1 \cup \dots, \Pi)$ .

Claim:  $\mathcal{S}$  is consistent and complete and has witness.

Proof of claim:

Consistency: If  $\mathcal{S} \vdash \perp$ , then  $\mathcal{S} = S_1 \cup S_2 \dots$  and as proof is finite, we have some  $S_M \vdash \perp$  which is a contradiction.

Complete: For  $p \in \mathcal{L}$ , we have  $p \in L_n$  for some  $n$  because sentence is finite and  $p \in S_{n+1}$  or  $\neg p \in S_{n+1}$  by definition of  $S_{n+1}$ .

Witness: If  $(\exists x)p \in \mathcal{S}$ , then  $(\exists x)p \in S_n$  for some  $n$  and so  $p[c/x] \in \mathcal{S}$  for some constant  $c$ .

On closed term of  $L$ , define  $\sim$  by  $S \sim t$  if  $S \vdash (s = t)$ . Clearly is an equivalence relation. Let  $A$  be the set of equivalence classes, for  $f \in \Omega$  define  $f_A((t_1) \dots (t_n)) = [ft_1 \dots t_n]$ . For  $\phi \in \Pi$ , define  $\phi_A = \{[(t_1) \dots (t_n)] \in A_n\} \vdash \phi t_1 \dots t_n$ . Claim for any  $p \in \mathcal{L}$ ,  $p \in \mathcal{S}$  if and only if  $p$  holds in  $A$ .

Proof of the claim: Induction

Atomic case: Set  $\mathcal{S} \vdash (s = t) \iff [s] = [t]$ .

$s_n = t_n, (s = t)_A = 1$ .

same for  $\phi t_1 \dots t_n$ .

for  $\perp$ :  $\perp \notin \mathcal{S}$  and  $\perp_A = 0$ .

Now for induction step  $p \Rightarrow q$ :  $\mathcal{S} \vdash (p \Rightarrow q) \iff \mathcal{S} \vdash \neg p$  or  $\mathcal{S} \vdash q$ . If  $\mathcal{S} \not\vdash \neg p, \mathcal{S} \not\vdash q$  then  $\mathcal{S} \vdash p, \mathcal{S} \vdash \neg q$  and so  $\mathcal{S} \vdash \perp$  which is a contradiction. So  $p_A = 0$  or  $q_A = 1$  by induction and so  $(p \Rightarrow q)_A = 1$ .

$(\exists x)p$ :  $\mathcal{S} \vdash (\exists x)p \iff \mathcal{S} \vdash p[t/x]$  for some closed term  $t$ . We have witness, so  $p[t/x] = 1$  and so  $(\exists x)p$  holds in  $A$ .

Now we define the same valuation as in Chapter 1. □

**Remark 5.19.** If the language is countable then we don't need Zorn's Lemma. The word 'first-order' means our variables run over elements of the structure.

**Corollary 5.20.** Let  $S$  be a theory s.t. every finite subset has a model, then  $S$  has a model.

*Proof.* This is trivial if we replace  $\vdash$  by  $\models$ . □

Note: We don't have dedicate theorem because we cannot check  $S \models p$ .



**Proposition 5.21.** *The class of finite group is not axiomatisable.*

*Proof.* Suppose  $S$  axiomatises finite groups. Then we add to  $S$  by:

$(\exists x_1)(\exists x_2)(x_1 \neq x_2)$  (This says we have group of order  $\geq 2$ ).

$(\exists x_1)(\exists x_2)(\exists x_3)(x_1, x_2, x_3 \text{ distinct})$

.

.

.

Then  $S'$  has no model, but every finite subset of  $S'$  has a model, which contradicts the corollary.  $\square$

The same proof shows that:

**Theorem 5.22.** *Let  $S$  be a theory having arbitrarily large finite model, then  $S$  has an infinite model.*

**Theorem 5.23. [Upward Lowenheim–Skolem Theorem]** *Let  $S$  be a theory which has an infinite model, then  $S$  has an uncountable model.*

*Proof.* Form a new language  $L'$  from  $L$  by adding uncountably many constants,  $(c_i : c_u \in I)$

Let  $S' = S \cup \{c_i \neq c_j : i, j \in I\}$ . Then every finite subset of  $S'$  has a model, as it can only mention finitely many  $c_i$ . So any infinite model of  $S$  will do. Then by compactness,  $S'$  has a model.  $\square$

**Theorem 5.24. [Downward Lowenheim–Skolem Theorem]** *Let  $S$  be a theory, if  $S$  has a model, then it has a countable model.*

*Proof.*  $S$  is consistent. So the model constructed previously is countable.  $\square$

## Peano Arithmetic

We try to make the usual axioms for  $\mathbb{N}$  into a first-order theory.  $\Omega = \{0, S, +, \times\}, \Pi = \phi$ .

1.  $(\forall x)(\forall y)((S(x) = S(y)) \Rightarrow (x = y))$  where  $S(x)$  means the successor of  $x$ .
2.  $(\forall x)(\neg(0 = S(x)))$ .

3.  $(\forall y_1)(\forall y_2) \dots (\forall y_n) \{p[0/x] \wedge (\forall x)(p \Rightarrow p[S(x)/x])\} \Rightarrow (\forall x)p$ . Here  $y_i$ 's are parameters.
4.  $(\forall x)(x + 0 = x)$ .
5.  $(\forall x)(\forall y)(x + S(y) = S(x + y))$ .
6.  $(\forall x)(x \times 0 = 0)$ .
7.  $(\forall x)(\forall y)(x \times S(y) = (x \times y) + x)$ .

This is called Peano Arithmetic.

**Remark 5.25.** *For the parameters in the third axiom, one's first guess would be the same without parameters, but then we are missing the sets like  $\{x : x \geq y\}$  for some fixed  $y$ .*

Now, PA (Peano Arithmetic) has an infinite model, which is  $\mathbb{N}$  and so by theorem it has an uncountable model, and so this model is not isomorphic to  $\mathbb{N}$ . Also the third axiom is not full induction (for all subset of our structure), and even in  $\mathbb{N}$ , this can only refer to any countably many subsets.

**Theorem 5.26. [Incompleteness theorem]** *PA is not complete. (Non-examinable).*

Conclusion:  $\exists p$ , true in  $\mathbb{N}$  but  $PA \not\vdash p$ . This is not contradicting completeness because there are lots of structures for PA. So ' $p$  is true in  $\mathbb{N}$ ' is not necessarily true in every model of PA.

## 6 Set Theory

Key idea: View the set theory as just another first-order theory.

ZF (Zermelo–Frankel set theory). Language of ZF:  $\Omega = \phi$ ,  $\Pi = \{\in\}$  where  $\in$  has arity 2. We have the following axioms:

1. Axiom of extension: Informally, it says if two sets have the same member, then they are the same. Mathematically, it says  $(\forall x)(\forall y)[(\forall z)(z \in x \iff z \in y) \Rightarrow (x = y)]$ .

2. Axiom of separation: Informally, it says that we can form subset. Mathematically, it says  $(\forall y_1) \dots (\forall y_n)(\forall x)(\exists y)(\forall z)((z \in y) \Rightarrow (z \in x \wedge p(z)))$  for some first-order predicate  $p$ .
3. Empty-Set Axiom: Informally, it says that there is an empty set. Mathematically, it says  $(\exists x)(\forall y)(\neg y \in x)$ . and we write  $\emptyset$  for the set.  $p(\emptyset)$  is abbreviation for  $(\exists x)(\forall y)((\neg y \in x) \wedge p(x))$ .
4. Pair-Set Axiom: Informally, it says that we can form the set  $\{x, y\}$  from  $x, y$ . Mathematically, it is  $(\forall x)(\forall y)(\exists z)(\forall t)(t \in z \iff t = x \vee t = y)$ . Write  $\{x, y\}$  for the abbreviation, and write  $\{x\}$  for  $\{x, x\}$ , and  $(x, y)$  for  $\{\{x\}, \{x, y\}\}$ . We can check that  $(x, y) = (t, u)$  if and only if  $x = t$  and  $y = u$ . We say  $x$  is an ordered pair if  $(\exists y)(\exists z)(x = (y, z))$ . Say  $f$  is a function if  $(\forall x)(x \in f \iff x \text{ is an ordered pair}) \wedge (\forall x)(\forall y)(\forall z)((x, y) \in f \wedge ((x, z) \in f \Rightarrow (y = z)))$ . Say domain of  $f$  is  $x$  if  $(f \text{ is a function}) \wedge (\forall y)((y \in x) \Rightarrow (\exists z)(y, z) \in f)$ . Say  $f : x \rightarrow y$  is  $(f \text{ is a function}) \wedge (\text{domain is } x) \wedge (\forall z)(\exists t)((t, z) \in f \Rightarrow (z \in y))$ .
5. Union Axiom: Informally, it says that we can form union of the set. Mathematically,  $(\forall x)(\exists y)(\forall z)((z \in y) \iff (\exists t)(z \in t \wedge t \in x))$ , and we call this set  $\bigcup x$ . Note that there is no need to axiomatise intersection, as it is a subset and we use axiom of separation.
6. Power Set Axiom: Informally, this says that we can form power set of a given set. Mathematically,  $(\forall x)(\exists y)(\forall z)((z \in y) \iff (z \subset x))$ , where  $z \subset x$  means that  $(\forall t)((t \in z) \Rightarrow (t \in x))$ . The Cartesian product  $X \times Y$  is a subset of  $\mathbb{P}(\mathbb{P}(X \cup Y))$ , so we are able to define the Cartesian product. And we can also form the set of all functions from  $x$  to  $y$  as a subset of  $\mathbb{P}(x \times y)$ .
7. Axiom of Infinity: Informally, this says that there exists an infinite set. Mathematically, we say a set is successor set if  $(\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x))$ . Axiom of infinity says  $(\exists x)(x \text{ is a successor set})$ . As any intersection of successor set is a successor set, then there exists a least one. We call this set  $\omega$ , the copy of natural number inside the universe.  $(\forall x \subset \omega)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x))) \Rightarrow x = \omega$ . Note we can also show  $(\forall x)(\neg(0 = x^+))$  and  $(\forall x, y \in \omega)((x^+ = y^+) \Rightarrow (x = y))$ .

8. Axiom of Foundation: We want to ban  $x \in x$  and  $(x \in y) \wedge (y \in x)$ . Also ban  $x_0, x_1 \dots x_1 \in x_0, x_2 \in x_1 \dots$ . So informally we want to say every non-empty set has a  $\in$  lest element. Mathematically,  $(\forall x)(x \neq \emptyset) \Rightarrow (\exists y)((y \in x) \wedge (\forall z \in x)(\neg z \in y))$ .
9. Axiom of Replacement: Often in maths, we have sets  $a_i$  for each  $i \in I$  and sometimes we say  $\{a_i : i \in I\}$  but why should this be a set? It feels like the image of the function  $i \rightarrow a_i$ . But why should this be a function or even a set. So we want: the image of a set under something which looks like a function is a set.

Before explaining the formal bit of Replacement, we introduce the following concept:

**Definition 6.1.** For a given  $(V, \in)$ , a class  $C$  is a collection of points of  $V$  s.t. for some formulae  $p$ , free variable  $x$  (and maybe more), we have  $x \in C \iff p(x)$  holds.

**Example 6.2.** 1.  $V$  is a class, we take  $p$  to be  $x = x$ .

2. For any  $t \in V$ ,  $\{x : t \in x\}$  is a class and we take  $p$  to be  $t \in x$ .

**Definition 6.3.** We call  $C$  a proper class if it is not a set in  $V$ .  $\neg(\exists y)(\forall x)((x \in y) \iff p)$ .

e.g.  $V$  is a proper class since  $\neg(v \in v)$ .

For functions, the idea is  $x \rightarrow \{x\}$  looks like a function, but it is not even a set. A function class is a collection  $C$  of ordered pairs  $(x, y)$  (and might be more), we have  $(x, y) \in C \iff p(x, y)$  holds and if  $(x, y) \in C, (x, z) \in C$  then  $y = z$ .

e.g.  $x \rightarrow \{x\}$  is a function class, take  $p(x, y)$  to be  $y = \{x\}$ .

Now we can state Axiom of Replacement: The image of a set under a function class is a set. Mathematically,  $(\forall t_1) \dots (\forall t_n)[(\forall x)(\forall y)(\forall z)(p \wedge p[z/y] \Rightarrow (y = z)) \Rightarrow (\forall x)(\exists y)(\forall z)((z \in y) \iff (\exists w)((w \in x) \wedge p[w/x, z/y])]$ .

e.g. For any set  $x$ , can form  $\{\{t\} : t \in x\}$ .

Note: ZF does not include axiom of choice (AC)

$(\forall f)(f \text{ is a function} \wedge (\forall x \in \text{domain } f)(f(x) \neq \emptyset) \Rightarrow (\exists g)(g \text{ is a function} \wedge \text{domain } f = \text{domain } g) \wedge (\forall x \in \text{domain } g)(g(x) \in f(x))$ .

We write ZFC to be ZF with AC.

**Definition 6.4.** A set  $x$  is transitive if  $(\forall y)(\forall z)((y \in z) \wedge (z \in x) \Rightarrow (y \in x))$ . Equivalently,  $\bigcup x \subset x$ .

**Theorem 6.5.** Every set is contained in a transitive set, and as any intersection of transitive set is again transitive, we will have a smallest transitive set, called the transitive closure.

*Proof.* We want to take something like  $x \cup (\bigcup x) \cup (\bigcup \bigcup x) \dots$ . This is a set by Union Axiom applied to  $\{x, \bigcup x \dots\}$ , and it remains to show that the later is a set by replacement. The idea is to apply replacement on the set  $\omega$  with the function class  $0 \rightarrow x, 1 \rightarrow \bigcup x \dots$  and we check this is a function class. Let  $f$  be an attempt for:  $f$  is a function  $\wedge \text{dom}(f) \in \omega \wedge \text{dom}(f) \neq \emptyset \wedge f(0) = x \wedge (\forall n)(n+1 \in \text{dom}(f) \Rightarrow f(n+1) = \bigcup f(n))$ .

By usual  $\omega$  induction, we can check that  $(\forall f)(\forall g)(\forall n \in \omega)(f \text{ is an attempt} \wedge g \text{ is an attempt} \Rightarrow f(n) = g(n))$ . Also we can check that  $(\forall n \in \omega)(\exists f)(f \text{ is an attempt} \wedge n \in \text{dom}(f))$  by induction. (Details are left as an exercise, it is the same as in the proof of Recursion theorem). Therefore, our formulae  $p(u, v)$  for the function class is  $(\exists f)(f \text{ is an attempt} \wedge u \in \text{dom}(f) \wedge f(u) = v)$ .  $\square$

**Theorem 6.6. [Principle of  $\in$  induction]** For each formulae  $p$ , free variable  $t_1 \dots t_n, x$ , ( $t_i$ 's are parameters) we have that:  
 $(\forall t_1) \dots (\forall t_n)[(\forall x)(\forall y \in x)(p(y) \Rightarrow p(x)) \Rightarrow (\forall x)p(x)]$ .

*Proof.* Given  $t_1 \dots t_n$ , suppose  $\neg(\forall x)p(x)$ , and so  $(\exists x)\neg p(x)$ . Take  $x$  with  $\neg p(x)$  and consider the set  $u = \{y \in TC(\{x\}) : \neg p(y)\}$  where  $TC$  is the transitive closure. Then as  $x \in u, u \neq \emptyset$ , and by Well Foundness, we have an  $\in$  least element, say  $y$ . Then  $\neg p(y)$  and so  $(\forall z)((z \in y) \Rightarrow p(z))$ , because  $z \in y$  and  $y \in TC(\{x\})$  so  $z \in TC(\{x\})$  and as  $y$  is  $\in$  least so we must have  $p(z)$ . But by assumption if  $(\forall z)((z \in y) \Rightarrow p(z))$  then  $p(y)$ , which is a contradiction.  $\square$

**Remark 6.7.** Atomically,  $\in$  induction is equivalent to Axiom of Foundation. The other direction is as follows: Say  $x$  is regular, if  $(\forall y)((x \in y) \Rightarrow y$  has an  $\in$  least element). Foundation says every  $x$  is regular. To show this we use  $\in$  induction, which we assume to be true now.

*Claim:* For any  $x$ , if  $\forall y \in x$  is regular, so is  $x$ .

*Indeed,* given  $z$  with  $x \in z$ , if  $x$  is least in  $z$  we are done. If not, then  $(\exists y)((y \in z) \wedge (y \in x))$  and so  $y$  is regular because  $y \in x$ . Hence  $z$  has an  $\in$  least element as  $y \in z$ . Then by induction, every  $x$  is regular.

What about recursion? We want to define  $F(x)$  in terms of  $\{F(y) : y \in x\}$ .

**Theorem 6.8. ∈ Recursion Theorem** For any function class  $G$ ,  $(x, y) \in G \iff p(x, y)$  for some fixed formulae  $p$  everywhere defined. Then there is a function class  $F$ ,  $(x, y) \in F \iff q(x, y)$  for some formulae  $q$  everywhere defined, s.t.  $(\forall x)(F(x) = G(F|_x))$ . Moreover,  $F$  is unique.

**Remark 6.9.**  $F|_x = \{(t, F(t)) : t \in x\}$  is a set by Replacement.

*Proof.* Existence: Say  $f$  is an attempt if  $f$  is a function and domain of  $f$  is transitive and  $(\forall x)((x \in \text{dom}(f)) \wedge f(x) \Rightarrow G(f|_x))$ . So  $f$  is defined at  $y$ ,  $\forall y \in x$  if  $f$  is defined at  $x$  because the domain is transitive. Then  $(\forall x)(\forall f, f')((f, f'$  are attempts)  $\wedge (x \in \text{dom}(f)) \wedge (x \in \text{dom}(f')) \Rightarrow (f(x) = f'(x))$ , by  $\in$  induction. i.e. if  $f(y) = f'(y) \forall y \in x$ , then  $f(x) = f'(x)$  by definition of  $f, f'$ . Also,  $(\forall x)(\exists f)(f \text{ is attempt} \wedge (x \in \text{dom}(f)))$ , again by  $\in$  induction. Indeed, suppose that  $\forall y \in x$  there is an attempt defined at  $y$  and so let it be  $f_y$ , with domain transitive closure of  $\{y\}$ , then let  $f = \bigcup \{f_y : y \in x\}$  and let  $f' = f \cup \{(x, G(f|_x))\}$  hence the result.

Uniqueness has already be proved above, as at each  $x$  we have only one attempt.  $\square$

**Remark 6.10.** Let's briefly discuss the properties we used to prove the above theorems:

1.  $\in$  is well founded: Every non-empty set has an  $\in$  least element.
2.  $\in$  is local, i.e. for any  $y, \{x : x \in y\}$  is a set.

Therefore, in fact we only need the above properties for any induction, recursion on an binary relation. So the special case is that we have the relation only defined on a well-founded set, like what we have before on well-orderings.

When can we model a relation by  $\in$ ?

e.g. on  $\{a, b, c\}$  and a relation  $r$ , suppose  $arb, brc$ , put  $a' = \emptyset, b' = \{\emptyset\}, c' = \{\{\emptyset\}\}$ . Then  $\{a', b', c'\}$  have  $x' \in y' \iff x \in y$ . Analogue of subset of collapse is the following: Say relation  $r$  on a set an extension if  $(\forall x, y \in a)((\forall z \in a)(zrx \iff zry) \Rightarrow (x = y))$ .

**Theorem 6.11.** Let  $r$  be a relation on a set  $a$  which is well founded and extensional. Then there is a transitive  $b$  and bijection  $f : a \rightarrow b$  s.t.  $(\forall x, y \in a)(xry \iff f(x) \in f(y))$ . Moreover  $b$  and  $f$  are unique.

The proof is just an application of Recursion and Replacement.

The theorem tells us that for each well ordering  $x$ , there is a unique order isomorphism from an ordinal to  $x$ . This is called the order type.(which is a stronger or more concrete definition than before).

**Remark 6.12.** Each initial segment of  $x$  is sent to its order type. So  $x$  is sent to  $\{\text{order type of } I_y : y \in x\}$ , which is  $\alpha = \{\beta : \beta < \alpha\}$ . Thus,  $\alpha < \beta \iff \alpha \in \beta$ ,  $\alpha^+ = \alpha \sqcup \{\alpha\}$ , and  $\text{Sup } \{\alpha_i : i \in I\} = \bigcup \{\alpha_i : i \in I\}$ .

## Picture of Universe

Start with an empty set and keep taking power set. Define the sets  $V_\alpha$  for each  $\alpha \in ON$ , inductively as:

1.  $V_0 = \emptyset$ .
2.  $V_{\alpha+1} = \mathbb{P}V_\alpha$ .
3.  $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$  for  $\lambda$  a non-zero limit.

**Lemma 6.13.** Each  $V_\alpha$  is transitive.

*Proof.* Induction on  $\alpha$ . For  $V_0$ , it is clearly transitive. For successor, we need to show that if  $x$  is transitive, then  $\mathbb{P}x$  is also transitive. Let  $z \in y, y \in \mathbb{P}x$ , then  $y \subset x$  and so  $\forall v \in y, v \in x$ , and as  $z \in y$ , we have  $z \in x$ . Now take any  $u \in z$  as  $x$  is transitive, so  $u \in x$  and hence  $z \subset x, z \in \mathbb{P}x$  and so  $\mathbb{P}x$  is transitive. Finally, for limit, we need to check that if  $\forall \alpha < \lambda, V_\alpha$  is transitive, then  $V_\lambda$  is transitive. It is enough to check the union of transitive sets is again transitive by definition of  $V_\lambda$ . Take  $z \in y, y \in \bigcup x$ , we want to show  $z \in \bigcup x$ .  $y \in \bigcup x$  means that  $\exists u \in x, y \in u$ . We know that  $x$  is transitive, so we have  $y \in x$  and as  $z \in y$  so we have  $z \in \bigcup x$ .  $\square$

**Lemma 6.14.** If  $\alpha \leq \beta$  then  $V_\alpha \subset V_\beta$ .

*Proof.* Induction on  $\beta$ . If  $\beta = \alpha$ , we have  $V_\alpha = V_\alpha$  which is trivial. For successor,  $V_{\beta+} = \mathbb{P}V_\beta$ . We have proved that  $V_\beta, V_{\beta+}$  are transitive so we have  $V_\beta \subset \mathbb{P}V_\beta$ , and similarly for limit (exercise).  $\square$

**Theorem 6.15.**  $(\forall x)(\exists \alpha)(x \subset V_\alpha)$ . And so we take the universe  $V = \bigcup_{\alpha \in ON} V_\alpha$ .

Note:

- (i)  $x \subset V_\alpha \iff x \in V_{\alpha+1}$ .
- (ii) If  $x \subset V_\alpha$  then there is a least  $\alpha$ , we call this rank of  $x$ . e.g.  $\text{rank}(\omega) = \omega$ . (And moreover,  $\text{rank}(\alpha) = \alpha, \forall \alpha \in ON$ ).

*Proof.* Use induction. Given  $x$  we have  $(\forall y \in x)(\exists \alpha)(y \subset V_\alpha)$ . Assume that for each  $y \in x$ , we have  $y \subset V_{\text{rank}(y)}, y \in V_{\text{rank}(y)+1}$ . Let  $\alpha = \text{Sup} \{\text{rank}(y)+1 : y \in x\}$ . It's a set by replacement. Then as  $V_\alpha$  is transitive for each  $\alpha$ , then we have  $y \in V_\alpha, \forall y \in x$ . Therefore,  $x \subset V_\alpha$ .  $\square$

## 7 Cardinal

Informally, cardinals measure the size of sets.

**Definition 7.1.** Write  $x \leftrightarrow y$  for  $(\exists f)(f \text{ is a bijection from } x \text{ to } y)$ .

The idea is define the cardinality,  $\text{card}(x)$  of a set  $x$  s.t.  $\text{card}(x) = \text{card}(y) \iff x \leftrightarrow y$ .

**Remark 7.2.** We cannot define  $x = \{y : y \leftrightarrow x\}$ . In ZFC, we could define  $\text{card}(x)$  to be  $\alpha$  s.t.  $x \leftrightarrow \alpha$ . In ZF, we take the least  $\alpha$  s.t.  $\exists y$  of rank  $\alpha$  s.t.  $y \leftrightarrow x$  (sometimes called the essential rank of  $x$ ) and set  $\text{card}(x) = \{y : \text{rank}(y) = \alpha, y \leftrightarrow x\}$ .

**Definition 7.3.** We say an ordinal  $\alpha$  is initial if  $(\forall \beta \in ON)(\beta < \alpha \Rightarrow \neg \beta \rightarrow \alpha)$ .

**Example 7.4.**  $0, 1, 2 \dots \omega, \omega_1 \dots \gamma(x)$  for any  $x$  are all initial. But  $\omega^2$  is not as  $\omega^2 \leftrightarrow \omega$  but  $\omega < \omega^2$ .

**Definition 7.5.** We define  $\omega_\alpha, \alpha \in ON$  inductively by:

1.  $\omega_0 = \omega$ .
2.  $\omega_{\alpha+1} = \gamma(\omega_\alpha)$ .
3.  $\omega_\lambda = \text{Sup} \{\omega_\alpha : \alpha < \lambda\}$  for  $\lambda$  a non-zero limit.

Clearly, each  $\omega_\alpha$  is initial. Also every initial ordinal  $\delta \geq \omega$  is an  $\omega_\alpha$ . Indeed, the  $\omega_\alpha$  are unbounded as for each  $\alpha, \omega_\alpha \geq \alpha$ , by induction). So there is a least  $\alpha$ , with  $\omega_\alpha \geq \delta$ . But then,  $\omega_\alpha = \delta$  because, if not, say  $\omega_\alpha > \delta$ . We have two cases: if  $\alpha$  is a limit then we could have some  $\beta < \alpha$  s.t.  $\omega_\beta \geq \delta$  by definition of  $\omega_\alpha$ , which is a contradiction. If  $\alpha$  is a successor, then write  $\beta + 1 = \alpha$ , then by definition  $\omega_\alpha$  is the least ordinal which does not inject into  $\omega_\beta$ , but as  $\delta$  is initial, it also does not inject into  $\omega_\beta$ , which is again a contradiction.

We write  $\aleph_\alpha$  (reads aleph) for  $\text{card}(\omega_\alpha)$ . So the alephs are the cardinalities of all well orderable sets.



**Definition 7.6.** We say  $m \leq n$  if there is an injection  $M \rightarrow N$  ( $m = \text{card}(M)$ ,  $n = \text{card}(N)$ ). And say  $m < n$  if  $m \leq n$  and  $m \neq n$ .

**Example 7.7.**  $\aleph_0 < \aleph_1$ .

**Remark 7.8.**  $m \leq n, n \leq m \Rightarrow m = n$  (by Cantor Bernstein), and so  $\leq$  is an partial order.

Is  $\leq$  a total order?

In ZFC: It is, as all cardinals are  $0, 1, 2, \dots$  and  $\aleph_\alpha, \alpha \in ON$ .

In ZF: It need not be.

## Cardinal Arithmetic

**Definition 7.9.** For cardinal  $m, n$ , define  $m + n = \text{card}(M \sqcup N)$ ,  $m \cdot n = \text{card}(M \times N)$ ,  $m^n = \text{card}(M^N)$ , where  $M^N = \{f : f \text{ is a function from } N \text{ to } M\}$ .

**Example 7.10.** 1.  $\text{card}(\mathbb{R})$ : We have  $\mathbb{R} \leftrightarrow \mathbb{P}(\omega)$  so  $\text{card}(\mathbb{R}) = \text{card}(\mathbb{P}(\omega))$ , which is the same as  $\text{card}\{\{0, 1\}^\omega\} = 2^{\aleph_0}$ .

2. What is the cardinality of set consisting all real sequences? It is  $\text{card}(\mathbb{R}^{\mathbb{N}}) = \text{card}((2^{\aleph_0})^{\aleph_0})$ , which is  $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$ .

**Remark 7.11.** We have used the following facts to justify the above:

1.  $\aleph_0 \cdot \aleph_0 = \aleph_0$  i.e.  $\omega \times \omega \leftrightarrow \omega$ .

2.  $n + m = m + n$ . i.e.  $(M \sqcup N \leftrightarrow N \sqcup M)$ .

3.  $m \cdot n = n \cdot m$  i.e.  $(M \times N \leftrightarrow N \times M)$ .

4.  $(m^n)^p = m^{np}$ . i.e.  $((M^N)^P \leftrightarrow M^{N \times P})$ .

Warning: Cardinal exponentials are different from ordinals. e.g.  $\omega^\omega$  is countable but  $\aleph_0^{\aleph_0} \geq 2^{\aleph_0} > \aleph_0$ .

**Theorem 7.12.**  $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha \forall \alpha \in ON$ .

*Proof.* Induction on  $\alpha$ : We want to show that  $\omega_\alpha \times \omega_\alpha \leftrightarrow \omega_\alpha$ . We well order  $\omega_\alpha \times \omega_\alpha$  by going up in squares, i.e.  $(x, y) < (u, v)$  if:

$\max(x, y) < \max(u, v)$

or  $\max(x, y) = \max(u, v) = \beta$ , say and  $y < \beta, u < \beta$  or  $x = u = \beta, y < v$  or  $y = v = \beta, x < u$ .

For  $\delta \in \omega_\alpha \times \omega_\alpha : I_\delta \subset \beta \times \beta$  for some  $\beta < \omega_\alpha, \text{card}(I_\delta) \leq \text{card}(\beta \times \beta) = \text{card}(\beta)$  by induction. So the order type of  $I_\delta$  is  $< \omega_\alpha$ . And hence the order type of  $\omega_\alpha \times \omega_\alpha$  is  $\leq \omega_\alpha$ . And clearly,  $\omega_\alpha \leq \omega_\alpha \times \omega_\alpha$  and therefore,  $\omega_\alpha \times \omega_\alpha = \omega_\alpha$ .  $\square$

Now the addition and multiplication are easier by the above theorem and in fact we have:

**Corollary 7.13.** *Let  $\alpha \leq \beta$ , then  $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$ .*

*Proof.* We have the following inequalities:

$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta \leq 2 \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$ .  $\square$

**Example 7.14.** *In ZFC, every infinite  $x$  has  $x \leftrightarrow x \sqcup x$ .*

However, cardinal exponential is much harder. For example,  $2^{\aleph_0}$ , in ZF, might not even be an aleph. In ZFC, it is unknown that whether  $2^{\aleph_0} = \aleph_1$ . This is called the Continuum Hypothesis (CH).  $\text{ZFC} \not\vdash \text{CH}$  and  $\text{ZFC} \not\vdash \neg \text{CH}$ . We don't know how this may work yet.

## 8 Brief Discussion on Example Sheet 2011

Note: Any discussion is based on my own work and therefore is NOT model solution or not possibly the quickest way to do the question, and I was not able to solve every question on the example sheet. Any correction is happily received (zc231@cam.ac.uk or drop me a message on Facebook) and any discussion on the questions which I didn't solve is welcome (But don't ask me any starred question, as they are beyond my knowledge and sometimes ridiculous). I have my handwritten solutions, please drop me an e-mail if you want them. You may find these questions on:  
<http://www.dpmms.cam.ac.uk/study/II/Logic/>

### 8.1 Example sheet 1

1. All of them are tautologies. The way to check that is arguing by contradiction just as the examples in first chapter.

2. Use  $A_1$  we have  $\perp \Rightarrow ((q \Rightarrow \perp) \Rightarrow \perp)$ . Then use  $A_3$  we have  $((q \Rightarrow \perp) \Rightarrow \perp) \Rightarrow q$ . And finally use MP.

For the next part:

(a) Use  $A_1$ ,  $(\perp \Rightarrow q) \Rightarrow (p \Rightarrow (\perp \Rightarrow q))$ .

(b) Use MP, and  $\perp \Rightarrow q$  we have  $(p \Rightarrow (\perp \Rightarrow q))$ .

(c) Use  $A_2$ ,  $(p \Rightarrow (\perp \Rightarrow q)) \Rightarrow (((p \Rightarrow \perp) \Rightarrow (p \Rightarrow q)))$ .

(d) Use MP,  $(p \Rightarrow \perp) \Rightarrow (p \Rightarrow q)$ .

3.  $\neg\neg p$  is  $(p \Rightarrow \perp) \Rightarrow \perp$ . Let  $S = \{p, p \Rightarrow \perp\}$  and so use MP, we have  $S \vdash \perp$  and then by Deduction Theorem we have  $p \vdash (p \Rightarrow \perp) \Rightarrow \perp$ .

4. The proof way is very tedious. Ask me if you want to have a look at my solution (You don't need  $A_3$  in the proof but you may need to apply  $A_2$  twice). The deduction way is: Let  $S = \{p, q, p \Rightarrow (q \Rightarrow \perp)\}$ . And so by MP,  $S \vdash (q \Rightarrow \perp)$  and also  $q \in S$  so  $S \vdash \perp$ . Now use Deduction Theorem,  $\{p, q\} \vdash \neg(p \Rightarrow (q \Rightarrow \perp))$ , which is  $p \wedge q$ . The third method is by  $v(p), v(q) = 1$ , it is easy to check that  $v((p \Rightarrow (q \Rightarrow \perp)) \Rightarrow \perp) = 1$ .

5. When this is a tautology, then there is an valuation  $v$  for which the value is 0. Therefore,  $v(p \Rightarrow q) = 1$  and  $v(\neg(p \Rightarrow p)) = 0$ . So  $v(q \Rightarrow p) = 1$  and so  $v(p) = v(q)$ . So if it is a tautology then  $v(p) \neq v(q)$ . For example, we can take  $p$  to be an axiom and  $q$  to be  $\perp$ .

6. We don't want to use AC in this question. We can give values to each symbol, say ( has value 1,) has value 2,  $p$  has value 3, ' has value 4,  $\Rightarrow$  has value 5 and  $\perp$  has value 6. And so each proposition in the language is constructed in above way and so correspond to a unique natural number by a suitable hash function (e.g. take the prime power, see the example below).

So we have an injection from the set to  $\mathbb{N}$ . e.g.  $\perp \Rightarrow (p'' \Rightarrow p)$  corresponds to  $2^6 \cdot 3^5 \cdot 7^1 \cdot 11^3 \cdot 13^4 \cdot 17^4 \cdot 19^5 \cdot 23^2 \cdot 29^2$ .

7.  $A \not\vdash \perp, B \not\vdash \perp, A \cap B \subset A, B$ . So  $A \cap B \not\vdash \perp$  and similarly, if  $A \vdash a$  implies  $a \in A, B \vdash b$  implies  $b \in B$  then  $A \cap B \vdash c$  implies  $A \vdash c, B \vdash c$  and so  $c \in A, B$  and hence  $c \in A \cap B$ . The answer to the next part is:

No. Consider that if  $\frac{2}{3}$  people believe  $p, \neg q$ ,  $\frac{2}{3}$  people believe  $\neg q, p \Rightarrow q$ , and  $\frac{2}{3}$  people believe  $p, p \Rightarrow q$ . Then as  $3 \cdot \frac{2}{3} > 1$  we have some intersection of the groups. But intersection of any two groups will give a contradiction, i.e. inconsistent. (Any two will give  $p, q, \neg q$ . It is not deductively closed because suppose it is, then  $p, q, \neg q \in S$  and so  $S \vdash \perp$  and by assumption we have  $\perp \in S$ . But people never believe  $\perp$ .)

8. No. Suppose we can, then as in  $A_1, A_2$  we don't even mention the symbol  $\perp$ , therefore if we have a proof of  $A_3$  from  $\{A_1, A_2\}$ , as  $A_3$  mentions  $\perp$ , so whenever in the proof  $\perp$  occurs, we replace that with any symbol, say  $A$ . Then  $((p \Rightarrow \perp) \Rightarrow \perp) \Rightarrow p$  is  $((p \Rightarrow A) \Rightarrow A) \Rightarrow p$ . But clearly we can choose some  $A$  s.t. it is not a tautology, hence not an axiom.

9.  $S = \{t_1, t_2 \dots\}$ . Compactness theorem says that if every finite subset of  $T$  has a model, then  $T$  itself has a model. This is equivalent to, if  $T$  has no model then some finite subset has no model. Let  $T = \{\neg t_1, \neg t_2 \dots\}$ , then  $T \models \perp$  because  $\forall v, \exists n$ , s.t.  $v(t_n) = 1$ , i.e.  $v(\neg t_n) = 0$  and so  $T$  has no model. Then  $\exists N$  s.t.  $\{\neg t_i : i \leq N\} \models \perp$ . (Some finite subset, take the largest  $n$  to be  $N$ ). Therefore,  $\forall v, \exists t_i, i \leq N$  s.t.  $v(t_i) = 1$ .

10. The first part is by induction. Let  $S$  to be the finite set of propositions. We start with  $S$ . Clearly,  $S$  is equivalent to  $S$ . If  $S$  is independent then we are done. If not,  $\exists t$ , s.t.  $S - \{t\} \vdash t$ . Remove  $t$  and let  $S' = S - \{t\}$  and we also have  $S'$  equivalent to  $S$ . Continue this until the remaining set is independent and this procedure must stop as  $S$  is finite.

For the second part, we have the following example:

$\{p_1, p_1 \wedge p_2, p_1 \wedge p_2 \wedge p_3 \dots\}$ . We have  $p_1 \wedge p_2 \dots p_n \vdash p_1 \wedge \dots \wedge p_n, \forall n \geq m$ . Therefore, if it is independent, then it contains at most one element, say  $p_1 \wedge \dots \wedge p_j$  for some  $j$ , but this is not equivalent to the original set as  $p_1 \wedge \dots \wedge p_j \not\vdash p_1 \wedge \dots \wedge p_{j+1}$ .

For the last part, let  $S = \{t_1, t_2 \dots\}$  be the set of proposition. We construct  $S_n$  inductively.  $S_0 = \emptyset$ . Given  $S_n$ , if  $S_n \vdash t_{n+1}$ ,  $S_{n+1} = S_n$ .

If not, say  $S_n = \{r_1 \dots r_k\}$ . Let  $S_{n+1} = S_n \cup \{\bigwedge_{i \leq k} r_i \Rightarrow t_{n+1}\}$ .

Now it is equivalent to  $\{t_1 \dots t_{n+1}\}$  because  $S_{n+1} \vdash t_i \forall i \leq n+1$ . (Since  $\bigwedge r_i \in S_n$  for  $i \leq k$ , and use MP, we have  $t_{n+1}$ ).

Conversely,  $\{t_1 \dots t_n\}$  is equivalent to  $S_n$ , and so we can prove  $r_i$  by  $t_i$  and use  $A_1$  we have  $t_{n+1} \Rightarrow (\bigwedge r_i \Rightarrow t_{n+1})$  and so we can prove  $\bigwedge r_i \Rightarrow t_{n+1}$ .

It is independent. We can check this by induction.  $S_0$  is clearly independent. Suppose  $S_n$  is independent. This is clear when  $S_{n+1} = S_n$ . For the other case,  $S_n \not\vdash t_{n+1}$  so consider  $S_n \setminus \{r_i\} \cup \{\bigwedge r_i \Rightarrow t_{n+1}\} \not\vdash r_i$  by independence of  $S_n$ . And so it must be independent.

11. Let  $V$  be the set of valuations which is equivalent to  $\{0,1\}^L$ , where  $L = \{p_1, p_2, \dots\}$  and is countable. It is easy to check that  $\{0,1\}$  is a compact topological space with discrete topology. Hence  $\{0,1\}^L$  is compact (by property of product space). Let  $F_t = \{v : v(t) = 1\}$ . Then  $\bigcap_{t \in S} F_t = \{v : v(t) = 1 \ \forall t \in S\} = \{\text{models of } S\}$ . The compactness theorem says that, if any finite  $S' \subset S$  has a model, then  $S$  has a model. So it is equivalent to check that if  $\bigcap_{t \in S'} F_t \neq \emptyset, \forall S' \subset S$ , finite, then  $\bigcap_{t \in S} F_t \neq \emptyset$ .  
 Note that  $F_t$  is closed, in discrete topology. Hence if  $\bigcap_{t \in S'} F_t \neq \emptyset, \forall S'$  finite, then  $\bigcap_{t \in S} F_t \neq \emptyset$ . Because, if not, say  $\bigcap_{t \in S} F_t = \emptyset$ , then  $\bigcup_{t \in S} F_t^c = \{0,1\}^L$ . As  $\{0,1\}^L$  is compact, we have a finite subcover, say  $\bigcup_{t \in S'} F_t^c = \{0,1\}^L$  and so  $\bigcap_{t \in S'} F_t = \emptyset$ , which is a contradiction.

12. I am not sure for this question but I think it should be  $3 \cdot 2^n$ . Ask me if you want to see my solution.

13.  $\{p_1, p_2 \Rightarrow p_1, p_3 \Rightarrow (p_2 \Rightarrow p_1) \dots\}$  is clearly a chain. We cannot have an uncountable chain here because for every element in the chain, we can send it to a unique rational number, which is the proportion of valuations for which it is true. So if it has length  $n$ , the total possibility is  $2^n$  (The possible values we can have for each proposition in this element). And so we only need  $2^n$  valuations to describe the behavior of this element. Suppose  $k$  valuations says it is true, then we send this element to  $\frac{k}{2^n}$ . Now, for  $p, q$  in the chain, either  $p \vdash q$  or  $q \vdash p$ . WLOG, say  $p \vdash q$  and so  $q \not\vdash p$ . By Completeness Theorem,  $p \models q$  and so if  $v(p) = 1$ , then  $v(q) = 1$ . But there is some valuation  $v$ , s.t.  $v(q) = 1$  and  $v(p) = 0$  because  $q \not\vdash p$ .

Hence we have the proposition for which  $q$  is true is greater than the proportion for which  $p$  is true. Therefore, it defines an injection from the chain to  $\mathbb{Q}$  (as  $p, q$  must have different value) and so it is countable.

## 8.2 Example sheet 2

Note:  $\epsilon_0$  is the limit of  $\{w, w^w, w^{w^w}, w^{w^{w^w}} \dots\}$ .

1. For the first one we may try  $\{1, \frac{1}{2}, \frac{1}{3} \dots; 2, 1 + \frac{1}{2}, 1 + \frac{1}{3} \dots\}$ . For the second one, we may try  $\{-\frac{1}{2^n} - \frac{1}{2^{m+n}} : 0 \leq m, n < \omega\}$ . This has order type  $\omega^2$  as for each  $n$ ,  $-\frac{1}{2^n}$  is a limit for  $-\frac{1}{2^{m+n}}$ . For the third one we take  $\{-\frac{1}{2^n} - \frac{1}{2^{m+n}} - \frac{1}{2^{m+n+k}} : 0 \leq m, n, k < \omega\}$ .
2. The first statement is true. You can either use an inductive argument which is easy to check. Or you can use synthetic definition. The second one is not true. Consider  $\alpha = 1, \beta = \omega$ , then  $\alpha + \beta = 1 + \omega = \omega = \beta$ .
3. There is no non-zero  $\alpha$  for which  $\alpha \cdot \omega = \alpha$ . Because if  $\alpha \neq 0$ , then  $\alpha \cdot \omega > \alpha \cdot 2 > \alpha$ . For the second one, pick  $\alpha = \omega^2$ .
4. Induction. Write  $\cdot$  for the inductive definition and  $\times$  for the synthetic definition. Then consider  $\alpha \cdot \beta$ .
  - (a)  $\beta = 0$ , we have  $\alpha \cdot 0 = 0$  and  $\alpha \times 0$  is the order type of  $X \times \emptyset$  and so it is also 0.
  - (b) For  $\beta^+$  successor,  $\alpha \cdot \beta^+ = \alpha \cdot \beta + \beta$ , and  $\alpha \times \beta^+$  is the order type of  $\alpha \times \beta \sqcup \alpha \times \{\beta\}$ . Now by induction, as  $\alpha \times \beta$  is the same as  $\alpha \cdot \beta$  and clearly,  $\alpha \times \{\beta\}$  is the same as  $\beta$  and therefore by synthetic definition of addition, we conclude that these two are the same. (To be more, precise, we may construct an order isomorphism).
  - (c) For  $\beta$  limit.  $\alpha \cdot \beta = \text{Sup} \{\alpha \cdot \gamma : \gamma < \beta\} = \text{Sup} \{\alpha \times \gamma : \gamma < \beta\}$  by induction. Now as the set is nested and taking  $\text{Sup}$  is the same as taking union, so by the knowledge of nested set we learned from lectures, we know the union is an well ordering and it is just by definition,  $\alpha \times \beta$ .

Therefore, these two definitions coincide.

5. Synthetic definition is much easier, though one can prove this by induction. A suitable picture is helpful when we prove this sort of stuff by synthetic definition.
6. The first one is not true. Consider  $\alpha = \beta = 1, \gamma = \omega$  then  $(\alpha + \beta) \cdot \gamma = 2 \cdot \omega = \omega$ , but  $\alpha \cdot \gamma + \beta \cdot \gamma = \omega \cdot 2$ . The later is true. Here, I shall give a

proof using synthetic definition and give a precise order isomorphism. Consider that  $\alpha \times (\beta \sqcup \gamma) = \{(a, (b, c)) : a \in \alpha, \text{ either } (b \in \beta, c = 0) \text{ or } (b \in \gamma, c = 1)\}$ . And  $(\alpha \times \beta) \sqcup (\alpha \times \gamma) = \{((a, b), c) : \text{either } ((a, b) \in \alpha \times \beta, c = 0) \text{ or } ((a, b) \in \alpha \times \gamma, c = 1)\}$ .

In  $\alpha \times (\beta \sqcup \gamma)$ ,  $(a, (b, c)) < (d, (e, f))$  if:

(a)  $a < d$

(b)  $a = d, c = f, b < e$

(c)  $a = d, c < f$ .

In  $(\alpha \times \beta) \sqcup (\alpha \times \gamma)$ ,  $((a, b), c) < ((d, e), f)$  if:

(d)  $c = f, a < d$

(e)  $c = f, a = d, b < e$

(f)  $c < f$ .

Now we can see that (a),(c) correspond to (d),(f) and (b) corresponds to (e). And therefore, sending  $(a, (b, c))$  from  $\alpha \times (\beta \sqcup \gamma)$  to  $((a, b), c)$  in  $(\alpha \times \beta) \sqcup (\alpha \times \gamma)$  and so it is an order isomorphism.

7. You can use induction on  $\alpha$  (that's what I tried) to show the result, or you may use synthetic definition by realising  $\beta$  as an initial segment and so it is easier to see from the picture (if you have a picture in mind..) that there is a unique  $\gamma$  for which it is true. For the second part you may take  $\beta = 1, \alpha = \omega$ , as a counter example. Suppose  $\gamma + 1 = \omega$ , then  $\gamma^+ = \omega$  and so  $\omega$  is a successor, which is a contradiction.
8. The easier way to do this require some knowledge of normal function and need some other results. There is one question on Tripos paper which is the same as this and so I will explain the way to do this question later. (See discussion in Tripos Question). And for the second part, the Cantor normal form for  $\epsilon_0$  is  $\omega^\epsilon$ .

9. It must be a limit. By Hartog's Lemma, we know that  $\omega_1$  is the least ordinal which does not inject into  $\omega$  and so it is the least uncountable ordinal. Suppose it is a successor, say  $\omega_1 = \alpha^+$ , then  $\alpha$  must also be uncountable and therefore contradicts  $\omega_1$  being the least uncountable ordinal.
10. As  $\alpha$  is a countable ordinal, so there is a countable set  $X = \{x_1, x_2 \dots\}$  with order type  $\alpha$ . And as  $X$  is well ordered, we take the enumeration of  $X$  to be increasing w.r.t the usual ordering. Then let  $\alpha_i$  be the order type of the set  $\{x_1, x_2 \dots x_i\}$  and so  $\alpha$  is the supremum of those. This is impossible when  $\alpha$  is  $\omega_1$ . Suppose we have such sequence  $\alpha_i$  and we must have each  $\alpha_i$  countable by the property of  $\omega_1$ . Then by synthetic definition, the sequence  $\alpha_i$  is increasing and if we set  $X_i$  to be the set with order type  $\alpha_i$  and  $X_i \subset X_{i+1}$  then the family  $(X_i, \alpha_i)$  is nested and so taking the *Sup* is the same as taking the union. The union is also a well ordering but it is a countable union of countable set as sequence is countable (The subscript implies that we have an enumeration) and the union has to be countable. But  $\omega_1$  is uncountable, which is a contradiction.
11. You can use induction to check this but it is very long and not easy. There is a clever way to do this question: Let  $X$  to be a countable set of order type  $\alpha$ , say  $X = \{x_1, x_2 \dots\}$ , where the way of counting has nothing to do with the ordering  $\alpha$ . We may construct an order isomorphism between  $X$  and  $Y \subset \mathbb{Q}$ . Let  $f : X \rightarrow \mathbb{Q}$ , defined inductively by :  $f(x_0) = y_0, y_0$  is arbitrary in  $\mathbb{Q}$ . Suppose we have defined  $f(x_0) \dots f(x_n)$ , in the way s.t.  $f(x_i) < f(x_j)$  whenever  $x_i <_\alpha x_j$  where  $<_\alpha$  is the ordering given by  $\alpha$ . We rearrange  $x_0, x_1 \dots$ . Let  $\{i_0 \dots i_n\} = \{0, 1 \dots n\}$  s.t.  $x_{i_0} <_\alpha x_{i_1} \dots <_\alpha x_{i_n}$ . If we set  $y_{i_k} = f(x_{i_k})$ , then we have  $y_{i_0} < \dots y_{i_n}$ . For  $x_{n+1}$ , we have  $n + 2$  cases:
- (0) :  $x_{n+1} <_\alpha x_{i_0} <_\alpha \dots$
- (m) :  $x_{i_{m-1}} <_\alpha x_{n+1} <_\alpha x_{i_m}$  for some  $1 \leq m \leq n$ .
- (n+1) :  $x_{i_0} <_\alpha \dots <_\alpha x_{i_n} <_\alpha x_{n+1}$ .
- For (0), pick  $y_{n+1} = f(x_{n+1})$  s.t.  $y_{n+1} < y_{i_0}$ . For (m), pick  $y_{n+1}$  s.t.  $y_{i_{m-1}} < y_{n+1} < y_{i_m}$  and for (n+1), pick  $y_{n+1} > y_{i_n}$ . We can do this



because  $\mathbb{Q}$  is unbounded. Then we have defined  $y_0 \dots y_{n+1}$  s.t.  $y_i < y_j$  whenever  $x_i <_\alpha x_j$ . and continue this inductively, we have an order isomorphism from  $X$  to  $Y \subset \mathbb{Q}$ . And so  $Y$  has order type  $\alpha$ .

For the second part, suppose there is, say  $X$  and so  $X$  is uncountable. Now if we take out any  $x \in X$ , let  $X' = X - \{x\}$ . It is still well ordered, because for each non-empty  $S \subset X'$ , if the least element is  $x$  then we consider the set  $S - \{x\}$ , it must also have a least element as  $X$  is well ordered. Also  $X'$  is uncountable, but then this contradicts the fact that  $\omega_1$  is the least uncountable ordinal.

12. We construct functions  $f_\alpha : ON \rightarrow ON$  by  $f_0(\beta) = \omega^\beta, f_{\alpha^+}(\beta) = \beta^{th}$  ordinal which is fixed by  $f_\alpha$ , i.e.  $f_\alpha(\gamma) = \gamma$ , and  $f_\lambda(\beta) = Sup \{f_\alpha(\beta) : \alpha < \lambda\}$  for  $\lambda$  a non-zero limit. Clearly, we can check that if  $\beta \leq \gamma$ , then  $f_\alpha(\beta) \leq f_\alpha(\gamma) \forall \alpha \in ON$  and so it is order preserving and so by fixed point theorem, as the set is complete, we have a fixed point  $\gamma$  and so  $f_{\alpha^+}$  is well defined and so the limit is also well defined. (it seems easy to state these but it requires some inductive arguments). I think:  
 $1 * 0 = \epsilon_0, 1 * 1 = \epsilon_1, 1 * 2 = 2^{nd}$  ordinal s.t.  $0 * \gamma = \gamma$ , which is  $\epsilon_2 = Sup \{\epsilon_1 + 1, w^{\epsilon_1} + 1, w^{w^{\epsilon_1+1}} \dots\}$ .  $2 * 0 = 0^{th}$  ordinal  $\gamma$  that  $1 * \gamma = \gamma$ . Take  $\alpha = Sup \{\epsilon_0, \epsilon_0 * 0, (\epsilon_0 * 0) * 0 \dots\}$ . And for each  $(\dots((\epsilon_0 * 0) * 0) \dots) * 0$ , if  $((\epsilon_0 * 0) * 0) \dots = \lambda$  is countable, then  $\lambda * 0 = Sup \{\alpha * 0 : \alpha < \lambda\}$  is also countable as each  $\alpha < \lambda$  is countable. And so the above ordinal is countable.

13. No. Suppose it is true, take  $f$  to be the function that  $f(\alpha) = x_\alpha < \alpha$  in such a way that the  $x_\alpha$  are distinct. Let  $g$  be the inverse function, so we have:

$$g(\beta) = \begin{cases} \alpha & \text{if } x_\alpha = \beta \\ \beta + 1 & \text{otherwise} \end{cases}$$

And so  $g(\beta) > \beta$ . Now consider  $y_n$ , defined inductively as:

$$y_0 = \emptyset$$

$$y_{n+1} = \{g(\beta) : \beta \leq y_n\}$$

Let  $y = Sup y_n$ . And clearly,  $y_{n+1} \geq g(y_n) > y_n$ . As  $x_y < y$ , we have  $x_y < y_k$  for some  $k$  and so by definition  $y = g(x_y) \leq y_{k+1}$ , which is a contradiction.

### 8.3 Example sheet 3

1. It is very helpful to draw Hasse diagrams to list every possibility. There are 16 of them and 2 of them are complete.
2. (i): No. e.g. Take  $\{\{1\}, \{3\}, \{5\} \dots\} = \{\text{odd number}\} \subset X$  (As each singleton lies in  $X$ ). The upper bound of this must contain every odd number, and therefore must be cofinite. But it has no least upper bound. Suppose we have some  $P$  cofinite, containing every odd number, then  $P$  must contain some even number as it is cofinite. Then remove any even number from  $P$  will give a smaller set containing every odd number and is smaller than  $P$ .  
(ii): No. Consider  $\mathbb{Q}$  as a  $\mathbb{Q}$ -vector space. As singleton,  $\{1\}, \{2\}$  are both independent. But the set  $\{1, 2\}$  does not have an upper bound in the set as every set containing 1, 2 must be dependent.  
(iii): Yes. Take any non-empty subset  $X'$  which contains some subspaces of  $V$ . For each subspace we have a basis, and take the union of those. Let  $Y$  be a subspace generated by that union. Then  $Y$  is the least upper bound. (The closure of the union).
3.  $X = \{0, 1\}, f(0) = 1, f(1) = 0$ , which is order reversing and it has no fixed points.  
Now consider for any order reversing  $f$ ,  $f^2$  is order preserving, and so  $f^2(z) = z$  for some  $z$ . Hence either  $f(z) = z$  or  $f(z) = w, f(w) = z$  for some  $w$ .
4. Let  $(R, \leq_R)$  be a poset equipped with partial order  $\leq_R$ . Take  $X$  to be the set of all partial ordering on  $R$  extending  $\leq_R$ , ordered by extension. i.e. for any  $a, b \in X$ ,  $a \leq b$  if  $b$  extends  $a$ . (Equivalently, if we realise a relation as a subset of  $\mathbb{P}(R \times R)$ , then  $a \leq b$  if  $a \subset b$ .) And  $X$  is non-empty as we know  $\leq_R$  is a partial order. Now given a chain  $x_1 \leq x_2 \dots$  in  $X$ , let  $x = \bigcup x_i$ . So  $x$  is a partial order on  $R$  extending  $\leq_R$ , so  $x \in X$ . As we take the union, it is an upper bound. Hence by Zorn's Lemma, we have a maximal element. And the maximal element must be total order.
5. Let  $X$  be countable and  $X = \{x_0, x_1 \dots\}$  be an enumeration of  $X$ . Given  $x_0$ , pick  $y_1$  to be the first one in the sequence  $x_i$  s.t.  $x_0 < y_1$ ,

and having defined  $y_n$ , we set  $y_{n+1}$  to be the first one in the sequence greater than  $y_n$ . Note that, if  $x_k = y_{n+1}$  and  $x_l = y_n$  then  $k > l$  because if not then we would have picked  $x_k$  to be  $y_n$  instead of  $x_l$ . Now  $x_0 < y_1 < y_2 \dots$  is a chain. Suppose the set  $X$  has no maximal element. By assumption, this chain has an upper bound, say  $x_i$  for some  $i$ . But this  $i$  is finite, so by construction of the chain, we must have passed through  $x_i$  at some stage and so there must be some  $y_j$  s.t.  $y_j > x_i$ , as  $X$  has no maximal element. So  $x_i$  is not upper bound, which is a contradiction.

6.  $\Leftarrow$ : AC  $\iff$  WOP, because AC  $\Rightarrow$  Zorn's Lemma  $\Rightarrow$  WOP. So we can well order  $X$  and  $Y$ . And by one of the theorem in the notes, for any two well-orderings, either  $X \leq Y$  or  $Y \leq X$ .

$\Rightarrow$ : Suppose for every two  $X, Y$ , either  $X$  injects into  $Y$  or  $Y$  injects into  $X$ , then we know, by Hartog's Lemma, we have  $\gamma(X)$  does not inject into  $X$  and so we must have  $X$  injects into  $\gamma(X)$ . Hence each set is injected into an ordinal, and so can be well ordered. i.e. we have shown WOP, and WOP  $\Rightarrow$  AC.

7. This is a typical Maths joke..The answer is Zorn's Lemon.(Not Lemma...)

8. The usual axiomatisation for field, poset, graph and group is given in the lecture so I will just quote them.

(i): L=Language of field, T=field and  $1 + 1 = 0$ .

(ii):L=Language of poset, T=poset and  $\neg(\exists x)(\forall y)(y \leq x)$ .

(iii): L=Language of graph,T=:

Graph

$(\forall x_1)(\forall x_2)(\forall x_3)\{\neg[(x_1 \sim x_2) \wedge (x_2 \sim x_3) \wedge (x_3 \sim x_1)]\}$

.

.

$(\forall x_1) \dots (\forall x_n)\{\neg[(x_1 \sim x_2) \dots (x_n \sim x_1)]\}$  where n is odd.

.

.

i.e odd cycle free

(iv): L=Language of field, T=:

field

$(\forall a_0)(\forall a_1)(\exists x)(a_0 + a_1 \cdot x = 0)$

.

$(\forall a_0) \dots (\forall a_n)(\exists x)(a_0 + a_1 \cdot x + \dots a_n \cdot x^n = 0)$ . .

(v): L=Language of Group, T= Group and  $(\exists x_1) \dots (\exists x_60)((\bigwedge_{i,j} x_i \neq x_j) \wedge (\forall x)[(x = x_1) \vee \dots (x = x_60)])$ .

(vi):L=Language of Group, T= Group of order 60 by above and:

$(\exists x_1) \dots (\exists x_n)(\forall x)((\forall y)(y = x_1 \vee \dots y = x_n)) \Rightarrow (xyx^{-1} \neq x_1 \wedge \dots xyx^{-1} \neq x_n)$ .

(vii): The basic axiomatisation for vector space is easy. In first order logic, we cannot axiomatise the set of real number. So what we may do is something like: add uncountably many symbols and give the axioms of the real addition, multiplication to realise it as an equivalence set of real number. But in general it is very hard to do. I think it should be fine to assume the knowledge of real numbers.

9. T=:

Group

$(\exists a_0) \dots (\exists)(a_{101})(\bigwedge_{i,j} a_i \neq a_j) \Rightarrow (\exists a_0) \dots (\exists a_{200})(\bigwedge_{i,j} a_i \neq a_j)$

$(\exists a_0) \dots (\exists)(a_{201})(\bigwedge_{i,j} a_i \neq a_j) \Rightarrow (\exists a_0) \dots (\exists a_{300})(\bigwedge_{i,j} a_i \neq a_j)$

.  
.
  
.

10. Assume T axiomatises the fields of positive characteristic. We add the following:

$1 + 1 \neq 0$

$1 + 1 + 1 \neq 0$

.  
.

So this has no model, as the model does not have any positive characteristic but any finite subset has a model, which contradicts Compactness Theorem.

Now to axiomatise field of characteristic 0, we let T=:

field

$1 + 1 \neq 0$

$1 + 1 + 1 \neq 0$

.  
.  
.

Finally, suppose we have some finite T which axiomatises field of char-

acteristic 0. Let  $T'$  be the theory we had above, then  $T' \vdash T$ . Hence a finite subset of  $T'$  proves  $T$ , but this is certainly impossible.

11. We add to the language by a constant  $c$ , with the theory  $T$  that:  
 Peano Arithmetic(quote those theories)

$$1 < c$$

$$2 < c$$

.

.

.

Then this certainly cannot have a model which is isomorphic to  $\mathbb{N}$ , since  $\mathbb{N}$  has no upper bound. Then we check this has a countable model. By Downward Lowenheim–Skolem Theorem, if it has a model, then we have a countable model. But every finite subset has a countable model, as for every finite subset if  $c$  is mentioned then it can be treated as a largest element of the finite subset. Hence by Compactness Theorem, it has a model and hence a countable model.

12.  $L$ =Language of Groups  $\cup \{x\}$ .  $T$ =:

$$x \neq e$$

$$x^2 \neq e, \text{ where } x^2 \text{ is a shorthand for } m(x, x).$$

$$x^3 \neq e$$

.

.

.

This cannot be done in language of groups. If you want to know more about this, look up Ultraproduct.

13.  $T$ =:

$$(\forall x)(\forall y)((f(x) = f(y) \Rightarrow (x = y))$$

$$(\forall x)(\exists y)(f(y) = x)$$

$$(\forall x)(\neq (\exists n))(f^n(x) = x)$$

The model is something like: If we think about  $\mathbb{Z}$ , the set of integers, and take  $f(x)$  to be  $x + 1$ , say. But in fact, any countable copies of  $\mathbb{Z}$  can be a model.

Now to prove  $T$  is complete, the idea is to realise any model as some copies of  $\mathbb{Z}$ . But I am not sure about the details.

14. (i): If T axiomatises it, then add two constants  $w, z$  and the following:

$$w \not\sim z$$

$$(\forall x)\{\neg[(w \sim x) \wedge (x \sim z)]\}$$

.

.

$$(\forall x_1) \dots (\forall x_n)\{\neg[(w \sim x_1) \wedge (x_1 \sim x_2) \wedge \dots \wedge (x_{n-1} \sim x_n) \wedge (x_n \sim z)]\}$$

.

.

This is saying that the shortest path in the graph has length  $n, n \in \mathbb{N}$ . So it has no model, as any connected graph has a shortest path of finite length. But any finite subset has a model, which contradicts Compactness Theorem.

## 8.4 Example sheet 4

1. Axiom of Infinity mentions  $\emptyset$ , and we can take it as a subset by Separation.

For replacement, it says that  $(\forall x)(\exists y)(\forall z)((z \in y) \iff (\exists w)((w \in x) \wedge (z = f(w)))$  for any function class  $f$ . Let  $f$  be:

$$f(w) = \begin{cases} w & \text{if } p(w) \\ v & \text{if } \neg p(w) \end{cases}$$

for some predicate  $p$  and  $v \in x$  s.t.  $p(v)$ . Then we have separation for this  $p$ .

2. Apply axiom of replacement to two elements  $x, y$ . Let  $z = \{\emptyset, \{\emptyset\}\}$ , where  $\emptyset$  exists by Empty-Set Axiom, and  $z$  is a set by Power Set Axiom. Now let  $f(\emptyset) = x, f(\{\emptyset\}) = y$ , and so by Replacement,  $\{x, y\}$  is a set and hence the Pair Set Axiom.

3. We have seen the ordered pair  $(x, y) = \{\{x\}, \{x, y\}\}$ . Let  $a_{(x,y)} = \bigcap \bigcup (x, y) = x, b_{(x,y)} = \bigcup (\bigcup (x, y) \setminus \bigcap (x, y)) = y$ , where the intersection is taken by Axiom of Separation, so informally,  $a_x, b_x$  represent the first and second coordinate respectively. Define  $A \times B = \{x \in \mathbb{P}^2(\bigcup\{A, B\}) : x \text{ is an ordered pair and } (a_x \in A) \wedge (b_x \in B)\}$ . For  $f : x \rightarrow y$ , it means  $(f \text{ is a function}) \wedge (\text{domain is } x) \wedge (\forall z)(\exists t)((t, z) \in f \Rightarrow (z \in y))$ . So we define  $B^A = \{f \in \mathbb{P}(A \times B) : f : A \rightarrow B\}$ .

4. We have counterexamples for both statement. For the first part, consider  $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ . It is transitive, but  $\in$  on  $X$  is not. For the second part, take  $x = \{y, \mathbb{P}(y), \mathbb{P}^2(y)\}$ , we have  $\in$  transitive in this set, but  $X$  itself is not transitive.

5. Rank of  $\{2, 3, 6\}$  is 7. Rank of  $\{\{2, 3\}, \{6\}\}$  is 8. Rank of  $\mathbb{Z}$  is  $\omega$  because we can send  $\mathbb{Z}$  to  $\mathbb{N}^2$  by:

$$f(x) = \begin{cases} (x, 0) & \text{if } x > 0 \\ (-x, 1) & \text{if } x < 0 \end{cases}$$

Then each  $x$  has finite rank, and so  $\text{rank}(\mathbb{Z}) = \omega$ . Similarly, we can send  $\mathbb{Q}$  to  $\mathbb{N}^3$  and so the rank of  $\mathbb{Q}$  is  $\omega$ .

For  $\mathbb{R}$ , we can construct it by set of ordered pair  $(a, b), a, b \in \mathbb{N}$ , meaning the decimal  $a$  is in the  $b^{\text{th}}$  digit. But we know  $b$  is unbounded, and so  $\text{rank}(\mathbb{R}) = \omega + 1$ .

6. Consider  $z \in V_{\omega+1} \setminus v_\omega$  and so  $z$  cannot be finite. So  $V_{\omega+1} \setminus V_\omega \not\subset \text{HF}$ . But  $V_\omega \subset \text{HF}$ . So  $V_\omega = \text{HF}$ . It satisfies all axioms except infinity, because all of its elements have finite rank. You may find it useful to prove that  $x \in \text{HF} \iff x \subset \text{HF}$ . (One way is clear, and the other way should use transitivity).

7. All but replacement. Because, consider  $f(n) = n + \omega$ . Then  $f(\mathbb{N}) \rightarrow \{\omega, \omega + 1 \dots\}$  The rank of the image is  $\omega + \omega$  and so it is certainly not in  $V_{\omega+\omega}$ .

8. Continuous functions are determined by the image of  $\mathbb{Q}$  as a subset of  $\mathbb{R}$  as each real number is a limit of a rational sequence. So  $\text{card}(\mathbb{R}^{\mathbb{R}}) \leq \text{card}(\mathbb{R}^{\mathbb{Q}})$ . Now use  $\mathbb{Q} \leftrightarrow \mathbb{N}$ , and  $\text{card}(\mathbb{R}) = 2^{\aleph_0}$ . So we have  $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$ . And the constant functions are continuous, so  $\text{card}(\mathbb{R}^{\mathbb{R}}) \geq \text{card}(\mathbb{R}) = 2^{\aleph_0}$ . And so we conclude that the cardinality is  $2^{\aleph_0}$ .

9. Consider  $\alpha = \text{Sup} \{0, \omega_0, \omega_{\omega_0} \dots\}$ . We need Axiom of replacement to check the class in the bracket is indeed a set.

10. If we have a surjection from  $\aleph_n$  to  $\aleph_{n+1}$  then we could inject  $\omega_{n+1}$  to  $\omega_n$ , which is a contradiction. Now we check firstly that if  $A_i < B_i \forall i$ , then  $f : \bigcup A_i \rightarrow \prod B_i$  is not surjective. Let  $f_i : A_i \rightarrow \prod B_i$ , and  $f$  sends  $a \in A_i$  to  $f(a) \in \prod B_i$  s.t.  $f(a)(i) = f_i(a)$ . By assumption, as  $A_i < B_i$ ,  $f_i$  is not surjective. Let  $g(i)$  be in  $B_i \setminus f_i(A_i)$ , then  $g \in \prod B_i$ , but  $g$  is not in the image of  $f$ , by using diagonal argument. Then for  $\sum_{i \in \omega} m_i, \prod_{i \in \omega} n_i$ , we let  $m_i = \aleph_i$  and  $n_i = \aleph_\omega$ . So we have  $\sum_{i \in \omega} \aleph_i = \aleph_\omega < \aleph_\omega^{\aleph_0} = \prod_{i \in \omega} \aleph_\omega$ . And if  $2^{\aleph_0} = \aleph_0$  then raise both sides to the power of  $\aleph_0$ , and use  $2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$ , we have  $\aleph_\omega = \aleph_\omega^{\aleph_0}$ , which is a contradiction.
11. Let  $V$  be a model of set theory, and we say a set  $x$  in  $V$  is  $V$ -uncountable if there is no injection in  $V$  (very important!) from  $x$  to the natural numbers in  $V$ . For simplicity let us assume that  $V$  itself lives inside another model of set theory  $U$ . (This is a big assumption, and not justified by ZF(C): if it were true, then ZF(C) would be able to prove itself consistent, a contradiction!) It's not surprising that there is a  $V$ -uncountable set  $x$  which only contains  $U$ -countably many members in  $V$ : remember that the language of set theory is countable, so you can only prove the existence of countably many sets (in the sense that there are only countably many sets that you can describe). As such,  $V$  is only required to have countably many sets.
13. Let  $(A_i)_{i \in \omega}$  be a countable union of countable sets. Suppose  $\omega_2 = \bigcup_{i \in \omega} A_i$ . For each  $i \in \omega$ ,  $A_i$  is the set of ordinals ordered by  $\in$  of countable order type  $\alpha_i$ , so have injections  $f_i : A_i \rightarrow \alpha_i$  and  $\alpha_i \subset \omega$ . (That is, in ZF model, the countable really means that  $\alpha_i \subset \omega$ ). Then  $f : \omega_2 \rightarrow \omega_1 \times \omega_1$  by  $f(x) = (i_x, f_{i_x}(x))$ , where  $i_x$  is the least ordinal s.t.  $x \in A_{i_x}$ , so  $f$  is an injection. Also  $\omega_1 \times \omega_1 \leftrightarrow \omega_1$ . So let  $g$  be a bijection from  $\omega_1 \times \omega_1$  to  $\omega_1$  and so  $f \circ g : \omega_2 \rightarrow \omega_1$  is an injection, which is a contradiction.
14. Make two copies of  $V$ , say  $V \times \{0, 1\}$ . In the new copy  $x \in y$  if  $y$  has  $2^{nd}$  component 0 and  $x \in y$  in the first component; Or if  $y$  has  $2^{nd}$  component 1 and  $x \notin y$  in the first component. So, by this, we have complementation. (This is just a rough idea for this question, and I am not sure about the details).



## 9 Discussion on Tripos Paper

You may find the recent Tripos paper on:

<http://www.maths.cam.ac.uk/undergrad/pastpapers/>

Note: These solutions or hints are based on my own work, not the model solutions given by the faculty. All errors are happily received (zc231@cam.ac.uk or drop me a message on Facebook) and if you want to discuss some questions which I do not discuss below, please do email me. I will only discuss the Tripos questions I did when I prepared for my PartII exam and therefore I will not be able to cover questions from every single year..

### 9.1 2004

$A_1/7$  The first part is book work. For (ii) Let  $T$  be the set of up-set. Take any non-empty subset of  $T$ , say  $X$ , consisting  $T_i, i \in I$ , for some family  $I$ , where  $T_i$  is up-set of  $X$ . Let  $\mathbb{T} = \bigcup_{i \in I} T_i$ . It is clearly an upper bound if this is an up-set. Let  $x \in \mathbb{T}$  and  $x \leq y$ , so  $x \in T_i$  for some  $i$ , and as  $T_i$  is up-set, we have  $y \in T_i$  and so  $y \in \mathbb{T}$ . Hence  $\mathbb{T}$  is an up-set, and clearly it is the least upper bound so the set  $T$  is complete.

Let  $S$  be an up-set in  $Y$ , and  $X$  is isomorphic to  $S$ , and let  $P \subset X$  s.t.  $Y$  is isomorphic to  $X \setminus P$ . Let  $f : X \rightarrow S, g : Y \rightarrow X \setminus P$  be isomorphisms. We aim to find some  $\theta$ , and  $P$  s.t.  $\theta(P) = X \setminus g(Y \setminus (f(P)))$ . Let  $\theta : \mathbb{T}_x \rightarrow \mathbb{T}_X$ , where  $\mathbb{T}_X$  is the set of up-set of  $X$  and clearly, as a whole set,  $X, Y$  are up-sets. So  $\mathbb{T}_X$  is complete. For each up-set  $P$ , define  $\theta(P) = X \setminus g(Y \setminus (f(P)))$ . Now, if  $P_1 \subset P_2$ , and they are both up-sets. As  $f(X) = S$ , so  $f(P) \subset S$  and let  $u, v$  be in the image of  $f$  and  $u \leq v$ . Write  $f(x) = u, f(y) = v$ , as  $X$  is a total order, we have  $u \leq v \Rightarrow x \leq y$ , for if not,  $x \not\leq y$ , then  $x \geq y$  and so  $u \geq v$  which is a contradiction. Now let  $u \in f(P)$ , and  $v \in S, v = f(y)$  and  $u \leq v$ , so  $x \leq y$ . As  $P$  is a up-set,  $x \in P$ , so  $y \in P$  and hence  $y \in f(P)$ . Hence by definition  $f(P)$  is an up-set in  $Y$ . And so  $g(Y \setminus f(P))$  is a complement of an up-set and so  $\theta(P)$  is indeed an up-set in  $X$  and so  $\theta$  is well define, and is clearly order-preserving. Therefore, use fixed point theorem, we have a fixed point for  $\theta$  and so we have a bijection which is the same function as we defined in the proof of Cantor-Berstein Theorem in the lecture.

$B_2/11$  The first part is book work.

(a): Yes. Suppose  $X$  is finite, say  $X = \{a_1, a_2 \dots a_n\}$  and so the rank of  $X$  is  $\max_i \{\text{rank}(a_i) + 1\}$ , which is a successor.

(b): No. Clearly,  $\omega + 1$  has rank  $\omega + 1$  but  $\omega + 1$  is not finite. (c): No. As is discussed in Example sheet 4, the rank of  $\mathbb{R}$  is  $\omega + 1$ , which is finite but  $\mathbb{R}$  is uncountable.

$A_3/8$  (i) book work.

(ii)(a)  $T =$  Theory of posets,  $\Omega = \{\leq\}$ ,  $\leq$  has arity 2.

$$(a) (\forall x)(x \leq x)$$

$$(b) (\forall x)(\forall y)((x \leq y) \wedge (y \leq x)) \Rightarrow (x = y)$$

$$(c) (\forall x)(\forall y)(\forall z)((x \leq y) \wedge (y \leq z)) \Rightarrow (x \leq z)$$

$$(d) (\forall x)(\exists y)((x \leq y) \wedge (x \neq y))$$

(b) Take the first three lines above, which axiomatises the theory of poset, and add:

$$(\exists x)(\forall y)((\neg(x \leq y) \wedge (y \neq x)) \Rightarrow (\exists z)(y \leq z) \wedge (y \neq z)).$$

(c) Take the first three lines in (a) and add:

$$(\exists x_1)(\forall y)(\neg(x_1 \leq y))$$

$$(\exists x_2)(\forall y)(\neg(x_2 \leq y))$$

$$(\exists x_3)(\forall y)(\neg(x_3 \leq y))$$

.

.

(d) No. Suppose we can, then let  $T$  be the theory and we add:

$$(\exists x_1)(\forall y)(\neg(x_1 \leq y)).$$

.

.

Take  $S$  to be the new theory, and any finite subset of  $S$  has a model, but  $S$  does not.

(e) No. Suppose we can, then let  $T$  be the theory and we add uncountably many constants, and:

$$(\forall i \neq j)(c_i \neq c_j)$$

$$(\forall c_i)(\exists x)(x \geq c_i)$$

Then the new theory has a model as any finite subset has a model. Then by Downward Lowenheim–Skolem Theorem, we have a countable model, which is impossible.

## 9.2 2005

1/II/16F The first part is book work and we used Axiom of Choice when we are defining  $x_{\alpha+} = x'_\alpha$  for some  $x'_\alpha > x_\alpha$  and we use Axiom of Choice to take one such  $x'_\alpha$ .

Now, let  $V$  be the set of independent sets in the vector space, ordered by inclusion. Then given a chain  $(A_i : i \in I)$  we take  $A = \bigcup_{i \in I} A_i$  and claim it is an upper bound. Firstly, as it is the union of those elements in the chain, so clearly, it contains every element in the chain as a subset. Then, suppose it is linearly dependent, then  $\exists$  non-zero  $\lambda_i \in \mathbb{Q}, v_i \in A$  s.t.  $\sum \lambda_i \cdot v_i = 0$ , and so there exists some  $N$  large enough s.t.  $v_i \in A_N$  for which this is true, and then  $A_N$  is linearly dependent, which is a contradiction. So indeed  $A$  is an upper bound, and so by Zorn's Lemma, we have a maximal element in  $V$ . The maximal element must be a basis, for if not, we have some  $v$  which is not a linear combination of elements in  $A$  and so  $A \cup \{v\}$  will also be independent, contradicting maximality. For the last part, it is in general hard to find an explicit isomorphism, but we have the following way to deduce the result: Firstly, the cardinality of  $\mathbb{R}$  is the same as that of  $\mathbb{R}^2$  by Cardinal arithmetic. (Both of them are  $2^{\aleph_0}$ ) and therefore, we have  $\mathbb{R} \leftrightarrow \mathbb{R}^2$ , say  $f : \mathbb{R} \rightarrow \mathbb{R}^2$ , which is bijective. And now we look at the image of  $\mathbb{R}$  under  $f$ , which is an order isomorphism. i.e. we have well-ordered  $\mathbb{R}^2$  in the same nature of  $\mathbb{R}$ .

2/II/16F The first part is book work (Picture is useful!) and the counterexample to show ordinal addition is not commutative is:  $1 + \omega = \omega$  but  $\omega + 1 > \omega$ .

(i) True. book work.

(ii) False.  $\omega + \omega^2 = \omega^2$ , but  $\omega^2 + \omega > \omega^2$ .

(iii) False. e.g.  $\alpha = 1, \beta = \omega_1$ .

(iv) True. As we know that  $\omega_1$  is the least uncountable ordinal, and so if both  $\alpha, \beta$  are countable, then  $\alpha + \beta$  would be countable. So at least one of  $\alpha, \beta$  is uncountable. Now, if  $\alpha \geq \omega_1$ , then we have  $\alpha + \beta \geq \omega_1$ , and equality holds only when  $\beta = 0$ . If  $\alpha < \omega_1$  i.e.  $\alpha$  is countable, then  $\beta$  must be uncountable and so  $\beta \geq \omega_1$ . But if  $\beta > \omega_1$  then  $\alpha + \beta = \beta > \omega_1$ . Therefore,  $\beta = \omega_1$  and hence the result.

3/II/16F The first part is book work and the trick is to remember that we introduced the concept of regular set. Then, we use induction to check that: every set  $x$  is a subset of  $V_\alpha$  for some ordinal  $\alpha$ , which is a-

gain book work.  $\text{card}(V_0) = 1, \text{card}(V_1) = 2$  etc. and for a set of  $k$  elements, the power set contains  $2^k$  elements, so it is  $2^{2^{\dots}}$ . Finally,  $\text{card}(V_\omega = \text{card}(\mathbb{R}))$ , because  $\text{card}(V_\omega) > 2^n \forall n \in \omega$  and is the first one with infinite cardinality. So  $\text{card}(V_\omega) = 2^{\aleph_0} = \text{card}(\mathbb{R})$ . More specifically, we have a 1-1 correspondence between  $V_\omega$  and  $\{0, 1\}^\omega$ . Each function  $f$  in  $\{0, 1\}^\omega$  corresponds to a sequence  $(a_1, a_2 \dots)$  and this corresponds to an element  $A \in V_\omega$ , where  $i \in A$  if  $a_i = 1$  and  $i \notin A$  if  $a_i = 0$  and so we have the above equality.

4/II/16F These are all book work. We used  $\neg\neg p \Rightarrow p$  when we prove  $\vdash \perp \Rightarrow p$  when we check our construction  $v$  is a valuation. (see lecture notes)

### 9.3 2006

1/II/16H The first part is book work. To check this is a lattice homomorphism, you should define something like: let  $X$  be the set of partial functions on  $f$  s.t.  $x \in X$  if  $x$  is a lattice homomorphism from  $A$  to  $\{0, 1\}$ , with  $f(a) = 0, f(b) = 1, a, b \in A$  and  $A \subset L$ , ordered by extension. And the upper bound of a chain is obtained by taking union. But lattice homomorphism is usually not in the syllabus so you don't need to worry too much about it. Email me if you want my handwritten solution for this question.

2/II/16H (a) Yes. The function  $\beta \rightarrow \beta \cdot \gamma$  is normal, as if  $\gamma_1 < \gamma_2$ , then  $\beta \cdot \gamma_1 < \beta \cdot \gamma_2$ . Also  $\beta \cdot \text{Sup} \{\gamma : \gamma < \lambda\} = \text{Sup} \{\beta \cdot \gamma : \gamma < \lambda\}$ . So we have a largest  $\gamma$ , s.t.  $\beta \cdot \gamma \leq \alpha$  and so  $\beta \cdot \gamma \leq \alpha < \beta \cdot \gamma + \beta$ . And now  $\alpha \geq \beta \cdot \gamma$ , so  $\exists \delta$ , which is unique s.t.  $\beta \cdot \gamma + \delta = \alpha$  and  $\delta < \beta$  (use Synthetic proof). Note: The key thing here is to show that the function is increasing and preserves the limit. That's why we could take the 'largest' one, by taking  $\text{Sup} \{\gamma : \beta \cdot \gamma \leq \alpha\}$ .

(b) No. Consider  $\alpha = \omega, \beta = 2$ , if we have  $\alpha = \gamma \cdot \beta + \delta$ , then if  $\gamma < \omega$  i.e.  $\gamma \cdot \beta$  must be finite and so  $\delta = \omega$  but  $\beta < \delta$ , which is a contradiction.

(c) Yes. That's the same as one of the questions on example sheet 2.

(d) No. Take  $\alpha = \beta = 1, \gamma = \omega$ .

(e) Yes. Do it by induction, using two facts which can be easily proved: the sum of two limits is again a limit, and the  $\text{Sup}$  of the limits is again a limit.

(f) Yes. Let  $\lambda$  be the given limit, and we chase the limit less than  $\lambda$ . Each time, when we pass one limit to the next one, it must be

increasing by  $\omega$  and hence  $\lambda$  is a multiple of  $\omega$ . To be more precise, as  $\alpha \rightarrow \omega \cdot \alpha$  is normal. So  $\exists \alpha$  s.t.  $\omega \cdot \omega \leq \lambda$ . Suppose  $\omega \cdot \alpha \neq \lambda$ , then  $\omega \cdot \alpha < \lambda < \omega \cdot \alpha + \alpha$ , but any ordinal between these two are successors, which is a contradiction.

3/II/16H This is not in the syllabus.

4/II/16H The first part is book work.  $\Rightarrow$ : We define  $f$  by  $f(x) = \min_{ON} \{f(y) : yrx\}$ . As  $\alpha$  is well ordered, so the minimum exists. And as  $r$  is well-founded, so  $f$  is well defined (as we send the  $r$  least element to 0. And then if  $yrx$ , we have  $f(y) < f(x)$ .

$\Leftarrow$ : Conversely, suppose we have such  $f$ . so that  $f : a \rightarrow \alpha$  and  $yrx$  implies  $f(x) < f(y)$ . We aim to find a  $r$  least element in  $a$ . Suppose not, so that  $(\forall x \in a)(\exists y)((y \in a) \wedge yrx)$ . Now we fix some  $x$ , and we have  $x_1rx, x_2rx_1 \dots$  where  $x_i \in a$ . so we have  $f(x_1) < f(x), f(x_2) < f(x_1) \dots$  and so  $f(x) > f(x_1) > f(x_2) \dots$ , which is an infinite descending chain, and so  $\alpha$  is not well-ordered, which is a contradiction.

AC is equivalent to Zorn's Lemma. Let  $r$  be a well-founded relation on a set  $a$ . So by previous we have a function  $f$  sending  $a$  to  $\alpha \in ON$  s.t.  $yrx \Rightarrow f(y) < f(x)$ . But the problem is that not every  $x, y$  need to be related. Consider in the image of  $a$  under  $f$ , if  $f(y) < f(x)$  then we say  $yrx$ . This does not contradicts the function we constructed. So by this, every  $x, y \in a$  are related, either  $xry$  or  $yrx$ . Formally, let  $X = \{\text{relation on } a, \text{ extending } r, \text{ in the above way}\}$ , ordered by extension. Given a chain, we take the union and so it is an upper bound. Therefore by Zorn's Lemma, we have a maximal element. Thus we have extend the relation to a well-ordering as now the set  $a$  is order isomorphic to  $\alpha$ .

## 9.4 2007

1/II/16G If  $P$  is complete, then every subset has a least upper bound and so is directed complete and has joins for finite subsets. Converse; y, pick any  $D \subset P$ , if  $|D| = 1$ , then  $D$  itself is a least upper bound. If  $|D| > 1$ , take any  $\{x, y\} \subset D$ , we have a join of this set, and so we have an upper bound in  $D$ . Therefore,  $D$  is directed set and by directed completeness,  $D$  has a least upper bound in  $P$ .

Now for  $[A \rightarrow B]$ , take a directed set  $D$ . For any  $f_1, f_2 \in D$ ,  $\exists f$ , extending both  $f_1, f_2$  and  $f \in D$ . Let  $g = \bigvee_{f \in D} f$  (the join), and we check that  $g$  is a least upper bound. Firstly, as  $g$  extends every  $f \in D$

so it is an upper bound. Also we need to check  $g$  is a partial function. It is equivalent to check that  $\forall x \in A$ , if  $x \in \text{dom}(g)$ , then  $x$  is only mapped to one element  $y \in B$ . Suppose not, say  $g(x) = y_1, y_2$  (So  $g$  is ill-defined). By construction,  $g$  extends  $f \in D$ . So  $\exists f_1, f_2 \in D$ , s.t.  $f_1(x) = y_1, f_2(x) = y_2$  but then we have no function which extends  $f_1, f_2$ , and  $D$  is not directed, which is a contradiction. And finally, we check it is the least upper bound. Suppose  $\exists h$ , extending every  $f \in D$ , but  $g > h$ . Then  $\exists x \in A$ , s.t.  $x \in \text{dom}(g)$  but  $x \notin \text{dom}(h)$ . Then by construction of  $g$ ,  $x \in \text{dom}(f)$  for some  $f$  and then  $h$  does not extend  $f$ . So  $h$  is not an upper bound. Hence it is directed complete.

We firstly show that  $x \ll y$  implies  $x \leq y$ .

Consider the set  $\{x, f(x), ff(x) \dots\} = F(x)$ .  $F(x)$  is closed by definition, and so if  $x \ll y$ , then  $y \in F(x)$ . But  $f(x) \geq x$  and  $f$  is order-preserving so that  $f^k(x) \geq x, \forall k \geq 1$ .

To show  $\ll$  is a partial ordering, we need:

**Symmetric** If  $x \ll y$  and  $y \ll x$ , then  $x \leq y$  and  $y \leq x$ , and so  $x = y$ .

**Reflexive** Clearly, by definition  $x \ll x$ .

**Transitivity** If  $x \ll y, y \ll z$ . Take any closed  $C$ , and  $x \in C$ , then  $y \in C$  as  $x \ll y$ . And so  $z \in C$  as  $y \ll z$ . Hence  $x \ll z$ .

$H = \{h : P \rightarrow P : h \text{ is order-preserving and } x \ll h(x) \forall x\}$  Now clearly the composition of two order preserving functions is again order preserving. And take  $h \in H$ , and any  $x \in P$ . We have  $x \ll h(x)$ , and take any closed set  $C$ , which contains  $x$ . So  $h(x) \in C$  and so  $f(h(x)) \in C$ . Hence  $x \ll f(h(x))$ , and so  $f \circ h \in H$ , so  $H$  is closed under  $f$ . Now as  $h$  is also inflationary, so by the same reason as before,  $h_1 \circ h_2 \in H, \forall h_1, h_2 \in H$ . Pick any  $h_1(x), h_2(x) \in H_x$ . We want an upper bound of them in  $H_x$ . As  $x \ll h_1(x) \forall x$ , and  $h_2(x) \in P$ , so  $h_2(x) \ll h_1(h_2(x))$  and so  $h_2(x) \leq h_1(h_2(x))$ . Also, we have  $x \leq h_2(x)$ , so  $h_1(x) \leq h_1(h_2(x))$  as  $h$  is order-preserving. And therefore,  $h_1 \circ h_2$  is an upper bound in  $H$ .

$h_0(x) = \bigvee H_x$ . Let  $x \leq y$ , then  $h(x) \leq h(y) \forall h \in H$ . So  $\bigvee H_x \leq \bigvee H_y$  and so  $h_0(x) \leq h_0(y)$ . Also, pick any closed  $C$  containing  $x$ , then  $h(x) \in C \forall h \in H$  and so  $H_x \subset C \forall x$ .  $C$  is closed, so the joins of  $h(x)$ ,  $\bigvee H_x \in C$  and so  $x \ll \bigvee H_x = h_0(x)$ . So  $h_0 \in H$ .

**Fixed point:**  $f(h_0(x)) \geq h_0(x)$  by definition.

And as  $H$  is closed, and  $h_0 \in H$ , so  $f \circ h_0 \in H$ . So  $f(h_0(x)) \in H_x$  and so  $f(h_0(x)) \leq \bigvee H_x = h_0(x)$ . So  $f(h_0(x)) = h_0(x)$ .

It lies above  $x$ , as the identity map is in  $H$  and so  $x \leq \bigvee H_x = h_0(x)$ . It is the least upper bound, as if  $x < y < h_0(x)$ , and  $f(y) = y$ . Now as  $f$  is order-preserving, we have  $f^k(x) < y < h_0(x)$ ,  $\forall k \geq 1$ , but  $f^k(x) \rightarrow h_0(x)$ , which is a contradiction.

2/II/16G I didn't manage to solve this problem, as I didn't know what happens when the set  $\{\neg q : q \in Q, v(q) = 0\} = \emptyset$ . There is a book published by London mathematical society (blue cover), by Dr.T.Forster, you may find a similar problem like this in that book.

3/II/16G The first part is book work. Now to check that  $\omega^\alpha \geq \alpha$ , use induction. And then we can easily show that  $\alpha \rightarrow \omega^\alpha$  is normal function. And so we have the largest  $\alpha_0$  s.t.  $\omega^{\alpha_0} \leq \alpha < \omega^{\alpha_0+1}$ . And it is easy to check that  $\alpha \rightarrow \omega \cdot \alpha$  is also normal. So we get Cantor normal form by induction, and use  $\forall \beta \leq \alpha, \exists$  unique  $\gamma$  s.t.  $\beta + \gamma = \alpha$ . (i.e. let  $\alpha_0$  be the largest s.t.  $\omega^{\alpha_0} \leq \alpha$  and then let  $a_0$  be the largest s.t.  $\omega^{\alpha_0} \cdot a_0 \leq \alpha$  and set  $\gamma$  to be that  $\gamma + \omega^{\alpha_0} \cdot a_0 = \alpha$  and then continue this). Now let  $R = \{\delta : \omega^\alpha \leq \delta < \omega^{\alpha+1}\}$ . If  $\beta, \gamma \in R$ , then  $\exists \alpha, \omega^\alpha \leq \beta, \gamma < \omega^{\alpha+1}$ . Let the Cantor normal form of  $\beta, \gamma$  be:

$$\beta = \omega^\alpha \cdot a_0 + \dots$$

$$\gamma = \omega^\alpha \cdot b_0 + \dots$$

So  $\beta + \gamma \geq \omega^\alpha \cdot (a_0 + b_0) > \beta, \gamma$ , and  $\gamma + \beta > \beta, \gamma$  as well. so  $\beta + \gamma \neq \beta, \gamma$ . Conversely, if we don't have such  $\alpha$ , so that means the leading term in Cantor normal form are different. So WLOG, let:

$$\beta = \omega^{\alpha_0} \cdot a_0 + \dots$$

$$\gamma = \omega^{\beta_0} \cdot b_0 + \dots, \text{ and assume } \beta_0 < \alpha_0.$$

Then  $\gamma + \beta = (\omega^{\beta_0} \cdot b_0 + \dots) + \omega^{\alpha_0} \cdot a_0 + \dots$ . And if  $\beta_0 < \alpha_0$ , we have  $\omega^{\beta_0} + \omega^{\alpha_0} = \omega^{\alpha_0}$ . To check this, we use induction applied on  $\alpha_0$ , and observe that  $\omega^{\alpha_0+1} = \omega^{\alpha_0} \cdot \omega$ , and  $\omega^{\alpha_0} + \omega^{\alpha_0} \cdot \omega = \omega^{\alpha_0+1}$ .

4/II/16G One direction is just reprove Recursion Theorem, and define  $h(a) = g\{h(a') : a' \in f(a)\}$  as an attempt.

For the other direction, suppose  $\{(a, b) : a \in f(b)\}$  is not well-founded. We try to find a  $\beta$  and  $g : \mathbb{P}(B) \rightarrow B$  s.t. there is more than one  $h$  satisfying  $(\forall a \in A)(h(a) = g\{h(a') : a' \in f(a)\})$ . Let  $B$  be a set with at least two members and  $b_1, b_2$  are two members of  $B$ . Let  $g : \mathbb{P}(B) \rightarrow B$  by:

$$g(B') = \begin{cases} b_1 & \text{if } B' = \emptyset \text{ or } B' = \{b_1\} \\ b_2 & \text{otherwise} \end{cases}$$

Suppose now  $A' \subset A$  with no minimal member of the relation  $\{< a, b > : a \in f(b)\}$ . So  $h_1(a) = b_1$  and

$$h_2(a) = \begin{cases} b_2 & \text{if } a \in A' \\ b_1 & \text{otherwise} \end{cases}$$

are solutions to  $h(a) = g\{h(a') : a' \in f(a)\}$ . Clearly,  $h_1(a) = b_1$  so  $h(a) = b_1$  and so  $g\{b_1\} = b_1$ , which satisfies the equation. For  $h_2(a)$ , if  $a \in A'$ , then  $\exists a' \in f(a)$  and  $\exists a'' \in a'$  etc. So  $g\{h(a') : a' \in f(a)\} = b_2 = h_2(a)$ .

Finally, If  $a \notin A'$ ,  $h_2(a) = b_1$ , then  $g\{h(a') : a' \in f(a)\} = g\emptyset = b_1$  and so  $h_2$  also satisfies the equation.

## 9.5 2008

1/II/16G The first part is book work. We need to be careful here as we don't know which set is larger. So we may try:  $f(x) = y$  where  $x = \min X, y = \min Y$  and for any  $x \in X$ , we define  $f$  on the subset  $I_x$  s.t.  $f(I_x) = \{f(y) : y < x\}$  and this is well defined by recursion. i.e.  $f(x) = \min Y \setminus \{f(y) : y < x\}$ . So we only have two cases:

(1) Either  $X$  is isomorphic to an initial segment of  $Y$ .

(2) Or  $f(I_x) = Y$  for some  $x \in X$ , and so  $Y$  is isomorphic to an initial segment of  $X$  as  $f$  is order-preserving.

The second part is similar to what we did in previous Tripos question. Just use the property of normal function. And the last part is the same as 2006, 2/II/16H.

2/II/16G (i) book work

(ii) book work except for the last part. Suppose we have a finite axiomatisation, then we add:

$(\forall x_1) \dots (\exists x_{2^n})(x_i \neq x_j)(2x_i = 0)$  (This is a shorthand, we add this for every natural number  $n$ ). Then this is an infinite axiomatisation, which proves the theory, and so some finite subset proves the theory, which is impossible.

(iii) Not in syllabus.

3/II/16G The first part is proved in lecture notes. For the converse, consider  $x = \{\emptyset, \{\{\emptyset\}\}\}$ , which is not transitive. But  $\bigcup x = \{\{\emptyset\}\}$  is transitive. For the second one, it is true. Let  $y \in z, z \in x$ . So



$\{y\} \in \{z\}, \{z\} \in \{x\} \in \mathbb{P}x$ . By transitivity,  $\{z\} \in \mathbb{P}x$  and so  $\{y\} \in \mathbb{P}x$ . But if  $\{y\} \in \mathbb{P}x$ , then  $\{y\} \subset x$  and so  $y \in x$ .

The second part is book work.

For the last part, rank of  $\mathbb{P}x$  is  $\alpha+1$ . This is clear, when  $\alpha$  is a successor. Now suppose  $\alpha$  is a limit, then  $rank(x) = Sup \{rank(y) + 1 : y \in x\}$  and clearly, as  $x \in \mathbb{P}x$ , so  $rank(\mathbb{P}x) \geq \alpha$ . (Here we have used the transitivity of  $V_\alpha$ ). Suppose  $rank(\mathbb{P}x) = \alpha$ , then we have  $V_\alpha = \bigcup_{\beta < \alpha} V_\beta$  and if  $\mathbb{P}x \subset V_\alpha$ , as  $x \in \mathbb{P}x$ , so  $x \in V_\alpha$ . The by definition of union,  $x \in V_d$  for some  $d < \alpha$  and so  $rank(x) \leq d + 1$ , which is a contradiction. Hence  $rank(\mathbb{P}x) = \alpha$ .

The rank of  $TC\{x\}$  is  $\alpha - 1$ , as  $rank(TC\{x\}) = Sup \{rank(y) + 1 : y \in TC\{x\}\}$ , and we have  $y = (\cup \cup \dots \cup)x$ . Now that for each  $x$ ,  $\bigcup x$  takes every element in  $v$ , for some  $v \in x$ , and so  $rank(\bigcup x) = rank(x) - 1$ . So we have  $rank(TC\{x\}) = \alpha - 1$ . e.g. consider,  $x = \{\{1, 2\}, \{3\}\}$ ,  $rank(x) = 5$ , but  $\bigcup x = \{1, 2, 3\}$ ,  $rank(\bigcup x) = 4$ .

4/II/16G book work.

## 9.6 2009

1/II/16G We say  $F$  is an attempt if  $F(\alpha) = G(\alpha, \{F(\beta) : \beta < \alpha\})$  at  $\alpha$  and  $dom(F)$  is transitive. Then we can check by induction that, if  $F, F'$  both attempt at  $\alpha$ , then  $F(\alpha) = F'(\alpha)$ , and  $\forall \alpha, \exists F$  which is an attempt at  $\alpha$ . The second part is book work. (For the significance, just write down the basic results of Cardinal Arithmetic).

For the last part, it is  $\alpha = Sup \{\omega, \omega_\omega, \omega_{\omega_\omega} \dots\}$  and the later is a set by replacement. To check that  $\alpha = \omega_\alpha$ , firstly,  $\alpha \leq \omega_\alpha$ , as for each  $\omega_{\omega \dots}$  we have some  $z < \alpha$  s.t.  $\omega_{\omega \dots} \leq z < \alpha$  and so  $\alpha \leq \omega_\alpha$ . Conversely, if  $z < \alpha$ , then  $z < \omega_{\omega \dots}$  for some  $\omega_{\omega \dots}$  and so  $\omega_z < \omega_{\omega \dots}$ . And therefore, take the supremum of that we have  $\omega_\alpha \leq \alpha$ . Hence  $\alpha = \omega_\alpha$ .

2/II/16G (i) book work.

(ii) Let T be the theory of groups.  $\Omega = \{m, i, e\}$  with arity 2, 1, 0 respectively.

$$(\forall a)(\forall b)(\forall c)m(a, m(b, c)) = m(m(a, b), c)$$

$$(\forall a)(m(e, a) = a = m(a, e)) \quad (\forall a)(m(a, i(a)) = e)$$

$$(\forall a)((a \neq e) \Rightarrow (a^2 \neq e))$$

$$(\forall a)((a \neq e) \Rightarrow (a^3 \neq e))$$

.

.

It is not finitely axiomatisable. Suppose it is, and let it be  $T$ , then the above theory would prove  $T$  and as proof is finite, so some finite subset of the above theory would prove  $T$ , which is impossible.

It is not axiomatisable. Suppose it is, let  $T'$  be the theory, and we add a constant  $x$  and:

$(x \neq e)$ .

$(x^2 \neq e)$ .

$(x^3 \neq e)$ .

.

.

.

Then every finite subset has a model, but the whole theory does not (as it implies  $x$  has infinite order), which contradicts Compactness Theorem.

3/II/16G We want to inject  $x$  into  $\alpha$  as an initial segment. Define  $f(x)$  recursively, by:

$f : x \rightarrow \alpha, f(x) = \min \alpha \setminus \{f(y) : y < x\}$ . It is well defined and is unique by recursion theorem, and we can define the minimum of the above set as  $\alpha$  is well ordering and the set is non-empty because  $x \subset \alpha$ . And so let  $\mu(x)$  be the induced order type. Now if  $x \subset y \subset \alpha$ , we have  $\mu(x)$  the order type of an initial segment of  $y$  and as  $y \subset \alpha$ ,  $\mu(y)$  is the order type of an initial segment of  $\alpha$  and hence  $\mu(x) \leq \mu(y)$ . (We could just define the function on  $y$  and on  $x$  as a subset of  $y$ ).

Now as each  $x_i$  is an initial segment of  $x_j$ , so  $(x_i)$  is nested. We define  $\mu(\bigcup_n x_n)$  by  $a, b \in \bigcup_n x_n$ , and  $a < b$  if  $a <_n b$  for some  $n$  where  $<_n$  is the ordering given by  $\mu(x_n)$  on  $x_n$ . And for any  $a, b \in \bigcup_n x_n, \exists N$ , s.t.  $a, b \in x_N$  as  $x_n$  is increasing. So we have well defined  $\mu(\bigcup_n x_n)$  to be a well ordering. The details are in the lecture notes. Now for  $\bigcup_n \mu(x_n)$ , the above ordering is the same as order  $x_1$  by  $\mu(x_1)$ , then extend to  $x_2$  as  $x_1$  is an initial segment of  $x_2$ , by  $a < b$  if  $a < b$  in  $x_1$  or  $a \in x_1, b \in x_2$  or  $a < b$  in  $x_2 \setminus x_1$ . And continue this inductively. Therefore, the two ordering collapse.

It does not hold if we remove that condition. Consider  $x_1 = \{\omega\}, x_2 = \{1, \omega, \omega + 1\}, x_3 = \{1, 2, \omega, \omega + 1, \omega + 2\} \dots$ . So  $\mu(x_n) = 2n - 1$  and so  $\bigcup_n \mu(x_n) = \omega$  but  $\mu(\bigcup_n x_n) = \omega \cdot 2$ .

It is decreasing and bounded below by 0, by using  $(\mu(x) \leq \mu(y))$  if  $x \subset y$ . So it must tend to a constant.

No. Consider  $x_1 = \omega = \{1, 2, \dots\}$ ,  $x_2 = \omega \setminus \{1\}$ ,  $\dots$ ,  $x_n = \omega \setminus \{1, 2, \dots, n\}$ ,  $\dots$ . Then  $\mu(x_n) = \omega$  as it is still infinite and  $\leq \omega$ . So  $\bigcap_n \mu(x_n) = \omega$ . But  $\mu(\bigcap_n x_n) = 0$ .

4/II/16G The first two parts are book work and it is clear by the notion of  $TC(x)$  that  $TC(x) = x \cup TC(\bigcup x)$ , and use  $\bigcup\{x\} = x$ , we have that  $TC(\{x\}) = \{x\} \cup TC(x)$ .

$HC$  is transitive. Let  $y \in x, x \in HC$ .

So we know that  $\{x\}, x, \bigcup x, \bigcup\bigcup x \dots$  are all countable. Now  $y \in x$ , and so  $y \subset \bigcup x$ . Hence,  $y$  is countable. Also  $\bigcup y \subset \bigcup\bigcup x$  etc. So  $y, \bigcup y \dots$  are countable, and also  $\{y\}$  is countable, so  $y \in HC$ . Moreover, if  $x \in HC$ ,  $x \subset HC$ . Conversely, suppose  $x \subset HC$ , then as  $HC$  does not contain uncountable element, so itself is a countable class, and so  $x$  is countable.  $\bigcup x$  is a countable union of countable class as  $\forall y \in x, y \in HC$ , and similarly for  $\bigcup x, \bigcup\bigcup x$ . Therefore,  $x \in HC$ . Now we want to show, if  $x \in HC$ , then  $\bigcup x \in HC$ . But  $\forall y \in x, y \in HC$  and so  $\bigcup x \subset HC$  and therefore,  $\bigcup x \in HC$ . For separation, for a formulae  $p$ , we let  $y = \{a \in x : p(a)\}$ . So we have  $y \subset x$  and as  $x \in HC$ , we have  $x \subset HC$ , and so  $y \subset HC$ . Therefore,  $y \in HC$ . In fact, it satisfies all axioms except power set. (the power set of infinite set is uncountable).

## 9.7 2010

1/II/16G This is a special case of  $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta, \alpha < \beta$  and the proof is book work.  $\aleph_0$  is regular. As it is the first infinite cardinal, and any finite sum of finite cardinal is still finite. Similarly,  $\aleph_1$  is the first uncountable cardinal, and any countable sum of countable cardinal is still countable.  $\aleph_2$  is again regular. By definition,  $\omega_2$  is the least ordinal which does not inject into  $\omega_1$  and  $\aleph_2$  is its cardinality. Suppose we have a sum of fewer than  $\aleph_2$  cardinals, each of which is less than  $\aleph_2$ . Then each such ordinal can be injected into  $\omega_1$  and we have less than  $\omega_1$  copies of them. So the cardinality of the set (We treat addition as disjoint union) is  $\aleph_1 \cdot \aleph_1 = \aleph_1$ . Then we have  $\aleph_1 = \aleph_2$ , which is a contradiction. Finally, for  $\aleph_\omega$ , it is not regular.  $\omega_\omega = \text{Sup} \{\omega_0, \omega_1, \omega_2, \dots\}$ . The later is a set by Replacement, so it is well defined. Now, we have  $\sum_{n \in \omega} \aleph_n = \aleph_\omega$ , which is a required sum.

2/II/16G We have seen several questions like this before, so I don't need to explain anything for the first part.

If  $\alpha$  is not a power of  $\omega$ . Then  $\exists$  largest  $\beta$ , s.t.  $\omega^\beta \leq \alpha$  and  $\exists \gamma < \alpha$  s.t.  $\omega^\beta + \gamma = \alpha$ . Now  $\alpha$  is not a power of  $\omega$  and so  $\gamma$  is non-zero. But then this implies that  $\alpha$  is decomposable.

Conversely, if  $\alpha$  is a power of  $\omega$ , if  $\alpha = \omega^0 = 1$ , it is clearly not decomposable. For successor,  $\alpha = \omega^{\beta+1} = \omega^\beta \cdot \omega$ . Suppose it is decomposable, say  $\omega^\beta \cdot \omega = \delta + \gamma$ , then  $\delta < \omega^\beta \cdot \omega$ , then by definition of the limit,  $\delta < \omega^\beta \cdot k$ , for some  $k < \omega$ . Then use synthetic definition, the order type of  $\gamma$  is still  $\omega^\beta \cdot \omega$ , as  $\omega$  itself cannot be a sum of two finite ordinals. Hence  $\alpha$  is not decomposable. Finally, when  $\beta$  is a limit,  $\alpha = \omega^\beta$ . Let  $\alpha = \delta + \gamma$ . Then we have  $\delta < \omega^{\beta_1}, \gamma < \omega^{\beta_2}$  for some  $\beta_1, \beta_2 \leq \beta$ , as  $\alpha = \text{Sup} \{ \omega^\theta : \theta < \beta \}$ . If  $\beta_1 = \beta_2$ , then we have  $\omega^{\beta_1} \cdot 2$ , which cannot be  $\alpha$ . So WLOG, say  $\beta_1 < \beta_2$ . Then  $\delta + \gamma = \gamma$ . So  $\gamma = \beta$ . And  $\gamma + \delta = \omega^{\beta_2} + \omega^{\beta_1} < \omega^{\beta_2} \cdot 2$ . And  $\omega^{\beta_2} < \omega^\beta$ , so we have  $\beta_2 < \beta$ . Hence  $\omega^{\beta_2} \cdot 2 < \omega^{\beta_2} \cdot \omega = \omega^{\beta_2+1} < \omega^\beta$ , as  $\beta$  is a limit.

Therefore, we conclude that  $\alpha = \omega^\beta$  is not decomposable when  $\beta$  is a limit, and hence the result.

3/II/16G The first two parts are book work.

Let  $x$  be transitive of rank  $\alpha$ . Then  $\alpha = \text{Sup} \{ \text{rank}(y) + 1 : y \in x \}$ , and  $x \subset V_\alpha$ . We use induction on  $\alpha$ . It is nothing to prove when  $\alpha = 0$ . For successor, say  $\alpha = \gamma^+$ , by definition of Sup,  $\exists y \in x$ , s.t.  $\text{rank}(y) = \gamma < \alpha$ . Then by induction, we have  $\beta < \gamma, \exists z \in y$ , s.t.  $\text{rank}(z) = \beta$  and as  $x$  is transitive so  $z \in x$ . For  $\alpha$  a non-zero limit.  $V_\alpha = \bigcup_{\lambda < \alpha} V_\lambda$ . Then we have a sequence of ordinals  $\lambda_i$  s.t.  $\text{Sup} \{ \lambda_i \} = \alpha$ , and  $y_i \in x$  s.t.  $\text{rank}(y_i) = \lambda_i$ . (If not, then  $\text{rank}(x) < \alpha$ ). For each  $y_i$ , if  $\beta_i < \lambda_i, \exists z_i \in y_i$ , s.t.  $\text{rank}(z_i) = \beta_i$ , by induction. Then  $z_i \in x$  as  $x$  is transitive. Now as  $\lambda_i$  is increasing to  $\alpha$ , so  $\forall \beta < \alpha$ , we have  $z$  s.t.  $\text{rank}(z) = \beta$ .

For  $\alpha < \omega$ , as  $\{ \alpha - 1 \}$  has rank  $\alpha, \forall \alpha < \omega$ . But if  $\alpha = \omega$ , then  $V_\alpha = \bigcup_{\lambda < \alpha} V_\lambda$ . Then if  $x \subset V_\omega$ , and  $x \not\subset V_\lambda \forall \lambda < \omega$ . Then  $x$  must be infinite.

For the last part, we may try  $\{x, \{x\}\}$ . The rank of this set is  $\text{rank}(x) + 2$  and so we can form this for all rank  $< \omega$  but  $\geq 2$ . For 1, we have  $\{\emptyset\}$  transitive, and similarly,  $\emptyset$  itself is transitive. Therefore, the answer is still  $\alpha < \omega$ .

4/II/16G book work. For the last part, use Zorn's Lemma to find a maximal consistent set as we did in the lecture.