# Part II — Logic and Set Theory

## Theorems with proof

Based on lectures by I. B. Leader

Notes taken by Dexter Chua

Lent 2015



*No specific prerequisites.*

**Ordinals and cardinals**
Well-orderings and order-types. Examples of countable ordinals. Uncountable ordinals and Hartogs' lemma. Induction and recursion for ordinals. Ordinal arithmetic. Cardinals; the hierarchy of alephs. Cardinal arithmetic. [5]

**Posets and Zorn's lemma**
Partially ordered sets; Hasse diagrams, chains, maximal elements. Lattices and Boolean algebras. Complete and chain-complete posets; fixed-point theorems. The axiom of choice and Zorn's lemma. Applications of Zorn's lemma in mathematics. The well-ordering principle. [5]

**Propositional logic**
The propositional calculus. Semantic and syntactic entailment. The deduction and completeness theorems. Applications: compactness and decidability. [3]

**Predicate logic**
The predicate calculus with equality. Examples of first-order languages and theories. Statement of the completeness theorem; *sketch of proof*. The compactness theorem and the Lowenheim-Skolem theorems. Limitations of first-order logic. Model theory. [5]

**Set theory**
Set theory as a first-order theory; the axioms of ZF set theory. Transitive closures, epsilon-induction and epsilon-recursion. Well-founded relations. Mostowski's collapsing theorem. The rank function and the von Neumann hierarchy. [5]

**Consistency**
*Problems of consistency and independence* [1]

# Contents

# 0 Introduction

# 1 Propositional calculus

## 1.1 Propositions

## 1.2 Semantic entailment

**Proposition.**

(i) If $v$ and $v'$ are valuations with $v(p) = v'(p)$ for all $p \in P$, then $v = v'$.

(ii) For any function $w : P \to \{0, 1\}$, we can extend it to a valuation $v$ such that $v(p) = w(p)$ for all $p \in L$.

*Proof.*

(i) Recall that $L$ is defined inductively. We are given that $v(p) = v'(p)$ on $L_0$. Then for all $p \in L_1$, $p$ must be in the form $q \Rightarrow r$ for $q, r \in L_0$. Then $v(q \Rightarrow r) = v(p \Rightarrow q)$ since the value of $v$ is uniquely determined by the definition. So for all $p \in L_1$, $v(p) = v'(p)$.

Continue inductively to show that $v(p) = v'(p)$ for all $p \in L_n$ for any $n$.

(ii) Set $v$ to agree with $w$ for all $p \in P$, and set $v(\bot) = 0$. Then define $v$ on $L_n$ inductively according to the definition. □

## 1.3 Syntactic implication

**Proposition** (Deduction theorem)**.** Let $S \subset L$ and $p, q \in L$. Then we have

$$S \vdash (p \Rightarrow q) \quad \Leftrightarrow \quad S \cup \{p\} \vdash q.$$

This says that $\vdash$ behaves like the connective $\Rightarrow$ in the language.

*Proof.* ($\Rightarrow$) Given a proof of $p \Rightarrow q$ from $S$, append the lines

- $p$ Hypothesis
- $q$ MP

to obtain a proof of $q$ from $S \cup \{p\}$.

($\Leftarrow$) Let $t_1, t_2, \cdots, t_n = q$ be a proof of $q$ from $S \cup \{p\}$. We'll show that $S \vdash p \Rightarrow t_i$ for all $i$.

We consider different possibilities of $t_i$:

- $t_i$ is an axiom: Write down
  - $t_i \Rightarrow (p \Rightarrow t_i)$ Axiom 1
  - $t_i$ Axiom
  - $p \Rightarrow t_i$ MP
- $t_i \in S$: Write down
  - $t_i \Rightarrow (p \Rightarrow t_i)$ Axiom 1
  - $t_i$ Hypothesis
  - $p \Rightarrow t_i$ MP

- $t_i = p$: Write down our proof of $p \Rightarrow p$ from our example above.
- $t_i$ is obtained by MP: we have some $j, k < i$ such that $t_k = (t_j \Rightarrow t_i)$. We can assume that $S \vdash (p \Rightarrow t_j)$ and $S \vdash (p \Rightarrow t_k)$ by induction on $i$. Now we can write down
  - $[p \Rightarrow (t_j \Rightarrow t_i)] \Rightarrow [(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)]$ Axiom 2
  - $p \Rightarrow (t_j \Rightarrow t_i)$ Known already
  - $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ MP
  - $p \Rightarrow t_j$ Known already
  - $p \Rightarrow t_i$ MP

  to get $S \models (p \Rightarrow t_i)$.

This is the reason why we have this weird-looking Axiom 2 — it enables us to easily prove the deduction theorem. □

**Proposition** (Soundness theorem)**.** If $S \vdash t$, then $S \models t$.

*Proof.* Given valuation $v$ with $v(s) = 1$ for all $s \in S$, we need to show that $v(t) = 1$. We will show that every line $t_i$ in the proof has $v(t_i) = 1$.

If $t_i$ is an axiom, then $v(t_i) = 1$ since axioms are tautologies. If $t_i$ is a hypothesis, then by assumption $v(s) = 1$. If $t_i$ is obtained by modus ponens, say from $t_j \Rightarrow t_i$, since $v(t_j) = 1$ and $v(t_j \Rightarrow t_i) = 1$, we must have $v(t_i) = 1$. □

**Theorem** (Model existence theorem)**.** If $S \models \bot$, then $S \vdash \bot$. i.e. if $S$ has no model, then $S$ is inconsistent. Equivalently, if $S$ is consistent, then $S$ has a model.

**Lemma.** For consistent $S \subset L$ and $p \in L$, at least one of $S \cup \{p\}$ and $S \cup \{\neg p\}$ is consistent.

*Proof.* Suppose instead that both $S \cup \{p\} \vdash \bot$ and $S \cup \{\neg p\} \vdash \bot$. Then by the deduction theorem, $S \vdash p$ and $S \vdash \neg p$. So $S \vdash \bot$, contradicting consistency of $S$. □

*Proof.* Assuming that $L$ is countable, list $L$ as $\{t_1, t_2, \cdots\}$.

Let $S_0 = S$. Then at least one of $S \cup \{t_1\}$ and $S \cup \{\neg t_1\}$ is consistent. Pick $S_1$ to be the consistent one. Then let $S_2 = S_1 \cup \{t_2\}$ or $S_1 \cup \{\neg t_2\}$ such that $S_2$ is consistent. Continue inductively.

Set $\bar{S} = S_0 \cup S_1 \cup S_2 \cdots$. Then $p \in \bar{S}$ or $\neg p \in \bar{S}$ for each $p \in L$ by construction. Also, we know that $\bar{S}$ is consistent. If we had $\bar{S} \vdash \bot$, then since proofs are finite, there is some $S_n$ that contains all assumptions used in the proof of $\bar{S} \vdash \bot$. Hence $S_n \vdash \bot$, but we know that all $S_n$ are consistent.

Finally, we check that $\bar{S}$ is deductively closed: if $\bar{S} \vdash p$, we must have $p \in \bar{S}$. Otherwise, $\neg p \in \bar{S}$. But this implies that $\bar{S}$ is inconsistent.

Define $v : L \to \{0, 1\}$ by

$$p \mapsto \begin{cases} 1 & \text{if } p \in \bar{S} \\ 0 & \text{if not} \end{cases}.$$

All that is left to show is that this is indeed a valuation.

First of all, we have $v(\bot) = 0$ as $\bot \notin \bar{S}$ (since $\bar{S}$ is consistent).

For $p \Rightarrow q$, we check all possible cases.

(i) If $v(p) = 1, v(q) = 0$, we have $p \in \bar{S}$, $q \notin \bar{S}$. We want to show $p \Rightarrow q \notin \bar{S}$. Suppose instead that $p \Rightarrow q \in \bar{S}$. Then $\bar{S} \vdash q$ by modus ponens. Hence $q \in \bar{S}$ since $\bar{S}$ is deductively closed. This is a contradiction. Hence we must have $v(p \Rightarrow q) = 0$.

(ii) If $v(q) = 1$, then $q \in \bar{S}$. We want to show $p \Rightarrow q \in \bar{S}$. By our first axiom, we know that $\vdash q \Rightarrow (p \Rightarrow q)$. So $\bar{S} \vdash p \Rightarrow q$. So $p \Rightarrow q \in \bar{S}$ by deductive closure. Hence we have $v(p \Rightarrow q) = 1$.

(iii) If $v(p) = 0$, then $p \notin \bar{S}$. So $\neg p \in \bar{S}$. We want to show $p \Rightarrow q \in \bar{S}$.

- This is equivalent to showing $\neg p \vdash p \Rightarrow q$.
- By the deduction theorem, this is equivalent to proving $\{p, \neg p\} \vdash q$.
- We know that $\{p, \neg p\} \vdash \bot$. So it is sufficient to show $\bot \vdash q$.
- By axiom 3, this is equivalent to showing $\bot \vdash \neg\neg q$.
- By the deduction theorem, this is again equivalent to showing $\vdash \bot \Rightarrow \neg\neg q$.
- By definition of $\neg$, this is equivalent to showing $\vdash \bot \Rightarrow (\neg q \Rightarrow \bot)$.

But this is just an instance of the first axiom. So we know that $\bar{S} \vdash p \Rightarrow q$. So $v(p \Rightarrow q) = 1$. □

**Corollary** (Adequacy theorem)**.** Let $S \subset L$, $t \in L$. Then $S \models t$ implies $S \vdash t$.

**Theorem** (Completeness theorem)**.** Le $S \subset L$ and $t \in L$. Then $S \models t$ if and only if $S \vdash t$.

**Corollary** (Compactness theorem)**.** Let $S \subset L$ and $t \in L$ with $S \models t$. Then there is some finite $S' \subset S$ has $S' \models t$.

*Proof.* Trivial with $\models$ replaced by $\vdash$, because proofs are finite. □

**Corollary** (Decidability theorem)**.** Let $S \subset L$ be a finite set and $t \in L$. Then there exists an algorithm that determines, in finite and bounded time, whether or not $S \vdash t$.

*Proof.* Trivial with $\vdash$ replaced by $\models$, by making a truth table. □

# 2 Well-orderings and ordinals

## 2.1 Well-orderings

**Proposition.** A total order is a well-ordering if and only if it has no infinite strictly decreasing sequence.

*Proof.* If $x_1 > x_2 > x_3 > \cdots$, then $\{x_i : i \in \mathbb{N}\}$ has no least element.

Conversely, if non-empty $S \subset X$ has no least element, then each $x \in S$ have $x' \in S$ with $x' < x$. Similarly, we can find some $x'' < x'$ *ad infinitum*. So

$$x > x' > x'' > x''' > \cdots$$

is an infinite decreasing sequence. □

**Proposition** (Principle by induction)**.** Let $X$ be a well-ordered set. Suppose $S \subseteq X$ has the property:

$$(\forall x)\Big(\big((\forall y)\, y < x \Rightarrow y \in S\big) \Rightarrow x \in S\Big),$$

then $S = X$.

In particular, if a property $P(x)$ satisfies

$$(\forall x)\Big(\big((\forall y)\, y < x \Rightarrow P(y)\big) \Rightarrow P(x)\Big),$$

then $P(x)$ for all $x$.

*Proof.* Suppose $S \neq X$. Let $x$ be the least element of $X \setminus S$. Then by minimality of $x$, for all $y$, $y < x \Rightarrow y \in S$. Hence $x \in S$. Contradiction. □

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

*Proof.* Let $f$ and $g$ be two isomorphisms $X \to Y$. To show that $f = g$, it is enough, by induction, to show $f(x) = g(x)$ given $f(y) = g(y)$ for all $y < x$.

Given a fixed $x$, let $S = \{f(y) : y < x\}$. We know that $Y \setminus S$ is non-empty since $f(x) \notin S$. So let $a$ be the least member of $Y \setminus S$. Then we must have $f(x) = a$. Otherwise, we will have $a < f(x)$ by minimality of $a$, which implies that $f^{-1}(a) < x$ since $f$ is order-preserving. However, by definition of $S$, this implies that $a = f(f^{-1}(a)) \in S$. This is a contradiction since $a \in Y \setminus S$.

By the induction hypothesis, for $y < x$, we have $f(y) = g(y)$. So we have $S = \{g(y) : y < x\}$ as well. Hence $g(x) = \min(Y \setminus S) = f(x)$. □

**Proposition.** Every initial segment $Y$ of a well-ordered set $X$ is of the form $I_x = \{y \in X : y < x\}$.

*Proof.* Take $x = \min X \setminus Y$. Then for any $y \in I_x$, we have $y < x$. So $y \in Y$ by definition of $x$. So $I_x \subseteq Y$.

On the other hand, if $y \in Y$, then definitely $y \neq x$. We also cannot have $y > x$ since this implies $x \in Y$. Hence we must have $y < x$. So $y \in I_x$. Hence $Y \subseteq I_x$. So $Y = I_x$. □

**Theorem** (Definition by recursion)**.** Let $X$ be a well-ordered set and $Y$ be any set. Then for any function $G : \mathbb{P}(X \times Y) \to Y$, there exists a function $f : X \to Y$ such that

$$f(x) = G(f|_{I_x})$$

for all $x$.

This is a rather weird definition. Intuitively, it means that $G$ takes previous values of $f(x)$ and returns the desired output. This means that in defining $f$ at $x$, we are allowed to make use of values of $f$ on $I_x$. For example, we define $f(n) = nf(n-1)$ for the factorial function, with $f(0) = 1$.

*Proof.* We might want to jump into the proof and define $f(0) = G(\emptyset)$, where 0 is the minimum element. Then we define $f(1) = G(f(0))$ etc. But doing so is simply recursion, which is the thing we want to prove that works!

Instead, we use the following clever trick: We define an "$h$ is an attempt" to mean

$$h : I \to Y \text{ for some initial segment } I \text{ of } X, \text{ and } h(x) = G(h|_{I_x}) \text{ for } x \in I.$$

The idea is to show that for any $x$, there is an attempt $h$ that is defined at $x$. Then take the value $f(x)$ to be $h(x)$. However, we must show this is well-defined first:

**Claim.** If attempts $h$ and $h'$ are defined at $x$, then $h(x) = h'(x)$.

By induction on $x$, it is enough to show that $h(x) = h'(x)$ assuming $h(y) = h'(y)$ for all $y < x$. But then $h(x) = G(h|_{I_x}) = G(h'|_{I_x}) = h'(x)$. So done.

**Claim.** For any $x$, there must exist an attempt $h$ that is defined at $x$.

Again, we may assume (by induction) that for each $y < x$, there exists an attempt $h_y$ defined at $y$. Then we put all these functions together, and take $h' = \bigcup_{y<x} h_y$. This is defined for all $y < x$, and is well-defined since the $h_y$ never disagree.

Finally, add to it $(x, G(h'|_{I_x}))$. Then $h = h' \cup (x, G(h'|_{I_x}))$ is an attempt defined at $x$.

Now define $f : X \to Y$ by $f(x) = y$ if there exists an attempt $h$, defined at $x$, with $h(x) = y$.

**Claim.** There is a unique such $f$.

Suppose $f$ and $f'$ both work. Then if $f(y) = f'(y)$ for all $y < x$, then $f(x) = f'(x)$ by definition. So by induction, we know for all $x$, we have $f'(x) = f(x)$. □

**Lemma** (Subset collapse)**.** Let $X$ be a well-ordering and let $Y \subseteq X$. Then $Y$ is isomorphic to an initial segment of $X$. Moreover, this initial segment is unique.

*Proof.* For $f : Y \to X$ to be an order-preserving bijection with an initial segment of $X$, we need to map $x$ to the smallest thing not yet mapped to, i.e.

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

To be able to take the minimum, we have to make sure the set is non-empty, i.e. $\{f(y) : y < x\} \neq X$. We can show this by proving that $f(z) < x$ for all $z < x$ by induction, and hence $x \notin \{f(y) : y < x\}$.

Then by the recursion theorem, this function exists and is unique. □

**Theorem.** Let $X, Y$ be well-orderings. Then $X \leq Y$ or $Y \leq X$.

*Proof.* We attempt to define $f : X \to Y$ by

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

By the law of excluded middle, this function is either well-defined or not.

If it is well-defined, then it is an isomorphism from $X$ to an initial segment of $Y$.

If it is not, then there is some $x$ such that $\{f(y) : y < x\} = Y$ and we cannot take the minimum. Then $f$ is a bijection between $I_x = \{y : y < x\}$ and $Y$. So $f$ is an isomorphism between $Y$ and an initial segment of $X$.

Hence either $X \leq Y$ or $Y \leq X$. □

**Theorem.** Let $X, Y$ be well-orderings with $X \leq Y$ and $Y \leq X$. Then $X$ and $Y$ are isomorphic.

*Proof.* Since $X \leq Y$, there is an order-preserving function $f : X \to Y$ that bijects $X$ with an initial segment of $Y$. Similarly, since $Y \leq X$, we get an analogous $g : Y \to X$. Then $g \circ f : X \to X$ defines a bijection between $X$ and an initial segment of $X$.

Since there is no bijection between $X$ and a *proper* initial segment of itself, the image of $g \circ f$ must be $X$ itself. Hence $g \circ f$ is a bijection.

Similarly, $f \circ g$ is a bijection. Hence $f$ and $g$ are both bijections, and $X$ and $Y$ are isomorphic. □

## 2.2 New well-orderings from old

**Proposition.** Let $\{X_i : i \in I\}$ be a nested set of well-orderings. Then there exists a well-ordering $X$ with $X_i \leq X$ for all $i$.

*Proof.* Let $X = \bigcup_{i \in I} X_i$ with $<$ defined on $X$ as $\bigcup_{i \in I} <_i$ (where $<_i$ is the ordering of $X_i$), i.e. we inherit the orders from the $X_i$'s. This is clearly a total ordering. Since $\{X_i : i \in I\}$ is a nested family, each $X_i$ is an initial segment of $X$.

To show that it is a well-ordering, let $S \subseteq X$ be a non-empty subset of $X$. Then $S \cap X_i$ is non-empty for some $i$. Let $x$ be the minimum element (in $X_i$) of $S \cap X_i$. Then also for any $y \in S$, we must have $x \leq y$, as $X_i$ is an initial segment of $X$. □

## 2.3 Ordinals

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

*Proof.* Let $X$ have order type $\alpha$. The well-orderings $< X$ are precisely (up to isomorphism) the proper initial segments of $X$ (by uniqueness of subset collapse). But these are the $I_x$ for all $x \in X$. So we can biject $X$ with the well-orderings $< X$ by $x \mapsto I_x$. □

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

*Proof.* Choose $\alpha \in S$. If it is minimal, done.

If not, then $S \cap I_\alpha$ is non-empty. But $I_\alpha$ is well-ordered. So $S \cap I_\alpha$ has a least element, $\beta$. Then this is a minimal element of $S$. □

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

*Proof.* Suppose not. Let $X$ be the set of ordinals. Then $X$ is a well-ordering. Let its order-type be $\alpha$. Then $X$ is isomorphic to $I_\alpha$, a proper initial subset of $X$. Contradiction. □

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

*Proof.* This is easy by looking at the supremum of the set of all countable ordinals. However, this works only if the collection of countable ordinals is a set.

Let $A = \{R \in \mathbb{P}(\mathbb{N} \times \mathbb{N}) : R \text{ is a well-ordering of a subset of } \mathbb{N}\}$. So $A \subseteq \mathbb{P}(\mathbb{N} \times \mathbb{N})$. Then $B = \{\text{order type of } R : R \in A\}$ is the set of all countable ordinals.

Let $\omega_1 = \sup B$. Then $\omega_1$ is uncountable. Indeed, if $\omega_1$ were countable, then it would be the greatest countable ordinal, but $\omega_1 + 1$ is greater and is also countable. □

**Theorem** (Hartogs' lemma)**.** For any set $X$, there is an ordinal that does not inject into $X$.

*Proof.* As before, with $B = \{\alpha : \alpha \text{ injects into } X\}$. □

## 2.4 Successors and limits

## 2.5 Ordinal arithmetic

**Proposition.** Addition is associative, i.e. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

*Proof.* Since we define addition by recursion, it makes sense to prove this by induction. Since we recursed on the right-hand term in the definition, it only makes sense to induct on $\gamma$ (and fix $\alpha + \beta$).

(i) If $\gamma = 0$, then $\alpha + (\beta + 0) = \alpha + \beta = (\alpha + \beta) + 0$.

(ii) If $\gamma = \delta^+$ is a successor, then

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

(iii) If $\gamma$ is a limit ordinal, we have

$$\begin{aligned}(\alpha + \beta) + \lambda &= \sup\{(\alpha + \beta) + \gamma : \gamma < \lambda\} \\ &= \sup\{\alpha + (\beta + \gamma) : \gamma < \lambda\}\end{aligned}$$

If we want to evaluate $\alpha + (\beta + \lambda)$, we have to first know whether $\beta + \lambda$ is a successor or a limit. We now claim it is a limit:

$\beta + \lambda = \sup\{\beta + \gamma : \gamma < \lambda\}$. We show that this cannot have a greatest element: for any $\beta + \gamma$, since $\lambda$ is a limit ordinal, we can find a $\gamma'$ such that $\gamma < \gamma' < \lambda$. So $\beta + \gamma' > \beta + \gamma$. So $\beta + \gamma$ cannot be the greatest element.

So

$$\alpha + (\beta + \lambda) = \sup\{\alpha + \delta : \delta < \beta + \lambda\}.$$

We need to show that

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

Note that the two sets are not equal. For example, if $\beta = 3$ and $\lambda = \omega$, then the left contains $\alpha + 2$ but the right does not.

So we show that the left is both $\geq$ and $\leq$ the right.

$\geq$: Each element of the right hand set is an element of the left.

$\leq$: For $\delta < \beta + \lambda$, we have $\delta < \sup\{\beta + \gamma : \gamma < \lambda\}$. So $\delta < \beta + \gamma$ for some $\gamma < \lambda$. Hence $\alpha + \delta < \alpha + (\beta + \gamma)$. □

**Proposition.** The inductive and synthetic definition of + coincide.

*Proof.* Write + for inductive definition, and $+'$ for synthetic. We want to show that $\alpha + \beta = \alpha +' \beta$. We induct on $\beta$.

(i) $\alpha + 0 = \alpha = \alpha +' 0$.

(ii) $\alpha + \beta^+ = (\alpha + \beta)^+ = (\alpha +' \beta)^+ = \text{otp}\underbrace{\alpha}\underbrace{\beta}\underbrace{\cdot} = \alpha +' \beta^+$

(iii) $\alpha + \lambda = \sup\{\alpha + \gamma : \gamma < \lambda\} = \sup\{\alpha +' \gamma : \gamma < \lambda\} = \alpha +' \lambda$. This works because taking the supremum is the same as taking the union.

$$\underbrace{\alpha}\underbrace{\gamma \quad \gamma' \, \gamma'' \cdots \lambda}$$

□

## 2.6 Normal functions*

**Lemma.** Let $f$ be a normal function. Then $f$ is strictly increasing.

*Proof.* Let $\alpha$ be a fixed ordinal. We induct on all $\beta > \alpha$ that $f(\alpha) < f(\beta)$.

If $\beta = \alpha^+$, then the result is obvious.

If $\beta = \gamma^+$ with $\gamma \neq \alpha$, then $\alpha < \gamma$. So $f(\alpha) < f(\gamma) < f(\gamma^+) = f(\beta)$ by induction.

If $\beta$ is a limit and is greater than $\alpha$, then

$$f(\beta) = \sup\{f(\gamma) : \gamma < \beta\} \geq f(\alpha^+) > f(\alpha),$$

since $\alpha^+ < \beta$. So the result follows. □

**Lemma.** Let $f$ be a normal function, and $\alpha$ an ordinal. Then $f(\alpha) \geq \alpha$.

*Proof.* We prove by induction. It is trivial for zero. For successors, we have $f(\alpha^+) > f(\alpha) \geq \alpha$, so $f(\alpha^+) \geq \alpha^+$. For limits, we have

$$f(\lambda) = \sup\{f(\gamma) : \gamma < \lambda\} \geq \sup\{\gamma : \gamma < \lambda\} = \lambda.$$ □

**Lemma.** If $f$ is a normal function, then for any non-empty set $\{\alpha_i\}_{i\in I}$, we have

$$f(\sup\{\alpha_i : i \in I\}) = \sup\{f(\alpha_i) : i \in I\}.$$

*Proof.* If $\{\alpha_i\}$ has a maximal element, then the result is obvious, as $f$ is increasing, and the supremum is a maximum.

Otherwise, let

$$\alpha = \sup\{\alpha_i : i \in I\}$$

Since the $\alpha_i$ has no maximal element, we know $\alpha$ must be a limit ordinal. So we have

$$f(\alpha) = \sup\{f(\beta) : \beta < \alpha\}.$$

So it suffices to prove that

$$\sup\{f(\beta) : \beta < \alpha\} = \sup\{f(\alpha_i) : i \in I\}.$$

Since all $\alpha_i < \alpha$, we have $\sup\{f(\beta) : \beta < \alpha\} \geq \sup\{f(\alpha_i) : i \in I\}$.

For the other direction, it suffices, by definition, to show that

$$f(\beta) \leq \sup\{f(\alpha_\gamma) : i \in I\}$$

for all $\beta < \alpha$.

Given such a $\beta$, since $\alpha$ is the supremum of the $\alpha_i$, we can find some particular $\alpha_i$ such that $\beta < \alpha_i$. So $f(\beta) < f(\alpha_i) \leq \sup\{f(\alpha_i) : i \in I\}$. So we are done. □

**Lemma** (Fixed-point lemma)**.** Let $f$ be a normal function. Then for each ordinal $\alpha$, there is some $\beta \geq \alpha$ such that $f(\beta) = \beta$.

*Proof.* We thus define

$$\beta = \sup\{f(\alpha), f(f(\alpha)), f(f(f(\alpha))), \cdots\}.$$

If the sequence eventually stops, then we have found a fixed point. Otherwise, $\beta$ is a limit ordinal, and thus normality gives

$$f(\beta) = \sup\{f(f(\alpha)), f(f(f(\alpha))), f(f(f(f(\alpha)))), \cdots\} = \beta.$$

So $\beta$ is a fixed point, and $\beta \geq f(\alpha) \geq \alpha$. □

**Lemma** (Division algorithm for normal functions)**.** Let $f$ be a normal function. Then for all $\alpha$, there is some maximal $\gamma$ such that $\alpha \geq f(\gamma)$.

*Proof.* Let $\gamma = \sup\{\beta : f(\beta) \leq \alpha\}$. Then we have

$$f(\gamma) = \sup\{f(\beta) : f(b) \leq \alpha\} \leq \alpha.$$

This is clearly maximal. □

# 3 Posets and Zorn's lemma

## 3.1 Partial orders

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

*Proof.* To show that $f(x) = x$, we need $f(x) \leq x$ and $f(x) \geq x$. Let's not be too greedy and just want half of it:

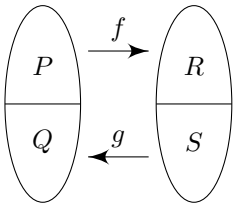
Let $E = \{x : x \leq f(x)\}$. Let $s = \sup E$. We claim that this is a fixed point, by showing $f(s) \leq s$ and $s \leq f(s)$.

To show $s \leq f(s)$, we use the fact that $s$ is the least upper bound. So if we can show that $f(s)$ is also an upper bound, then $s \leq f(s)$. Now let $x \in E$. So $x \leq s$. Therefore $f(x) \leq f(s)$ by order-preservingness. Since $x \leq f(x)$ (by definition of $E$) $x \leq f(x) \leq f(s)$. So $f(s)$ is an upper bound.

To show $f(s) \leq s$, we simply have to show $f(s) \in E$, since $s$ is an upper bound. But we already know $s \leq f(s)$. By order-preservingness, $f(s) \leq f(f(s))$. So $f(s) \in E$ by definition. □

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

*Proof.* We try to partition $A$ into $P$ and $Q$, and $B$ into $R$ and $S$, such that $f(P) = R$ and $g(S) = Q$. Then we let $h = f$ on $R$ and $g^{-1}$ on $Q$.




Since $S = B \setminus R$ and $Q = A \setminus P$, so we want

$$P = A \setminus g(B \setminus f(P))$$

Since the function $P \mapsto A \setminus g(B \setminus f(P))$ from $\mathbb{P}(A)$ to $\mathbb{P}(A)$ is order-preserving (and $\mathbb{P}(a)$ is complete), the result follows. □

**Theorem** (Zorn's lemma)**.** Assuming Axiom of Choice, let $X$ be a (non-empty) poset in which every chain has an upper bound. Then it has a maximal element.

*Proof.* Suppose not. So for each $x \in X$, we have $x' \in X$ with $x' > x$. We denote the-element-larger-than-$x$ by $x'$.

We know that each chain $C$ has an upper bound, say $u(C)$.

Let $\gamma = \gamma(X)$, the ordinal-larger-than-$X$ by Hartogs' lemma.

We pick $x \in X$, and define $x_\alpha$ for $\alpha < \gamma$ recursively by

- $x_0 = x$
- $x_{\alpha^+} = x'_\alpha$
- $x_\lambda = u(\{x_\alpha : \alpha < \lambda\})'$ for non-zero limit $\lambda$

Of course, we have to show that $\{x_\alpha : \alpha < \lambda\}$ is a chain. This is trivial by induction.

Then $\alpha \mapsto x_\alpha$ is an injection from $\gamma \to X$. Contradiction. □

**Theorem.** Every vector space $V$ has a basis.

*Proof.* We go for a maximal linearly independent subset.

Let $X$ be the set of all linearly independent subsets of $V$, ordered by inclusion. We want to find a maximal $B \in X$. Then $B$ is a basis. Otherwise, if $B$ does not span $V$, choose $x \notin \operatorname{span} B$. Then $B \cup \{x\}$ is independent, contradicting maximality.

So we have to find such a maximal $B$. By Zorn's lemma, we simply have to show that every chain has an upper bound.

Given a chain $\{A_i : i \in I\}$ in $X$, a reasonable guess is to try the union. Let $A = \bigcup A_i$. Then $A \subseteq A_i$ for all $i$, by definition. So it is enough to check that $A \in X$, i.e. is linearly independent.

Suppose not. Say $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ for some $\lambda_1 \cdots \lambda_n$ scalars (not all 0). Suppose $x_1 \in A_{i_1}, \cdots x_n \in A_{i_n}$ for some $i_1, \cdots i_n \in I$. Then there is some $A_{i_m}$ that contains all $A_{i_k}$, since they form a finite chain. So $A_{i_m}$ contains all $x_i$. This contradicts the independence of $A_{i_m}$.

Hence by Zorn's lemma, $X$ has a maximal element. Done. □

**Theorem** (Model existence theorem (uncountable case))**.** Let $S \subseteq L(P)$ for any set of primitive propositions $P$. Then if $S$ is consistent, $S$ has a model.

*Proof.* We need a consistent $\bar{S} \subseteq S$ such that $\forall t \in L$, $t \in \bar{S}$ or $\neg t \in \bar{S}$. Then we have a valuation $v(t) = \begin{cases} 1 & t \in \bar{S} \\ 0 & t \notin \bar{S} \end{cases}$, as in our original proof for the countable case.

So we seek a *maximal* consistent $\bar{S} \supseteq S$. If $\bar{S}$ is maximal, then if $t \notin \bar{S}$, then we must have $\bar{S} \cup \{t\}$ inconsistent, i.e. $\bar{S} \cup \{t\} \vdash \bot$. By deduction theorem, this means that $\bar{S} \vdash \neg t$. By maximality, we must have $\neg t \in \bar{S}$. So either $t$ or $\neg t$ is in $\bar{S}$.

Now we show that there is such a maximal $\bar{S}$. Let $X = \{T \subseteq L : T \text{ is consistent }, T \supseteq S\}$. Then $X \neq \emptyset$ since $S \in X$. We show that any non-empty chain has an upper bound. An obvious choice is, again the union.

Let $\{T_i : i \in I\}$ be a non-empty chain. Let $T = \bigcup T_i$. Then $T \supseteq T_i$ for all $i$. So to show that $T$ is an upper bound, we have to show $T \in X$.

Certainly, $T \supseteq S$, as any $T_i$ contains $S$ (and the chain is non-empty). So we want to show $T$ is consistent. Suppose $T \vdash \bot$. So we have $t_1, \cdots, t_n \in T$ with $\{t_1, \cdots, t_n\} \vdash \bot$, since proofs are finite. Then some $T_k$ contains all $t_i$ since $T_i$ are nested. So $T_k$ is inconsistent. This is a contradiction. Therefore $T$ must be consistent.

Hence by Zorn's lemma, there is a maximal element of $X$. □

## 3.2 Zorn's lemma and axiom of choice

**Axiom** (Axiom of choice)**.** Given any family $\{A_i : i \in I\}$ of non-empty sets, there is a *choice function* $f : i \to \bigcup A_i$ such that $f(i) \in A_i$.

**Theorem.** Zorn's Lemma $\Leftrightarrow$ Axiom of choice.

*Proof.* We have already proved that AC $\Rightarrow$ Zorn. We now proved the other way round.

Given a family $\{A_i : i \in I\}$ of non-empty sets. We say a *partial choice function* is a function $f : J \to \bigcup_{i\in I} A_i$ (for some $J \subseteq I$) such that $f(j) \in A$ for all $j \in J$.

Let $X = \{(J, f) : f \text{ is a partial choice function with domain } J\}$. We order by extension, i.e. $(J, f) \leq (J', f')$ iff $J \subseteq J'$ and $f'$ agrees with $f$ when both are defined.

Given a chain $\{(J_k, f_k) : k \in K\}$, we have an upper bound $(\bigcup J_k, \bigcup f_k)$, ie the function obtained by combining all functions in the chain. So by Zorn's, it has a maximal element $(J, f)$.

Suppose $J \neq I$. Then pick $i \in I \setminus J$. Then pick $x \in A_i$. Set $J' = J \cup \{i\}$ and $f' = f \cup \{(i, x)\}$. Then this is greater than $(J, f)$. This contradicts the maximality of $(J, f)$. So we must have $J = I$, i.e. $f$ is a full choice function. □

**Theorem** (Well-ordering theorem)**.** Axiom of choice $\Rightarrow$ every set $X$ can be well-ordered.

*Proof.* The idea is to pick an element from $X$ and call it the first; pick another element and call it the second, and continue transfinitely until we pick everything.

For each $A \subseteq X$ with $A \neq X$, we let $y_A$ be an element of $X \setminus A$. Here we are using Choice to pick out $y_A$.

Define $x_\alpha$ recursively: Having defined $x_\beta$ for all $\beta < \alpha$, if $\{x_\beta : \beta < \alpha\} = X$, then stop. Otherwise, set $x_\alpha = y_{\{x_\beta : \beta<\alpha\}}$, ie pick $x_\alpha$ to be something not yet chosen.

We must stop at some time. Otherwise, we have injected $\gamma(X)$ (ie the ordinal larger than $X$) into $X$, which is a contradiction. So when stop, we have bijected $X$ with an well-ordered set (i.e. $I_\alpha$, where $\alpha$ is when you've stopped). Hence we have well-ordered $X$. □

**Theorem.** Well-ordering theorem $\Rightarrow$ Axiom of Choice.

*Proof.* Given non-empty sets $\{A_i : i \in I\}$, well-order $\bigcup A_i$. Then define $f(i)$ to be the least element of $A_i$. □

## 3.3 Bourbaki-Witt theorem*

**Theorem** (Bourbaki-Witt theorem)**.** If $X$ is chain-complete and $f : X \to X$ is inflationary, then $f$ has a fixed point.

# 4 Predicate logic

## 4.1 Language of predicate logic

## 4.2 Semantic entailment

## 4.3 Syntactic implication

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

*Proof.* The proof is exactly the same as the one for propositional logic, except in the $\Rightarrow$ case, we have to check Gen.

Suppose we have lines

- $r$
- $(\forall x)r$ Gen

and we have a proof of $S \vdash p \Rightarrow r$ (by induction). We want to seek a proof of $p \Rightarrow (\forall x)r$ from $S$.

We know that no premise used in the proof of $r$ from $S \cup \{p\}$ had $x$ as a free variable, as required by the conditions of the use of Gen. Hence no premise used in the proof of $p \Rightarrow r$ from $S$ had $x$ as a free variable.

Hence $S \vdash (\forall x)(p \Rightarrow r)$.

If $x$ is not free in $p$, then we get $S \vdash p \Rightarrow (\forall x)r$ by Axiom 7 (and MP).

If $x$ *is* free in $p$, then we did not use premise $p$ in our proof $r$ from $S \cup \{p\}$ (by the conditions of the use of Gen). So $S \vdash r$, and hence $S \vdash (\forall x)r$ by Gen. So $S \vdash p \Rightarrow (\forall x)r$. □

**Proposition** (Soundness theorem)**.** Let $S$ be a set of sentences, $p$ a sentence. Then $S \vdash p$ implies $S \models p$.

*Proof.* (non-examinable) We have a proof of $p$ from $S$, and want to show that for every model of $S$, $p$ holds.

This is an easy induction on the lines of the proof, since our axioms are tautologies and our rules of deduction are sane. □

**Theorem** (Model existence lemma)**.** Let $S$ be a consistent set of sentences. Then $S$ has a model.

*Proof.* (non-examinable) Suppose we have a consistent $S$ in the language $L = L(\Omega, \Pi)$. Extend $S$ to a consistent $S_1$ such that $p \in S_1$ or $(\neg p) \in S$ for each sentence $p \in L$ (by applying Zorn's lemma to get a maximal consistent $S_1$). In particular, $S_1$ is *complete*, meaning $S_1 \vdash p$ or $S_1 \vdash \neg p$ for all $p$.

Then for each sentence of the form $(\exists x)p$ in $S_1$, add a new constant $c$ to $L$ and add $p[c/x]$ to $S_1$ — obtaining $T_1$ in language $L_1 = L(\Omega \cup C_1, \Pi)$. It is easy to check that $T_1$ is consistent.

Extend $T_1$ to a complete theory $S_2 \subseteq L_1$, and add witnesses to form $T_2 \subseteq L_2 = L(\Omega \cup C_1 \cup C_2, \Pi)$. Continue inductively.

Let $\bar{S} = S_1 \cup S_2 \cup \cdots$ in language $\bar{L} = L_1 \cup L_2 \cup \cdots$ (i.e. $\bar{L} = L(\Omega \cup C_1 \cup C_2 \cup \cdots, \Pi)$).

**Claim.** $\bar{S}$ is consistent, complete, and has witnesses, i.e. if $(\exists x)p \in \bar{S}$, then $p[t/x] \in \bar{S}$ For some term $t$.

It is consistent since if $\bar{S} \vdash \bot$, then some $S_n \vdash \bot$ since proofs are finite. But all $S_n$ are consistent. So $\bar{S}$ is consistent.

To show completeness, for sentence $p \in \bar{L}$, we have $p \in L_n$ for some $n$, as $p$ has only finitely many symbols. So $S_{n+1} \vdash p$ or $S_{n+1} \vdash \neg p$. Hence $\bar{S} \vdash p$ or $\bar{S} \vdash \neg p$.

To show existence of witnesses, if $(\exists x)p \in \bar{S}$, then $(\exists x)p \in S_n$ for some $n$. Hence (by construction of $T_n$), we have $p[c/x] \in T_n$ for some constant $c$.

Now define an equivalence relation $\sim$ on closed term of $\bar{L}$ by $s \sim t$ if $\bar{S} \vdash (s = t)$. It is easy to check that this is indeed an equivalence relation. Let $A$ be the set of equivalence classes. Define

(i) $f_A([t_1], \cdots, [t_n]) = [ft_1, \cdots, t_n]$ for each formula $f \in \Omega$, $\alpha(f) = n$.

(ii) $\phi_A = \{([t_1], \cdots, [t_n]) : \bar{S} \vdash \phi(t_1, \cdots, t_n)\}$ for each relation $\phi \in \Pi$ and $\alpha(\phi) = n$.

It is easy to check that this is well-defined.

**Claim.** For each sentence $p$, $\bar{S} \vdash p$ (i.e. $p \in \bar{S}$) if and only if $p$ holds in $A$, i.e. $p_A = 1$.

We prove this by an easy induction.

- Atomic sentences:
  - $\bot$: $\bar{S} \nvdash \bot$, and $\bot_A = 0$. So good.
  - $s = t$: $\bar{S} \vdash s = t$ iff $[s] = [t]$ (by definition) iff $s_A = t_A$ (by definition of $s_A$) iff $(s = t)_A$. So done.
  - $\phi t_1, \cdots, t_n$ is the same.
- Induction step:
  - $p \Rightarrow q$: $\bar{S} \vdash (p \Rightarrow q)$ iff $\bar{S} \vdash (\neg p)$ or $\bar{S} \vdash q$ (justification: if $\bar{S} \nvdash \neg p$ and $\bar{S} \nvdash q$, then $\bar{S} \vdash p$ and $\bar{S} \vdash \neg q$ by completeness, hence $\bar{S} \vdash \neg(p \Rightarrow q)$, contradiction). This is true iff $p_A = 0$ or $q_A = 1$ iff $(p \Rightarrow q)_A = 1$.
  - $(\exists x)p$: $\bar{S} \vdash (\exists x)p$ iff $\bar{S} \vdash p[t/x]$ for some closed term $t$. This is true since $\bar{S}$ has witnesses. Now this holds iff $p[t/x]_A = 1$ for some closed term $t$ (by induction). This is the same as saying $(\exists x)p$ holds in $A$, because $A$ is the set of (equivalence classes of) closed terms.

  Here it is convenient to pretend $\exists$ is the primitive symbol instead of $\forall$. Then we can define $(\forall x)p$ to be $\neg(\exists x)\neg p$, instead of the other way round. It is clear that the two approaches are equivalent, but using $\exists$ as primitive makes the proof look clearer here.

Hence $A$ is a model of $\bar{S}$. Hence it is also a model of $S$. So $S$ has a model. □

**Corollary** (Adequacy theorem)**.** Let $S$ be a theory, and $p$ a sentence. Then $S \models p$ implies $S \vdash p$.

**Theorem** (Gödel's completeness theorem (for first order logic))**.** Let $S$ be a theory, $p$ and sentence. Then $S \vdash p$ if and only if $S \models p$.

*Proof.* ($\Rightarrow$) Soundness, ($\Leftarrow$) Adequacy. □

**Corollary** (Compactness theorem)**.** Let $S$ be a theory such that every finite subset of $S$ has a model. Then so does $S$.

*Proof.* Trivial if we replace "has a model" with "is consistent", because proofs are finite. □

**Corollary.** The theory of finite groups cannot be axiomatized (in the language of groups).

*Proof.* Suppose theory $T$ has models all finite groups and nothing else. Let $T'$ be $T$ together with

- $(\exists x_1)(\exists x_2)(x_1 \neq x_2)$ (intuitively, $|G| \geq 2$)
- $(\exists x_1)(\exists x_2)(\exists x_3)(x_1 \neq x_2 \neq x_3)$ (intuitively, $|G| \geq 3$)
- ...

Then $T'$ has no model, since each model has to be simultaneously arbitrarily large and finite. But every finite subset of $T'$ does have a model (e.g. $\mathbb{Z}_n$ for some $n$). Contradiction. □

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

"Finiteness is not a first-order property"

*Proof.* Same as above. □

**Corollary** (Upward Löwenheim-Skolem theorem)**.** Let $S$ be a theory with an infinite model. Then $S$ has an uncountable model.

*Proof.* Add constants $\{c_i : i \in I\}$ to $L$ for some uncountable $I$.

Let $T = S \bigcup \{\text{“}c_i \neq c_j\text{”} : i, j \in I, i \neq j\}$.

Then any finite $T' \subseteq T$ has a model, since it can only mention finitely many of the $C_i$. So any infinite model of $S$ will do. Hence by compactness, $T$ has a model □

**Theorem** (Downward Löwenheim-Skolem theorem)**.** Let $L$ be a countable language (i.e. $\Omega$ and $\Pi$ are countable). Then if $S$ has a model, then it has a countable model.

*Proof.* The model constructed in the proof of model existence theorem is countable. □

## 4.4 Peano Arithmetic

## 4.5 Completeness and categoricity*

**Proposition.** Let $T$ be a theory that is $\kappa$ categorical for some $\kappa$, and suppose $T$ has no finite models. Then $T$ is complete.

*Proof.* Let $p$ be a proposition. Suppose $T \nvdash p$ and $T \nvdash \neg p$. Then there are infinite models of $T \cup \{p\}$ and $T \cup \{\neg p\}$ (since the models cannot be finite), and so by the Löwenhein–Skolem theorems, we can find such models of cardinality $\kappa$. But since one satisfies $p$ and the other does not, they cannot be isomorphic. This contradicts $\kappa$-categoricity. □

**Theorem** (Ax-Grothendieck theorem)**.** Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a complex polynomial. If $f$ is injective, then it is in fact a bijection.

**Lemma.** Any two uncountable algebraically closed fields with the same dimension and same characteristic are isomorphic. In other words, the theory of algebraically closed fields of characteristic $p$ (for $p$ a prime or 0) is $\kappa$-categorical for all uncountable cardinals $\kappa$, and in particular complete.

*Proof of Ax-Grothendieck.* We will use compactness and completeness to show that we only have to prove this for fields of positive characteristic, and the result can be easily proven since we end up dealing with finite fields.

Let ACF be the theory of algebraically closed fields. The language is the language of rings, and the axioms are the usual axioms of a field, plus the following axiom for each $n > 0$:

$$(\forall a_0, a_1, \cdots, a_{n-1})(\exists x)(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0).$$

Let $\mathrm{ACF}_0$ denote the theory of algebraically closed fields of characteristic 0, where we add the axiom

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \neq 0 \qquad (*)$$

for all $n$ to $\mathrm{ACF}_n$.

Let $\mathrm{ACF}_p$ denote the theory of algebraically closed fields of characteristic $p$, where we add the axiom

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0$$

to ACF.

We now notice the following fact: if $r$ is a proposition that is a theorem of $\mathrm{ACF}_p$ for all $p$, then it is true of $\mathrm{ACF}_0$. Indeed, we know that $\mathrm{ACF}_0$ is complete. So if $r$ is not a theorem in $\mathrm{ACF}_0$, then $\neg r$ is a theorem. But the proof is finite, so it can only use finitely many instances of $(*)$. So there is some large $p$ where $\neg r$ can be proven in $\mathrm{ACF}_p$, which is a contradiction.

Now the statement "If $f$ is a polynomial of degree $d$ and $f$ is injective, then $f$ is surjective" can be expressed as a first-order statement. So we just have to prove it for all fields of characteristic $p > 0$. Moreover, by completeness, for each $p$, we only need to prove it for *some* algebraically complete field of characteristic $p$.

Fix a prime $p$, and consider $F = \bar{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. This is an algebraically closed field with the property that every element is algebraic over $\mathbb{F}_p$, i.e. the field generated by any finite subset of elements is finite.

Let $f : F^n \to F^n$ be a polynomial function involving coefficients $a_1, \cdots, a_K$. Let $b = (b_1, \cdots, b_n) \in F^n$ be a point. Then $F$ restricts to a function from the field $\tilde{F}$ generated by $\{b_1, \cdots, b_n, a_1, \cdots, a_K\}$ to itself. But $\tilde{F}$ is finite, so any function $f|_{\tilde{F}} : \tilde{F} \to \tilde{F}$ that is injective must also be surjective. So $b$ is in the image of $f$. So $f$ is surjective. So done. □

**Theorem** (Morley's categoricity theorem)**.** Let $T$ be a theory with a countable language. If $T$ is $\kappa$-categorical for *some* uncountable cardinal $\kappa$, then it is $\mu$-categorical for *all* uncountable cardinals $\mu$.

# 5 Set theory

## 5.1 Axioms of set theory

**Axiom** (Axiom of extension)**.** "If two sets have the same elements, they are the same set".

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

**Axiom** (Axiom of separation)**.** "Can form subsets of sets". More precisely, for any set $x$ and a formula $p$, we can form $\{z \in x : p(z)\}$.

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

This is an axiom scheme, with one instance for each formula $p$ with free variables $t_1, \cdots, t_n, z$.

Note again that we have those funny $(\forall t_i)$. We do need them to form, e.g. $\{z \in x : t \in z\}$, where $t$ is a parameter.

This is sometimes known as Axiom of comprehension.

**Axiom** (Axiom of empty set)**.** "The empty-set exists"

$$(\exists x)(\forall y)(y \notin x).$$

We write $\emptyset$ for the (unique, by extension) set with no members. This is an abbreviation: $p(\emptyset)$ means $(\exists x)(x$ has no members $\wedge\, p(x))$. Similarly, we tend to write $\{z \in x : p(z)\}$ for the set given by separation.

**Axiom** (Axiom of pair set)**.** "Can form $\{x, y\}$".

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

We write $\{x, y\}$ for this set. We write $\{x\}$ for $\{x, x\}$.

**Axiom** (Axiom of union)**.** "We can form unions" Intuitively, we have $a \cup b \cup c = \{x : x \in a \text{ or } x \in b \text{ or } x \in c\}$. but instead of $a \cup b \cup c$, we write $\bigcup\{a, b, c\}$ so that we can express infinite unions as well.

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

We tend to write $\bigcup x$ for the set given above. We also write $x \cup y$ for $\bigcup\{x, y\}$.

**Axiom** (Axiom of power set)**.** "Can form power sets".

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

where $z \subseteq x$ means $(\forall t)(t \in z \Rightarrow t \in x)$.

We tend to write $\mathbb{P}(x)$ for the set generated above.

**Axiom** (Axiom of infinity)**.** "There is an infinite set".

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

We say any set that satisfies the above axiom is a successor set.

**Axiom** (Axiom of foundation)**.** "Every (non-empty) set has an $\in$-minimal member"

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

This is sometimes known as the Axiom of regularity.

**Axiom** (Axiom of replacement)**.** "The image of a set under a function-class is a set". This is an axiom scheme, with an instance for each first-order formula $p$:

$$\underbrace{(\forall t_1)\cdots(\forall t_n)}_{\text{parameters}}\Big(\underbrace{[(\forall x)(\forall y)(\forall z)((p \wedge p[z/y]) \Rightarrow y = z)]}_{p \text{ defines a function-class}}$$
$$\Rightarrow \underbrace{[(\forall x)(\exists y)(z \in y \Leftrightarrow (\exists t)(t \in x \wedge p[t/x, z/y]))]}_{\text{image of } x \text{ under } F \text{ is a set}}\Big).$$

## 5.2 Properties of ZF

**Lemma.** Every $x$ is contained in a transitive set.

*Proof.* We'd like to form "$x \cup (\bigcup x) \cup (\bigcup\bigcup x) \cup (\bigcup\bigcup\bigcup x) \cup \cdots$". If this makes sense, then we are done, since the final product is clearly transitive. This will be a set by the union axiom applied to $\{x, \bigcup x, \bigcup\bigcup x, \cdots\}$, which itself is a set by replacement applied to $\omega$, for the function-class $0 \mapsto x$, $1 \mapsto \bigcup x$, $2 \mapsto \bigcup\bigcup x$ etc.

Of course we have to show that the above is a function class, i.e. can be expressed as a first order relation. We might want to write the sentence as:

$$p(s,t) \text{ is } (s = 0 \wedge t = x) \vee (\exists u)(\exists v)(s = u + 1 \wedge t = \bigcup v \wedge p(u,v)),$$

but this is complete nonsense! We are defining $p$ in terms of itself!

The solution would be to use attempts, as we did previously for recursion. We define "$f$ is an attempt" to mean "$f$ is a function and $\operatorname{dom} f \in \omega$ and $\operatorname{dom} f \neq \emptyset$ and $f(0) = x$ and $(\forall n)(n \in \omega \wedge n \in \operatorname{dom} f) \Rightarrow f(n) = \bigcup f(n-1)$, i.e. $f$ is defined for some natural numbers and meet our requirements when it is defined.

Then it is easy to show that two attempts $f$ and $f'$ agree whenever both are defined. Also, $\forall n \in \omega$, there is an attempt $f$ defined for $n$ (both by $\omega$-induction).

Note that the definition of an attempt is a first-order formula. So our function class is

$$p(s,t) \text{ is } (\exists f)(f \text{ is an attempt} \wedge y \in \operatorname{dom} f \wedge f(y) = z). \qquad \square$$

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

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

Note that officially, $p(y)$ means $p[y/x]$ and $p(x)$ is simply $x$.

*Proof.* Given $t_1, \cdots, t_n$, suppose $\neg(\forall x)p(x)$. So we have some $x$ with $\neg p(x)$. Similar to how we proved regular induction on naturals from the well-ordering principle (in IA Numbers and Sets), we find a minimal $x$ such that $p(x)$ does not hold.

While foundation allows us to take the minimal element of a *set*, $\{y : \neg p(y)\}$ need not be a set — e.g. if $p(y)$ is $y \neq y$.

Instead, we pick a single $x$ such that $\neg p(x)$. Let $u = TC(\{x\})$. Then $\{y \in u : \neg p(y)\} \neq \emptyset$, since $x \in u$. So it has an $\in$-minimal element, say $y$, by Foundation. Then each $z \in y$ has $z \in u$ since $u$ is transitive. Hence $p(z)$ by minimality of $y$. But this implies $p(y)$. Contradiction. $\square$

**Proposition.** $\in$-induction $\Rightarrow$ Foundation.

*Proof.* To deduce foundation from $\in$-induction, the obvious $p(x)$ — $x$ has an $\in$-minimal member, doesn't work.

Instead, consider $p(x)$ given by

$$(\forall y)\, x \in y \Rightarrow y \text{ has an } \in\text{-minimal member.}$$

If $p(x)$ is true, we say $x$ is *regular*. To show that $(\forall x)p(x)$, it is enough to show that: if every $y \in x$ is regular, then $x$ is regular.

Given any $z$ with $x \in z$, we want to show that $z$ has an $\in$-minimal member.

If $x$ is itself minimal in $z$, then done. Otherwise, then $y \in z$ for some $y \in x$. But since $y \in x$, $y$ is regular. So $z$ has a minimal element.

Hence all $x$ is regular. Since all non-empty sets contain at least one element (by definition), all sets have $\in$-minimal member. □

**Theorem** ($\in$-recursion theorem)**.** Let $G$ be a function-class, everywhere defined. Then there is a function-class $F$ such that $F(x) = G(F|_x)$ for all $x$. Moreover, $F$ is unique (cf. definition of recursion on well-orderings).

*Proof.* We first show existence. Again, we prove this with attempts. Define "$f$ is an attempt" to mean "$f$ is a function and $\operatorname{dom} f$ is transitive and $(\forall x)(x \in \operatorname{dom} f \Rightarrow f(x) = G(f|_x))$".

Then by simple $\in$-induction, we have

$$\begin{aligned}(\forall x)(\forall f')[(&f \text{ an attempt defined at } x \wedge \\ &f' \text{ an attempt defined at } x) \Rightarrow f(x) = f'(x)].\end{aligned}$$

Also, $(\forall x)(\exists f)(f$ an attempt defined at $x)$, again by $\in$-induction: suppose for each $y \in x$, there exists an attempt defined at $y$. So there exists a unique attempt $f_y$ with domain $TC(\{y\})$. Set $f = \bigcup_{y \in x} f_y$, and let $f' = f \bigcup \{(x, G(f|_x)\}$. Then this is an attempt defined at $x$.

So we take $q(x, y)$ to be

$$(\exists f)(f \text{ is an attempt defined at } x \text{ with } f(x) = y).$$

Uniqueness follows form $\in$-induction. □

**Proposition.** $p$-induction and $p$-recursion are well-defined and valid for any $p(x, y)$ that is well-founded and local.

*Proof.* Same as above. □

**Theorem** (Mostowski collapse theorem)**.** Let $r$ be a relation on a set $a$ that is well-founded and extensional. Then there exists a transitive $b$ and a bijection $f : a \to b$ such that $(\forall x, y \in a)(x\, r\, y \Leftrightarrow f(x) \in f(y))$. Moreover, $b$ and $f$ are unique.

*Proof.* Existence: define $f$ on $a$ the obvious way — $f(x) = \{f(y) : y\, r\, x\}$. This is well-defined by $r$-recursion, and is a genuine function, not just of a function class by replacement — it is an image of $a$.

Let $b = \{f(x) : x \in a\}$ (this is a set by replacement). We need to show that it is transitive and bijective.

By definition of $f$, $b$ is transitive, and $f$ is surjective as $b$ is *defined* to be the image of $f$. So we have to show that $f$ is injective.

We'll show that $(\forall x \in a)(f(y) = f(x) \Rightarrow y = x)$ for each $x \in a$, by $r$-induction. Given $y \in a$, with $f(y) = f(x)$, we have $\{f(t) : t\, r\, y\} = \{f(s) : s\, r\, y\}$ by definition of $f$. So $\{t : t\, r\, y\} = \{s : s\, r\, x\}$ by the induction hypothesis. Hence $x = y$ since $r$ is extensional.

So we have constructed such an $b$ and $f$. Now we show it is unique: for any suitable $f, f'$, we have $f(x) = f'(x)$ for all $x \in a$ by $r$-induction. □

## 5.3 Picture of the universe

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

*Proof.* Since we define $V_\alpha$ by recursion, it is sensible to prove this by induction: By induction on $\alpha$:

(i) Zero: $V_0 = \emptyset$ is transitive.

(ii) Successors: If $x$ is transitive, then so is $\mathbb{P}(x)$: given $y \in z \in \mathbb{P}(x)$, we want to show that $y \in \mathbb{P}(x)$. Since $y$ is in a member of $\mathbb{P}(x)$, i.e. a subset of $x$, we must have $y \in x$. So $y \subseteq x$ since $x$ is transitive. So $y \in \mathbb{P}(x)$.

(iii) Limits: Any union of transitive sets is transitive. □

**Lemma.** If $\alpha \leq \beta$, then $V_\alpha \subseteq V_\beta$.

*Proof.* Fix $\alpha$, and induct on $\beta$.

(i) $\beta = \alpha$: trivial

(ii) Successors: $V_{\beta^+} \subseteq V_\beta$ since $x \subseteq \mathbb{P}(x)$ for transitive $x$. So $V_\alpha \subseteq V_\beta \Rightarrow V_\alpha \subseteq V_{\beta^+}$.

(iii) Limits: Trivial by definition □

**Theorem.** Every $x$ belongs to some $V_\alpha$. Intuitively, we want to say

$$V = \bigcup_{\alpha \in \mathrm{On}} V_\alpha,$$

*Proof.* We'll show that $(\forall x)(\exists \alpha)(x \in V_\alpha)$ by $\in$-induction on $x$.

So we are allowed to assume that for each $y \in x$, we have $y \subseteq V_\alpha$ for some $\alpha$. So $y \subseteq V_{\mathrm{rank}(y)}$, or $y \in V_{\mathrm{rank}(y)+1}$.

Let $\alpha = \sup\{(\mathrm{rank}(y)^+ : y \in x\}$. Then $y \in V_\alpha$ for every $y \in x$. So $x \subseteq V_\alpha$. □

**Proposition.** $\mathrm{rank}(x)$ is the first $\alpha$ such that $x \subseteq V_\alpha$.

# 6 Cardinals

## 6.1 Definitions

**Theorem.** The $\aleph_\alpha$ are the cardinals of all infinite sets (or, in ZF, the cardinals of all infinite well-orderable sets). For example, $\operatorname{card}(\omega) = \aleph_0$, $\operatorname{card}\omega_1 = \aleph_1$.

## 6.2 Cardinal arithmetic

**Proposition.**

(i) $m + n = n + m$ since $N \sqcup M \leftrightarrow N \sqcup N$ with the obvious bijection.

(ii) $mn = nm$ using the obvious bijection

(iii) $(m^n)^p = m^{np}$ as $(M^N)^P \leftrightarrow M^{N\times P}$ since both objects take in a $P$ and an $N$ and returns an $M$.

**Theorem.** For every ordinal $\alpha$,

$$\aleph_\alpha \aleph_\alpha = \aleph_\alpha.$$

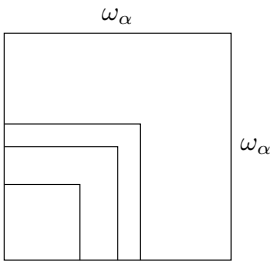
This is the best we could ever ask for. What can be simpler?

*Proof.* Since the Alephs are defined by induction, it makes sense to prove it by induction.

In the following proof, there is a small part that doesn't work nicely with $\alpha = 0$. But $\alpha = 0$ case (ie $\aleph_0\aleph_0 = \aleph_0$) is already done. So assume $\alpha \neq 0$.

Induct on $\alpha$. We want $\omega_\alpha \times \omega_\alpha$ to biject with $\omega_\alpha$, i.e. well-order $\omega_\alpha \times \omega_\alpha$ to an ordering of length $\omega_\alpha$.

Using the ordinal product clearly doesn't work. The ordinal product counts the product in rows, so we have many copies of $\omega_\alpha$. When we proved $\aleph_0\aleph_0 = \aleph_0$, we counted them diagonally. But counting diagonally here doesn't look very nice, since we will have to "jump over" infinities. Instead, we count in squares




We set $(x, y) < (x', y')$ if *either* $\max(x, y) < \max(x', y')$ (this says that $(x', y')$ is in a bigger square), *or*, (say $\max(x, y) = \max(x', y') = \beta$ and $y' = \beta, y < \beta$ or $x = x' = \beta, y < y'$ or $y = y' = \beta, x < x'$) (nonsense used to order things in the same square — utterly unimportant).

How do we show that this has order type $\omega_\alpha$? We show that any initial segment has order type $< \omega_\alpha$.

For any proper initial segment $I_{(x,y)}$, we have

$$I_{(x,y)} \subseteq \beta \times \beta$$

for some $\beta < \omega_\alpha$, since $\omega_\alpha$ is a limit, with wlog $\beta$ infinite. So

$$\beta \times \beta \leftrightarrow \beta$$

by induction hypothesis (their cardinality is less that $\omega_\alpha$). So

$$\text{card}(\beta \times \beta) < \text{card}(\omega_\alpha).$$

Hence $I_{(x,y)}$ has order type $< \omega_\alpha$. Thus the order type of our well-order is $\leq \omega_\alpha$. So $\omega_\alpha \times \omega_\alpha$ injects into $\omega_\alpha$. Since trivially $\omega_\alpha$ injects into $\omega_\alpha \times \omega_\alpha$, we have $\omega_\alpha \times \omega_\alpha \leftrightarrow \omega_\alpha$. □

**Corollary.** Let $\alpha \leq \beta$. Then

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \aleph_\beta = \aleph_\beta.$$

*Proof.*

$$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2\aleph_\beta \leq \aleph_\beta \times \aleph_\beta = \aleph_\beta,$$

So done □

# 7 Incompleteness*

**Theorem** (Gödel's incompleteness theorem)**.** PA is incomplete.

**Theorem.** "Truth is not definable"
$T = \{p : p \text{ holds in } \mathbb{N}\}$ is not definable. This officially means

$$\{m : m \text{ codes a member of } T\}$$

is not a definable set.

**Theorem.** PA $\nvdash$ con(PA).