University of Cambridge

Part II of the Mathematical Tripos

Logic and Set Theory

Lectured by András Zsák, Lent 2024–25

Notes by Avish Kumar
ak2461@cam.ac.uk
https://ak1089.github.io/maths/notes

Version 1.17

Contents

1 Propositional Logic **3**
- **1.1 Propositions** **3**
- **1.2 Semantic Entailment** **4**
- **1.3 Syntactic Entailment** **5**

2 Well-Orderings and Ordinals **9**
- **2.1 Orderings and Order-Isomorphism** **9**
- **2.2 Ordering Well-Ordered Sets** **13**
- **2.3 Ordinals** **14**
- **2.4 Ordinal Arithmetic** **17**

3 Posets and Zorn's Lemma **21**
- **3.1 Partially Ordered Sets** **21**
- **3.2 Zorn's Lemma** **24**
- **3.3 The Axiom of Choice** **27**

4 First-Order Predicate Logic **29**
- **4.1 Language** **29**
- **4.2 Theories and Models** **32**
- **4.3 Syntactic Entailment** **35**
- **4.4 Peano Arithmetic** **41**

5 Set Theory **43**
- **5.1 Zermelo-Fraenkel Set Theory (ZF)** **43**

1 Propositional Logic

1.1 Propositions

The language of propositional logic consists of a set P of *primitive propositions*, and the set $L(P)$ of propositions. These statements in the language are meaningful, and can be `true` or `false`.

Definition 1.1 (Set of Propositions L)

Given a set P of primitive propositions, the set L is defined to be the smallest set containing P with $\bot \in L$ (the symbol for `false`) such that if p and q are in L, then $(p \Rightarrow q)$ is in L.

Often, $P = \{p_1, p_2, p_3, \ldots\}$ is a countably infinite set of primitive propositions. In this case, we have propositions in L like $(p_1 \Rightarrow p_2)$ or $(p_1 \Rightarrow p_2)$, $(\bot \Rightarrow (p_1 \Rightarrow p_2))$, and $((p_1 \Rightarrow p_2) \Rightarrow (p_1 \Rightarrow p_3))$. Also, we have $((p \Rightarrow \bot) \Rightarrow \bot)$ for each $p \in L$.

The set L is built from $P \cup \{\bot\}$ inductively, which means that we can define it inductively. Define $L_1 = P \cup \{\bot\}$ and $L_{n+1} = L_n \cup \{(p \Rightarrow q) : p, q \in L_n\}$. Each of these are countable, by induction, and $L = L(P)$ is the countable union of these sets, and thus countable.

In fact, every proposition is built *uniquely* using this construction. For each $p \in L$, either $p \in P$ is primitive, or $p = \bot$, or $p = (q \Rightarrow r)$ for unique $q, r \in L$.

Note: Each proposition is a finite string of symbols in the alphabet $P \cup \{\bot, \Rightarrow, (,)\}$. However, not every such string is a proposition: "$(\Rightarrow (\Rightarrow \bot\bot)\bot)$" is nonsense.

Definition 1.2 (Valuation)

A *definition-propositional-valuation* on L is a function $v : L \to \{\mathtt{0}, \mathtt{1}\}$ with $v(\bot) = \mathtt{0}$ satisfying:

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

This ensures the value of $\bot =$ `false` is `0`, and a true statement doesn't imply a false one.

For example, if $v(p_1) = \mathtt{1}$ and $v(p_2) = \mathtt{0}$, then $v((\bot \Rightarrow p_1) \Rightarrow (p_2 \Rightarrow p_1)) = \mathtt{1}$.

Proposition 1.3 (Valuations on Primitives)

If v and v' are valuations which agree on P, then in fact they agree on $L(P)$. Also, for any function $w : P \to \{\mathtt{0}, \mathtt{1}\}$, there is a valuation v on L such that v and w agree on P.

Proof: We have $v(\bot) = v'(\bot) = \mathtt{0}$ by definition, and by assumption they agree on P. Then they agree on L_1. Continue inductively, assuming that v and v' agree on L_n.

Let $p \in L_{n+1} \setminus L_n$. Then $p = (q \Rightarrow r)$ for unique $q, r \in L_n$. By induction, v and v' agree on q and r. But then they must agree on p, and since p was arbitrary they agree on L_{n+1}. Thus they agree on all L_n, and so they must agree on L.

For the second part, we define $v(p) = w(p)$ for all $p \in P$, and $v(\bot) = \mathtt{0}$. This defines a unique valuation v on L_1. Having defined v on L_n for some n, write $p \in L_{n+1} \setminus L_n$ as $p = (q \Rightarrow r)$ for unique $q, r \in L_n$, and define $v(p)$ using the rule based on $v(q)$ and $v(r)$. This gives a unique extension of v to L_{n+1}: by induction, this gives a unique valuation v on all of L. □

Definition 1.4 (Tautology)

Let $t \in L$. We say that t is a *tautology* if $v(t) = \texttt{1}$ for all valuations v on L. For example, $(\bot \Rightarrow \bot)$ is a tautology, as any valuation v gives it value $\texttt{1}$.

We now enrich our language by introducing a few more symbols.

notation	expansion	interpretation
$\top$	$(\bot \Rightarrow \bot)$	"true": a tautology, true in all cases
$\neg p$	$(p \Rightarrow \bot)$	"not-p": false if p is true and true if p is false
$p \vee q$	$(\neg p \Rightarrow q)$	"p or q": true if either p or q is true
$p \wedge q$	$\neg(p \Rightarrow \neg q)$	"p and q": true only if both p and q are true

Note: There are tautologies not involving the symbol $\bot$, for example $(p \Rightarrow (q \Rightarrow p))$. One can check that this statement is a tautology by checking every possible valuation for p and q in a truth table. Such a table enumerates these values to check the possible valuations of the statement.

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

As desired, the valuation of $(p \Rightarrow (q \Rightarrow p))$ is always $\texttt{1}$.

Example 1.5 (Important Tautologies)

The above statement has a heuristic interpretation: "a true statement is implied by anything". There are other such basic tautologies which are important:

1. "The law of excluded middle" is the tautology $(\neg\neg p \Rightarrow p)$, or alternatively $(p \vee \neg p)$. This is the statement that p is either `true` or `false`, in which case $\neg p$ holds.
2. For any $p, q, r \in L$, the tautology $(p \Rightarrow (q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)))$ holds. Note that the truth table demonstrating this has $2^3 = 8$ rows to check.

1.2 Semantic Entailment

Definition 1.6 (Semantic Entailment)

For $S \subseteq L$ and $t \in L$, we say S *semantically entails* t if for any valuation v which satisfies $v(s) = \texttt{1}$ for all $s \in S$, we also have $v(t) = \texttt{1}$. We write $S \vDash t$.

This is an extension of the idea of implication to sets of propositions.

Corollary: t is a tautology if and only if $\varnothing \vDash t$. We write $\vDash t$ for short.

Example 1.7 (Modus Ponens)

We have $\{p, (p \Rightarrow q)\} \vDash q$. The process of deducing q from p and $(p \Rightarrow q)$ is known as *modus ponens*, which is Latin for "affirming mode".

(This is because if $v(p) = \texttt{1}$ and $v(q) = \texttt{0}$, then $v(p \Rightarrow q) = \texttt{0}$ by the implication rule.)

Definition 1.8 (Model)

For $t \in L$ and a valuation v, we say that t is "true in v" (or "v is a *definition-propositional-model* of t") if $v(t) = \mathtt{1}$. Similarly, for $S \subseteq L$, we say v is a model of S if $v(s) = \mathtt{1}$ for all $s \in S$.

Corollary: $S \vDash t$ if and only if t is true in every model of S.

1.3 Syntactic Entailment

A notion of *proof* consists of *axioms* and *rules of deduction*. These are statements taken as true no matter what, and rules by which we can deduce more statements as true. In the model of propositional logic, we have the following three axioms:

1. For $p, q \in L$, $p \Rightarrow (q \Rightarrow p)$.
2. For $p, q, r \in L$, $p \Rightarrow (q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.
3. For $p \in L$, $\neg\neg p \Rightarrow p$.

Note: These axioms are all tautologies.

In propositional logic, we also have only one rule of deduction.

Definition 1.9 (Modus Ponens)

From p and $(p \Rightarrow q)$, we may deduce q.

How do we use this rule of deduction?

Definition 1.10 (Proof)

Given $S \subset L$ and $t \in L \setminus S$, a proof of t from S is a finite sequence of propositions $t_1 \dots t_n \in L$ such that $t_n = t$, and for each t_i we have either:

1. t_i is an axiom of propositional logic.
2. $t_i \in S$, so that t_i is a *premise* or *hypothesis*
3. t_i is obtained by *modus ponens* from earlier lines: there are $j, k < i$ with $t_k = (t_j \Rightarrow t_i)$.

If there is such a proof of t from S, we say that S *syntactically entails* t, and write $S \vdash t$. If t is such that $\varnothing \vdash t$, we say that t is a *theorem* and write $\vdash t$.

Example 1.11 (Proof given 2 Hypotheses)

We would like to show that $\{(p \Rightarrow q), (q \Rightarrow r)\} \vdash (p \Rightarrow r)$. We prove this as follows:

1. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ (A2)
2. $(q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$ (A1)
3. $q \Rightarrow r$ (premise)
4. $p \Rightarrow (q \Rightarrow r)$ (MP)
5. $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ (MP)
6. $p \Rightarrow q$ (premise)
7. $p \Rightarrow r$ (MP)

Example 1.12 (Proof of a Theorem)

We would like to show that $\vdash (p \Rightarrow p)$. We prove this as follows:

1. $p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$ (A1)
2. $(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$ (A2)
3. $(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$ (MP)
4. $p \Rightarrow (p \Rightarrow p)$ (A1)
5. $p \Rightarrow p$ (MP)

Theorem 1.13 (Deduction Theorem)

Let $S \subseteq L$ with $p, q \in L$. Then $S \vdash (p \Rightarrow q)$ if and only if $(S \cup \{p\}) \vdash q$.

Proof: Assume $S \vdash (p \Rightarrow q)$. Then we can write down a proof of $(p \Rightarrow q)$ from S. Now, we can simply add p (premise) and q (MP) to obtain a proof of q from $S \cup \{p\}$ as desired.

Now suppose that $(S \cup \{p\}) \vdash q$, and let $t_1 \dots t_n$ be a proof of q witnessing this. Then $S \vdash (p \Rightarrow t_i)$ for all i, which we demonstrate by induction. In the case of $i = n$, this will show $S \vdash (p \Rightarrow q)$.

If t_i is an axiom or $t_i \in S$, we can prove this using:

1. t_i (premise or axiom)
2. $t_i \Rightarrow (p \Rightarrow t_i)$ (A1)

which gives a proof of $p \Rightarrow t_i$ (by MP). Otherwise, $t_i = p$ in which case we wish to show only that $S \vdash (p \Rightarrow p)$. But we have seen this is a theorem, so clearly it is provable. Finally, we must deal with the case where t_i is an instance of modus ponens, and $t_k = (t_j \Rightarrow t_i)$ for $j, k < i$. Here:

1. $(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$ (A2)
2. $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ (MP)

which gives a proof of $p \Rightarrow t_i$ (again by MP).

Thus $S \vdash (p \Rightarrow t_i)$ for all $1 \leqslant i \leqslant n$, in particular, as $t_n = q$, we have $S \vdash (p \Rightarrow q)$. □

Corollary: The symbol "⇒" really does behave like implication in familiar formal proofs!

We now have two notions of entailment: semantic entailment $\vDash$ and syntactic entailment $\vdash$. We want to prove the *completeness theorem*, which states that these two notions are equal.

This splits into two parts: the Soundness Theorem claims that $(S \vdash t)$ implies $(S \vDash t)$, while the Adequacy Theorem means the converse. This means that our syntactic system is *sound* (it doesn't prove false statements) and that it is *adequate* (it is able to prove all true statements).

Theorem 1.14 (Soundness Theorem)

If $S \subseteq L$ and $t \in L$ where $S \vdash t$, then $S \vDash t$.

Proof: Let $t_1 \dots t_n$ be a proof of t from S. Let v be a model of S. We require $v(t) = \mathtt{1}$. We prove this via induction on the steps t_i.

Suppose t_i is an axiom. Then it is a tautology, and so $v(t_i) = \mathtt{1}$. Similarly, if t_i is a premise, then $t_i \in S$, and so $v(t_i) = \mathtt{1}$ since v is a model of S.

Now suppose t_i is an application of modus ponens. All previous lines have value $v(t_j) = v(t_k) = \mathtt{1}$, so given that $t_k = (t_j \Rightarrow t_i)$, we must have $v(t_i) = \mathtt{1}$ as well. Thus $v(t) = v(t_n) = \mathtt{1}$, ie. $S \vDash t$. □

Now, we aim for the Adequacy Theorem, which is the converse of this statement. To do so, we introduce a few concepts.

Definition 1.15 (Consistency)

Let $S \subseteq L$. We say S is *inconsistent* if $S \vdash \bot$, and *consistent* otherwise.

Corollary: For the special case of consistency, the Adequacy Theorem holds. If $S \vDash \bot$, then any model v of S has $v(\bot) = \mathtt{1}$, but this is not allowed, so in fact there cannot be a model of S.

Definition 1.16 (Deductive Closure)

A set $S \subseteq L$ is *deductively closed* if every $t \in L$ with $S \vdash t$ is itself contained in S.

Note: Every deductively closed set must be infinite, as for any $t \in S$ there is a proof of $t \Rightarrow (t \Rightarrow t)$ from S using the first axiom. (Equivalently, as $\top$ is a theorem, there are infinitely many theorems).

This definition allows us to prove an important theorem.

Theorem 1.17 (Model Existence Lemma)

Let $S \subseteq L$. If S is consistent, then S has a model.

Proof: Let us build up such a model by construction. Define v by $v(t) = \mathtt{1}$ for all $t \in S$, with $v(\bot) = \mathtt{0}$. More generally, if $S \vdash t$, then by the Soundness Theorem $v(t) = \mathtt{1}$ for any such t. Thus we might first try

$$v(t) = \begin{cases} \mathtt{1} & \text{if } S \vdash t \\ \mathtt{0} & \text{otherwise} \end{cases}$$

Unfortunately, this is nonsense. It is quite possible that $S \nvdash t$ and $S \nvdash \neg t$. We will enlarge S to avoid this issue. (Note that we only consider the case where set P of primitive propositions is countable: we prove the general case later on in 3.16.)

Consider the recursive definition of the set of propositions (following 1.1). We note that L must be countable as a consequence of this definition, as the countable union of countable sets L_n.

We enumerate L as $t_1, t_2 \dots$ and consider consistent sets $T \subseteq L$. If $t \in L$, then one of $T \cup \{t\}$ or $T \cup \{\neg t\}$ is consistent. If not, then we would have $(T \cup \{t\}) \vdash \bot$ and $(T \cup \{\neg t\}) \vdash \bot$, so by the Deduction Theorem (1.13) we have both $T \vdash t$ and $T \vdash (t \Rightarrow \bot)$, and hence Modus Ponens (1.9) yields $T \vdash \bot$, contradicting the consistency of T.

Now start with the consistent set $S_0 = S$. Define the sets S_n by induction, assuming that S_{n-1} is defined and consisrent. Then let S_n be either $S_{n-1} \cup \{t_n\}$ or $S_{n-1} \cup \{\neg t_n\}$ so that it is consistent. Finally, we define $\bar{S}$ to be the union of these S_n.

Observe that $S \subseteq \bar{S}.$, and for all $t \in L$ either $t \in \bar{S}$ or $\neg t \in \bar{S}$. Also, $\bar{S}$ is consistent: if there was a proof witnessing $S \vdash \bot$, then since this proof is finite it uses a finite number of propositions, and so there is some S_n which contains all those propositions, which would then be inconsistent.

$\bar{S}$ is deductively closed. Indeed, if $t \notin S$ then $\neg t = (t \Rightarrow \bot) \in S$. So we can write down a proof of t from S, and add the lines $t \Rightarrow \bot$ (premise) and $\bot$ (MP), so $\bar{S}$ would not be consistent.

We now define the valuation $v : L \to \{\mathtt{0}, \mathtt{1}\}$ by

$$v(t) = \begin{cases} \mathtt{1} & \text{if } \bar{S} \vdash t \text{ (that is, } t \in \bar{S}) \\ \mathtt{0} & \text{otherwise} \end{cases}$$

which is a model of $\bar{S}$ and thus a model of S, once we prove it is a valuation. Note that this *cc* indeed satisfies $v(\bot) = \mathtt{0}$ since $\bot \notin \bar{S}$ by deductive closure and consistency.

We consider three cases.

1. If $v(p) = \mathtt{1}$ and $v(q) = \mathtt{0}$, we need $v(p \Rightarrow q) = \mathtt{0}$. If not, then we have $\bar{S} \vdash (p \Rightarrow q)$. This allows us to write down a proof of $p \Rightarrow q$ from $\bar{S}$ and follow it by p (premise) and q (MP) to attain a proof of q from $\bar{S}$. By deductive closure, $q \in \bar{S}$, so $v(q) = \mathtt{1}$ (a contradiction).
2. If $v(q) = \mathtt{1}$, we need $v(p \Rightarrow q) = \mathtt{1}$. Given q, we can write down the proof $q \Rightarrow (p \Rightarrow q)$ (A1), q (premise), and then $p \Rightarrow q$ (MP). So $\bar{S} \vdash (p \Rightarrow q)$, so $v(p \Rightarrow q) = \mathtt{1}$ as required.
3. Finally, consider $v(p) = \mathtt{0}$, so we need $v(p \Rightarrow q) = \mathtt{1}$, that is $\bar{S} \vdash (p \Rightarrow q)$. By the Deduction Theorem (1.13) this is equivalent to $\bar{S} \cup \{p\} \vdash q$. We can do this using p (premise), $p \Rightarrow \bot$ (premise, since $p \notin \bar{S}$), $\bot$ (MP), $\bot \Rightarrow ((q \Rightarrow \bot) \Rightarrow \bot)$ (A1), and then using MP to prove $\neg q$ followed by q. Therefore we have $v(p \Rightarrow q) = \mathtt{1}$ as required.

Therefore this v is a valuation, and thus a model of $\bar{S}$ and thereby S. □

Theorem 1.18 (Adequacy Theorem)

If $S \subseteq L$ and $t \in L$ where $S \vDash t$, then $S \vdash t$.

Proof: Since $S \vDash t$, we have $S \cup \{\neg t\} \vDash \bot$. Then $S \cup \{\neg t\} \vdash \bot$, and so by the Deduction Theorem we have $S \vdash \neg\neg t$. We then add the lines $\neg\neg t \Rightarrow t$ (A3) and t (MP) to show $S \vdash t$. □

Theorem 1.19 (Completeness Theorem)

The notions of semantic and syntactic entailment "$\vDash$" and "$\vdash$" are in fact equivalent: if $S \subseteq L$ and $t \in L$, then $S \vDash t \iff S \vdash t$.

Proof: Obvious by the Soundness Theorem (1.14) and the Adequacy Theorem (1.18). □

Theorem 1.20 (Compactness Theorem)

Let $S \subseteq L$ and $t \in L$. If $S \vDash t$, then there is a finite subset $S' \subseteq S$ with $S \vDash t$.

Proof: By the Completeness Theorem, we may replace "$\vDash$" by "$\vdash$", which makes the proof trivial: take a proof witnessing $S \vdash t$, and define S' to be the finite set of premises used. □

Note: This is highly nontrivial without the Completeness Theorem!

Corollary: Let $S \subseteq L$. If every finite subset of S has a model, then S has a model.

Proof: Suppose that S does not have a model. Then $S \vDash \bot$. By the Compactness Theorem, there is a finite subset $S' \subseteq S$ with $S' \vDash \bot$, which contradicts S' having a model. □

Note: This corollary is actually equivalent to the Completeness Theorem. If $S \vDash t$, then we have $S \cup \{\neg t\} \vDash \bot$. Then there is a finite subset $S' \subseteq S$ with $S' \cup \{\neg t\} \vDash t$, and so $S' \vDash t$.

Theorem 1.21 (Decidability Theorem)

Let $S \subseteq L$ be a finite set with $t \in L \setminus S$. Then there is an algorithm which can determine in finite time whether $S \vdash t$.

Proof: By the Completeness Theorem, we may replace "$\vdash$" by "$\vDash$", which makes the proof trivial: if there are n primitive propositions which occur in $S \cup \{t\}$, simply enumerate a truth table with 2^n possible values, and evaluate $v(t)$ to see whether $v(t)$ is always $\mathtt{1}$. □

Note: This is again highly nontrivial without the Completeness Theorem! If $S \vdash t$, we can write proofs from S and eventually arrive at t, but if $S \nvdash t$ then this algorithm never terminates.

2 Well-Orderings and Ordinals

2.1 Orderings and Order-Isomorphism

We now consider *orderings*, which are ways of equipping sets with a notion of "bigger" elements.

Definition 2.1 (Total Order)

A *linear* (or *total*) order on a set X is a binary relation $<$ on X which is:

1. irreflexive: for all $x \in X$, we have $\neg(x < x)$.
2. transitive: for all $x, y, z \in X$, we have $((x < y) \wedge (y < z)) \Rightarrow (x < z)$.
3. trichotomous: for all $x, y \in X$, we have $(x < y) \vee (x = y) \vee (y < x)$.

Note that *precisely* one of the three options in trichotomy occurs. For example, if $x = y$, then neither $x < y$ nor $y < x$, and if $x < y$, then $y < x$ implies $x < x$ by transitivity, violating the irreflexivity condition.

We say that "X is linearly ordered by $<$" if the relation $<$ satisfies this definition. In general, we may say that "X is a linearly ordered set".

Note: When we use the symbols $\wedge$, $\neg$, and so on, we are back to simply using these by the usual definitions we know and love, rather than the overly formal meanings from the previous section!

Example 2.2 (Linearly Ordered Sets)

The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are linearly ordered under the usual order $<$.

An important non-example is the relation on the powerset $\wp(X)$ given by $a < b$ if and only if $a \subset b$. This is not trichotomous for $|X| > 2$: if $x, y \in X$ then neither $\{x\}$ nor $\{y\}$ are less than the other.

Note: For a linear order $<$ on a set X, we write $x > y$ for $y < x$ as notational shorthand.

Definition 2.3 ($\leqslant$)

For a linear order $<$ on a set X define the relation $\leqslant$ by $x \leqslant y$ if and only if $(x < y) \vee (x = y)$. Note that this relation satisfies:

1. reflexivity: $x \leqslant x$ for all $x \in X$.
2. antisymmetry: if $x \leqslant y$ and $y \leqslant x$, then $x = y$.
3. transititivty: if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$.
4. trichotomous: either $x \leqslant y$ or $y \leqslant x$ (or both, if $x = y$).

Note: If a set X is linearly ordered by $<$, then every subset $Y \subseteq X$ is also linearly ordered by the restriction of $<$ to Y.

Definition 2.4 (Well-Ordering)

A *well-ordering* of a set X is a linear order $<$ on X such that every nonempty subset of X has a *least element* satisfying $(\forall\, S \subseteq X) : (S \neq \varnothing \implies (\exists\, m \in S) : (\forall\, x \in S,\, m \leqslant x))$.

This least element m must be unique by the antisymmetry of $\leqslant$.

Example 2.5 (Well-Ordering)

$\mathbb{N}$ with the usual order is well-ordered. $\mathbb{Z}$ is not (for example, the set of negative integers has no least element). However, $\mathbb{Z}$ can be well-ordered using another relation:

$$x < y \iff (|x| < |y|) \vee ((x = -y) \wedge (x < 0))$$

which orders the integers as $0, -1, 1, -2, 2, -3, 3, \ldots$, which is a well-ordering.

$\mathbb{R}$ cannot be well-ordered. The usual ordering works for some sets like $[1, 2]$, but not sets like $(1, 4) \cup (5, 6)$ or $\mathbb{R} \setminus \mathbb{Q}$.

Note: If $<$ is a well-ordering of X, say "X is well-ordered by $<$" or "X is a well-ordered set".

Definition 2.6 (Order-Isomorphism)

Let X and Y be linearly ordered sets. Then we say X and Y are *order-isomorphic* if there is an *order-preserving bijection*: a function $f : X \to Y$ which respects the order in that

$$(x < y) \implies (f(x) < f(y)) \quad \text{for all } x, y \in X.$$

Note that f^{-1} is then also an order-isomorphism, so $x < y \iff f(x) < f(y)$.

Corollary: If X and Y are order-isomorphic linearly ordered sets, then if X is well-ordered then Y must also be well-ordered by the isomorphism.

Example 2.7 (Order-Isomorphism)

$\mathbb{N}$ is isomorphic to $\mathbb{Q}$, but it the sets are not order-isomorphic. However, $\mathbb{Q}$ is order-isomorphic to $\mathbb{Q} \setminus \{0\}$. Similarly, define

$$A = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots \right\} = \left\{ \frac{n}{n+1} : n \in \mathbb{N} \right\}.$$

Then A is well-ordered and order-isomorphic to $\mathbb{N}$ by the obvious isomorphism. However:

1. $B = A \cup \{1\}$ is well-ordered but *not* order-isomorphic to A, since it has a maximum.
2. $C = A \cup \{a + 1 : a \in A\}$ is also well-ordered but not order-isomorphic to A or B, since it has infinite sets with a maximum.

Definition 2.8 (Initial Segment)

A subset $I \subseteq X$ of a linearly ordered set X is an initial segment of X if for every element $x \in I$, I contains all the predecessors of x. That is, $(x \in I) \wedge (y < x) \implies (y \in I)$.

For example, $\{1, 2, 3, 4\}$ is an initial segment of $\mathbb{N}$, but $\{1, 2, 3, 5\}$ is not.

A *proper* initial segment is an initial segment $I \neq X$. The sets $I_x = \{y \in X : y < x\}$ is an example of this for any $x \in X$, since $x \notin I_x$.

Corollary: In general, the I_x are not the only types of initial segment: the set $\mathbb{R}_{\leqslant 0}$ is not of this form. However, the I_x are the only types of initial segments in the case of X being well-ordered.

Proof: If I is a proper initial segment of a well-ordered set X, then $I = I_x$ for the least element $x \in X \setminus I$. If $y < x$, then $y \notin X \setminus I$, so $y \in I$. Conversely, f $y \in I$ and $x < y$, then $x \in I$ by the fact that I is an initial segment. Therefore $I = I_x$. □

Proposition 2.9 (Order-Isomorphism Restriction)

Suppose X and Y are well-ordered sets, and $I \subseteq Y$ is an initial segment of Y. If $f : X \to I$ is an order-isomorphism, then for every $x \in X$ we have

$$f(x) = \min(Y \setminus \{f(y) : y < x\}).$$

Proof: Fix $x \in X$ and let $A = Y \setminus \{f(y) : y < x\}$. Note that $A \neq \varnothing$, as $f(x) \in A$. Let $a = \min A$. Then $a \leqslant f(x)$, so $a \in I$. Therefore $a = f(z)$ for some $z \in X$. We want to show that $z = x$.

Since $f(z) = a \leqslant f(x)$, then certainly $z \leqslant x$, since f is order-preserving. If $z < x$, then $f(z) \notin A$, that is $a \notin A$. But this is a contradiction, so $z \not< x$, and therefore $z = x$ as required. □

Proposition 2.10 (Proof by Induction)

Let X be a well-ordered set and $S \subseteq X$ be a set such that for every $x \in X$, if $y \in S$ for all $y < x$, then $x \in S$. Then $S = X$.

Proof: If not, take a minimal "counterexample": that is, $x = \min(X \setminus S)$. Then for $y < x$, we have $y \in S$ by minimality. But by definition, this means $x \in S$, a contradiction. □

Note: We really do require well-ordering here. In $\mathbb{R}$ under the usual order, the set $\mathbb{R}_{\leqslant 0}$ has this property, but is clearly not the entire set.

Note: The usual formulation of "induction" for the natural numbers takes the set S to be defined by some property p with $S = \{n \in \mathbb{N} : p(n)\}$. The "base case" corresponds to $n = 1$, since there are no such $m < n$, and thus we require $n \in S$. This is already contained in our assumption.

Proposition 2.11 (Unique Order-Isomorphism)

Let X and Y be order-isomorphic well-ordered sets. Then there is a unique order-isomorphism f between them.

Proof: Assume f and g are order-isomorphisms $X \to Y$. We prove the statement $f(x) = g(x)$ for all $x \in X$ by induction. Fix $x \in X$ and assume that for all $y < x$, $f(y) = g(y)$. This is called the *induction hypothesis*. We want to show that then in fact $f(x) = g(x)$ as well.

By Proposition 2.9, we know that $f(x) = \min F$ and $g(x) = \min G$, where

$$A = Y \setminus \{f(y) : y < x\} \qquad B = Y \setminus \{g(y) : y < x\}.$$

But by assumption, these are the same set, and so have the same minimum. Thus $f(x) = f(y)$. By induction, we therefore have $\{x \in X : f(x) = g(x)\} = X$, and thus $f = g$ as required. □

Note: Again, this does not work for arbitrary linearly ordered sets. For example, from $\mathbb{Z} \to \mathbb{Z}$ there is an infinite family of order-isomorphisms given by $f_k : n \mapsto n + k$ for $k \in \mathbb{Z}$.

Induction has allowed us to prove things. Now, we need a tool to *construct* things: recursion.

Remark 2.12 (Formal Functions)

Recall that a *function* from a set X to a set Y is a subset $f \subseteq X \times Y$ such that for each $x \in X$, we have some $y \in Y$ with $(x, y) \in f$, and moreover this value is unique: if $(x, y) \in f$ and $(x, z) \in f$, then actually $y = z$. Of course, we write $f(x) = y$ for $(x, y) \in f$, or $f : x \mapsto y$.

Notice that $f \in \wp(X \times Y)$. For a subset $Z \subseteq Y$, the *restriction* of f to Z is given by the set $f|_Z = \{(x, y) \in f : x \in Z\}$. This is a function $Z \to Y$, so $f|_Z \in \wp(Z \times Y) \subseteq \wp(X \times Y)$.

Theorem 2.13 (Definition by Recursion)

Let X be a well-ordered set and Y an arbitrary set. Then for any function $G : \wp(X \times Y) \to Y$ there is a unique $f : X \to Y$ such that for all $x \in X$, we have $f(x) = G(f|_{I_x})$.

For example, we take $x = \min X$. Then $f(x) = G(\varnothing)$. Then, let $y = \min X \setminus \{x\}$. Then $f(y) = G(\{x, G(\varnothing)\})$ and $I_y = \{x\}$, and so on.

Say h is an *attempt* if h is a function $I \to Y$ where the domain of h (denoted $\operatorname{dom} h$) is an initial segment (2.8) $I \subseteq X$ and for all $x \in \operatorname{dom} h$, $h(x) = G(h|_{I_x})$.

Then, there is a unique attempt whose domain is X.

Proof: We first show that if h and h' are attempts, then $h(x) = h'(x)$ for all x in the intersection $\operatorname{dom} h \cap \operatorname{dom} h'$, by induction. This will show uniqueness.

We fix x in this intersection, and assume $h(y) = h'(y)$ for all $y < x$ (the induction hypothesis). Note that $\operatorname{dom} h \cap \operatorname{dom} h'$ is an initial segment of X. We have $h(x) = G(h|_{I_x})$ (because h is an attempt) and $G(h|_{I_x}) = G(h'|_{I_x}) = h'(x)$, by the induction hypothesis, as required.

Now, we show existence. Let f be the union of all attempts. Then for any x, there is an attempt h defined at x, so $h(x)$ is independent of h by the above. Therefore f is indeed a function. What is its domain? Well it is the union of the domains of all attempts, which is an initial segment of X. So given any $x \in \operatorname{dom} f$, there is an attempt h defined at x, and $f(x) = h(x)$.

It follows that $f(y) = h(y)$ for all $y < x$. But then $f(x) = h(x) = G(h|_{I_x}) = G(f|I_x)$. This means that f is an attempt! It remains to check that its domain is the entire set X, but this is easy to do. If not, $\operatorname{dom} f = I_x$ for some $x \in X$. This cannot be true, since there would be no attempt defined at x, but $f \cup \{(x, G(f))\}$ is such an attempt. □

Proposition 2.14 (Subset Collapse)

Let Y be a well-ordered set and $X \subseteq Y$. Then there is a unique initial segment of Y which is order-isomorphic (2.6) to X.

Proof: First, we show uniqueness. Assume that f is an order-isomorphism from X to some initial segment of Y. By Proposition 2.9, $f(x) = \min(Y \setminus \{f(y) : y < x\})$ for all x. By induction, f must be uniquely determined, as in the proof of order-isomorphisms being unique (2.11).

Now, we show existence. As the case $Y = \varnothing$ is trivial, we take $Y \neq \varnothing$ and fix $y_0 \in Y$. Define the function $f : X \to Y$ by recursion (2.13), using:

$$f(x) = \begin{cases} \min(Y \setminus \{f(y) : y < x\}) & \text{if this is non-empty} \\ y_0 & \text{otherwise} \end{cases}$$

We first prove that the otherwise clause does not actually arise, by proving that $f(x) \leqslant x$ for all $x \in X$ by induction. Fix $x \in X$ and assume that $f(y) \leqslant y$ for all $y < x$. But then we must have $x \in Y \setminus \{f(y) : y < x\}$, so the minimum of this set is at most x. Since we set $f(x)$ to this value, we have $f(x) \leqslant x$, and so by induction this holds everywhere.

Now fix $y < x$, and notice that $f(x) \in Y \setminus \{f(z) : z < x\} \subseteq Y \setminus \{f(z) : z < y\}$. Then $f(y) \leqslant f(x)$, but we cannot have equality, since $f(y) \in Y \setminus \{f(z) : z < y\}$. Thus f is order-preserving, and in particular must be injective.

Let $a \in Y \setminus \operatorname{im}(f)$. We show that $f(x) < a$ for all $x \in X$. By induction, fix $x \in X$ and assume that $f(y) < a$ for all $y < a$. But then $a \in Y \setminus \{f(y) : y < x\}$, and so $f(x) \leqslant a$, since we choose $f(x)$ to be the minimum of this set. But $f(x) \neq a$, since $a \notin \operatorname{im}(f)$, so $f(x) < a$ too. By induction, $\operatorname{im}(f)$ is therefore an initial segment of Y, and so we are done. □

Corollary: No well-ordered set is order-isomorphic to a proper initial segment of itself.

2.2 Ordering Well-Ordered Sets

For well-ordered sets X and Y, we write $X \leqslant Y$ for "X is order-isomorphic to some initial segment of Y". Is this notation sensible? In fact, it is: we have trichotomy for this relation.

Theorem 2.15 (Order-Isomorphism Trichotomy)

Let X and Y be well-ordered. Then $X \leqslant Y$ or $Y \leqslant X$.

Proof: Assume $Y \not\leqslant X$. In particular, $Y \neq \varnothing$, so fix $y_0 \in Y$. Define $f : X \to Y$ by recursion:

$$f(x) = \begin{cases} \min(Y \setminus \{f(y) : y < x\}) & \text{if this is nonempty} \\ y_0 & \text{otherwise} \end{cases}$$

Assume the "otherwise" case arises. Then there is a least $x \in X$ where this happens. Then consider the initial segment I_x. Since $Y \setminus \{f(y) : y < x\} = \varnothing$, we must have $f(I_x) = Y$, and so for all $y < x$ we have $f(y) = \min(Y \setminus \{f(z) : z < y\})$. Previously (in Proposition 2.14), we showed that $f|_{I_x}$ is order-preserving. So Y is order-isomorphic to an initial segment of X: a contradiction.

If the "otherwise" case doesn't arise, then f is an order-preserving function with $\mathrm{im}(f)$ an initial segment of Y, and so $X \leqslant Y$, which proves trichotomy. □

Can we have both directions of this relation hold? Obviously we can, for example if $X = Y$. But in fact this *only* happens when X and Y are order-isomorphic.

Proposition 2.16 (Order-Isomorphism Equivalence)

If X and Y are well-ordered sets with $X \leqslant Y$ and $Y \leqslant X$, then they are order-isomorphic.

Proof: Let $f : X \to Y$ and $g : Y \to X$ be order-isomorphisms to initial segments of Y and X respectively. Then $g \circ f : X \to X$ is an order-isomorphism to an initial segment of X. The range of the only such order-isomorphism is X itself, so $g \circ f$ is the identity function on X. Similarly, $f \circ g$ is the identity function on Y, and so f and g are inverses as required. □

We write $X < Y$ for well-ordered sets with $X \leqslant Y$ and X not order-isomorphic to Y.

Corollary: $<$ is a linear order (2.1) on the collection of well-ordered sets, if we identify sets which are order-isomorphic to each other as being equivalent. Reflexivity is obvious, transitivity is easy to show, and we have just shown trichotomy.

Note: The natural question to ask now is whether the collection of all well-ordered sets, given that it is linearly ordered, is in fact itself well-ordered. We return to this later.

Note: We can construct a new well-ordered set from any old one. For any well-ordered set X, pick any $z \notin X$ and let $X^+ = X \cup \{z\}$ such that the well-ordering on X holds with $x < z$ for all $x \in X$. Then X^+ is clearly also well-ordered, and unique up to order-isomorphism, with $X < X^+$.

Note: Let $\{X_i : i \in I\}$ be a set of well-ordered sets X_i, indexed by some index set I. Then we want to show that this set has an upper bound: there exists a well-ordered set X with $X_i \leqslant X$ for all $i \in I$. We cannot yet prove this in general, but we consider a special case for now.

Definition 2.17 (Extension, Nesting)

Given well-ordered sets $(X, <_X)$ and $(Y, <_Y)$, we say Y *extends* X if X is an initial segment of Y and $<_X$ is the restriction of $<_Y$ to X.

We say that a collection $\{X_i : i \in I\}$ of well-ordered sets is *nested* if for all $i, j \in I$ either X_i extends X_j or X_j extends X_i.

Proposition 2.18 (Nested Collection Upper Bound)

Let $\mathcal{X} = \{X_i : i \in I\}$ be a nested set of well-ordered sets. Then there is a well-ordered set X which is an upper bound for $\mathcal{X}$, such that $X_i \leqslant X$ for all $i \in I$.

Proof: Take X to be the union $\bigcup_{i \in I} X_i$. For $x, y \in X$, we let $x < y$ if there is some $i \in I$ such that $x, y \in X_i$ and $x <_i y$ within this set X_i. We claim that this is our upper bound.

Since the X_i are nested, it follows that $<$ on X is a well-defined linear order such that each X_i is an initial segment of X. Let $S \subseteq X$ be a non-empty subset. Then there is some $i \in I$ with $X_i \cap S \neq \varnothing$. Since X_i is well-ordered, $X_i \cap S$ has a least element, say x. But now x must be the least element of S, since X_i is an initial segment of S. □

Note: In fact, this construction yields the *least* upper bound for $\mathcal{X}$: for any other upper bound Y, we have $X \leqslant Y$.

Note: This proposition holds even without the assumption that the X_i are nested.

2.3 Ordinals

Now, we consider *ordinals*. These are the same as the well-ordered sets on which we have focused so far in this section, but we treat them differently.

Definition 2.19 (Ordinal)

An *ordinal* is an class of well-ordered sets under the order-isomorphism equivalence relation. The *order type* of a well-ordered set X is the unique ordinal to which it is order-isomorphic.

Note: This definition is still quite informal: we give a more formal definition later on.

Definition 2.20 (Relation on Ordinals)

Let α and β be ordinals, and X and Y be well-ordered sets of order type α and β respectively. Then we say $\alpha \leqslant \beta$ to mean that $X \leqslant Y$, and $\alpha < \beta$ to mean $X < Y$.

We also define α^+ to be the order type of X^+.

Note: This is indeed well-defined: they don't depend on the specific sets X and Y.

Corollary: For ordinals, we therefore have $\alpha \leqslant \beta$ or $\beta \leqslant \alpha$, with both of these relations holding if and only if $\alpha = \beta$.

Example 2.21 (Basic Ordinals)

For $k \in \mathbb{N}_0$, we write k for the order type of a well-ordered finite set of size k.

We write ω for the order type of $\mathbb{N}$ (or equivalently $\mathbb{N}_0$).

Notice that $\mathbb{Q}$ contains subsets of order type 0, 1, 2, and so on, as well as of order type ω. For example, the set A from Example 2.7 has order type ω.

However, the set $A \cup \{1\}$ doesn't have any of these order types: it must be something more. In fact, it must be α^+.

Now, we consider the ordinals as being themselves well-ordered.

Proposition 2.22 (Ordinals Ordered)

Let α be some ordinal. Then the set of all ordinals which are strictly less than α form a well-ordered set, and this set has order type α.

Proof: Let X be a well-ordered set whose order type is α, and let X' be the set of proper initial segments of X. X' is linearly ordered (genuinely, not just up to order-isomorphism) by $<$. Then the map $X \to X'$, $x \mapsto I_x$ is an order-isomorphism, and hence X' is well-ordered by $<$.

But then so is the set of order types of proper initial segments of X, and this is exactly the set of ordinals less than α. In fact, since the map $Y \mapsto$ order type of Y is an order-isomorphism, the set of such ordinals must have order type α. □

Note: We write the set of ordinals less than α as $I_\alpha : \{\beta \text{ an ordinal} : \beta < \alpha\}$.

Corollary: I_α always has order type α.

Theorem 2.23 (Least Ordinal)

Let $S \neq \varnothing$ be a set of ordinals. Then S has a least element.

Proof: Let $\alpha \in S$. If α is not a least element, then $S \cap I_\alpha \neq \varnothing$. We have seen that $S \cap I_\alpha$ has a least element β. Since I_α is an initial segment of ordinals ($\gamma < \beta$ and $\beta \in I_\alpha \implies \gamma \in I_\alpha$), it follows that β must in fact be the least element of S. □

So we have seen that any nonempty set of ordinals has a least element. Does this mean that the set of ordinals is thus well-ordered? Well, it would, if such a set existed. But actually the so-called "set of ordinals" cannot exist!

Theorem 2.24 (Burali-Forti Paradox)

The ordinals do not form a set.

Proof: Assume that X is a set consisting of all ordinals. Then X is well-ordered by $<$. Let α be the order type of X. But then $\alpha \in X$, and so I_α is a proper initial segment of X of order type α: in particular, I_α is order-isomorphic to X. But this is a contradiction. □

Note: We let ON be the *class* of all ordinals. Remember that is not a set! The difference is that a class cannot be a member of anything: it is not an entity in itself, just a convenient structure for us to talk about a collection of objects with a given property.

Corollary: Let $S = \{\alpha_i : i \in I\}$ be a set of ordinals. Using the set $\{I_{\alpha_i} : i \in I\}$, there exists an ordinal α which is an upper bound for S. Then S has a least upper bound, denoted by $\sup S$. Note that this is the least element of $\{\beta \in I_\alpha \cup \{\alpha\} : \beta \text{ is an upper bound of } S\}$.

So far, we have seen the ordinals 0, 1, 2, and so on for $n \in \mathbb{N}$. We have also seen the supremum of the collection of these ordinals, which is ω. Next, we have ω^+, which we will denote $\omega + 1$. For now, this is just a notational quirk, but in section **??** we will define ordinal addition, and this definition will be consistent with it.

We then define $\omega + 2$, $\omega + 3$, and so on, and the supremum of $\{\omega + n : n \in \mathbb{N}_0\}$ is denoted $\omega + \omega$, or equivalently $\omega \times 2$. We then continue this pattern, eventually defining $\omega \times 3$, $\omega \times 4$, and so on. After this, we define $\sup\{\omega \times n : n \in \mathbb{N}\}$ to be ω^2.

We can then continue this all the way to $\omega^2 + \omega$, then $\omega^2 + \omega \times 2$, and so on, which is eventually bounded by $\omega^2 \times 2$, and then we continue this to $\omega^2 \times 3$ and eventually $\omega^2 \times \omega = \omega^3$. After this, we exhaust the ω^n, and must define ω^ω.

From here, we get $\omega^\omega + 1$, all the way up to $\omega^\omega + \omega$, then $\omega^\omega + \omega^\omega = \omega^\omega \times 2$, then $\omega^\omega \times \omega = \omega^{\omega+1}$. This eventually yields $\omega^{\omega+n}$ for each n, then $\omega^{\omega+\omega} = \omega^{\omega\times 2}$, then $\omega^{\omega\times n}$ for each n, then $\omega^{\omega\times\omega} = \omega^{\omega^2}$.

But then this can be continued to yield ω^{ω^n} for each n, and the set of these is bounded by ω^{ω^ω}. Eventually, this can be extended to a tower of ω which is n high for each n, and after this a tower which is ω high. This tower is called ε_0.

Eventually, we get ε_1, and then ε_2, and then ε_n for each n, then ε_ω. After this, we soon get $\varepsilon_{\varepsilon_0}$. Finally, we turn these into an infinite tower of descending ε.

But of course this can also be continued, and so on ad infinitum (and beyond!)

All of the ordinals we have constructed so far have been countable. Are there uncountable ordinals?

Theorem 2.25 (Uncountable Ordinals)

There exist uncountable ordinals.

Proof: If there is an uncountable ordinal, then there is a *least* uncountable ordinal α. Then I_α is the set of all countable ordinals, and so is the set of order-types of well-orderings of subsets of $\mathbb{N}$.

Let $A = \{(M, R) \in \wp(\mathbb{N}) \times \wp(\mathbb{N} \times \mathbb{N}) : R \text{ is a well-ordering of } M\}$. Then the set B of order types of elements of A consists of all countable ordinals.

Let $\omega_1 = \sup B$. If ω_1 is countable, then so is ω_1^+, and so $\omega_1^+ \in \mathbb{B}$. But then $\omega_1^+ \leqslant \omega_1$, which is a contradiction. Therefore ω_1 must be uncountable. □

Corollary: The ordinal ω_1 constructed in the proof is the least uncountable ordinal. Suppose we have $\alpha < \omega_1 = \sup B$. Then there exists some $\beta \in B$ with $\alpha < \beta$. Since β is countable, so is α.

Corollary: Every proper initial segment of ω_1 is countable.

Corollary: If $\alpha_1, \alpha_2, \ldots$ is a sequence of countable ordinals, then so is $\alpha = \sup\{a_n : n \in \mathbb{N}\}$. This is because the set I_α is a countable union of countable sets.

Theorem 2.26 (Hartog's Lemma)

For any set X, there is some ordinal γ which does not inject into X, which we write as $\gamma(X)$.

Proof: This is a generalisation of the previous theorem, choosing X in place of $\mathbb{N}$. Form the set B consisting of order-types of well-orderings of subsets of X, and let $\gamma = (\sup B)^+$.

If γ injects into X, it induces a well-ordering on a subset of X of order type γ. Then $\gamma \in B$, and so we have $\gamma = (\sup B)^+ \leqslant \sup B = \gamma$, which is a contradiction. □

Note: This theorem states something slightly stronger than "there is no biggest ordinal". In fact, any set has a bigger ordinal!

Definition 2.27 (Successor, Limit Ordinal)

Let α be an ordinal. We consider two cases, depending whether I_α has a greatest element.

1. Suppose I_α has a greatest element β. Then $I_\alpha = I_\beta \cup \{\beta\}$. Then $\alpha = \beta^+$, and so we say α is the *successor* of β. Here, $\beta = \sup I_\alpha < \alpha$.
2. Now suppose I_α has no greatest element. Then if $\beta \in I_\alpha$ (equivalently, $\beta < \alpha$) then there is some $\beta < \gamma < \alpha$. It then follows that $\alpha = \sup I_\alpha$: no other element can be an upper bound, as there is always some bigger element. We say α is a *limit ordinal*.

For example, 0 is a limit ordinal. The set $I_0 = \varnothing$ has no greatest element (indeed, no *element*). However, $0^+ = 1$ is a successor. Indeed, *any* $n \in \mathbb{N}$ is a successor of $n - 1$.

Also, ω is a limit ordinal. The set $\mathbb{N}$ has no upper bound, since any n has $n < n + 1 < \omega$. However, $\omega^+ = \omega + 1$ is a successor.

2.4 Ordinal Arithmetic

Now, we formalise our notion of adding ordinals. We had loosely constructed $\omega+1$ and even $\omega+\omega$, but introduced this as notation only, without ever formally defining ordinal addition.

Definition 2.28 (Ordinal Addition)

For ordinals α and β, we define the ordinal sum $\alpha+\beta$ by recursion on β with α fixed:

1. $\alpha+0=\alpha$ for the unique zero ordinal.
2. $\alpha+\beta^+=(\alpha+\beta)^+$ for a successor ordinal β.
3. $\alpha+\lambda=\sup\{\alpha+\beta:\beta<\lambda\}$ for a nonzero limit ordinal λ.

This matches the heuristic definition we have used, and respects integer addition.

Note: Technically, recursion as defined in 2.13 relies on a set, but we saw in 2.24 that the ordinals do not form a set. We should therefore fix an ordinal γ and define $\alpha+\beta$ by recursion on β in the well-ordered set I_γ. By uniqueness in recursion, this does indeed give a well-defined $\alpha+\beta$ for any pair of ordinals. In general, this justifies recursive definitions on all ordinals.

Proposition 2.29 (Ordinal Induction)

Proof by induction works on ordinals. Let $p(\alpha)$ be some property of ordinals. Then we have

$$(\forall\alpha)((\forall\beta)((\beta<\alpha)\Rightarrow p(\beta))\Rightarrow p(\alpha))\Rightarrow(\forall\alpha)p(\alpha).$$

Proof: For contradiction, assume $(\forall\alpha)((\forall\beta)((\beta<\alpha)\Rightarrow p(\beta))\Rightarrow p(\alpha))$ but not $(\forall\alpha)p(\alpha)$. Then there is some γ with $\neg p(\gamma)$. The non-empty set $\{\delta\leqslant\gamma:\neg p(\delta)\}$ of ordinals therefore has a least element, say α. If $\beta<\alpha$, then $\beta\leqslant\gamma$, and so $p(\beta)$ holds. But then by assumption, $p(\alpha)$ holds. □

Note: For $m,n<\omega$, we have $m+0=m$, and $m+(n+1)=m+n^+=(m+n)^+=(m+n)+1$. This is exactly the recursive definition of integer addition, which is why we say ordinal addition respects integer addition.

Proposition 2.30 (Noncommutativity)

Ordinal addition is not commutative.

Proof: Since 1 is a successor ordinal, $\omega+1=\omega^+$. However, since ω is a limit ordinal, we have:

$$1+\omega=\sup\{1+n:n<\omega\}=\sup\mathbb{N}=\omega\neq\omega^+.$$

This means $\omega+1\neq1+\omega$, so ordinal addition is not commutative. □

Proposition 2.31 (Addition Respects $\leqslant$)

For any ordinal α, if $\beta\leqslant\gamma$, then $\alpha+\beta\leqslant\alpha+\gamma$.

Proof: We fix α and proceed by induction on γ. If $\gamma=0$, then $\beta=\gamma=0$, so both sides are just α, and thus the inequality holds. Now, without loss of generality we take $\beta<\gamma$.

If $\gamma=\delta^+$ is a successor ordinal, then we have $\alpha+\beta\leqslant(\alpha+\delta)^+$. We have $\beta\leqslant\delta$, so by induction this holds. Similarly, if γ is a limit ordinal, we define $\alpha+\gamma$ to be the supremum of the set $\{\alpha+\delta:\delta<\gamma\}$. Since $\beta<\gamma$, this set contains $\alpha+\beta$, and so $\alpha+\beta\leqslant\alpha+\gamma$ as required. □

Corollary: The strict version also holds: if $\beta<\gamma$, then $\alpha+\beta<\alpha+\gamma$. However, we do *not* always have $\beta+\alpha<\gamma+\alpha$, for example if $\beta=0$, $\gamma=1$, and $\alpha=\omega$ this would give $\omega<\omega$. However, we do have $\beta+\alpha\leqslant\gamma+\alpha$, simply by induction on α.

Proposition 2.32 (Supremum Addition)

Let $S \neq \varnothing$ be a set of ordinals. Then for any ordinal α, we have

$$\alpha + \sup S = \sup \{\alpha + \beta : \beta \in S\}.$$

Proof: Let $T = \{\alpha + \beta : \beta \in S\}$. We then want $\alpha + \sup S = \sup T$. For any $\beta \in S$, we know $\alpha + \beta \leqslant \alpha + \sup S$. Then $\sup T \leqslant \alpha + \sup S$. To prove the converse, we consider two cases, based on whether S has a greatest element.

1. If S has greatest element γ, then $\alpha + \gamma$ is a greatest element of T. So $\alpha + \gamma = \sup T$, but as $\gamma = \sup S$, indeed we have $\alpha + \sup S = \sup T$.
2. If S has no greatest element, let $\lambda = \sup S$. Then $\lambda \neq 0$, since $S \neq \varnothing$. Note that $\lambda \notin S$, so $S \subseteq I_\lambda$. Then $\lambda = \sup S \leqslant \sup I_\lambda = \lambda$, so $\lambda = \sup I_\lambda$, and so λ is a limit ordinal. Therefore we have by definition $\alpha + \sup S = \alpha + \lambda = \sup \{\alpha + \gamma : \gamma < \lambda\}$.

   Now, for any $\gamma < \lambda = \sup S$, there exists $\beta \in S$ with $\gamma < \beta$. Then $\alpha + \gamma \leqslant \alpha + \beta \leqslant \sup T$. But then we have $\alpha + \sup S \leqslant \sup T$.

Thus in either case, we have $\alpha + \sup S \leqslant \sup T$ and $\sup T \leqslant \alpha + \sup S$, so $\alpha + \sup S = \sup T$. □

Proposition 2.33 (Associativity of Ordinal Addition)

For all ordinals α, β, γ we have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

Proof: We prove this by induction on γ, with α and β fixed. We consider three cases.

1. If $\gamma = 0$, then we have $\alpha + (\beta + 0) = \alpha + \beta = (\alpha + \beta) + 0$.
2. If $\gamma = \delta^+$ is a successor ordinal, then $\alpha + (\beta + \gamma) = \alpha + (\beta + \delta)^+$ by definition. The induction hypothesis shows that this is equal to $(\alpha + (\beta + \delta))^+ = (\alpha + \beta) + \gamma$.
3. If $\gamma \neq 0$ is a limit ordinal, $\alpha + (\beta + \gamma) = \alpha + \sup \{\beta + \delta : \delta < \gamma\} = \sup \{\alpha + (\beta + \delta) : \delta < \gamma\}$ by the previous proposition. But then this is $\sup \{(\alpha + \beta) + \delta : \delta < \gamma\}$ by the induction hypothesis, and this is simply $(\alpha + \beta) + \gamma$ as required.

Therefore $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, and so ordinal addition is associative. □

Note: The definition of ordinal addition given in 2.28 is called the *inductive definition*. We now give an alternative *synthetic* definition, which yields the same result.

Definition 2.34 (Ordinal Addition)

Let X and Y be well-ordered sets. Then $X \sqcup Y = (X \times \{0\}) \cup (Y \times \{1\})$ is well-ordered too, by the ordering:

$$(x, i) < (y, j) \iff \text{one of } \begin{cases} i = j = 0 \text{ and } x < y \text{ in } X \\ i = j = 1 \text{ and } x < y \text{ in } Y \\ i = 0 \text{ and } j = 1 \end{cases}$$

That is, we say that every element in X is "less" than every element in Y, and compare pairs of elements from the same set as they are compared within that set. $X \sqcup Y$ is then the disjoint union of X and Y, or the set "X then Y".

Now, if X and Y have order type α and β, we let $\alpha + \beta$ be the order type of $X \sqcup Y$.

Note: In the synthetic definition of ordinal addition, we let $\alpha + 1$ be the order type of $\alpha \sqcup \{0\}$, which is clearly α^+.

Note: This definition makes it easier to see various properties, like associativity (2.33), as the well-ordered sets $(X \sqcup Y) \sqcup Z$ and $X \sqcup (Y \sqcup Z)$ are order-isomorphic. Also, we have $\alpha + \beta \leqslant \alpha + \gamma$ whenever $\beta \leqslant \gamma$ (2.31), since if Y is an initial segment of Z, $X \sqcup Y$ is an initial segment of $X \sqcup Z$.

Note: We usually write the more concise $\alpha \sqcup \beta$ for "$X \sqcup Y$, where X is of order type α and Y is of order type β". More generally, we identify α and I_α.

Proposition 2.35 (Addition Well-Defined)

The definitions of ordinal addition given in 2.28 (inductive) and 2.34 (synthetic) coincide.

Proof: We write $\alpha \oplus \beta$ for the synthetic definition, and $\alpha + \beta$ for the inductive definition. Now, we perform induction, considering three cases based on β.

1. If $\beta = 0$, then $\alpha + 0 = \alpha$ is indeed the order type of $X \sqcup \varnothing$, where X has order type α.
2. If $\beta = \delta^+$, then $\alpha + \beta = (\alpha + \delta)^+$, which is the order type of $(\alpha \sqcup \delta) \sqcup 1$ by induction. This is order-isomorphic to $\alpha \sqcup (\delta \sqcup 1)$, which has order type $\alpha \oplus \beta$ as required.
3. If $\beta \neq 0$ is a limit ordinal, then $\alpha + \beta = \sup\{\alpha + \gamma : \gamma < \beta\}$. By induction, this is equal to $\sup\{\alpha \oplus \gamma : \gamma < \beta\}$. But $\alpha \oplus \gamma$ is the order type of $\alpha \sqcup \gamma$, and the supremum of the nested set $\{\alpha \sqcup \gamma : \gamma < \beta\}$ is the union $\bigcup_{\gamma<\beta} \alpha \sqcup \gamma$, which is $\alpha \sqcup \beta$. This has order type $\alpha \oplus \beta$ as required, so the definitions coincide in this case too.

Thus the definitions coincide for every ordinal, and so are equal. □

Now, we define ordinal multiplication. Again, we start with the *inductive* definition.

Definition 2.36 (Inductive Ordinal Multiplication)

We define $\alpha \cdot \beta$ by recursion on β, with α fixed. $\alpha \cdot 0 = 0$ for all ordinals α. Then:

1. $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$ for successor ordinals β^+.
2. $\alpha \cdot \lambda = \sup\{\alpha \cdot \gamma : \gamma < \lambda\}$ for limit ordinals λ.

This clearly respects traditional multiplication on the natural numbers $\mathbb{N}_0$.

Definition 2.37 (Synthetic Ordinal Multiplication)

For well-ordered sets X and Y, we well-order the Cartesian product $X \times Y$ by:

$$(x, y) < (x', y') \iff \text{one of } \begin{cases} y < y' \text{ in } Y \\ y = y' \text{ and } x < x' \text{ in } X \end{cases}$$

This is the lexicographic ordering on $X \times Y$, where the second element takes precedence, with ties broken by the first element.

We then define $\alpha \cdot \beta$ to be the order type of $\alpha \times \beta$, or more precisely $I_\alpha \times I_\beta$.

Corollary: It is straightforward to check that the two definitions of $\alpha \cdot \beta$ once again coincide.

Corollary: Ordinal multiplication respects $\leqslant$ in the same way that ordinal addition does (2.31): we have $\alpha \cdot \beta \leqslant \alpha \cdot \gamma$ for all $\beta \leqslant \gamma$. The strict version holds too, provided that $\alpha \neq 0$. The reversed version also holds: for all $\beta \leqslant \gamma$ we have $\beta \cdot \alpha \leqslant \gamma \cdot \alpha$.

Corollary: Ordinal multiplication is also associative: $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$. However, ordinal multiplication is *not* commutative: $\omega \cdot 2 = \omega + \omega$, but $2 \cdot \omega = \sup 2\mathbb{N} = \omega$.

We define ordinal exponentiation likewise, with $\alpha^0 = 1$, and $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$.

Definition 2.38 (Ordinal Exponentiation)

We define α^β by recursion on β, with α fixed. $\alpha^0 = 1$ for all ordinals α. Then:

1. $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$ for successor ordinals β^+.
2. $\alpha^\lambda = \sup\{\alpha^\gamma : \gamma < \lambda\}$ for limit ordinals λ.

This clearly respects traditional exponentiation on the natural numbers $\mathbb{N}_0$.

Note: This definition sets $0^0 = 1$. In fact, this is a natural definition, even in general! The empty product is clearly 1, since this is the identity for multiplication. Additionally, the limit in the real numbers of x^x approaches 1 as $x \to 0$ from above.

With this, we can construct a table of inequalities, which is useful for reference. Suppose we have ordinals $\alpha < \beta$, and another ordinal γ. Then, which arithmetic inequalities hold?

operation $\circ$	strict, left side $\gamma \circ \alpha < \gamma \circ \beta$	non-strict, left-side $\gamma \circ \alpha \leqslant \gamma \circ \beta$	strict, right side $\alpha \circ \gamma < \beta \circ \gamma$	non-strict, right side $\alpha \circ \gamma \leqslant \beta \circ \gamma$
addition $+$	✓ (everywhere)	✓ (everywhere)	$2 + \omega = 3 + \omega$	✓ (everywhere)
multiplication $\cdot$	✓ (if $\gamma \neq 0$)	✓ (everywhere)	$2 \cdot \omega = 3 \cdot \omega$	✓ (everywhere)
exponentiation $\hat{}$	✓ (if $\gamma \neq 0, 1$)	✓ (if $\gamma \neq 0$)	$2^\omega = 3^\omega$	✓ (everywhere)

In general, these inequalities tend to hold when we operate by γ on the left. This is because, for a fixed γ, these operations are defined inductively, and so:

1. If β^+ is a successor, then $\gamma \circ \beta^+ = \gamma \circ \beta * \gamma$, which is at least $\gamma \circ \beta$. This means for sucessor ordinals, the ordering is preserved.
2. If λ is a non-zero limit ordinal, then $\gamma \circ \lambda = \sup\{\gamma \circ \beta : \beta < \lambda\}$, and so by definition $\gamma \circ \lambda$ is at least $\gamma \circ \beta$ for all smaller β.

A similar induction shows the non-strict version on the right side.

Note: The only non-strict example which does *not* always hold is the one of exponentiation, in which we see $0^0 = 1 > 0^2 = 0$, even though $0 < 2$. In fact, this counterexample holds even within the natural numbers $\mathbb{N}_0$, without requiring ordinal arithmetic!

Corollary: Using the top left entry in the table, we may perform "ordinal subtraction" on the left. If $\beta \leqslant \alpha$, then there is a unique ordinal γ with $\beta + \gamma = \alpha$. This does not work on the right: there is no γ with $\gamma + 1 = \omega$, even though $1 \leqslant \omega$.

3 Posets and Zorn's Lemma

3.1 Partially Ordered Sets

This section will require a lot of basic definitions and examples before we see any results.

Definition 3.1 (Partial Order)

A *partial order* on a set X is a relation $\leqslant$ on X which is:

1. *reflexive*: $x \leqslant x$ for all $x \in X$.
2. *antisymmetric*: if $x \leqslant y$ and $y \leqslant x$, then $x = y$.
3. *transitive*: if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$.

We then write $x < y$ if $x \leqslant y$ and $x \neq y$. Note that this is irreflexive and transitive.

If $\leqslant$ is a partial order on X, we say that X is a *partially ordered set*, or *poset*.

Note: Compare this to the definition of a *total* order given in 2.1. In fact, any linearly ordered set is also a poset.

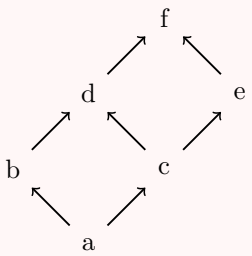
Example 3.2 (Posets)

Any linearly ordered set is a poset, but are there posets which are not linearly ordered?

1. In $\mathbb{N}$, the relation $a \leqslant b$ if $a \mid b$ is a partial but not linear order. For example, 4 and 7 are incomparable: neither divide the other.
2. For any set S, the powerset $\wp(S)$ is a poset under the order $\subseteq$.
3. Any subset of a poset is a poset, simply by restricting the partial order.

Definition 3.3 (Hasse Diagrams)

We can describe posets using *Hasse diagrams*, like this:



This is an order of a set $X = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}, \mathrm{f}\}$ where the relation is given by:

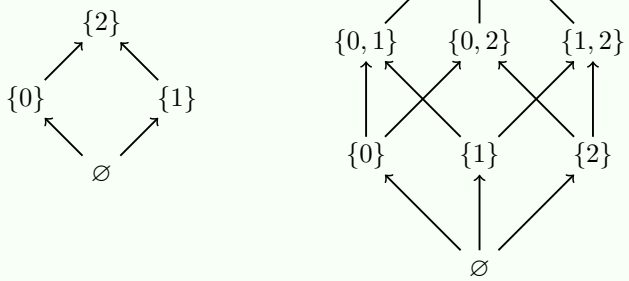
$$\mathrm{a} \leqslant \mathrm{b},\ \mathrm{a} \leqslant \mathrm{c},\ \mathrm{b} \leqslant \mathrm{d},\ \mathrm{c} \leqslant \mathrm{d},\ \mathrm{c} \leqslant \mathrm{e},\ \mathrm{d} \leqslant \mathrm{f},\ \mathrm{e} \leqslant \mathrm{f}$$

and all consequences of reflexivity and transitivity from here. More generally, we join x to y with an upward edge if y *covers* x, that is if $x < y$ and there is no z with $x < z < y$. We then interpret the diagram to mean $x \leqslant y$ if $x = y$ or there is an upward path from x to y.

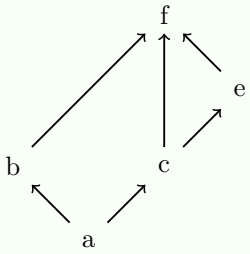
Note: Not all posets can be described using Hasse diagrams. For example, in $\mathbb{Q}$, the set is dense, and so between any $x < y$ there is some element z with $x < z < y$. But then we cannot draw a line between any x and an element which covers it. However, all *finite* posets have Hasse diagrams.

Example 3.4 (Hasse Diagrams)

We can draw the subsets of $\{0, 1\}$ and $\{0, 1, 2\}$ using Hasse diagrams.

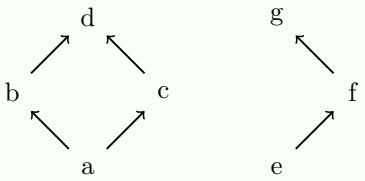


In a poset, there need not be a coherent notion of "height". For example, consider the original example of a Hasse diagram, and remove the element "e", but retain the relation d $\leqslant$ f. Then we are left with the following diagram:



Here, there is no way to assign each element a "layer" such that each element covers one from the layer directly below it.

There also need not be any connection between paths.



Here, the set is split into two, where no pair of elements from opposite parts are comparable.

Definition 3.5 (Chain, Antichain)

A subset S of a poset X is a *chain* if S is linearly ordered by the partial order on X.

Meanwhile, a subset S is called an *antichain* if no two distinct elements of S are related. That is, for all x, y in S, if $x \leqslant y$ then $x = y$.

Of course, this is the opposite of a chain, where every pair of elements is comparable.

Corollary: If X is linearly ordered, then every subset of X is a chain.

Corollary: Any subset of size 1 is both a chain and an antichain.

Example 3.6 (Chains and Antichains)

We can write down some chains and antichains.

1. Any subset of size 1 is both a chain and an antichain. In a linearly ordered set X, these are the *only* antichains, as any two elements are related.
2. Any subset of a chain or antichain is still a chain or antichain respectively.
3. In $\mathbb{N}$, with $a \leqslant b$ if $a \mid b$, the set $\{1, 2, 4, 8, 16 \ldots\}$ is a chain, while the set of primes is an antichain (as no two elements divide each other).
4. In the powerset of $\{1, 2, 3\}$, the set $\{\varnothing, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$ is a chain. Meanwhile, the set $\{\{1\}, \{2\}, \{3\}\}$ is an antichain.
5. In $\wp(\mathbb{Q})$, the set $\{(\infty, x) \cap \mathbb{Q} : x \in \mathbb{R}\}$ is an uncountable chain.
6. In our original Hasse diagram from 3.3, the sets $\{\mathrm{b}, \mathrm{c}\}$ and $\{\mathrm{d}, \mathrm{e}\}$ are antichains, while the set $\{\mathrm{a}, \mathrm{c}, \mathrm{d}, \mathrm{f}\}$ is a chain.

Definition 3.7 (Supremum)

Let X be a poset, with $S \subseteq X$ and $x \in X$. Then:

1. x is an *upper bound* for S if $y \leqslant x$ for all $y \in S$.
2. x is a *least upper bound* for S if x is an upper bound for S and $x \leqslant y$ for all other upper bounds of S. If this exists, then it is called the *supremum* and is denoted by $\sup S$.

If every subset S of a poset X has a supremum, then we say X is *complete*.

Note: If a set S has supremum x and supremum y, then x and y are both upper bounds, and we must have $x \leqslant y$ and $y \leqslant x$ by the supremum property. Then $x = y$ by antisymmetry. Therefore the supremum of a set, if it exists, must be unique.

Corollary: A complete poset X has greatest element $\sup X$ and least element $\sup \varnothing$. In particular, this means the empty set $\varnothing$ is not complete, as it has no element.

Example 3.8 (Supremum)

If $S \subseteq \wp(X)$, then $\sup S = \bigcup \{A : A \in S\}$.

In $\mathbb{R}$, we have $\sup(0,\, 1) = \sup[0,\, 1] = 1$.

In $\mathbb{Q}$, the set $\left\{x : x^2 < 2\right\}$ has upper bounds (like 2), but no supremum, and so is not complete.

$\mathbb{R}$ is also not complete: for example $\mathbb{R}$ has no upper bound.

Definition 3.9 (Order-Preserving)

A map $f : X \to Y$ between posets X and Y is *order-preserving* if $x \leqslant y \implies f(x) \leqslant f(y)$.

Note: In Definition 2.6, we defined an order-preserving map using strict equalities. In particular, this guaranteed that any such map was injective. This is not the case for posets: indeed, any map of the form $f(x) = y_0$ for some constant $y_0 \in Y$ independent of X is order-preserving.

Corollary: If f is order-preserving and injective, then $x < y \implies f(x) < f(y)$. If X is linearly ordered, then the reverse direction is also true.

Theorem 3.10 (Knaster-Tarski Fixed Point Theorem)

Let X be a complete poset and $f : X \to X$ be an order-preserving map. Then f must have a fixed point $x \in X$, such that $f(x) = x$.

Proof: Let $S = \{x \in X : x \leqslant f(x)\}$ and define $z = \sup S$ (which exists by completeness). We show that $f(z) = z$. Note that for $x \in S$, we have $x \leqslant z$, so $x \leqslant f(x) \leqslant f(z)$. That means $f(z)$ is an upper bound for S. Since z is the *least* upper bound, we have $z \leqslant f(z)$.

It then follows that $f(z) \leqslant f(f(z))$. But this means that $f(z) \in S$ by definition of S! This means that $f(z) \leqslant z$, since z is an upper bound for S. Thus by antisymmetry, we have $f(z) = z$, and so z is a fixed point of an arbitrary order-preserving map. □

Note: We really did require the set X to be complete! For example, the order-preserving map $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = n + 1$ clearly has no fixed points.

Theorem 3.11 (Schröder-Bernstein Theorem)

Let A and B be sets. If there are injections $f : A \to B$ and $g : B \to A$, then in fact there is some bijection $h : A \to B$.

Proof: We seek partitions $A = P \cup Q$ and $B = R \cup S$ such that $f(P) = R$ and $g(S) = Q$. Then

$$h(x) = \begin{cases} f(x) & x \in P \\ g^{-1}(x) & x \in Q \end{cases}$$

defines a bijection $A \to B$. For such partitions, $A \setminus g(B \setminus f(P)) = P$. This is because $f(P) = R$, and $B \setminus R = S$, then $A \setminus g(S) = A \setminus Q = P$.

Define $H : \wp(A) \to \wp(A)$ by $H(P) = A \setminus g(B \setminus f(P))$. Recall that $\wp(A)$ is a complete poset under the inclusion relation, and H is order-preserving.

By Knaster-Tarski (Theorem 3.10), there is a fixed point $P \subseteq A$ such that $H(P) = P$. Then setting $Q = A \setminus P$, $R = f(P)$, and $S = B \setminus R$ gives the required partitions. □

3.2 Zorn's Lemma

We now prove one of the most important and famous results in set theory: Zorn's Lemma. First, we need an introductory definition.

Definition 3.12 (Maximal Element)

An element x in a poset X is called *maximal* if $x \leqslant y$ implies $x = y$. Equivalently, there is no $y \in X$ with $x < y$.

Note: Maximal elements need not necessarily be unique! In the set $\{a, b, c\}$ with the ordering given by $a \leqslant b$ and $a \leqslant c$, both b and c are maximal.

Example 3.13 (Maximal Elements)

Sets may or may not have a maximal element.

1. In the powerset $\wp(S)$ ordered by inclusion, the element S is maximal.
2. In $\mathbb{N}$ under the usual order, there is no maximal element, as $n \leqslant n + 1$.

Now, we are ready to prove Zorn's Lemma.

Theorem 3.14 (Zorn's Lemma)

Let X be a non-empty poset in which every chain (3.5) has an upper bound. Then X must have a maximal element.

Proof: Assume that X has no maximal element. For each x, fix $x' \in X$ such that $x < x'$. Also, for each chain $C \subseteq X$, let $u(C)$ be an upper bound for C.

Let $\gamma = \gamma(X)$ be some ordinal which does not inject into X, which is possible by Hartog's Lemma (Theorem 2.26). Define $f : \gamma \to X$ by the recursion:

$$\begin{aligned} f(0) &= u(\varnothing) \text{ the base case} \\ f(\alpha+1) &= f(\alpha)' \text{ for successor ordinals} \\ f(\lambda) &= u(\{f(\alpha) : \alpha < \lambda\}) \text{ for limit ordinals} \end{aligned}$$

Now, an induction on β with α fixed shows that $\alpha < \beta \implies f(\alpha) < f(\beta)$. But then f is injective, which is a contradiction! Therefore there is a maximal element.

In this definition, we used $\{f(\alpha) : \alpha < \lambda\}$, and found its upper bound. In fact, this relies on the fact that this set is always a chain for every limit ordinal λ. □

Note: Recall that $\varnothing$ is a chain in X, and thus has an upper bound $x \in X$. Therefore X is anyway guaranteed to be non-empty. When applying Zorn's Lemma, we often first check that $X \neq \varnothing$ and then verify that non-empty chain has an bound.

Theorem 3.15 (Vector Space Basis)

Every vector space V has a basis.

Proof: Partially order the linearly independent subsets of V by inclusion. Assuming each chain has an upper bound, we apply Zorn's lemma and take the maximal element $B \subseteq V$.

Then B is a basis, that is $\operatorname{span}(v) = V$. Otherwise, we could take some x in V but not the span of B, which would make $B \cup \{x\}$ a larger linearly independent set, contradicting maximality.

We now check that each chain has an upper bound. Let $X = \{A \subseteq V : A \text{ is linearly independent}\}$, partially ordered by inclusion. Let $C = \{A_i : i \in I\}$ be some chain in X. Then the union of all the sets is $A = \bigcup_{i \in I} A_i$ is an upper bound for C in $\wp(V)$: we prove that it is linearly independent, and thus that it is also an upper bound for C in X.

Assume otherwise, so that:

$$\sum_{j=1}^{n} \lambda_j x_j = 0$$

for some x_i all in A with λ_i scalars. Since C is a chain, each x_i is in some A_k. Then we can choose some $1 \leqslant \ell \leqslant n$ with

$$\bigcup_{j=1}^{n} A_{i_j} = A_{i_k}.$$

But A_{i_k} is linearly independent, so the λ_i are all zero. Therefore A is linearly independent too. By Zorn's Lemma, there is a maximal element $B \subseteq X$, which is therefore a basis. □

Corollary: Every linearly independent set $B_0 \subseteq V$ is contained in some basis of V.

Note: $\mathbb{R}$ is a vector space over $\mathbb{Q}$. A basis of $\mathbb{R}$ over $\mathbb{Q}$ is called a *Hamel basis*. The real vector space $\mathbb{R}^{\mathbb{N}}$, the set of real-valued sequences, has a basis, but has no countable basis.

Note: Zorn's lemma is very widely applicable. For example, the existence of maximal ideals in rings with 1, the existence of continuous linear functionals in a normed space, the proof that every connected graph has a spanning tree, and more all use this result.

We now complete the proof of the *model existence lemma* (Theorem 1.17) from the first section on propositional logic, in the case of an arbitrary (possibly uncountable) set of primitive propositions.

Theorem 3.16 (General Model Existence Lemma)

Let $S \subseteq L$. If S is consistent, then S has a model.

That is, if P is any set of primitive propositions, with $S \subseteq L(P)$ a consistent set, then there is some consistent set $\bar{S}$ with $S \subseteq \bar{S}$ and for all $t \in L$, either $t \in \bar{S}$ or $\neg t \in \bar{S}$.

Proof: We seek a maximal (with regard to inclusion) consistent set $\bar{S}$ containing S. Then we complete the proof by taking an arbitrary $t \in L$ and noticing that either $\bar{S} \cup \{t\}$ or $\bar{S} \cup \{\neg t\}$ is consistent: if not then $\bar{S} \vdash \neg t$ and $\bar{S} \vdash \neg\neg t$ by the Deduction Theorem (1.13). Then $\bar{S} \vdash \bot$ by modus ponens, which contradicts $\bar{S}$ being consistent.

Now, let $X = \{T \subseteq L : T \text{ is consistent and } S \subseteq T\}$, partially ordered by inclusion. Since $S \in X$, $X \neq \varnothing$. We now prove that every chain has an upper bound.

Let $C = \{T_i : i \in I\}$ be a non-empty chain in X. Clearly, the union of these sets T is an upper bound, and $S \subseteq T_i$, so we have $S \subseteq T$. It remains to show that T is consistent.

Otherwise, if $T \vdash \bot$, then there is some finite proof of this. Then there is some finite union of T_i which proves $\bot$: the ones with propositions used in the proof of $\bot$. But since C is a chain, there is some k with $T_{i_k} \vdash \bot$, but this is a contradiction. Therefore T is an upper bound in X.

But then X has a maximal element, by Zorn's Lemma. By maximality, we have either $t \in \bar{S}$ or $\neg t \in \bar{S}$, so $\bar{S}$ is a model of S, as required. □

Theorem 3.17 (Well-Ordering Principle)

Every set A can be well-ordered.

Proof: Let $X = \{(B, R) \in \wp(A) \times \wp(A \times A) : R \text{ is a well-ordering of } B\}$ be partially ordered by inclusion: $(B_1, R_1) \leqslant (B_2, R_2)$ if and only if $B_1 \subseteq B_2$ and $R_1 = R_2 \cap (B_1 \times B_1)$: B_1 is an initial segment of B_2.

Notice that $(\varnothing, \varnothing) \in X$, so $X \neq \varnothing$. Now let $C = \{(B_i, R_i) : i \in I\}$ be a non-empty chain in X: a nested collection of well-ordered sets. Then the element-wise union is an upper bound, by Proposition 2.18.

By Zorn's Lemma, we thus have a maximal element $(B, R) \in X$. If $B \neq A$, then for $x \in A \setminus B$, we can construct a new well-ordering by $(B \cup \{x\}, R \cup \{(b, x) : b \in B\} \cup \{(x, x)\})$. That is, we take (B, R) and add a new element x to B greater than all previous elements.

But then this is a bigger element of X, so (B, R) was not maximal. Therefore the maximal element is such that $B = A$. Therefore there is some (A, R) with R a well-ordering of A. Equivalently, the set A can be well-ordered! □

Corollary: The set of real numbers $\mathbb{R}$ can be well-ordered! Despite this, no well-ordering of $\mathbb{R}$ has ever been explicitly constructed.

In the proof of Zorn's Lemma (Theorem 3.14), we used a function from $X \to X$ which mapped $x \mapsto x' \in \{y \in X \mid x < y\}$. We also used a function $u : \{C \subseteq X : C \text{ a chain}\} \to X$, where $u(C)$ selects an element which is an upper bound for C. These functions are called *choice functions*. Another example of such a function is used in the proof that a countable union of countable sets is itself countable: we fix injections $f_n : A_n \to \mathbb{N}$ for each n.

The ability to do this is one of the most controversial disputes in mathematics, and is commonly termed the *Axiom of Choice*. We now turn to study it.

3.3 The Axiom of Choice

The *Axiom of Choice* is the assertion that for any set $X = \{A_i : i \in I\}$ of nonempty sets, there is a function $f : I \to \cup_{i\in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$. This is called a *choice function*. This is trivial when I is finite: we can prove it by induction on the size of I. However, when I is infinite, the existence of such a function is granted only by this axiom.

Note: This assertion is very different from the other rules for constructing sets which we have met so far, such as the union, intersection, or powerset constructions. These are all unique constructions which entirely specify a set, but this axiom just asserts that an object exists, without any regard to uniqueness.

Note: As mentioned in the motivation for this section, the existence of this axiom (AC for short) is controversial. Many people do not like the idea of asserting this, because the axiom has many strange consequences, and even those that do often want to verify whether proofs which use AC are in fact still valid without AC.

In fact, the seminal result of this section will be that two results we have seen before are in fact equivalent to the Axiom of Choice, and thus equivalent to each other: Zorn's Lemma and the Well-Ordering Principle (Theorems 3.14 and 3.17).

Theorem 3.18 (Axiom of Choice Equivalence)

The Axiom of Choice is equivalent to Zorn's Lemma (3.14), which is itself equivalent to the Well-Ordering Principle (3.17). That is, each of these imply the others.

Proof: We used the Axiom of Choice in the proof of Zorn's Lemma, so AC $\implies$ ZL.

We used Zorn's Lemma in the proof of the Well-Ordering Principle, so ZL $\implies$ WP.

We now show that the Well-Ordering Principle implies the Axiom of Choice. Let $X = \{A_i : i \in I\}$ be a set of non-empty sets A_i indexed by elements in some set I. Define A to be the union of these sets, so $A = \bigcup_{i\in I} A_i$. Fix a well-ordering of A.

Now we may define $f : I \to A$ by $f(i) \mapsto$ the least element of A_i. This is a choice function, so we have WP $\implies$ AC as required.

Therefore the three statements are equivalent, as required. □

Note: The rest of this chapter is **not examinable**.

We now consider two definitions, which seek to formalise ideas we have seen before. We use this to prove another fixed-point theorem (like Theorem 3.10) with and without the Axiom of Choice.

Definition 3.19 (Chain-Complete)

A poset X is *chain-complete* if $X \neq \varnothing$ and every non-empty chain has a supremum.

Corollary: Every complete poset (Definition 3.7) and every finite poset is chain-complete.

Corollary: If X is a poset, then $\{C \subseteq X : C \text{ a chain}\}$ ordered by inclusion is chain-complete.

Definition 3.20 (Inflationary)

A function $f : X \to X$ on a poset X is *inflationary* if $x \leqslant f(x)$ for all $x \in X$.

We may now use these two definitions to state and prove a fixed-point theorem.

Theorem 3.21 (Bourbaki-Witt Fixed Point Theorem)

If X is a chain-complete poset and $f : X \to X$ is inflationary, then f has a fixed point.

Proof: (With AC) We may use Zorn's Lemma to claim that X has a maximal element x. Then $x \leqslant f(x)$ by f being inflationary, but $x \geqslant f(x)$ by maximality, so $x = f(x)$. □

Proof: (Without AC) Assume f has no fixed point. Fix $x_0 \in X$. Let $\gamma = \gamma(X)$ be an ordinal which does not inject into X, by Hartog's Lemma (Theorem 2.26). Define $g : \gamma \to X$ by recursion:

$$\begin{aligned} g(0) &= x_0 \\ g(\alpha + 1) &= f(g(\alpha)) \\ g(\lambda) &= \sup \{g(\alpha) : \alpha < \lambda\} \end{aligned}$$

for successor and nonzero limit ordinals $\alpha + 1$ and λ.

By induction, for $\alpha < \beta$ we have that $g(\lambda)$ is well-defined and $g(\alpha) < g(\beta)$. But then g is injective, which is a contradiction. □

Note: The AC-free proof is very similar to the proof of the Knaster-Tarski Fixed Point Theorem (Theorem 3.10). In fact, this theorem is often called the *choice-free* part of Zorn's Lemma.

Theorem 3.22 (AC + BW ⇒ ZL)

The Axiom of Choice, along with Bourbaki-Witt, together imply Zorn's Lemma.

Proof: Let X be a poset in which every chain has an upper bound.

If X is chain complete, fix a choice function $g : \wp(X) \setminus \{\varnothing\} \to X$ where $g(Y) \in Y$ for all non-empty $Y \subseteq X$. That is, g maps non-empty subsets of X to elements of X contained within them.

Suppose that X has no maximal element. Then define $f : X \to X$ by $f(x) = g(\{y \in X : x < y\})$. Then for all x, we have $x < f(x)$ for all X, so this contradicts Bourbaki-Witt.

What if X is not chain-complete? Then let $Y = \{C \subseteq X : C \text{ a chain}\}$. This *is* chain-complete, so it has a maximal element, say C. Let x be an upper bound for C.

If x is not maximal, pick $y \in X$ with $x < y$. Then $C \cup \{y\}$ is a chain with $y \notin C$. But this means C was not maximal in Y, so in fact x is maximal in X. □

Note: In fact, we proved the *Hausdorff Maximality Principle*, which states that every poset has a maximal chain. This is also equivalent to the Axiom of Choice!

4 First-Order Predicate Logic

Now, we return from set theory to logic once more. Our original model of basic propositional logic was easy to work with, but it was difficult to model actual mathematical theories, let alone the rich variety of statements present in modern mathematics. We aim now to take another step towards being able to formalise as much as we can.

To this end, we replace the primitive propositions of propositional logic with actual mathematical statements. For example, we have statements like:

$$\text{“}m(x,\, m(y,z)) = m(m(x,y),\, z)\text{”} \text{ (associativity of group multiplication)}$$

or in the language of posets, statements like $x \leqslant y$.

But these are meaningless right now! We need variables like x, y, and z, and we also need operator symbols, like the binary symbol m which denotes multiplication, or the unary symbol i which denotes the identity, or even “nullary symbols” which operate on zero variables and are thus just constants. Will our statements then have meaning?

No! We need to have predicate statements, like the binary predicate $\leqslant$ or $=$. This is something with a truth value: yes, $m(x,y)$ operates on two arguments, but it has no truth value.

We will then combine statements built in this way into *formulae*, which finally mean something: they are actual declarations of things which can be true! We can formalise associativity as:

$$\text{“}(\forall x)(\forall y)(\forall z)(m(x,\, m(y,z)) = m(m(x,y),\, z))\text{”}.$$

In fact, we can formalise all manner of other things, like transitivity:

$$\text{“}(\forall x)(\forall y)(\forall z)(((x \leqslant y) \wedge (y \leqslant z)) \Rightarrow (x \leqslant z))\text{”}.$$

The valuations we have described so far (Definition 1.2) will become *structures*. These are sets A together with functions $p_A : A^n \to \{0,1\}$ for any formula p, with n the number of variables in p.

Similarly, if S is a set of formulae, we regard the notion of a *definition-propositional-model* (Definition 1.8) for S, as well as the notions of semantic and syntactic entailment from the chapter on Propositional Logic, all in the language of First-Order Predicate Logic.

4.1 Language

Now, having introduced a heuristic idea of logic, we begin to consider it formally.

Definition 4.1 (Language)

A *language* L in first-order predicate logic is specified by a disjoint pair of sets:

Ω the set of *operation* symbols, and

Π the set of *predicate* symbols,

as well as an *arity function* $\alpha : \Omega \cup \Pi \to \mathbb{N}_0$. This function represents how many arguments each operation or predicate takes: for example, $\alpha(\leqslant) = 2$. Then $L = L(\Omega, \Pi)$ consists of:

1. The set of *variables* is a countably infinite set disjoint from Ω and Π. Each formula only uses finitely many variables: we use $x_1, x_2, \ldots$ to denote them, or often x, y, and z.
2. The set of Ω-terms (or simply *terms*) is defined inductively: every variable is a term, and if $\omega \in \Omega$ has arity $n = \alpha(\omega)$, then $\omega t_1 \ldots t_n$ is a term for all terms $t_1, \ldots, t_n$.

We now have terms, but can't do much with them. This is where *formulae* come in.

Definition 4.2 (Atomic Formula)

If s and t are terms, then $(s = t)$ is an atomic formula.

If $\varphi \in \Pi$ has arity $n = \alpha(\varphi)$, and $t_1, \ldots, t_n$ are all terms, then $\varphi t_1 t_2 \ldots t_n$ is an atomic formula.

Nothing else is an atomic formula.

Example 4.3 (Language of Groups and Posets)

For example, we take the language of groups, with $\Omega = \{m, i, e\}$ and $\Pi = \varnothing$. These are the symbols for multiplication, inverses, and the identity: binary, unary, and nullary symbols respectively. That is, they have arities 2, 1, and 0.

Then we can write down some terms:

1. $mxmyz$ is a term, representing the multiplication $x(yz) = m(x, m(y, z))$.
2. $mmxyz$ is a term representing $(xy)z$.
3. $imxix$ is a term representing $(xx^{-1})^{-1}$.
4. mee is a term representing e^2.

However, $mxyz$, $xmyy$, and ex, among others, are not terms!

Then $(mxmyz = mmxyz)$ is an atomic formula, representing associativity of multiplication in groups. Similarly, $(mxix = e)$ is the statement of left-inverses.

Now consider the language of posets. Now, we have $\Omega = \varnothing$ and $\Pi = \{\leqslant\}$, with $\alpha(\leqslant) = 2$. Then the only terms are the variables, since Ω is empty, and some atomic formulae include $(x_1 = x_2)$ and $(x_1 \leqslant x_2)$

In fact, this last atomic formula should be $\leqslant x_1 x_2$, but we follow conventional notation when we know what they represent.

Note: We don't need brackets for terms: everything is uniquely defined by the order of symbols and the arities of everything in Ω and Π.

These are not the only type of formulae: we now introduce the rest.

Definition 4.4 (Formula)

The set of formulae is defined as follows:

1. Atomic formulae are formulae.
2. $\bot$ is a formulae.
3. If p and q are formulae, then so is $(p \Rightarrow q)$.
4. If p is a formula and x is a free variable (to be defined) in p, then $(\forall x)p$ is a formula. This is to be read as "for all x, we have p".

Nothing else is a formula. We also introduce several abbreviations. $\neg x$ is short for $(x \Rightarrow \bot)$, $\top = \neg\bot$, and so on for $\wedge$, $\vee$ as in propositional logic. We also use $\Leftrightarrow$ for $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

We also abbreviate the formula $\neg(\forall x)\neg p$ as $(\exists x)p$.

Really, a formula is a finite string from $\Omega \cup \Pi$, variables, and the symbols $\{\bot, \Rightarrow, (,)\}$, plus other symbols introduced as abbreviations. An occurrence of a variable can be either *free* or *bound*, defined by induction on the language.

Definition 4.5 (Free and Bound Variables, Sentence)

Any occurrence of any variable in an atomic formula is *free*.

If p and q are formulae, then any occurrence of a variable in p or q remains of the same type in the formula $(p \Rightarrow q)$.

If p is a formula, and a variable x has at least one free ocrrence in p, then every free occurrence of x in p becomes bound in the formula $(\forall x)p$. Everything else is unchanged.

We let $\mathrm{FV}(p)$ be the set of free variables in a formula p. These are variables with at least one free occurrence in p.

A formula with no free variables is called a *sentence*.

Example 4.6 (Free and Bound Variables)

Take the language of groups again, from the previous example.

Consider the formula $(mxix = e) \Rightarrow (mixx = e)$. Clearly, x is free in either atomic formula on the left or right, so remains free here.

Now, consider $(\forall x)(mxx = e) \Rightarrow (\forall x)(\forall y)(mxy = myx)$, which is the statement that groups where all elements have order at most 2 are abelian. The occurrences of x and y in $mxx = e$ and $mxy = myx$ are free originally, but then by the rule they become bound. The occurrences in $(\forall x)$ and $(\forall y)$ are thought of as being neither bound nor free, so there are no free variables in this formula.

Definition 4.7 (Structure)

A *structure* in a first-order language $L = L(\Omega, \Pi)$, sometimes known as an L-structure, is a non-empty set A together with functions $\omega_A : A^n \to A$, where $\omega \in \Omega$ and $n = \alpha(\omega)$, and a subset $\varphi_A \subseteq A^n$ for each $\varphi \in \Pi$. We identify this subset with its indicator function $\varphi_A : A^n \to \{0, 1\}$, where again $n = \alpha(\varphi)$.

Note: If $\alpha(\omega) = 0$, then ω is called a *constant*, since it is a function $\omega_A : \{\varepsilon\} \to A$, which can be interpreted as an element $\omega_A \in A$.

Note: In fact, we do not allow $\varnothing$ as a structure, excluding it here as a simplifying assumption. See Remark 4.24 for more details as to why allowing $\varnothing$ as a structure causes problems.

In the language of groups, an L-structure is therefore a set A with 3 functions $m_A : A \times A \to A$, $i_A : A \to A$, and $e_A \in A$. This is not a group yet! Similarly, in the language of posets, a structure is therefore a non-empty set with a subset $\leqslant_A \subseteq A \times A$. Again, this is not yet a poset!

Now, let A be a structure on the language of groups, and let p be the atomic formula $(mxix = e)$. We want to interpret p in the structure, and ask "is p satisfied in A?"

Intuitively, we should have $p_A = \{a \in A : m_A(a, i_A(a)) = e_A\}$. That is, p_A is the set of elements of A for which the atomic formula is "true". Then, we say p is satisfied in A if $p_A = A$.

If q is the formula $(\forall x)p$, what should q_A be? This should be a function from $A^0 = \{\varepsilon\}$ to $\{0, 1\}$, and we say q_A is "true" (1) if $p_A = A$ and "false" (0) otherwise.

This holds for all sentences: one simply substitutes the basic symbols in the language L for their interpretations in the structure as functions.

We now formalise this definition of interpretation for first-order languages: assigning sentences the values of "true" and "false".

Definition 4.8 (Interpretation)

Let $L = L(\Omega, \Pi)$ be a first-order language, and A an L-structure.

Given a term $t \in L$ and a formula p in L, both with free variables contained in $\{x_1, \dots, x_n\}$, we define *interpretations* $t_A : A^n \to A$ of t and $p_A : A^n \to \{0, 1\}$ (or equivalently, $p_A \subseteq A^n$).

These interpretations are fixed by induction on L.

1. If $t = x_i$ for some $1 \leqslant i \leqslant n$, then $t_A(a_1, \dots, a_n) = a_i$.
2. If $t = \omega t_1 \dots t_m$ for some $\omega \in \Omega$ and $m = \alpha(\Omega)$, and $t_1, \dots, t_m$ are terms, then we define $t_A(a_1, \dots, a_n) = \omega_A((t_1)_A(a_1, \dots, a_n), \dots, (t_m)_A(a_1, \dots, a_n))$

If $\alpha(\omega) = n$ and $t = \omega x_1 \dots x_n$, then $t_A = \omega_A$.

1. If p is the formula $(u = v)$, where u and v are terms, then we define p_A to be the subset $p_A = \{(a_1, \dots, a_n) \in A^n : u_A(a_1, \dots, a_n) = v_A(a_1, \dots, a_n)\}$, or its indicator function.
2. If p is $\varphi t_1 \dots t_m$ where $\varphi \in \Pi$ with $\alpha(\varphi) = m$, and $t_1, \dots, t_m$ are terms, then we define $p_A(a_1, \dots, a_n) = \varphi_A((t_1)_A(a_1, \dots, a_n), \dots, (t_m)_A(a_1, \dots, a_n))$, or the subset where this function takes the value 1.

That defines interpretations of terms and atomic formulae. What about other formulae?

1. $\bot_A : A^n \to \{0, 1\}$ is the constant function always equal to 0, or equivalently $\varnothing$.
2. If p is the formula $(q \Rightarrow r)$, then $p_A = (A^n \setminus q_A) \cup r_A$. Equivalently, viewed as a function, it takes value 0 when $q_A = 1$ and $r_A = 0$ on the same input, or value 1 otherwise.
3. If p is the formula $(\forall x_{n+1})q$, where $\mathrm{FV}(q) \subseteq \{x_1, \dots, x_n\}$, then we can define the set $p_A = \{(a_1, \dots, a_n) \in A^n : q_A(a_1, \dots, a_n) = 1 \text{ for all } a_{n+1} \in A\}$.

All of these definitions are intuitively obvious, but difficult to formalise!

4.2 Theories and Models

Now, having formalised interpretation, we consider the truth values of formulae with respect to a given L-structure A. When is some formula p true in A?

Definition 4.9 (Model)

If $L = L(\Omega, \Pi)$ is a first order language, and A is an L-structure, then we say that a formula $p \in L$ "*holds* in A", or "p is *satisfied* in A", or "p is *true* in A", or "A is a *definition-propositional-model* of p", if $p_A = A^n$. Equivalently, if $p_A : A^n \to \{0, 1\}$ is the constant function 1, where $n = \#\mathrm{FV}(p)$.

Corollary: If p is a sentence, then $p_A : A^0 \to \{0, 1\}$, or equivalently $p_A \in \{0, 1\}$. So a sentence p_A holds in A if and only if $p_A = 1$.

Definition 4.10 (Theory)

A *theory* in L is a set of sentences in L.

A *model of a theory* T is an L-structure A in which every sentence $t \in T$ is satisfied.

Now, it's time to formalise some existing structures we know and love into first-order theories. To do this, we must write down sets Ω and Π, define the arities of all of their elements, and then write down sentences in the language $L = L(\Omega, \Pi)$.

Example 4.11 (Group Theory)

The language of group theory is $\Omega = \{m, i, e\}$ with arities $\alpha(m) = 2$, $\alpha(i) = 1$, $\alpha(e) = 0$, and $\Pi = \varnothing$. We now define a *theory* of groups.

$$\begin{aligned} T = \{&(\forall x)(\forall y)(\forall z)(mmxyz = mxmyz),\\ &(\forall x)((mex = x) \wedge (mxe = x)),\\ &(\forall x)((mixx = e) \wedge (mxix = e))\} \end{aligned}$$

These are the sentences representing associativity, identity, and inverses respectively. Every model of T is a group, and every group is a model of T. So we have successfully axiomatised groups as a first-order theory!

Example 4.12 (Posets)

The language of posets is $\Omega = \varnothing$ and $\Pi = \{\leqslant\}$ with arity $\alpha(\leqslant) = 2$. A theory of posets is:

$$\begin{aligned} T = \{&(\forall x)(x \leqslant x),\\ &(\forall x)(\forall y)(((x \leqslant y) \wedge (y \leqslant x)) \Rightarrow (x = y)),\\ &(\forall x)(\forall y)(\forall z)(((x \leqslant y) \wedge (y \leqslant z)) \Rightarrow (x \leqslant z))\} \end{aligned}$$

These are the sentences representing reflexivity, antisymmetry, and transitivity respectively. Every model of T is a poset, and every poset is a model of T.

An important difference with these examples of group theory and posets is that the latter theory *required* the use of the implication symbol $\Rightarrow$. Of course, we did use $\Rightarrow$ implicitly in the example of group theory, since $\wedge$ is shorthand for an implication, but this can be avoided by splitting the second and third sentences into two sentences each.

Note: Theories which can be formalised in first-order logic without using the $\Rightarrow$ symbol are called *algebraic* theories. The theory of groups is thus algebraic.

Example 4.13 (Rings and Fields)

We have $\Omega = \{+, \times, -, 0, 1\}$ with arities 2, 2, 1, 0, and 0 respectively, and $\Pi = \varnothing$. Then

$$\begin{aligned} T = \{&(\forall x)(\forall y)(\forall z)(((x + y) + z) = (x + (y + z))),\\ &(\forall x)(\forall y)(x + y = y + x),\\ &(\forall x)(x + 0 = x),\\ &(\forall x)(x + (-x) = 0),\\ &(\forall x)(\forall y)(\forall z)(((x \times y) \times z) = (x \times (y \times z))),\\ &(\forall x)(\forall y)(\forall z)(x \times (y + z) = x \times y + x \times z),\\ &(\forall x)(\forall y)(\forall z)((x + y) \times z = x \times z + y \times z),\\ &(\forall x)(1 \times x = x),\\ &(\forall x)(x \times 1 = x)\} \end{aligned}$$

is a theory of rings. To extend this to fields, we can take the same Ω and Π and define:

$$T' = T \cup \{(x \times y = y \times x),\ \neg(0 = 1),\ (\forall x)(\neg(x = 0) \Rightarrow (\exists y)(x \times y = 1))\}$$

to add commutativity of multiplication, zero and one distinct, and multiplicative inverses.

Note: This is *not* an algebraic theory! We really do require implication here.

Example 4.14 (Graphs)

We have $\Omega = \varnothing$ and $\Pi = \{\sim\}$ with arity 2 (the connectedness relation). The theory of graphs is then axiomatised by $T = \{(\forall x)(\sim xx), (\forall x)(\forall y)(\sim xy \Rightarrow \sim yx)\}$. That is, connectedness is a reflexive and symmetric relation.

Finally, we show that propositional logic, from §1.1, is a first-order theory. In fact, we show that it is a special case of first-order predicate logic!

Proposition 4.15 (Propositional is Predicate)

Propositional logic is a special case of first-order predicate logic.

Proof: We take a system of propositional logic and attempt to axiomatise it in the formal system of first-order predicate logic.

Let P be a set of primitive propositions. Define $\Omega = \varnothing$, and $\Pi = P$, with $\alpha(p) = 0$ for all $p \in P$. That is, every proposition is a predicate with arity 0, and thus each $p \in P$ is an atomic formula in the language $L = L(\Omega, \Pi)$.

Now, each formula $t \in L(P)$ (Definition 1.1) is a formula in L! An L-structure is a set A with associated functions $p_A : A^0 \to \{0, 1\}$ with $p \in P$. That is, $p_A \in \{0, 1\}$ for all $p \in P$.

But this yields a function $v : P \to \{0, 1\}$, with $v(p) = p_A$. This is just a valuation!

For every $t \in L(P)$, we have $t_A \in \{0, 1\}$ as defined earlier. So we have a natural extension of v to $L(P)$, with $v(t)$ matching the definition of a valuation given in Definition 1.2.

So for $S \subseteq L(P)$, a model of S in the sense of Definition 4.9 is an L-structure A together with a function $v : p \to \{0, 1\}$ such that for all $p \in S$, $p_A = 1$, that is $v(p) = 1$.

But this is the same as the notion of a model from Definition 1.8, so propositional logic really can be axiomatised in first-order predicate logic! □

Definition 4.16 (Basic Semantic Entailment)

Let $L = L(\Omega, \Pi)$ be a first-order language, and let S be a theory in L with t a sentence in L.

We say that S *semantically entails* t if t is satisfied in every model of S, and write $S \vDash t$.

Example 4.17 (Semantic Entailment)

Let T be the theory of fields, from Example 4.13. Let p be the formula $\neg(x = 0)$, and let t be the formula $(\exists y)(xy = 1)$. Then define $S = T \cup \{p\}$.

Intuitively, it should be the case that $S \vDash t$. That is, "if x is not 0, then it has a multiplicative inverse" really is true in the actual study of fields.

But in fact, we cannot do this, since there is no model of S: there is no structure that assigns a value to p.

If F is a field, then $p_F = F \setminus \{0\} \neq F$. But if $a \in F$ and $p_F(a) = 1$ (that is, $a \in F$ is not 0), then $t_F(a) = 1$. So there should be some notion of entailment which uses this.

In a sense, our original definition of semantic entailment seems lacking. We can't have a model which represents implication in the traditional sense. In fact, any formula which has one or more free variables (that is, any formula which is not a sentence) has no "truth value", and therefore any set including it cannot even be modelled.

Definition 4.18 (Semantic Entailment)

Let S be a set of formulae in a first-order language L, and let $t \in L$ be a formula. Introduce a new "constant" (that is, a nullary operation symbol) for each free variable which occurs in $S \cup \{t\}$. This creates a new language L'.

For $u \in S \cup \{t\}$, let u' be a formula in the new language L', obtained from u by replacing each free occurrence of a variable in u with the corresponding constant.

Then in L', we let $S' = \{s' : s \in S\}$. Then, we say S *semantically entails* t, and write $S \vDash t$, if $S' \vDash t'$. This really does use the definition of semantic entailment we used above, since there are (by construction) no free variables in S', and so we can have a model of S'.

This motivates many of the familiar definitions from §1.1, and some unfamiliar ones which basic propositional logic is insufficient to represent.

Definition 4.19 (Tautology)

A formula t in a first-order language L is a *tautology* if $\varnothing \vDash t$. Equivalently, tautologies are formulae t which are true in every L-structure. We write $\vDash t$.

Definition 4.20 (Replacement)

Let p be a formula in a language L, with $x \in \mathrm{FV}(p)$. If t is a term in L, no variable of which occurs bound in p, then the *replacement* $p[t/x]$ is the formula obtained from p by replacing each free occurrence of x in p by t.

Example 4.21 (Replacement in Group Theory)

Let p be the formula $(\forall y)(mmxyx = mmyxy)$ in the language of groups. In fact, this is the claim that $xyx = yxy$ for all y, and is a property of x, since x is the unique free variable in p.

Now, we compute some replacements.

1. If $t = mzz$, then $p[t/x]$ is $(\forall y)(mmmzzymzz = mmymzzy)$.
2. If $t = mxx$, then $p[t/x]$ is $(\forall y)(mmmxxymxx = mmymxxy)$.
3. If $t = myy$, then $p[t/x]$ is not defined: y is a variable of t which occurs bound in p.

4.3 Syntactic Entailment

Much like in the world of propositional logic, we may model formal syntactic proofs in first-order predicate logic. Previously in §1.3, we axiomatised propositional logic with three main axioms. Now, we do the same for first-order predicate logic. The seven axioms are:

1. For formulae $p, q \in L$, $p \Rightarrow (q \Rightarrow p)$.
2. For formulae $p, q, r \in L$, $p \Rightarrow (q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.
3. For formulae $p \in L$, $\neg\neg p \Rightarrow p$.
4. $(\forall x)(x = x)$.
5. $(\forall x)(\forall y)((x = y) \Rightarrow (p \Rightarrow p[y/x]))$.
6. $(\forall x)(p) \Rightarrow p[t/x]$.
7. $(\forall x)(p \Rightarrow q) \Rightarrow (p \Rightarrow (\forall x)q)$.

The first three of these are copied wholesale from propositional logic. The next four are new rules about how relations, quantifiers, and substitution work.

4. $(\forall x)(x = x)$ represents the reflexivity of equality.
5. $(\forall x)(\forall y)((x = y) \Rightarrow (p \Rightarrow p[y/x]))$ states that if p holds for x, and $x = y$, then p holds for y.
6. $(\forall x)(p) \Rightarrow p[t/x]$ states that if p holds for all x, then in particular it holds for t.
7. $(\forall x)(p \Rightarrow q) \Rightarrow (p \Rightarrow (\forall x)q)$ defines transferability of quantification.

As before, all of the axioms are tautologies. However, we now have *two* rules of deduction!

Definition 4.22 (Deduction Rules)

From p and $(p \Rightarrow q)$, we may deduce q. This is called *modus ponens*, as in Definition 1.9.

If $x \in \mathrm{FV}(p)$, then from p we may deduce $(\forall x)(p)$, provided that x does not occur as a free variable in any premise used in the proof of p. This is called *generalisation*.

In proofs, we write (MP) and (Gen) to represent these rules of deduction.

Definition 4.23 (Proof)

Let S be a set of formulae in a language L, and let p be a formula in L. A *proof* of p from S is a finite sequence $t_1, \ldots, t_k$ of formulae in L, such that $t_n = p$, and for every i, either:

1. t_i is one of the seven axioms of first-order predicate logic, or
2. t_i is a premise (that is, $t_i \in S$), or
3. t_i follows by *modus ponens*: there are $j, k < i$ with $t_k = (t_j \Rightarrow t_i)$, or
4. t_i follows by *generalisation*: there is $j < i$ with $t_i = (\forall x)(t_j)$, and $x \in \mathrm{FV}(t_j)$, where x is not a free variable in any premise t_k with $k \leqslant j$.

If there is such a proof of p from S, then we say that S *proves* p, and write $S \vdash t$. Alternatively, we say that S *syntactically entails* t (as opposed to *semantically*, per Definition 4.18).

If S is a theory in L and $p \in L$ is a sentence, then if $S \vdash p$ we say that p is a *theorem* of S.

Compare this definition to the one given in the first chapter (1.10). There are more axioms to choose from, and we may use generalisation, but otherwise the definitions are identical.

Remark 4.24 (Why Exclude $\varnothing$?)

In our definition of a structure (Definition 4.7), we insisted that the set A was non-empty. In fact, our notion of proof would cause problems if we were to allow $\varnothing$ as a valid structure.

Suppose $\varnothing$ was an L-structure. Then $(\forall x)(\neg(x = x))$ is satisfied in $\varnothing$, but $\bot$ is not. Thus we have $\{(\forall x)(\neg(x = x))\} \nvdash \bot$, since there is an L-structure in which the former is true but the latter is not. However, $\{(\forall x)(\neg(x = x))\} \vdash \bot$, as shown by the abridged proof below:

1. $\neg(x = x)$ (MP on premise and A6)
2. $(\forall x)(x = x) \Rightarrow (x = x)$ (A6, substituting x for x in $x = x$)
3. $(x = x)$ (MP on A4 and previous line)

which proves $\bot$ by modus ponens. Thus allowing $\varnothing$ as an L-structure breaks completeness.

This allows us to write down what a proof in first-order predicate logic looks like!

Example 4.25 (Proof of Symmetry)

We wish to prove that the equality relation is symmetric: that is, if $x = y$, then $y = x$. We formalise this as $\{(x = y)\} \vdash (y = x)$.

1. $(\forall x)(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$ (A5)
2. $(\forall x)(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z))) \Rightarrow (\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$ (A6)
3. $(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$ (MP)
4. $(\forall y)((x = y) \Rightarrow ((x = z) \Rightarrow (y = z))) \Rightarrow ((x = y) \Rightarrow ((x = z) \Rightarrow (y = z)))$ (A6)
5. $(x = y) \Rightarrow ((x = z) \Rightarrow (y = z))$ (MP)
6. $x = y$ (premise)
7. $(x = y) \Rightarrow (y = z)$ (MP)
8. $(\forall z)((x = z) \Rightarrow (y = z))$ (Gen)
9. $(\forall z)((x = z) \Rightarrow (y = z)) \Rightarrow ((x = x) \Rightarrow (y = x))$ (A6)
10. $(x = x) \Rightarrow (y = x)$ (MP)
11. $(\forall x)(x = x) \Rightarrow (x = x)$ (A6)
12. $(\forall x)(x = x)$ (A4)
13. $x = x$ (MP)
14. $y = x$ (MP)

This proof witnesses $\{(x = y)\} \vdash (y = x)$, as expected.

Note: In a sense, Axiom 6 is the opposite of generalisation. The latter states that if we can prove a statement p for a free variable x without using x in the proof, then it must be true for all x. This makes sense, since the same proof works no matter the value of x. The former states the opposite: if p is true for all x, then in particular it is true for any specific x you might care to name.

Our target for most of the rest of this chapter is to rebuild as many of the results we proved for propositional logic into the new system of first-order logic.

Now, we can extend one of the most important results from the first chapter to first-order predicate logic. This was the (Propositional) Deduction Theorem (1.13).

Theorem 4.26 (Deduction Theorem)

Let S be a set of formulae in a first-order language L, and let p and q be formulae in L. Then $S \vdash (p \Rightarrow q)$ if and only if $S \cup \{p\} \vdash q$.

Proof: Assume $S \vdash (p \Rightarrow q)$. Then we can write down a proof of $(p \Rightarrow q)$ from S. Now, we can simply add p (premise) and q (MP) to obtain a proof of q from $S \cup \{p\}$ as desired.

Now suppose that $(S \cup \{p\}) \vdash q$, and let $t_1 \dots t_n$ be a proof of q witnessing this. Then $S \vdash (p \Rightarrow t_i)$ for all i, which we demonstrate by induction. In the case of $i = n$, this will show $S \vdash (p \Rightarrow q)$.

In particular, the induction hypothesis at step i is that "for all $j < i$, we know that $S \vdash (p \Rightarrow t_j)$, in such a way that if a variable x does not occur free in any premise in the proof $t_1, \dots, t_j$ of t_j from $S \cup \{p\}$, then x does not occur free in any premise used in the proof of $(p \Rightarrow t_j)$ from S."

This augmented hypothesis is constructed to ensure that generalisation works. If we had instead just supposed that $S \vdash (p \Rightarrow t_j)$ for all $j < i$, this is sometimes not sufficient to continue the proof!

Now, we consider four possible cases, based on the form the new line t_i takes at step i.

If t_i is an axiom or $t_i \in S$, then we can write down the proof that $(p \Rightarrow t_i)$ in the same way as the original Deduction Theorem.

1. t_i (premise or axiom)
2. $t_i \Rightarrow (p \Rightarrow t_i)$ (A1)
3. $p \Rightarrow t_i$ (MP)

The same goes for the case $t_i = p$, which yields the five-line proof of $(p \Rightarrow p)$ from Example 1.12.

Likewise, if t_i follows by modus ponens, then by the induction hypothesis, we can write down proofs of $(p \Rightarrow t_j)$ and $(p \Rightarrow (t_j \Rightarrow t_i))$. We can add the usual three lines to prove $(p \Rightarrow t_i)$. This uses no new free variables and so satisfies our induction condition.

1. $(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$ (A2)
2. $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ (MP)
3. $p \Rightarrow t_i$ (MP)

The last case is when $t_i = (\forall x)t_j$ follows by generalisation from a previous line t_j, where $x \in \mathrm{FV}(t_j)$ does not occur free in any of the premises in $t_1, \ldots, t_j$. In fact, this splits into two further cases.

If x does not occur free in p, then our job is easy: we can append the three lines:

1. $(\forall x)(p \Rightarrow t_j)$ (Gen)
2. $(\forall x)(p \Rightarrow t_j) \Rightarrow (p \Rightarrow (\forall x)t_j)$ (A7)
3. $p \Rightarrow (\forall x)t_j$ (MP)

This obtains a proof of $(p \Rightarrow t_i)$. If x does occur free in p, then our job is slightly harder. However, notice that p is not among $t_1, \ldots, t_j$ by the induction hypothesis, so in fact we have a proof of t_j from S alone. This means we can append the three lines:

1. $(\forall x)t_j$ (Gen)
2. $(\forall x)t_j \Rightarrow (p \Rightarrow (\forall x)t_j)$ (A1)
3. $p \Rightarrow (\forall x)t_j$ (MP)

This also obtains a proof of $(p \Rightarrow t_i)$. Neither of the two extensions of our proofs have used x as a free variable in any further premise, so indeed the induction hypothesis is satisfied. In particular, this means $(p \Rightarrow t_i)$ for all i, including the final line: $(p \Rightarrow q)$ as required. □

Our aim now is to prove the Completeness Theorem (1.19) but for first-order logic. In particular, we want to show that the syntactic and semantic entailment symbols $\vdash$ and $\vDash$ coincide. As in the first chapter, this splits into two theorems for the two directions: the Soundness Theorem (1.14) and the Adequacy Theorem (1.18).

Theorem 4.27 (Soundness Theorem)

Let S be a set of formulae in a first-order language L, and let p be a formula in L. Then if $S \vdash p$, we must have $S \vDash p$: the proof structure is *sound*, and does not prove any semantically incorrect propositions.

Proof: We use induction on the length of a proof of p from S. In the case $p = (\forall x)q$, there is a subset $S' \subseteq S$ where x does not occur free in S', and also $S' \vdash q$. By induction, $S' \vDash q$.

Since x does not occur free in S', we have $S' \vDash (\forall x)q$, and so $S \vDash p$. □

We now reconstruct the Model Existence Lemma. This was originally Theorem 1.17, and in the chapter on posets we proved a more general case as Theorem 3.16.

Theorem 4.28 (Model Existence Lemma)

Let S be a *consistent* theory in a first order language $L = L(\Omega, \Pi)$: that is, $S \nvdash \bot$. Then S has a model (as defined in 4.9).

Note: The proof of this theorem is non-examinable.

Proof: The key idea is to build a model A from the language L itself. To begin with, we let A be the set of *closed terms* in L: terms with no variables.

We turn this into a structure in the obvious way, and deal with issues as they come up. Firstly, if we have an operation with arity n, and a list of n terms, then we can interpret this in the structure as simply the combination of their terms: $m_A xy = mxy$.

This is sometimes not a model! For example, if T is the theory of fields, then $T \vdash (0+1) = 1$, but in A, these are two different terms. However, we can solve this by defining an equivalence relation on A, whereby $s \sim t$ if and only if $T \vdash (s = t)$. We then consider A to be $A/\sim$.

This still doesn't solve all our issues. There are sentences p such that T proves neither p nor $\neg p$, and so by definition T is not *complete*, as in 1.17. We solve this in the same way: given a consistent theory S, there exists some $\bar{S} \supseteq S$ which is complete.

However, we are still not done! Consider the theory of fields T in which 2 has a square root: that is, the theory of fields and the sentence $(\forall x)((x \cdot x = 1 + 1) \Rightarrow \bot) \Rightarrow \bot$, or more concisely, $(\exists x)(x \cdot x = 1 + 1)$. There is no closed term t such that $T \vdash (t \cdot t = 1 + 1)$. The problem is that T lacks a witness for $(\exists x)p$. We solve this by adding a witness: a new constant c to L and a new sentence to T to obtain $T' = T \cup \{p[c/x]\}$.

Now, we formalise this. We start with four observations:

1. If S is a consistent theory and p is a sentence, then either $S \cup p$ or $S \cup \{\neg p\}$ is consistent. If not, by the Deduction Theorem (4.26), $S \vdash \neg p$ and $S \vdash \neg\neg p$, but then $S \vdash \bot$, a contradiction.
2. By Zorn's Lemma, there is therefore a maximal consistent theory $\bar{S}$ which contains S such that for every sentence p, either $p \in \bar{S}$ or $\neg p \in \bar{S}$.
3. Suppose that $S \vdash (\exists x)p$, where p is a formula with exactly one free variable x. If there is no witness, we add a new constant (nullary operator) to L, and claim that the set $S \cup \{p[c/x]\}$ is consistent. If not, the Deduction Theorem yields a proof witnessing $S \vdash \neg p[c/x]$. But c does not appear in S, which means $S \vdash \neg p$. By generalisation (4.22), $S \vdash (\forall x)\neg p$, but this is a contradiction, since $S \vdash (\exists x)p$.
4. We can do this for every theorem of S of the form $(\exists x)p$, to obtain a new language, which we write as $\bar{L} = L(\Omega \cup C, \Pi)$. Here, C is a set of new constants disjoint from Ω and Π. We also obtain a new consistent theory $\bar{S}$ with $S \subseteq \bar{S}$ containing witnesses for S: for any such theorem in S, there is a closed term in $\bar{L}$ with $\bar{S} \vdash p[t/x]$.

We now repeat the procedure in these observations. We start with a consistent theory $S_0 = S$ in the language $L_0 = L(\Omega, \Pi)$, and define by induction a series of theories $S_0 \subseteq S_1 \subseteq T_1 \subseteq S_2 \subseteq \dots$ and new languages $L_n = L(\Omega \cup C_1 \cup \dots \cup C_n, \Pi)$, with all $n + 2$ sets pairwise disjoint.

For all n, S_n is a complete and consistent theory in L_{n-1}, and T_n is a consistent theory in L_n with witnesses for each theorem in S_n of the form $(\exists x)p$. We set L^* and S^* to be the union of the L_n and S_n respectively: it is easy to check that S^* is a consistent theory in L^*, contains S, is complete, and has witnesses. Therefore, without loss of generality, take $S^* = S$ and $L^* = L$.

We let A be the set of equivalence classes of closed terms in L, where we say that two closed terms s and t are equivalent if and only if $S \vdash (s = t)$. We make A an L-structure in the obvious way:

$$\omega_A([t_1], \dots, [t_n]) = [\omega t_1 \dots t_n] \quad \text{where } \omega \in \Omega \text{ with } \alpha(\omega) = n, \text{ and } t_1, \dots, t_n \text{ are closed terms.}$$

We then set $\varphi_A([t_1], \dots, [t_n]) = 1$ if and only if $S \vdash \varphi t_1 \dots t_n$.

We prove by induction on the terms of the language: if S is a term with variables in $\{x_1, \ldots, x_n\}$, then we let $s_A([t_1], \ldots, [t_n])$ be the equivalence class of $s[t_1/x_1, \ldots, t_n/x_n]$. As a result, if S is a closed term, then s_A is the equivalence class of s.

Similarly, for any formula p with free variables $\mathrm{FV}(p) \subseteq \{x_1, \ldots, x_n\}$, we have:

$$p_A([t_1], \ldots, [t_n]) = 1 \iff S \vdash p[t_1/x_1, \ldots, t_n/x_n].$$

In particular, if $p \in S$, then $S \vdash p$, so $p_A = 1$. But this is exactly what we wanted! The A which we have constructed is an L-structure such that if $p \in S$, then $p_A = 1$. This is therefore a model of S, which is what we set out to find. □

Theorem 4.29 (Adequacy Theorem)

Let S be a set of formulae in a first-order language L, and let p be a formula in L. If $S \vDash p$, then in fact $S \vdash p$. That is, if S semantically entails p, then there is a proof witnessing that S also syntactically entails p.

Note: The proof of this theorem is also non-examinable.

Proof: Take S to be a theory, and p a sentence. As in the definition of semantic entailment (4.18), we take $S' \vDash p'$. If we can deduce that $S' \vdash p'$, then it follows that $S \vdash p$.

Since $S \vDash p$, we have $S \cup \{\neg p\} \vDash \bot$. By the Model Existence Lemma (4.28), $S \cup \{\neg p\} \vdash \bot$. Also, by the Deduction Theorem (4.26), we have $S \vdash \neg\neg p$. Putting these together yields a proof of p, using Axiom 3. □

Like in §1.3, we can combine two of results we have just proved. The Soundness Theorem and the Adequacy Theorem (originally 1.14 and 1.18, now 4.27 and 4.29) combine to make the Completeness Theorem (originally 1.19, now 4.30).

Theorem 4.30 (Gödel's Completeness Theorem For First-Order Logic)

Let S be a set of formulae in a first-order language L, and let p be a formula in L. Then the notions of semantic and syntactic entailment coincide: $S \vDash p$ if and only if $S \vdash p$.

Proof: Obvious by the Soundness Theorem (4.27) and the Adequacy Theorem (4.29). □

Theorem 4.31 (Compactness Theorem)

Let S be a first-order theory. If every finite subset of S has a model, then S has a model.

Proof: If $S \vDash \bot$, then $S \vdash \bot$. But then we can write down a proof of $\bot$ from S. Since this proof is finite, there is some finite $S' \subseteq S$ with $S' \vdash \bot$. But then $S' \vDash \bot$, which is a contradiction. □

Considering the Compactness Theorem, we might wonder if we can axiomatise the theory of finite groups. That is, does there exist a theory in a suitable first-order language whose models are precisely the finite groups?

We may try letting t_n be the sentence $(\exists x_1)(\exists x_2)\ldots(\exists x_n)(\forall x)(x = x_1 \vee \cdots \vee x = x_n)$. This is the sentence "there are at most n elements": if t_n is satisfied in some L-structure A, then A is a group of at most n elements.

But then we would need T to be the theory of groups together with the "sentence" $t = t_1 \vee t_2 \vee \cdots$, which is not actually a sentence, as it is infinite. Of course, this doesn't mean we cannot axiomatise the finite groups, merely that this attempt has failed. However, this really is impossible!

Proposition 4.32 (No Axiomatisation of Finite Groups)

The finite groups cannot be axiomatised as a first-order theory. That is, there is no theory T in any first-order language L whose models are exactly the finite groups.

Proof: Suppose that T is such a theory. Then let

$$S = T \cup \{\neg t_1, \neg t_2, \neg t_3, \ldots\} \text{ where } t_n = (\exists x_1)(\exists x_2)\ldots(\exists x_n)(\forall x)(x = x_1 \vee \cdots \vee x = x_n).$$

Any finite subset of S as a model. For example, C_n, where $n = 1 + \max\{i : \neg t_i \in S\}$, is a model of S. But then by compactness, S has a model, which is a contradiction. □

Corollary: If a first-order theory T has arbitrarily large finite models, then in fact it has some infinite model, using the same argument!

In fact, we can prove an even stronger result.

Theorem 4.33 (The Upward Löwenheim-Skolem Theorem)

If a first-order theory S has an infinite model, then S has an uncountable model.

Proof: We can add uncountably many new constants $\{c_i : i \in I\}$ to the language, for some index set I which is uncountable. Then, consider:

$$S' = S \cup \{\neg(c_i = c_j) : i, j \in I \text{ with } i \neq j\}.$$

By assumption, S has an infinite model, which is a model of every finite subset of S'. But then by compactness S' has a model A', which is a model A of S and a finite set of sentences given with an injection $I \to A$ with $c_i \mapsto (c_i)_A$. But then A' is uncountable, as required. □

Corollary: By Hartog's Lemma (Theorem 2.26), we can take $I = \gamma(X)$. Then the proof of the above yields a model of S which cannot inject into X.

Note: It is easy to write down arbitrarily large groups, but comparatively much harder to write down arbitrarily large fields.

There is also another version of this theorem, which is in some sense the opposite.

Theorem 4.34 (The Downward Löwenheim-Skolem Theorem)

Let S be a theory in a countable language $L = L(\Omega, \Pi)$. That is, $\Omega \cup \Pi$ is countable. Then if S has a (possibly uncountable) model, then in fact it has a countable model.

Proof: By the Soundness Theorem (4.27), S must be consistent, as it has a model. But then the model constructed in the proof of the first-order Model Existence Lemma (4.28) is countable! □

4.4 Peano Arithmetic

We now wish to axiomatise the natural numbers $\mathbb{N}$ as a first-order theory. In fact, the key property of $\mathbb{N}$ is *induction*: in fact, this uniquely determines the set! We will try to construct our set using the property of induction with some axioms.

The language then consists of operation symbols $\Omega = \{0, S, +, \times\}$, with arities 0, 1, 2, and 2. We take no predicates, so $\Pi = \varnothing$. 0 is the constant "zero", S is the "successor" operator $n \mapsto n + 1$, and addition $+$ and multiplication $\times$ will be constructed in the familiar way.

We are now ready to formalise the natural numbers!

Definition 4.35 (Peano Arithmetic)

Peano Arithmetic (PA), also known as *formal number theory*, consists of the sentences:

1. $(\forall x)(\neg Sx = 0)$. "Nothing comes before 0."
2. $(\forall x)(\forall y)((Sx = Sy) \Rightarrow (x = y))$. "The successor function is injective."
3. $(\forall x)(x + 0 = x)$. "Zero is the additive identity."
4. $(\forall x)(\forall y)(x + Sy = S(x + y))$. "Associativity of addition holds with 1."
5. $(\forall x)(x \times 0 = 0)$. "Zero is a multiplicative fixed point."
6. $(\forall x)(\forall y)(x \times Sy = x \times y + x)$. "Multiplication distributes over the successor."
7. $(\forall y_1)(\forall y_2)\dots(\forall y_n)((p[0/x] \wedge (\forall x)(p \Rightarrow p[Sx/x])) \Rightarrow (\forall x)p)$. "Induction works."

In the last sentence, p is a formula with free variables $\mathrm{FV}(p) = \{x, y_1, \dots y_n\}$. In fact, this is an infinite collection of sentences, which defines induction for every formula.

Example 4.36 (Induction)

To see why parameters are needed, consider the formula p given by $(x + y) + z = x + (y + z)$, representing associativity of addition. We prove that $(\forall x)(\forall y)(\forall z)p$ by induction on z.

Fix x and y in some model of PA. We verify that $p[0/z]$ and $(\forall z)(p \Rightarrow p[Sz/z])$ hold. By induction, $(\forall z)p$ holds. The Completeness Theorem (4.30) then yields $\mathrm{PA} \vdash (\forall x)(\forall y)(\forall z)p$.

An obvious model of PA is $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. In fact, $\mathbb{N}$ is also a model, but including 0 is more natural. But by the Upward Löwenheim-Skolem Theorem (4.33), there is an uncountable model of PA. So is the countable set $\mathbb{N}$ is not unique as a set with our desired properties?

Actually, no! The formulation of induction we wanted to replicate was:

$$(\forall A \subseteq \mathbb{N}_0)(0 \in A \wedge (\forall x)(x \in A \Rightarrow Sx \in A) \implies A = \mathbb{N}_0).$$

That is, if a subset of $\mathbb{N}_0$ contains 0 and is closed under the successor operation, then in fact the subset must contain every natural number. The problem is that in first-order logic, we cannot do this quantification over subsets of a structure. Since the language of PA is countable, the induction axiom-scheme only captures countably many subsets of $\mathbb{N}_0$.

Definition 4.37 (Definable)

A subset $A \subseteq \mathbb{N}_0$ is called *definable* in Peano Arithmetic if there is a formula p in PA with one free variable such that $A = p_{\mathbb{N}_0}$.

The set of squares is thus definable in PA by the formula $(\exists y)(y \times y = x)$. The set of primes is definable by $(x \neq 1) \wedge (y \mid x \Rightarrow (y = 1 \vee y = x))$.

Note: We tend to use a lot of abbreviations for conciseness, if it is clear what we mean. For example, $y \mid x$ is short for "$(\exists z)(y \times z = x)$", 1 is short for $S0$, and $(x \neq y)$ is short for $\neg(x = y)$.

Theorem 4.38 (Gödel's Incompleteness Theorem)

Peano Arithmetic is not a complete theory of the natural numbers. That is, there exists some formula p which is true in the natural numbers, but which Peano Arithmetic does not prove.

Proof: This theorem is proved using *Gödel numbering*, and constructing a sentence which means "this sentence is not provable in PA". This sentence cannot be provable, by consistency, but also cannot be disprovable! □

5 Set Theory

Set theory is really just another mathematical theory. We will axiomatise it as a first-order theory, much like the theory of groups and rings. This section is therefore a *very* extended worked example similar to Example 4.13.

Note: Of course, any model of set theory should contain all of mathematics, since everything is in some sense a set. We therefore expect this example to be really quite complicated.

5.1 Zermelo-Fraenkel Set Theory (ZF)

We will study a particular first-order axiomatisation of set theory, developed by Ernst Zermelo and Abraham Fraenkel. This is often referred to as ZF for short.

The language of this theory has no operation symbols, so $\Omega = \varnothing$. There is a single predicate $\in$, which has arity 2. This is going to be the "is a member of" predicate.

Definition 5.1 (Set-Theoretic Universe)

A *definition-propositional-model* of ZF will be denoted by V, which is a non-empty set with an interpretation of the binary predicate $\in_V \subseteq V \times V$. Elements of V will then be called *sets*.

If (a, b) is in $\in_V$, we say "a is a member of b", or "a is an element of b", or "b contains a".

V is then called the *set-theoretic universe*.

Note: The words "set", "member", and so on no longer have the theoretical meaning we usually ascribe to them in the world of mathematics. Instead, they simply refers to an object or predicate in V. However, we will still talk about the existing world of mathematics, of which V is a part! This is likely to become confusing, but using other words would be cumbersome.

The study of set theory is then really an attempt to describe V.

There are nine "axioms" of this theory, which are sentences in first-order logic of this theory. The first two are introductory, the next four allow us to build sets, and the last three are properties of sets which are perhaps less obvious.

Let us consider these axioms now. Each axiom comes with a name, as well as an abbreviation, for use in proofs. We give a heuristic description of each axiom as well as the sentence to which it corresponds in first-order logic. The first two axioms are *Extensionality* and *Separation*.

1. The Axiom of Extensionality (Ext): "if two sets have the same members, they are equal." $(\forall x)(\forall y)((\forall z)(z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.
2. The Axiom of Separation (Sep): "we can take a subset of an existing set using a property." $(\forall t_1)(\forall t_2)\dots(\forall t_n)((\forall x)(\exists y)((\forall z)(z \in y \Leftrightarrow (z \in x \wedge p))))$.

Note: Here, p is a formula with free variables $\mathrm{FV}(p) = \{z, t_1, \dots t_n\}$. By the first axiom, this y is unique: we denote it by $\{z \in X : p\}$. Formally, this is an $(n+1)$-ary operation symbol within the language. We need the parameters here: given t and x, we may want to form $\{z \in x : t \in z\}$.

These axioms do not guarantee that any sets exist! Let us construct the first set: the empty set.

3. The Empty-Set Axiom (Emp): "there is a set without any elements." $(\exists x)((\forall y)\neg(y \in x))$. This is unique by (Ext), and we call it $\varnothing$, like a new nullary operator.
4. The Pair-Set Axiom (Pair): "for any x and y, we can form the set $\{x, y\}$." $(\forall x)(\forall y)(\exists z)(\forall t)(t \in z \Leftrightarrow (t = x \vee t = y))$.
   By (Ext), this is unique, and z is denoted by $\{x, y\}$. We write $\{x\}$ for $\{x, x\}$.

Note: Indeed, (Ext) gives us the general "ignore repeats" property of sets for free!