M3P65 Mathematical Logic

Lectured by Prof David Evans
Typed by David Kurniadi Angdinata

Autumn 2018

Extensionality $\equiv (\forall x)(\forall y)$
$$((x = y) \leftrightarrow (\forall z)((z \in x) \leftrightarrow (z \in y)))$$

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

Pairing $\equiv (\forall x)(\forall y)(\exists z)(\forall w)$
$$((w \in z) \leftrightarrow ((w = x) \vee (w = y)))$$

Union $\equiv (\forall x)(\exists y)(\forall z)$
$$((z \in y) \leftrightarrow (\exists w)((w \in x) \wedge (z \in w)))$$

Power $\equiv (\forall x)(\exists y)(\forall z)$
$$((z \in y) \leftrightarrow (\forall w)((w \in z) \rightarrow (w \in x)))$$

Specification $\equiv (\forall x)(\forall y_1)\dots(\forall y_n)(\exists z)(\forall w)$
$$((w \in z) \leftrightarrow ((w \in x) \wedge \phi(x, y_1, \dots, y_n)))$$

Infinity $\equiv (\exists x)$
$$((\exists y)((y \in x) \wedge (\forall z)(\neg (z \in y))) \wedge (\forall y)((y \in x)$$
$$\rightarrow (\exists z)((z \in x) \wedge ((\forall w)((w \in y) \rightarrow (w \in z)) \wedge (\exists w)((w \in z) \wedge (\neg (w \in y)))))))$$

Replacement $\equiv (\forall x)(\forall y_1)\dots(\forall y_n)$
$$((\forall w)((w \in x) \rightarrow (\exists v)(\phi(v, w, y_1, \dots, y_n) \wedge (\forall u)(\phi(u, w, y_1, \dots, y_n) \rightarrow (u = v))))$$
$$\rightarrow (\exists z)(\forall v)((v \in z) \rightarrow (\exists w)((w \in x) \wedge \phi(v, w, y_1, \dots, y_n))))$$

Regularity $\equiv (\forall x)$
$$((\exists y)(y \in x) \rightarrow (\exists y)((y \in x) \wedge (\forall z)((\neg (z \in x)) \wedge (\neg (z \in y)))))$$

Choice $\equiv (\forall x)$
$$\left((\exists y)(y \in x) \rightarrow \left(\exists \phi : x \rightarrow \bigcup x\right)(\forall z)((z \in x) \rightarrow (\phi(z) \in z))\right)$$

Syllabus

Propositional formulas and logical validity. The formal system L. Soundness and completeness. First-order languages and structures. Satisfaction and truth of formulas. The formal system $K_{\mathcal{L}}$. Gödel's completeness theorem. The compactness theorem. The Löwenheim-Skolem theorem. The axioms of Zermelo-Fraenkel set theory. Ordinals. Cardinality. The axiom of choice.

Contents

0   Introduction

The module is concerned with some of the foundational issues of mathematics. In propositional and predicate logic, we analyse the way in which we reason formally about mathematical structures. In set theory, we will look at the ZFC axioms and use these to develop the notion of cardinality. These topics have applications to other areas of mathematics. Formal logic has applications via model theory and ZFC provides an essential toolkit for handling infinite objects.

The first level of the subject is propositional logic. We look at the way simple statements or propositions can be built into more complicated ones using connectives and make precise how the truth or falsity of the component statements influences the truth or falsity of the compound statement. This is done using truth tables and can be useful for testing the validity of various forms of reasoning. It provides a way of analysing deductions. We then move on to a completely symbolic process of deduction and describe the formal deduction system for propositional calculus. The statements we consider, propositional formulas, are regarded as strings of symbols and we give rules for deducing a new formula from a given collection of formulas. We want these deduction rules to have the property that anything that could be deduced using truth tables, so by considering truth or falsity of the various statements, can be deduced in this formal way, and vice versa. This is the soundness and completeness of our formal system.

The next level of the subject is predicate logic. This is what is needed to analyse real mathematics and the extra ingredient is the use of quantifiers. We introduce the notion of a first-order structure, which is general enough to include many of the algebraic objects you come across in mathematics. We then have to be precise about the expressions, formulas, which make statements about these structures, and give a precise definition of what it means for a particular formula to be true in a structure. This is quite intricate, and the clever part is in getting the definitions right, but it corresponds to ordinary mathematical usage. Once this is done, we set up a formal deduction system for predicate logic. This parallels what we did for propositional logic, but is much harder. Nevertheless, the end result is the same. The formulas which are produced by our formal deduction system, the theorems, are precisely the formulas which are true in all first-order structures. This is Gödel's completeness theorem.

Set theory provides the basic foundations and the language in which most of modern mathematics can be expressed, as well as the means for discussing the various notions of sizes of infinity. For example, although the set of natural numbers, the set of integers and the set of real numbers are all infinite, there is a very natural sense in which the first two have the same size, whereas the third is strictly bigger. This is expressed properly in the notion of cardinality. To avoid paradoxes and inconsistencies, we have to be careful about what collections of objects we allow to be called sets. This is done by the Zermelo-Fraenkel axioms, which essentially tell us how we are allowed to create new sets out of old ones. Of course, having laid down these quite rigid rules, we have to show that they are sufficiently flexible to allow us to talk about everyday objects of mathematics. There are also situations in mathematics where an extra axiom is needed, the the axiom of choice. For example without this axiom, or rather, method of construction of a new set from given ones, we cannot show that every vector space has a basis. But it also has some slightly counterintuitive consequences, and we shall also look at some of these.

The lecture notes should be fairly self-contained, but the following books might also be of use. You might find that the notation which they use differs form that used in the lectures. You will be able to find various lecture notes on the internet. Some will be good, others not so good.

1. P Johnstone, Notes on logic and set theory, 1987

2. P J Cameron, Sets, logic and categories, 1999

3. A G Hamilton, Logic for mathematicians, 1988

4. R Cori and D Lascar, Mathematical logic: a course with exercises parts I and II, 2001

5. K Hrbacek and T Jech, Introduction to set theory 3rd edition, 1999

1 is very concise, but covers a surprising amount. 2 is friendlier, but skips some of the harder material. 4 is quite comprehensive and also available in the original French. 3 is useful for the logic part and 5 is a very nice introduction to set theory.

1   Propositional logic

Let
$$p : \text{Mr Jones is happy}, \qquad q : \text{Mrs Jones is unhappy}.$$

Then

if Mr Jones is happy, then Mrs Jones is unhappy,

and if Mrs Jones is unhappy, then Mr Jones is unhappy, so Mr Jones is unhappy

is
$$(((p \to q) \land (q \to (\neg p))) \to (\neg p)) .$$

1.1   Propositional formulas

A **proposition** is a statement that is either **True (T)** or **False (F)**. The following are **truth table rules**.

Definition 1.1.1. Represent propositions symbolically using **propositional variables**.

$$p, \quad q, \quad \ldots \qquad p_1, \quad p_2, \quad \ldots$$

Combine basic propositions into others using the following **connectives**.

- **Negation (not)**, where

$$(\neg p) \text{ has value F} \qquad \Longleftrightarrow \qquad p \text{ has value T}.$$

- **Conjunction (and)**, where

$$(p \land q) \text{ has value T} \qquad \Longleftrightarrow \qquad p \text{ and } q \text{ both have value T}.$$

- **Disjunction (or)**, where

$$(p \lor q) \text{ has value T} \qquad \Longleftrightarrow \qquad \text{at least one of } p \text{ and } q \text{ has value T}.$$

- **Implication (implies)**, where

$$(p \to q) \text{ has value F} \qquad \Longleftrightarrow \qquad p \text{ has value T and } q \text{ has value F}.$$

- **Biconditional (iff)**, where

$$(p \leftrightarrow q) \text{ has value T} \qquad \Longleftrightarrow \qquad p \text{ and } q \text{ have the same value}.$$

The following is a **truth table**.

p	q	$(p \land q)$	$(p \lor q)$	$(p \to q)$	$(p \leftrightarrow q)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Definition 1.1.2. A **propositional formula** is obtained in the following way.

- Any propositional variable is a formula.

- If ϕ and ψ are formulas, then so are

$$(\neg \phi), \qquad (\phi \land \psi), \qquad (\phi \lor \psi), \qquad (\phi \to \psi), \qquad (\phi \leftrightarrow \psi).$$

- Any formula arises in this way.

Example.

- Formulas.

$$p_1 \qquad p_2 \qquad (\neg p_1) \qquad (p_1 \to (\neg p_2)) \qquad ((p_1 \to (\neg p_2)) \to p_2)$$

- Not formulas.

$$p_1 \wedge p_2 \quad \text{(missing brackets)} \qquad)(\neg p_1 \quad \text{(not well-formed)}$$

Because of the brackets, every formula is either a propositional variable or is built from shorter formulas in a unique way. Arguments are often proved by induction, on length of the formula, or the number of connectives in the formula.

Definition 1.1.3. Let $n \in \mathbb{N}$.

- A **truth function** of n variables is a function $f : \{T, F\}^n \to \{T, F\}$, where

$$\{T, F\}^n = \{(x_1, \ldots, x_n) \mid x_i = T, F\}.$$

  How many truth functions of n variables are there? [1]

- Suppose ϕ is a formula whose variables are amongst $p_1, \ldots, p_n$. We obtain a truth function

$$F_\phi : \{T, F\}^n \to \{T, F\},$$

  whose value at $(x_1, \ldots, x_n)$ is the truth value of ϕ when p_i has value x_i for $i = 1, \ldots, n$, computed using the rules in 1.1.1. Then F_ϕ is the **truth function of** ϕ.

Example. Let

$$\phi : ((p \to (\neg q)) \to p).$$

Then

p	q	$(\neg q)$	$(p \to (\neg q))$	ϕ
T	T	F	F	T
T	F	T	T	T
F	T	F	T	F
F	F	T	T	F

So, for example, $F_\phi(T, F) = T$. The following is its **condensed form**.

$((p$	$\to$	$(\neg$	$q))$	$\to$	$p)$
T	F	F	T	T	T
T	T	T	F	T	T
F	T	F	T	F	F
F	T	T	F	F	F
				ϕ	

Example. What is the truth function of

$$(((p \to q) \wedge (q \to (\neg p))) \to (\neg p))?$$

Always T.

Definition 1.1.4.

- A propositional formula ϕ is a **tautology** if its truth function F_ϕ always has value T.

- Say that formulas ϕ and ψ are **logically equivalent (LE)** if they have the same truth function, that is $F_\phi = F_\psi$.

Remark 1.1.5.

1. ϕ and ψ are logically equivalent if and only if $(\phi \leftrightarrow \psi)$ is a tautology.

2. Suppose ϕ is a formula with variables $p_1, \ldots, p_n$, and $\phi_1, \ldots, \phi_n$ are formulas with variables $q_1, \ldots, q_r$. For each $i \leq n$, substitute ϕ_i in place of p_i in ϕ. Then the result is a formula θ, and if ϕ is a tautology, then so is θ.

---

[1]Exercise

Example 1.1.6. Check that
$$(((\neg p_2) \to (\neg p_1)) \to (p_1 \to p_2))$$
is a tautology. So by 1.1.5.2, if ϕ_1 and ϕ_2 are any formulas, then

$$(((\neg \phi_2) \to (\neg \phi_1)) \to (\phi_1 \to \phi_2))$$

is a tautology.

Proof of 1.1.5.

1. Easy.

2. Prove
$$\mathrm{F}_\theta (p_1, \ldots, p_r) = \mathrm{F}_\phi (\mathrm{F}_{\phi_1} (q_1, \ldots, q_r), \ldots, \mathrm{F}_{\phi_n} (q_1, \ldots, q_r)),$$
   by induction on the number of connectives in ϕ.

   $\square$

Example. Logically equivalent formulas.

$$(p_1 \wedge (p_2 \wedge p_3)) \text{ is logically equivalent to } ((p_1 \wedge p_2) \wedge p_3).$$
$$(p_1 \vee (p_2 \vee p_3)) \text{ is logically equivalent to } ((p_1 \vee p_2) \vee p_3).$$
$$(p_1 \vee (p_2 \wedge p_3)) \text{ is logically equivalent to } ((p_1 \vee p_2) \wedge (p_1 \vee p_3)).$$
$$(p_1 \wedge (p_2 \vee p_3)) \text{ is logically equivalent to } ((p_1 \wedge p_2) \vee (p_1 \wedge p_3)).$$
$$(\neg (\neg p_1)) \text{ is logically equivalent to } p_1.$$
$$(\neg (p_1 \wedge p_2)) \text{ is logically equivalent to } ((\neg p_1) \vee (\neg p_2)).$$
$$(\neg (p_1 \vee p_2)) \text{ is logically equivalent to } ((\neg p_1) \wedge (\neg p_2)).$$

So we usually omit brackets in $(p_1 \wedge p_2 \wedge p_3)$ and $(p_1 \vee p_2 \vee p_3)$.

Note. By 1.1.5, we obtain, for formulas ϕ, ψ, χ,

$$(\phi \wedge (\psi \wedge \chi)) \text{ is logically equivalent to } ((\phi \wedge \psi) \wedge \chi),$$

etc.

Lemma 1.1.7. *There are 2^{2^n} truth functions of n variables.*

Proof. A truth function is a function
$$\mathrm{F} : \{\mathrm{T}, \mathrm{F}\}^n \to \{\mathrm{T}, \mathrm{F}\}.$$
Then $|\{\mathrm{T}, \mathrm{F}\}^n| = 2^n$, and for each $\overline{x} \in \{\mathrm{T}, \mathrm{F}\}^n$, $\mathrm{F}(\overline{x}) = \mathrm{T}, \mathrm{F}$. Hence the result. $\square$

Definition 1.1.8. Say that a set of connectives is **adequate** if for every $n \geq 1$, every truth function of n variables is the truth function of some formula which involves only connectives from the set, and variables $p_1, \ldots, p_n$.

Theorem 1.1.9. *The set $\{\neg, \wedge, \vee\}$ is adequate.*

Proof. Let $G : \{\mathrm{T}, \mathrm{F}\}^n \to \{\mathrm{T}, \mathrm{F}\}$.

Case 1. $G(\overline{v}) = \mathrm{F}$ for all $\overline{v} \in \{\mathrm{T}, \mathrm{F}\}^n$. Take ϕ to be

$$(p_1 \wedge (\neg p_1)).$$

Then $G = \mathrm{F}_\phi$.

Case 2. List the $\overline{v} \in \{\mathrm{T}, \mathrm{F}\}^n$ with $G(\overline{v}) = \mathrm{T}$ as
$$\overline{v_1}, \ldots, \overline{v_r}.$$

Write
$$\overline{v_i} = (v_{i1}, \ldots, v_{in}),$$

where each v_{ij} is T or F. Define
$$q_{ij} = \begin{cases} p_j & v_{ij} = \mathrm{T} \\ (\neg p_j) & v_{ij} = \mathrm{F} \end{cases}.$$

So q_{ij} has value T if and only if p_j has value v_{ij}. Let
$$\psi_i : (q_{i1} \wedge \cdots \wedge q_{in}).$$

Then
$$\mathrm{F}_{\psi_i}(\overline{v}) = \mathrm{T} \qquad \Longleftrightarrow \qquad \text{each } q_{ij} \text{ has value T} \qquad \Longleftrightarrow \qquad \overline{v} = \overline{v_i}.$$

Let
$$\theta : (\psi_1 \vee \cdots \vee \psi_r).$$

Then
$$\mathrm{F}_\theta(\overline{v}) = \mathrm{T} \qquad \Longleftrightarrow \qquad \mathrm{F}_{\psi_i}(\overline{v}) = \mathrm{T} \qquad \Longleftrightarrow \qquad \overline{v} = \overline{v_i}, \qquad i \leq r.$$

Thus $\mathrm{F}_\theta(\overline{v}) = \mathrm{T}$ if and only if $G(\overline{v}) = \mathrm{T}$, that is $\mathrm{F}_\theta = G$.

As ϕ and θ were constructed using only $\neg, \wedge, \vee$, 1.1.9 follows. $\qquad\qquad\square$

A formula θ as in case 2 is said to be in **disjunctive normal form (DNF)**.

Corollary 1.1.10. *Suppose χ is a formula whose truth function is not always F. Then χ is logically equivalent to a formula in disjunctive normal form.*

Proof. Take $G = \mathrm{F}_\chi$, and apply case 2 of 1.1.9. $\qquad\qquad\square$

Example. Let
$$\chi : ((p_1 \to p_2) \to (\neg p_2)).$$

Then $\mathrm{F}_\chi(\overline{v}) = \mathrm{T}$ if and only if $\overline{v} = (\mathrm{T}, \mathrm{F}), (\mathrm{F}, \mathrm{F})$. Thus the disjunctive normal form is

$$((p_1 \wedge (\neg p_2)) \vee ((\neg p_1) \wedge (\neg p_2))).$$

Corollary 1.1.11. *The following sets of connectives are adequate.*

1. $\{\neg, \vee\}$,

2. $\{\neg, \wedge\}$, *and*

3. $\{\neg, \to\}$.

Proof.

1. By 1.1.9, enough to show that we can express $\wedge$ using $\neg$ and $\vee$, and

$$(p_1 \wedge p_2) \text{ is logically equivalent to } (\neg((\neg p_1) \vee (\neg p_2))).$$

2. By 1.1.9, enough to show that we can express $\vee$ using $\neg$ and $\wedge$, and

$$(p_1 \vee p_2) \text{ is logically equivalent to } (\neg((\neg p_1) \wedge (\neg p_2))).$$

3. By 1.1.9, enough to show that we can express $\vee$ using $\neg$ and $\to$, and

$$(p_1 \vee p_2) \text{ is logically equivalent to } ((\neg p_1) \to p_2).$$

$\qquad\qquad\square$

Example 1.1.12. The following are not adequate.

1. $\{\wedge, \vee\}$, and

2. $\{\neg, \leftrightarrow\}$.

Proof.

1. If ϕ is built using $\vee$ and $\wedge$, then $F_\phi (T, \ldots, T) = T$, by proof by induction on the number of connectives.

2. Exercise. [2]

$\square$

Example 1.1.13. The **NOR** connective $\downarrow$ has the following truth table.

p	q	$(p \downarrow q)$
T	T	F
T	F	F
F	T	F
F	F	T

Then $(p \downarrow q)$ is logically equivalent to $((\neg p) \wedge (\neg q))$. Then $\{\downarrow\}$ is adequate, since

- $(p \downarrow p)$ is logically equivalent to $(\neg p)$, and

- $((p \downarrow p) \downarrow (q \downarrow q))$ is logically equivalent to $(p \wedge q)$,

so, as $\{\neg, \wedge\}$ is adequate, so is $\{\downarrow\}$.

1.2   A formal system for propositional logic

The idea is to try to generate all tautologies from basic assumptions, or axioms, using appropriate deduction rules.

Definition 1.2.1. The following is a very general definition.

- A **formal deduction system** Σ has the following ingredients.

  - An **alphabet** $A \neq \emptyset$ of symbols.
  - A non-empty subset $\mathcal{F}$ of the set of all finite sequences, **strings**, of elements of A, the **formulas** of Σ.
  - A subset $\mathcal{A} \subseteq \mathcal{F}$ called the **axioms** of Σ.
  - A collection of **deduction rules**.

- A **proof** in Σ is a finite sequence of formulas in $\mathcal{F}$, $\phi_1, \ldots, \phi_n$ such that each ϕ_i is either an axiom, that is it is in $\mathcal{A}$, or is obtained from $\phi_1, \ldots, \phi_{i-1}$ using one of the deduction rules.

- The last, or any, formula in a proof is a **theorem** of Σ. Write $\vdash_\Sigma \phi$ if ϕ is a theorem of Σ.

Remark.

- If $\phi \in \mathcal{A}$, then $\vdash_\Sigma \phi$.

- Should have an algorithm to test whether a string is a formula and whether it is an axiom. Then a computer can systematically generate all possible proofs in Σ, and check whether something is a proof. Say Σ is **recursive** in this case.

---

[2]Exercise

The following is the main example.

Definition 1.2.2. The formal system L for propositional logic has the following.

- Alphabet.

Variables	p_1	p_2	$\ldots$
Connectives	$\neg$	$\rightarrow$	
Punctuation	(	)	

- Formulas. L-formulas defined in 1.1.2 for $\neg, \rightarrow$.

  - Any variable p_i is a formula.
  - If ϕ and ψ are formulas, then so are

  $$(\neg\phi), \qquad (\phi \rightarrow \psi).$$

  - Any formula arises in this way.

- Axioms. Suppose ϕ, ψ, χ are L-formulas. The following are axioms of L.

  (A1) $(\phi \rightarrow (\psi \rightarrow \phi))$,
  (A2) $((\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \chi)))$, and
  (A3) $(((\neg\psi) \rightarrow (\neg\phi)) \rightarrow (\phi \rightarrow \psi))$.

- Deduction rule.

  (MP) **Modus Ponens**. From ϕ and $(\phi \rightarrow \psi)$, deduce ψ.

Example 1.2.3. Theorem 0. Suppose ϕ is an L-formula. Then $\vdash_L (\phi \rightarrow \phi)$. Here is a proof in L.

1	$(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi))$	(A1)
2	$((\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi)))$	(A2)
3	$((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$	$(1, 2, \text{MP})$
4	$(\phi \rightarrow (\phi \rightarrow \phi))$	(A1)
5	$(\phi \rightarrow \phi)$	$(3, 4, \text{MP})$

Definition 1.2.4. Suppose Γ is a set of L-formulas.

- A **deduction** from Γ is a finite sequence of L-formulas $\phi_1, \ldots, \phi_n$ such that each ϕ_i is either an axiom, a formula in Γ, or is obtained from previous formulas $\phi_1, \ldots, \phi_{i-1}$ using the deduction rule MP.

- Write $\Gamma \vdash_L \phi$ if there is a deduction from Γ ending in ϕ. Say ϕ is a **consequence** of Γ. So $\emptyset \vdash_L \phi$ is the same as $\vdash_L \phi$.

Lecture 4
Thursday
11/10/18

Theorem 1.2.5 (Deduction theorem). *Suppose Γ is a set of L-formulas and ϕ and ψ are L-formulas. Suppose $\Gamma \cup \{\phi\} \vdash_L \psi$. Then $\Gamma \vdash_L (\phi \rightarrow \psi)$.*

Corollary 1.2.6 (Hypothetical syllogism). *Suppose ϕ, ψ, χ are L-formulas and $\vdash_L (\phi \rightarrow \psi)$ and $\vdash_L (\psi \rightarrow \chi)$. Then $\vdash_L (\phi \rightarrow \chi)$.*

Proof. Use deduction theorem with $\Gamma = \emptyset$. Show that $\{\phi\} \vdash_L \chi$. Here is a deduction of χ from ϕ.

1	$(\phi \rightarrow \psi)$	(theorem of L)
2	$(\psi \rightarrow \chi)$	(theorem of L)
3	ϕ	(assumption)
4	ψ	$(1, 3, \text{MP})$
5	χ	$(2, 4, \text{MP})$

Thus $\{\phi\} \vdash_L \chi$. By deduction theorem, $\emptyset \vdash_L (\phi \rightarrow \chi)$, that is $\vdash_L (\phi \rightarrow \chi)$. $\square$

Proposition 1.2.7. *Suppose ϕ and ψ are L-formulas. Then*

1. $\vdash_{\mathrm{L}} ((\neg\psi) \to (\psi \to \phi))$,

2. $\{(\neg\psi), \psi\} \vdash_{\mathrm{L}} \phi$, *and*

3. $\vdash_{\mathrm{L}} (((\neg\phi) \to \phi) \to \phi)$.

Proof.

1. Problem sheet 1.

2. By 1 and MP twice.

3. Suppose χ is any formula. Then

$$\{(\neg\phi), ((\neg\phi) \to \phi)\} \vdash_{\mathrm{L}} \chi,$$

   by MP and 2. Let α be any axiom and let χ be $(\neg\alpha)$. Apply deduction theorem to get

$$\{((\neg\phi) \to \phi)\} \vdash_{\mathrm{L}} ((\neg\phi) \to (\neg\alpha)).$$

   A3 is $\{((\neg\phi) \to (\neg\alpha))\} \vdash_{\mathrm{L}} (\alpha \to \phi)$. Using this and MP, we get

$$\{((\neg\phi) \to \phi)\} \vdash_{\mathrm{L}} (\alpha \to \phi).$$

   As α is an axiom, we get, from MP,

$$\{((\neg\phi) \to \phi)\} \vdash_{\mathrm{L}} \phi.$$

   Now use deduction theorem to obtain

$$\vdash_{\mathrm{L}} (((\neg\phi) \to \phi) \to \phi).$$

$\square$

Proof of 1.2.5. Suppose $\Gamma \cup \{\phi\} \vdash_{\mathrm{L}} \psi$ using a deduction of length n. Show, by induction on n, that $\Gamma \vdash_{\mathrm{L}} (\phi \to \psi)$.

- Base case. $n = 1$. In this case, ψ is either an axiom, or in Γ, or is ϕ. In the first two cases, $\Gamma \vdash_{\mathrm{L}} \psi$, a one line deduction. Using the A1 axiom $(\psi \to (\phi \to \psi))$ and MP, we obtain $\Gamma \vdash_{\mathrm{L}} (\phi \to \psi)$. If ϕ is ψ, we have $\Gamma \vdash_{\mathrm{L}} (\phi \to \phi)$, by 1.2.3. This finishes the base case.

- Inductive step. In our deduction of ψ from $\Gamma \cup \{\phi\}$, either

  Case 1. ψ is an axiom, or in Γ, or is ϕ, or

  Case 2. ψ is obtained from earlier steps using MP.

  In case 1, we argue as in the base case to get $\Gamma \vdash_{\mathrm{L}} (\phi \to \psi)$. In case 2, there are formulas χ and $(\chi \to \psi)$ earlier in the deduction. We use the inductive hypothesis to get

$$\Gamma \vdash_{\mathrm{L}} (\phi \to \chi), \qquad \Gamma \vdash_{\mathrm{L}} (\phi \to (\chi \to \psi)). \tag{1}$$

  We have the A2 axiom $((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))$. Using (1), the A2 axiom, and MP twice, we obtain $\Gamma \vdash_{\mathrm{L}} (\phi \to \chi)$, as required, completing the inductive step.

$\square$

1.3   Soundness and completeness of L

Theorem 1.3.1 (Soundness of L). *Suppose ϕ is a theorem of L. Then ϕ is a tautology.*

Definition 1.3.2. A **propositional valuation** v is an assignment of truth values to the propositional variables $p_1, p_2, \ldots$. So

$$\mathrm{v}(p_i) = \mathrm{T}, \mathrm{F}, \qquad i \in \mathbb{N}.$$

Note. Using the truth table rules, this assigns a truth value $\mathrm{v}(\phi) = \mathrm{T}, \mathrm{F}$ to every L-formula ϕ, satisfying $\mathrm{v}((\neg\phi)) \neq \mathrm{v}(\phi)$, etc. See problem sheet 2.

Lecture 5
Friday
12/10/18

Proof of 1.3.1. By induction on the length of a proof of ϕ, it is enough to show every axiom is a tautology, and MP preserves tautologies, that is if ψ and $(\psi \to \chi)$ are tautologies, so is χ.

- Use truth tables, or argue as follows. For A2, suppose for a contradiction there is a valuation v with

$$\text{v}\left(\left((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi))\right)\right) = \text{F}.$$

Then

$$\text{v}\left((\phi \to (\psi \to \chi))\right) = \text{T}, \tag{2}$$

and

$$\text{v}\left(((\phi \to \psi) \to (\phi \to \chi))\right) = \text{F}. \tag{3}$$

By (3),

$$\text{v}\left((\phi \to \psi)\right) = \text{T}, \tag{4}$$

and

$$\text{v}\left((\phi \to \chi)\right) = \text{F}. \tag{5}$$

So by (5), $\text{v}(\phi) = \text{T}$ and $\text{v}(\chi) = \text{F}$. By (4), $\text{v}(\psi) = \text{T}$. This contradicts (2). [3]

- If v is a valuation, and $\text{v}(\psi) = \text{T}$ and $\text{v}((\psi \to \chi)) = \text{T}$, then $\text{v}(\chi) = \text{T}$.

$\square$

Theorem 1.3.3 (Generalisation of soundness)**.** *Suppose Γ is a set of formulas and ϕ is a formula with $\Gamma \vdash_\text{L} \phi$. Suppose v is a valuation with $\text{v}(\psi) = \text{T}$ for all $\psi \in \Gamma$. Then $\text{v}(\phi) = \text{T}$.*

Proof. Same proof. [4] $\square$

Theorem 1.3.4 (Completeness (adequacy) of L)**.** *Suppose ϕ is a tautology, that is $\text{v}(\phi) = \text{T}$ for every valuation v. Then $\vdash_\text{L} \phi$.*

Remark 1.3.5. The following are the steps in the proof.

- If $\text{v}(\phi) = \text{T}$ for all valuations v, want to show $\vdash_\text{L} \phi$.

- Try to prove a generalisation. Suppose that, for every v with $\text{v}(\Gamma) = \text{T}$, that is $\text{v}(\psi) = \text{T}$ for all $\psi \in \Gamma$, we have $\text{v}(\phi) = \text{T}$. Then $\Gamma \vdash_\text{L} \phi$.

- Equivalently, if $\Gamma \nvdash_\text{L} \phi$, show there is a valuation v with $\text{v}(\Gamma) = \text{T}$ and $\text{v}(\phi) = \text{F}$.

Definition 1.3.6. A set Γ of L-formulas is **consistent** if there is no L-formula ϕ such that $\Gamma \vdash_\text{L} \phi$ and $\Gamma \vdash_\text{L} (\neg \phi)$.

Proposition 1.3.7. *Suppose Γ is a consistent set of L-formulas and $\Gamma \nvdash_\text{L} \phi$. Then $\Gamma \cup \{(\neg \phi)\}$ is consistent.*

Proof. Suppose not. So there is some formula ψ with

$$\Gamma \cup \{(\neg \phi)\} \vdash_\text{L} \psi, \tag{6}$$

and

$$\Gamma \cup \{(\neg \phi)\} \vdash_\text{L} (\neg \psi). \tag{7}$$

Apply deduction theorem to (7), $\Gamma \vdash_\text{L} ((\neg \phi) \to (\neg \psi))$. By A3 and MP, we obtain

$$\Gamma \vdash_\text{L} (\psi \to \phi). \tag{8}$$

By (6), (8), and MP, $\Gamma \cup \{(\neg \phi)\} \vdash_\text{L} \phi$. By deduction theorem,

$$\Gamma \vdash_\text{L} ((\neg \phi) \to \phi). \tag{9}$$

By 1.2.7.3, $\vdash_\text{L} (((\neg \phi) \to \phi) \to \phi)$. So by this, (9), and MP, $\Gamma \vdash_\text{L} \phi$. This contradicts $\Gamma \nvdash_\text{L} \phi$. $\square$

---

[3]Exercise: A1 and A3
[4]Exercise

Proposition 1.3.8 (Lindenbaum lemma). *Suppose Γ is a consistent set of L-formulas. Then there is a consistent set of formulas $\Gamma^* \supseteq \Gamma$ such that, for every ϕ, either $\Gamma^* \vdash_L \phi$ or $\Gamma^* \vdash_L (\neg\phi)$. Sometimes say Γ^* is* **complete**.

Proof. The set of L-formulas is countable, so we can list the L-formulas as $\phi_0, \phi_1, \ldots$. This is countable, since the alphabet

$$\neg \quad \rightarrow \quad) \quad (\quad p_1 \quad p_2 \quad \ldots$$

is countable, and the formulas are finite sequences from this alphabet, so there are only countable many. Define inductively the sets of formulas

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \ldots, \qquad \Gamma_0 = \Gamma, \qquad \Gamma_{n+1} = \begin{cases} \Gamma_n & \Gamma_n \vdash_L \phi_n \\ \Gamma_n \cup \{(\neg\phi_n)\} & \Gamma_n \nvdash_L \phi_n \end{cases}.$$

An easy induction using 1.3.7 shows that each Γ_i is consistent. Then let $\Gamma^* = \bigcup_{i \in \mathbb{N}} \Gamma_i$. Claim that Γ^* is consistent. If $\Gamma^* \vdash_L \phi$ and $\Gamma^* \vdash_L (\neg\phi)$, then as deductions are finite sequence of formulas,

$$\Gamma_n \vdash_L \phi, \qquad \Gamma_n \vdash_L (\neg\phi), \qquad n \in \mathbb{N},$$

a contradiction. Let ϕ be any formula. So $\phi = \phi_n$ for some n. If $\Gamma^* \nvdash_L \phi$, then $\Gamma_n \nvdash_L \phi$. So by construction,

$$\Gamma_{n+1} \vdash_L (\neg\phi),$$

as $(\neg\phi) = (\neg\phi_n) \in \Gamma_{n+1}$. Thus $\Gamma^* \vdash_L (\neg\phi)$. □

Lemma 1.3.9. *Let Γ^* be as above. Then there is a valuation v such that, for every L-formula ϕ, $v(\phi) = T$ if and only if $\Gamma^* \vdash_L \phi$.*

The proof is later.

Corollary 1.3.10. *Suppose Δ is a set of L-formulas which is consistent and $\Delta \nvdash_L \phi$. Then there is a valuation v with $v(\Delta) = T$ and $v(\phi) = F$.*

Proof. Let

$$\Gamma = \Delta \cup \{(\neg\phi)\}.$$

By 1.3.7, Γ is consistent. By 1.3.8, there is $\Gamma^* \supseteq \Gamma$ which is still consistent, and such that, for every χ, either $\Gamma^* \vdash_L \chi$ or $\Gamma^* \vdash_L (\neg\chi)$. By 1.3.9, there is a valuation v with $v(\Gamma^*) = T$. In particular, $v(\Delta) = T$ and $v((\neg\phi)) = T$. So $v(\phi) = F$. □

Proof of 1.3.4. Suppose $\nvdash_L \phi$. Apply 1.3.10 with $\Delta = \emptyset$. This is consistent, by the soundness theorem. There is a valuation v with $v(\phi) = F$. □

Proof of 1.3.9. Let Γ^* be a consistent set of L-formulas such that, for every L-formula ϕ, either $\Gamma^* \vdash_L \phi$ or $\Gamma^* \vdash_L (\neg\phi)$. Want a valuation v with $v(\phi) = T$ for all $\phi \in \Gamma^*$, that is $v(\phi) = T$ if and only if $\Gamma^* \vdash_L \phi$. Note that, for each variable p_i, either $\Gamma^* \vdash_L p_i$ or $\Gamma^* \vdash_L (\neg p_i)$. So let v be the valuation with $v(p_i) = T$ if and only if $\Gamma^* \vdash_L p_i$. Prove, by induction on the length of ϕ, that $v(\phi) = T$ if and only if $\Gamma^* \vdash_L \phi$.

- Base case. ϕ is just a propositional variable. This case is by definition of v.

- Inductive step.

  Case 1. ϕ is $(\neg\psi)$.

  $\implies$ As v is a valuation,

  $$\begin{array}{llll} v(\phi) = T & \implies & v(\psi) = F & \text{as } v \text{ is a valuation} \\ & \implies & \Gamma^* \nvdash_L \psi & \text{by the inductive hypothesis} \\ & \implies & \Gamma^* \vdash_L (\neg\psi) & \text{by Lindenbaum property} \\ & \implies & \Gamma^* \vdash_L \phi. \end{array}$$

$\Longleftarrow$ Conversely suppose $\Gamma^* \vdash_{\mathrm{L}} \phi$. Then

$$
\begin{array}{llll}
\Gamma^* \vdash_{\mathrm{L}} \phi & \Longrightarrow & \Gamma^* \nvdash_{\mathrm{L}} \psi & \text{by consistency} \\
& \Longrightarrow & \mathrm{v}\,(\psi) = \mathrm{F} & \text{by the inductive hypothesis} \\
& \Longrightarrow & \mathrm{v}\,((\neg\psi)) = \mathrm{T} & \text{as v is a valuation} \\
& \Longrightarrow & \mathrm{v}\,(\phi) = \mathrm{T}.
\end{array}
$$

Case 2. ϕ is $(\psi \to \chi)$.

$\Longleftarrow$ Suppose $\mathrm{v}\,(\phi) = \mathrm{F}$. Show that $\Gamma^* \nvdash_{\mathrm{L}} \phi$. Then $\mathrm{v}\,(\psi) = \mathrm{T}$ and $\mathrm{v}\,(\chi) = \mathrm{F}$. By the inductive hypothesis, $\Gamma^* \vdash_{\mathrm{L}} \psi$ and $\Gamma^* \nvdash_{\mathrm{L}} \chi$. If $\Gamma^* \vdash_{\mathrm{L}} \phi$, then using $\Gamma^* \vdash_{\mathrm{L}} \psi$ and MP, we get $\Gamma^* \vdash_{\mathrm{L}} \chi$, a contradiction. So $\Gamma^* \nvdash_{\mathrm{L}} \phi$.

$\Longrightarrow$ Suppose $\Gamma^* \nvdash_{\mathrm{L}} \phi$, that is $\Gamma^* \nvdash_{\mathrm{L}} (\psi \to \chi)$. Then

$$\Gamma^* \nvdash_{\mathrm{L}} \chi, \tag{10}$$

as $\vdash_{\mathrm{L}} (\chi \to (\psi \to \chi))$. Also

$$\Gamma^* \nvdash_{\mathrm{L}} (\neg\psi), \tag{11}$$

as $\vdash_{\mathrm{L}} ((\neg\psi) \to (\psi \to \chi))$ by 1.2.7.1. By (10), (11), and the inductive hypothesis, $\mathrm{v}\,(\chi) = \mathrm{F}$ and $\mathrm{v}\,((\neg\psi)) = \mathrm{F}$, so $\mathrm{v}\,(\psi) = \mathrm{T}$. Thus $\mathrm{v}\,(\phi) = \mathrm{F}$, which does the inductive step.

$\square$

Corollary 1.3.11. *Suppose Δ is a set of L-formulas and ϕ is an L-formula. Then*

1. *Δ is consistent if and only if there is a valuation v with $\mathrm{v}\,(\Delta) = \mathrm{T}$, and*

2. *$\Delta \vdash_{\mathrm{L}} \phi$ if and only if, for every valuation v with $\mathrm{v}\,(\Delta) = \mathrm{T}$, we have $\mathrm{v}\,(\phi) = \mathrm{T}$.*

Proof. Deduce these from the preliminaries to the completeness theorem. [5] A warning is that, in 2, do not assume that Δ is consistent. $\square$

Theorem 1.3.12 (Compactness theorem for L)**.** *Suppose Δ is a set of L-formulas. The following are equivalent.*

1. *There is a valuation v with $\mathrm{v}\,(\Delta) = \mathrm{T}$.*

2. *For every finite subset $\Delta_0 \subseteq \Delta$, there is a valuation w with $\mathrm{w}\,(\Delta_0) = \mathrm{T}$.*

Proof. By 1.3.11, 1 holds if and only if Δ is consistent. Similarly, 2 holds if and only if every finite subset of Δ is consistent. But if $\Delta \vdash_{\mathrm{L}} \psi$ and $\Delta \vdash_{\mathrm{L}} (\neg\psi)$, then, as deductions are finite, and therefore only involve finitely many formulas in Δ, for some finite $\Delta_0 \subseteq \Delta$, $\Delta_0 \vdash_{\mathrm{L}} \psi$ and $\Delta_0 \vdash_{\mathrm{L}} (\neg\psi)$. $\square$

Example. Let
$$P = \{\text{sequences of } \{\mathrm{T}, \mathrm{F}\}\} = \{\text{functions } f : \mathbb{N} \to \{\mathrm{T}, \mathrm{F}\}\}.$$

Topologise with basic open sets. For $a_1, \ldots, a_n = \mathrm{T}, \mathrm{F}$, consider

$$\mathrm{O}\,(a_1, \ldots, a_n) = \{\text{all sequences starting } a_1, \ldots, a_n, \ldots\}.$$

Use the compactness theorem to prove P is compact. [6]

Lecture 7 is a problems class.

---

[5] Exercise

[6] Exercise

13

2   Predicate logic

The following is the plan.

- Semantics.

  - Introduce the mathematical objects, the first-order structures.
  - Introduce the formulas, the first-order languages.

- Syntax.

  - Describe a formal system.
  - Show that its theorems are precisely the formulas true in all structures. This is Gödel's completeness theorem.

2.1   Structures

Definition 2.1.1. Suppose A is a set and $n \in \mathbb{N}_{\geq 1}$.

- An n-**ary relation** on A is a subset

$$\overline{R} \subseteq A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\},$$

- An n-**ary function** on A is a function
$$\overline{f} : A^n \to A.$$

Example.

- The ordering $\leq$ on $\mathbb{R}$ is a binary relation on $\mathbb{R}$.

- $+$ on $\mathbb{C}$ is a binary function on $\mathbb{C}$.

- The even integers as a subset of $\mathbb{Z}$ is a unary relation on $\mathbb{Z}$.

Notation. If $\overline{R} \subseteq A^n$ is an n-ary relation and $a_1, \ldots, a_n \in A$, write $\overline{R}(a_1, \ldots, a_n)$ to mean $(a_1, \ldots, a_n) \in \overline{R}$.

Definition 2.1.2. A **first-order structure** $\mathcal{A}$ consists of

- a non-empty set A, the **domain** of $\mathcal{A}$,

- a set of **relations** on A,
$$\left\{ \overline{R_i} \subseteq A^{n_i} \mid i \in I \right\},$$

- a set of **functions** on A,
$$\left\{ \overline{f_j} : A^{m_j} \to A \mid j \in J \right\},$$

- a set of **constants**, just elements of A,
$$\{ \overline{c_k} \mid k \in K \}.$$

The sets I, J, K are indexing sets, which can be empty. Usually subsets of $\mathbb{N}$. The information

$$(n_i \mid i \in I), \qquad (m_j \mid j \in J), \qquad K$$

is called the **signature** of $\mathcal{A}$. Might denote the structure by

$$\mathcal{A} = \left\langle A; \left(\overline{R_i} \mid i \in I \right), \left(\overline{f_j} \mid j \in J \right), \left(\overline{c_k} \mid k \in K \right) \right\rangle$$
$$= \langle \text{domain; relations, functions, constants} \rangle.$$

Example 2.1.3.

- Orderings.
$$A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \qquad I = \{1\}, \qquad J = \emptyset, \qquad K = \emptyset$$
$$\overline{R_1}(a_1, a_2) \qquad \text{to mean} \qquad a_1 < a_2$$

- Groups.

$\overline{R}$	the binary relation for equality
$\overline{m}$	the binary function for multiplication
$\overline{i}$	the unary function for inversion
$\overline{e}$	the constant for identity element

- Rings.

$\overline{R}$	the binary relation for equality
$\overline{m}$	the binary function for multiplication
$\overline{a}$	the binary function for addition
$\overline{n}$	the binary function for negation
$\overline{0}$	the constant for zero
$\overline{1}$	the constant for one

- Graphs.

$\overline{R}$	the binary relation for equality
$\overline{E}$	the binary relation for adjacency

2.2   First-order languages

Definition 2.2.1. A **first-order language** $\mathcal{L}$ has an alphabet of **symbols** of the following types.

Variables	x_0	x_1	$\ldots$
Connectives	$\neg$	$\rightarrow$	
Punctuation	(	)	,
Quantifier	$\forall$		
Relation symbols	$R_i,$	$i \in I$	
Function symbols	$f_j,$	$j \in J$	
Constant symbols	$c_k,$	$k \in K$	

Here I, J, K are indexing sets, which could have $J, K = \emptyset$.

- Each R_i comes equipped with an arity n_i.

- Each f_j comes equipped with an arity m_j.

The information
$$(n_i \mid i \in I), \qquad (m_j \mid j \in J), \qquad K$$
is called the **signature** of $\mathcal{L}$.

Definition 2.2.2. A **term** of $\mathcal{L}$ is defined as follows.

- Any variable is a term.

- Any constant symbol is a term.

- If f is an m-ary function symbol of $\mathcal{L}$ and $t_1, \ldots, t_m$ are terms, then

$$f(t_1, \ldots, t_m)$$

  is also a term.

- Any term arises in this way.

Example. Suppose $\mathcal{L}$ has a binary function symbol f and constant symbols c_1 and c_2.

- Some terms.

$$c_1 \qquad c_2 \qquad x_1 \qquad f(c_1, x_1) \qquad f(f(c_1, x_2), c_2) \qquad f(x_1, f(f(c_1, x_2), c_2))$$

- Not terms.

$$ffx_1 \quad \text{(not well-formed)}$$

Definition 2.2.3. Use the previous notation.

- An **atomic formula** of $\mathcal{L}$ is of the form

$$R(t_1, \ldots, t_n),$$

  where R is an n-ary relation symbol of $\mathcal{L}$ and $t_1, \ldots, t_n$ are terms.

- The formulas of $\mathcal{L}$ are defined as follows.

  – Any atomic formula is a formula.
  – If ϕ and ψ are $\mathcal{L}$-formulas, then

$$(\neg\phi), \qquad (\phi \to \psi), \qquad (\forall x)\,\phi$$

  are $\mathcal{L}$-formulas, where x is any variable.
  – Every $\mathcal{L}$-formula arises in this way.

Example. Suppose $\mathcal{L}$ has a binary function symbol f, a unary relation symbol P, a binary relation symbol R, and constant symbols c_1 and c_2.

- Some terms.
$$x_1 \qquad c_1 \qquad f(x_1, c_1) \qquad f(f(x_1, c_1), x_2)$$

- Some atomic formulas.
$$P(x_1) \qquad R(f(x_1, c_1), x_2)$$

- Some formulas.
$$(\forall x_1)(R(f(x_1, c_1), x_2) \to P(x_1))$$

Definition 2.2.4. Suppose ϕ and ψ are $\mathcal{L}$-formulas.

- $(\exists x)\,\phi$ means $(\neg(\forall x)(\neg\phi))$.

- $(\phi \vee \psi)$ means $((\neg\phi) \to \psi)$, etc, as in propositional logic.

Definition 2.2.5. Suppose $\mathcal{L}$ is a first-order language with relation symbols R_i of arity n_i for $i \in I$, function symbols f_j of arity m_j for $j \in J$, and constant symbols c_k for $k \in K$. An $\mathcal{L}$-**structure** is a structure

$$\mathcal{A} = \left\langle A; \left(\overline{R_i} \mid i \in I\right), \left(\overline{f_j} \mid j \in J\right), \left(\overline{c_k} \mid k \in K\right) \right\rangle$$

of the same signature as $\mathcal{L}$.

There is a correspondence between the relation, function, and constant symbols of $\mathcal{L}$ and the actual relations, functions, and constants in $\mathcal{A}$, and the arities match up. This correspondence

$$R_i \longleftrightarrow \overline{R_i}, \qquad f_j \longleftrightarrow \overline{f_j}, \qquad c_k \longleftrightarrow \overline{c_k},$$

or $\mathcal{A}$, is called an **interpretation** of $\mathcal{L}$.

Definition 2.2.6. With the same notation, suppose $\mathcal{A}$ is an $\mathcal{L}$-structure. A **valuation** in $\mathcal{A}$ is a function v from the set of terms of $\mathcal{L}$ to A satisfying

- $v(c_k) = \overline{c_k}$, and

- if $t_1, \ldots, t_m$ are terms of $\mathcal{L}$ and f is an m-ary function symbol, then

$$v(f(t_1, \ldots, t_m)) = \overline{f}(v(t_1), \ldots, v(t_m)),$$

  where $\overline{f}$ is an interpretation of f in $\mathcal{A}$.

Lemma 2.2.7. *Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and $a_0, a_1, \cdots \in A$. Then there is a unique valuation v, in $\mathcal{A}$, with $v(x_l) = a_l$, for all $l \in \mathbb{N}$, where the variables of $\mathcal{L}$ are $x_0, x_1, \ldots$.*

Proof. By induction on the length of terms. Show that, if we let

- $v(x_l) = a_l$ for all $l \in \mathbb{N}$,

- $v(c_k) = \overline{c_k}$ for all $k \in K$, and

- $v(f(t_1, \ldots, t_m)) = \overline{f}(v(t_1), \ldots, v(t_m))$,

then v is a well-defined valuation. [7] $\square$

Example. Groups. Signature, as in 2.1.3, has

- a binary relation symbol R, for equality,

- a binary function symbol m, for multiplication,

- a unary function symbol i, for inversion, and

- a constant symbol e, for identity element.

Let G be a group and $g, h \in G$. Let v be a valuation with $v(x_0) = g$ and $v(x_1) = h$. Then

$$v(m(m(x_0, x_1), i(x_0))) = \overline{m}(v(m(x_0, x_1)), v(i(x_0))) = \overline{m}(\overline{m}(v(x_0), v(x_1)), \overline{i}(v(x_0)))$$
$$= \overline{m}(\overline{m}(g, h), \overline{i}(g)) = \overline{m}(gh, g^{-1}) = ghg^{-1}.$$

Definition 2.2.8. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and x_l is any variable. Suppose v and w are valuations in $\mathcal{A}$. We say v and w are x_l-**equivalent** if $v(x_m) = w(x_m)$ whenever $m \neq l$.

Definition 2.2.9. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and v is a valuation in $\mathcal{A}$. Define, for an $\mathcal{L}$-formula ϕ, what is meant by v **satisfies** ϕ, in $\mathcal{A}$.

- Atomic formulas. Suppose R is an n-ary relation symbol and $t_1, \ldots, t_n$ are terms of $\mathcal{L}$. Then

  v satisfies the atomic formula $R(t_1, \ldots, t_n)$ $\quad \Longleftrightarrow \quad$ $\overline{R}(v(t_1), \ldots, v(t_n))$ holds in $\mathcal{A}$.

- Suppose ϕ and ψ are $\mathcal{L}$-formulas, and we already know about valuations satisfying ϕ and ψ. Then

v satisfies $(\neg\phi)$ in $\mathcal{A}$	$\Longleftrightarrow$	v does not satisfy ϕ in $\mathcal{A}$,
v satisfies $(\phi \to \psi)$ in $\mathcal{A}$	$\Longleftrightarrow$	it is not the case that v satisfies ϕ in $\mathcal{A}$ and v does not satisfy ψ in $\mathcal{A}$,
v satisfies $(\forall x_l)\phi$ in $\mathcal{A}$	$\Longleftrightarrow$	whenever w is a valuation in $\mathcal{A}$ which is x_l-equivalent to v, then w satisfies ϕ *in* $\mathcal{A}$.

Remark. 2.2.9 does not work if we allow the empty structure.

Notation. If v satisfies ϕ, write $v[\phi] = T$. If v does not satisfy ϕ, write $v[\phi] = F$. If every valuation in $\mathcal{A}$ satisfies ϕ, say that ϕ is **true** in $\mathcal{A}$ or $\mathcal{A}$ is a **model** of ϕ, and write $\mathcal{A} \vDash \phi$. If $\mathcal{A} \vDash \phi$ for every $\mathcal{L}$-structure $\mathcal{A}$, we say that ϕ is **logically valid**, and write $\vDash \phi$.

These are the analogues of tautologies in the propositional logic. The difference is that in propositional logic there is an algorithm to decide whether a given formula is a tautology. There is no such algorithm to decide whether a given $\mathcal{L}$-formula is logically valid or not. This is a consequence of Gödel's incompleteness theorem.

Lecture 10
Thursday
25/10/18

---
[7]Exercise

Example 2.2.10.

- Suppose $\mathcal{L}$ has a binary relation symbol R. The $\mathcal{L}$-formula

$$(R(x_1, x_2) \to (R(x_2, x_3) \to R(x_1, x_3)))$$

  is true in $\mathcal{A} = \langle \mathbb{N}; R \rangle$, where R is interpreted as $<$. If not, there is a valuation v, in $\mathcal{A}$, such that v satisfies $R(x_1, x_2)$ and v does not satisfy $(R(x_2, x_3) \to R(x_1, x_3))$. So

$$\text{v}[R(x_2, x_3)] = \text{T}, \qquad \text{v}[R(x_1, x_3)] = \text{F}.$$

  Let $\text{v}(x_i) = a_i \in \mathbb{N}$. So

$$a_1 < a_2, \qquad a_2 < a_3, \qquad a_1 \not< a_3.$$

  As $<$ is transitive on $\mathbb{N}$, this is a contradiction.

- The same formula is not true in the structure $\mathcal{B}$ with domain $\mathbb{N}$ where we interpret $R(x_i, x_j)$ as $x_i \neq x_j$. Take a valuation in $\mathcal{B}$ with

$$\text{v}(x_1) = 1 = \text{v}(x_3), \qquad \text{v}(x_2) = 2.$$

  Then v does not satisfy the formula in $\mathcal{B}$.

- Recall that $(\exists x_1)\,\phi$ is an abbreviation for $(\neg(\forall x_1)(\neg\phi))$. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and ϕ an $\mathcal{L}$-formula. Let v be a valuation in $\mathcal{A}$. Claim that then v satisfies $(\exists x_1)\,\phi$ in $\mathcal{A}$ if and only if there is a valuation w, which is x_1-equivalent to v, such that w satisfies ϕ.

  $\implies$ Suppose v satisfies $(\neg(\forall x_1)(\neg\phi))$. Using 2.2.9, v does not satisfy $(\forall x_1)(\neg\phi)$. So there is valuation w, x_1-equivalent to v, such that w does not satisfy $(\neg\phi)$. Such a w satisfies ϕ.

  $\impliedby$ Exercise. [8]

Example 2.2.11.

$$(\forall x_1)(\exists x_2)\,R(x_1, x_2)$$

is true in $\langle \mathbb{Z}; < \rangle$ and $\langle \mathbb{N}; < \rangle$, but not in $\langle \mathbb{N}; > \rangle$.

Example 2.2.12. Suppose ϕ is any $\mathcal{L}$-formula. Then

1. $((\exists x_1)(\forall x_2)\,\phi \to (\forall x_2)(\exists x_1)\,\phi)$ is logically valid, and

2. $((\forall x_2)(\exists x_1)\,\phi \to (\exists x_1)(\forall x_2)\,\phi)$ is not necessarily logically valid.

Proof. Exercise. [9]

1. Argument with valuation.

2. Give an example.

$\square$

Example. Consider the propositional formula

$$\chi : (p_1 \to (p_2 \to p_1)).$$

Suppose $\mathcal{L}$ is a first-order language and ϕ_1 and ϕ_2 are $\mathcal{L}$-formulas. Substitute ϕ_1 in place of p_1, and ϕ_2 in place of p_2, in χ. We obtain an $\mathcal{L}$-formula

$$\theta : (\phi_1 \to (\phi_2 \to \phi_1)).$$

Check that, as χ is a tautology, θ is logically valid.

Definition 2.2.13. Suppose χ is an $\mathcal{L}$-formula involving propositional variables $p_1, \ldots, p_n$. Suppose $\mathcal{L}$ is a first-order language and $\phi_1, \ldots, \phi_n$ are $\mathcal{L}$-formulas. A **substitution instance** of χ is obtained by replacing each p_i in χ by ϕ_i for $i = 1, \ldots, n$.

Call the result θ.

---

[8]Exercise

[9]Exercise

Theorem 2.2.14.

- *θ is an $\mathcal{L}$-formula, and*

- *if χ is a tautology, then θ is logically valid.*

Proof. Take an $\mathcal{L}$-structure $\mathcal{A}$ and a valuation v in $\mathcal{A}$. Use this to define a propositional valuation w with

$$\mathrm{w}\left(p_i\right) = \mathrm{v}\left[\phi_i\right], \qquad i \leq n.$$

Then prove, by induction on the number of connectives in χ, that

$$\mathrm{w}\left(\chi\right) = \mathrm{v}\left[\theta\right].$$

In particular, if χ is a tautology, then $\mathrm{v}\left[\theta\right] = \mathrm{T}$. [10] For example, in the inductive step, consider

$$\chi : \left(\alpha \to \beta\right).$$

So θ is $(\theta_1 \to \theta_2)$, where θ_1 is obtained from α and θ_2 is obtained from β. By the induction hypothesis, $\mathrm{w}\left(\alpha\right) = \mathrm{v}\left[\theta_1\right]$ and $\mathrm{w}\left(\beta\right) = \mathrm{v}\left[\theta_2\right]$. So $\mathrm{w}\left((\alpha \to \beta)\right) = \mathrm{v}\left[(\theta_1 \to \theta_2)\right]$, etc. $\qquad\square$

Note. Not all logically valid formulas arise in this way.

Example.

$$\left(\left(\exists x_2\right)\left(\forall x_1\right)\phi \to \left(\forall x_1\right)\left(\exists x_2\right)\phi\right).$$

2.3   Bound and free variables in formulas

Definition 2.3.1. Suppose ϕ and ψ are $\mathcal{L}$-formulas and $(\forall x_i)\phi$ occurs as a subformula of ψ, that is ψ is

$$\ldots \quad \left(\forall x_i\right)\phi \quad \ldots.$$

- We say that ϕ is the **scope** of that quantifier $(\forall x_i)$ here in ψ. An occurrence of a variable x_j in ψ is **bound** if it is in the scope of a quantifier $(\forall x_j)$ in ψ, or it is the x_j here in $(\forall x_j)$.

- Otherwise, it is a **free** occurrence, of x_j. Variables having a free occurrence in ψ are called **free variables** of ψ.

- A formula with no free variables is called a **closed formula** or a **sentence**, of $\mathcal{L}$.

Example.

$$\psi_1 : \left(R_1\left(\overbrace{x_1, x_2}^{\text{free}} \right) \to \left(\forall x_3\right)\underbrace{R_2\left(\overbrace{x_1}^{\text{free}}, \overbrace{x_3}^{\text{bound}} \right)}_{\text{scope of } (\forall x_3)} \right)$$

$$\psi_2 : \left(\underbrace{\left(\forall x_1\right)R_1\left(\overbrace{x_1}^{\text{bound}}, \overbrace{x_2}^{\text{free}} \right)}_{\text{scope of } (\forall x_1)} \to R_2\left(\overbrace{x_1, x_2}^{\text{free}} \right) \right)$$

$$\psi_3 : \left(\forall x_1\right)\underbrace{\left(R_1\left(\overbrace{x_1}^{\text{bound}}, \overbrace{x_2}^{\text{free}} \right) \to R_2\left(\overbrace{x_1}^{\text{bound}}, \overbrace{x_2}^{\text{free}} \right) \right)}_{\text{scope of } (\forall x_1)}$$

$$\psi_4 : \left(\underbrace{\left(\exists x_1\right)R_1\left(\overbrace{x_1}^{\text{bound}}, \overbrace{x_2}^{\text{free}} \right)}_{\text{scope of } (\exists x_1)} \to \underbrace{\left(\forall x_2\right)R_2\left(\overbrace{x_2}^{\text{bound}}, \overbrace{x_3}^{\text{free}} \right)}_{\text{scope of } (\forall x_2)} \right)$$

---

[10]Exercise

Definition 2.3.2. If ψ is an $\mathcal{L}$-formula with free variables amongst $x_1, \ldots, x_n$, we might write

$$\psi(x_1, \ldots, x_n),$$

instead of ψ. If $t_1, \ldots, t_n$ are terms, by

$$\psi(t_1, \ldots, t_n),$$

we mean the $\mathcal{L}$-formula obtained by replacing each free occurrence of x_i in ψ by t_i.

Example. Let t_1 be $f_1(x_1)$, t_2 be $f_2(x_1, x_2)$, and

$$\psi(x_1, x_2): \left((\forall x_1) R\left(x_1, \overbrace{x_2}^{\text{free}} \right) \to (\forall x_3) R\left(\overbrace{x_1}^{\text{free}}, \overbrace{x_2}^{\text{free}}, x_3 \right) \right).$$

So

$$\psi(t_1, t_2): ((\forall x_1) R_1(x_1, f_2(x_1, x_2)) \to (\forall x_3) R_2(f_1(x_1), f_2(x_1, x_2), x_3)).$$

Theorem 2.3.3. *Suppose ϕ is a closed $\mathcal{L}$-formula and $\mathcal{A}$ is an $\mathcal{L}$-structure. Then either $\mathcal{A} \vDash \phi$ or $\mathcal{A} \vDash (\neg\phi)$. More generally, if ϕ has free variables amongst $x_1, \ldots, x_n$, and v and w are valuations in $\mathcal{A}$ with*

$$\mathrm{v}(x_i) = \mathrm{w}(x_i), \qquad i = 1, \ldots, n,$$

then $\mathrm{v}[\phi] = \mathrm{T}$ if and only if $\mathrm{w}[\phi] = \mathrm{T}$. Allow $n = 0$ here, for no free variables.

Proof. Note that the first statement follows from the generalisation, since if ϕ has no free variables, then, for any valuations v and w in $\mathcal{A}$, they agree on the free variables of ϕ, so

$$\mathrm{v}[\phi] = \mathrm{w}[\phi].$$

Prove the generalisation by induction on the number of connectives and quantifiers in ϕ.

- Base case. ϕ is atomic. Let

$$\phi: R(t_1, \ldots, t_m),$$

  where t_j are terms. The t_j only involve variables amongst $x_1, \ldots, x_n$. As v and w agree on these variables,

$$\mathrm{v}(t_j) = \mathrm{w}(t_j).$$

  So

$$\mathrm{v}[R(t_1, \ldots, t_m)] = \mathrm{T} \quad \Longleftrightarrow \quad \overline{R}(\mathrm{v}(t_1), \ldots, \mathrm{v}(t_m)) \quad \Longleftrightarrow \quad \mathrm{w}[R(t_1, \ldots, t_m)] = \mathrm{T}.$$

- Inductive step. ϕ is $(\neg\psi)$, $(\psi \to \chi)$, or $(\forall x_i)\psi$. [11] Suppose ϕ is $(\forall x_i)\psi$. Suppose $\mathrm{v}[\phi] = \mathrm{F}$. By 2.2.9, there is a valuation v', x_i-equivalent to v, with $\mathrm{v}'[\psi] = \mathrm{F}$. The free variables of ψ are amongst $x_1, \ldots, x_n, x_i$. Let w' be the valuation x_i-equivalent to w with

$$\mathrm{w}'(x_i) = \mathrm{v}'(x_i).$$

  Then v' and w' agree on the free variables of ψ. By the induction hypothesis,

$$\mathrm{v}'[\psi] = \mathrm{w}'[\psi],$$

  so $\mathrm{w}'[\psi] = \mathrm{F}$. As w' is x_i-equivalent to w, we obtain $\mathrm{w}[(\forall x_i)\psi] = \mathrm{F}$.

$\square$

Remark 2.3.4. If $\mathcal{A}$ is an $\mathcal{L}$-structure and $\psi(x_1, \ldots, x_n)$ an $\mathcal{L}$-formula, whose free variables are amongst $x_1, \ldots, x_n$, and $a_1, \ldots, a_n \in A$, for domain A, then we write

$$\mathcal{A} \vDash \psi(a_1, \ldots, a_n),$$

to mean $\mathrm{v}[\psi] = \mathrm{T}$ for every valuation v in $\mathcal{A}$ with

$$\mathrm{v}(x_i) = a_i, \qquad i = 1, \ldots, n.$$

Remark. By the proof of 2.3.3, this holds if $\mathrm{v}[\psi] = \mathrm{T}$ for some such valuation.

---

[11]Exercise: first two cases

Example. A warning example, where $\mathcal{A} \vDash (\forall x_1) \, \phi \, (x_1)$, but we have a term t, and a valuation v in $\mathcal{A}$, with $\text{v} \, [\phi \, (t)] = \text{F}$. Let

$$\phi \, (x_1) : \left((\forall x_2) \, \underbrace{R \left(\overbrace{x_1}^{\text{free}}, x_2 \right)}_{\text{scope of } (\forall x_2)} \to S \left(\overbrace{x_1}^{\text{free}} \right) \right).$$

Let t_1 be x_2. Then $\phi \, (t_1)$ is

$$((\forall x_2) \, R \, (x_2, x_2) \to S \, (x_2)).$$

Suppose $\mathcal{A} = \langle \mathbb{N}; \leq, = 0 \rangle$.

- Domain is $\mathbb{N} = \{0, 1, \dots\}$.

- $R \, (x_1, x_2)$ is interpreted as $x_1 \leq x_2$.

- $S \, (x_1)$ is interpreted as $x_1 = 0$.

So $\mathcal{A} \vDash (\forall x_1) \, \phi \, (x_1)$. But if we choose a valuation $\text{v} \, (x_2) = 1$, then $\text{v} \, [\phi \, (t_1)] = \text{F}$ in $\mathcal{A}$.

Definition 2.3.5. Let ϕ be an $\mathcal{L}$-formula, x_i a variable, and t an $\mathcal{L}$-term. We say t is **free for** x_i in ϕ if there is no variable x_j in t, such that x_i has a free occurrence within the scope of a quantifier $(\forall x_j)$ in ϕ.

Example. Let $t = f \, (x_3, x_2, x_5)$. Let

$$\phi_1 : (((\forall x_2) \, R \, (x_2, x_4) \to K \, (x_1)) \to (\forall x_1) \, R \, (x_1, x_1)),$$
$$\phi_2 : ((\forall x_2) \, (R \, (x_2, x_4) \to (\forall x_1) \, K \, (x_1)) \to (\forall x_2) \, R \, (x_1, x_1)).$$

For which is t free for x_1? ϕ_1. [12]

Theorem 2.3.6. *Suppose $\phi \, (x_1)$ is an $\mathcal{L}$-formula, possibly with other free variables. Let t be a term free for x_1 in ϕ, then*

$$\vDash ((\forall x_1) \, \phi \, (x_1) \to \phi \, (t)).$$

In particular, if $\mathcal{A}$ is an $\mathcal{L}$-structure with $\mathcal{A} \vDash (\forall x_1) \, \phi \, (x_1)$, then $\mathcal{A} \vDash \phi \, (t)$.

Lemma 2.3.7. *With this notation, suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and v is a valuation in $\mathcal{A}$. Let v$'$ be the valuation in $\mathcal{A}$ which is x_1-equivalent to v, with $\text{v}' \, (x_1) = \text{v} \, (t)$. Then $\text{v}' \, [\phi \, (x_1)] = \text{T}$ if and only if $\text{v} \, [\phi \, (t)] = \text{T}$.*

Proof of 2.3.6. Suppose v is a valuation with $\text{v} \, [\phi \, (t)] = \text{F}$. Show that

$$\text{v} \, [(\forall x_1) \, \phi \, (x_1)] = \text{F},$$

then

$$\text{v} \, [((\forall x_1) \, \phi \, (x_1) \to \phi \, (t))] = \text{T}.$$

Take v$'$, x_1-equivalent to v, and

$$\text{v}' \, (x_1) = \text{v} \, (t).$$

Then by 2.3.7,

$$\text{v}' \, [\phi \, (x_1)] = \text{F}.$$

Thus $\text{v} \, [(\forall x_1) \, \phi \, (x_1)] = \text{F}$. $\qquad\qquad \square$

Proof of 2.3.7. Appendix A.1. $\qquad\qquad \square$

---

[12]Exercise

2.4 The formal system $K_{\mathcal{L}}$

Definition 2.4.1. Suppose $\mathcal{L}$ is a first-order language. The formal system $K_{\mathcal{L}}$ has, as formulas, $\mathcal{L}$-formulas, and the following.

- Axioms. For $\mathcal{L}$-formulas ϕ, χ, ψ,

   (A1) $(\phi \to (\psi \to \phi))$,
   (A2) $((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))$,
   (A3) $(((\neg \phi) \to (\neg \psi)) \to (\psi \to \phi))$,

   (K1) $((\forall x_i) \phi(x_i) \to \phi(t))$, where t is a term free for x_i in ϕ, and ϕ can have other free variables, and
   (K2) $((\forall x_i)(\phi \to \psi) \to (\phi \to (\forall x_i)\psi))$, if x_i is not free in ϕ.

- Deduction rules.

   (MP) Modus Ponens. From ϕ and $(\phi \to \psi)$, deduce ψ.
   (Gen) **Generalisation**. From ϕ, deduce $(\forall x_i)\phi$.

A **proof** in $K_{\mathcal{L}}$ is a finite sequence of $\mathcal{L}$-formulas, each of which is an axiom, or deduced from previous formulas in the proof using a rule of deduction. A **theorem** of $K_{\mathcal{L}}$ is the last formula in some proof. Write $\vdash_{K_{\mathcal{L}}} \phi$ if ϕ is a theorem in $K_{\mathcal{L}}$.

Note. Books do not always use $K_{\mathcal{L}}$, that is they write $\vdash \phi$.

Definition 2.4.2. Suppose Σ is a set of $\mathcal{L}$-formulas and ψ is an $\mathcal{L}$-formula. A **deduction** of ψ from Σ is a finite sequence of formulas, ending with ψ, each of which is one of

- an axiom,

- a formula in Σ, or

- obtained from earlier formulas in the deduction using MP or Gen, with the restriction that, when Gen is applied, it does not involve a variable occurring freely in a formula in Σ.

Write $\Sigma \vdash_{K_{\mathcal{L}}} \psi$ if there is a deduction from Σ to ψ.

Lecture 13 is a problems class.

Remark 2.4.3.

- If Σ consists of closed formulas, do not need to worry about the restriction on Gen.

- $\phi \vdash_{K_{\mathcal{L}}} (\forall x_1) \phi$.

Theorem 2.4.4. *Suppose ϕ is an $\mathcal{L}$-formula which is a substitution instance of a tautology in propositional logic. Then $\vdash_{K_{\mathcal{L}}} \phi$.*

Example. For an $\mathcal{L}$-formula ϕ,

$$\vdash_{K_{\mathcal{L}}} ((\neg(\neg\phi)) \to \phi),$$

as this is a substitution instance of

$$\vdash_{K_{\mathcal{L}}} ((\neg(\neg p_1)) \to p_1).$$

Proof. There is a tautology χ with propositional variables $p_1, \ldots, p_n$ and $\mathcal{L}$-formulas $\psi_1, \ldots, \psi_n$, such that ϕ is obtained from χ by substituting ψ_i for p_i for $i = 1, \ldots, n$. By completeness of propositional logic in 1.3.4, there is a proof in L of χ,

$$\chi_1, \ldots, \chi_r,$$

where each χ_i is a propositional formula, that is in L, and $\chi_r = \chi$. If we substitute $\psi_1, \ldots, \psi_n$ for $p_1, \ldots, p_n$ in all χ_j, we obtain a sequence of $\mathcal{L}$-formulas,

$$\phi_1, \ldots, \phi_r,$$

which is a proof of $\phi = \phi_r$ in $K_{\mathcal{L}}$. $\qquad\square$

Theorem 2.4.5 (Soundness of $K_{\mathcal{L}}$). *If $\vdash_{K_{\mathcal{L}}} \phi$, then $\vDash \phi$, that is it is logically valid.*

Proof. Like in the proof for L, we need to show

1. axioms are logically valid, and

2. deduction rules preserve logical validity.

1. A1, A2, A3 are substitution instances of propositional tautologies, by 2.2.1, so are logically valid by 2.4.4. K1 is logically valid by 2.3.6. K2 is $((\forall x_i)(\phi \to \psi) \to (\phi \to (\forall x_i)\psi))$, if x_i is not free in ϕ. Suppose we have valuation v such that $v\,[(\phi \to (\forall x_i)\psi)] = F$. So

$$v\,[\phi] = T, \qquad v\,[(\forall x_i)\psi] = F.$$

So there is a valuation v', x_i-equivalent to v, with $v'\,[\psi] = F$. Then v and v' agree on all variables free in ϕ. So by 2.3.3,
$$v\,[\phi] = v'\,[\phi] = T,$$
so $v'\,[(\phi \to \psi)] = F$. Thus $v\,[(\forall x_i)(\phi \to \psi)] = F$, so $v\,[K2] = T$.

2. For MP, if $\vDash \phi$ and $\vDash (\phi \to \psi)$, then $\vDash \psi$. For Gen, if $\vDash \phi$, then $\vDash (\forall x_i)\phi$. [13]

$\square$

Example 2.4.6. Suppose $\Sigma \vdash_{K_{\mathcal{L}}} \psi$, then for every valuation v with $v\,[\sigma] = T$ for all $\sigma \in \Sigma$, we have $v\,[\psi] = T$.

Proof. Exercise. [14] $\square$

Corollary 2.4.7. *There is no $\mathcal{L}$-formula ϕ with $\vdash_{K_{\mathcal{L}}} \phi$ and $\vdash_{K_{\mathcal{L}}} (\neg\phi)$.*

Theorem 2.4.8 (Deduction theorem). *Suppose $\mathcal{L}$ is a first-order language, Σ is a set of $\mathcal{L}$-formulas, and ϕ and ψ are $\mathcal{L}$-formulas. Then if $\Sigma \cup \{\phi\} \vdash_{K_{\mathcal{L}}} \psi$, then $\Sigma \vdash_{K_{\mathcal{L}}} (\phi \to \psi)$.*

Proof. Follows proof of deduction theorem for L in 1.2.5, by induction on the length of the deduction.

- Base case. One line deduction. Argue exactly as in 1.2.5. Note that $\vdash_{K_{\mathcal{L}}} (\phi \to \phi)$ by 2.4.4.

- Inductive step. Suppose ψ follows from earlier formulas in the deduction using MP or Gen. MP is exactly as in 1.2.5. For Gen, suppose ψ is obtained using Gen, then ψ is $(\forall x_i)\theta$ and

$$\Sigma \cup \{\phi\} \vdash_{K_{\mathcal{L}}} \theta,$$

and x_i is not free in any formula in $\Sigma \cup \{\phi\}$. By induction, we have

$$\Sigma \vdash_{K_{\mathcal{L}}} (\phi \to \theta).$$

By K2,
$$\Sigma \vdash_{K_{\mathcal{L}}} ((\forall x_i)(\phi \to \theta) \to (\phi \to (\forall x_i)\theta)).$$

By Gen,
$$\Sigma \vdash_{K_{\mathcal{L}}} (\forall x_i)(\phi \to \theta),$$

for x_i not free in any formula in Σ. So by MP, we get $\Sigma \vdash_{K_{\mathcal{L}}} (\phi \to (\forall x_i)\theta)$, which is $\Sigma \vdash_{K_{\mathcal{L}}} (\phi \to \psi)$.

$\square$

---

[13]Exercise
[14]Exercise

2.5   Gödel's completeness theorem

Definition 2.5.1. A set Σ of $\mathcal{L}$-formulas is **consistent** if there is no formula ϕ with

$$\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \phi, \qquad \Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} (\neg\phi).$$

By soundness, or 2.4.7, $\emptyset$ is consistent, so $\mathrm{K}_{\mathcal{L}}$ is consistent.

Remark. If Σ is inconsistent, then

$$\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \chi,$$

for any $\mathcal{L}$-formula χ.

Recall that a closed $\mathcal{L}$-formula is one without free variables, sometimes called a sentence of $\mathcal{L}$. Show that, if Σ is a set of closed $\mathcal{L}$-formulas which is consistent, then there is an $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$. For a simplification, suppose that $\mathcal{L}$ is countable, that is the variables are $x_0, x_1, \ldots$, and there are countably many relation, function, and constant symbols. So we can enumerate the $\mathcal{L}$-formulas, or any subset thereof, as a list indexed by $\mathbb{N}$. Enumerate the closed $\mathcal{L}$-formulas as

$$\psi_0, \psi_1, \cdots \in \{\psi_i : i \in \mathbb{N}\}.$$

Proposition 2.5.2. *Suppose Σ is a consistent set of closed $\mathcal{L}$-formulas and ϕ is a closed $\mathcal{L}$-formula.*

  1. *Comparing 1.3.7, if $\Sigma \nvdash_{\mathrm{K}_{\mathcal{L}}} \phi$, then $\Sigma \cup \{(\neg\phi)\}$ is consistent.*

  2. *Comparing the Lindenbaum lemma in 1.3.8, there is a consistent set $\Sigma^* \supseteq \Sigma$ of closed $\mathcal{L}$-formulas such that, for every closed $\mathcal{L}$-formula ψ, either $\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}}} \psi$ or $\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}}} (\neg\psi)$.*

Proof.

  1. As in 1.3.7, use deduction theorem and $\vdash_{\mathrm{K}_{\mathcal{L}}} (((\neg\phi) \to \phi) \to \phi)$.

  2. Use 1 and the enumeration $\psi_0, \psi_1, \ldots$ of the closed $\mathcal{L}$-formulas.

$\square$

Theorem 2.5.3. *Suppose $\mathcal{L}$ is a countable first-order language and Σ is a consistent set of closed $\mathcal{L}$-formulas. Then there is a countable $\mathcal{L}$-structure $\mathcal{A}$ such that $\mathcal{A} \vDash \Sigma$, that is $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$.*

Theorem 2.5.4. *Let Σ be a set of closed $\mathcal{L}$-formulas and ϕ a closed $\mathcal{L}$-formula. If every model of Σ is a model of ϕ, then $\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \phi$. That is, if $\mathcal{A} \vDash \Sigma$, or $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$, then $\mathcal{A} \vDash \phi$, then $\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \phi$.*

Notation. $\Sigma \vDash \phi$, if every model of Σ is a model of ϕ. Then $\Sigma \vDash \phi$ implies $\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \phi$. The converse is soundness.

Proof. May assume Σ is consistent. Otherwise, everything is a consequence of Σ. By assumption, there is no model of $\Sigma \cup \{(\neg\phi)\}$. So by 2.5.3, $\Sigma \cup \{(\neg\phi)\}$ is inconsistent. So by 2.5.2.1, $\Sigma \vdash_{\mathrm{K}_{\mathcal{L}}} \phi$. $\square$

Theorem 2.5.5 (Gödel's completeness theorem for $\mathrm{K}_{\mathcal{L}}$). *If ϕ is an $\mathcal{L}$-formula with $\vDash \phi$, then ϕ is a theorem of $\mathrm{K}_{\mathcal{L}}$, that is $\vdash_{\mathrm{K}_{\mathcal{L}}} \phi$.*

Proof. If ϕ is closed this follows from 2.5.4 with $\Sigma = \emptyset$. Suppose ϕ has free variables amongst $x_1, \ldots, x_n$, and consider the closed formula

$$\psi : (\forall x_1) \ldots (\forall x_n) \phi.$$

As $\vDash \phi$, we obtain $\vDash \psi$. So, by the closed case, $\vdash_{\mathrm{K}_{\mathcal{L}}} \psi$, that is

$$\vdash_{\mathrm{K}_{\mathcal{L}}} (\forall x_1) \ldots (\forall x_n) \phi. \tag{12}$$

If θ is any formula, then

$$\vdash_{\mathrm{K}_{\mathcal{L}}} ((\forall x_i) \theta \to \theta),$$

by the K1 axiom. So from (12) and this fact, and MP, applied n times, we obtain $\vdash_{\mathrm{K}_{\mathcal{L}}} \phi$. $\square$

Corollary 2.5.6 (Compactness theorem for $K_{\mathcal{L}}$). *Suppose Σ is a set of closed $\mathcal{L}$-formulas and every finite subset of Σ has a model. Then Σ has a model.*

Proof. Suppose Σ has no model. By 2.5.3, Σ is inconsistent, so there is a formula ϕ with

$$\Sigma \vdash_{K_{\mathcal{L}}} \phi, \qquad \Sigma \vdash_{K_{\mathcal{L}}} (\neg\phi).$$

Deductions only involve finitely many formulas in Σ. So there is a finite $\Sigma_0 \subseteq \Sigma$ with

$$\Sigma_0 \vdash_{K_{\mathcal{L}}} \phi, \qquad \Sigma_0 \vdash_{K_{\mathcal{L}}} (\neg\phi).$$

But then Σ_0 is inconsistent, so has no model, a contradiction. $\square$

Proof of 2.5.3. Appendix A.2. $\square$

Example. Think about this where Σ consists of the group axioms. What is $\mathcal{A}$? Is it a group? [15]

2.6 Equality

Example. In the language of groups, have a binary relation symbol $E(x_1, x_2)$ for equality $x_1 = x_2$.

Definition 2.6.1. Suppose $\mathcal{L}^E$ is a first-order language with a distinguished binary relation symbol E.

- An $\mathcal{L}^E$-structure in which E is interpreted as equality $=$ is a **normal $\mathcal{L}^E$-structure**.

- The following are the **axioms of equality**, Σ_E.

    - $(\forall x_1)\, E(x_1, x_1)$.
    - $(\forall x_1)(\forall x_2)(E(x_1, x_2) \rightarrow E(x_2, x_1))$.
    - $(\forall x_1)(\forall x_2)(\forall x_3)(E(x_1, x_2) \rightarrow (E(x_2, x_3) \rightarrow E(x_1, x_3)))$.
    - For each n-ary relation symbol R of $\mathcal{L}^E$,

      $$(\forall x_1 \ldots x_n)(\forall y_1 \ldots y_n)((R(x_1, \ldots, x_n) \wedge E(x_1, y_1) \wedge \cdots \wedge E(x_n, y_n)) \rightarrow R(y_1, \ldots, y_n)).$$

    - For each m-ary function symbol f of $\mathcal{L}^E$,

      $$(\forall x_1 \ldots x_m)(\forall y_1 \ldots y_m)((E(x_1, y_1) \wedge \cdots \wedge E(x_m, y_m)) \rightarrow E(f(x_1, \ldots, x_m), f(y_1, \ldots, y_m))).$$

Remark 2.6.2.

- If $\mathcal{A}$ is a normal $\mathcal{L}^E$-structure, then $\mathcal{A} \vDash \Sigma_E$.

- Suppose $\mathcal{A} = \langle A; \overline{E}, \ldots \rangle$ is an $\mathcal{L}^E$-structure and $\mathcal{A} \vDash \Sigma_E$. Then $\overline{E}$ is an equivalence relation on A. Denote, for $a \in A$,
  $$\widehat{a} = \{ b \in A \mid \overline{E}(a, b) \text{ holds} \},$$
  the equivalence class of a. Let
  $$\widehat{A} = \{ \widehat{a} \mid a \in A \}.$$
  Make $\widehat{A}$ into an $\mathcal{L}^E$-structure $\widehat{\mathcal{A}}$.

    - If R is an n-ary relation symbol and $\widehat{a_1}, \ldots, \widehat{a_n} \in \widehat{A}$, then say $\overline{R}(\widehat{a_1}, \ldots, \widehat{a_n})$ holds in $\widehat{\mathcal{A}}$ if and only if $\overline{R}(a_1, \ldots, a_n)$ holds in $\mathcal{A}$. This is well-defined by Σ_E.

    - Similarly, if f is an m-ary function symbol and $\widehat{a_1}, \ldots, \widehat{a_m} \in \widehat{A}$, let
      $$\overline{f}(\widehat{a_1}, \ldots, \widehat{a_m}) = \widehat{\overline{f}(a_1, \ldots, a_m)}.$$
      This is also well-defined by Σ_E.

    - If c is a constant symbol, then interpret c as $\widehat{\overline{c}}$ in $\widehat{\mathcal{A}}$, where $\overline{c}$ is the interpretation in $\mathcal{A}$.

Note. In $\widehat{\mathcal{A}}$,
$$\overline{E}(\widehat{a_1}, \widehat{a_2}) \qquad \Longleftrightarrow \qquad \overline{E}(a_1, a_2) \text{ in } \mathcal{A} \qquad \Longleftrightarrow \qquad \widehat{a_1} = \widehat{a_2}.$$

So $\widehat{\mathcal{A}}$ is a normal $\mathcal{L}^E$-structure.

---

[15]Exercise

Lemma 2.6.3. *Suppose $\mathcal{A}$ is an $\mathcal{L}^E$-structure with $\mathcal{A} \vDash \Sigma_E$. Let v be a valuation in $\mathcal{A}$. Let $\widehat{\mathcal{A}}$ be as given above. Let $\widehat{\mathrm{v}}$ be the valuation in $\widehat{\mathcal{A}}$ with*

$$\widehat{\mathrm{v}}\left(x_i\right) = \widehat{\mathrm{v}\left(x_i\right)}.$$

Then for every $\mathcal{L}^E$-formula ϕ, $\widehat{\mathrm{v}}$ satisfies ϕ in $\widehat{\mathcal{A}}$ if and only if v satisfies ϕ in $\mathcal{A}$. In particular, if ϕ is closed, then $\mathcal{A} \vDash \phi$ if and only if $\widehat{\mathcal{A}} \vDash \phi$.

Note. If t is any term, then $\widehat{\mathrm{v}}\left(t\right) = \widehat{\mathrm{v}\left(t\right)}$, by definition of $\overline{f}$ on the structure $\widehat{\mathcal{A}}$.

Proof of 2.6.3. Appendix A.3.   □

Lemma 2.6.4. *Suppose Δ is a set of closed $\mathcal{L}^E$-formulas. Then Δ has a **normal model**, that is a normal $\mathcal{L}^E$-structure $\mathcal{B}$ with $\mathcal{B} \vDash \sigma$ for all $\sigma \in \Delta$, if and only if $\Delta \cup \Sigma_E$ has a model.*

Proof.

$\Longrightarrow$ Trivial, as Σ_E holds in a normal $\mathcal{L}^E$-structure.

$\Longleftarrow$ If $\mathcal{A} \vDash \Delta \cup \Sigma_E$, then by 2.6.3, $\widehat{\mathcal{A}} \vDash \Delta$, and $\widehat{\mathcal{A}}$ is a normal $\mathcal{L}^E$-structure.

                                                                                                                             □

Theorem 2.6.5 (Compactness theorem for normal models)**.** *Suppose $\mathcal{L}^E$ is a countable language with equality, and Δ is a set of closed $\mathcal{L}^E$-formulas such that every finite subset of Δ has a normal model. Then Δ has a normal model.*

Proof. Every normal $\mathcal{L}^E$-structure is a model of Σ_E, so every finite subset of $\Delta \cup \Sigma_E$ has a model. By 2.5.6, $\Delta \cup \Sigma_E$ has a model $\mathcal{A}$. Then by 2.6.3 or 2.6.4, $\widehat{\mathcal{A}}$ is a normal model of Δ.   □

Notation. From now on, write $\mathcal{L}^=$ instead of $\mathcal{L}^E$, and $x_1 = x_2$ instead of $E\left(x_1, x_2\right)$, etc.

Theorem 2.6.6 (Countable downward Löwenheim-Skolem theorem)**.** *Suppose $\mathcal{L}^=$ is a countable first-order language with equality, and $\mathcal{B}$ is a normal $\mathcal{L}^=$-structure. Then there is a countable normal $\mathcal{L}^=$-structure $\mathcal{A}$ such that, for every closed $\mathcal{L}^=$-formula ϕ, $\mathcal{B} \vDash \phi$ if and only if $\mathcal{A} \vDash \phi$.*

Example. Let $\mathcal{B} = \langle \mathbb{R}; +, \cdot, 0, 1, \leq, \exp \rangle$. What is $\mathcal{A}$?

Proof. Let

$$\Sigma = \{\text{closed } \phi \mid \mathcal{B} \vDash \phi\},$$

called the **theory** of $\mathcal{B}$. Then $\Sigma \supseteq \Sigma_E$, the axioms of equality, and Σ is consistent. By 2.5.3, Σ has a countable model $\mathcal{C}$. Then $\widehat{\mathcal{C}}$ is a countable normal model of Σ by 2.6.3. So if ϕ is closed and $\mathcal{B} \vDash \phi$, then $\widehat{\mathcal{C}} \vDash \phi$. Conversely, if ϕ is closed and $\mathcal{B} \nvDash \phi$, then $\mathcal{B} \vDash (\neg\phi)$, by 2.3.3, so $\widehat{\mathcal{C}} \vDash (\neg\phi)$, so $\widehat{\mathcal{C}} \nvDash \phi$. Take $\mathcal{A} = \widehat{\mathcal{C}}$.   □

2.7   Examples and applications

Let $\mathcal{L}^=$ be a first-order language with equality and a binary relation symbol $\leq$.

Definition 2.7.1.

- A **linear order** $\mathcal{A} = \langle A; \leq_A \rangle$ is a normal model of

$$\phi_1 : \left(\forall x_1\right)\left(\forall x_2\right)\left(\left(\left(x_1 \leq x_2\right) \wedge \left(x_2 \leq x_1\right)\right) \leftrightarrow \left(x_1 = x_2\right)\right),$$
$$\phi_2 : \left(\forall x_1\right)\left(\forall x_2\right)\left(\forall x_3\right)\left(\left(\left(x_1 \leq x_2\right) \wedge \left(x_2 \leq x_3\right)\right) \rightarrow \left(x_1 \leq x_3\right)\right),$$
$$\phi_3 : \left(\forall x_1\right)\left(\forall x_2\right)\left(\left(x_1 \leq x_2\right) \vee \left(x_2 \leq x_1\right)\right).$$

- It is **dense** if also

$$\phi_4 : \left(\forall x_1\right)\left(\forall x_2\right)\left(\exists x_3\right)\left(\left(x_1 < x_2\right) \rightarrow \left(\left(x_1 < x_3\right) \wedge \left(x_3 < x_2\right)\right)\right),$$

  where $\left(x_1 < x_2\right)$ is an abbreviation for $\left(\left(x_1 \leq x_2\right) \wedge \left(x_1 \neq x_2\right)\right)$.

- It is **without endpoints** if

$$\phi_5 : \left(\forall x_1\right)\left(\exists x_2\right)\left(x_1 < x_2\right),$$
$$\phi_6 : \left(\forall x_1\right)\left(\exists x_2\right)\left(x_2 < x_1\right).$$

Let $\Delta = \{\phi_1, \ldots, \phi_6\}$.

- $\mathcal{Q} = \langle \mathbb{Q}; \leq \rangle$ is a normal model of Δ.

- $\mathcal{R} = \langle \mathbb{R}; \leq \rangle$ is also a model of Δ.

Will prove the following.

Theorem 2.7.2.

1. *For every closed $\mathcal{L}^=$-formula ϕ, $\mathcal{Q} \vDash \phi$ if and only if $\mathcal{R} \vDash \phi$.*

2. *There is an algorithm which decides, given a closed $\mathcal{L}^=$-formula ϕ, whether $\mathcal{Q} \vDash \phi$ or $\mathcal{Q} \nvDash \phi$, that is $\mathcal{Q} \vDash (\neg\phi)$, by 2.3.3.*

Definition 2.7.3.

1. Linear orders $\mathcal{A} = \langle A; \leq_A \rangle$ and $\mathcal{B} = \langle B; \leq_B \rangle$ are **isomorphic** if there is a bijection $\alpha : A \to B$ such that for all $a, a' \in A$, $a \leq_A a'$ if and only if $\alpha(a) \leq_B \alpha(a')$.

2. If $\mathcal{A}$ and $\mathcal{B}$ are isomorphic and ϕ is closed, then $\mathcal{A} \vDash \phi$ if and only if $\mathcal{B} \vDash \phi$.

Theorem 2.7.4 (Cantor). *If $\mathcal{A}$ and $\mathcal{B}$ are countable dense linear orders without endpoints, then $\mathcal{A}$ and $\mathcal{B}$ are isomorphic.*

Lemma 2.7.5 (Los-Vaught test). *Let $\Sigma = \Sigma_E \cup \Delta$. Then for every closed $\mathcal{L}^=$-formula ϕ, we have either $\Sigma \vdash_{K_{\mathcal{L}=}} \phi$ or $\Sigma \vdash_{K_{\mathcal{L}=}} (\neg\phi)$. Say Σ is **complete**.*

Proof. Suppose not. Then as Σ has a model, it is consistent, so we can use 2.5.2 to get that

$$\Sigma_1 = \Sigma \cup \{(\neg\phi)\}, \qquad \Sigma_2 = \Sigma \cup \{(\neg(\neg\phi))\}$$

are consistent. So $\Sigma \cup \{\phi\}$ is consistent. By 2.5.3 and 2.6.6, it follows that Σ_1 and Σ_2 have countable normal models $\mathcal{A}_1$ and $\mathcal{A}_2$. So $\mathcal{A}_1$ and $\mathcal{A}_2$ are countable dense linear orders without endpoints, and

$$\mathcal{A}_1 \vDash (\neg\phi), \qquad \mathcal{A}_2 \vDash \phi.$$

This contradicts 2.7.4 and 2.7.3.2. $\qquad\square$

Proof of 2.7.2.

1. Show that $\mathcal{Q} \vDash \phi$ if and only if $\Sigma \vdash_{K_{\mathcal{L}=}} \phi$.

   $\impliedby$ As $\mathcal{Q} \vDash \Sigma$, this is 2.4.6.
   $\implies$ If $\Sigma \nvdash_{K_{\mathcal{L}=}} \phi$, then by 2.7.5, $\Sigma \vdash_{K_{\mathcal{L}=}} (\neg\phi)$. So $\mathcal{Q} \vDash (\neg\phi)$, so $\mathcal{Q} \nvDash \phi$.

   Similarly, $\mathcal{R} \vDash \phi$ if and only if $\Sigma \vdash_{K_{\mathcal{L}=}} \phi$. So

   $$\mathcal{R} \vDash \phi \qquad \iff \qquad \Sigma \vdash_{K_{\mathcal{L}=}} \phi \qquad \iff \qquad \mathcal{Q} \vDash \phi.$$

2. Σ is a **recursively enumerable** set of formulas. That is, we can write an algorithm to systematically generate the formulas in Σ. Note that the set of axioms for $K_{\mathcal{L}}$ is also recursively enumerable. So the set of deductions from Σ is recursively enumerable. Therefore the set of consequences of Σ is recursively enumerable. The method is to run the algorithm which generates all consequences of Σ. By 1, at some point, we will see either θ or $(\neg\theta)$. At this point, the method stops.

$\qquad\square$

Lecture 19 is a problems class.

Note.

- Depends on the completeness theorem, and the axioms Δ for $\mathcal{Q}$.

- Works for some other structures, but can have better algorithms.

- But, there is no such algorithm for $\langle \mathbb{N}; +, \cdot, 0 \rangle$. This is **Gödel's incompleteness theorem**.

3   Set theory

3.0   Basic set theory

- Extensionality. Sets A and B are **equal** if and only if for all x, $x \in A$ if and only if $x \in B$.

- **Natural numbers** $\mathbb{N} = \{0, 1, \dots\}$. Think of

$$0 = \emptyset, \qquad \dots, \qquad n + 1 = \{0, \dots, n\}, \qquad \dots .$$

  - Note that, for $m, n \in \mathbb{N}$,

$$m < n \qquad \Longleftrightarrow \qquad m \in n \qquad \Longleftrightarrow \qquad m \subsetneq n.$$

- Ordered pairs. The **ordered pair** (x, y) is the set $\{\{x\}, \{x, y\}\}$.

  - For example, for any x, y, z, w, $(x, y) = (z, w)$ if and only if $x = z$ and $y = w$.
  - If A and B are sets, then
$$A \times B = \{(a, b) \mid a \in A, \ b \in B\},$$
$$A^0 = \{\emptyset\}, \qquad A^1 = A, \qquad A^2 = A \times A, \qquad \dots, \qquad A^{n+1} = A^n \times A, \qquad \dots,$$
$$\bigcup_{n \in \mathbb{N}} A^n = \{\text{finite sequences of elements of } A\}.$$

- Functions. Think of a **function** $f : A \to B$ as a subset of $A \times B$.

  - $A = \operatorname{dom} f$ is the **domain**, and
  - $B = \operatorname{ran} f$ is the **range**.
  - If $X \subseteq A$,
$$f[X] = \{f(a) \mid a \in X\} \subseteq B.$$

  - Set of functions from A to B is
$$B^A \subseteq \mathcal{P}(A \times B),$$

  where $\mathcal{P}$ is the powerset, that is the set of all subsets.

3.1   Cardinality

Definition 3.1.1. Sets A and B are **equinumerous**, or of the **same cardinality**, if there is a bijection $f : A \to B$. Write $A \approx B$ or $|A| = |B|$.

Definition 3.1.2.

- A set A is **finite** if it is equinumerous with some element $n = \{0, \dots, n-1\}$ of $\mathbb{N}$.

- A set A is **countably infinite** if it is equinumerous with $\mathbb{N}$.

- **Countable** is finite or countably infinite.

Remark 3.1.3. The following are basic facts.

- Every subset of a countable set is countable.

- A set A is countable if and only if there is an injective function $f : A \to \mathbb{N}$.

- If A and B are countable, then $A \times B$ is countable.

- If $A_0, A_1, \dots$ are countable, then $\bigcup_{i \in \mathbb{N}} A_i$ is countable. The proof uses the axiom of choice.

Example.

- $\mathbb{Q}$ is countable.

- $\bigcup_{n \in \mathbb{N}} A^n$ is countable if A is countable.

- $\mathbb{R}$ is not countable, by Cantor.

If X is any set, then $\mathcal{P}(X)$ is the set of all subsets of X.

Theorem 3.1.4 (Cantor). *There is no surjective function*

$$f : X \to \mathcal{P}(X).$$

Proof. Suppose there is such an f. Let

$$Y = \{y \in X \mid y \notin f(y)\}.$$

There is $z \in X$ with $f(z) = Y$.

- If $z \in Y$, then $z \notin f(z) = Y$, a contradiction.

- If $z \notin Y$, then $z \notin f(z)$, so $z \in Y$, a contradiction.

$\square$

Definition 3.1.5. For sets A and B, write $|A| \le |B|$, or $A \le B$, if there is an injective function $f : A \to B$.

Note. $|X| \le |\mathcal{P}(X)|$, by using $x \mapsto \{x\}$. So, as $|X| \ne |\mathcal{P}(X)|$, by 3.1.4, we have $|X| < |\mathcal{P}(X)|$.

Example. If $|A| \le |B|$ and $|B| \le |C|$, then $|A| \le |C|$.

Theorem 3.1.6 (Schröder-Bernstein). *Suppose A and B are sets, and $f : A \to B$ and $g : B \to A$ are injective functions. Then $A \approx B$. That is, if $|A| \le |B|$ and $|B| \le |A|$, then $|A| = |B|$.*

Proof. Let $h = g \circ f : A \to A$. Let $A_0 = A \setminus g[B]$, and for $n > 0$, let $A_n = h[A_{n-1}]$. Let

$$A^* = \bigcup_{n \in \mathbb{N}} A_n, \qquad B^* = f[A^*].$$

Note that $h[A^*] \subseteq A^*$, so $g[B^*] = h[A^*] \subseteq A^*$. Claim that

$$g[B \setminus B^*] = A \setminus A^*.$$

Once we have this, f gives a bijection $A^* \to B^*$, and g gives a bijection $B \setminus B^* \to A \setminus A^*$. So

$$k(a) = \begin{cases} f(a) & a \in A^* \\ g^{-1}(a) & a \in A \setminus A^* \end{cases}$$

is a bijection.

- Let $a \in A \setminus A^*$. As $a \notin A_0$, there is $b \in B$ with $g(b) = a$. Then $b \notin B^*$, as

$$b \in B^* \qquad \implies \qquad b \in f[A^*] \qquad \implies \qquad g(b) \in h[A^*] \subseteq A^* \qquad \implies \qquad a \in A^*,$$

a contradiction. Thus $g[B \setminus B^*] \supseteq A \setminus A^*$.

- Let $b \in B$. Suppose $g(b) \in A^*$. Show that $b \in B^*$. As $g(b) \notin A_0 = A \setminus g[B]$, we have $g(b) \in A_n$ for some $n > 0$. So $g(b) = h(a)$, for some $a \in A_{n-1}$. So $g(b) = g(f(a))$. Thus $b = f(a)$ for some $a \in A^*$. Thus $b \in f[A^*] = B^*$.

$\square$

Example 3.1.7. The following sets are equinumerous.

$$S_1 = \{\text{set of all sequences of zeroes and ones}\} = \{0,1\}^{\mathbb{N}}$$
$$S_2 = \mathbb{R}$$
$$S_3 = \mathcal{P}(\mathbb{N})$$
$$S_4 = \mathcal{P}(\mathbb{N} \times \mathbb{N})$$
$$S_5 = \{\text{set of all sequences of natural numbers}\} = \mathbb{N}^{\mathbb{N}}$$

Proof. Find injective functions

$$f_{i,j} : S_i \to S_j, \qquad i, j = 1, \ldots, 5.$$

Then use 3.1.6.

- As $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$, we get $S_3 \approx S_4$.

- Also $S_1 \subseteq S_5 \subseteq S_4$.

- $f_{3,1} : \mathcal{P}(\mathbb{N}) \to \{0,1\}^{\mathbb{N}}$.

$$X \subseteq \mathbb{N} \mapsto (a_n)_{n \in \mathbb{N}}, \qquad a_n = \begin{cases} 0 & n \notin X \\ 1 & n \in X \end{cases}$$

- $f_{1,2} : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$.

$$(a_n)_{n \in \mathbb{N}} \mapsto 0.a_1 a_2 \ldots$$

- $f_{2,5} : \mathbb{R} \to \mathbb{N}^{\mathbb{N}}$.

$$n.m_1 m_2 \cdots \mapsto \begin{cases} (0, n, m_1, m_2, \ldots) & n \geq 0 \\ (1, -n, m_1, m_2, \ldots) & n < 0 \end{cases}$$

$\square$

The following are questions.

- If A and B are sets, do we have $|A| \leq |B|$ or $|B| \leq |A|$? If we assume the axiom of choice, yes.

- Is there $X \subseteq \mathbb{R}$ with $|\mathbb{N}| < |X| < |\mathbb{R}|$? The **continuum hypothesis** says no.

3.2   Axioms for set theory

Zermelo-Fraenkel axioms (ZF) say how we are allowed to build sets. All can be expressed in a first-order language, with equality, using a single binary relation symbol $\in$. Have to avoid the **Russell paradox**. Let

$$S = \{x \mid x \text{ is a set and } x \notin x\}.$$

If this is a set, is $S \in S$?

$$(\exists S)(\forall x)((x \in S) \leftrightarrow (x \notin x))$$

leads to inconsistency.

Axiom 1 (Axiom of extensionality)**.** Two sets are equal if and only if they have the same elements.

$$(\forall x)(\forall y)((x = y) \leftrightarrow (\forall z)((z \in x) \leftrightarrow (z \in y)))$$

Axiom 2 (Empty set axiom)**.**

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

There is a unique set x with this property, $\emptyset$.

Axiom 3 (Pairing axiom)**.** Given sets x and y, then we can form $z = \{x, y\}$.

$$(\forall x)(\forall y)(\exists z)(\forall w)((w \in z) \leftrightarrow ((w = x) \vee (w = y)))$$

Remark.

- Use twice to form

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

- Use to produce

$$0 = \emptyset, \qquad 1 = \{\emptyset\}, \qquad 2 = \{0, 1\}.$$

Axiom 4 (Union axiom). For any set A, there is a set $B = \bigcup A$.
$$(\forall A)\,(\exists B)\,(\forall x)\,((x \in B) \leftrightarrow (\exists z)\,((z \in A) \wedge (x \in z)))$$

So
$$B = \bigcup \{z \mid z \in A\}.$$

If $A = \{x, y\}$, then $B = x \cup y$.

Example.
$$3 = \{0, 1, 2\} = \{0, 1\} \cup \{2\}.$$

Axiom 5 (Power set axiom). For any set A, there is a set $\mathcal{P}(A)$ whose elements are the subsets of A.
$$(\forall A)\,(\exists B)\,(\forall z)\,((z \in B) \leftrightarrow (z \subseteq A)),$$

where $z \subseteq A$ means
$$(\forall y)\,((y \in z) \rightarrow (y \in A)).$$

Axiom 6 (Axiom scheme of specification). Suppose $P(x, y_1, \ldots, y_r)$ is a formula in our language. Then we have an axiom
$$(\forall A)\,(\forall y_1)\ldots(\forall y_r)\,(\exists B)\,(\forall x)\,((x \in B) \leftrightarrow ((x \in A) \wedge P(x, y_1, \ldots, y_r))).$$

So this guarantees we can form the subset of A,
$$B = \{x \in A \mid P(x, y_1, \ldots, y_r) \text{ holds}\},$$

for all given sets $A, y_1, \ldots, y_r$.

Example.

- Let C be any non-empty set and $A \in C$. Then
$$\bigcap C = \{x \in A \mid P(x, C) = (\forall z)\,((z \in C) \rightarrow (x \in z))\}.$$

-
$$A \times B = \{w \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a)\,(\exists b)\,((a \in A) \wedge (b \in B) \wedge (w = \{\{a\}, \{a, b\}\}))\}.$$

Definition 3.2.1. For a set a, the **successor** of a is
$$a^\dagger = a \cup \{a\}.$$

A set A is **inductive** if
$$((\emptyset \in A) \wedge (\forall x)\,((x \in A) \rightarrow (x^\dagger \in A))).$$

Example.
$$2 = \{0, 1\} = \{0\} \cup \{1\} = 1^\dagger.$$

Axiom 7 (Axiom of infinity).
$$(\exists A)\,((\emptyset \in A) \wedge (\forall x)\,((x \in A) \rightarrow (x^\dagger \in A)))$$

Definition 3.2.2. Let A be an inductive set. We can form, using specification, the set
$$\mathbb{N} = \{x \in A \mid \text{if } B \text{ is an inductive set, then } x \in B\}.$$

Informally, this is the intersection of all inductive sets. This does not depend on the choice of A. Also denote this by ω.

Theorem 3.2.3.

1. $\mathbb{N}$ *is an inductive set, and if B is an inductive set, then $\mathbb{N} \subseteq B$.*

2. *Proof by induction works. Suppose $P(x)$ is a property of sets, that is a formula, such that*

   (a) *$P(\emptyset)$ holds, and*
   (b) *for every $k \in \mathbb{N}$, if $P(k)$ holds, then $P(k^\dagger)$ holds.*

   Then $P(n)$ holds for all $n \in \mathbb{N}$.

Proof.

1. Use definition. [16]

2. Consider $B \subseteq \mathbb{N}$ given by

$$B = \{x \in \mathbb{N} \mid P(x) \text{ holds}\}.$$

    (a) and (b) say that B is an inductive set. So by 1, $\mathbb{N} \subseteq B$. Thus $\mathbb{N} = B$.

$\square$

Could develop arithmetic in $\mathbb{N}$, using $n^{\dagger}$ as $n + 1$, etc, and in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, in the usual way, using ZF1-7.

Example. For $m, n \in \mathbb{N}$, write $m \leq n$ to mean

$$((m = n) \vee (m \in n)).$$

This is a well ordering on $\mathbb{N}$. [17]

3.3 Well orderings

Definition 3.3.1. A linear ordering $\langle A; \leq \rangle$ is a **well ordering**, or a **woset**, if every non-empty subset of A has a least element.

$$(\forall X)\left(((X \subseteq A) \wedge (X \neq \emptyset)) \to (\exists x)\left((x \in X) \wedge (\forall y)\left((y \in X) \to (x \in y)\right)\right)\right)$$

Example.

- $\langle \mathbb{Z}; \leq \rangle$ is not a well ordering.

- $\langle \mathbb{N}; \leq \rangle$ is a well ordering.

Suppose $\mathcal{A}_1 = \langle A_1; \leq_1 \rangle$ and $\mathcal{A}_2 = \langle A_2; \leq_2 \rangle$ are linearly ordered sets.

Definition 3.3.2.

- Say $\mathcal{A}_1$ and $\mathcal{A}_2$ are **similar**, or **isomorphic**, if there is a bijection

$$\alpha : A_1 \to A_2,$$

    with for all $a, b \in A_1$, $a <_1 b$ if and only if $\alpha(a) <_2 \alpha(b)$. Write $\mathcal{A}_1 \simeq \mathcal{A}_2$. Say α is a **similarity**.

- If $a <_1 b$ implies that $\alpha(a) <_2 \alpha(b)$, say α is **order-preserving**.

Definition 3.3.3.

- The **reverse-lexicographic product** is

$$\mathcal{A}_1 \times \mathcal{A}_2 = \langle A_1 \times A_2; \leq \rangle,$$

    where $(a_1, a_2) \leq (a_1', a_2')$ if and only if $a_2 <_2 a_2'$ or $a_2 = a_2'$ and $a_1 \leq_1 a_1'$. In $\mathcal{A}_2$, replace each element by a copy of $\mathcal{A}_1$.

- Regard A_1 and A_2 as disjoint, by replacing them by similar orderings on disjoint sets, such as

$$\{(a, 0) \mid a \in A_1\}, \qquad \{(b, 1) \mid b \in A_2\},$$

    and define the **sum**

$$\mathcal{A}_1 + \mathcal{A}_2 = \langle A_1 \cup A_2; \leq \rangle,$$

    where $\leq$ is the union of $\leq_1$ and $\leq_2$, and

$$a_1 \leq a_2, \qquad a_1 \in A_1, \qquad a_2 \in A_2.$$

---

[16]Exercise
[17]Exercise

Example.

- $\mathbb{N} + \mathbb{N}$ is

$$
\begin{array}{cccccccccc}
\mathbb{N} & & & & 0 & 1 & \ldots & & & \\
& \mathbb{N} & & & & & & & 0 & 1 & \ldots \\
\mathbb{N} & + & \mathbb{N} & & 0 & 1 & \ldots & & 0 & 1 & \ldots.
\end{array}
$$

- $\{0, 1\} \times \mathbb{N}$ is

$$
\begin{array}{ccccccccc}
& \mathbb{N} & & 0 & & 1 & & \ldots & \\
\{0, 1\} & \times & \mathbb{N} & 0 & 1 & 0 & 1 & \ldots & \ldots.
\end{array}
$$

  Thus $\{0, 1\} \times \mathbb{N} \simeq \mathbb{N}$.

- $\mathbb{N} \times \{0, 1\}$ is

$$
\begin{array}{ccccccccc}
& \{0, 1\} & & 0 & & 1 & \\
\mathbb{N} & \times & \{0, 1\} & 0 & 1 & \ldots & 0 & 1 & \ldots.
\end{array}
$$

  Thus $\mathbb{N} \times \{0, 1\} \simeq \mathbb{N} + \mathbb{N}$.

Lemma 3.3.4.

- *$\mathcal{A}_1 + \mathcal{A}_2$ and $\mathcal{A}_1 \times \mathcal{A}_2$ are linearly ordered sets.*

- *If $\mathcal{A}_1$ and $\mathcal{A}_2$ are well orderings, then so are $\mathcal{A}_1 + \mathcal{A}_2$ and $\mathcal{A}_1 \times \mathcal{A}_2$.*

Proof. For example, $\mathcal{A}_1 \times \mathcal{A}_2$ is a well ordering. Let

$$\emptyset \neq X \subsetneq A_1 \times A_2.$$

Let

$$Y = \{b \in A_2 \mid \text{there is } a \in A_1 \text{ with } (a, b) \in X\} \subseteq A_2.$$

Let y be the least element of Y. Let

$$Z = \{z \in A_1 \mid (z, y) \in X\}.$$

This has a least element x. Then (x, y) is the least element of X. [18]   □

Definition 3.3.5.

- Suppose $\mathcal{A} = \langle A; \leq \rangle$ is a linearly ordered set. A subset $X \subseteq A$ is an **initial segment** of A if

$$(\forall x \in X)\, (\forall a \in A)\, ((a < x) \to (a \in X))$$

- It is **proper** if $X \neq A$.

Example. Let $b \in A$.

- A proper initial segment is

$$A\,[b] = \{x \in A \mid x < b\}.$$

- An initial segment is

$$A\,[\leq b] = \{x \in A \mid x \leq b\}.$$

Lemma 3.3.6. *If $\mathcal{A} = \langle A; \leq \rangle$ is a well ordered set, then every proper initial segment X is of the form $A\,[b]$ for some $b \in A$.*

Remark. This is not true for linear orders in general.

Example.

$$\{x \in \mathbb{Q} \mid x < \pi\} \subseteq \mathbb{Q}$$

is not of the form $\mathbb{Q}\,[b]$ for some $b \in \mathbb{Q}$.

Proof. Let b be the minimal element of $A \setminus X$.   □

---

[18]Exercise

Theorem 3.3.7. *Suppose $\mathcal{A}_1 = \langle A_1; \leq_1 \rangle$ and $\mathcal{A}_2 = \langle A_2; \leq_2 \rangle$ are well ordered sets. Then exactly one of the following holds.*

1. *$\mathcal{A}_1$ and $\mathcal{A}_2$ are similar,*

2. *$\mathcal{A}_1$ is similar to a proper initial segment of $\mathcal{A}_2$, or*

3. *$\mathcal{A}_2$ is similar to a proper initial segment of $\mathcal{A}_1$.*

In each case, the similarity is unique.

Proof.

- Uniqueness. Suppose we have order preserving

$$\alpha, \beta : A_1 \to A_2,$$

  whose images are initial segments of A_2. Show that $\alpha = \beta$.

  Step 1. Check that, if $b \in A_1$, then
$$\alpha(A_1[b]) = A_2[\alpha(b)].$$

  Step 2. If $\alpha \neq \beta$, take $b \in A_1$ minimal with $\alpha(b) \neq \beta(b)$, so

$$\alpha|_{A_1[b]} = \beta|_{A_1[b]}.$$

    By step 1,
$$A_2[\alpha(b)] = A_2[\beta(b)].$$

    Conclude that $\alpha(b) = \beta(b)$, a contradiction.

  This shows

    - by taking $A_1 = A_2$ and α the identity, obtain that A_1 is not similar to a proper initial segment of itself, and
    - it follows that we cannot have two of $1, 2, 3$ holding.

- Existence. Suppose A_2 is not similar to an initial segment of A_1. Show that A_1 is similar to a proper initial segment of A_2. Look at

$$C = \{c \in A_1 \mid \text{there is a similarity between } A_1[\leq c] \text{ and an initial segment of } A_2\}.$$

  If $c \in C$, there is a unique
$$\alpha_c : A_1[\leq c] \to A_2,$$

  with image an initial segment, by the uniqueness part. Note that

    - C is an initial segment of A_1,
    - if $c_1 < c_2 \in C$, then α_{c_1} is the restriction of α_{c_2} to $A_1[\leq c_1]$, and
    - let

$$\alpha = \bigcup \{\alpha_c \mid c \in C\},$$

    then α is a similarity between C and an initial segment of A_2.

  If $C = A_1$, done. Suppose $C \neq A_1$. Let a be the minimal element of $A_1 \setminus C$.

$$\alpha(C) \neq A_2,$$

  otherwise A_2 is similar to C, so 3 holds. So $\alpha(C) = A_2[b]$ for some $b \in A_2$. Can extend α by sending a to b, and get
$$A_1[\leq a] \simeq A_2[\leq b].$$

  Thus $a \in C$, a contradiction.

$\square$

Remark. In the notation of 3.3.7, we have, in particular, an injective function

$$A_1 \to A_2,$$

for cases 1 and 2, or an injective function

$$A_2 \to A_1.$$

So either $|A_1| \leq |A_2|$ or $|A_2| \leq |A_1|$.

The axiom of choice implies that any set A can be well ordered. Putting this together with 3.3.7 implies that, for any sets A_1 and A_2, $|A_1| \leq |A_2|$ or $|A_2| \leq |A_1|$.

3.4   Ordinals

We now define some very particular well ordered sets which generalise the natural numbers,

$$0 = \emptyset, \qquad 1 = 0^\dagger = \{\emptyset\}, \qquad 2 = 1^\dagger = \{0, 1\}, \qquad 3 = 2^\dagger = \{0, 1, 2\}, \qquad \ldots.$$

to the transfinite.

Definition 3.4.1.

- A set X is a **transitive set** if every element of X is also a subset of X. That is, if $y \in x \in X$, then $y \in X$.

- A set α is an **ordinal** if

  - α is a transitive set, and
  - the relation $<$ on α given by, for $x, y \in \alpha$, $x < y$ if and only if $x \in y$ is a strict well ordering on α.

Note. As part of the definition, we have $\alpha \notin \alpha$ for an ordinal α.

It is standard to use lower case Greek letters for ordinals. The ordering on an ordinal α is sometimes denoted by $\in_\alpha$.

Lemma 3.4.2. *If α is an ordinal, then so is $\alpha^\dagger = \alpha \cup \{\alpha\}$.*

Proof. As α is a transitive set, then so is $\alpha^\dagger = \alpha \cup \{\alpha\}$. Moreover, the ordering $\in$ restricted to $\alpha^\dagger$ is an ordering. We have the ordering on α with the extra element α added on the end as the greatest element. This is a well ordering, as the ordering on α is a well ordering. $\square$

We also denote the ordinal $\alpha^\dagger$ by $\alpha + 1$. It is of course similar to the ordered set $\alpha + 1$ as defined previously.

Corollary 3.4.3. *If $n \in \omega$, then n is an ordinal.*

Proof. As $\emptyset$ is an ordinal, this follows by induction in 3.2.3 using 3.4.2 above. $\square$

Proposition 3.4.4.

1. *If α is an ordinal, then $\alpha \notin \alpha$.*

2. *If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.*

3. *If α and β are ordinals and $\alpha \subsetneq \beta$, then $\alpha \in \beta$.*

4. *If α is an ordinal, then $\alpha = \{\beta \mid \beta \text{ is an ordinal and } \beta \in \alpha\}$.*

Proof.

1. Otherwise, α has an element $x = \alpha$ with $x \in x$. But in terms of the ordering on α, this says $x < x$, which is impossible.

2. First show β is a transitive set. So let $x \in \beta$ and $y \in x$. We want $y \in \beta$. But we have $y \in x \in \beta \in \alpha$. Using twice that α is a transitive set, we get that $x, y \in \alpha$. So, as the restriction of $\in$ to α is an ordering, we get $y \in \beta$. As α is a transitive set, $\in_\beta$ is simply the restriction of $\in_\alpha$ to β, so this is a well ordering.

3. Note that, as $\alpha \subsetneq \beta$, $\beta \setminus \alpha$ is non-empty, so has a least element γ, under $\in_\beta$. We aim to show that $\alpha = \gamma$. Think about α and β as natural numbers to see why this is plausible. If $x \in \gamma$, then $x \in \beta$, so $x \in \alpha$, as γ is the least element of $\beta \setminus \alpha$. Thus $\gamma \subseteq \alpha$. Conversely suppose there is some $y \in \alpha \setminus \gamma$. Then, as $\in$ is an ordering on β and $y \notin \gamma$, either $y = \gamma$ or $\gamma \in y$. But in either case, we get $\gamma \in \alpha$, as α is a transitive set, a contradiction. So $\alpha \subseteq \gamma$.

4. Trivial, by 2.

$\square$

Definition 3.4.5. If α and β are ordinals, we write $\alpha < \beta$ to indicate that $\alpha \in \beta$, and $\alpha \leq \beta$ has the obvious meaning.

Note. By 3.4.4 above, $\alpha \leq \beta$ if and only if $\alpha \subseteq \beta$.

The following theorems can be paraphrased informally as saying that the class of all ordinals is well ordered by $\leq$.

Theorem 3.4.6. *Suppose α, β, γ are ordinals.*

1. If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$.

2. If $\alpha \leq \beta$ and $\beta \leq \alpha$, then $\alpha = \beta$.

3. Exactly one of
$$\alpha < \beta, \qquad \alpha = \beta, \qquad \beta < \alpha$$
holds.

4. If X is a non-empty set of ordinals, then X has a least element δ, and moreover,
$$\delta = \bigcap X.$$

Proof.

1. If $\alpha \in \beta \in \gamma$, then $\alpha \in \gamma$, as γ is a transitive set.

2. Otherwise, we have $\alpha \in \beta$ and $\beta \in \gamma$, whence $\alpha \in \alpha$, contradicting 3.4.4.

3. Certainly we already know that no more than one of these holds. Consider $\alpha \cap \beta$. This is also an ordinal, by 4. [19] Show that, if $\alpha \neq \beta$, then $\alpha \subsetneq \beta$ or $\beta \subsetneq \alpha$. If, for example $\alpha \cap \beta = \alpha$, then $\alpha \subseteq \beta$ and so $\alpha \leq \beta$. So for a contradiction, suppose $\alpha \cap \beta$ is a proper subset of both α and β. Thus, by 3.4.4.3, $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$. So $\alpha \cap \beta \in \alpha \cap \beta$, a contradiction, all using $\alpha \cap \beta$ is an ordinal.

4. Let $\alpha \in X$ be any element and consider $\alpha \cap X$. So this is the set of elements of X which are less than α. If this is empty, then α is the least element of X. Otherwise, it is a non-empty subset of α, so has a least element β. It is then obvious that β is the least element of X. If δ is the least element of X, then $\delta \subseteq \eta$ for all $\eta \in X$. It follows that $\delta = \bigcap X$.

$\square$

Corollary 3.4.7.

1. If X is a non-empty set of ordinals, then $\bigcup X$ is an ordinal.

2. ω is an ordinal.

Proof.

1. By 3.4.6, X is well ordered by $\in$. So it is enough to show that $\bigcup X$ is a transitive set. If $y \in z \in \bigcup X$, there is $x \in X$ with $z \in x$. So $y \in z \in x$, and therefore $y \in x$. So $y \in \bigcup X$, as required.

2. Check that $\bigcup \omega = \omega$, and use 1.

$\square$

---

[19]Exercise

So now we can form ordinals

$$\omega^\dagger = \{0, 1, \ldots, \omega\}, \qquad \left(\omega^\dagger\right)^\dagger = \{0, 1, \ldots, \omega, \omega^+\}, \qquad \ldots.$$

Just as the natural numbers provided us with canonical examples of finite sets, we will now show that ordinals do the same thing for all well ordered sets.

Theorem 3.4.8. *If $\langle A; \leq \rangle$ is a well ordered set, then there is a unique ordinal α which is similar to $\langle A; \leq \rangle$.*

Proof.

- Uniqueness. Suppose $\langle A; \leq \rangle$ is similar to ordinals α and β. Then α and β are similar. Without loss of generality, may assume $\alpha \leq \beta$, so if $\alpha \neq \beta$, we have that $\alpha < \beta$. Therefore α is a proper initial segment of β, and so β is similar to a proper initial segment of itself, which contradicts 3.3.7. This establishes the uniqueness part of the statement.

- Existence. Now we show that there is some ordinal similar to A. Let

$$X = \{x \in A \mid \text{the initial segment } A[x] \text{ is similar to an ordinal}\}.$$

For example, if $A \neq \emptyset$ and x is the least element of A, then $A[x]$ is empty, and the empty set is an ordinal, so $x \in X$. Note that, by uniqueness, if $x \in X$, then $A[x]$ is similar to a unique ordinal α_x. Let

$$S = \{\alpha_x \mid x \in X\}.$$

So S is a set of ordinals. In fact, S is an ordinal. To see this, note that we need to only show that it is a transitive set, that is, if $\beta \in \alpha_x \in S$, then $\beta \in S$. Let $\alpha_x \in S$ and let

$$\pi : A[x] \to \alpha_x$$

be a similarity. If $\beta \in \alpha_x$, let

$$y = \pi^{-1}(\beta).$$

Then the restriction of π to $A[y]$ gives a similarity

$$A[y] \to \{\delta \in \alpha_x \mid \delta < \beta\} = \beta.$$

So $\beta = \alpha_y \in S$. So now write α instead of S. By what we already did, this argument also shows that X is an initial segment of A. If we knew that $A = X$, then we would be done, as the function

$$\begin{array}{ccc} X & \longrightarrow & \alpha \\ x & \longmapsto & \alpha_x \end{array}$$

is easily seen to be a similarity $A \to \alpha$. So suppose that $X \neq A$, so X is a proper initial segment of A. By 3.3.6, we have that $X = A[z]$ for some $z \in A \setminus X$. Know that $x \mapsto \alpha_x$ gives a similarity $X \to \alpha$. But then $z \in X = A[z]$, by definition of X, a contradiction. So $X = A$ and $A \simeq \alpha$.

$\square$

There is a problem with this proof. Why is S a set? No combination of the axioms we have given so far actually justifies the existence of such a set. There is no alternative but to assume another axiom about how we are allowed to create new sets from old ones.

Definition 3.4.9. Suppose

$$F(x, y, z_1, \ldots, z_r)$$

is a property of sets, expressible in our first-order language such that, whenever $s_1, \ldots, s_r$ are sets, for every set b, there is a unique set a where

$$F(a, b, s_1, \ldots, s_r)$$

holds.

- F is called an **operation on sets**,

- with $z_1, \ldots, z_r$ being **parameter variables**,

- the $s_1, \ldots, s_r$ are referred to as the **parameters** of the operation, and

- $F(x, y, s_1, \ldots, s_r)$ gives us a **function on sets** $b \mapsto a$.

37

Example.

- No parameter variables.
$$F(a, b) \text{ says } a \text{ is the power set of } b.$$

- One parameter c.
$$F(a, b, c) \text{ says } a \text{ is the set of functions from } b \text{ to } c.$$

Axiom 8 (Axiom of replacement)**.** Suppose

$$F(x, y, z_1, \ldots, z_r)$$

is an operation on sets as above, and $s_1, \ldots, s_r$ are sets. Then for any set B, there is a set A such that

$$A = \{a \mid F(a, b, s_1, \ldots, s_r) \text{ holds for some } b \in B\}.$$

So here, the set A is obtained from B by replacing each $b \in B$ by the corresponding set a for which

$$F(a, b, s_1, \ldots, s_r)$$

holds. If we allow ourselves this axiom, then the set S in the above proof of 3.4.8 is justified. Obtain S from X using the operation $F(a, b)$ to say,

either b is a well ordered set similar to the ordinal a, or b is not a well ordered set and $a = \emptyset$.

Then apply this to

$$B = \{A[x] \mid x \in X\},$$

to get

$$S = \{x \mid F(x, A[y]) \text{ holds for some } y \in X\}.$$

3.5   Transfinite induction

Theorem 3.5.1 (Transfinite induction)**.** *Suppose $P(x)$ is a property of sets. Assume that, for all ordinals α,*

$$\text{if } P(\beta) \text{ holds for all ordinals } \beta < \alpha, \text{ then } P(\alpha) \text{ holds.} \tag{13}$$

Then $P(\gamma)$ holds for all ordinals γ.

Proof. Note that, if $\alpha = 0 = \emptyset$, then $P(\beta)$ holds for all $\beta < \alpha$, vacuously. So by (13), $P(0)$ holds. Suppose for a contradiction that there is some ordinal γ, such that $P(\gamma)$ does not hold. There is a least such γ, by applying 3.4.6.4 to

$$\{\beta \mid \beta \leq \gamma, \ P(\beta) \text{ does not hold}\}.$$

Call it α. Thus, for an ordinal $\beta < \alpha$, $P(\beta)$ holds. By (13), $P(\alpha)$ holds, a contradiction. $\square$

Theorem 3.5.2. *Suppose α is an infinite ordinal, that is $\omega \leq \alpha$. Then $\alpha \approx \alpha \times \alpha$.*

Corollary 3.5.3.

1. *If $\langle A; \leq \rangle$ is an infinite well ordered set, then $|A| = |A \times A|$.*

2. *Assuming the axiom of choice, if A is any infinite set, then $|A| = |A \times A|$.*

Proof.

1. By 3.4.8, there is an ordinal α with $\alpha \approx A$. So $|A| = |A \times A|$ follows from 3.5.2.

2. By the axiom of choice, A can be well ordered, so 2 follows from 1.

$\square$

2 is called the **fundamental theorem of cardinal arithmetic**.

Proof of 3.5.2. Appendix A.4. $\square$

Lecture 26
Friday
30/11/18

38

3.6   Transfinite recursion

Recall the notion of an operation F defined on sets. We have some property $F(x,y)$ of sets such that, for every set b, there is a unique set a such that $F(a,b)$ holds.

Notation. We denote, by $F(b)$, the result of applying F to the set b here, by 3.4.9.

Note. If A is any set, then by the axiom of replacement, we have a function with domain A with $a \mapsto F(a)$ for all $a \in A$. We refer to this as the restriction of F to A and denote it by $F \upharpoonright A$.

In transfinite recursion, we want to define an operation G on all ordinals α, in such a way that sets $G(\alpha)$ is obtained from the values of sets $G(\beta)$ for ordinals $\beta < \alpha$. Recall that

$$\alpha = \{\beta \mid \beta < \alpha\},$$

so another way of saying this is that $G(\alpha)$ is determined by

$$G \upharpoonright \alpha : \alpha \to \{G(\beta) \mid \beta < \alpha\},$$

which is a set, by the axiom of replacement. The way we construct $G(\alpha)$ from the previous values is controlled by applying some operation

$$F : G(0), \dots, G(\beta), \dots \to G(\alpha),$$

Theorem 3.6.1 (Transfinite recursion). *Let F be an operation. Then there is an operation G such that, for all ordinals α, we have*

$$G(\alpha) = F(G \upharpoonright \alpha).$$

If G' is another such operation, then $G(\alpha) = G'(\alpha)$ for all ordinals α.

We cannot say that G is unique here, as we have no control over what it does on sets which are not ordinals, and it is usually not relevant. We might say that G is uniquely determined on ordinals. In practice, we usually do not write F down explicitly as a first-order formula.

Remark 3.6.2. An application is the Lindenbaum lemma, comparing 1.3.8 and 2.5.2. Suppose $\mathcal{L}$ is a first-order language whose alphabet of symbols can be well ordered. Suppose Σ is a consistent set of closed $\mathcal{L}$-formulas. Then there is a consistent set $\Sigma^* \supseteq \Sigma$ of closed $\mathcal{L}$-formulas such that, for every closed $\mathcal{L}$-formula ψ, either $\Sigma^* \vdash_{\mathrm{K}_\mathcal{L}} \psi$ or $\Sigma^* \vdash_{\mathrm{K}_\mathcal{L}} (\neg\psi)$.

Proof. The set of $\mathcal{L}$-formulas can be well ordered. Any subset of a well ordered set is well ordered, so the set of closed $\mathcal{L}$-formulas is well ordered. Any well ordered set is similar to some ordinal, by 3.4.8. So we can write the set of closed $\mathcal{L}$-formulas as

$$\{\phi_\alpha \mid \alpha < \lambda\},$$

for some ordinal λ. Define, for each ordinal α, a consistent set $G(\alpha) \supseteq \Sigma$ of closed $\mathcal{L}$-formulas

$$G(\alpha) = \begin{cases} \Sigma \cup \bigcup_{\beta<\alpha} G(\beta) & \alpha < \lambda,\ \Sigma \cup \bigcup_{\beta<\alpha} G(\beta) \vdash_{\mathrm{K}_\mathcal{L}} \phi_\alpha \\ \Sigma \cup \bigcup_{\beta<\alpha} G(\beta) \cup \{(\neg\phi_\alpha)\} & \alpha < \lambda,\ \Sigma \cup \bigcup_{\beta<\alpha} G(\beta) \nvdash_{\mathrm{K}_\mathcal{L}} \phi_\alpha \\ \Sigma \cup \bigcup_{\beta<\lambda} G(\beta) & \alpha \geq \lambda \end{cases}.$$

Let $\Sigma^* = G(\lambda)$. The proof that it works is just as in the countable case. $\square$

Remark 3.6.3. Can use similar arguments at other points in the proof of the completeness theorem, by adding witnesses in 2.5.3, to get that the completeness theorem, the compactness theorem, etc holds.

Proof of 3.6.1. Appendix A.5. $\square$

Lecture 27
Monday
03/12/18

3.7   Axiom of regularity

Axiom 9 (Axiom of regularity (foundation))**.**

$$(\forall x)((x \neq \emptyset) \to (\exists a)((a \in x) \land (a \cap x = \emptyset)))$$

In particular, there is no set b with $b \in b$. Consider $x = \{b\}$. By ZF9, $b \cap \{b\} \neq \emptyset$, so $b \notin b$. We will not use this. Axioms ZF1-9 is **Zermelo-Fraenkel set theory**.

4   The axiom of choice and consequences

4.1   Statement and well ordering principle

Definition 4.1.1 (Axiom of choice)**.** Suppose A is a set of non-empty sets. Then there is a function

$$f : A \to \bigcup A,$$

with $f(a) \in a$ for every $a \in A$.

Axioms ZF1-9 and the axiom of choice (AC) is **ZFC**.

Example 4.1.2. Suppose X is any non-empty set. Let

$$A = \mathcal{P}(X) \setminus \{\emptyset\},$$

the non-empty subsets of X. By the axiom of choice, there is a function

$$f : A \to X,$$

such that $f(Y) \in Y$ for every $\emptyset \neq Y \subseteq X$. Such an f is called a **choice function**, on the subsets of X.

Note. If $\langle X; \leq \rangle$ is a well ordered set, we do not need the axiom of choice to get a choice function on X. Define, for $\emptyset \neq Y \subseteq X$, $f(Y) = \min(Y)$. Then

$$f = \{(Y, a) \in (\mathcal{P}(X) \setminus \{\emptyset\}) \times X \mid a = \min(Y)\}$$

exists, just by axiom of specification.

Theorem 4.1.3. *Suppose X is a non-empty set and*

$$f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$$

is a choice function. Then there is a well ordering $\leq$ of X, that is a well ordered set $\langle X; \leq \rangle$.

The proof needs Hartogs' lemma.

Lemma 4.1.4 (Hartogs' lemma)**.** *For any set X, there is an ordinal α such that there is no injective function*

$$h : \alpha \to X.$$

Proof of 4.1.3. Let α be such an ordinal. Consider

$$\widetilde{X} = X \cup \{\infty\},$$

where ∞ is some set with $\infty \notin X$. Use transfinite recursion and the choice function f to define an operation G, for an ordinal γ,

$$G(\gamma) = \begin{cases} f(X \setminus \{G(\beta) \mid \beta < \gamma\}) & X \setminus \{G(\beta) \mid \beta < \gamma\} \neq \emptyset \\ \infty & \text{otherwise} \end{cases}.$$

Note that, if $\infty \notin \operatorname{Im} G \restriction \gamma$, then $G \restriction \gamma$ is an injective function

$$\gamma \to X.$$

By Hartogs' lemma, there is some ordinal α with $G(\alpha) = \infty$. Take the least such ordinal and call it β. Then

$$g = G \restriction \beta : \beta \to X$$

is injective and surjective, as $G(\beta) = \infty$. So $g : \beta \to X$ is a bijection. Define $\leq$ on X by $x_1 \leq x_2$ if and only if $g^{-1}(x_1) \leq g^{-1}(x_2)$, where $\leq$ is the ordering $\in$ on β. $\qquad\square$

Proof of 4.1.4. Given A any set, find an ordinal α with no injective function $\alpha \to A$. Consider

$$X = \{\langle Y, \leq_Y \rangle \mid Y \subseteq A, \ \leq_Y \ \text{is a well order on } Y\}.$$

This is a set, by specification. Let

$$S = \{\beta \mid \beta \text{ is an ordinal similar to some } \langle Y, \leq_Y \rangle \in X\},$$

using 3.4.8 and axiom of replacement to get that S is a set. So

$$S = \{\beta \mid \beta \text{ is an ordinal and there is an injective function } \beta \to A\}.$$

Let $\sigma = \bigcup S$. This is an ordinal, and $\beta \leq \sigma$ for all $\beta \in S$, by 3.4.4 and 3.4.7. Let $\alpha = \sigma^\dagger$. So α is an ordinal, and for all $\beta \in S$,

$$\beta \leq \sigma < \alpha.$$

So $\alpha \notin S$. Thus there is no injective function $\alpha \to A$.   □

Lecture 28 is a problems class.

Corollary 4.1.5. *Assuming ZF, the axiom of choice is equivalent to the following **well ordering principle** (WO).*
> *If A is any set, there is $\leq_A \subseteq A \times A$ such that $\langle A; \leq_A \rangle$ is a well ordered set.*

That is,
$$ZF \vdash (\text{axiom of choice} \leftrightarrow \text{well ordering principle}).$$

Proof.

$\implies$ 4.1.3.

$\impliedby$ If A is a set of non-empty sets, let $B = \bigcup A$. By the well ordering principle, there is a well ordering $\leq_B$ of B. Then define
$$f : A \to \bigcup A,$$
by $f(a)$ as the least element of a, with respect to $\leq_B$.

□

Corollary 4.1.6. *Assume ZFC.*

1. *If A is any set, there is an ordinal α with $\alpha \approx A$.*

2. *If A and B are sets, then one of $|A| \leq |B|$ or $|B| \leq |A|$ holds.*

3. *Fundamental theorem of cardinal arithmetic. If A is any infinite set, then $|A \times A| = |A|$.*

Proof.

1. 3.5.3.

2. By the remark after the proof of 3.3.7.

3. 3.5.3.

□

Lemma 4.1.7. *Assuming ZFC, for sets A and B, with $A \neq \emptyset$, we have $|A| \leq |B|$ if and only if there is a surjective function $h : B \to A$.*

Proof. Problem class. [20]   □

---
[20]Exercise

4.2   Cardinals and cardinal arithmetic

Assume ZFC.

Definition 4.2.1. An ordinal α is a **cardinal** if it is not equinumerous with any $\beta < \alpha$.

Example.

- If $n \in \omega$, then n is a cardinal.

- ω is a cardinal.

- If β is an infinite ordinal, then $\beta^\dagger$ is not a cardinal, as $\beta \approx \beta^\dagger$.

Lemma 4.2.2.

1. Suppose γ is any ordinal. There is a unique cardinal α with $\alpha \approx \gamma$.

2. Suppose A is any set. There is a unique cardinal α such that $A \approx \alpha$.

Proof.

1. Take the least element of $\{\beta \leq \gamma \mid \beta \approx \gamma\}$.

2. By 4.1.6, there is an ordinal γ with $\gamma \approx A$. Use 1.

$\square$

Definition 4.2.3. The unique cardinal equinumerous with A is called the **cardinality** of A. Denote by card A or $|A|$.

Remark. There is an injective function $A \to B$ if and only if card $A \leq$ card B. [21] So ok to use $|A|$.

If α is an ordinal, then α is a cardinal if and only if $|\alpha| = \alpha$.

Example. If A is a countably infinite set, then $|A| = \omega$.

Definition 4.2.4. Suppose A and B are disjoint sets with $|A| = \kappa$ and $|B| = \lambda$. Let

- $\kappa + \lambda = |A \cup B|$, and

- $\kappa \cdot \lambda = |A \times B|$.

Remark. This does not depend on the choice of A and B.

Theorem 4.2.5. *Suppose κ and λ are cardinals, $\kappa \leq \lambda$, and λ is infinite. Then*

1. *$\kappa \cdot \lambda = \lambda$, if $\kappa \neq 0$, and*

2. *$\kappa + \lambda = \lambda$.*

Proof.

1. As $\kappa \subseteq \lambda$, we have $\kappa \times \lambda \subseteq \lambda \times \lambda$. So

$$\kappa \cdot \lambda = |\kappa \times \lambda| \leq |\lambda \times \lambda| = |\lambda| = \lambda,$$

   by the fundamental theorem of cardinal arithmetic, and λ is a cardinal. On the other hand, as $\kappa \neq 0$,

$$\lambda = |\lambda| = |\{0\} \times \lambda| \leq |\kappa \times \lambda| = \kappa \cdot \lambda.$$

2. By 1,

$$\lambda \leq \kappa + \lambda \leq \lambda + \lambda = \{0,1\} \cdot \lambda = 2 \cdot \lambda = \lambda.$$

   So $\lambda = \kappa + \lambda$.

$\square$

---

[21]Exercise

Theorem 4.2.6. *Suppose A is an infinite set of cardinality λ. Suppose each element of A is a set of cardinality at most κ. Then*

$$\left| \bigcup A \right| \leq \lambda \cdot \kappa.$$

Proof. Can assume $\emptyset \notin A$. For each $a \in A$, the set

$$S_a = \{\text{surjective functions } \kappa \to a\}$$

is non-empty, by 4.1.7. Assuming the axiom of choice, there is a function

$$
\begin{array}{rcl}
F & : & A \longrightarrow \bigcup_{a \in A} S_a \\
  &   & a \longmapsto \kappa \to a
\end{array},
$$

which is a surjective function. Denote this by F_a. Let $h : \lambda \to A$ be a bijection. Now define

$$
\begin{array}{rcl}
G & : & \lambda \times \kappa \longrightarrow \bigcup A \\
  &   & (\alpha, \beta) \longmapsto F_{h(\alpha)}(\beta)
\end{array}.
$$

This is surjective. So by 4.1.7, $|\lambda \times \kappa| \geq |\bigcup A|$, that is $|\bigcup A| \leq \lambda \cdot \kappa$. $\qquad\square$

Example 4.2.7.

1. Suppose A is an infinite set, so $|A| = \lambda \geq \omega$. Let

$$S = \{\text{finite sequences of elements of } A\} = \bigcup_{n \in \omega} A^n.$$

   Then $|S| = |A| = \lambda$.

2. Consider $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Suppose $B \subseteq \mathbb{R}$, such that the linear span of B, over $\mathbb{Q}$, is $\mathbb{R}$. Then $|B| = |\mathbb{R}|$.

Proof.

1. For $n \in \mathbb{N}, |A|^n = |A|$, by repeated use of the fundamental theorem of cardinal arithmetic. By 4.2.6,

$$|S| \leq \omega \cdot |A| = |\omega| \cdot |A| = \lambda,$$

   by 4.2.5.1. Then $A \subseteq S$, so $|S| \geq \lambda$.

2. Obviously $|B| \leq |\mathbb{R}|$, and B is infinite. If $x \in \mathbb{R}$, there are

$$n \in \mathbb{N}, \qquad q_0, \ldots, q_n \in \mathbb{Q}, \qquad b_0, \ldots, b_n \in B, \qquad x = \sum_{i=0}^{n} q_i b_i.$$

   Let

$$S_1 = \{\text{finite sequences from } \mathbb{Q}\}, \qquad S_2 = \{\text{finite sequences from } B\}.$$

   Consider

$$S_1 \times S_2 \supseteq T = \{((q_0, \ldots, q_n), (b_0, \ldots, b_n)) \mid q_i \in \mathbb{Q}, \ b_i \in B\}.$$

   We have a surjection

$$
\begin{array}{rcl}
T & \longrightarrow & \mathbb{R} \\
((q_0, \ldots, q_n), (b_0, \ldots, b_n)) & \longmapsto & x = \sum_{i=0}^{n} q_i b_i
\end{array}.
$$

   By 1, $|S_1| = |\mathbb{Q}| = \omega$ and $|S_2| = |B|$. By 4.1.7,

$$|\mathbb{R}| \leq |T| \leq |S_1 \times S_2| = \omega \cdot |B| = \max(\omega, |B|),$$

   by 4.2.5. As $|\mathbb{R}| > \omega$, we get $|B| = |\mathbb{R}|$.

$\qquad\square$

4.3   Zorn's lemma

A **partially ordered set (poset)** $\langle A; \leq \rangle$ satisfies

$$(\forall x \in A)\,(\forall y \in A)\,(\forall z \in A)\,(((x \leq y) \wedge (y \leq z)) \to (x \leq z))$$
$$\wedge\,(\forall x \in A)\,(\forall y \in A)\,(((x \leq y) \wedge (y \leq x)) \to (x = y))$$
$$\wedge\,(\forall x \in A)\,(x \leq x)\,.$$

Example. $\langle \mathcal{P}(X)\,;\subseteq \rangle$.

A **chain** C in a partially ordered set $\langle A; \leq \rangle$ is a subset $C \subseteq A$ such that

$$(\forall x \in C)\,(\forall y \in C)\,((x \leq y) \vee (y \leq x))\,.$$

An **upper bound** of C in A is $a \in A$ such that

$$(\forall x \in C)\,(x \leq a)\,.$$

Example. If $C \subseteq \mathcal{P}(X)$ is a chain, then $\bigcup C$ is an upper bound for C in $\mathcal{P}(X)$.

Definition 4.3.1 (Zorn's lemma)**.** Suppose $\langle A; \leq \rangle$ is a non-empty partially ordered set, in which every chain has an upper bound in A. Then A has a maximal element. That is,

$$(\exists z \in A)\,(\forall x \in A)\,((z \leq x) \to (x = z))\,.$$

Theorem 4.3.2.

$$ZF \vdash (\textit{the axiom of choice} \leftrightarrow \textit{Zorn's lemma})\,.$$

- *Assuming ZFC, then Zorn's lemma holds.*

- *Assuming ZF and Zorn's lemma, then the axiom of choice holds.*

Example 4.3.3. Assume ZFC. Suppose V is a vector space over a field F. Then V has a basis over F.

Proof. Use Zorn's lemma. Let

$$A = \{\text{linearly independent subsets of } V, \text{ ordered by } \subseteq\}\,.$$

Claim that, if C is a chain in A, then $\bigcup C \in A$. Must show that, if $y_1, \ldots, y_n \in \bigcup C$, then $y_1, \ldots, y_n$ are linearly independent. Let $C_1, \ldots, C_n \in C$, such that $y_i \in C_i$. As C is a chain, there is some $j \leq n$ with $C_i \subseteq C_j$ for all $i \leq n$. But then $y_1, \ldots, y_n \in C_j$, and so $y_1, \ldots, y_n$ are linearly independent. So in $\langle A; \subseteq \rangle$, every chain has an upper bound. So by Zorn's lemma, there is a maximal element B of A. So B is a linearly independent set, and if $v \in V \setminus B$, then $B \cup \{v\}$ is not linearly independent. It follows that v is a linear combination of elements of B. So span of B is V. $\qquad\square$

Proof of 4.3.2.

$\implies$ Let

$$f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$$

be a choice function. Suppose for a contradiction that A has no maximal element. Let $C \subseteq A$ be a chain. By assumption, there is some $y \in A$ with $c \leq y$ for all $c \in C$. So there is $z > y$ in A, and therefore $z > c$ for all $c \in C$. Use transfinite recursion to define an operation G such that, for all ordinals α, $G(\alpha) \in A$ and

$$G(\alpha) = f(\{z \in A \mid z > G(\beta) \text{ for all } \beta < \alpha\})\,.$$

So

$$G(0) < \cdots < G(\beta) < \ldots\,.$$

That is, for all ordinals $\beta < \alpha$,

$$G(\beta) < G(\alpha)\,.$$

By Hartogs' lemma, or by cardinality, this is impossible.

$\hfill\square$

5   Postscript

Assume ZFC. For a first-order language $\mathcal{L}$, the cardinality of $\mathcal{L}$ is the cardinality of the set of $\mathcal{L}$-formulas, which is the cardinality of the alphabet. Assuming ZFC, the following hold for $\mathcal{L}$ of arbitrary cardinality.

- Gödel's completeness theorem, and results leading to it. Compare 3.6.

- The compactness theorem, and the compactness theorem for normal models in $\mathcal{L}^{=}$.

A   Proofs

A.1   Lemma 2.3.7

Proof of 2.3.7. This is by induction on the number of connectives and quantifiers in ϕ.

- Base case. ϕ is an atomic formula $R(u_1, \ldots, u_m)$, where R is an m-ary relation symbol and $u_1, \ldots, u_m$ are terms. Let u_i^* be the result of substituting t for x_1 in u_i. Then by induction on the length of the terms, each u_i^* is a term and $\mathrm{v}'(u_i) = \mathrm{v}(u_i^*)$. Moreover, $\phi(t)$ is $R(u_1^*, \ldots, u_m^*)$. Then

$$\mathrm{v}'[\phi(x_1)] = \mathrm{T} \quad \Longleftrightarrow \quad \mathcal{A} \vDash R(\mathrm{v}'(u_1), \ldots, \mathrm{v}'(u_m))$$
$$\Longleftrightarrow \quad \mathcal{A} \vDash R(\mathrm{v}(u_1^*), \ldots, \mathrm{v}(u_m^*))$$
$$\Longleftrightarrow \quad \mathrm{v}[\phi(t)] = \mathrm{T}.$$

- Inductive step. There are three cases.

  Case 1. ϕ is $(\neg\psi)$. [22]

  Case 2. ϕ is $(\psi \to \chi)$. [23]

  Case 3. ϕ is $(\forall x_i)\,\psi$. We can assume that $i \neq 1$. Otherwise, x_1 is not free in ϕ, and $\phi(t)$ is just ϕ. 2.3.7 then follows from 2.3.3. Note also that, as t is free for x_1 in $(\forall x_i)\,\psi$, it follows that t is free for x_1 in ψ, and x_i is not a variable in t. Suppose first that $\mathrm{v}'[\phi(x_1)] = \mathrm{F}$. We show that $\mathrm{v}[\phi(t)] = \mathrm{F}$. By 2.2.9, there is a valuation w' which is x_i-equivalent to v' with $\mathrm{w}'[\psi(x_1)] = \mathrm{F}$. Note that, as $i \neq 1$,

$$\mathrm{w}'(x_1) = \mathrm{v}'(x_1) = \mathrm{v}(t). \tag{14}$$

  Define a valuation w by

$$\mathrm{w}(x_j) = \begin{cases} \mathrm{v}(x_j) & j \neq 1, i \\ \mathrm{w}'(x_i) & j = i \\ \mathrm{v}(x_1) & j = 1 \end{cases}.$$

  So w is x_1-equivalent to w' and x_i-equivalent to v, noting that v and v' are x_i-equivalent, and w and v' are x_i-equivalent. As x_i does not occur in t, we have, by 2.3.3 and (14),

$$\mathrm{w}(t) = \mathrm{v}(t) = \mathrm{w}'(x_1).$$

  We can now apply the inductive hypothesis to $\mathrm{w}, \mathrm{w}', \psi$. We obtain that

$$\mathrm{w}[\psi(t)] = \mathrm{w}'[\psi(x_1)] = \mathrm{F}.$$

  As w and v are x_i-equivalent, it follows that

$$\mathrm{v}[(\forall x_i)\,\psi(t)] = \mathrm{F}.$$

  So $\mathrm{v}[\phi(t)] = \mathrm{F}$, as required. We now prove the converse direction, since we cannot argue by symmetry here. So suppose $\mathrm{v}[\phi(t)] = \mathrm{F}$. There is a valuation w which is x_i-equivalent to v with $\mathrm{w}[\psi(t)] = \mathrm{F}$. Let w' be the valuation x_1-equivalent to w with

$$\mathrm{w}'(x_1) = \mathrm{w}(t) = \mathrm{v}(t) = \mathrm{v}'(x_1).$$

  The fact that $\mathrm{w}(t) = \mathrm{v}(t)$ is as before. By the inductive hypothesis,

$$\mathrm{w}'[\psi(x_1)] = \mathrm{w}(\psi(t)) = \mathrm{F}.$$

  As w' is x_i-equivalent to v', we have

$$\mathrm{v}'[(\forall x_i)\,\psi(x_1)] = \mathrm{F}.$$

  So $\mathrm{v}'[\phi(x_1)] = \mathrm{F}$. This completes the inductive step.

  $\square$

---

[22]Exercise
[23]Exercise

A.2   Theorem 2.5.3

Proof of 2.5.3. A series of steps. The notation is cumulative.

Step 1. Let $b_0, b_1, \ldots$ be new constant symbols. Form $\mathcal{L}^+$ by adding these to the symbols of $\mathcal{L}$. Regard Σ as a set of $\mathcal{L}^+$-formulas. Check that Σ is still consistent, in the formal system $K_{\mathcal{L}^+}$. Note that $\mathcal{L}^+$ is still a countable language.

Step 2. Adding **witnesses**. Claim that there is a consistent set of closed $\mathcal{L}^+$-formulas $\Sigma_\infty \supseteq \Sigma$ such that, for every $\mathcal{L}^+$-formula $\theta(x_i)$ with one free variable, there is some b_j with

$$\Sigma_\infty \vdash_{K_{\mathcal{L}^+}} ((\neg(\forall x_i)\,\theta(x_i)) \to (\neg\theta(b_j))).$$

Think of $\theta(x_i)$ as $(\neg\chi(x_i))$. Then this formula is essentially

$$((\exists x_i)\,\chi(x_i) \to \chi(b_j)),$$

so b_j witnesses the existence of x_i satisfying χ.

Step 3. By the Lindenbaum lemma in 2.5.2, there is a consistent set $\Sigma^* \supseteq \Sigma_\infty$ of closed $\mathcal{L}^+$-formulas such that, for every closed ϕ, either $\Sigma^* \vdash_{K_{\mathcal{L}^+}} \phi$ or $\Sigma^* \vdash_{K_{\mathcal{L}^+}} (\neg\phi)$.

Step 4. Building a structure. Let
$$A = \left\{ \bar{t} \mid t \text{ is a closed term of } \mathcal{L}^+ \right\}.$$

Note that

- a term is closed if it only involves constant symbols and function symbols, and no variables,
- use the $\bar{\cdot}$ to distinguish when we are thinking of a term as an element of A, and
- as $\mathcal{L}^+$ is countable, A is countable.

Make A into an $\mathcal{L}^+$ structure.

(a) Each constant symbol c of $\mathcal{L}^+$ is interpreted as $\bar{c} \in A$.

(b) Suppose R is an n-ary relation symbol. Define the relation $\overline{R} \subseteq A^n$ by $(\overline{t_1}, \ldots, \overline{t_n}) \in \overline{R}$ if and only if $\Sigma^* \vdash_{K_{\mathcal{L}^+}} R(t_1, \ldots, t_n)$, where $R(t_1, \ldots, t_n)$ is a closed atomic $\mathcal{L}^+$-formula and $t_1, \ldots, t_n$ are closed $\mathcal{L}^+$-terms.

(c) Suppose f is an m-ary function symbol. Define a function $\overline{f} : A^m \to A$ by

$$\overline{f}\left(\overline{t_1}, \ldots, \overline{t_m}\right) = \overline{f(t_1, \ldots, t_m)},$$

for closed terms $t_1, \ldots, t_m$.

Call this structure $\mathcal{A}$. Note that, if v is a valuation in $\mathcal{A}$ and t is a closed term, then $\text{v}(t) = \bar{t}$, by (a) and (c) here.

Step 5. Main lemma. Claim that, for every closed $\mathcal{L}^+$-formula ϕ,

$$\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} \phi \qquad \Longleftrightarrow \qquad \mathcal{A} \vDash \phi. \tag{15}$$

Prove by induction on the number of connectives and quantifiers in ϕ.

- Base case. ϕ is atomic, that is ϕ is $R(t_1, \ldots, t_n)$, for some closed terms t_i, and relation symbol R. Then (15) holds by (b) in definition of $\mathcal{A}$.

- Inductive step. Assume (15) holds for closed formulas involving fewer connectives and quantifiers.

  Case 1. ϕ is $(\neg\psi)$.

  Case 2. ϕ is $(\psi \to \chi)$.

  Case 3. ϕ is $(\forall x_i)\,\psi$.

  In cases 1 and 2, ψ and χ are closed. So (15) holds for these.

  Case 1. ϕ is $(\neg\psi)$.

$$
\begin{aligned}
\mathcal{A} \vDash \phi \qquad &\Longleftrightarrow \qquad \mathcal{A} \nvDash \psi && \text{by 2.3.3} \\
&\Longleftrightarrow \qquad \Sigma^* \nvdash_{\mathrm{K}_{\mathcal{L}^+}} \psi && \text{by the induction hypothesis (15)} \\
&\Longleftrightarrow \qquad \Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} (\neg\psi) && \text{by step 3.}
\end{aligned}
$$

  Case 2. Exercise. [24]

  Case 3. ϕ is $(\forall x_i)\,\psi$.

   Case 3a. x_i is not free in ψ. So ψ is closed and we can use the inductive hypothesis.

   Case 3b. x_i is free in ψ. So $\psi(x_i)$ has a single free variable.

   $\Longleftarrow$ Suppose for a contradiction that $\mathcal{A} \vDash \phi$ and $\Sigma^* \nvdash_{\mathrm{K}_{\mathcal{L}^+}} \phi$. Then by step 3,

$$\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} (\neg\phi).$$

   By step 2,
$$\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} ((\neg (\forall x_i)\,\psi(x_i)) \to (\neg\psi(b_j))),$$

   for some constant symbol b_j. That is,

$$\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} ((\neg\phi) \to (\neg\psi(b_j))).$$

   So
$$\Sigma^* \vdash_{\mathrm{K}_{\mathcal{L}^+}} (\neg\psi(b_j)).$$

   $(\neg\psi(b_j))$ is closed and, by case 1, (15) applies. We obtain

$$\mathcal{A} \vDash (\neg\psi(b_j)). \tag{16}$$

   This contradicts $\mathcal{A} \vDash (\forall x_i)\,\psi$. Take a valuation v in $\mathcal{A}$ with $\mathrm{v}(x_i) = \overline{b_j}$, then v does not satisfy ψ, by (16).

$\square$

---

[24]Exercise

A.3   Lemma 2.6.3

Proof of 2.6.3. The result 2.6.3 is proved by induction on the number of connectives and quantifiers in ϕ.

- Base case. ϕ is an atomic formula $R(t_1, \ldots, t_n)$, where R is an n-ary relation symbol and $t_1, \ldots, t_n$ are terms. Then

$$
\begin{aligned}
\text{v}[\phi] = \text{T} \quad &\Longleftrightarrow \quad \overline{R}(\text{v}(t_1), \ldots, \text{v}(t_n)) \text{ holds in } \mathcal{A} \\
&\Longleftrightarrow \quad \overline{R}\left(\widehat{\text{v}(t_1)}, \ldots, \widehat{\text{v}(t_n)}\right) \text{ holds in } \mathcal{A} \qquad \text{by definition of } \overline{R} \text{ in } \widehat{\mathcal{A}} \\
&\Longleftrightarrow \quad \overline{R}(\widehat{\text{v}}(t_1), \ldots, \widehat{\text{v}}(t_n)) \text{ holds in } \mathcal{A} \\
&\Longleftrightarrow \quad \widehat{\text{v}}[\phi] = \text{T},
\end{aligned}
$$

  as required.

- Inductive step.

  Case 1. ϕ is $(\neg \psi)$. [25]

  Case 2. ϕ is $(\theta \to \chi)$. [26]

  Case 3. ϕ is $(\forall x_i)\psi$.

  $\Longrightarrow$ If $\text{v}[(\forall x_i)\psi] = \text{F}$, there is a v', x_i-equivalent to v, with $\text{v}'[\psi] = \text{F}$. Then $\widehat{\text{v}'}$ is x_i-equivalent to $\widehat{\text{v}}$, and by the inductive hypothesis,

  $$\widehat{\text{v}'}[\psi] = \text{F}.$$

  So $\widehat{\text{v}}[(\forall x_i)\psi] = \text{F}$.

  $\Longleftarrow$ Suppose $\widehat{\text{v}}[(\forall x_i)\psi] = \text{F}$. So there is a valuation w in $\widehat{\mathcal{A}}$ which is x_i-equivalent to $\widehat{\text{v}}$ and $\text{w}[\psi] = \text{F}$. There is a valuation v' in $\mathcal{A}$, x_i-equivalent to v, with $\widehat{\text{v}'} = \text{w}$. We just change $\text{v}(x_i)$, so

  $$\widehat{\text{v}'(x_i)} = \text{w}(x_i).$$

  Then $\text{v}'[\psi] = \text{F}$, by the induction hypothesis. So $\text{v}[(\forall x_i)\psi] = \text{F}$.

  $\square$

---

[25] Exercise

[26] Exercise

A.4   Theorem 3.5.2

Proof of 3.5.2.

- Assume that, if $\omega \neq \beta < \alpha$, then $\beta \approx \beta \times \beta$, the transfinite inductive hypothesis. Deduce $\alpha \approx \alpha \times \alpha$.

- May assume that, if $\beta < \alpha$, then $|\beta| < |\alpha|$. This implies $\left|\beta^\dagger\right| < |\alpha|$.

- Enough to show $|\alpha \times \alpha| \leq |\alpha|$, by 3.1.6.

Step 1. Suppose we have a well ordering $\leq$ of $A = \alpha \times \alpha$ such that, for all $x \in A$,

$$|A[x]| = |\{y \in A \mid y < x\}| < |\alpha|.$$

Then prove that $|\alpha \times \alpha| = |\alpha|$. By 3.4.6, there is an ordinal γ which is similar to $\langle A; \leq \rangle$. Let

$$f : \gamma \to A$$

be the similarity. Show that $\gamma \subseteq \alpha$. Thus $|\gamma| \leq |\alpha|$, so $|A| \leq |\alpha|$. Let $\eta \in \gamma$, so $\eta < \gamma$. As f is a similarity, it gives a bijection

$$\eta = \{\delta \in \gamma \mid \delta < \eta\} \to A[f(\eta)].$$

So

$$|\eta| = |A[f(\eta)]| < |\alpha|.$$

Thus $\eta < \alpha$. Otherwise $\alpha \leq \eta$, so $\alpha \subseteq \eta$, and then $|\alpha| \leq |\eta|$, a contradiction. Thus $\eta \in \alpha$.

Step 2. Find an ordering $\leq$ on $\alpha \times \alpha = A$ as in step 1. For $\lambda < \alpha$, let

$$A_\lambda = \{(\theta, \zeta) \in \alpha \times \alpha \mid \max(\theta, \zeta) = \lambda\}.$$

Define $\leq$ on A by

$$(\theta', \zeta') < (\theta, \zeta) \qquad \Longleftrightarrow \qquad \begin{cases} \max(\theta', \zeta') < \max(\theta, \zeta) \\[2mm] \max(\theta', \zeta') = \lambda = \max(\theta, \zeta) \text{ and } \begin{cases} \zeta = \zeta' = \lambda \text{ and } \theta' < \theta \\ \zeta' < \zeta = \lambda \\ \theta = \theta' = \lambda \text{ and } \zeta' < \zeta \end{cases} \end{cases}.$$

Check that $\leq$ is a well ordering on A. Show that the property in step 1 holds. Let $x = (\theta, \zeta) \in A$. Let $\lambda = \max(\theta, \zeta)$. May assume $\lambda \geq \omega$. Let $\mu = \lambda^\dagger$. So $|\mu| < |\alpha|$, and by the induction hypothesis, $|\mu \times \mu| = |\mu| < |\alpha|$. Then

$$\{y \in A \mid y < x\} \subseteq \{(\theta', \zeta') \in A \mid \max(\theta', \zeta') \leq \lambda\} \subseteq \mu \times \mu.$$

Thus $|A[x]| \leq |\mu \times \mu| < |\alpha|$.

$\square$

A.5   Theorem 3.6.1

Proof of 3.6.1. Suppose α is an ordinal and t is a function with domain $\alpha^\dagger$ such that, for all $\beta \leq \alpha$, we have that $t(\beta) = F(t \restriction \beta)$. For the purposes of the proof, we say that t is a **computation of length α based on** F. Note that, in this case, if $\gamma \leq \alpha$, then

$$t \restriction \{\beta \mid \beta \leq \gamma\}$$

is a computation of length γ based on F. The main thing to prove is the claim that, for each ordinal α, there is a unique computation t based on F of length α. Once we have this, consider the property $G(x,y)$ given by

either x is an ordinal and $y = t(x)$, or x is not an ordinal and $y = \emptyset$,

where t is a computation based on F of length x. According to the claim, $G(x,y)$ defines an operation G, with $G(a) = b$ if and only if $G(a,b)$ holds. Moreover, by definition, we have that, if α is an ordinal, then $G(\alpha) = t(\alpha)$ for the unique computation t of length α. It follows, by the uniqueness, and the fact that the restriction of a computation to a successor initial segment is a computation, that $G(\beta) = t(\beta)$ for all $\beta \leq \alpha$. So

$$t \restriction \alpha = G \restriction \alpha,$$

and we have $G(\alpha) = F(G \restriction \alpha)$, as required. To prove the claim, we use transfinite induction, in 3.5.1. So assume that, for all $\beta < \alpha$, there is a unique computation t_β of length β, based on F. We must show that there is a unique computation of length α. This comes in two parts, existence and uniqueness.

- Existence. Note that, if $\gamma < \beta < \alpha$, then the uniqueness part of the inductive hypothesis implies that t_γ must be the restriction of t_β to $\gamma^\dagger$. So

$$s = \bigcup_{\beta < \alpha} t_\beta$$

  is a function with domain α, and

$$s(\beta) = t_\beta(\beta) = F(s \restriction \beta), \qquad \beta < \alpha.$$

  We extend s to a function t with domain $\alpha^\dagger$ by setting $t(\alpha) = F(s)$. Then for all $\beta \leq \alpha$, we have that $t(\beta) = F(t \restriction \beta)$. So t is a computation of length α based on F.

- Uniqueness. Suppose t and t' are computations of length α. We must show $t(\beta) = t'(\beta)$ for all $\beta \leq \alpha$. We do this by transfinite induction on β. Indeed, if $t(\gamma) = t'(\gamma)$ for all $\gamma < \beta$, then

$$t(\beta) = F(t \restriction \beta) = F(t' \restriction \beta) = t'(\beta).$$

So this establishes the inductive step, and proves the claim. As we have seen, 3.6.1 then follows. $\square$

There is a reformulation which is convenient in practice. First, some terminology. We say that an ordinal α is a **successor ordinal** if there is an ordinal β such that $\alpha = \beta^\dagger$. Otherwise it is a **limit ordinal**. It is easy to see that an ordinal α is a limit ordinal if and only if

$$\alpha = \bigcup \{\beta \mid \beta < \alpha\}.$$

Example. 0 and ω are limit ordinals.

Theorem A.5.1 (Definition by transfinite recursion). *Let F_1 and F_2 be operations on sets and a_0 a set. Then there is an operation G such that, for all ordinals α,*

- $G(\emptyset) = a_0$,

- $G(\alpha^\dagger) = F_1(G \restriction \alpha^\dagger)$, *and*

- $G(\alpha) = F_2(G \restriction \alpha)$ *if α is a limit ordinal.*

The operation G is uniquely determined on ordinals.

The second version of transfinite recursion is obtained simply by combining F_1 and F_2 into a suitable property F. We omit the details.