Logic and Set Theory

Cambridge University Mathematical Tripos: Part II

17th May 2024

Contents

1 Propositional logic

1.1 Languages

Let P be a set of *primitive propositions*. Unless otherwise stated, we let $P = \{p_1, p_2, \dots\}$. The *language* $L = L(P)$ is defined inductively by

(i) if $p \in P$, then $p \in L$;

(ii) $\bot \in L$, where the symbol $\bot$ is read 'false';

(iii) if $p, q \in L$, then $(p \Rightarrow q) \in L$.

Example. $((p_1 \Rightarrow p_2) \Rightarrow (p_1 \Rightarrow p_3)) \in L$. $(p_4 \Rightarrow \bot) \in L$.

Remark. Note that the elements of L, called propositions, are just strings of symbols from the alphabet $\{(,), \Rightarrow, \bot, p_1, p_2, \dots\}$. Brackets are only given for clarity; we omit those that are unnecessary, and may use other types of brackets such as square brackets.

Note that the phrase 'L is defined inductively' means more precisely the following. Let $L_1 = P \cup \{\bot\}$, and define $L_{n+1} = L_n \cup \{(p \Rightarrow q) \mid p, q \in L_n\}$. We set $L = \bigcup_{n=1}^{\infty} L_n$. Note that the introduction rules for the language are injective and have disjoint ranges, so there is exactly one way in which any element of the language can be constructed using rules (i) to (iii).

We can now introduce the abbreviations $\neg, \wedge, \vee$ defined by

$$\neg p = (p \Rightarrow \bot); \quad p \vee q = \neg p \Rightarrow q; \quad p \wedge q = \neg(p \Rightarrow \neg q)$$

1.2 Semantic implication

Definition. A *valuation* is a function $v : L \to \{0,1\}$ such that

(i) $v(\bot) = 0$;

(ii) $v(p \Rightarrow q) = 0$ if $v(p) = 1$ and $v(q) = 0$, and 1 otherwise.

Remark. On $\{0,1\}$, we can define the constant $\bot = 0$ and the operation $\Rightarrow$ in the obvious way. Then, a valuation is precisely a mapping $L \to \{0,1\}$ preserving all structure, so it can be considered a homomorphism.

Proposition. Let $v, v' : L \to \{0,1\}$ be valuations that agree on the primitives p_i. Then $v = v'$. Further, any function $w : P \to \{0,1\}$ extends to a valuation.

Remark. This is analogous to the definition of a linear map by its action on the basis vectors.

Proof. Clearly, v, v' agree on L_1, the set of elements of the language of length 1. If v, v' agree at p, q, then they agree at $p \Rightarrow q$. So by induction, v, v' agree on L_n for all n, and hence on L.

Let $v(p) = w(p)$ for all $p \in P$, and $v(\bot) = 0$ to obtain v on the set L_1. Assuming v is defined on p, q we can define it at $p \Rightarrow q$ in the obvious way. This defines v on all of L. □

Example. Let v be the valuation with $v(p_1) = v(p_3) = 1$, and $v(p_n) = 0$ for all $n \neq 1, 3$. Then, $v((p_1 \Rightarrow p_3) \Rightarrow p_2) = 0$.

Definition. A *tautology* is $t \in L$ such that $v(t) = 1$ for every valuation v. We write $\models t$.

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

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

Since the right-hand column is always 1, $\models p \Rightarrow (q \Rightarrow p)$.

Example. $\neg\neg p \Rightarrow p$, which expands to $((p \Rightarrow \bot) \Rightarrow \bot) \Rightarrow p$.

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

Hence $\models \neg\neg p \Rightarrow p$.

Example. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$. Suppose this is not a tautology. Then we have a valuation v such that $v(p \Rightarrow (q \Rightarrow r)) = 1$ and $v((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) = 0$. Hence, $v(p \Rightarrow q) = 1, v(p \Rightarrow r) = 0$, so $v(p) = 1, v(r) = 0$, giving $v(q) = 1$, but then $v(p \Rightarrow (q \Rightarrow r)) = 0$ contradicting the assumption.

Definition. Let $S \subseteq L$ and $t \in L$. We say S *entails* or *semantically implies* t, written $S \models t$, if $v(t) = 1$ whenever $v(s) = 1$ for all $s \in S$.

Example. Let $S = \{p \Rightarrow q, q \Rightarrow r\}$, and let $t = p \Rightarrow r$. Suppose $S \not\models t$, so there is a valuation v such that $v(p \Rightarrow q) = 1, v(q \Rightarrow r) = 1, v(p \Rightarrow r) = 0$. Then $v(p) = 1, v(r) = 0$, so $v(q) = 1$ and $v(q) = 0$.

Definition. We say that v is a *model* of S in L if $v(s) = 1$ for all $s \in S$.

Thus, $S \models t$ is the statement that every model of S is also a model of t.

Remark. The notation $\models t$ is equivalent to $\varnothing \models t$.

1.3 Syntactic implication

For a notion of proof, we require a system of axioms and deduction rules. As axioms, we take (for any $p, q, r \in L$),

(i) $p \Rightarrow (q \Rightarrow p)$;

(ii) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$;

(iii) $((p \Rightarrow \bot) \Rightarrow \bot) \Rightarrow p$.

Remark. Sometimes, these three axioms are considered axiom *schemes*, since they are really a different axiom for each $p, q, r \in L$. These are all tautologies.

For deduction rules, we will have only the rule *modus ponens*, that from p and $p \Rightarrow q$ one can deduce q.

Definition. Let $S \subseteq L$, $t \in L$. We say S *proves* or *syntactically implies* t, written $S \vdash t$, if there exists a sequence $t_1, \dots, t_n = t$ in L such that every t_i is either

(i) an axiom;
(ii) an element of S; or
(iii) q, where $t_j = p$ and $t_k = p \Rightarrow q$ where $j, k < i$.

We say that S is the set of *premises* or *hypotheses*, and t is the *conclusion*.

Example. We will show $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$.

1. $q \Rightarrow r$ (hypothesis)
2. $(q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$ (axiom 1)
3. $p \Rightarrow (q \Rightarrow r)$ (modus ponens on lines 1, 2)
4. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ (axiom 2)
5. $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ (modus ponens on lines 3, 4)
6. $p \Rightarrow q$ (hypothesis)
7. $p \Rightarrow r$ (modus ponens on lines 5, 6)

Definition. If $\varnothing \vdash t$, we say t is a *theorem*, written $\vdash t$.

Example. $\vdash p \Rightarrow p$.

1. $(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$ (axiom 2)
2. $p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$ (axiom 1)
3. $(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$ (modus ponens on lines 1, 2)
4. $p \Rightarrow (p \Rightarrow p)$ (axiom 1)
5. $p \Rightarrow p$ (modus ponens on lines 3, 4)

1.4 Deduction theorem

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

Intuitively, provability corresponds to the implication connective in L.

Proof. For the forward direction, given a proof of $p \Rightarrow q$ from S, add the line p by hypothesis and deduce q from modus ponens, to obtain a proof of q from $S \cup \{p\}$.

Conversely, suppose we have a proof of q from $S \cup \{p\}$. Let $t_1, \dots, t_n$ be the lines of the proof. We will prove that $S \vdash (p \Rightarrow t_i)$ for all i.

- If t_i is an axiom, we write t_i (axiom); $t_i \Rightarrow (p \Rightarrow t_i)$ (axiom 1); $p \Rightarrow t_i$ (modus ponens).
- If $t_i \in S$, we write t_i (hypothesis); $t_i \Rightarrow (p \Rightarrow t_i)$ (axiom 1); $p \Rightarrow t_i$ (modus ponens).
- If $t_i = p$, we write the proof of $\vdash p \Rightarrow p$ given above.

- Suppose t_i is obtained by modus ponens from t_j and $t_k = t_j \Rightarrow t_i$. We may assume by induction that $S \vdash p \Rightarrow t_k$ and $S \vdash p \Rightarrow (t_j \Rightarrow t_i)$. We write
  1. $(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$ (axiom 2)
  2. $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ (modus ponens)
  3. $p \Rightarrow t_i$ (modus ponens)

  giving $S \vdash p \Rightarrow t_i$.

□

Example. Consider $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$. By the deduction theorem, it suffices to prove $\{p \Rightarrow q, q \Rightarrow r, p\} \vdash r$, which is obtained easily from modus ponens.

1.5 Soundness

We aim to show $S \vDash t$ if and only if $S \vdash t$. The direction $S \vdash t$ implies $S \vDash t$ is called *soundness*, which is a way of verifying that our axioms and deduction rule make sense. The direction $S \vDash t$ implies $S \vdash t$ is called *adequacy*, which states that our axioms are powerful enough to deduce everything that is (semantically) true.

Proposition. Let $S \subseteq L$ and $t \in L$. Then $S \vdash t$ implies $S \vDash t$.

Proof. We have a proof $t_1, \dots, t_n$ of t from S. We aim to show that any model of S is also a model of t, so if v is a valuation that maps every element of S to 1, then $v(t) = 1$. We show this by induction on the length of the proof. $v(p) = 1$ for each axiom p and for each $p \in S$. Further, $v(t_i) = 1, v(t_i \Rightarrow t_j) = 1$, then $v(t_j) = 1$. Therefore, $v(t_i) = 1$ for all i. □

1.6 Adequacy

Consider the case of adequacy where $t = \bot$. If our axioms are adequate, $S \vDash \bot$ implies $S \vdash \bot$, so $S \nvDash \bot$. We say S is *consistent* if $S \nvdash \bot$. Therefore, in an adequate system, if S has no models then S is inconsistent; equivalently, if S is consistent then it has a model.

In fact, the statement that consistent axiom sets have a model implies adequacy in general. Indeed, if $S \vDash t$, then $S \cup \{\neg t\}$ has no models, and so it is inconsistent by assumption. Then $S \cup \{\neg t\} \vdash \bot$, so $S \vdash \neg t \Rightarrow \bot$ by the deduction theorem, giving $S \vdash t$ by axiom 3.

We aim to construct a model of S given that S is consistent. Intuitively, we want to write

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

but this does not work on the set $S = \{p_1, p_1 \Rightarrow p_2\}$ as it would evaluate p_2 to false.

We say a set $S \subseteq L$ is *deductively closed* if $p \in S$ whenever $S \vdash p$. Any set S has a *deductive closure*, which is the (deductively closed) set of statements $\{t \in L \mid S \vdash t\}$ that S proves. If S is consistent, then the deductive closure is also consistent. Computing the deductive closure before the valuation solves the problem for $S = \{p_1, p_1 \Rightarrow p_2\}$. However, if a primitive proposition p is not in S, but $\neg p$ is also not in S, this technique still does not work, as it would assign false to both p and $\neg p$.

Theorem (model existence lemma). Every consistent set $S \subseteq L$ has a model.

Proof. First, we claim that for any consistent $S \subseteq L$ and proposition $p \in L$, either $S \cup \{p\}$ is consistent or $S \cup \{\neg p\}$ is consistent. If this were not the case, then $S \cup \{p\} \vdash \bot$, and also $S \cup \{\neg p\} \vdash \bot$. By the deduction theorem, $S \vdash p \Rightarrow \bot$ and $S \vdash (\neg p) \Rightarrow \bot$. But then $S \vdash \neg p$ and $S \vdash \neg\neg p$, so $S \vdash \bot$ contradicting consistency of S.

Now, L is a countable set as each L_n is countable, so we can enumerate L as $t_1, t_2, \dots$. Let $S_0 = S$, and define $S_1 = S_0 \cup \{t_1\}$ or $S_1 = S_0 \cup \{\neg t_1\}$, chosen such that S_1 is consistent. Continuing inductively, define $\overline{S} = \bigcup_{i \in \mathbb{N}} S_i$. Then, for all $t \in L$, either $t \in \overline{S}$ or $\neg t \in \overline{S}$. Note that $\overline{S}$ is consistent; indeed, if $\overline{S} \vdash \bot$, then this proof uses hypotheses only in S_n for some n, but then $S_n \vdash \bot$ contradicting consistency of S_n. Note also that $\overline{S}$ is deductively closed, so if $\overline{S} \vdash p$, we must have $p \in \overline{S}$; otherwise, $\neg p \in \overline{S}$ so $\overline{S} \vdash \neg p$, giving $\overline{S} \vdash \bot$, contradicting consistency of $\overline{S}$. Now, define the function

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

We show that v is a valuation, then the proof is complete as $v(s) = 1$ for all $s \in S$. Since $\overline{S}$ is consistent, $\bot \notin \overline{S}$, so $v(\bot) = 0$.

Suppose $v(p) = 1, v(q) = 0$. Then $p \in \overline{S}$ and $q \notin \overline{S}$, and we want to show $(p \Rightarrow q) \notin \overline{S}$. If this were not the case, we would have $(p \Rightarrow q) \in \overline{S}$ and $p \in \overline{S}$, so $q \in \overline{S}$ as $\overline{S}$ is deductively closed.

Now suppose $v(q) = 1$, so $q \in \overline{S}$, and we need to show $(p \Rightarrow q) \in \overline{S}$. Then $\overline{S} \vdash q$, and by axiom 1, $\overline{S} \vdash q \Rightarrow (p \Rightarrow q)$. Therefore, as $\overline{S}$ is deductively closed, $(p \Rightarrow q) \in \overline{S}$.

Finally, suppose $v(p) = 0$, so $p \notin \overline{S}$, and we want to show $(p \Rightarrow q) \in \overline{S}$. We know that $\neg p \in \overline{S}$, so it suffices to show that $p \Rightarrow \bot \vdash p \Rightarrow q$. By the deduction theorem, this is equivalent to proving $\{p, p \Rightarrow \bot\} \vdash q$, or equivalently, $\bot \vdash q$. But by axiom 1, $\bot \Rightarrow (\neg q \Rightarrow \bot)$ where $(\neg q \Rightarrow \bot) = \neg\neg q$, so the proof is complete by axiom 3. □

Remark. We used the fact that P was a countable set in order to show that L was countable. The result does in fact hold if P is uncountable, but requires more tools to prove. Some sources call this theorem the 'completeness theorem'.

Corollary (adequacy). Let $S \subseteq L$ and let $t \in L$, such that $S \vDash t$. Then $S \vdash t$.

Proof. Follows from the remarks before the model existence lemma. □

1.7 Completeness

Theorem (completeness theorem for propositional logic). Let $S \subseteq L$ and $t \in L$. Then $S \vDash t$ if and only if $S \vdash t$.

Proof. Follows from soundness and adequacy. □

Theorem (compactness theorem)**.** Let $S \subseteq L$ and $t \in L$ with $S \vDash t$. Then there exists a finite subset $S' \subseteq S$ such that $S' \vDash t$.

Proof. Trivial after applying the completeness theorem, since proofs depend on only finitely many hypotheses in S. □

Corollary (compactness theorem, equivalent form)**.** Let $S \subseteq L$. Then if every finite subset $S' \subseteq S$ has a model, then S has a model.

Proof. Let $t = \bot$ in the compactness theorem. Then, if $S \vDash \bot$, some finite $S' \subseteq S$ has $S' \vDash \bot$. But this is not true by assumption, so there is a model for S. □

Remark. This corollary is equivalent to the more general compactness theorem, since the assertion that $S \vDash t$ is equivalent to the statement that $S \cup \{\neg t\}$ has no model, and $S' \vDash t$ is equivalent to the statement that $S' \cup \{\neg t\}$ has no model.

Theorem (decidability theorem)**.** Let $S \subseteq L$ and $t \in L$. Then, there is an algorithm to decide (in finite time) if $S \vdash t$.

Proof. Trivial after replacing $\vdash$ with $\vDash$, by drawing the relevant truth tables. □

2 Well-orderings

2.1 Definition

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

- (irreflexivity) for all $x \in X$, $x \not< x$;
- (transitivity) for all $x, y, z \in X$, $x < y$ and $y < z$ implies $x < z$;
- (trichotomy) for all $x, y \in X$, either $x < y$, $y < x$, or $x = y$.

We use the obvious notation $x > y$ to denote $y < x$. In terms of the $\leq$ relation, we can equivalently write the axioms of a total order as

- (reflexivity) for all $x \in X$, $x \leq x$;
- (transitivity) for all $x, y, z \in X$, $x \leq y$ and $y \leq z$ implies $x \leq z$;
- (antisymmetry) for all $x, y \in X$, if $x \leq y$ and $y \leq x$ then $x = y$.
- (trichotomy, or totality) for all $x, y \in X$, either $x \leq y$ or $y \leq x$.

Example. (i) $(\mathbb{N}, \leq)$ is a total order.

(ii) $(\mathbb{Q}, \leq)$ is a total order.

(iii) $(\mathbb{R}, \leq)$ is a total order.

(iv) $(\mathbb{N}^+, |)$ is not a total order, where $|$ is the divides relation, since 2 and 3 are not related.

(v) $(\mathcal{P}(S), \subseteq)$ is not a total order if $|S| > 1$, since it fails trichotomy.

Definition. A total order $(X, <)$ is a *well-ordering* if every nonempty subset $S \subseteq X$ has a least element.

$$\forall S \subseteq X,\ S \neq \varnothing \implies \exists x \in S,\ \forall y \in S,\ x \leq y$$

Example. (i) $(\mathbb{N}, <)$ is a well-ordering.

(ii) $(\mathbb{Z}, <)$ is not a well-ordering, since $\mathbb{Z}$ has no least element.

(iii) $(\mathbb{Q}, <)$ is not a well-ordering.

(iv) $(\mathbb{R}, <)$ is not a well-ordering.

(v) $[0, 1] \subset \mathbb{R}$ with the usual order is not a well-ordering, since $(0, 1]$ has no least element.

(vi) $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\} \subset \mathbb{R}$ with the usual order is a well-ordering.

(vii) $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\} \cup \{1\}$ with the usual order is also a well-ordering.

(viii) $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\} \cup \{2\}$ with the usual order is another example.

(ix) $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\} \cup \left\{1 + \frac{1}{2}, 1 + \frac{2}{3}, 1 + \frac{3}{4}, \dots\right\}$ is another example.

Remark. Let $(X, <)$ be a total order. $(X, <)$ is a well-ordering if and only if there is no infinite decreasing sequence $x_1 > x_2 > \dots$. Indeed, if $(X, <)$ is a well-ordering, then the set $\{x_1, x_2, \dots\}$ has no minimal element, contradicting the assumption. Conversely, if $S \subseteq X$ has no minimal element, then we can construct an infinite decreasing sequence by arbitrarily choosing points $x_1 > x_2 > \dots$ in S, which exists as S has no minimal element.

Definition. Total orders X, Y are *isomorphic* if there is a bijection f between X and Y that preserves $<$: $x < y$ if and only if $f(x) < f(y)$.

Examples (i) and (vi) are isomorphic, and (vii) and (viii) are isomorphic. Examples (i) and (vii) are not isomorphic, since example (vii) has a greatest element and (i) does not.

Proposition (proof by induction)**.** Let X be a well-ordered set, and let $S \subseteq X$ such that

$$\forall x \in S,\ (\forall y < x,\ y \in S) \implies x \in S$$

Then $S = X$.

Remark. Equivalently, if $p(x)$ is a property such that if $p(y)$ is true for all $y < x$ then $p(x)$, then $p(x)$ holds for all x.

Proof. Suppose $S \neq X$. Then $X \setminus S$ is nonempty, and therefore has a least element x. But all elements $y < x$ lie in S, and so by the property of S, we must have $x \in S$, contradicting the assumption. □

Proposition. Let X, Y be isomorphic well-orderings. Then there is exactly one isomorphism between X and Y.

Note that this does not hold for general total orderings, such as $\mathbb{Q}$ to itself or $[0,1]$ to itself.

Proof. Let $f, g : X \to Y$ be isomorphisms. We show that $f(x) = g(x)$ for all x by induction on x. Suppose $f(y) = g(y)$ for all $y < x$. We must have that $f(x) = a$, where a is the least element of $Y \setminus \{f(y) \mid y < x\}$. Indeed, if not, we have $f(x') = a$ for some $x' > x$ by bijectivity, contradicting the order-preserving property. Note that the set $Y \setminus \{f(x) \mid y < x\}$ is nonempty as it contains $f(x)$. So $f(x) = a = g(x)$, as required. □

2.2 Initial segments

Definition. A subset I of a totally ordered set X is an *initial segment* if $x \in I$ implies $y \in I$ for all $y < x$.

Example. In any total ordering X and element $x \in X$, the set $\{y \mid y < x\}$ is an initial segment. Not every initial segment is of this form, for instance $\{x \mid x \leq 3\}$ in $\mathbb{R}$, or $\left\{x \mid x > 0, x^2 < 2\right\}$ in $\mathbb{Q}$.

In a well-ordering, every proper initial segment $I \neq X$ is of this form. Indeed, $I = \{y \mid y < x\}$ where x is the least element of $X \setminus I$: $y \in I$ implies $y < x$, otherwise $y = x$ or $x < y$, giving the contradiction $x \in I$; and conversely, $y < x$ implies $y \in I$, otherwise y is a smaller element of $X \setminus I$.

Theorem (definition by recursion). Let X be a well-ordering and Y be any set. Let $G : \mathcal{P}(X \times Y) \to Y$ be a rule that assigns a point in Y given a definition of the function 'so far', represented as a set of ordered pairs. Then there exists a function $f : X \to Y$ such that $f(x) = G\left(f|_{I_x}\right)$, and such a function is unique.

Remark. In defining $f(x)$, we may use the value of $f(y)$ for all $y < x$.

Proof. We say that h is an *attempt* to mean that $h : I \to Y$ where I is some initial segment of X, and for all $x \in I$ we have that $h(x) = G\left(h|_{I_x}\right)$. Note that if h, h' are attempts both defined at x, then $h(x) = h'(x)$ by induction on x.

Also, for all x, there exists an attempt defined at x, by induction on x. Indeed, by induction we can assume there exists an attempt h_y defined at y for all $y < x$, and then we can define h to be the union of the h_y. This is an attempt with domain I_x, so the attempt $h' = h \cup \{(x, G(h))\}$ is an attempt defined at x. Therefore, there is an attempt defined at each x, so we can define the function $f : X \to Y$ by setting $f(x)$ to be the value of $h(x)$ where h is some attempt defined at x.

For uniqueness, we apply induction on x. If f, f' agree below x, then they must agree at x since $f(x) = G\left(f|_{I_x}\right) = G\left(f'|_{I_x}\right) = f'(x)$. □

Proposition (subset collapse). Any subset Y of a well-ordering X is isomorphic to a unique initial segment of X.

This is not true for general total orderings, such as $\{1, 2, 3\} \subset \mathbb{Z}$, or $\mathbb{Q}$ in $\mathbb{R}$.

Proof. If f is some such isomorphism, we must have that $f(x)$ is the least element of X not of the form $f(y)$ for $y < x$. We define f in this way by recursion, and this is an isomorphism as required. Note that this is always well-defined as $f(y) \leq y$, so there is always some element of X (namely, x) not of the form $f(y)$ for $y < x$. Uniqueness follows by induction. □

Remark. X itself cannot be isomorphic to a proper initial segment by uniqueness as it is isomorphic to itself.

2.3 Relating well-orderings

Definition. For well-orderings X, Y, we will write $X \leq Y$ if X is isomorphic to an initial segment of Y.

$X \leq Y$ if and only if X is isomorphic to some subset of Y.

Example. $\mathbb{N} \leq \left\{\frac{1}{2}, \frac{2}{3}, \dots\right\}$.

Proposition. Let X, Y be well-orderings. Then either $X \leq Y$ or $Y \leq X$.

Proof. By recursion we define the function $f : X \to Y$ by letting $f(x)$ be the least element of Y not of the form $f(y)$ for all $y < x$. If a least element of this form always exists, this is a well-defined isomorphism from X to an initial segment of Y as required. Suppose that $Y \setminus \{f(y) \mid y < x\}$ is empty, so $\{f(y) \mid y < x\} = Y$. Then Y is isomorphic to $I_x \subseteq X$, so $Y \leq X$. □

Proposition. Let X, Y be well-orderings, and suppose $X \leq Y$ and $Y \leq X$. Then X is isomorphic to Y.

Proof. Let $f : X \to Y$ and $g : Y \to X$ be isomorphisms to initial segments. Then $g \circ f$ is an isomorphism from X to some initial segment of X, as an initial segment of an initial segment is an initial segment. So by uniqueness, $g \circ f$ is the identity map on X. Similarly, $f \circ g$ is the identity on Y, so f and g are inverses. □

2.4 Constructing larger well-orderings

Definition. For well-orderings X, Y, we write $X < Y$ if $X \leq Y$ and X is not isomorphic to Y.

Equivalently, $X < Y$ if X is isomorphic to a proper initial segment of Y.

Let X be a well-ordering, and let $x \notin X$. Construct the well-ordering on $X \cup \{x\}$ by setting $y < x$ for all $y \in X$. This well-ordering is strictly greater than X, since X is isomorphic to a proper initial segment. This is called the *successor* of X, written X^+.

For well-orderings $(X, <_X), (Y, <_Y)$, we say that $(Y, <_Y)$ *extends* $(X, <_X)$ if $X \subseteq Y$, $<_Y |_X = <_X$, and X is an initial segment of Y. We say that well-orderings X_i for $i \in I$ are *nested* if for all $i, j \in I$, either X_i extends X_j or X_j extends X_i.

Proposition. Let X_i for $i \in I$ be a nested set of well-orderings. Then, there exists a well-ordering X such that $X_i \leq X$ for all $i \in I$.

Proof. Let $X = \bigcup_{i \in I} X_i$ with ordering $<_X = \bigcup_{i \in I} <_i$. Then, as the X_i are nested, each X_i is an initial segment of X. We show that this is a well-ordering. Let $S \subseteq X$ be a nonempty set. Then $S \cap X_i \neq \varnothing$ for some $i \in I$. Let x be the least element of $S \cap X_i$. Thus, x is the least element of S, as X_i is an initial segment of X. □

Remark. The proposition holds without the nestedness assumption.

2.5 Ordinals

Definition. An *ordinal* is a well-ordered set, where we regard two ordinals as equal if they are isomorphic.

Remark. We cannot construct ordinals as equivalence classes of well-orderings, due to Russell's paradox. Later, we will see a different construction that deals with this problem.

Definition. Let X be a well-ordering corresponding to an ordinal α. Then, we say that X has *order type* α.

The order type of the unique well-ordering on a collection of $k \in \mathbb{N}$ points is named k. The order type of $(\mathbb{N}, <)$ is named ω.

Example. In the reals, the set $\{-2, 3, -\pi, 5\}$ has order type 4. The set $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\}$ has order type ω.

We will write $\alpha \leq \beta$ if $X \leq Y$ where X has order type α and Y has order type β. This does not depend on the choice of representative X or Y. We define $\alpha < \beta$ and α^+ in a similar way. Note that $\alpha \leq \beta, \beta \leq \alpha$ implies $\alpha = \beta$. Therefore, ordinals are totally ordered.

Proposition. Let α be an ordinal. Then the set of ordinals less than α form a well-ordered set of order type α.

Proof. Let X be a well-ordering with order type α. Then, the well-orderings less than X are precisely the proper initial segments of X, up to isomorphism. The initial segments of X are precisely the sets $I_x = \{y \in X \mid y < x\}$ for $x \in X$. But these are order isomorphic to X itself by mapping $I_x \mapsto x$. □

We define $I_\alpha = \{\beta < \alpha\}$, which is a well-ordered set of order type α. This is often a convenient representative to choose for an ordinal.

Proposition. Every nonempty set S of ordinals has a least element.

Proof. Let $\alpha \in S$. Suppose α is not the least element of S. Then $S \cap I_\alpha$ is nonempty. But I_α is well-ordered, so $S \cap I_\alpha$ has a minimal element as required. □

Theorem (Burali-Forti paradox). The ordinals do not form a set.

Proof. Suppose X is the set of all ordinals. Then X is a well-ordered set, so it has an order type α. Then X is isomorphic to I_α, which is a proper initial segment of X. $\square$

Remark. Given a set $S = \{\alpha_i : i \in I\}$ of ordinals, there exists an upper bound α for S, so $\alpha_i \leq \alpha$ for all $i \in I$, by considering the nested family of well-orderings I_{α_i}. Hence, by the previous proposition, there exists a least upper bound, as I_α is a set. We write $\alpha = \sup S$.

Example. $\sup\{2, 4, 6, \dots\} = \omega$.

Remark. If we represent ordinals by sets of smaller ordinals, $\sup S = \bigcup_{\alpha \in S} \alpha$.

2.6 Some ordinals

$$0, 1, 2, 3, \dots, \omega$$

Write $\alpha + 1$ for the successor α^+ of α.

$$\omega + 1, \omega + 2, \omega + 3, \dots, \omega + \omega = \omega \cdot 2$$

where $\omega + \omega = \omega \cdot 2$ is defined by $\sup\{\omega, \omega + 1, \omega + 2, \dots\}$.

$$\omega \cdot 2 + 1, \omega \cdot 2 + 2, \dots, \omega \cdot 3, \omega \cdot 4, \omega \cdot 5, \dots, \omega \cdot \omega = \omega^2$$

where we define $\omega \cdot \omega = \sup\{\omega \cdot 2, \omega \cdot 3, \dots\}$.

$$\omega^2 + 1, \omega^2 + 2, \dots, \omega^2 + \omega, \dots, \omega^2 + \omega \cdot 2, \dots, \omega^2 + \omega^2 = \omega^2 \cdot 2$$

Continue in the same way.

$$\omega^2 \cdot 3, \omega^2 \cdot 4, \dots, \omega^3$$

where $\omega^3 = \sup\left\{\omega^2 \cdot 2, \omega^2 \cdot 3, \dots\right\}$.

$$\omega^3 + \omega^2 \cdot 7 + \omega \cdot 4 + 13, \dots, \omega^4, \omega^5, \dots, \omega^\omega$$

where $\omega^\omega = \sup\left\{\omega, \omega^2, \omega^3, \dots\right\}$.

$$\omega^\omega \cdot 2, \omega^\omega \cdot 3, \dots, \omega^\omega \cdot \omega = \omega^{\omega+1}$$

$$\omega^{\omega+2}, \dots, \omega^{\omega \cdot 2}, \omega^{\omega \cdot 3}, \dots, \omega^{\omega^2}, \dots, \omega^{\omega^3}, \dots, \omega^{\omega^\omega}, \dots, \omega^{\omega^{\omega^\omega}}, \dots, \omega^{\omega^{\omega^{\cdots}}} = \varepsilon_0$$

where $\varepsilon_0 = \sup\left\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\right\}$.

$$\varepsilon_0 + 1, \varepsilon_0 + \omega, \varepsilon_0 + \varepsilon_0 = \varepsilon_0 \cdot 2, \dots, \varepsilon_0^2, \varepsilon_0^3, \dots, \varepsilon_0^{\varepsilon_0}$$

where $\varepsilon_0^{\varepsilon_0} = \sup\left\{\varepsilon_0^\omega, \varepsilon_0^{\omega^\omega}, \dots\right\}$.

$$\varepsilon_0^{\varepsilon_0^{\varepsilon_0^{\cdots}}} = \varepsilon_1$$

All of these ordinals are countable, as each operation only takes a countable union of countable sets.

2.7 Uncountable ordinals

Theorem. There exists an uncountable ordinal.

Remark. The reals cannot be explicitly well-ordered.

Proof. Let $A \subseteq \mathcal{P}(\omega \times \omega)$ be the set of well-orderings of subsets of $\mathbb{N}$. Let B be the set of order types of A. Then B is the set of all countable ordinals. Let $\omega_1 = \sup B$. ω_1 is uncountable, and in particular, the least uncountable ordinal. Indeed, if it were countable, it would be the greatest element of B, but $\omega_1 + 1$ would also lie in B. □

Remark. Without introducing A, it would be difficult to show that B was in fact a set.

Remark. Another ending to the proof above is as follows. B cannot be the set of all ordinals, since the ordinals do not form a set by the Burali-Forti paradox, so there exists an uncountable ordinal. In particular, there exists a least uncountable ordinal.

The ordinal ω_1 has a number of remarkable properties.

(i) ω_1 is uncountable, but $\{\beta \mid \beta < \alpha\}$ is countable for all $\alpha < \omega_1$.

(ii) There exists no sequence $\alpha_1, \alpha_2, \dots$ in I_{ω_1} with supremum ω_1, as it is bounded by $\sup\{\alpha_1, \alpha_2, \dots\}$, which is a countable ordinal.

Theorem (Hartogs' lemma)**.** For every set X, there exists an ordinal γ that does not inject into X.

Proof. Use the argument above from the existence of an uncountable ordinal. □

We write $\gamma(X)$ for the least ordinal that does not inject into X. For example $\gamma(\omega) = \omega_1$.

2.8 Successors and limits

Definition. We say that an ordinal α is a *successor* if there exists β such that $\alpha = \beta^+$. Otherwise, α is a *limit*.

Equivalently, an ordinal is a successor if and only if it has a greatest element. An ordinal α is a limit if and only if it has no greatest element, or equivalently, for all $\beta < \alpha$, there exists $\gamma < \alpha$ with $\gamma > \beta$, giving $\alpha = \sup\{\beta \mid \beta < \alpha\}$.

Example. 5 is a successor. $\omega + 2 = (\omega^+)^+$ is a successor. ω is a limit as it has no greatest element. 0 is a limit.

2.9 Ordinal arithmetic

Let α, β be ordinals. We define $\alpha + \beta$ by induction on β, by

- $\alpha + 0 = \alpha$;
- $\alpha + \beta^+ = (\alpha + \beta)^+$;
- $\alpha + \lambda = \sup\{\alpha + \gamma \mid \gamma < \lambda\}$ for a nonzero limit ordinal.

Example. $\omega + 1 = \omega + 0^+ = (\omega + 0)^+ = \omega^+$. $\omega + 2 = \omega + 1^+ = (\omega + 1)^+ = (\omega^+)^+$. $1 + \omega = \sup\{1 + \gamma \mid \gamma < \omega\} = \omega$. Therefore, addition is noncommutative.

Remark. As the ordinals do not form a set, we must technically define addition $\alpha + \gamma$ by induction on the set $\{\gamma \mid \gamma \leq \beta\}$. The choice of β does not change the definition of $\alpha + \gamma$ as defined for $\gamma \leq \beta$.

Proposition. Ordinal addition is associative.

Proof. Let α, β, γ be ordinals. We use induction on γ. Suppose $\alpha + (\beta + \delta) = (\alpha + \beta) + \delta$ for all $\delta < \gamma$.

First, suppose $\gamma = 0$. $\alpha + (\beta + 0) = \alpha + \beta = (\alpha + \beta) = 0$, as required. Now consider γ^+.

$$\alpha + (\beta + \gamma^+) = \alpha + (\beta + \gamma)^+ = (\alpha + (\beta + \gamma))^+ = ((\alpha + \beta) + \gamma)^+ = (\alpha + \beta) + \gamma^+$$

Finally, consider λ a nonzero limit.

$$(\alpha + \beta) + \lambda = \sup\{(\alpha + \beta) + \gamma \mid \gamma < \lambda\} = \sup\{\alpha + (\beta + \gamma) \mid \gamma < \lambda\}$$

We claim that $\beta + \lambda$ is a limit. Indeed, $\beta + \lambda = \sup\{\beta + \gamma \mid \gamma < \lambda\}$, but for every $\gamma < \lambda$ there exists $\gamma' < \lambda$ with $\gamma < \gamma'$ as λ is a limit, so $\beta + \gamma < \beta + \gamma'$. Thus, there is no greatest element in the set $\{\beta + \gamma \mid \gamma < \lambda\}$, so $\beta + \lambda$ is a limit.

Now, $\alpha + (\beta + \lambda) = \sup\{\alpha + \delta \mid \delta < \beta + \lambda\}$. So it suffices to show that

$$\sup\{\alpha + (\beta + \gamma) \mid \gamma < \lambda\} = \sup\{\alpha + \delta \mid \delta < \beta + \lambda\}$$

Certainly

$$\{\alpha + (\beta + \gamma) \mid \gamma < \lambda\} \subseteq \{\alpha + \delta \mid \delta < \beta + \lambda\}$$

as $\gamma < \lambda$ implies $\beta + \gamma < \beta + \lambda$. Further, for any $\delta < \beta + \lambda$, $\delta \leq \beta + \gamma$ for some $\gamma < \lambda$ by definition of $\beta + \lambda$. Therefore, $\alpha + \delta \leq \alpha + (\beta + \gamma)$, so each element of $\{\alpha + \delta \mid \delta < \beta + \lambda\}$ is at most some element of $\{\alpha + (\beta + \gamma) \mid \gamma < \lambda\}$. So the two suprema agree. □

Remark. We used the facts

(i) $\beta \leq \gamma \implies \alpha + \beta \leq \alpha + \gamma$, which is trivial by induction on γ;

(ii) $\beta < \gamma \implies \alpha + \beta < \alpha + \gamma$, as $\beta^+ \leq \gamma$ so $\alpha + \beta^+ \leq \alpha + \gamma$ by (i).

However, $1 < 2$ but $1 + \omega \not< 2 + \omega$.

The above is the *inductive* definition of addition; there is also a *synthetic* definition of addition. We can define $\alpha + \beta$ to be the order type of $\alpha \sqcup \beta$, where every element of α is taken to be less than every element of β.

For instance, $\omega + 1$ is the order type of ω with a point afterwards, and $1 + \omega$ is the order type of a point followed by ω, which is clearly isomorphic to ω. Associativity is clear, as $(\alpha + \beta) + \gamma$ and $\alpha + (\beta + \gamma)$ are the order type of $\alpha \sqcup \beta \sqcup \gamma$.

Proposition. The inductive and synthetic definitions of addition coincide.

Proof. We write $+'$ for synthetic addition, and aim to show $\alpha + \beta = \alpha +' \beta$. We perform induction on β.

For $\beta = 0$, $\alpha + 0 = \alpha$ and $\alpha +' 0 = \alpha$. For successors, $\alpha + \beta^+ = (\alpha + \beta)^+ = (\alpha +' \beta)^+$, which is the order type of $\alpha \sqcup \beta \sqcup \{\star\}$, which is equal to $\alpha +' \beta^+$.

Let λ be a nonzero limit. We have $\alpha + \lambda = \sup\{\alpha + \gamma \mid \gamma < \lambda\}$. But $\alpha + \gamma = \alpha +' \gamma$ for $\gamma < \lambda$, so $\alpha + \lambda = \sup\{\alpha +' \gamma \mid \gamma < \lambda\}$. As the set $\{\alpha +' \gamma \mid \gamma < \lambda\}$ is nested, it is equal to its union, which is $\alpha +' \lambda$. □

Synthetic definitions can be easier to work with if such definitions exist. However, there are many definitions that can only easily be represented inductively, and not synthetically.

We define multiplication inductively by

- $\alpha 0 = 0$;
- $\alpha\beta^+ = \alpha\beta + \alpha$;
- $\alpha\lambda = \sup\{\alpha\gamma \mid \gamma < \lambda\}$ for λ a nonzero limit.

Example. $\omega 2 = \omega 1 + \omega = \omega 0 + \omega + \omega = \omega + \omega$. Similarly, $\omega 3 = \omega + \omega + \omega$. $\omega\omega = \sup\{0, \omega 1, \omega 2, \dots\} = \{0, \omega, \omega + \omega, \dots\}$. Note that $2\omega = \sup\{0, 2, 4, \dots\} = \omega$. Multiplication is noncommutative. One can show in a similar way that multiplication is associative.

We can produce a synthetic definition of multiplication, which can be shown to coincide with the inductive definition. We define $\alpha\beta$ to be the order type of the Cartesian product $\alpha \times \beta$ where we say $(\gamma, \delta) < (\gamma', \delta')$ if $\delta < \delta'$ or $\delta = \delta'$ and $\gamma < \gamma'$. For instance, $\omega 2$ is the order type of two infinite sequences, and 2ω is the order type of a sequence of pairs.

Similar definitions can be created for exponentiation, towers, and so on. For instance, α^β can be defined by

- $\alpha^0 = 1$;
- $\alpha^{(\beta^+)} = \alpha^\beta\alpha$;
- $\alpha^\lambda = \sup\{\alpha^\gamma \mid \gamma < \lambda\}$ for λ a nonzero limit.

For example, $\omega^2 = \omega^1\omega = \omega^0\omega\omega = \omega\omega$. Further, $2^\omega = \sup\{2^0, 2^1, \dots\} = \omega$, which is countable.

3 Posets

3.1 Definitions

Definition. A *partially ordered set* or *poset* is a pair $(X, \leq)$ where X is a set, and $\leq$ is a relation on X such that

- (reflexivity) for all $x \in X$, $x \leq x$;
- (transitivity) for all $x, y, z \in X$, $x \leq y$ and $y \leq z$ implies $x \leq z$;
- (antisymmetry) for all $x, y \in X$, $x \leq y$ and $y \leq x$ implies $x = y$.

We write $x < y$ for $x \leq y$ and $x \neq y$. Alternatively, a post is a pair $(X, <)$ where X is a set, and $<$ is a relation on X such that

- (irreflexivity) for all $x \in X$, $x \not< x$;
- (transitivity) for all $x, y, z \in X$, $x < y$ and $y < z$ implies $x < z$.

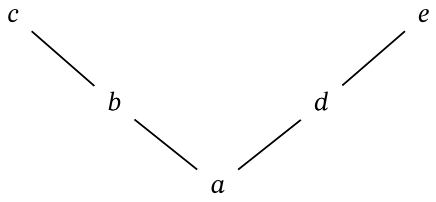
Example. (i) Any total order is a poset.

(ii) $\mathbb{N}^+$ with the divides relation is a poset.

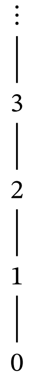
(iii) $(\mathcal{P}(S), \subseteq)$ is a poset.

(iv) $(X, \subseteq)$ is a poset where $X \subseteq \mathcal{P}(S)$, such as the set of vector subspaces of a vector space.

(v) The following diagram is also a poset, where the lines from a upwards to b denote relations $a \leq b$.

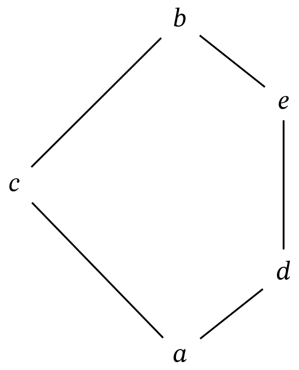


This is called a *Hasse diagram*. An upwards line from x to y is drawn if *y covers x*, so $y > x$ and no z has $y > z > x$. The natural numbers can be represented as a Hasse diagram.

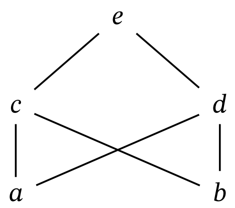


The rationals cannot, since no element covers another.

(vi) There is no notion of 'height' in a poset, illustrated by the following diagram.



(vii)



Definition. A subset S of a poset X is a *chain* if it is totally ordered.

Example. The powers of 2 in $(\mathbb{N}^+, |)$ is a chain.

Definition. A subset S of a poset X is an *antichain* if no two distinct elements are related.

Example. The set of primes in $(\mathbb{N}^+, |)$ is an antichain.

Definition. For $S \subseteq X$, an *upper bound* for S is an $x \in X$ such that $x \geq y$ for all $y \in S$. A *least upper bound* is an upper bound $x \in X$ for S such that for all upper bounds $y \in X$ for S, $x \leq y$.

Example. If $S = \left\{x \mid x < \sqrt{2}\right\} \subset \mathbb{R}$, 7 is an upper bound, and $\sqrt{2}$ is a least upper bound. We write $\sqrt{2} = \sup S = \bigvee S$ for the least upper bound or *join* of S.

In $\mathbb{Q}$, the set $\left\{x \mid x^2 < 2\right\}$ has 7 as an upper bound but has no least upper bound.

In example (v), $\{a, b\}$ has upper bounds b and c, so the least upper bound is b. $\{b, d\}$ has no upper bound. In example (vii), $\{a, b\}$ has upper bounds c, d, e, so does not have a least upper bound.

Definition. A poset X is *complete* if every $S \subseteq X$ has a least upper bound.

Example. $\mathbb{R}$ is not complete, as $\mathbb{Z}$ has no upper bound. $[0, 1] \subseteq \mathbb{R}$ is complete. $(0, 1) \subseteq \mathbb{R}$ is not complete, as $(0, 1)$ has no upper bound.

Example. $X = \mathcal{P}(S)$ is always complete as a poset under inclusion, with $\sup\{A_i \mid i \in I\} = \bigcup_{i \in I} A_i$.

Note that every complete poset X has a greatest element $\sup X$. A complete poset also has a least element $\sup \varnothing$. In the case $X = \mathcal{P}(S)$, $\sup X = S$ and $\sup \varnothing = \varnothing$.

Definition. Let $f : X \to Y$ be a function where X, Y are posets. We say f is *order-preserving* if $x \leq y$ implies $f(x) \leq f(y)$.

Example. The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + 1$ is order-preserving. The function $f : [0, 1] \to [0, 1]$ defined by $x \mapsto \frac{x+1}{2}$ is order-preserving. The function $f : \mathcal{P}(S) \to \mathcal{P}(S)$ defined by $f(A) = A \cup \{i\}$ for some fixed $i \in S$ is order-preserving.

Not all order-preserving functions have a fixed point x such that $f(x) = x$, for example $f(x) = x + 1$ on $\mathbb{N}$.

Theorem (Knaster–Tarski fixed point theorem)**.** Let X be a complete poset. Then every order-preserving $f : X \to X$ has a fixed point.

Proof. Let $E = \{x \in X \mid x \leq f(x)\}$, and let $s = \sup E$. We show that s is a fixed point for f.

First, we show $s \leq f(s)$, so $s \in E$. It suffices to show $f(s)$ is an upper bound for E, then the result holds as s is the least such upper bound. If $x \in E$, we know $x \leq s$, so $f(x) \leq f(s)$ as f is order-preserving, as required.

Now, we show $f(s) \leq s$. It suffices to show $f(s) \in E$, as s is an upper bound for E. Since $s \leq f(s)$, we have $f(s) \leq f(f(s))$, but this is precisely the fact that $f(s) \in E$. □

Corollary (Schröder–Bernstein theorem)**.** Let $f : A \to B$ and $g : B \to A$ be injections. Then there is a bijection $A \to B$.

Proof. We seek partitions $A = P \sqcup Q$, $B = R \sqcup S$ such that $f(P) = R$ and $g(S) = Q$; then we define h to equal to f on P and g^{-1} on Q. Thus, we need a set P that is a fixed point of $\theta : \mathcal{P}(A) \to \mathcal{P}(A)$ given by $P \mapsto A \setminus g(B \setminus f(P))$. But θ is order-preserving and $\mathcal{P}(A)$ is a complete poset. So P exists by the Knaster–Tarski fixed point theorem. □

3.2 Zorn's lemma

Definition. Let X be a poset. We say that $x \in X$ is *maximal* if there is no $y \in X$ with $y > x$.

Example. In $[0,1]$, 1 is maximal. In example (v), there are two maximal elements c and e.

Note that $(\mathbb{R}, \leq)$ and $(\mathbb{N}, |)$ have no maximal elements, and they both have a chain with no upper bound, such as $\mathbb{N} \subset \mathbb{R}$, and powers of two.

Theorem (Zorn's lemma)**.** Let X be a poset in which every chain has an upper bound. Then X has a maximal element.

The empty chain must have an upper bound in X, so X must be nonempty to apply Zorn's lemma. Zorn's lemma can be equivalently be stated as the following.

Theorem. Let X be a nonempty poset in which every nonempty chain has an upper bound. Then X has a maximal element.

One can view Zorn's lemma as a fixed point theorem on a function $f : X \to X$ with the property that $x \leq f(x)$.

Proof. Suppose that X has no maximal element. Then for each $x \in X$, we have $x' \in X$ and $x' > x$. For each chain C, we have an upper bound $u(C)$. Let $x \in X$ be any element, and define x_α for each $\alpha < \gamma(X)$ by recursion.

- $x_0 = x$;

- $x_{\alpha+1} = x'_\alpha$;
- $x_\lambda = u\{x_\beta \mid \beta < \lambda\}$ for λ a nonzero limit.

Note that $\{x_\beta \mid \beta < \lambda\}$ forms a chain, so it has an upper bound as required. Then, we have an injection from $\gamma(X)$ into X, contradicting the definition of $\gamma(X)$. □

Remark. Although this proof was short, it relied on the infrastructure of well-orderings, recursion, ordinals, and Hartogs' lemma.

We show that every vector space has a basis. Recall that a basis is a linearly independent spanning set; no nontrivial finite linear combination of basis elements is zero, and each element of the vector space is a finite linear combination of the basis elements. For instance, the space of real polynomials has basis $1, X, X^2, \dots$. The space of real sequences has a linearly independent set $(1, 0, 0, \dots), (0, 1, 0, \dots), \dots$, but this is not a basis as the sequence $(1, 1, 1, \dots)$ cannot be constructed as a finite linear combination of these vectors. In fact, there is no countable basis for this space, and no explicitly definable basis in general. $\mathbb{R}$ is a vector space over $\mathbb{Q}$. There is clearly no countable basis, and in fact no explicit basis. A basis in this case is called a *Hamel basis*.

Theorem. Every vector space V has a basis.

Proof. Let X be the set of all linearly independent subsets of V, ordered by inclusion. We seek a maximal element of X; this is clearly a basis, as any vector not in its span could be added to the set to increase the set of basis vectors. X is nonempty as $\varnothing \in X$.

We apply Zorn's lemma. Let $(A_i)_{i\in I}$ be a chain in X. We show that its union $A = \bigcup_{i\in I} A_i$ is a linearly independent set, and therefore lies in X and is an upper bound. Suppose $x_1, \dots, x_n \in A$ are linearly dependent. Then $x_1 \in A_{i_1}, \dots, x_n \in A_{i_n}$, so all x_i lie in some A_k as the A_i are a chain. But A_k is linearly independent, which is a contradiction. □

Remark. The only time that linear algebra was used was to show that the maximal element obtained by Zorn's lemma performs the required task; this is usual for proofs in this style.

We can now prove the completeness theorem for propositional logic with no restrictions on the size of the set of primitive propositions.

Theorem. Let $S \subseteq L = L(P)$ be consistent. Then S has a model.

Proof. We will extend S to a consistent set $\overline{S}$ such that for all $t \in L$, either $t \in S$ or $\neg t \in \overline{S}$; we then complete the proof by defining a valuation v such that $v(t) = 1$ if $t \in \overline{S}$.

Let $X = \{T \supseteq S \mid T \text{ consistent}\}$ be the poset of consistent extensions of S, ordered by inclusion. We seek a maximal element of X. Then, if $\overline{S}$ is maximal and $t \notin \overline{S}$, then $\overline{S} \cup \{t\} \vdash \bot$ by maximality, so $\overline{S} \vdash \neg t$ by the deduction theorem, giving $\neg t \in \overline{S}$ again by maximality.

Note that $X \neq \varnothing$ as $S \in X$. Given a nonempty chain $(T_i)_{i\in I}$, let $T = \bigcup_{i\in I} T_i$. We have $T \supseteq T_i$ for all i and $T \supseteq S$ as the chain is nonempty, so it suffices to show T is consistent. Indeed, suppose $T \vdash \bot$. Then there exists a subset $\{t_1, \dots, t_n\} \in T$ with $\{t_1, \dots, t_n\} \vdash \bot$ as proofs are finite. Now, $t_1 \in T_{i_1}, \dots, t_n \in T_{i_n}$ so all t_j are elements of T_{i_k} for some k. But T_{i_k} is consistent, so $\{t_1, \dots, t_n\} \nvdash \bot$, giving a contradiction. □

3.3 Well-ordering principle

Theorem. Every set has a well-ordering.

There exist sets with no definable well-ordering, such as $\mathbb{R}$.

Proof. Let S be a set, and let X be the set of pairs (A, R) such that $A \subseteq S$ and R is a well-ordering on A. We define the partial order on X by $(A, R) \leq (A', R')$ if (A', R') extends (A, R), so $R'|_A = A$ and A is an initial segment of A' for R'.

X is nonempty as the empty relation is a well-ordering of the empty set. Given a nonempty chain $(A_i, R_i)_{i \in I}$, there is an upper bound $\left(\bigcup_{i \in I} A_i, \bigcup_{i \in I} R_i\right)$, because the well-orderings are nested. By Zorn's lemma, there exists a maximal element $(A, R) \in X$.

Suppose $x \in S \setminus A$. Then we can construct the well-ordering on $A \cup \{x\}$ by defining $a < x$ for $a \in A$, contradicting maximality of A. Hence $A = S$, so R is a well-ordering on S. □

3.4 Zorn's lemma and the axiom of choice

In the proof of Zorn's lemma, for each $x \in S$ we chose an arbitrary $x' > x$. This requires potentially infinitely many arbitrary choices. Other proofs, such as that the countable union of countable sets is countable, also required infinitely many choices; in this example, we chose arbitrary enumerations of the countable sets $A_1, A_2, \dots$ at once.

Formally, this process of making infinitely many arbitrary choices is known as the *axiom of choice* AC: if we have a family of nonempty sets, one can choose an element from each one. More precisely, for any family of nonempty sets $(A_i)_{i \in I}$, there is a *choice function* $f : I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all i.

Unlike the other axioms of set theory, the function obtained from the axiom of choice is not uniquely defined. For instance, the axiom of union allows for the construction of $A \cup B$ given A and B, which can be fully described; but applying the axiom of choice to the family $\star \mapsto \{1, 2\}$ could give the choice function $\star \mapsto 1$ or $\star \mapsto 2$.

Use of the axiom of choice gives rise to nonconstructive proofs. In modern mathematics it is sometimes considered useful to note when the axiom of choice is being used. However, many proofs that do not even use the axiom of choice are nonconstructive, such as the proof of existence of transcendentals, or Hilbert's basis theorem that every ideal over $\mathbb{Q}[X_1, \dots, X_n]$ is finitely generated.

Although our proof of Zorn's lemma required the axiom of choice, it is not immediately clear that all such proofs require it. However, it can be shown that Zorn's lemma implies the axiom of choice in the presence of the other axioms of ZF set theory. Indeed, if $(A_i)_{i \in I}$ is a family of sets, we can well-order it using the well-ordering principle, and define the choice function by setting $f(i)$ to be the least element of A_i. Hence, Zorn's lemma, the axiom of choice, and the well-ordering principle are equivalent, given ZF.

AC can be proven trivially in ZF for the case $|I| = 1$, because a set being nonempty means precisely that there exists an element inside it. Clearly, AC holds for all finite index sets in ZF by induction on $|I|$. However, ZF does not prove the most general form of AC.

Zorn's lemma is a difficult lemma to prove from first principles because of its reliance on ordinals and Hartogs' lemma; the use of the axiom of choice does not contribute significantly to its difficulty. The construction and properties of the ordinals did not rely on the axiom of choice. The axiom of choice was only used twice in the section on well-orderings: the fact that in a set that is not well-ordered, there is an infinite decreasing sequence; and the fact that ω_1 is not a countable supremum.

4 Predicate logic

4.1 Languages

Recall that a *group* is a set A equipped with functions $m : A^2 \to A$ of arity 2, and $i : A^1 \to A$ of arity 1, and a constant $e \in A$ which can be viewed as a function $A^0 \to A$ of arity 0, such that a set of axioms hold. A *poset* is a set A equipped with a relation $(\leq) \subseteq A^2$ of arity 2, such that a set of axioms hold. Other algebraic structures can be described in the same way.

Let Ω and Π be disjoint sets of functions and relations, and $\alpha : \Omega \cup \Pi \to \mathbb{N}$ be an arity function. *Variables* are symbols of the form x_i for some $i \in \mathbb{N}$. *Terms* are defined inductively by

(i) each variable is a term;

(ii) if $f \in \Omega$ with $\alpha(f) = n$ and terms $t_1, \dots, t_n$, then $f\ t_1 \dots\ t_n$ is a term.

The *atomic formulae* are defined inductively by

(i) $\perp$ is an atomic formula;

(ii) for terms s, t, $(s = t)$ is an atomic formula;

(iii) if $\varphi \in \Pi$ with $\alpha(\varphi) = n$ and terms $t_1, \dots, t_n$, then $\varphi(t_1, \dots, t_n)$ is an atomic formula.

The *formulae* are defined inductively by

(i) each atomic formula is a formula;

(ii) if p and q are formulae then $(p \Rightarrow q)$ is a formula;

(iii) if p is a formula and x is a variable, then $(\forall x)p$ is a formula.

The *language* $L = L(\Omega, \Pi, \alpha)$ is the set of formulae.

Example. In the language of groups, $\Omega = \{m, i, e\}$ and $\Pi = \varnothing$ with $\alpha(m) = 2, \alpha(i) = 1, \alpha(e) = 0$. $m(x_1, x_2), m(x_1, i(x_2)), e, m(e, e)$ are examples of terms of the language. $e = m(\ell, e), m(x, y) = m(y, x)$ are atomic formulae.

Example. In the language of posets, $\Omega = \varnothing$ and $\Pi = \{\leq\}$ with $\alpha(\leq) = 2$. $x = y, x \leq y$ are atomic formulae. Technically, $x \leq y$ is written $\leq (x, y)$.

Example. In the language of groups, $(\forall x)(m(x, x) = e)$ is a formula. Another formula is $m(x, x) = e \Rightarrow (\exists y)(m(y, y) = x)$.

Remark. A formula is a certain finite string of symbols; it has no intrinsic semantics. We define $\neg p, p \wedge q, p \vee q$ in the usual way. We define $(\exists x)p$ to mean $\neg(\forall x)(\neg p)$.

A term is *closed* if it contains no variables. For example, $e, m(e, i(e))$ are closed in the language of groups, but $m(x, i(x))$ is not closed.

An occurrence of a variable x in a formula p is *bound* if it is inside the brackets of a $(\forall x)$ quantifier. Otherwise, we say the occurrence is *free*. In the formula $(\forall x)(m(x, x) = e)$, each occurrence of x is bound. In $m(x, x) = e \Rightarrow (\exists y)(m(y, y) = x)$, the occurrences of x are free and the occurrences of y

are bound. In the formula $m(x, x) = e \Rightarrow (\forall x)(\forall y)(m(x, y) = m(y, x))$, the occurrences of x on the left hand side are free, and the occurrences of x on the right hand side are bound.

A *sentence* is a formula with no free variables. For instance, $(\forall x)(m(x, x) = e)$ is a sentence, and $(\forall x)(m(x, x) \Rightarrow (\exists y)(m(y, y) = x))$ is a sentence. In the language of posets, $(\forall x)(\exists y)(x \geq y \wedge \neg(x = y))$ is a sentence.

For a formula p, term t, and variable x, the *substitution* $p[t/x]$ is obtained from p by replacing every free occurrence of x with t. For example,

$$p = (\exists y)(m(y, y) = x); \quad p[e/x] = (\exists y)(m(y, y) = e)$$

4.2 Semantic implication

Definition. Let $L = L(\Omega, \Pi, \alpha)$ be a language. An *L-structure* is

- a nonempty set A;
- for each $f \in \Omega$, a function $f_A : A^n \to A$ where $n = \alpha(f)$;
- for each $\varphi \in \Pi$, a subset $\varphi_A \subseteq A^n$ where $n = \alpha(\varphi)$.

Remark. We will see later why the restriction that A is nonempty is given here.

Example. In the language of groups, an L-structure is a nonempty set A with functions $m_A : A^2 \to A, i_A : A \to A, e_A \in A$. Such a structure may not be a group, as we have not placed any axioms on A.

Example. In the language of posets, an L-structure is a nonempty set A with a relation $(\leq_A) \subseteq A^2$.

We define the *interpretation* $p_A \in \{0, 1\}$ of a sentence p in an L-structure A as follows.

- The interpretation t_A of a closed term t in an L-structure A is defined inductively as $(f\, t_1 \dots t_n)_A = f_A(t_{1_A}, \dots, t_{n_A})$ for $f \in \Omega, \alpha(f) = n$, where $t_1, \dots, t_n$ are closed.
- The interpretation of an atomic sentence is defined inductively.
  - $\bot_A = 0$.
  - $(s = t)_A$ is 1 if $s_A = t_A$ and 0 if $s_A \neq t_A$.
  - $(\varphi(t_1, \dots, t_n))_A$ is 1 if $(t_{1_A}, \dots, t_{n_A}) \in \varphi_A$ and 0 otherwise, for $\varphi \in \Pi, \alpha(\varphi) = n$, where $t_1, \dots, t_n$ are closed.
- We now inductively define the interpretation of sentences, which is technically induction by length over all languages at once.
  - $(p \Rightarrow q)_A$ is 0 if $p_A = 1$ and $q_A = 0$, and 1 otherwise.
  - $((\forall x)p)_A$ is 1 if $p[\overline{a}/x]$ is 1 for all $a \in A$ and 0 otherwise, where we add a constant symbol $\overline{a}$ to L for a fixed $a \in A$ to form the language L', and we make A into an L'-structure by defining $\overline{a}_A = a$.

Remark. For a formula p with free variables, we can define p_A to be the subset of A^k where k is the number of free variables, defined such that $x \in p_A$ if and only if the substitution of x in p is evaluated to 1.

Definition. If $p_A = 1$, we say p *holds* in A, or p is *true* in A, or A is a *model* of p. A *theory* is a set of sentences, known as its *axioms*. We say that A is a *model* of a theory T if $p_A = 1$ for all $p \in T$. For a theory T and a sentence p, we say that $T \vDash p$, read T *entails* or *semantically implies* p, if every model of T is a model of p.

Example. Let L be the language of groups, and let

$$\begin{aligned} T = \{&(\forall x)(\forall y)(\forall z)(m(x, m(y, z)) = m(m(x, y), z)),\\ &(\forall x)(m(x, e) = x \wedge m(e, x) = x),\\ &(\forall x)(m(x, i(x)) = e \wedge m(i(x), x) = e)\}\end{aligned}$$

Then, an L-structure is a model of T if and only if it is a group. Note that this statement has two assertions; every L-structure that is a model of T is a group, and that every group can be turned into an L-structure that models T. We say that T *axiomatises* the theory of groups or the class of groups.

Example. Let L be the language of posets, and T be the poset axioms. Then T axiomatises the class of posets.

Example. Let L be the language of fields, so $\Omega = \{0, 1, +, \cdot, -\}$ with $\alpha(0) = \alpha(1) = 0, \alpha(+) = \alpha(\cdot) = 2, \alpha(-) = 1$. T is the usual field axioms, including the statement $(\forall x)(\neg(x = 0) \Rightarrow (\exists y)(x \cdot y = 1))$. Then T entails the statement that inverses are unique: $(\forall x)(\neg(x = 0) \Rightarrow (\forall y)(\forall z)(y \cdot x = 1 \wedge z \cdot x = 1 \Rightarrow y = z))$.

Example. Let L be the language of graphs, defined by $\Omega = \varnothing$ and $\Pi = \{a\}$ where $\alpha(a) = 2$ is the adjacency relation. Define $T = \{(\forall x)(\neg a(x, x)), (\forall x)(\forall y)(a(x, y) \Rightarrow a(y, x))\}$. Then T axiomatises the class of graphs.

4.3 Syntactic implication

We need to define (logical) axioms and deduction rules in order to construct proofs.

(i) $p \Rightarrow (q \Rightarrow p)$ for formulae p, q.

(ii) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ for formulae p, q, r.

(iii) $\neg\neg p \Rightarrow p$ for each formula p.

(iv) $(\forall x)(x = x)$ for any variable x.

(v) $(\forall x)(\forall y)(x = y \Rightarrow (p \Rightarrow p[y/x]))$ for any variables x, y where y is not bound in the formula p.

(vi) $((\forall x)p) \Rightarrow p[t/x]$ for any variable x, formula p, and term t that has no free variable that occurs bound in p.

(vii) $(\forall x)(p \Rightarrow q) \Rightarrow (p \Rightarrow (\forall x)q)$ for any formulae p, q and variable x that does not appear free in p.

Note that all of these axioms are tautologies; they hold in every structure. We define the following deduction rules.

(i) (modus ponens) From p and $p \Rightarrow q$, we can deduce q.

(ii) (generalisation) From p, we can deduce $(\forall x)p$ provided that x does not occur free in any premise used to deduce p.

For $S \subseteq L$ and $t \in L$, we say that $S \vdash p$, read S *proves* p, if there exists a *proof* of p from S, which is a finite sequence of formulae ending with p such that each formula is a logical axiom, a hypothesis in S, or obtained from earlier lines by one of the deduction rules.

Remark. Suppose we allow the empty structure for a language with no constants. Then, $\bot$ is false in A, and the statement $(\forall x)\bot$ is true in A. Therefore, $((\forall x)\bot) \Rightarrow \bot$ is false by modus ponens. But this is an instance of axiom (vi), showing that it would not be a tautology.

Example. We show $\{x = y, x = z\} \vdash y = z$ where x, y, z are different variables.

1. $(\forall x)(\forall y)(x = y \Rightarrow (x = z \Rightarrow y = z))$ (axiom 5)
2. $((\forall x)(\forall y)(x = y \Rightarrow (x = z \Rightarrow y = z))) \Rightarrow (\forall y)(x = y \Rightarrow (x = z \Rightarrow y = z))$ (axiom 6)
3. $(\forall y)(x = y \Rightarrow (x = z \Rightarrow y = z))$ (modus ponens on lines 1, 2)
4. $((\forall y)(x = y \Rightarrow (x = z \Rightarrow y = z))) \Rightarrow (x = y \Rightarrow (x = z \Rightarrow y = z))$ (axiom 6)
5. $x = y \Rightarrow (x = z \Rightarrow y = z)$ (modus ponens on lines 3, 4)
6. $x = y$ (hypothesis)
7. $x = z \Rightarrow y = z$ (modus ponens on lines 5, 6)
8. $x = z$ (hypothesis)
9. $y = z$ (modus ponens on lines 7, 8)

4.4 Deduction theorem

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

Proof. As before, given a proof of $p \Rightarrow q$ from S, one can establish a proof of q from $S \cup \{p\} \vdash q$ by writing p and applying modus ponens to the original proof.

Conversely, suppose we have a proof $S \cup \{p\} \vdash q$. We convert each line t_i into $p \Rightarrow t_i$ as in the proof in propositional logic. The only new case is generalisation. Suppose we have the line r and then the line $(\forall x)r$ obtained by generalisation, and we have a proof $S \vdash p \Rightarrow r$ by induction. In the proof $S \cup \{p\} \vdash r$, no hypothesis has a free occurrence of x. Therefore, in the proof $S \vdash p \Rightarrow r$, the same holds. Thus, $S \vdash (\forall x)(p \Rightarrow r)$ by generalisation.

Suppose x is not free in p. Then, $S \vdash p \Rightarrow (\forall x)r$ by axiom 7 and modus ponens.

Now, suppose x occurs free in p. In this case, the proof $S \cup \{p\} \vdash r$ cannot have used the hypothesis p. Hence, $S \vdash r$, and so $S \vdash (\forall x)r$ by generalisation. This gives $S \vdash p \Rightarrow (\forall x)r$ by axiom 1. □

4.5 Soundness

This section is non-examinable.

Proposition. Let S be a set of sentences in L, and p a sentence in L. Then $S \vdash t$ implies $S \vDash t$.

Proof. We have a proof $t_1, \dots, t_n$ of p from S. We show that if A is a model of S, A is also a model of t_i for each i (interpreting free variables as quantified); this can be shown by induction. Hence, $S \vDash p$. □

4.6 Adequacy

This section is non-examinable.

We want to show that $S \vDash p$ implies $S \vdash p$. Equivalently, $S \cup \{\neg p\} \vDash \bot$ implies $S \cup \{\neg p\} \vdash \bot$. In other words, if $S \cup \{\neg p\}$ is consistent, it has a model.

Theorem (model existence lemma)**.** Every consistent theory has a model.

We will need a number of key ideas in order to prove this.

(i) We will construct our model out of the language itself using the closed terms of L. For instance, if L is the language of fields and S is the usual field axioms, we take the closed terms and combine them with $+$ and $\cdot$ in the obvious way.

(ii) However, we can prove $S \vdash 1 + 0 = 1$, but $1 + 0$ and 1 are distinct as strings. We will therefore take the quotient of this set by the equivalence relation defined by $s \sim t$ if $S \vdash s = t$. If this set is A, we define $[s] +_A [t] = [s + t]$, and this is a well-defined operation.

(iii) Suppose S is the set of field axioms with the statement that $1 + 1 = 0 \vee 1 + 1 + 1 = 0$. In this theory, $S \nvdash 1 + 1 = 0$ and $S \nvdash 1 + 1 + 1 = 0$. Therefore, $[1 + 1] \neq [0]$ and $[1 + 1 + 1] \neq [0]$, so our structure A is not of characteristic 2 or 3. We can overcome this by first extending S to a maximal consistent theory.

(iv) Suppose S is the set of field axioms with the statement that $(\exists x)(x \cdot x = 1 + 1)$. There is no closed term t with the property that $[t \cdot t] = [1 + 1]$. The problem is that S lacks *witnesses* to existential quantifiers. For each statement of the form $(\exists x)p \in S$, we add a new constant c to the language and add to S the sentence $p[c/x]$. This still forms a consistent set.

(v) The resulting set may no longer be maximal, as we have extended our language with new constants. We must then return to step (iii) then step (iv); it is not clear if this process ever terminates.

Proof. Let S be a consistent set in a language $L = L(\Omega, \Pi)$. Extend S to a maximal consistent set S_1, using Zorn's lemma. Then, for each sentence $p \in L$, either $p \in S_1$ or $\neg p \in S_1$. Such a theory is called *complete*; each sentence or its negation is proven. Now, we add witnesses to S_1: for each sentence of the form $(\exists x)p \in S_1$, we add a new constant symbol c to the language, and also add the sentence $p[c/x]$. We then obtain a new theory T_1 in the language $L_1 = L(\Omega \cup C_1 \Pi)$ that has witnesses for every existential in S_1. One can check easily that T_1 is consistent.

We then extend T_1 to a maximal consistent theory S_2 in L_1, and add witnesses to produce T_2 in the language $L_2 = L(\Omega \cup C_1 \cup C_2, \Pi)$. Continue inductively, and let $\overline{S} = \bigcup_{n \in \mathbb{N}} S_n$ in the language $\overline{L} = L\big(\Omega \cup \bigcup_{n \in \mathbb{N}} C_n, \Pi\big)$.

We claim that $\overline{S}$ is consistent, complete, and has witnesses for every existential in $\overline{S}$. Clearly $\overline{S}$ is consistent: if $\overline{S} \vdash \bot$ then $S_n \vdash \bot$ for some n as proofs are finite, contradicting consistency of S_n. For completeness, if p is a sentence in $\overline{L}$, p must lie in L_n for some n as it is a finite string of symbols. But

S_{n+1} is complete in L_n, so $S_{n+1} \vdash p$ or $S_{n+1} \vdash \neg p$, so certainly $\overline{S} \vdash p$ or $\overline{S} \vdash \neg p$. If $(\exists x)p \in \overline{S}$, then $(\exists x)p \in S_n$ for some n, so T_n provides a witness.

On the closed terms of $\overline{L}$, we define the relation $s \sim t$ if $\overline{S} \vdash s = t$. This is clearly an equivalence relation, so we can define A to be the set of equivalence classes of $\overline{L}$ under $\sim$. This is an $\overline{L}$-structure by defining

- $f_A([t_1], \dots, [t_n]) = [f\ t_1 \dots t_n]$ for each $f \in \Omega \cup \bigcup_{n \in \mathbb{N}} C_n, \alpha(f) = n, t_i$ closed terms;
- $\varphi_A = \left\{([t_1], \dots, [t_n]) \in A^n \mid \overline{S} \vdash \varphi(t_1, \dots, t_n)\right\}$ for each $\varphi \in \Pi, \alpha(\varphi) = n, t_i$ closed terms.

We claim that for a sentence $p \in \overline{L}$, we have $p_A = 1$ if and only if $\overline{S} \vdash p$. Then the proof is complete, as $S \subseteq \overline{S}$ so $p_A = 1$ for every $p \in S$, so A is a model of S.

We prove this by induction on the length of sentences. First, suppose p is atomic. $\bot_A = 0$, as $\overline{S} \nvdash \bot$. For closed terms s, t, $\overline{S} \vdash s = t$ if and only if $[s] = [t]$ by definition of $\sim$. This holds if and only if $s_A = t_A$ by definition of the operations in A. This is precisely the statement that $s = t$ holds in A. The same holds for relations.

Now consider $p \Rightarrow q$. $\overline{S} \vdash p \Rightarrow q$ if and only if $\overline{S} \vdash \neg p$ or $\overline{S} \vdash q$ as $\overline{S}$ is complete and consistent; if $\overline{S} \nvdash \neg p$ and $\overline{S} \nvdash q$, then $\overline{S} \vdash p$ and $\overline{S} \vdash \neg p$. By induction on the length of the formula, this holds if and only if $p_A = 0$ or $q_A = 1$. This is the definition of the interpretation of $p \Rightarrow q$ in A.

Finally, consider the existential $(\exists x)p$. $\overline{S} \vdash (\exists x)p$ if and only if there is a closed term t such that $\overline{S} \vdash p[t/x]$, as $\overline{S}$ has witnesses to every existential. By induction (for example on the amount of quantifiers in a formula), this holds if and only if $p[t/x]_A = 1$ for some closed term t. This is true exactly when $(\exists x)p$ holds in A, as A is precisely the set of equivalence classes of closed terms. □

Corollary (adequacy)**.** Let $S \subseteq L$ be a theory and $t \in L$ be a sentence. Then $S \vDash t$ implies $S \vdash t$.

4.7 Completeness

Theorem (Gödel's completeness theorem for first order logic)**.** Let $S \subseteq L$ be a theory and $t \in L$ be a sentence. Then $S \vDash t$ if and only if $S \vdash t$.

Proof. Follows from soundness and adequacy. □

Note that *first order* refers to the fact that variables quantify over elements, rather than sets of elements.

Remark. If L is countable, or equivalently Ω and Π are countable, Zorn's lemma is not needed in the above proof.

Theorem (compactness theorem)**.** Let $S \subseteq L$ be a theory. Then if every finite subset $S' \subseteq S$ has a model, S has a model.

Proof. Trivial after applying completeness as proofs are finite. □

There is no decidability theorem for first order logic, as $S \vDash p$ can only be verified by checking its valuation in every L-structure.

Corollary. The class of finite groups is not axiomatisable in the language of groups: there is no theory S such that a group is finite if and only if each $p \in S$ holds in the group.

Proof. Suppose S is a set of sentences that axiomatises the theory of finite groups. Consider S together with the sentences $(\exists x_1)(\exists x_2)(x_1 \neq x_2)$, $(\exists x_1)(\exists x_2)(\exists x_3)(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3)$ and so on, which collectively assert that the group has at least k elements for every k. Each finite subset $S' \subseteq S$ has a model, such as a cyclic group of sufficiently large order. So by compactness, there is a model of S, which is a finite group with at least k elements for every k, giving a contradiction. □

Corollary. Let S be a theory with arbitrarily large finite models. Then S has an infinite model.

Proof. Add sentences and apply compactness as in the previous corollary. □

Finiteness is not a first-order property.

Theorem (upward Löwenheim–Skolem theorem)**.** Let S be a theory with an infinite model. Then S has an uncountable model.

Proof. Add constants $\{c_i \mid i \in I\}$ to the language, where I is an uncountable set. Add sentences $c_i \neq c_j$ to the theory for all $i \neq j$ to obtain a theory S'. Any finite set of sentences in S' has a model: indeed, the infinite model of S suffices. By compactness, S' has a model. □

Remark. Similarly, we can prove the existence of models of S that do not inject into X for any fixed set X. Adding $\gamma(X)$ constants or $\mathcal{P}(X)$ constants both suffice.

Example. There is an uncountable field, as there is an infinite field $\mathbb{Q}$. There is also a field that does not inject into X for any fixed set X.

Theorem (downard Löwenheim–Skolem theorem)**.** Let S be a theory in a countable language L, or equivalently, Ω and Π are countable. Then if S has a model, it has a countable model.

Proof. S is consistent, so the model constructed in the proof of the model existence lemma is countable. □

4.8 Peano arithmetic

Consider the language L given by $\Omega = \{0, s, +, \cdot\}$ with $\alpha(0) = 0, \alpha(s) = 1, \alpha(+) = \alpha(\cdot) = 2$, and $\Pi = \varnothing$. It has axioms

(i) $(\forall x)(s(x) \neq 0)$;

(ii) $(\forall x)(\forall y)(s(x) = s(y) \Rightarrow x = y)$;

(iii) $(\forall y_1) \dots (\forall y_n)[p[0/x] \wedge (\forall x)(p \Rightarrow p[s(x)/x]) \Rightarrow (\forall x)p]$ for each formula p with free variables $x, y_1, \dots, y_n$;

(iv) $(\forall x)(x + 0 = x)$;

(v) $(\forall x)(\forall y)(x + s(y) = s(x + y))$;

(vi) $(\forall x)(x \cdot 0 = 0)$;

(vii) $(\forall x)(\forall y)(x \cdot s(y) = x \cdot y + x)$.

These axioms are sometimes called Peano arithmetic, PA, or formal number theory. The y_i in (iii) are called *parameters*. Without the parameters, we would not be able to perform induction on sets such as $\{x \mid x \geq y\}$ if y is a variable.

Note that PA clearly has an infinite model, namely $\mathbb{N}$. So by the upward Löwenheim–Skolem theorem, it has an uncountable model, which in particular is not isomorphic to $\mathbb{N}$. This is because (iii) is not 'true' induction, stating that all subsets of $\mathbb{N}$ either have a least element not in it, or it is $\mathbb{N}$ itself. Axiom (iii) applies only to countably many formulae p, and therefore only asserts that induction holds for countably many subsets of $\mathbb{N}$.

Definition. A set $S \subseteq \mathbb{N}$ is *definable* in the language of PA if there is a formula p with a free variable x such that for each $m \in \mathbb{N}$, $m \in S$ if and only if $p[m/x]$ holds in $\mathbb{N}$.

Only countably many formulae exist, so only countably many sets are definable.

Example. The set of squares is definable, as it can be defined by the formula $(\exists y)(y \cdot y = x)$. The set of primes is also definable by $x \neq 0 \wedge x \neq 1 \wedge (\forall y)(y \mid x \Rightarrow y = 1 \wedge y = x)$, where $y \mid x$ is defined to mean $(\exists z)(z \cdot y = x)$. The set of powers of 2 can be defined by $(\forall y)(y \text{ is prime} \wedge y \mid x \Rightarrow y = 2)$. The set of powers of 4 and the set of powers of 6 are also definable.

Theorem (Gödel's incompleteness theorem)**.** PA is not complete.

This theorem shows that there is a sentence p such that PA $\nvdash p$ and PA $\nvdash \neg p$. However, one of $p, \neg p$ must hold in $\mathbb{N}$, so there is a sentence p that is true in $\mathbb{N}$ that PA does not prove. This does not contradict the completeness theorem, which is that if p is true in *every* model in PA then PA $\vdash p$.

5 Set theory

5.1 Axioms of ZF

In this section, we will attempt to understand the structure of the universe of sets. In order to do this, we will treat set theory as a first-order theory like any other, and can therefore study it with our usual tools. In particular, we will study a particular theory called *Zermelo–Fraenkel set theory*, denoted ZF. The language has $\Omega = \varnothing, \Pi = \{\in\}, \alpha(\in) = 2$. A 'universe of sets' is simply a model $(V, \in_V) = (V, \in)$ for the axioms of ZF. We can view this section as a worked example of the concepts of predicate logic, but every model of ZF will contain a copy of (most of) mathematics, so they will be very complicated.

We now define the axioms of ZF set theory.

(i) *Axiom of extension.*

$$(\forall x)(\forall y)((\forall z)(z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$$

Note that the converse follows from the definition of equality. This implies that sets have no duplicate elements, and have no ordering.

(ii) *Axiom of separation* or *comprehension*. For a set x and a property p, we can form the set of $z \in x$ such that $p(z)$ holds.

$$(\forall t_1) \dots (\forall t_n)(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow z \in x \wedge p)$$

where the t_i are the parameters, and p is a formula with free variables $t_1, \dots, t_n, z$. Note that we need the parameters as we may wish to form the set $\{z \in x \mid z \in t\}$ for some variable t. We write $\{z \in x \mid p(z)\}$ for the set guaranteed by this axiom; this is an abbreviation and does not change the language.

(iii) *Empty-set axiom.*

$$(\exists x)(\forall y)(\neg y \in x)$$

This empty set is unique by extensionality. We write $\varnothing$ for the set guaranteed by this axiom. For instance, $p(\varnothing)$ is the sentence $(\exists x)((\forall y)(\neg y \in x) \wedge p(x))$.

(iv) *Pair-set axiom.*

$$(\forall x)(\forall y)(\exists z)(\forall t)(t \in z \Leftrightarrow t = x \vee t = y)$$

We write $\{x, y\}$ for this set z, which is unique by extensionality. Some basic set-theoretic principles can now be defined.

- We write $\{x\} = \{x, x\}$ for the singleton set containing x.
- We can now define the ordered pair $(x, y) = \{\{x\}, \{x, y\}\}$; from the axioms so far we can prove that $(x, y) = (z, t)$ if and only if $x = z$ and $y = t$.
- We say that x is an ordered pair if $(\exists y)(\exists z)(x = (y, z))$, and f is a function if

  $$(\forall x)(x \in f \Rightarrow x \text{ is an ordered pair})$$

  and

  $$(\forall x)(\forall y)(\forall z)((x, y) \in f \wedge (x, z) \in f \Rightarrow y = z)$$

- We call a set x the domain of f, written $x = \operatorname{dom} f$, if f is a function and

  $$(\forall y)(y \in x \Leftrightarrow (\exists z)((y, z) \in f))$$

- The notation $f : x \to y$ means that f is a function, $x = \operatorname{dom} f$, and

  $$(\forall z)(\forall t)((z, t) \in f \Rightarrow t \in y)$$

(v) *Union axiom.* For each family of sets x, we can form its union $\bigcup_{t \in x} t$.

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\exists t)(z \in t \wedge t \in x))$$

The set guaranteed by this axiom can be written $\bigcup x$, and we can write $x \cup y$ for $\bigcup \{x, y\}$. We need no intersection axiom, as such intersections already exist by the axiom of separation. This cannot be used to create empty intersections, as the axiom of separation can only create subsets of a set that already exists.

(vi) *Power-set axiom.*

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow z \subseteq x)$$

where $z \subseteq x$ means $(\forall t)(t \in z \Rightarrow t \in x)$. We write $\mathcal{P}(x)$ for the power set of x. We can form the Cartesian product $x \times y$ as a suitable subset of $\mathcal{P}(\mathcal{P}(x \cup y))$, as if $z \in x, t \in y$, we have $(z,t) = \{\{z\},\{z,t\}\} \in \mathcal{P}(\mathcal{P}(x \cup y))$. The set of all functions $x \to y$ can be defined as a subset of $\mathcal{P}(x \times y)$.

(vii) *Axiom of infinity*. Using our currently defined axioms, any model V must be infinite. For example, writing x^+ for the *successor* of x defined as $x \cup \{x\}$, the sets $\varnothing, \varnothing^+, \varnothing^{++}, \dots$ are distinct.

$$\varnothing^+ = \{\varnothing\}; \quad \varnothing^{++} = \{\varnothing,\{\varnothing\}\}; \quad \varnothing^{+++} = \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}; \quad \dots$$

We write $0 = \varnothing, 1 = \varnothing^+, 2 = \varnothing^{++}, \dots$ for the successors created in this way. For instance, $3 = \{0,1,2\}$. V may not have an infinite element, even though V itself is infinite, because no $x \in V$ has all $y \in V$ as elements: V does not think of itself as a set, because Russell's paradox follows from the axioms defined so far.

We say that x is a successor set if $\varnothing \in x$ and $(\forall y)(y \in x \Rightarrow y^+ \in x)$. Note that this is a finite-length formula that characterises an infinite set. The axiom of infinity is that there exists a successor set.

$$(\exists x)(\varnothing \in x \wedge (\forall y)(y \in x \Rightarrow y^+ \in x))$$

Note that this set is not uniquely defined, but any intersection of successor sets is a successor set. We can therefore take the intersection of all successor sets by the axiom of separation, giving a least successor set denoted ω. Thus, $(\forall x)(x \in \omega \Leftrightarrow (\forall y)(y \text{ is a successor set} \Rightarrow x \in y))$. For example, we can prove that $3 \in \omega$.

In particular, if x is a successor set and a subset of ω, then $x = \omega$. Hence, $(\forall x)(x \subseteq \omega \wedge \varnothing \in x \wedge (\forall y)(y \in x \Rightarrow y^+ \in x) \Rightarrow x = \omega)$. This is 'proper' induction over all subsets of ω, unlike the weaker first-order induction defined in the Peano axioms. It is easy to check that $(\forall x)(x \in \omega \Rightarrow x^+ \neq \varnothing)$ and $(\forall x)(\forall y)(x \in \omega \wedge y \in \omega \wedge x^+ = y^+ \Rightarrow x = y)$, so ω satisfies (in V) the usual axioms for the natural numbers. We can now define 'x is finite' to mean $(\exists y)(y \in \omega \wedge x$ bijects with $y)$, and define 'x is countable' to mean that x is finite or bijects with ω.

(viii) *Axiom of foundation* or *regularity*. We require that sets are built out of simpler sets. For example, we want to disallow a set from being a member of itself, and similarly forbid $x \in y$ and $y \in x$. In general, we want to forbid sets x_i such that $x_{i+1} \in x_i$ for each $i \in \mathbb{N}$.

Note that if $x \in x$, $\{x\}$ has no $\in$-minimal element. If $x \in y, y \in x$, $\{x,y\}$ has no $\in$-minimal element. In the last example, $\{x_0, x_1, \dots\}$ has no $\in$-minimal element. We now define the axiom of foundation: every nonempty set has an $\in$-minimal element.

$$(\forall x)(x \neq \varnothing \Rightarrow (\exists y)(y \in x \wedge (\forall z)(z \in x \Rightarrow z \notin y)))$$

Any model of ZF without this axiom has a submodel of all of ZF.

(ix) *Axiom of replacement*. Often, we are given an index set I and construct a set A_i for each $i \in I$, then take the collection $\{A_i \mid i \in I\}$. In order to write this down, the mapping $i \mapsto A_i$ must be a function, or equivalently, there must be a set $\{(i, A_i) \mid i \in I\}$. This is not clear from the other axioms. We would like to say that the image of a set under something that looks like a function (since we do not yet have such a set-theoretic function) is a set.

Let $(V, \in)$ be an L-structure. A *class* is a set $C \subseteq V$ such that for some formula p with free variables x and some parameters, we have $x \in C$ if and only if p holds in V. C is a set outside of our model; it may not correspond to a set $x \in V$ inside the model. For instance, V is a class, taking p to be $x = x$. There is a class of infinite sets, taking p to be 'x is not finite'. For any $t \in V$, the collection of x with $t \in x$ is a class; here, t is a parameter to the class. Every set $y \in V$ is a class by setting p to be $x \in y$. A *proper class* is a class that does not correspond to a set $x \in V$: $\neg(\exists y)(\forall x)(x \in y \Leftrightarrow p)$. When writing about classes inside ZF, we instead write about their defining formulae, as classes have no direct representation in the language.

Similarly, a *function-class* is a set $F \subseteq V$ of ordered pairs from V such that for some formula p with free variables x, y and parameters, we have (x, y) belongs to F if and only if p, and if $(x, y), (x, z)$ belong to F, $y = z$. This is intuitively a function whose domain may not be a set. For example, the mapping $x \mapsto \{x\}$ is a function-class, taking p to be $y = \{x\}$. This is not a function, for example, every f has a domain which is a set in V, and this function has domain V which is not a set.

We can now define the axiom of replacement: the image of a set under a function-class is a set.

$$(\forall t_1) \dots (\forall t_n)[(\forall x)(\forall y)(\forall z)(p \wedge p[z/y] \Rightarrow y = z) \Rightarrow$$

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\exists t)(t \in x \wedge p[t/x, z/y]))]$$

For example, for any set x, we can form the set $\{\{t\} \mid t \in x\}$, which is the image of x under the function class $t \mapsto \{t\}$. This set could alternatively have been formed using the power-set and separation axioms; we will later present some examples of sets built with this axiom that cannot be constructed from the other axioms.

This completes the description of the axioms of ZF. We write ZFC for ZF + AC, where AC is the axiom

$$(\forall f)[f \text{ is a function} \wedge (\forall x)(x \in \operatorname{dom} f \Rightarrow f(x) \neq \varnothing) \Rightarrow$$

$$(\exists g)(g \text{ is a function} \wedge (\operatorname{dom} g = \operatorname{dom} f) \wedge (\forall x)(x \in \operatorname{dom} f \Rightarrow g(x) \in f(x)))]$$

5.2 Transitive sets

Definition. x is *transitive* if each member of a member of x is a member of x.

$$(\forall y)((\exists z)(y \in z \wedge z \in x) \Rightarrow y \in x)$$

Equivalently, $\bigcup x \subseteq x$.

Example. $\varnothing$ is a transitive set. $\{\varnothing\}$ is also transitive, and $\{\varnothing, \{\varnothing\}\}$ is transitive. In general, elements of ω are transitive. This can be proven by ω-induction (inside a model): $\varnothing$ is transitive, and if y is transitive, $y^+ = y \cup \{y\}$ is clearly transitive.

Lemma. Every set is contained in a transitive set.

Here, we define 'x contains y' to mean $y \subseteq x$, not $y \in x$.

Remark. This proof takes place inside an arbitrary model of ZF. Technically, the statement of the lemma is 'let $(V, \in)$ be a model of ZF, then for all sets $x \in V$, x is contained in a transitive set $y \in V$'. By completeness, this will show that there is a proof of this fact from the axioms of ZF.

Note also that once this lemma is proven, any x is contained in a least transitive set by taking intersections, called its *transitive closure*, written $TC(x)$. This holds as any intersection of transitive sets is transitive.

Proof. We want to form $x \cup (\bigcup x) \cup (\bigcup \bigcup x) \cup \dots$; if this is a set, it is clearly transitive and contains x. We can show that this is a set by the union axiom applied to the set $\{x, \bigcup x, \bigcup \bigcup x, \dots\}$. This is a set by applying the axiom of replacement, it is an image of ω under the function-class $0 \mapsto x, 1 \mapsto \bigcup x, 2 \mapsto \bigcup \bigcup x$ and so on. We want to define the function-class $p(z,w)$ to be $(z = 0 \wedge w = x) \vee ((\exists t)(\exists u) z = t^+ \wedge w = \bigcup u \wedge p(t,u))$, but this is not a first-order formula.

Define that f is an *attempt* to mean that

$$(f \text{ is a function}) \wedge (\operatorname{dom} f \in \omega) \wedge (\operatorname{dom} f \neq \varnothing) \wedge (f(0) = x) \wedge$$

$$(\forall n)\Big(n \in \omega \wedge n \in \operatorname{dom} f \wedge n \neq 0 \Rightarrow f(n) = \bigcup f(n-1)\Big)$$

Then,

$$(\forall n)(n \in \omega \Rightarrow (\exists f)(f \text{ is an attempt} \wedge n \in \operatorname{dom} f))$$

can be proven by ω-induction. We can similarly prove

$$(\forall n)(n \in \omega \Rightarrow (\forall f)(\forall g)(f, g \text{ are attempts} \wedge n \in \operatorname{dom} f \cap \operatorname{dom} g \Rightarrow f(n) = g(n)))$$

by ω-induction. We now define the function-class $p = p(z,w)$ to be

$$(\exists f)(f \text{ is an attempt} \wedge z \in \operatorname{dom} f \wedge f(z) = w)$$

□

Intuitively, we needed to use the axiom of replacement because we started with a set x and needed to go 'far away' from it, forming $\bigcup^n x$ for all x. We could not have used the other axioms such as the power-set axiom, as the $\bigcup^n x$ are not contained in an obvious larger set.

Transitive closures allow us to pass from the large universe of sets, which is not a set itself, into a smaller world which is a set closed under $\in$ that contains the relevant sets in question.

5.3 $\in$-induction

We want the axiom of foundation to capture the idea that sets are built out of simpler sets.

Theorem (principle of $\in$-induction). For each formula p with free variables $t_1, \dots, t_n, x$,

$$(\forall t_1) \dots (\forall t_n)[(\forall x)((\forall y)(y \in x \Rightarrow p(y)) \Rightarrow p(x)) \Rightarrow (\forall x)p(x)]$$

Proof. Given $t_1, \dots, t_n$ and the statement $(\forall x)((\forall y)(y \in x \Rightarrow p(y)) \Rightarrow p(x))$, we want to show $(\forall x)p(x)$. Suppose this is not the case, so there exists x such that $\neg p(x)$. We want to look at the set $\{t \mid \neg p(t)\}$ and take an $\in$-minimal element, but this is not necessarily a set, for instance if $p(x)$ is the assertion $x \neq x$.

Let $u = \{t \in TC(\{x\}) \mid \neg p(t)\}$; this is clearly a set in the model, and $u \neq \varnothing$ as $x \in u$. Let t be an $\in$-minimal element of u, guaranteed by the axiom of foundation. Then $\neg p(t)$ as $t \in u$, but $p(z)$ for all $z \in t$ by minimality of t, noting that $z \in t$ implies $z \in TC(\{x\})$. This gives a contradiction. □

The name of this theorem should be read 'epsilon-induction', even though the membership relation is denoted $\in$ and not ϵ or ε.

The principle of $\in$-induction is equivalent to the axiom of foundation in the presence of the other axioms of ZF. We say that x is *regular* if $(\forall y)(x \in y \Rightarrow y$ has a minimal element$)$. The axiom of foundation is equivalent to the assertion that every set is regular. Given $\in$-induction, we can prove every set is regular. Suppose $(\forall y \in x)(y$ is regular$)$; we need to show x is regular. For a set z with $x \in z$, if x is minimal in z, x is clearly regular as required. If x is not minimal in z, there exists $y \in x$ such that $y \in z$. So z has a minimal element as y is regular. Hence x is regular.

5.4 $\in$-recursion

We want to be able to define $f(x)$ given $f(y)$ for all $y \in x$.

Theorem ($\in$-recursion theorem)**.** Let G be a function-class, so $(x, y) \in G$ if and only if $p(x, y)$ for some formula p. Suppose that G is defined for all sets. Then there is a function-class F defined for all sets by a formula $q(x, y)$ such that

$$(\forall x)\left(F(x) = G\left(F\Big|_x\right)\right)$$

Moreover, this F is unique.

Note that $F|_x = \{(y, F(y)) \mid y \in x\}$ is a set by the axiom of replacement.

Proof. Define that f is an *attempt* if

$$f \text{ is a function} \wedge \operatorname{dom} f \text{ is transitive} \wedge (\forall x)\left(x \in \operatorname{dom} f \Rightarrow f(x) = G\left(f\Big|_x\right)\right)$$

Note that $f|_x$ is defined as $\operatorname{dom} f$ is transitive. Then,

$$(\forall x)(\forall f)(\forall f')(f, f' \text{ are attempts} \wedge x \in \operatorname{dom} f \cap \operatorname{dom} f' \Rightarrow f(x) = f'(x))$$

by $\in$-induction: if $f(y) = f'(y)$ for all $y \in x$, then $f(x) = f'(x)$. Also,

$$(\forall x)(\exists f)(f \text{ is an attempt} \wedge x \in \operatorname{dom} f)$$

by $\in$-induction. Indeed, if for all $y \in x$ there exists an attempt defined at y, then for each $y \in x$ there is a unique attempt f_y defined on $TC(\{y\})$. Let $f = \bigcup\{f_y \mid y \in x\}$, which is an attempt with domain $TC(x)$. We can then define $f' = f \cup \{(x, G(f|_x))\}$. This is an attempt defined at x. We can then take $q(x, y)$ to be

$$(\exists f)(f \text{ is an attempt} \wedge x \in \operatorname{dom} f \wedge f(x) = y)$$

This defines the function-class F as required. Uniqueness follows from the fact that if F, F' are suitable function-classes, we have $(\forall x)(F(x) = F'(x))$ by $\in$-induction. □

5.5 Well-founded relations

Note the similarity between the proofs of $\in$-induction and $\in$-recursion and the proofs of induction and recursion on ordinals. These proofs are not specific to the relation $\in$; we only used some of its properties.

(i) p is *well-founded*: every nonempty set has a p-minimal element.

(ii) p is *local*: $\{x \mid p(x,y)\}$ is a set. This was required to build the p-transitive closure.

Therefore, p-induction and p-recursion hold for all relation-classes p that are well-founded and local. In particular, if r is a well-founded relation on a set a, it is clearly local and hence we have r-induction and r-recursion. The theorems about induction and recursion on ordinals are therefore special cases of this, as a well-ordering is precisely a well-founded total order.

On the set $\{a,b,c\}$, let r be the relation arb, brc. Choosing $a' = \varnothing, b' = \{\varnothing\}, c' = \{\{\varnothing\}\}$, the map $f : \{a,b,c\} \to \{a',b',c'\}$ given by $x \mapsto x'$ is a bijection with a transitive set such that xry if and only if $f(x) \in f(y)$. This models the relation r by $\in$.

We say that a relation r on a set a is *extensional* if

$$(\forall x \in a)(\forall y \in a)((\forall z \in a)(zrx \Leftrightarrow zry) \Rightarrow x = y)$$

The relation r in the above example is extensional.

Theorem (Mostowski's collapsing theorem)**.** Let r be a relation on a set a that is well-founded and extensional. Then, there exists a transitive set b and a bijection $f : a \to b$ such that

$$(\forall x \in a)(\forall y \in a)(xry \Leftrightarrow f(x) \in f(y))$$

Moreover, b and f are unique.

This is an analogue of subset collapse from the section on ordinals. Transitive sets are playing the role of initial segments. Note that the well-foundedness and extensionality conditions are clearly necessary for the theorem, consider $(\mathbb{Z}, <)$ or $(\{a,b,c,\}, <)$ with $a < b, a < c$ for counterexamples.

Proof. We define the function f by $f(x) = \{f(y) \mid yrx\}$ using r-recursion. Note that f is a function by the axiom of replacement as it is given by a function-class F obtained from r-recursion that is defined on the set a. Let $b = \{f(x) \mid x \in a\}$; this is a set by the axiom of replacement. Clearly f is surjective by the definition of b, and b is transitive by definition.

We claim that f is injective, and then we have that yrx if and only if $f(y) \in f(x)$ by definition of f. We show

$$(\forall x \in a)(\forall x' \in a)(f(x') = f(x) \Rightarrow x' = x)$$

by r-induction on x. Suppose that $(\forall yrx)(\forall z \in a)(f(y) = f(z) \Rightarrow y = z)$, we have $f(x) = f(x')$, and we want to show that $x = x'$. Note that $\{f(y) \mid yrx\} = \{f(z) \mid zrx'\}$ by the definition of f as $f(x) = f(x')$. So $\{y \mid yrx\} = \{z \mid zrx'\}$, so $x = x'$ as r is extensional. Uniqueness holds by r-induction, as we must have $f(x) = \{f(y) \mid yrx\}$ for all $x \in a$. □

In particular, every well-ordered set has a unique order isomorphism to a unique transitive set well-ordered by $\in$. We can now define that an ordinal is a transitive set well-ordered by $\in$ (or equivalently, totally-ordered, due to the axiom of foundation). For example, $\varnothing$ is an ordinal, $n \in \omega$ is an ordinal, ω is also an ordinal, and so on. Therefore, each well-ordering is order-isomorphic to a unique ordinal called its order type, by Mostowski collapse.

Remark. If x, y are elements of a well-ordered set a with $y < x$, then the order type of I_x, which is precisely the image $f(x)$ under the Mostowski collapse, has an element $f(y)$, the order type of I_y. In particular, given two ordinals α, β, the statement $\alpha < \beta$ is equivalent to $\alpha \in \beta$. Hence $\alpha = \{\beta \mid \beta < \alpha\}$. Thus, $\alpha^+ = \alpha \cup \{\alpha\}$, and $\sup\{\alpha_i \mid i \in I\} = \bigcup\{\alpha_i \mid i \in I\}$.

5.6 The universe of sets

We would like the universe to be V-shaped, in the sense that we begin with $\varnothing$ and continue taking power sets to create larger and larger sets. Define sets V_α for each ordinal α by

- $V_0 = \varnothing$;
- $V_{\alpha+1} = \mathcal{P}(V_\alpha)$;
- $V_\lambda = \bigcup\{V_\alpha \mid \alpha < \lambda\}$ for a nonzero limit ordinal λ.

This can be viewed as a well-founded recursion on ordinals, or $\in$-recursion on the universe but mapping non-ordinals to $\varnothing$. For example, $V_\omega = V_0 \cup V_1 \cup \dots$, and $V_{\omega+1} = \mathcal{P}(V_\omega)$. We will now show that every set is contained within some V_α.

Lemma. Each V_α is transitive.

Proof. We show this by induction on α. Clearly $V_0 = \varnothing$ is transitive. Suppose V_α is transitive. Then $V_{\alpha+1}$ is transitive as the power set of a transitive set is transitive. Indeed, if x is transitive and $z \in y \in \mathcal{P}(x)$, we have $z \in x$, so $z \subseteq x$ as x is transitive, so $z \in \mathcal{P}(x)$. Now suppose λ is a limit ordinal, and that the V_α are transitive for $\alpha < \lambda$. Any union of transitive sets is transitive, so V_λ is transitive. □

Lemma. Let $\alpha \leq \beta$. Then $V_\alpha \subseteq V_\beta$.

Proof. We show this by induction on β for a fixed α. If $\beta = \alpha$, $V_\alpha \subseteq V_\beta$ is trivial. For successors, note that $V_\beta \subseteq \mathcal{P}(V_\beta)$ as V_β is transitive. So if $V_\alpha \subseteq V_\beta$, then $V_\alpha \subseteq V_{\beta+1}$. Limits are trivial. □

Theorem. Every set x belongs to V_α for some α.

If we could construct the set V defined as the union of the V_α over all ordinals α, V would be a model of ZF.

Remark. Note that $x \subseteq V_\alpha$ if and only if $x \in V_{\alpha+1}$, so it suffices to show that each set x is a subset of some V_α. Once we have $x \subseteq V_\alpha$ for some α, there is a least such α, called the *rank* of x. For example, the rank of $\varnothing$ is 0, the rank of 1 is 1, the rank of ω is ω, and in general the rank of any ordinal α is α. Intuitively, the rank of a set is the time at which it was created.

Proof. We proceed by $\in$-induction on x; we may assume that for all $y \in x$, there exists α such that $y \subseteq V_\alpha$, so $y \subseteq V_{\mathrm{rank}(y)}$. Thus, for each $y \in x$, $y \in V_{\mathrm{rank}(y)+1}$, so define $\alpha = \sup\{\mathrm{rank}(y) + 1 \mid y \in x\}$. Then for all $y \in x$, we have $y \in V_\alpha$. So $x \subseteq V_\alpha$ as required. □

The ordinals can be viewed as the backbone of the universe of sets; each V_α can be thought of as resting on the ordinal α.

Remark. The V_α are called the *von Neumann hierarchy*. The above proof shows that for all x, $\mathrm{rank}(x) = \sup\{\mathrm{rank}(y) + 1 \mid y \in x\}$. For example, the rank of $\{\{2, 3\}, 6\}$ is

$$\sup\{\mathrm{rank}\{2, 3\} + 1, 6 + 1\} = \sup\{5, 7\} = 7$$

6 Cardinals

6.1 Definitions

We will study the possible sizes of sets in ZFC. Write $x \leftrightarrow y$ if there exists a bijection from x to y; we wish to define $\mathrm{card}(x) = |x|$ such that $x \leftrightarrow y$ if and only if $\mathrm{card}(x) = \mathrm{card}(y)$. This cannot be formulated as an equivalence class, due to Russell's paradox. However, for any x, there exists an ordinal α such that $x \leftrightarrow \alpha$ by the well-ordering theorem. Hence, we can define $\mathrm{card}(x)$ to be the least ordinal that x bijects with. We say that a set m is a *cardinality* or a *cardinal* if $m = \mathrm{card}(x)$ for some set x.

If we were studying sets in ZF and not ZFC, there may not be an ordinal that bijects with a given set x. However, we can apply *Scott's trick*, which is as follows. We can consider the least α such that there exists $y \leftrightarrow x$ with $\mathrm{rank}(y) = \alpha$. This is often called the *essential rank* of x. In this case, we let $\mathrm{card}(x)$ be the set $\{y \subseteq V_\alpha \mid y \leftrightarrow x\}$.

6.2 The hierarchy of alephs

An ordinal is *initial* if it does not biject with any smaller ordinal. Any finite ordinal is initial, and ω, ω_1 are initial. For any set x, $\gamma(x)$ is initial. ω^2 is not initial as it bijects with ω. We define ω_α for each ordinal α by recursion.

- $\omega_0 = \omega$;
- $\omega_{\alpha+1} = \gamma(\omega_\alpha)$;
- $\omega_\lambda = \sup\{\omega_\alpha \mid \alpha < \lambda\}$ for a nonzero limit ordinal λ.

Each of these ordinals is initial, and every initial ordinal β is of the form ω_α. Indeed, the ω_α are unbounded, as $\omega_\alpha \geq \alpha$ for each α by induction, so there exists a least ordinal δ such that $\beta < \omega_\delta$. δ must be a successor, otherwise $\omega_\delta = \sup\{\omega_\alpha \mid \alpha < \beta\}$, contradicting the definition of δ. So $\delta = \alpha + 1$, so $\omega_\alpha \leq \beta < \omega_{\alpha+1}$. Hence $\beta = \omega_\alpha$, otherwise we contradict $\omega_{\alpha+1} = \gamma(\omega_\alpha)$.

Since we have potentially different definitions of cardinals, we will write $\aleph_\alpha$ for $\mathrm{card}(\omega_\alpha)$ to avoid ambiguity. The $\aleph_\alpha$ are precisely the cardinalities of the infinite sets. In ZF without AC, the $\aleph_\alpha$ are the cardinalities of the well-orderable sets.

For cardinals m, n, we write $m \leq n$ if there exists an injection from M to N where $\mathrm{card}(M) = m, \mathrm{card}(N) = n$. Similarly, we write $m < n$ if $m \leq n$ and $m \neq n$. For example, $\mathrm{card}(\omega) < \mathrm{card}(\mathcal{P}(\omega))$. By the Schröder–Bernstein theorem, if $m \leq n$ and $n \leq m$, then $m = n$. Hence, $\leq$ is a partial order on cardinals. This is in fact a total order in ZFC, since we can well-order the two sets in question, and one injects into the other; alternatively, the $\aleph$ numbers are clearly totally ordered.

6.3 Cardinal arithmetic

Let m, n be cardinals. Then,

(i) $m + n = \mathrm{card}(M \amalg N)$;

(ii) $m \cdot n = \mathrm{card}(M \times N)$;

(iii) $m^n = \mathrm{card}(M^N)$;

where $m = \mathrm{card}(M), n = \mathrm{card}(N)$, and M^N is the set of functions $N \to M$. The choice of representatives M, N do not influence the result. We can also define $\sum_{i\in I} m_i = \mathrm{card}\left(\coprod_{i\in I} M_i\right)$; this is only well-defined assuming the axiom of choice, as forming the bijection requires infinitely many choices.

Example. $\mathbb{R}, \mathcal{P}(\omega), \{0,1\}^\omega$ biject. Hence, $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathcal{P}(\omega)) = 2^{\aleph_0}$. In particular, cardinal exponentiation and ordinal exponentiation do not coincide, as $2^\omega = \omega$.

The cardinality of the set of sequences of reals is

$$\mathrm{card}(\mathbb{R}^\omega) = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$$

Note that this statement requires that addition and multiplication are commutative, $\aleph_0 \cdot \aleph_0 = \aleph_0$ as $\omega \times \omega$ bijects with ω, and that $(m^n)^p = m^{np}$. The latter holds as $(M^N)^P$ is the set of functions $P \to (N \to M)$, and $M^{N \times P}$ is the set of functions $N \times P \to M$.

Theorem. $m^2 = m$ for all infinite cardinals m.

Proof. We show by induction that $\aleph_\alpha^2 = \aleph_\alpha$ for all α. Define a well-ordering of $\omega_\alpha \times \omega_\alpha$ by 'going up in squares':

$$\begin{aligned}(x,y) < (z,w) \iff &(\max(x,y) < \max(z,w)) \vee \\ &(\max(x,y) = \max(z,w) = \beta \\ &\quad \wedge (y < \beta, z < \beta \vee x = z = \beta, y < w \vee y = w = \beta, x < z))\end{aligned}$$

For any $\delta \in \omega_\alpha \times \omega_\alpha$, $\delta \in \beta \times \beta$ for some $\beta < \omega_\alpha$, as ω_α is a limit ordinal. By induction, we can assume $\beta \times \beta$ bijects with β (or β is finite). Hence, the initial segment I_δ is contained in $\beta \times \beta$ and hence has cardinality at most $\mathrm{card}(\beta \times \beta) < \mathrm{card}(\omega_\alpha)$.

Therefore, the well-ordering has order type at most ω_α. Thus, $\omega_\alpha \times \omega_\alpha$ injects into ω_α, and the converse injection is trivial. So $\omega_\alpha \times \omega_\alpha$ bijects with ω_α. □

Corollary. For any ordinals $\alpha < \beta$, we have $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$.

Proof.

$$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq 2 \cdot \aleph_\beta \leq \aleph_\alpha \aleph_\beta \leq \aleph_\beta^2 = \aleph_\beta$$

□

Hence, for example, $X \sqcup X$ bijects with X for any infinite set X.

Cardinal exponentiation is not as simple as addition and multiplication. For instance, in ZF, $2^{\aleph_0}$ need not even be an aleph number, for instance if $\mathbb{R}$ is not well-orderable. In ZFC, the statement $2^{\aleph_0} = \aleph_1$ is independent of the axioms; this is called the *continuum hypothesis*. ZFC does not even decide if $2^{\aleph_0} < 2^{\aleph_1}$. Even today, not all implications about cardinal exponentiation (such as $\aleph_\alpha^{\aleph_\beta}$) are known.

7 Incompleteness

We aim to show that PA is incomplete: there is a sentence p such that PA does not prove p or $\neg p$. Equivalently, there is a sentence p that is true in $\mathbb{N}$ but PA $\nvdash p$. In this section, by 'true' we mean true in $\mathbb{N}$, and by 'unprovable' we mean PA does not prove it, so more concisely we wish to find an unprovable true sentence. Our aim is to find a sentence p that asserts that it is not provable in PA; then p is true if and only if p is not provable. Then the proof is complete, as if p is false, p is provable and hence true by soundness.

7.1 Definability

Recall that a subset $S \subseteq \mathbb{N}$ is *definable* if there is a formula p with free variable x such that $m \in S$ if and only if $p(m)$ is true. For example, the set of primes is definable, taking $p(x)$ to be $(x \neq 1) \wedge (\forall y)(\forall z)(yz = x \Rightarrow (y = 1) \vee (z = 1))$. We might say that '$m$ is prime' is definable.

A function $f : \mathbb{N} \to \mathbb{N}$ is similarly called definable if there is a formula p with free variables x, y such that $f(m) = n$ if and only if $p(m, n)$ is true. The function $f(x) = \left\lfloor \frac{x}{2} \right\rfloor$ is definable, setting $p(x, y)$ to be $(x = 2y) \vee (x = 2y + 1)$. Similarly, x^2 is definable. In fact, any function f given by an algorithm is definable in PA, but this will not be proven in this section.

7.2 Coding

L has symbols

$$0, s, +, \cdot, =, \bot, \Rightarrow, (,), \forall, x, '$$

labelling each variable x, x', x'' and so on. We code each symbol by assigning it a number, so $v(0) = 1, \dots, v(') = 12$. A formula p is encoded by

$$c(p) = 2^{v(\text{first symbol})} 3^{v(\text{second symbol})} \dots n\text{th prime}^{v(n\text{th symbol})}$$

For instance, if p is the assertion $(\forall x)(x = 0)$, then

$$c(p) = 2^8 3^{10} 5^{11} 7^9 11^8 13^{11} 17^5 19^1 23^9$$

Clearly, not all numbers encode formulae. We will write S_n for the formula encoded by n, with $S_n = \bot$ if n does not encode a formula. Observe that the statement 'n codes a formula' is definable, as there is an algorithm to decide it.

The statement 'l, m, n code formulae and S_n is obtained from S_l, S_m by modus ponens' is definable. The analogous statement for generalisation is also definable in a similar way. The axioms of PA are clearly definable, and 'n codes a logical axiom or axiom of PA' is definable. Given formulae $p_1, \dots, p_n$, we code the sequence as

$$s(p_1, \dots, p_n) = 2^{c(p_1)} 3^{c(p_2)} \dots n\text{th prime}^{c(p_n)}$$

Thus, 'n codes a proof' is definable, and 'n codes a proof of S_m' is definable. Let $\theta(m, n)$ be a formula defining 'n codes a proof of S_m'. Let $\phi(m) =$ 'S_m is provable' is definable, as $\phi(m) = (\exists n)(\theta(m, n))$.

7.3 Gödel's incompleteness theorem

Consider $\chi(m) =$ 'm codes a formula S_m with one free variable, and $S_m(m)$ is unprovable'. This is definable, so is given by some formula $p(x)$, so $\chi(m)$ holds if and only if $p(m)$ holds. Let N be the code for $p(x)$. Then, $p(N)$ is the assertion that N codes a formula S_N with one free variable, such that $S_N(N)$ is unprovable. Note that $S_N = p$ and $S_N(N) = p(N)$, so $p(N)$ asserts that $p(N)$ is unprovable. The sentence $p(N)$ suffices for the above argument, so we have shown the following theorem.

Theorem. PA is incomplete.

Note that if our proof above could be written in PA, we would then have that $p(N)$ is provable in PA. One can check that the proof used the fact that a model of PA exists (namely, $\mathbb{N}$, although this was not particularly important). We thus used the statement $\mathrm{Con}(\mathsf{PA})$, that PA is consistent, or equivalently,

$$(\forall x)(x \text{ does not code a proof of } \bot)$$

Thus, our proof above formalises to the statement

$$\mathsf{PA} \cup \{\mathrm{Con}(\mathsf{PA})\} \vdash p(N)$$

The next theorem then follows.

Theorem. $\mathsf{PA} \nvdash \mathrm{Con}(\mathsf{PA})$.

PA is incomplete, but we cannot add any true sentence t to obtain a complete theory. Indeed, the proof above can be performed on this new theory $\mathsf{PA} \cup \{t\}$ to show that it is incomplete. However, PA can certainly be extended to some complete theory by taking the set of all sentences that hold in $\mathbb{N}$. We cannot use the above proof to show that T is incomplete, since this would immediately derive a contradiction. Almost all of the above proof is still valid, so the only invalid part must lead to this contradiction; there must be no algorithm to decide truth of sentences in PA.

Theorem. T is not decidable.

Note that $\mathsf{ZFC} \vdash \mathrm{Con}(\mathsf{PA})$, where $\mathrm{Con}(\mathsf{PA})$ represents the sentence

$$(\forall x \in \omega)(x \text{ does not code a proof of } \bot)$$

This is because ZFC proves that PA has a model, namely ω. However, as for the above theorems, we obtain the following.

Theorem. ZFC is incomplete (if ZFC is consistent).

Theorem. $\mathsf{ZFC} \nvdash \mathrm{Con}(\mathsf{ZFC})$ (if ZFC is consistent).