Sets, Models and Proofs

I. Moerdijk and J. van Oosten
Department of Mathematics
Utrecht University

2000; revised, 2013

Introduction

In these lecture notes we present an introduction to the field of (Mathematical) Logic.

Mathematical knowledge is organized in the form of *statements* (propositions, theorems, but also: conjectures, questions) and Logic aims to analyze at least two aspects of these statements: they can be true or false (that is to say: they have a relationship with reality), and they can sometimes be proved.

In order to study these aspects in a precise way, we restrict our attention to a kind of idealized, abstract statements which are just strings of symbols of a certain alphabet: the sentences of a formal language. We can then define what it means, for such an abstract sentence, that it is 'true' in a particular interpretation (for example, the sentence "2 is a square" is true in $\mathbb{R}$ but false in $\mathbb{N}$). This definition is due to Alfred Tarski. We treat this in chapter 2, *Models*.

An abstract proof, then, is a collection of sentences which is structured in such a way that every sentence which appears in it, is either an assumption or can be seen as a direct consequence of sentences which have appeared 'before' in the proof; we use the picture of a tree, and our proofs are so-called *natural deduction trees*. Every proof has a unique conclusion, which is a sentence. The theory of proofs takes up chapter 3, *Proofs*. We prove the most fundamental theorem of Logic, *Gödel's Completeness Theorem*, in this chapter. This theorem says, that a sentence is always true (in all possible interpretations) precisely if it is the conclusion of such a proof tree.

But before we can even start, we must broaden our idea of the world of sets. Chapter 1, *Sets*, reviews in an informal way some topics that are important in many areas of Mathematics, such as: cardinalities, Zorn's Lemma and the Axiom of Choice, well-orders and transfinite induction.

However, once we know what a formal theory is (a collection of sentences in the sense of Chapters 2 and 3), we can also look at the formal theory of sets. In Chapter 4, *Sets Again*, we explain how the theory of sets can be set up with axioms. We hope to convince you that these axioms are sufficient for 'doing mathematics'; but actually we cannot (in the scope of these lecture notes) even scratch the surface of this vast topic.

Acknowledgement: we are indebted to Benno van den Berg, Nicola Gambino, Jeroen Goudsmit, Fabio Pasquali, Marcel de Reus, Sebastiaan Terwijn, Andreas Weiermann and Ittay Weiss for pointing out typos and inaccuracies in earlier versions of these notes. We have corrected them. Needless to say,

all remaining errors are ours.

Contents

Chapter 1

Sets

This chapter intends to further develop your understanding of sets.

The first mathematician who thought about sets, and realized that it makes sense to organize mathematical knowledge using the concept of 'set', was Georg Cantor (1845–1918). His name will appear at several places in these lecture notes. For biographical information on Cantor, whose genius did not receive proper recognition in his time and who had a troubled life, see [6] or the sketch in [15].

The first triumph of Cantor's theory of sets was that he could show that there are 'different kinds of infinity': although the set of rational numbers and the set of irrational numbers are both infinite, there are 'more' irrational numbers than rational ones.

An important part of this chapter is about how to calculate with these different kinds of infinity. It turns out that in order to set up the theory, it is necessary to adopt a principle which was first formulated by Ernst Zermelo in 1904: the Axiom of Choice. In sections 1.2 and 1.2.1, we introduce you to how to work with this axiom and with a useful equivalent principle: Zorn's Lemma.

Then, in section 1.3, we develop another concept which originates with Cantor: that of a *well-order*. Thanks to this idea, we can extend proofs by induction to arbitrarily 'large' sets.

Finally, in section 1.4, which is an appendix to this chapter, precise proofs are given of the equivalence between various versions of the Axiom of Choice.

So let us start. Instead of trying to formulate what a 'set' is, we assume that you already have some idea of it. A set has 'elements'. If X is a set and x is an element of X, we write $x \in X$. Think of X as a *property*, and

the elements of X as the things having property X.

A set is completely determined by its elements. That means: suppose the sets X and Y have the same elements. So for all $x \in X$ we have $x \in Y$, and vice versa. Then we consider X and Y to be the same set: $X = Y$.

A set X is called a *subset* of a set Y, if every element of X is also an element of Y. We write: $X \subset Y$ (or $X \subseteq Y$ if we want to stress that X and Y might be equal). For example, if $x \in X$ then there is a subset $\{x\}$ of X, which has only the one element x.

We also assume that you have an idea of what a *function* between sets is: a function f from X to Y (notation $f : X \to Y$) gives us for each element x of X a unique element $f(x)$ of Y, the value of the function f at x.

A function $f : X \to Y$ is completely determined by its values. That means: if f and g are functions from X to Y and for every $x \in X$ we have $f(x) = g(x)$, then f and g are the same function: $f = g$.

The following examples of sets are familiar to you: the *empty set* $\emptyset$, which has no elements, the set $\mathbb{N} = \{0, 1, \ldots\}$ of *natural numbers*, and likewise the sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ of integers, rational numbers and real numbers, respectively. By the way, it was Cantor who introduced the notation $\mathbb{R}$!

You see that we have started to use the *curly bracket notation* $\{\}$ for writing sets: we specify a set by giving its elements, either by listing them all (using dots if necessary, as in $\{0, 1, 2, \ldots\}$), or by giving the property that the elements of the set must satisfy, as in for example

$$\mathbb{R}_{>0} \;=\; \{x \,|\, x \in \mathbb{R} \text{ and } x > 0\}$$

The following are examples of functions: for every set X, there is the *empty function* from $\emptyset$ to X, and the *identity function* from X to X (this function, say $I_X : X \to X$, is such that $I_X(x) = x$ for every $x \in X$). Given functions $f : X \to Y$ and $g : Y \to Z$ there is the *composition* $g \circ f : X \to Z$ (or $gf : X \to Z$), which is defined by: $g \circ f(x) = g(f(x))$ for all $x \in X$.

In general, if X and Y are sets, and for every element x of X a subset Y_x of Y is given such that Y_x has exactly one element, then there is a (unique) function $f : X \to Y$ with the property that $f(x) \in Y_x$ for every $x \in X$.

Let us recall some more definitions.

A function $f : X \to Y$ is called *injective* (or 1-1) if for each $x, y \in X$ it holds that $f(x) = f(y)$ implies $x = y$.

The function f is *surjective* (or onto) if every $y \in Y$ is equal to $f(x)$ for some $x \in X$.

And f is called *bijective* if there is a function $g : Y \to X$ such that for all $x \in X$ and all $y \in Y$ the equalities $g(f(x)) = x$ and $f(g(y)) = y$ hold. Given f, the function g is unique if it exists, and is called the *inverse* of f, notation: f^{-1}.

If $f : X \to Y$ is a function, there is the subset of Y which consists of all elements of the form $f(x)$ for $x \in X$. This subset is called the *image* of the function f. Likewise, if A is a subset of Y, there is the subset of X which consists of all elements $x \in X$ such that $f(x) \in A$. This subset is sometimes denoted by $f^{-1}(A)$, and called the *inverse image* of A under f.

Exercise 1 Prove:

a) A function $f : X \to Y$ is bijective if and only if it is both injective and surjective;

b) a function $f : X \to Y$ is surjective if and only if the image of f is equal to Y;

c) if $f : X \to Y$ is injective, then f is a bijective function from X to the image of f.

Let us also recall the following basic operations on sets:

The *union* $X \cup Y$ of X and Y is the set $\{z \mid z \in X \text{ or } z \in Y\}$.

The *intersection* $X \cap Y$ is the set $\{z \mid z \in X \text{ and } z \in Y\}$.

If $X \subseteq Y$, the *complement* of X in Y, written as $Y - X$, is the set of those elements of Y that are not elements of X (in the literature, one also finds the notation $Y \setminus X$).

The sets X and Y are *disjoint* if they have no elements in common. This is equivalent to: $X \cap Y = \emptyset$.

1.1 Cardinal Numbers

A set X is *finite* if for some $n \in \mathbb{N}$ there is a bijective function $f : \{1, \ldots, n\} \to X$ (for $n = 0$, the set $\{1, \ldots, n\}$ is empty). This means that X has exactly n elements; we call n the *cardinality* of X and write $|X|$ for this number (in the literature, the notation $\sharp(X)$ is also sometimes used). A set which is not finite is called *infinite*.

Exercise 2 For an arbitrary set X there is at most one n such that $|X| = n$.

We introduce the following notations for (constructions on) sets:

- We assume that given sets X and Y, for every $x \in X$ and $y \in Y$ the *ordered pair* (x, y) is given, and that we have a set $X \times Y$, given as

  $$X \times Y \;=\; \{(x, y) \,|\, x \in X, y \in Y\}$$

  which we call the *Cartesian product* of X and Y; there are projection functions $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ sending the pair (x, y) to x and to y, respectively; whenever we have functions $f : Z \to X$ and $g : Z \to Y$ there is a *unique* function $h : Z \to X \times Y$ (sending $z \in Z$ to the pair $(f(z), g(z))$) with the property that $\pi_X h = f$ and $\pi_Y h = g$;

- $X + Y$ is the *disjoint sum* of X and Y, constructed as

  $$\{(0.x) \,|\, x \in X\} \cup \{(1, y) \,|\, y \in Y\}$$

- Y^X is the set of functions $f : X \to Y$;

- $\mathcal{P}(X)$, the *power set* of X, is the set of all subsets of X.

Exercise 3 For finite sets X, Y:

a) $|X \times Y| = |X| \times |Y|$

b) $|X + Y| = |X| + |Y|$

c) $|Y^X| = |Y|^{|X|}$

d) $|\mathcal{P}(X)| = 2^{|X|}$

For arbitrary sets X and Y we write $X \sim Y$ to indicate that there is a bijective function from X to Y.

Exercise 4 Prove the following facts about $\sim$:

a) $X \sim X$;

b) if $X \sim Y$, then $Y \sim X$;

c) if $X \sim Y$ and $Y \sim Z$, then $X \sim Z$.

We write $X \leq Y$ if there is an injective function from X to Y.

Since every bijective function is injective, $X \sim Y$ implies $X \leq Y$. Notice also that if $X' \sim X$ and $Y \sim Y'$, then $X' \leq Y'$ whenever $X \leq Y$.

The following theorem is, in the literature, sometimes called the "Schröder-Bernstein Theorem", sometimes the "Cantor-Bernstein Theorem".

Theorem 1.1.1 (Schröder-Cantor-Bernstein) *If $X \leq Y$ and $Y \leq X$, then $X \sim Y$.*

Proof. First notice that we may assume that X and Y are disjoint, for otherwise we can replace them by disjoint sets X' and Y' such that $X \sim X'$ and $Y \sim Y'$ (for example, as in the construction of the disjoint sum).

Suppose $f : X \to Y$ and $g : Y \to X$ are two 1-1 functions. We have to indicate a bijective function $h : X \to Y$.

To this end, we construct a "graph" as follows. The vertices (or nodes) of the graph are the elements of the union $X \cup Y$. We shall denote these elements by just x or y (recall that X and Y are assumed disjoint).

For $x \in X$, there is an edge (labelled f) from x to $f(x)$, and for $y \in Y$ there is an edge (labelled g) from y to $g(y)$. The whole graph decomposes into connected components. These components can have the following forms:

$$\begin{array}{ll}
\text{Type 1} & x_0 \xrightarrow{f} y_0 \xrightarrow{g} x_1 \xrightarrow{f} y_1 \to \dots \\
\text{Type 2} & y_0 \xrightarrow{g} x_0 \xrightarrow{f} y_1 \xrightarrow{g} x_1 \to \dots \\
\text{Type 3} & \dots \to x_{-1} \xrightarrow{f} y_{-1} \xrightarrow{g} x_0 \xrightarrow{f} y_0 \to \dots \\
\text{Type 4} & x_0 \xrightarrow{f} y_0 \to \dots \to y_n \xrightarrow{g} x_0
\end{array}$$

Here, in Type 1, it is assumed that x_0 is not in the image of g; in Type 2, the element y_0 is not in the image of f. Types 1 and 2 extend to the right infinitely. Type 3 extends to both left and right infinitely; Type 4 is finite. Now clearly, within each type there is a bijective correspondence between the x's and the y's in the type; together, these form a bijective function from X to Y. ∎

We extend the notation $|X|$ to arbitrary (not necessarily finite) sets X and use it as follows:

We say $|X| = |Y|$ if $X \sim Y$;

the notation $|X| \leq |Y|$ means $X \leq Y$;

and we write $|X| < |Y|$ if $|X| \leq |Y|$ but not $|X| = |Y|$ (equivalently, by Theorem 1.1.1: $|X| \leq |Y|$ but not $|Y| \leq |X|$).

When $|X| < |Y|$ we think of X as "smaller than" Y; similarly, if $|X| \leq |Y|$ we think of X as "at most as large as" Y.

Definition 1.1.2 For a set X, we refer to $|X|$ as the *cardinality* of X. An object of the form $|X|$ is called a *cardinal number*.

We regard every $n \in \mathbb{N}$ as a cardinal number, namely $n = |\{1, \ldots, n\}|$. Note that this also means $0 = |\emptyset|$. Note also, that $n \leq m$ as cardinal numbers if and only if $n \leq m$ in the usual ordering of $\mathbb{N}$. There are also infinite cardinal numbers, such as $|\mathbb{N}|$.

Definition 1.1.3 We have the following operations on cardinal numbers:

- $|X| \times |Y| = |X \times Y|$
- $|X| + |Y| = |X + Y|$
- $|Y|^{|X|} = |Y^X|$

Exercise 5 Is this a correct definition? What do you have to check?

Exercise 6 Prove that the operations $+$, $\times$ and $(-)^{(-)}$ for cardinal numbers satisfy the following usual rules of arithmetic:

a) $(|X| + |Y|) \times |Z| = (|X| \times |Z|) + (|Y| \times |Z|)$

b) $|X|^{|Y|+|Z|} = (|X|^{|Y|}) \times (|X|^{|Z|})$

c) $(|X| \times |Y|)^{|Z|} = (|X|^{|Z|}) \times (|Y|^{|Z|})$

Formulate and prove some more of these rules yourself.

Now let us consider the cardinalities of power sets.

There is a bijective function from $\mathcal{P}(X)$ to $\{0,1\}^X$: with a subset $S \subseteq X$ we associate the function $\chi_S : X \to \{0,1\}$ (the *characteristic function* of S), defined by:

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

Conversely, every function $\chi : X \to \{0,1\}$ is of the form χ_S for a unique subset S of X, namely $S = \{x \in X \mid \chi(x) = 1\}$.
Therefore, $|\mathcal{P}(X)| = |\{0,1\}^X| = 2^{|X|}$.

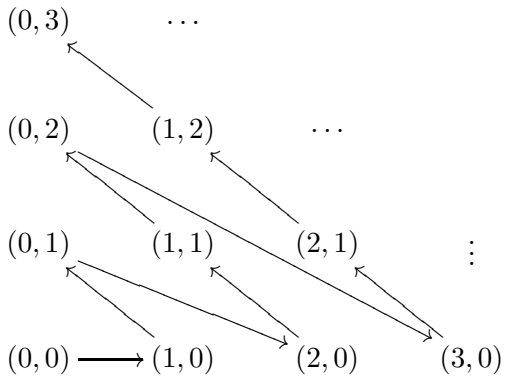
Proposition 1.1.4

i) $|\mathbb{N}| = |\mathbb{N}| + |\mathbb{N}|$

ii) $|\mathbb{N}| = |\mathbb{N}| \times |\mathbb{N}|$

iii) $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$

Proof. We indicate only a proof of ii), leaving the other statements as exercises. A bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is indicated in the following diagram:



The path obtained by following the arrows indicates the successive values of f. Thus $f(0) = (0, 0)$, $f(1) = (1, 0)$, etc. ∎

Exercise 7 Find a formula for the inverse of the function f indicated in the proof above. Give also proofs of the other statements of proposition 1.1.4.

Proposition 1.1.5 (Cantor) *For every set A we have the strict inequality*

$$|A| < 2^{|A|}$$

In other words, there is an injective function $A \to \mathcal{P}(A)$ but there is no bijective function between these sets.

Notice, that you already know Proposition 1.1.5 for finite sets; indeed, $n < 2^n$ is true for every natural number n.

Proof. It is easy to construct the required injective function $f : A \to \mathcal{P}(A)$. Just define $f(a) = \{a\}$ (the *singleton set* whose only element is a).

For the statement in the proposition, we shall show something stronger than required, namely that there cannot be any surjective function from A to $\mathcal{P}(A)$. The argument we use is known as the *Cantor diagonal argument*. Suppose that

$$s : A \to \mathcal{P}(A)$$

is surjective. We can construct a subset D of A by putting

$$D = \{a \in A \,|\, a \notin s(a)\}$$

Since s is assumed surjective, there must be some $a_0 \in A$ with $s(a_0) = D$. But now the simple question 'does a_0 belong to D?' brings us in trouble: we have

$$\begin{array}{lll} a_0 \in D & \text{iff} & a_0 \notin s(a_0) \quad \text{(by definition of } D\text{)} \\ & \text{iff} & a_0 \notin D \qquad \text{(since } D = s(a_0)\text{)} \end{array}$$

Thus, our assumption that such a surjective s exists, leads to a contradiction. ∎

Example. This example illustrates the proof of 1.1.5 and explains the term 'diagonal argument'. In order to prove that $|\mathbb{N}| < 2^{|\mathbb{N}|}$, suppose for a contradiction that the set $\{0,1\}^{\mathbb{N}}$ of infinite sequences of 0-s and 1-s is in bijective correspondence with $\mathbb{N}$. Then we can list this set as $a_0, a_1, \ldots$, where a_i is the sequence $a_{i0}, a_{i1}, \ldots$. Now consider:

$$\begin{array}{cccc} a_{00} & a_{01} & a_{02} & \cdots \\ a_{10} & a_{11} & a_{12} & \cdots \\ a_{20} & a_{21} & a_{22} & \cdots \\ \vdots & \vdots & \vdots & \end{array}$$

Clearly, the sequence

$$(1 - a_{00}), (1 - a_{11}), (1 - a_{22}), \ldots$$

does not appear in the list, contradicting the assumption that we were listing *all* 01-sequences. You should convince yourself, that this pictorial argument is essentially the same as the more general one of the proof of 1.1.5.

Proposition 1.1.5 has an important consequence: there are infinitely many infinite cardinal numbers. In fact, if we write $|\mathbb{N}| = \omega$ as is customary, we have

$$\omega < 2^{\omega} < 2^{(2^{\omega})} < \cdots$$

Let us try to determine the position of some familiar sets from analysis from the point of view of their cardinal numbers. We have already seen that the cardinal numbers of $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{Z}$ are the same (Proposition 1.1.4). These are so-called *countable sets*. We make the following definition:

Definition 1.1.6 A set X is called *countable* if X is empty or there is a surjective function $\mathbb{N} \to X$.

So, if a non-empty set X is countable, one can 'enumerate' all its elements as

$$X = \{x_0, x_1, x_2, \ldots\}$$

(but repetitions may occur).

Exercise 8 i) Show that if $f : \mathbb{N} \to X$ is surjective, there is a function $g : X \to \mathbb{N}$ such that $f(g(x)) = x$ for all $x \in X$. How do you define $g(x)$? Conclude that $|X| \leq |\mathbb{N}|$.

ii) Show that if X is countable then X is finite or $|X| = \omega$.

iii) Show that if X and Y are countable, so are $X \times Y$ and $X + Y$.

iv) Show that every subset of a countable set is countable.

An example of an *un*countable set is $\{0, 1\}^{\mathbb{N}}$, as follows from proposition 1.1.5.

What about the real numbers? There are several ways to determine the cardinality of $\mathbb{R}$. Our approach uses the so-called *Cantor set*, a subset C of $\mathbb{R}$ that was defined by Cantor in order to prove that $\mathbb{R}$ is not countable. However, the set C has a lot of independent interest and is also often used in topology. It is constructed as the intersection

$$C = \bigcap_{n \in \mathbb{N}} C_n$$

of an infinite sequence of smaller and smaller subsets of $\mathbb{R}$,

$$\mathbb{R} \supset C_0 \supset C_1 \supset C_2 \supset \cdots$$

Each C_i is a union of closed intervals. C_0 is the interval $[0, 1]$, and C_{n+1} is obtained from C_n by "cutting out the middle third" of each of the intervals which make up C_n:

$C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$

$C_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$

etc.

Thus a point p of C is uniquely determined by specifying for each n the interval of C_n to which p belongs. We can code this specification as a sequence of 0's and 1's where 0 means "left" and 1 means "right" (for each subinterval of C_n, there are exactly two subintervals of C_{n+1} contained in it). For example,

$$p = 010\cdots$$

is the point which lies in the left part $[0, \frac{1}{3}]$ of C_1, then in the right part $[\frac{2}{9}, \frac{1}{3}]$ of the two intervals of C_2 contained in $[0, \frac{1}{3}]$, then in the left part $[\frac{6}{27}, \frac{7}{27}]$ at the next stage, etcetera. Since the length of the intervals tends to zero, the sequence p defines a unique element of C. In this way, we obtain a bijective function

$$\varphi : \{0,1\}^{\mathbb{N}} \to C$$

Thus,

$$|C| = 2^{\omega}$$

Although C is just a subset of $\mathbb{R}$, the two sets are equally large in some sense:

Proposition 1.1.7 $|C| = |\mathbb{R}|$.

Proof. By 1.1.1, it suffices to prove that $|C| \leq |\mathbb{R}|$ and $|\mathbb{R}| \leq |C|$. Since C is a subset of $\mathbb{R}$ we obviously have

$$|C| \leq |\mathbb{R}|$$

There are many ways to prove the converse inequality. For example, each real number x is determined by the set of rational numbers which are $< x$. This defines an injective function

$$\psi : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$$

Since $|\mathbb{Q}| = |\mathbb{N}|$ hence $|\mathcal{P}(\mathbb{Q})| = 2^{\omega}$, we see that

$$|\mathbb{R}| \leq 2^{\omega}$$

Since $|C| = 2^{\omega}$, we are done. ∎

Exercise 9 Show that $2^{\omega} \times 2^{\omega} = 2^{\omega}$. Conclude that the field of complex numbers has the same cardinality as $\mathbb{R}$.

Exercise 10 Prove that for a subset A of $\mathbb{R}$, if $|A| = \omega$ then $|\mathbb{R} - A| = 2^{\omega}$. Conclude that $C \sim P$, where P is the set of irrational numbers.

Hint: use that $\mathbb{R} \sim \{0,1\}^{\mathbb{N}}$

Exercise 11 Prove that $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$.

Exercise 12 Let Cont denote the set of continuous functions $\mathbb{R} \to \mathbb{R}$.

a) Show that the function Cont $\to \mathbb{R}^{\mathbb{Q}}$, which sends a continuous function $f : \mathbb{R} \to \mathbb{R}$ to its restriction to $\mathbb{Q}$, is injective;

b) Prove that $|\text{Cont}| = |\mathbb{R}|$.

1.1.1 The Continuum Hypothesis

Suppose A is a subset of $\mathbb{R}$ such that $\mathbb{N} \subseteq A \subseteq \mathbb{R}$. We know then, that

$$\omega \leq |A| \leq 2^{\omega} = |\mathbb{R}|$$

and at least one of the inequalities must be strict because $\omega < 2^{\omega}$. We may ask ourselves: can it happen that *both* inequalities are strict? Is there a subset A of $\mathbb{R}$ such that

$$\omega < |A| < 2^{\omega}$$

holds?

This problem was raised by Cantor. Unable to find such a set, he formulated the so-called *Continuum Hypothesis*, which states that every subset of $\mathbb{R}$ which contains $\mathbb{N}$, is either countable or has cardinality 2^{ω}.

It cannot be decided on the basis of the axioms of Set Theory (see Chapter 4) whether the Continuum Hypothesis (CH) is true or false. Two famous results of Logic show that, on the one hand, CH does not contradict these axioms (Gödel, 1940;[11]), and on the other, that its negation doesn't either (Cohen, 1963;[2]). This means: one cannot derive a contradiction by logical reasoning on the basis of CH and the axioms of Set Theory, but it is also impossible to prove CH from these axioms.

Kurt Gödel was already famous for his "Incompleteness Theorems" when he proved the "Consistency of the Continuum Hypothesis". Paul Cohen's result, usually referred to as "Independence of the Continuum Hypothesis", solved a problem posed by Hilbert in 1900, and won him the Fields Medal in 1966. The Fields Medal is, in Mathematics, what the Nobel Prize is for Physics and other sciences. Cohen's is the only Fields Medal ever awarded for work in Logic.

1.2 The Axiom of Choice

An axiom in mathematics is a statement or a principle of reasoning that is simply assumed, because it is so basic that it cannot be proved. An

example of such an axiom is the principle of *mathematical induction* for natural numbers (see also the statements just before Proposition 1.3.4).

Of course, in general it is far from easy to see that a principle 'cannot be proved': for over 2000 years, mathematicians have tried to prove that Euclid's controversial "Parallel postulate" could be proved from the other axioms in geometry, until it was established beyond doubt in the 19th century that this axiom does not follow from the other 4 axioms of Euclid.

The Axiom of Choice is a bit peculiar among axioms of mathematics, because it asserts the *existence* of a function, without telling you what it is. It takes a while to get used to the axiom, and it has remained somewhat controversial ever since its formulation by Zermelo in 1904. Nevertheless, modern mathematics is unthinkable without it, and almost all mathematicians accept it as true. Moreover, the Axiom of Choice has been shown not to contradict the other axioms of Set Theory (this is another famous result of Gödel, also in [11]): we will see these axioms in Chapter 4 of these notes. Eventually, it was again Paul Cohen who showed that the Axiom of Choice does not follow from the other axioms of set theory ([3]).

Informally, the Axiom of Choice states that given a collection of non-empty sets, there is a way to choose an element from each set in the collection. Here is a more precise formulation, which looks simpler.

Definition 1.2.1 The *Axiom of Choice* (AC) is the assertion that for every surjective function $f : X \to Y$ there exists a "section", that is a function $s : Y \to X$ such that $f(s(y)) = y$ for each $y \in Y$.

In order to "define" such a section as in definition 1.2.1, one has to "choose", for each $y \in Y$, an $x \in X$ such that $f(x) = y$. In general, the Axiom of Choice is needed when:

- there is more than one x such that $f(x) = y$ (see Exercise 14), and
- Y is infinite (see Exercise 15)

But even in these circumstances the Axiom of Choice is not *always* necessary; for example, if, in definition 1.2.1, $X = \mathbb{N}$, we can simply define $s(y)$ as the *least* n such that $f(n) = y$ (this is the solution of Exercise 8 i)).

An example of a genuine application of the Axiom of Choice is given by the following simple proposition, which you may have thought was self-evident.

Proposition 1.2.2 *If X is an infinite set, there is an injective function $\mathbb{N} \to X$, hence $\omega \leq |X|$.*

Proof. Intuitively, one can 'choose' for each $n \in \mathbb{N}$ an element $g(n) \in X$ such that $g(n)$ is different from all elements chosen before. This reasoning is perfectly correct, but below we present a detailed proof, just in order to make clear exactly how the Axiom of Choice is used.

First we remark that if $(x_1, \ldots, x_n)$ is a finite sequence of elements of X such that $x_i \neq x_j$ whenever $i \neq j$, there is an element $x_{n+1} \in X$ such that $x_i \neq x_{n+1}$ for all $i \leq n$; for if not, we would have $|X| = n$, and X would be finite.

Now let A be the set of all such finite sequences $(x_1, \ldots, x_n)$ with at least one element; and let B be the union $A \cup \{*\}$, where $*$ is any element not in A. Define a function $f : A \to B$ by:

$$\begin{aligned} f((x_1)) &= * \\ f((x_1, \ldots, x_{n+1})) &= (x_1, \ldots, x_n) \end{aligned}$$

Then by our remark, we see that $f : A \to B$ is surjective, and so the Axiom of Choice says there is a section $s : B \to A$.

This section s allows us to define a function $g : \mathbb{N} \to X$ by induction: let $g(0)$ be the element of X such that $s(*) = (g(0))$; if $g(0), \ldots, g(n)$ have been defined, let $g(n+1)$ be the element of X such that

$$s((g(0), \ldots, g(n))) = (g(0), \ldots, g(n+1))$$

Convince yourself that the function g thus defined, is indeed injective. ∎

Exercise 13 Use proposition 1.2.2 to show that if A is infinite and B is finite,

$$|A| + |B| = |A|$$

Exercise 14 If A is nonempty and $s : A \to B$ is injective, there is a surjective function $f : B \to A$ such that $f(s(a)) = a$ for all $a \in A$. Prove this, and show that the proof does *not* require the axiom of choice.

Exercise 15 Prove the Axiom of Choice (every surjective $f : X \to Y$ has a section) in the following two special cases:

a) Y is finite [Hint: induction on the cardinality of Y];

b) X is countable.

The axiom of choice is essential for deriving basic properties of cardinalities, such as given by the following proposition.

Proposition 1.2.3 *Let I be a countable set and suppose for each $i \in I$, a countable set X_i is given. Then the union*

$$\bigcup_{i \in I} X_i$$

is again a countable set.

Proof. If $I' \subseteq I$ is the subset $\{i \in I \,|\, X_i \neq \emptyset\}$ then $\bigcup_{i \in I} X_i = \bigcup_{i \in I'} X_i$, and I' is countable by Exercise 8 iv). So we may as well assume that X_i is nonempty for each $i \in I$.

If I is empty, the union is empty, hence countable. So let I be nonempty.

Let $g : \mathbb{N} \to I$ be a surjective function; such g exists because I is countable.

Let J be the set of all pairs (f, i) such that $f : \mathbb{N} \to X_i$ is surjective. The function $J \to I$, given by $(f, i) \mapsto i$, is surjective, because each X_i is nonempty and countable. By AC, it has a section s. Let $f_i : \mathbb{N} \to X_i$ be such that $s(i) = (f_i, i)$.

Now consider the function

$$h : \mathbb{N} \times \mathbb{N} \to \bigcup_{i \in I} X_i$$

defined by: $h(n, m) = f_{g(n)}(m)$. Convince yourself that h is surjective. Combining with a surjective function $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, we see that $\bigcup_{i \in I} X_i$ is indeed countable, as required. ∎

No doubt you have seen theorem 1.2.3 before, but it may not be clear to you why the Axiom of Choice is *necessary* for its proof. The reason is, that in order to do the construction in the proof we have to *choose* surjective functions $\mathbb{N} \to X_i$ for all (possibly infinitely many) i. Indeed, without the Axiom of Choice we cannot prove that $\mathbb{R}$ (which is always an uncountable set, as we have seen) is not a union of countably many countable sets ([25])!

Exercise 16 Prove that the set

$$\{x \in \mathbb{R} \,|\, \sin(x) \in \mathbb{Q}\}$$

is countable.

Another simple application of the axiom of choice is in the following theorem of analysis: if A is a bounded, infinite subset of $\mathbb{R}$, then there is an element

$a \in A$ such that $A - \{a\}$ contains a sequence which converges to a (Bolzano-Weierstrass).

Later we shall see that, as a consequence of AC, we have for any two sets X and Y: either $|X| \leq |Y|$ or $|Y| \leq |X|$.

There are many statements which are equivalent to the Axiom of Choice. We shall now present one, which is closer to our intuitive description of AC at the beginning of this section. We need the following definitions:

Definition 1.2.4 Let I be a set and let X_i be a set for each $i \in I$.

a) The *disjoint sum* $\coprod_{i\in I} X_i$ is the set of all pairs (i, x) with $i \in I$ and $x \in X_i$.

b) The *product* $\prod_{i\in I} X_i$ is the set of functions $f : I \to \bigcup_{i\in I} X_i$ such that $f(i) \in X_i$ for each $i \in I$.

Proposition 1.2.5 *The Axiom of Choice is equivalent to the statement:*

(Π) *For every family of sets $\{X_i \mid i \in I\}$ such that X_i is nonempty for each $i \in I$, the set*

$$\prod_{i\in I} X_i$$

is nonempty.

Proof. First we show that AC implies the statement (Π). So let X_i be nonempty for each i. Then the function $\coprod_{i\in I} X_i \to I$ which takes (i, x) to i, is surjective and has therefore a section s by AC.
Let

$$t : I \to \bigcup_{i\in I} X_i$$

be such that $s(i) = (i, t(i))$; then t is an element of $\prod_{i\in I} X_i$, as is easy to check.

Conversely, assume (Π) and let $f : X \to Y$ be a surjective function. Then we have, for each $y \in Y$, the nonempty set $X_y = \{x \in X \mid f(x) = y\}$. By (Π), the set $\prod_{y\in Y} X_y$ is nonempty. But any element of this set is a section of f. ∎

Example. This example is meant to give some intuition about the use or non-use of AC. Consider the sets $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{Q}$. We have the equivalence relations $\sim_{\mathbb{Z}}$ and $\sim_{\mathbb{Q}}$ on $\mathbb{R}$:

$$\begin{aligned} x \sim_{\mathbb{Z}} y \quad &\text{iff} \quad y - x \in \mathbb{Z} \\ x \sim_{\mathbb{Q}} y \quad &\text{iff} \quad y - x \in \mathbb{Q} \end{aligned}$$

and write $\mathbb{R}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Q}$ respectively for the sets of equivalence classes. There are evident surjective functions

$$\varphi : \mathbb{R} \to \mathbb{R}/\mathbb{Z} \qquad \psi : \mathbb{R} \to \mathbb{R}/\mathbb{Q}$$

For φ, we can explicitly describe a section $\sigma : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$: for every equivalence class ξ, the intersection of ξ with the half-open interval $[0, 1)$ contains exactly one point, which we take as $\sigma(\xi)$.

We can not do something similar for ψ. The Axiom of Choice says that there must be a section, but it cannot be described explicitly.

1.2.1 Partially Ordered Sets and Zorn's Lemma

Zorn's Lemma (formulated independently by Kazimierz Kuratowski and Max Zorn) is a principle which is equivalent to the Axiom of Choice, but formulated quite differently; in many cases, it is easier to apply than AC.

The formulation uses the notions of a *chain in a partially ordered set*, which we shall define first.

Definition 1.2.6 A *partially ordered set* or *poset* is a set P together with a relation $\leq$ between elements of P, such that the following conditions are satisfied:

i) For every $p \in P$, $p \leq p$ holds (one says that the relation $\leq$ is "reflexive");

ii) for every $p, q, r \in P$, if $p \leq q$ and $q \leq r$ hold, then $p \leq r$ holds (the relation $\leq$ is said to be "transitive"), and

iii) for every $p, q \in P$, if both $p \leq q$ and $q \leq p$ hold then $p = q$ (the relation $\leq$ is "antisymmetric").

We shall usually denote a poset as $(P, \leq)$, and the relation $\leq$ is pronounced as "less than or equal to". The converse relation $\geq$, "greater than or equal to", is defined by $x \geq y$ if and only if $y \leq x$.

Examples.

a) The most important example of a poset is the powerset $\mathcal{P}(A)$ of a set A: the relation $p \leq q$ holds for subsets p and q of A, if and only if p is a subset of q ($p \subseteq q$).

b) If $(P, \leq)$ is a poset and $S \subseteq P$ then clearly the restriction of the relation $\leq$ to elements of S gives a poset $(S, \leq)$.

c) Combining a) and b), we see that any collection $\mathcal{C}$ of subsets of a set X (i.e., $\mathcal{C} \subseteq \mathcal{P}(X)$) is naturally a poset when ordered by inclusion.

d) The usual order relations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ make these sets into posets. These posets have the additional property that every two elements are comparable; that is, for each x and y, we have either $x \leq y$ or $y \leq x$. Posets in which every two elements are comparable are called *total* or *linear* orders. Note, that the poset $\mathcal{P}(X)$ is not a total order (at least if X has more than one element).

e) Note, that if $(P, \leq)$ is a poset, then $(P, \geq)$ is a poset too.

Definition 1.2.7 Let $(P, \leq)$ be a poset.

i) A subset C of P is called a *chain* if C with the restricted order, is a total order. In other words, if either $p \leq q$ or $q \leq p$ holds, for any two elements p, q of C.

ii) If S is any subset of P, an element p of P is called an *upper bound* for S if for each $s \in S$ we have $s \leq p$ (p itself doesn't need to be a member of S).

iii) An element $p \in P$ is called *maximal* if no element is strictly greater: whenever $p \leq q$ we must have $p = q$.

Example. Let A be a fixed set with more than one element, and $P = \{S \subseteq A \,|\, S \neq A\}$, ordered by inclusion. This poset P has many maximal elements, namely the sets $A - \{a\}$ for $a \in A$. On the other hand, P does not have a greatest element.

If $C \subseteq P$ is a chain and the union

$$\bigcup C = \{x \in A \,|\, \exists S \in C \, x \in S\}$$

is not equal to A, then this set is an upper bound for C. If $\bigcup C = A$, the chain C does not have an upper bound in P.

Exercise 17 Suppose X and Y are sets. Let P be the set of all pairs (A, f) where A is a subset of X and f is a function $A \to Y$. Then P is a poset with the following relation: $(A, f) \leq (B, g)$ iff $A \subseteq B$ and f is the restriction of g to A.
Show that if $C = \{(A_i, f_i) \,|\, i \in I\}$ is a chain in P, there is a unique function $f : \bigcup_{i \in I} A_i \to Y$ such that for each i, f_i is the restriction of f to A_i. Conclude that every chain in P has an upper bound in P.

Definition 1.2.8 *Zorn's Lemma* is the following assertion: if $(P, \leq)$ is a poset with the property that every chain in P has an upper bound in P, then P has a maximal element.

Note that if P satisfies the hypothesis of Zorn's Lemma, then P is nonempty. This is so because the empty subset of P is always a chain. However, checking that every chain has an upper bound in P usually involves checking this for the empty chain separately; that is, checking that P is nonempty (see the Example below).

Zorn's Lemma isn't a lemma, but a "principle" of a status similar to that of the Axiom of Choice (cf. the remarks at the beginning of the section on AC).

Example: Maximal ideals in rings. Let R be a commutative ring with 1. Let P be the poset of all proper ideals of R (that is, ideals $I \neq R$), ordered by inclusion. If C is a nonempty chain of ideals, its union $\bigcup C$ is an ideal too, and $\bigcup C$ is proper, since $1 \notin \bigcup C$ because C consists of proper ideals. Moreover, P is nonempty since $\{0\}$ is a proper ideal (why?). So, every chain in P has an upper bound. Hence, by Zorn's Lemma, P has a maximal element, which is a maximal ideal in R.

Example: Bases for vector spaces. Let V be a vector space over $\mathbb{R}$ (or, in fact, any other field), for example the set of continuous functions from $[0, 1]$ into $\mathbb{R}$. Then V has a *basis*, that is a subset $B \subset V$ with the property that every $v \in V$ can be written as a finite sum

$$v = k_1 b_1 + \cdots + k_n b_n$$

with $k_1, \ldots, k_n \in \mathbb{R}$ and $b_1, \ldots, b_n \in B$, and moreover this finite sum is *unique*. In order to prove this, let P be the poset of those subsets $B \subset V$ which are linearly independent (no element of B can be written as a linear combination of other elements of B), ordered by inclusion. If B is a maximal element of P, B must be a basis (check!).

Our next example uses Zorn's Lemma to prove the Axiom of Choice.

Proposition 1.2.9 *Zorn's Lemma implies the Axiom of Choice.*

As we have already remarked, Zorn's Lemma is equivalent to AC. Here we prove the most important implication. For the other direction, see section 1.4.

Proof. We assume that Zorn's Lemma is true.

Suppose given a surjective function $f : X \to Y$. A *partial section* of f is a pair (A, u) where A is a subset of Y and $u : A \to X$ a function such that $f(u(y)) = y$ for each $y \in A$. Given two such partial sections (A, u) and (B, v), put $(A, u) \leq (B, v)$ iff $A \subseteq B$ and u is the restriction of v to A. Let P be the set of partial sections (A, u) of f; then with the relation $\leq$, P is a poset, as is easy to see.

P is nonempty; this is left to you. Moreover, if $C = \{(A_i, u_i) \mid i \in I\}$ is a chain in P, C has an upper bound; this is similar to Exercise 17. So the poset $(P, \leq)$ satisfies the hypotheses of Zorn's Lemma, and has therefore a maximal element (A, s).

We claim that $A = Y$, and therefore that s is a section for f. Suppose that $y \notin A$. Then since f is surjective, there is an element $x \in X$ such that $f(x) = y$. If we define the function $s' : A \cup \{y\} \to X$ by

$$s'(w) = \begin{cases} s(w) & \text{if } w \in A \\ x & \text{if } w = y \end{cases}$$

then we see that $(A \cup \{y\}, s')$ is a partial section of f which is strictly greater than (A, s); this contradicts the fact that (A, s) is *maximal*. It follows that $A = Y$ and we have found a section for f. ∎

It is another important consequence of Zorn's Lemma that any two cardinal numbers $|X|$ and $|Y|$ can be compared: we have either $|X| \leq |Y|$ or $|Y| \leq |X|$. In other words, for every two sets X and Y, there is an injective function $X \to Y$, or there is an injective function $Y \to X$ (or both, of course).

Proposition 1.2.10 *Zorn's Lemma implies the following statement: for any two sets X and Y,*

$$|X| \leq |Y| \quad \text{or} \quad |Y| \leq |X|$$

holds.

The statement in the proposition is sometimes called the "Law of Trichotomy" (because one can equivalently put it as: one of the three possibilities $|X| < |Y|$, $|X| = |Y|$ or $|Y| < |X|$ is true). We shall refer to it as the *Principle of Cardinal Comparability* (PCC).
Conversely, the Principle of Cardinal Comparability can be shown to be equivalent to Zorn's Lemma (or AC). For this, see the Appendix (section 1.4).

Proof. Let X and Y be sets.

We consider a poset P of triples (U, f, V), where $U \subseteq X$, $V \subseteq Y$ and $f : U \to V$ is a bijective function. This is ordered similarly as in the proof of 1.2.9: $(U, f, V) \leq (U', f', V')$ iff $U \subseteq U'$ and f is the restriction of f' to U (note, that this implies that $V \subseteq V'$).

P is nonempty, since we have $\emptyset$ as subset of both X and Y, and the "empty function" is bijective.

If $\{(U_i, f_i, V_i) \mid i \in I\}$ is a chain in P, there is a well-defined function $f : \bigcup_{i\in I} U_i \to \bigcup_{i\in I} V_i$ which is a bijection. Therefore, every chain in P has an upper bound, and by Zorn's Lemma P has a maximal element (U, f, V). If $U \neq X$ *and* $V \neq Y$, say $x \in X - U$ and $y \in Y - V$, we can obviously define a bijection between $U \cup \{x\}$ and $V \cup \{y\}$ which extends f, and this contradicts the maximality of (U, f, V). Hence, either $U = X$, in which case f is an injective function from X into Y, or $V = Y$, in which case the inverse of f is an injective function $Y \to X$. ∎

Exercise 18 Prove the following variation: if X and Y are nonempty sets, then there is either a surjective function $X \to Y$ or a surjective function $Y \to X$. You can do this either by using Zorn's Lemma (and mimicking the proof of Proposition 1.2.10), or by applying that proposition directly.

It follows from Proposition 1.2.10, that we can define the maximum of two cardinal numbers: $\max(|X|, |Y|) = |X|$ if $|Y| \leq |X|$, and it is $|Y|$ otherwise.

This allows us to state the following properties of the arithmetic of cardinal numbers, which generalize Proposition 1.1.4. The proof makes essential use of Zorn's Lemma.

Proposition 1.2.11 *Let A and B be infinite sets. Then the following hold:*

i) $|A| + |A| = |A|$

ii) $|A| + |B| = \max(|A|, |B|)$

iii) $|A| \times |A| = |A|$

iv) $|A|^{|A|} = 2^{|A|}$

Proof. For i), we have to show that there is a bijective function: $A+A \to A$. To this end, we consider the poset of pairs (X, f) where X is a subset of A and $f : X + X \to X$ is bijective. This is ordered by: $(X, f) \leq (Y, g)$ if $X \subseteq Y$ and f is the restriction of g to $X + X$.

If $\{(X_i, f_i) \mid i \in I\}$ is a chain in this poset, then there is a well-defined bijective function $f : X + X \to X$, where $X = \bigcup_{i\in I} X_i$ and f is such that f extends each f_i.

Therefore, the poset under consideration satisfies the hypothesis of Zorn's Lemma (check this!) and has therefore a maximal element (X, f). We claim that for this (X, f), $A - X$ must be finite.

To prove this claim, we use Proposition 1.2.2: if $A-X$ is infinite, there is an injective function $\mathbb{N} \to A - X$. Let $N \subseteq A$ be the image of this function; then we have a bijective function $g : N + N \to N$ (by 1.1.4), and since N and X are disjoint, we can combine f and g to obtain a bijective function

$$(X \cup N) + (X \cup N) \to X \cup N$$

which extends f; but this contradicts the maximality of the pair (X, f) in our poset. Therefore, $A - X$ is finite and we have proved the claim.

Now $A \sim X + (A - X)$, so by Exercise 13, there is a bijective function $\varphi : A \to X$. Combining f and φ we obtain a bijection between $A + A$ and A:

$$A + A \overset{\varphi+\varphi}{\to} X + X \overset{f}{\to} X \overset{\psi}{\to} A$$

where ψ is the inverse of φ.

For ii): suppose that $|A| \leq |B|$. We have to show that $|A|+|B| = |B|$. Since obviously $|B| \leq |A| + |B|$ and $|A| + |B| \leq |B| + |B|$ by hypothesis, using i) we have

$$|B| \leq |A| + |B| \leq |B| + |B| \leq |B|$$

so $|B| = |A| + |B|$ as required. Note that this proof does not require that A is infinite.

For iii), we form again a poset P of pairs (X, f) with $X \subseteq A$, but now with X infinite and $f : X \times X \to X$ bijective. By Propositions 1.2.2 and 1.1.4ii), the poset P is nonempty. We order this 'by extension' as in the proof of i) (note that $X \subseteq Y$ implies $X \times X \subseteq Y \times Y$). In the same way as in i) we see that every chain in P has an upper bound (check for yourself that if $\{X_i \mid i \in I\}$ is a chain of sets under the inclusion ordering, and $X = \bigcup_{i\in I} X_i$, then $X \times X = \bigcup_{i\in I}(X_i \times X_i)$).

By Zorn's Lemma, P has a maximal element (M, f). If $|M| = |A|$ we use the bijection between M and A, together with f, to obtain a bijection between $A \times A$ and A and we are done.

So suppose $|M| < |A|$. Now M is infinite by definition of P, and also $A - M$ is infinite: if $A - M$ were finite then we would have $A \sim M + (A - M) \sim M$, contradicting our assumption. Therefore, we can apply part ii), to conclude that $A \sim A - M$.

Let $g : A \to A - M$ be bijective. If M' is the image of M under g, then M and M' are disjoint and g restricts to a bijection between M and M'.

Combining g and f, we also find a bijection $f' : M' \times M' \to M'$. Moreover, since M and M' are disjoint, we have $M \cup M' \sim M + M'$, and we can find a bijective function

$$F : (M \cup M') \times (M \cup M') \to M \cup M'$$

which extends f, as follows: we have

$$(M + M') \times (M + M') \sim (M \times M) + (M \times M') + (M' \times M) + (M' \times M')$$

We have $M \times M \sim M$ via f, and we have $(M \times M') + (M' \times M) + (M' \times M') \sim M'$ by using f, g, f' and part i) of the proposition twice.

Finally, for iv) we first notice that since A is infinite, $2 < |A|$ so $2^{|A|} \leq |A|^{|A|}$; for the converse inequality, we know from Proposition 1.1.5 that $|A| < 2^{|A|}$, so $|A|^{|A|} \leq (2^{|A|})^{|A|}$. Using iii) of the proposition, we see that $(2^{|A|})^{|A|} = 2^{|A| \times |A|} = 2^{|A|}$, and we are done. ∎

Exercise 19 a) Let A and B be nonempty sets, at least one of them infinite. Show that

$$|A| \times |B| = \max(|A|, |B|)$$

b) Show that if A is infinite, then there is a bijection between A and $\mathbb{N} \times A$.

c) Let A be an infinite set. Denote by A^* the set of all finite sequences of elements of A; that is,

$$A^* = \bigcup_{n=0}^{\infty} A^n$$

(here A^0 has just one element, the *empty sequence* $(\cdot)$).

Show, that $|A^*| = |A|$.

d) Let A be infinite; show that $|A| = |\mathcal{P}_{\text{fin}}(A)|$ (where $\mathcal{P}_{\text{fin}}(A)$ is the set of finite subsets of A).

Let us come back to the example of vector spaces and show that if both B and B' are bases of a vector space V, then $|B| = |B'|$. This cannot be proved without the Axiom of Choice!

We make use of the fact that a basis of a vector space V is a subset B which generates V (every element of V can be written as a finite linear

combination of elements of B) but is *minimal* with this property: no proper subset of B generates V.

So, let B and B' be bases of V. We assume that you know the result in the case that B and B' are finite. So suppose B is infinite.

For every $b \in B'$ there is a finite subset B_b of B such that b can be written as a linear combination of elements of B_b. Then $\bigcup_{b\in B'} B_b$ is a subset of B which generates V, so by minimality of B,

$$B = \bigcup_{b\in B'} B_b$$

It follows that also B' is infinite (otherwise, B would be a finite union of finite sets). Since every B_b is finite, there are injective functions $B_b \to \mathbb{N}$ and we see that

$$|B| \leq |B'| \times \omega = |B'|$$

By symmetry, $|B| = |B'|$, as required.

We close this section with some miscellaneous exercises involving Zorn's Lemma and cardinalities.

Exercise 20 Let X be an infinite set. Prove that there is a bijection $f : X \to X$ with the property that for every $x \in X$ and all $n > 0$, $f^n(x) \neq x$ [Hint: consider $\mathbb{Z} \times X$, or use Zorn directly].

Exercise 21 Prove that there is a linear order on any set.

Exercise 22 Prove that there is a dense linear order on any infinite set: that is, a linear order such that whenever $x < y$, there is a z such that $x < z < y$ [Hint: use the previous exercise to find a linear order on X; then consider $\mathbb{Q} \times X$]

Exercise 23 This exercise is one of the first applications, given by Cantor ([1]), of his theory of cardinalities to number theory.

A real number r is called *algebraic* if there is a non-zero polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

with $a_1, \ldots, a_n \in \mathbb{Q}$ and $f(r) = 0$. A number which is not algebraic, is called *transcendental*. Write A for the set of algebraic real numbers, and T for the set of transcendental real numbers.

Prove that $|A| = \omega$ and $|T| = |\mathbb{R}|$.
This was Cantor's proof that transcendental numbers exist, and that there are very many of them.

Exercise 24 In this exercise we consider $\mathbb{R}$ as a group under addition.

a) Prove, using Zorn's Lemma, that there is a subgroup G of $\mathbb{R}$ which is maximal w.r.t. the property that $1 \notin G$.

b) Suppose G is as in a). Show that there is a unique prime number p such that $p \in G$.

c) Let p be as in b). Prove that for every $x \in \mathbb{R}$ there is an $n \geq 0$ such that $p^n x \in G$.

Exercise 25 For a subset A of $\mathbb{R}$ such that $0 \notin A$, we define:

$$\begin{array}{rcl} \sqrt{\mathbb{Q}} & = & \{x \in \mathbb{R} \,|\, x^2 \in \mathbb{Q}\} \\ \mathbb{Q}/A & = & \{\frac{q}{a} \,|\, q \in \mathbb{Q} - \{0\}, a \in A\} \end{array}$$

Prove, that there is a subset $A \subset \mathbb{R} - \{0\}$ such that $\mathbb{R}$ can be written as a *disjoint* union

$$A \cup \sqrt{\mathbb{Q}} \cup \mathbb{Q}/A$$

[Hint: apply Zorn's Lemma to the poset of those $A \subset \mathbb{R}$ for which the following holds: for all $x, y \in A$, $xy \notin \mathbb{Q}$]

1.3 Well-Ordered Sets

Definition 1.3.1 A partial order $(L, \leq)$ is a *well-order*, or a *well-ordered set*, if every nonempty subset S of L has a least element w.r.t. the order $\leq$: there is an element $s_0 \in S$ such that for each $s \in S$, $s_0 \leq s$.
We shall also sometimes say, that the relation $\leq$ *well-orders* L.

Recall that a partial order $(L, \leq)$ is linear or total if for all $x, y \in L$ we have $x \leq y$ or $y \leq x$.

Exercise 26 Prove that every well-order is linear.

Let us see some examples of well-orders.

1) The set $\mathbb{N}$ is a well-ordered set. That this is so, is exactly the principle of *induction* for natural numbers. We shall see later, that conversely for every well-order there is a similar 'induction principle' (Proposition 1.3.4).

2) $\mathbb{Z}$ is not a well-ordered set (with the usual ordering): $\mathbb{Z}$ itself has no least element. In the same way, $\mathbb{Q}$ and $\mathbb{R}$ are not well-ordered in the usual ordering.

3) Define a new ordering on $\mathbb{N}$ by putting: $n \leq m$ if either n and m are both odd and n is smaller than m in the usual ordering, or n and m are both even and n is smaller than m in the usual ordering, or n is even and m is odd. This looks like:

$$0 \leq 2 \leq 4 \leq \cdots \leq 1 \leq 3 \leq 5 \leq \cdots$$

and $\leq$ is a well-ordering. In a similar way, we can have:

$$0 \leq 3 \leq 6 \leq \cdots \leq 1 \leq 4 \leq 7 \leq \cdots \leq 2 \leq 5 \leq 8 \leq \cdots$$

and so on.

4) Every finite linear order is a well-order.

5) The set $\{1 - \frac{1}{n} \,|\, n > 0\} \cup \{1\}$ is a well-ordered subset of $\mathbb{R}$.

The *Well-Ordering Theorem* (Zermelo, see section 1.4) says that for *every* set X there is a well-order on X.

Exercise 27 Prove:

a) If $(L, \leq)$ is a well-order, then so is every subset of L, with the restricted order.

b) If $(L, \leq_L)$ and $(M, \leq_M)$ are two well-ordered sets, we can define the *lexicographic order* on the product $L \times M$: for elements (x, y) and (x', y') of $L \times M$, put $(x, y) \leq (x', y')$ if either $y <_M y'$, or $y = y'$ and $x \leq_L x'$. Then $\leq$ well-orders $L \times M$.
The lexicographic order can be pictured as follows: view M as points on a line (since M is linearly ordered) and replace every point of M by a copy of L.

Generalize this construction to: if L is a well-order and for each $i \in L$ we are given a well-order M_i, then there is a well-order on the set $\coprod_{i \in L} M_i$.

c) This is a special case of the generalization in part b):

If $(L, \leq_L)$ and $(M, \leq_M)$ are two disjoint well-ordered sets, we can define an order on the union $L \cup M$ as follows: for $x, y \in L \cup M$ we put $x \leq y$ iff: either both x and y are elements of L, and $x \leq_L y$, or $x \in L$ and $y \in M$, or both x and y are elements of M and $x \leq_M y$. Then $\leq$ well-orders $L \cup M$.
This well-order on $L \cup M$, which we denote by $L + M$, looks like putting M "on top of" L.

The following criterion gives an equivalent way of defining well-orders.

Proposition 1.3.2 *A linear order $(L, \leq)$ is a well-order if and only if for every infinite decreasing sequence*

$$x_0 \geq x_1 \geq x_2 \geq \cdots$$

in L, there is an n such that for all $m > n$, $x_n = x_m$.

Exercise 28 Prove Proposition 1.3.2. In one direction, you need to use the Axiom of Choice, in a way similar to the proof of Proposition 1.2.2.

Exercise 29 Recall that if $(X, \leq)$ is a poset, then $(X, \geq)$ is one too.
Prove: if $(X, \leq)$ and $(X, \geq)$ are both well-orders, then X is finite.

We introduce some terminology for elements of a well-ordered set L. Clearly, the empty set is well-ordered; but since it has no elements, we don't have to say anything about it.

If L is nonempty, L (as nonempty subset of itself) has a least element, which we may as well call 0_L. If 0_L is the only element of L, we are done.

In general, if x is not the greatest element of L, the set $\{y \in L \,|\, x < y\}$ has a least element, which we call $x + 1$. So if L is infinite, L contains

$$\{0_L, 0_L + 1 = 1_L, 1_L + 1 = 2_L, 3_L, 4_L, \ldots\}$$

as a subset; let us call this the *finite part* of L. If this subset is not the whole of L, its complement has a least element ω_L, and we may have $\omega_L, \omega_L + 1, \ldots$. This process may continue indefinitely!

An element of L is called a *successor* element, if it is the smallest element in L strictly greater than some $x \in L$, i.e. if it is of the form $x+1$; otherwise, it is called a *limit* element. Note, that 0_L is a limit element, as is ω_L.

In a well-order (or more generally, in a poset), a *least upper bound* or l.u.b. of a subset S, is an upper bound x for S (see Definition 1.2.7) such that for every upper bound y for S we have $x \leq y$. Note, that least upper bounds need not always exist in a poset, but if they exist, they are unique. Note also, that x is a l.u.b. of the empty set if and only if x is the least element.

Proposition 1.3.3 *In a well-order $(L, \leq)$, every subset of L which has an upper bound in L, has a least upper bound. Moreover, an element x of L is a limit element, if and only if x is the least upper bound of the set*

$$\{y \in L \,|\, y < x\}$$

Proof. If S has an upper bound in L, the set of upper bounds (in L) of S is nonempty, so it has a least element.

Suppose x is the l.u.b. of $L_x = \{y \mid y < x\}$. Then if $x = z + 1$ we must have that z is the greatest element of L_x and therefore its least upper bound; but z and x are distinct, so we see that x is a limit element.

Conversely, suppose x is a limit element. Then for each $y < x$, x is not equal to $y + 1$, so $y + 1 < x$. It follows that no element smaller than x can be the l.u.b. of L_x; but x is an upper bound for L_x, so it is the l.u.b. ∎

We are now going to look at the principle of *induction* for well-ordered sets L. The well-known induction principle for natural numbers,

(I_0) If $S \subseteq \mathbb{N}$ has the properties that $0 \in S$ and for all $n \in \mathbb{N}$, $n \in S$ implies $n + 1 \in S$, then $S = \mathbb{N}$

has an equivalent formulation:

(I_1) If $S \subseteq \mathbb{N}$ has the property that for each $n \in \mathbb{N}$, $n \in S$ whenever $\forall m < n\,(m \in S)$, then $S = \mathbb{N}$

In a similar way, we have two equivalent induction principles for an arbitrary well-ordered set L.

Proposition 1.3.4 *Let $(L, \leq)$ be a well-ordered set, and $S \subseteq L$ an arbitrary subset.*

i) If for each $x \in L$, the statement $\forall y \in L\,(y < x \Rightarrow y \in S)$ implies $x \in S$, then $S = L$.

ii) If $0_L \in S$, S is closed under the successor function (mapping x to $x+1$) and for each nonzero limit element $l \in L$ we have $l \in S$ whenever $\{x \in L \mid x < l\} \subseteq S$, then $S = L$.

Proof. i) If $S \neq L$ then $L - S$ has a least element x. Then we must have $\forall y < x\,(y \in S)$ yet $x \notin S$ which contradicts the assumption of i).

ii) is left to you as exercise. ∎

Exercise 30 Prove Proposition 1.3.4ii).

Example. Let us prove, by induction on L, that for each $x \in L$ there is a unique limit element $l \leq x$ and a unique natural number n such that

$$x = l + n$$

($l + n$ is shorthand for: the n-th successor of l, so $l + 0 = l$, etc.)

Since the successor function is 1-1 where it is defined (check this!), it is easy to show that such a representation is unique. Suppose $l + n = l' + n'$. Then by induction on n we show that $l = l'$ and $n = n'$: if $n = 0$, we have $l = l' + n'$ whence $n' = 0$ because l is a limit; and if $n = k + 1$ then $l + n$ is a successor, so $n' = k' + 1$ for some k'. By injectivity of the successor, we have $l + k = l' + k'$ and by induction hypothesis it follows that $l = l'$ and $k = k'$, so $n = n'$.
For existence of the representation, we use induction on L: clearly, 0_L has the representation $0_L + 0$, for 0_L is a limit. If $x = l + n$ then $x + 1 = l + (n + 1)$, and if l is a limit, it has representation $l + 0$.

For natural numbers, one has, beside induction to prove properties of natural numbers, also the possibility of defining functions by *recursion*: a function f is defined on natural numbers by a scheme which defines $f(n+1)$ in terms of $f(n)$ or in terms of $\{f(k) \,|\, k \leq n\}$. An example is the well-known Fibonacci sequence: $f(0) = f(1) = 1$, and $f(n + 2) = f(n) + f(n + 1)$. Induction and recursion are really two sides of the same coin, so it is not surprising that we can also define functions on an arbitrary well-ordered set L by recursion. The idea is, that one defines $f(x)$ in terms of the (not necessarily finite) *set* $\{f(y) \,|\, y < x\}$. There are various formulations. We prove one in the proposition below, and give others as exercises.

Proposition 1.3.5 *Let $(L, \leq)$ be a well-order, and S a set. Suppose we are given a function $R : L \times \mathcal{P}(S) \to S$. Then there is a unique function $F : L \to S$ with the property that*

$$(*) \qquad F(l) = R(l, \{F(x) \,|\, x < l\})$$

for each $l \in L$.
The function F is said to be defined by recursion *from R.*

Proof. In this proof, let L_z denote the set $\{y \in L \,|\, y \leq z\}$, for $z \in L$.

First, let us see that if F is a function from L_z to S such that F satisfies condition $(*)$, then F is unique with this property; for if also $G : L_z \to S$ satisfies $(*)$ and $F \neq G$, there must be a *least* element $m \in L_z$ such that $F(m) \neq G(m)$; however in that case the sets $\{F(x) \,|\, x < m\}$ and $\{G(x) \,|\, x < m\}$ are equal so that by $(*)$, $F(m) = G(m)$ which contradicts our assumption on m.

Similarly, any $F : L \to S$ satisfying $(*)$ must be unique.

From this uniqueness it follows that if $z_1 < z_2$ in L and $F_1 : L_{z_1} \to S$ and $F_2 : L_{z_2} \to S$ satisfy $(*)$, then F_1 must be the restriction of F_2 to the subset L_{z_1}.

Therefore, if for each $z \in L$ a function $F_z : L_z \to S$ exists which satisfies $(*)$, the functions F_z can be patched together to a unique function

$$F : L = \bigcup_{z \in L} L_z \ \to \ S$$

and F also satisfies $(*)$ because for $z \in L$ we have $F(z) = F_z(z)$.

We see that in order to finish the proof it is enough to show that for each $z \in L$, a function F_z as above exists. We do this by induction on L: for an application of 1.3.4(i) let E be the set $\{z \in L \,|\, F_z \text{ exists}\}$. We wish to show $E = L$.

Suppose, for a given $z \in L$, that $w \in E$ for all $w < z$; that is $F_w : L_w \to S$ exists and satisfies $(*)$. We define $F_z : L_z \to S$ by putting

$$\begin{array}{rcll} F_z(w) & = & F_w(w) & \text{for } w < z \\ F_z(z) & = & R(z, \{F_w(w) \,|\, w < z\}) & \end{array}$$

Check yourself that F_z satisfies $(*)$. We have proved that $z \in E$ on the assumption that $w \in E$ for all $w < z$, that is, the hypothesis of 1.3.4(i), and may conclude that $E = L$, as desired. ∎

Exercise 31 Let $(L, \leq)$ be a well-order and S a set. Prove the following two variations on the principle of recursion.

i) For any $R : \mathcal{P}(S \times L) \to S$ there is a unique $F : L \to S$ with

$$F(x) = R(\{(F(y), y) \,|\, y < x\})$$

ii) For any $s_0 \in S$, any $R : \mathcal{P}(S) \to S$ and any $g : S \to S$ there is a unique function $F : L \to S$ such that

$$\begin{array}{rcll} F(0_L) & = & s_0 & \\ F(l+1) & = & g(F(l)) & \text{if } l \text{ is not maximal in } L \\ F(l) & = & R(\{F(y) \,|\, y < l\}) & \text{if } l \text{ is a nonzero limit in } L \end{array}$$

Example Let us give a simple example of a function $L \to \{0, 1\}$ defined by recursion: the *parity* function. If, in the formulation of Exercise 31ii), $s_0 = 0$, g the switch ($g(x) = 1 - x$), and R the constant 0 function, one obtains a unique function $F : L \to \{0, 1\}$ such that $F(x)$ is $n \bmod 2$ where n is the unique natural number such that for some limit element l, $x = l + n$.

More fundamental examples of functions defined by recursion appear in the proof of Proposition 1.3.9 below, and in the Appendix (1.4).

We conclude this section by discussing how to compare well-orders.

Definition 1.3.6 Let $(L, \leq)$ and $(M, \leq)$ be well-orders.

i) An *initial segment* of L is a subset $B \subseteq L$ such that for each $x, y \in L$: if $x \in B$ and $y \leq x$, then $y \in B$.

ii) An *(order-)isomorphism* $f : L \to M$ is an order-preserving bijective function.

iii) An *embedding* $f : L \to M$ is an order-isomorphism from L to an initial segment of M.

We write $L \cong M$ if there is an order-isomorphism between L and M, and $L \preceq M$ if there exists an embedding of L into M.

Lemma 1.3.7 *There can be at most one embedding from one well-order L into another well-order M. Therefore, if L is a well-ordered set and $l \in L$, L is never isomorphic to $\{l' \in L \,|\, l' < l\}$.*

Proof. Suppose f and f' are two different embeddings: $L \to M$. Then $\{x \in L \,|\, f(x) \neq f'(x)\}$ is nonempty and has a least element x_0. We may suppose (since M is in particular a total order) that $f(x_0) < f'(x_0)$. But now we have: if $y < x_0$ then $f'(y) = f(y) < f(x_0)$ and if $y \geq x_0$ then $f'(y) \geq f'(x_0) > f(x_0)$. We conclude that $f(x_0)$ is not in the image of f', which is therefore not an initial segment.

For the second statement we notice that every isomorphism is in particular an embedding. The only embedding of $\{l' \in L \,|\, l' < l\}$ into L is the inclusion map, but l is not in the image of this map, so it is not an isomorphism. ∎

Corollary 1.3.8 *If $L \preceq M$ and $M \preceq L$ then $L \cong M$.*

Proof. If $i : L \to M$ and $j : M \to L$ are embeddings, then the composition $ji : L \to L$ is an embedding too. Since there is only one embedding from L to L by Proposition 1.3.7 and the identity function $f(x) = x$ is one, we see that $j(i(x)) = x$ for all $x \in L$. Similarly, $i(j(y)) = y$ for all $y \in M$; so $L \cong M$. ∎

Proposition 1.3.9 *For any two well-orders L and M, we have either $L \preceq M$ or $M \preceq L$.*

Proof. Let ∞ be a new point not contained in M. Let $M' = M \cup \{\infty\}$.

Define $R : L \times \mathcal{P}(M') \to M'$ as follows: $R(l, S)$ is the least element in M of $M - S$, if this set is nonempty, and ∞ otherwise. The function R does not really depend on l, but that doesn't matter.

By proposition 1.3.5 there is a unique function $F : L \to M'$, such that

$$F(l) = R(l, \{F(x) \,|\, x < l\})$$

for all $l \in L$.

If $F(l) \neq \infty$ for all $l \in L$, then F is an embedding from L into M (as we leave for you to check). Otherwise, if l_0 is the least element of L such that $F(l_0) = \infty$, then F restricts to an isomorphism between M and $\{x \in L \,|\, x < l_0\}$, in which case there is an embedding of M into L. ∎

Exercise 32 Prove: if L and M are well-orders, $L \preceq M$ and $L \ncong M$, then there is an $m \in M$ such that $L \cong M_m$ where $M_m = \{x \in M \,|\, x < m\}$. Prove also, that this m is unique.

Exercise 33 Let L be a well-order and $f : L \to L$ a map with the property that $x < y$ implies $f(x) < f(y)$ for all $x, y \in L$.

Show that $x \leq f(x)$ for all $x \in L$. Show also, that this does not follow from the weaker condition that $x \leq y$ implies $f(x) \leq f(y)$.

Exercise 34 Let L be a set. Write $\mathcal{P}^*(L)$ for the set of nonempty subsets of L. Suppose that $h : \mathcal{P}^*(L) \to L$ is a function such that the following two conditions are satisfied:

i) For each nonempty family $\{A_i \,|\, i \in I\}$ of elements of $\mathcal{P}^*(L)$, we have

$$h(\bigcup_{i \in I} A_i) = h(\{h(A_i) \,|\, i \in I\})$$

ii) For each $A \in \mathcal{P}^*(L)$, $h(A) \in A$

Show that there is a unique relation $\leq$ on L, which well-orders L, and such that for each nonempty subset A of L, $h(A)$ is the least element of A.

Exercise 35 Let L be a linear order. If $A \subset L$ and $a \in L$, then a is called a *strict upper bound* for A, if $x < a$ for every $x \in A$. Now suppose that the following is true for every $A \subseteq L$: if A has a strict upper bound, then A has a *least* strict upper bound.

a) Prove: if $L \neq \emptyset$, then L has a least element.

b) Prove that L is a well-order [Hint: given a nonempty subset X of L, consider the set $A_X = \{x \in L \,|\, \text{for all } y \in X,\ x < y\}$]

c) Show that b) may fail if we drop the 'strict' in 'strict upper bound'.

Exercise 36 Extend the definition of 'initial segment' (1.3.6) to arbitrary linear orders: an initial segment of $(P, \leq)$ is a subset $B \subseteq P$ such that whenever $x \leq y$ and $y \in B$, then $x \in B$.

Prove that a linear order $(P, \leq)$ is a well-order if and only if for every subset S of P, $(S, \leq)$ is isomorphic to an initial segment of $(P, \leq)$.

1.4 Appendix: Equivalents of the Axiom of Choice

We start with a lemma that ensures the existence of "sufficiently large" well-ordered sets. Then we formulate yet another principle, Zermelo's *Well-Ordering Theorem* (1.4.2), and prove rigorously that the Axiom of Choice, Zorn's Lemma, the Principle of Cardinal Comparability and the Well-Ordering Theorem are all equivalent, relative to basic set theory.

In fact, these are just a few examples out of many: by now, there is a multitude of statements and theorems for which it has been shown that they are equivalent to the Axiom of Choice (you may have a look at the books [16, 23]). Here we mention just two more such forms, without proof:

> *Hausdorff's Maximality Principle* says that every poset contains a maximal chain (maximal w.r.t. inclusion of chains). It is actually rather easy to show that this is equivalent to Zorn's lemma.
>
> *Tychonoff's Theorem* in Topology says, that if $\{X_i \mid i \in I\}$ is an arbitrary set of compact topological spaces, the product space
>
> $$\prod_{i \in I} X_i$$
>
> is again a compact space. The proof of Tychonoff's Theorem makes use of AC. On the other hand it can be shown that the theorem implies AC (first proved in [18]; see also [16]).

It should be noted (and emphasized) that the proof of the following lemma does *not* use the Axiom of Choice or Zorn's Lemma. It was proved by Friedrich Hartogs in [13].

Lemma 1.4.1 (Hartogs' Lemma) *For every set X there is a well-ordering $(L_X, \leq)$ such that there is no injective function from L_X to X.*

Proof. Let P be the set of all pairs $(L, \leq)$ where L is a subset of X and $\leq$ is a well-ordering on L. We shall denote the pair $(L, \leq)$ simply by L.

For two such L and M, we write $L \preceq M$ if there is a (necessarily unique, by Lemma 1.3.7) embedding of well-ordered sets: $L \to M$. Note:

- we have both $L \preceq M$ and $M \preceq L$, if and only if $L \cong M$;

- if $L \cong L'$ and $M \cong M'$, then $L \preceq M$ if and only if $L' \preceq M'$.

We can therefore define an order relation $\leq$ on the set $P/\cong$ of equivalence classes of P modulo the equivalence relation $\cong$. By Proposition 1.3.9, the set $P/\cong$ is a linear order with the relation $\leq$.

Note, that if $L \prec M$ (that is, $L \preceq M$ but $M \ncong L$), there is (by Exercise 32) a unique $m \in M$ such that L is isomorphic to the set $M_m = \{m' \in M \,|\, m' < m\}$ with the inherited order from M.

Therefore, if we denote the $\cong$-equivalence class of L by $[L]$, the set

$$\{\alpha \in P/\cong \,|\, \alpha < [L]\}$$

is isomorphic to L.

Now suppose that $W \subseteq P/\cong$ is a nonempty set of $\cong$-equivalence classes. Let $\alpha = [L]$ be an arbitrary element of W. Consider the set

$$L_W = \{l \in L \,|\, [L_l] \in W\}$$

If L_W is empty, clearly $[L]$ is the least element of W. If L_W is nonempty, then it has (as subset of the well-ordered set L) a least element l_W. But then $[L_{l_W}]$ is the least element of W. So every nonempty subset of $P/\cong$ has a least element, and therefore $P/\cong$ is a well-ordered set.

There cannot be an injective function from $P/\cong$ into X, for suppose f is such a function. Then f gives a bijective function between $P/\cong$ and a subset Y_f of X; we can then give Y_f the same well-ordering as $P/\cong$, so we have $(Y_f, \leq) \cong (P/\cong, \leq)$. This is impossible however, since $[(Y_f, \leq)]$ is an element of $P/\cong$ (see Proposition 1.3.7). ∎

In his paper [27], Zermelo formulated the Axiom of Choice in order to prove the following statement.

Definition 1.4.2 The *Well-Ordering Theorem* is the statement that for every set X there exists a relation $\leq$ which well-orders X.

Remark. Although the Axiom of Choice is intuitively correct, here we see a consequence which is less intuitive, for it asserts that there is a relation which well-orders the set of real numbers, for example. However, it can be shown that it is impossible to define such a relation explicitly ([8]).

Proposition 1.4.3 *The following assertions are equivalent:*

i) *The Axiom of Choice*

ii) *Zorn's Lemma*

iii) *The Principle of Cardinal Comparability*

iv) *The Well-Ordering Theorem*

Proof. We shall prove i)⇒ii)⇒iii)⇒iv)⇒i).
The implication i)⇒ii) uses Hartogs' Lemma (1.4.1). Suppose that $(P, \leq)$ is a poset in which every chain has an upper bound, yet P has no maximal element. We shall prove, using the Axiom of Choice, that in that case for every well-ordered set L there is an embedding of L into P. But this is a contradiction with Hartogs' Lemma.

Since in P every chain has an upper bound, P is nonempty; let $p_0 \in P$. By the Axiom of Choice there is a function $R : \mathcal{P}(P) \to P$, such that for every subset C of P we have: if C is a chain in P then $R(C)$ is an upper bound for C; and $R(C) = p_0$ otherwise. Also, since P has no maximal element, for every $p \in P$ there is $q \in P$ with $p < q$; again using AC, there is a function $g : P \to P$ such that $p < g(p)$ for every $p \in P$.

Let $(L, \leq)$ be an arbitrary well-ordered set. Define a function $F : L \to P$ by recursion over L as follows:

- $F(0_L) = p_0$
- $F(x + 1) = g(F(x))$
- $F(l) = R(\{F(x) \mid x < l\})$ if l is a non-zero limit element of L

It is easy to check that F is an injective function from L into P. L was arbitrary, so we get a contradiction with Hartogs' Lemma.
The implication ii)⇒iii) was done in the proof of Proposition 1.2.10.
The implication iii)⇒iv) uses Hartogs' Lemma once again. Let X be a set. According to Hartogs' Lemma there is a well-ordered set $(L_X, \leq)$ such that there is no injective function from L_X into X. By Cardinal Comparability then, there must be an injective function from X into L_X; but this gives us a well-ordering on X.
Finally, iv)⇒i) is easy. Suppose $f : X \to Y$ is surjective. In order to find a section for f, apply iv) to find a relation $\leq$ on X which well-orders X. Now one can simply define a section $s : Y \to X$ by putting: $s(y)$ is the least element of the nonempty set $f^{-1}(y)$ in the well-ordering on X. ∎

Exercise 37 Give a direct proof of the fact that Zorn's Lemma implies the Well-Ordering Theorem.

Exercise 38 Let X be a set, and S a subset of $\mathcal{P}(X)$. We say that S is *of finite character* if for every $A \subseteq X$ it holds that A is an element of S, if and only if every finite subset of A is an element of S.

The *Teichmüller-Tukey Lemma* states that if S is nonempty and of finite character, S contains a maximal element (with respect to the subset ordering).

a) Use Zorn's Lemma to prove the Teichmüller-Tukey Lemma.

b) Show that the Teichmüller-Tukey Lemma implies the Axiom of Choice.

Chapter 2

Models

In this chapter we develop the notion of 'formal language' as promised in the Introduction; and also its 'interpretation' in mathematical structures.

In the nineteenth century, a number of mathematicians started to reflect on Logic; that is to say, the reasoning principles that are used in mathematical arguments (before that time, Logic belonged to the realm of Philosophy and consisted in studying *syllogisms* – separate reasoning steps – such as had been formulated by Aristotle).

It occurred to George Boole (1815–1864) and Augustus de Morgan (1806–1871) that the mathematical use of the words 'and', 'or' and 'not' obeys the rules of algebra. This is why we have 'Boolean rings'. Further steps, introducing quantifiers ('for all' and 'there exists') were taken by Charles Sanders Peirce (1839–1914), but the most important work of this era is *Begriffsschrift* of Friedrich Ludwig Gottlob Frege (1848–1925), which appeared in 1879. 'Begriffsschrift' can be roughly translated as 'the notation of concepts'. Frege not only defined a complete logical language, but also set out to develop mathematics in it. He abruptly abandoned the whole project after Bertrand Russell (1872–1970) had pointed out an antinomy in his work, but Russell himself continued it in *Principia Mathematica* (with A.N. Whitehead).

By this time (around 1900), the developing field of Logic had captured the attention of great mathematicians such as David Hilbert and Henri Poincaré.

The idea that abstract mathematical statements (and therefore also the 'sentences' of a logical language) can be interpreted in various 'models', certainly existed in the first decades of the 20th century (it is already implicit in Lobachevsky's 1826 proof of the independence of the parallel postulate in

geometry), but most often, the formal definition of the notion 'sentence ϕ is true in model X' is attributed to Alfred Tarski (1901–1983): see [26] for the German translation of his original Polish paper.

Certainly, Tarski created *Model Theory*, of which you will get a first glimpse in this chapter.

2.1 Rings and Orders: an Example

This section is meant to serve as introduction and motivation for the formal definition of an abstract *language* in the next section.

When we say that the real numbers $\mathbb{R}$ form a *commutative ring with* 1, we mean that there are two *distinguished* elements 0 and 1, as well as *operations* $+$ and $\cdot$, such that certain *axioms* hold, for example:

$$x\cdot(y+z) = (x\cdot y) + (x\cdot z)$$

This is to be read as: whenever real numbers are substituted for the *variables* x, y and z, we get an equality as above.

We call the whole of $\{0, 1, +, \cdot\}$ the *ring structure* of $\mathbb{R}$. Now of course you know there are plenty of other rings. For example, let X be any set. The power set $\mathcal{P}(X)$ can be made into a commutative ring with 1: take X for 1, $\emptyset$ for 0, and let for $U, V \subseteq X$, $U + V = (U \cup V) - (U \cap V)$ and $U\cdot V = U \cap V$.

Exercise 39 Check that this indeed gives a ring structure on $\mathcal{P}(X)$.

The example of $\mathcal{P}(X)$ makes it clear that the operation $+$ does not, a priori, mean addition of numbers, but is an abstract symbol generally used for the operation in abelian groups; we might as well have used something like $a(x, y)$ and $m(x, y)$ instead of $x + y$ and $x\cdot y$, respectively, and written the distributivity axiom as

$$m(x, a(y, z)) = a(m(x, y), m(x, z))$$

Similarly, one should regard 0 and 1 as abstract symbols that only acquire meaning once they are *interpreted* in a particular set.

Many axioms for rings have a very simple form: they are equalities between *terms*, where a term is an expression built up using variables, the symbols 0 and 1, and the operation symbols $+, \cdot$ (and brackets). From simple equalities we can form more involved statements using *logical operations*: the operations $\wedge$ ("and"), $\vee$ ("or"), $\rightarrow$ ("if... then"), $\leftrightarrow$ ("if and only if") and

$\neg$ ("not"); and *quantifiers* $\exists$ ("there is") and $\forall$ ("for all"). For example, if we want to express that $\mathbb{R}$ is in fact a field, we may write

$$\forall x(\neg(x = 0) \to \exists y(x{\cdot}y = 1))$$

or equivalently

$$\forall x \exists y(x = 0 \vee x{\cdot}y = 1)$$

We say that the statement $\forall x \exists y(x = 0 \vee x{\cdot}y = 1)$ "is true in $\mathbb{R}$" (of course, what we really mean is: in $\mathbb{R}$ together with the meaning of $0, 1, +, \cdot$). Such statements can be used to distinguish between various rings: for example, the statement

$$\exists x(x{\cdot}x = 1 + 1)$$

is true in $\mathbb{R}$ but not in the ring $\mathbb{Q}$, and the statement

$$\forall x(x{\cdot}x = x)$$

is true in the ring $\mathcal{P}(X)$ but not in $\mathbb{R}$.

Apart from operations on a set, one may also consider certain *relations*. In $\mathbb{R}$ we have the relation of *order*, expressed by $x < y$. As before, we might have used a different symbol for this relation, for example $L(x, y)$ ("x is less than y"). And we can form statements using this new symbol together with the old ones, for example

$$\forall x \forall y \forall z(x < y \to x + z < y + z)$$

which is one of the axioms for an *ordered ring*. In $\mathbb{R}$, the order relation is *definable* from the ring structure, because the statement

$$\forall x \forall y(x < y \leftrightarrow \exists z(\neg(z = 0) \wedge x + z{\cdot}z = y))$$

is true in $\mathbb{R}$. However, this statement is not true in the ordered ring $\mathbb{Q}$. Also the ring $\mathcal{P}(X)$ is (partially) ordered by $U \subset V$; in this ring, the order is definable, but now in a different way:

$$\forall x \forall y(x < y \leftrightarrow (\neg(x = y) \wedge x{\cdot}y = x))$$

In yet another way, the order in $\mathbb{Q}$ is definable from the ring structure. In this case, we use the theorem (first proved by Lagrange) which says that every natural number may be written as the sum of four squares. Since every positive rational number is the quotient of two positive natural numbers, we have:

$$x > 0 \leftrightarrow \exists y_1 \cdots y_8 \, (x{\cdot}(y_1^2 + \cdots + y_4^2 + 1) = y_5^2 + \cdots + y_8^2 + 1)$$

for all $x \in \mathbb{Q}$. Since $x < y$ is equivalent to $\exists z(z > 0 \wedge x + z = y)$, we can define the order on $\mathbb{Q}$ in terms of 0, + and $\cdot$ only.

We see that in general, when we wish to discuss a certain type of mathematical structures, we choose symbols for the distinguished elements, the operations and the relations which make up the structure, and using these we write down statements. The use of such statements is varied: they may be axioms, required to be true in all structures we wish to consider; they may be true in some, but not in others; or they may be used to *define* elements or subsets of a structure.

In Mathematical Logic, we study these statements, and their relation to mathematical structures, formally; in order to do this, *we define formal statements as mathematical objects*. This is done in the next section.

We shall see many examples of different types of structures in the coming sections.

2.2 Languages of First Order Logic

This section is purely "linguistic" and introduces the formal languages for first-order logic – or "predicate logic".

Definition 2.2.1 A *language* L is given by three sets of symbols: *constants*, *function symbols* and *relation symbols*. We may write

$$L = (\mathrm{con}(L), \mathrm{fun}(L), \mathrm{rel}(L))$$

Moreover, for each function symbol f and each relation symbol R the number n of arguments is specified, and called the *arity* of f (or R). If f or R has arity n, we say that it is an *n-ary* (or *n-place*) function (relation) symbol.

For example, the language of rings has two constants, 0 and 1, and two 2-place function symbols for addition and multiplication. There are no relation symbols.

The language of orders has one 2-place relation symbol (S or $<$) for "less than".
Given such a language L, one can build *terms* (to denote elements) and *formulas* (to state properties), using the following auxiliary symbols:

- A countably infinite set of *variables*. This set is usually left unspecified, and its elements are denoted by $x, y, z, \ldots$ or $x_0, x_1, \ldots$

- The equality symbol $=$

- The symbol $\perp$ ("absurdity")
- Connectives: the symbols $\wedge$ ("and") for *conjunction*, $\vee$ ("or") for *disjunction*, $\rightarrow$ ("if... then") for *implication* and $\neg$ ("not") for *negation*
- Quantifiers: the *universal quantifier* $\forall$ ("for all") and the *existential quantifier* $\exists$ ("there exists")
- Some readability symbols, like the comma, and brackets.

Definition 2.2.2 The set of *terms* of a language L is inductively defined as follows:

- any constant c of L is a term of L;
- any variable x is a term of L;
- if $t_1, \ldots, t_n$ is an n-tuple of terms of L and f is an n-place function symbol of L, then $f(t_1, \ldots, t_n)$ is a term of L.

A term which does not contain variables (and hence is built up from constants and function symbols alone) is called *closed*.

Examples

a) Suppose L has a constant c and a 2-place function symbol f. The following are terms of L: $x, y, c, f(x, c), f(f(x, c), c), \ldots$

b) Suppose L has no function symbols. The only terms are variables and constants.

Definition 2.2.3 The set of *formulas* of a given language L is inductively defined as follows:

- If t and s are terms of L, then $(t = s)$ is a formula of L.
- If $t_1, \ldots, t_n$ is an n-tuple of terms of L and R is an n-place relation symbol of L, then $R(t_1, \ldots, t_n)$ is a formula of L.
- $\perp$ is a formula of L.
- If φ and ψ are formulas of L, then so are $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ and $\neg\varphi$.
- If φ is a formula of L, and x is a variable, then also $\forall x\varphi$ and $\exists x\varphi$ are formulas of L.

Remarks/Examples.

a) Given a language L, let V be the set of variables, and A the set of auxiliary symbols that we have listed. Let $S = L \cup V \cup A$. Then formally, terms of L and formulas of L are finite tuples of elements of S.

b) However, the sets of terms of a language and of formulas of a language have a more meaningful structure. Suppose t is a term. Then there are three possibilities: t is a variable, t is a constant, or there is an n-place function symbol f of L, and terms $t_1, \ldots, t_n$, such that $t = f(t_1, \ldots, t_n)$. The terms $t_1, \ldots, t_n$ have the property that each one of them contains *fewer* function symbols of L than t. One uses this to prove properties of terms "by induction on the number of function symbols occurring in them". Similarly, one can prove properties of formulas by induction on the number of symbols from the set $\{\wedge, \vee, \rightarrow, \neg, \forall, \exists\}$ in them. If this number is zero, we call the formula *atomic*.

c) The use of brackets and commas is *only* for the sake of readability and to avoid ambiguity, such as $\varphi \vee \psi \rightarrow \chi$. Outermost brackets are usually omitted.

d) Suppose the language L has one constant c, one 2-place function symbol f and one 3-place relation symbol R. Then

$$\forall x \forall y R(c, x, f(y, c))$$
$$\forall x (x = f(x, x) \rightarrow \exists y R(x, c, y))$$
$$R(f(x, f(c, f(y, c))), c, y) \wedge (x = y \vee \neg R(c, c, x))$$

are formulas of L (note how we use the brackets!), but

$$\forall R \neg R(x, x, c)$$

isn't (this might be called a "second order formula"; quantifying over relations).

Free and bound variables. Roughly speaking, a variable which is "quantified away" in a formula, is called *bound* in that formula; otherwise, it is called *free*.

For example, in the formula

$$\forall x (R(x, y) \rightarrow \exists z P(x, z))$$

the variables x and z are bound whereas y is free. The x in "$\forall x$" is not considered to be either free or bound, nor z in "$\exists z$".

The intuition is, that the formula above states a property of the variable y but not of the variables x, z; it should mean the same thing as the formula

$$\forall u(R(u, y) \to \exists v P(u, v))$$

This is similar to the use of variables in expressions such as $\int_0^x f(t)dt$: this expression is usually a function of x, not of t.

A formula with no free variables is called *closed*, or a *sentence*. Such a formula should be thought of as an *assertion*.

It is an unfortunate consequence of the way we defined formulas, that expressions like

$$\forall x \forall y \forall x R(x, y)$$
$$\forall y(R(x, y) \to \forall x R(x, x))$$

are formulas. The first one has the strange property that the variable x is bound twice; and the second one has the undesirable feature that the variable x occurs both bound and free. In practice, we shall always stick to the following

CONVENTION ON VARIABLES *In formulas, a variable will always be either bound or free but not both; and if it is bound, it is only bound once*

This convention is not meant to exclude formulas like $\forall x P(x) \vee \neg \forall x P(x)$; certainly one can argue that the 'same' variable (namely, x) is 'bound twice'; but in fact every *occurrence* of the variable is only bound once. However, in the case of $\forall x(P(x) \vee \neg \forall x P(x))$ we shall rather use the equivalent form $\forall x(P(x) \vee \neg \forall y P(y))$.

Definition 2.2.4 (Substitution) Suppose φ is a formula of L, and t a term of L. By the *substitution* $\varphi[t/x]$ we mean the formula which results by replacing each occurrence of the variable x by the term t, provided x is a free variable in φ, and no variable in the term t becomes bound in φ (in this definition, the Convention on variables is in force!).

Examples. Suppose φ is the formula $\forall x R(x, y)$. If t is the term $f(u, v)$, then $\varphi[t/x]$ is just φ, since x is bound in φ; $\varphi[t/y]$ is $\forall x R(x, f(u, v))$.

Suppose t is the term $f(x, y)$. Now the substitution $\varphi[t/y]$ presents us with a problem; if we carry out the replacement of y by t we get $\forall x R(x, f(x, y))$, which intuitively does not "mean" that the property expressed by φ, holds

for the element denoted by t! Therefore, we say that the substitution is not defined in this case. In practice though, as said before, we shall consider φ as the "same" formula as $\forall u R(u, y)$, and now the substitution makes sense: we get $\forall u R(u, f(x, y))$.

If the term t is closed (in particular, if t is a constant), the substitution $\varphi[t/x]$ is always defined, as is easy to see.

First order logic and other kinds of logic. In these lecture notes, we shall limit ourselves to the study of "first order logic", which is the study of the formal languages and formulas as we have described here, and their relation to structures, as we will see in the next section.

This logic has good mathematical properties, but it has also severe limitations. Our variables denote, as we shall see, elements of structures. So we can only say things about *all elements* of a structure, not about all subsets, or about sequences of elements. For example, consider the language of orders: we have a 2-place relation symbol $<$ for "less than". We can express that $<$ really is a partial order:

$$(\forall x \neg(x < x)) \wedge (\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z))$$

and that $<$ is a linear order:

$$\forall x \forall y (x < y \vee x = y \vee y < x)$$

but we can *not* express that $<$ is a well-order, since for that we have to say something about *all subsets* (we shall return to this example in Exercise 60).

It is possible to consider logics where such statements can be formed: these are called "higher order" logics. There are also logics in which it is possible to form the conjunction, or disjunction, of an infinite set of formulas (so, formulas will be infinite objects in such a logic).

2.3 Structures for first order logic

In this section we consider a fixed but arbitrary first order language L, and discuss what it means to have a *structure for* L.

Definition 2.3.1 An *L-structure* M consists of a nonempty set, also denoted M, together with the following data:

- for each constant c of L, an element c^M of M;
- for each n-place function symbol f of L, a function

$$f^M : M^n \rightarrow M$$

- for each n-place relation symbol R of L, a subset

$$R^M \subseteq M^n$$

We call the element c^M the *interpretation* of c in M, and similarly, f^M and R^M are called the interpretations of f and R, respectively.

Given an L-structure M, we consider the language L_M (the *language of the structure* M): L_M is L together with, for each element m of M, an extra constant (also denoted m). Here it is assumed that $\mathrm{con}(L) \cap M = \emptyset$. If we stipulate that the interpretation in M of each new constant m is the element m, then M is also an L_M-structure.

Definition 2.3.2 (Interpretation of terms) For each closed term t of the language L_M, we define its interpretation t^M as element of M, by induction on t, as follows. If t is a constant, then its interpretation is already defined since M is an L_M-structure. If t is of the form $f(t_1, \ldots, t_n)$ then also $t_1, \ldots, t_n$ are closed terms of L_M, so by induction hypothesis their interpretations $t_1^M, \ldots, t_n^M$ have already been defined; we put

$$t^M = f^M(t_1^M, \ldots, t_n^M)$$

Next, we define for a closed formula φ of L_M what it means that "φ is *true in* M" (other ways of saying this, are: φ *holds* in M, or M *satisfies* φ). Notation:

$$M \models \varphi$$

Definition 2.3.3 (Interpretation of formulas) For a closed formula φ of L_M, the relation $M \models \varphi$ is defined by induction on φ:

- If φ is an atomic formula, it is equal to $\bot$, of the form $(t_1 = t_2)$, or of the form $R(t_1, \ldots, t_n)$ with $t_1, t_2, \ldots, t_n$ closed terms; define:

$$\begin{array}{rcl} M \models \bot & \textit{never} \text{ holds} & \\ M \models (t_1 = t_2) & \text{iff} & t_1^M = t_2^M \\ M \models R(t_1, \ldots, t_n) & \text{iff} & (t_1^M, \ldots, t_n^M) \in R^M \end{array}$$

  where the t_i^M are the interpretations of the terms according to definition 2.3.2, and R^M the interpretation of R in the structure M.

- If φ is of the form $(\varphi_1 \wedge \varphi_2)$ define

$$M \models \varphi \quad \text{iff} \quad M \models \varphi_1 \text{ and } M \models \varphi_2$$

- If φ is of the form $(\varphi_1 \vee \varphi_2)$ define

$$M \models \varphi \quad \text{iff} \quad M \models \varphi_1 \text{ or } M \models \varphi_2$$

(the "or" is to be read as *inclusive*: as either... or, or both)

- If φ is of the form $(\varphi_1 \to \varphi_2)$ define

$$M \models \varphi \quad \text{iff} \quad M \models \varphi_2 \text{ whenever } M \models \varphi_1$$

- If φ is of the form $(\neg\psi)$ define

$$M \models \varphi \quad \text{iff} \quad M \not\models \psi$$

(here $\not\models$ means "not $\models$")

- If φ is of the form $\forall x\psi$ define

$$M \models \varphi \quad \text{iff} \quad M \models \psi[m/x] \text{ for all } m \in M$$

- If φ is of the form $\exists x\psi$ define

$$M \models \varphi \quad \text{iff} \quad M \models \psi[m/x] \text{ for some } m \in M$$

(in the last two clauses, $\psi[m/x]$ results by substitution of the new constant m for x in ψ)

In a way, this truth definition 2.3.3 simply translates the formulas of L_M (and hence, of L) into ordinary language. For example, if R is a binary (2-place) relation symbol of L and M is an L-structure, then $M \models \forall x \exists y R(x, y)$ if and only if for each $m \in M$ there is an $n \in M$ such that $(m, n) \in R^M$; that is, R^M contains the graph of a function $M \to M$.

2.3.1 Validity and Equivalence of Formulas

The symbol $\leftrightarrow$ is usually treated as an abbreviation: $\varphi \leftrightarrow \psi$ abbreviates $(\varphi \to \psi) \wedge (\psi \to \varphi)$. So, $M \models \varphi \leftrightarrow \psi$ if and only if the two statements $M \models \varphi$ and $M \models \psi$ are either both true or both false. We call the formulas φ and ψ *(logically) equivalent* if this is the case for all M.

Note, that the closed formula $\exists x(x = x)$ is always true, in every structure (this is a formula of every language!), since structures are required to be nonempty. In general, if φ is a formula in a language L such that for every L-structure M and every substitution of constants from M for the free

variables of φ, $M \models \varphi$, then φ is called *valid*. So, φ and ψ are equivalent formulas, if and only if the formula

$$\varphi \leftrightarrow \psi$$

is valid.

The next couple of exercises provide you with a number of useful equivalences between formulas.

Exercise 40 Show that the following formulas are valid:

$\varphi \leftrightarrow \neg\neg\varphi$
$\neg\varphi \leftrightarrow (\varphi \rightarrow \bot)$
$(\varphi \rightarrow \psi) \leftrightarrow (\neg\varphi \vee \psi)$
$(\varphi \vee \psi) \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$
$(\varphi \wedge \psi) \leftrightarrow \neg(\neg\varphi \vee \neg\psi)$
$\exists x\varphi \leftrightarrow \neg\forall x\neg\varphi$
$\forall x\varphi \leftrightarrow \neg\exists x\neg\varphi$

The equivalences $\neg(\varphi \vee \psi) \leftrightarrow (\neg\varphi \wedge \neg\psi)$ and $\neg(\varphi \wedge \psi) \leftrightarrow (\neg\varphi \vee \neg\psi)$ are called *De Morgan's Laws*.

$(\varphi \wedge (\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$
$(\varphi \vee (\psi \wedge \chi)) \leftrightarrow ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$
$(\varphi \rightarrow (\psi \vee \chi)) \leftrightarrow ((\varphi \rightarrow \psi) \vee (\varphi \rightarrow \chi))$
$(\varphi \rightarrow (\psi \wedge \chi)) \leftrightarrow ((\varphi \rightarrow \psi) \wedge (\varphi \rightarrow \chi))$

In the following, assume that x does not occur in φ
$(\varphi \rightarrow \exists x\psi) \leftrightarrow \exists x(\varphi \rightarrow \psi)$
$(\exists x\psi \rightarrow \varphi) \leftrightarrow \forall x(\psi \rightarrow \varphi)$
$(\forall x\psi \rightarrow \varphi) \leftrightarrow \exists x(\psi \rightarrow \varphi)$

Check for yourself that a formula like $\exists x\varphi \leftrightarrow \neg\forall x\neg\varphi$ does *not* violate our Convention on Variables!

Exercise 41 Show by counterexamples that the following sentences are not valid:

$$\exists v(\phi(v) \rightarrow \psi) \;\rightarrow\; (\exists v\phi(v) \rightarrow \psi)$$
$$((\forall x\phi(x)) \rightarrow \psi) \;\rightarrow\; \forall x(\phi(x) \rightarrow \psi)$$

Exercise 42 Prove that for every formula φ, φ is equivalent to a formula which starts with a string of quantifiers, followed by a formula in which no quantifiers occur. Such a formula is called *in prenex normal form*.

Exercise 43 a) Let φ be a formula in which no quantifiers occur. Show that φ is logically equivalent to a formula of the form:

$$\psi_1 \vee \cdots \vee \psi_k$$

where each ψ_i is a conjunction of atomic formulas and negations of atomic formulas. This form is called a *disjunctive normal form* for φ.

b) Let φ be as in a); show that φ is also equivalent to a formula of the form

$$\psi_1 \wedge \cdots \wedge \psi_k$$

where each ψ_i is a disjunction of atomic formulas and negations of atomic formulas. This form is called a *conjunctive normal form* for φ.

In the following exercises you are asked to give L-sentences which "express" certain properties of structures. This means: give an L-sentence ϕ such that for every L-structure M it holds that $M \models \phi$ if and only if the structure M has the given property.

Exercise 44 Let L be the empty language. An L-structure is "just" a nonempty set M.
Express by means of an L-sentence that M has exactly 4 elements.

Exercise 45 Let L be a language with one 2-place relation symbol R. Give L-sentences which express:

a) R is an equivalence relation.

b) There are exactly 2 equivalence classes.

[That is, e.g. for a): $M \models \phi$ if and only if R^M is an equivalence relation on M, etc.]

Exercise 46 Let L be a language with just one 1-place function symbol F. Give an L-sentence ϕ which expresses that F is a bijective function.

Exercise 47 Let L be the language with just the 2-place function symbol $\cdot$. We consider the L-structures $\mathbb{Z}$ and $\mathbb{Q}$ where $\cdot$ is interpreted as ordinary multiplication.

a) "Define" the numbers 0 and 1. That is, give L-formulas $\varphi_0(x)$ and $\varphi_1(x)$ with one free variable x, such that in both $\mathbb{Q}$ and $\mathbb{Z}$, $\varphi_i(a)$ is true exactly when $a = i$ $(i = 0, 1)$.

b) Give an L-sentence which is true in $\mathbb{Z}$ but not in $\mathbb{Q}$.

Exercise 48 Let L be the language $\{f, g\}$ where f is a 2-place function symbol and g a 1-place function symbol. Consider the L-structure M, with underlying set $\mathbb{R}$, f^M is multiplication on $\mathbb{R}$, and g^M is the sine function. Give an L-formula $\phi(x)$ with one free variable x, such that for all $a \in \mathbb{R}$ the following holds:

$$M \models \phi(a) \Leftrightarrow \text{ there is an } n \in \mathbb{N} \text{ such that } a = (2n + \frac{1}{2})\pi$$

Exercise 49 Let $L = \{\leq\}$ be the language of posets; here $\leq$ is a 2-place relation symbol (and we naturally write $x \leq y$ instead of $\leq (x, y)$). So a poset is nothing but an L-structure which satisfies the following L-sentences:

$$\forall x(x \leq x)$$
$$\forall x \forall y \forall z((x \leq y \wedge y \leq z) \rightarrow x \leq z)$$
$$\forall x \forall y((x \leq y \wedge y \leq x) \rightarrow x = y)$$

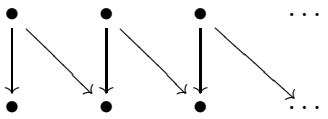
Suppose M is a well-order, seen as L-structure. Give an L-formula $\phi(x)$ in one free variable, such that for every $a \in M$ the following holds:

$$M \models \phi(a) \Leftrightarrow a \text{ is a limit element}$$

2.4 Examples of languages and structures

2.4.1 Graphs

A directed graph is a structure with vertices (points) and edges (arrows) between them, such as:



The language L_{graph} of directed graphs has two 1-place relation symbols, E and V (for "edge" and "vertex"), and two 2-place relation symbols S and T (for "source" and "target"; $S(x, y)$ will mean "the vertex x is the source of the edge y").

An L_{graph}-structure is a nonempty set G together with two subsets E^G, V^G of G, and two subsets S^G, T^G of G^2. G is a directed graph precisely when G satisfies the following 'axioms' for directed graphs:

$$\begin{array}{ll} \forall x(E(x) \vee V(x)) & \forall x \neg(E(x) \wedge V(x)) \\ \forall x \forall y(S(x,y) \rightarrow (V(x) \wedge E(y))) & \forall x \forall y(T(x,y) \rightarrow (V(x) \wedge E(y))) \\ \forall x \forall y \forall z((S(x,z) \wedge S(y,z)) \rightarrow x = y) & \forall x \forall y \forall z((T(x,z) \wedge T(y,z)) \rightarrow x = y) \\ \forall z(E(z) \rightarrow \exists x \exists y(S(x,z) \wedge T(y,z))) & \end{array}$$

2.4.2 Local Rings

The language L_{rings} of rings has constants 0 and 1, two 2-place function symbols for multiplication and addition, denoted $\cdot$ and $+$. There are no relation symbols.

A *commutative ring with* 1 is an L_{rings}-structure which satisfies the axioms for commutative rings with 1:

$$\begin{array}{ll} \forall x(x + 0 = x) & \forall x(x \cdot 1 = x) \\ \forall xy(x + y = y + x) & \forall xy(x \cdot y = y \cdot x) \\ \forall xyz(x + (y + z) = (x + y) + z) & \forall xyz(x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\ \forall x \exists y(x + y = 0) & \forall xyz(x \cdot (y + z) = x \cdot y + x \cdot z) \end{array}$$

(We have started to abbreviate a string of quantifiers of the same kind: instead of $\forall x \forall y$ write $\forall xy$)
A *local ring* is a commutative ring with 1 which has exactly one maximal ideal. This is a condition that involves quantifying over subsets (ideals) of the ring, and cannot be formulated in first order logic. However, one can show that a commutative ring with 1 is local, precisely when for each pair of elements x, y it holds that if $x + y$ is a unit, then either x or y must be a unit. That is, a commutative ring R with 1 is local, if and only if

$$R \models \forall xy(\exists z(z \cdot (x + y) = 1) \rightarrow (\exists v(v \cdot x = 1) \vee \exists w(w \cdot y = 1)))$$

Exercise 50 Let L be L_{rings} together with an extra 1-place relation symbol I. Give L-formulas which express that the subset defined by I is:

a) an ideal;

b) a prime ideal;

c) a maximal ideal.

2.4.3 Vector Spaces

Fix a field k. We can write down a language L_k of first order logic, and axioms in this language, such that the L_k-structures which satisfy the axioms are precisely the k-vector spaces.

The language L_k has a constant 0 and a binary function symbol $+$ to describe the abelian group structure. Furthermore, it has a 1-place function symbol f_m for every element m of k, to describe scalar multiplication. Apart from the axioms for an abelian group (which are the left side of the axioms for rings given above), there are the axioms:

$$\begin{array}{ll} f_m(0) = 0 & \forall xy(f_m(x+y) = f_m(x) + f_m(y)) \\ \forall x(f_1(x) = x) & \forall x(f_m(f_{m'}(x)) = f_{mm'}(x)) \\ \forall x(f_{m+m'}(x) = f_m(x) + f_{m'}(x)) & \forall x\,(f_0(x) = 0) \end{array}$$

In the second line of these axioms, 1 is the unit of the field k, and mm' refers to multiplication in k. In the third line, $m + m'$ refers to addition in k, and the 0 in $f_0(x)$ is the 0 in k. Note, that if the field k is infinite, there are infinitely many axioms to satisfy!

Exercise 51 The language L_k and the axioms for vector spaces given above, are not very satisfactory in the sense that there are many important things about vectors that cannot be expressed by L_k-formulas; for example, that x and y are linearly independent vectors.

Devise yourself a different language and different axioms which do allow you to express that two vectors are linearly independent over k. Mimicking the example of graphs, have two 1-place relation symbols S and V (for "scalar" and "vector" respectively). How do you express addition of vectors and scalar multiplication?

2.4.4 Basic Plane Geometry

The language L_{geom} of basic plane geometry has two 1-place relation symbols P and L for "point" and "line", and a 2-place relation symbol I for "point x lies on line y". The axioms are:

$$\begin{array}{l} \forall x(P(x) \vee L(x)) \\ \forall x\neg(P(x) \wedge L(x)) \\ \forall xy(I(x,y) \rightarrow (P(x) \wedge L(y))) \\ \forall xx'(P(x) \wedge P(x') \rightarrow \exists y(I(x,y) \wedge I(x',y))) \\ \forall xx'yy'((I(x,y) \wedge I(x',y) \wedge I(x,y') \wedge I(x',y')) \rightarrow (x = x' \vee y = y')) \end{array}$$

Convince yourself that these axioms mean: everything is either a point or a line (and not both), for every two points there is a line they lie on, and two distinct lines can have at most one point in common.

Exercise 52 A famous extra axiom says, that for every line l and point x not on l, there is a unique line m through x, which does not intersect l. Show how to express this axiom in L_{geom}.

2.5 The Compactness Theorem

Before we can state the main theorem of this section, we first discuss some abstract general notions concerning first order languages and structures.

Let L be a language. A *theory* in L (or L-theory) is simply a set of L-sentences (closed formulas). Usually this is a set of axioms for a meaningful mathematical theory, such as the axioms for local rings.

If T is an L-theory, an L-structure M is called a *model* of T if every sentence in T is true in M; in other words, if

$$M \models \varphi$$

for every $\varphi \in T$. We shall also write $M \models T$ in this case. So, a local ring is the same thing as a model of the theory of local rings, etc.

Usually, if T is a theory, there will be sentences which are true in every model of T: the consequences of the axioms. We write $T \models \varphi$ to mean: φ holds in every model of T.

A theory T need not have models; T is said to be *consistent* if T has a model. The antonym is *inconsistent*.

Exercise 53 If T is inconsistent, $T \models \varphi$ holds for every L-sentence φ. Show also, that $T \models \varphi$ if and only if $T \cup \{\neg\varphi\}$ is inconsistent.

Clearly, every model of T is also a model of every subtheory $T' \subseteq T$; so if T is consistent, so is T'. The following important theorem says, that in order to check whether a theory T is consistent, one only needs to look at its *finite* subtheories:

Theorem 2.5.1 (Compactness Theorem; Gödel 1929) *Let T be a theory in a language L. If every finite $T' \subseteq T$ is consistent, then so is T.*

We will not prove Theorem 2.5.1 here, because it is a consequence of the Completeness Theorem (Theorem 3.2.2), which is proved in Chapter 3.

Exercise 54 Use the Compactness Theorem to show: if $T \models \varphi$ then there is a finite subtheory $T' \subseteq T$ such that $T' \models \varphi$.

The Compactness Theorem can be used to explore the boundaries of what can be expressed using first order logic. Here are a few examples.

Example 1. Consider the empty language L: no constants, function symbols or relation symbols. An L-structure is nothing but a nonempty set. Still, there are meaningful L-sentences; for example the sentence

$$\forall xyz(x = y \vee x = z \vee y = z)$$

will be true in a set S if and only if S has at most two elements. Likewise, there is for any natural number $n \geq 1$ a sentence ϕ_n, such that ϕ_n is true in S if and only if S has at most n elements.

Exercise 55 Prove this.

Consequently, if T is the theory $\{\neg\phi_n \,|\, n \geq 1\}$, then S is a model of T if and only if S is infinite.

In contrast, there is no theory T such that S is a model of T if and only if S is *finite*. This can be proved with the help of the Compactness Theorem. For, suppose that such a theory T exists. Consider then the theory

$$T' = T \cup \{\neg\phi_n \,|\, n \geq 1\}$$

A model S of T' must be finite, since S is a model of T, yet it must have, for each $n \geq 1$, at least $n + 1$ elements since $S \models \neg\phi_n$. Clearly, this is impossible, so T' has no models.

But now by the Compactness Theorem, there must be a finite subtheory $T'' \subseteq T'$ such that T'' has no models. Consider such T''. Then for some $k \in \mathbb{N}$ we must have that

$$T'' \subseteq T \cup \{\neg\phi_n \,|\, 1 \leq n \leq k\}$$

But any finite set with at least $k + 1$ elements is a model of $T \cup \{\neg\phi_n \,|\, 1 \leq n \leq k\}$, hence of T''. We have obtained a contradiction, showing that the assumed theory T does not exist.

Exercise 56 Conclude from this reasoning, that there cannot be a single sentence ϕ in the empty language, such that ϕ is true in a set S precisely when S is infinite.

Example 2. The language L_{grp} of groups has one constant e and one 2-place function symbol $\cdot$. The theory T_{grp} of groups consists of the sentences:

$$\begin{array}{ll} \forall x(e{\cdot}x = x) & \forall x(x{\cdot}e = x) \\ \forall xyz(x{\cdot}(y{\cdot}z) = (x{\cdot}y){\cdot}z) & \forall x\exists y(x{\cdot}y = e \wedge y{\cdot}x = e) \end{array}$$

A group is nothing but an L_{grp}-structure which is a model of T_{grp}. Given a group G, an element g is said to have finite order, if for some n, $g^n = \underbrace{g{\cdot}\ldots{\cdot}g}_{n}$ is the unit element of the group. The least such n is in this case called the order of g.

For each $n \geq 2$, there is a sentence ϕ_n of L_{grp} such that for any group G it holds that $G \models \phi_n$ if and only if G has no elements whose order is a divisor of n:

$$\forall x(\underbrace{x{\cdot}\ldots{\cdot}x}_{n} = e \rightarrow x = e)$$

Therefore, in complete analogy to the case with sets as structures for the empty language (Example 1), there is a theory T, with $T_{\text{grp}} \subseteq T$, such that the models of T are precisely the groups which do not contain elements with finite order (such as the group $\mathbb{Z}$).

And again, in contrast there is *no* theory T such that its models are precisely the groups which *do* contain elements of finite order. This is proved, using the Compactness Theorem, in a way completely analogous to Example 1, and therefore left as an exercise:

Exercise 57 Carry out the proof of the statement above.

There are many variations on Example 2. We mention one in the following exercise.

Exercise 58 Consider the language L_{graph} of directed graphs.

a) Show that for each $n \geq 1$ there is an L_{graph}-sentence ϕ_n which is true in a graph G exactly when G has no cycles of length n.

b) Show that there is no theory T in L_{graph} such that the models of T are precisely the graphs which contain cycles.

c) Show that there is no finite theory T in the language L_{graph} such that the models of T are precisely the graphs which have no cycles.

Example 3. This and the next example illustrate another use of the Compactness Theorem: it can be used to show the existence of new models of certain theories. Technically, this example is a little different from the first two in that it uses an extension of the language by a constant.

The theory PA of *Peano Arithmetic* describes the basic structure of the natural numbers. The language has two constants 0 and 1 and two binary function symbols $+$ and $\cdot$, and is therefore the same as the language for rings. PA has the following axioms:

$$\begin{array}{ll} \forall x \neg(x+1=0) & \forall xy(x+1=y+1 \to x=y) \\ \forall x(x+0=x) & \forall x(x\cdot 0=0) \\ \forall xy(x+(y+1)=(x+y)+1) & \forall xy(x\cdot(y+1)=x\cdot y+x) \end{array}$$

but, in addition, there are the so-called *induction axioms*. Suppose φ contains the free variables $x, y_1, \ldots y_n$ and does not contain the variable u; then the following is an axiom of PA:

$$\forall y_1 \cdots y_n((\varphi[0/x] \wedge \forall x(\varphi \to \varphi[x+1/x])) \to \forall u \varphi[u/x])$$

PA is a consistent theory, for the ordinary set $\mathbb{N}$ of natural numbers, with the ordinary $0, 1, +, \cdot$ is a model of PA.

However, there are other models of PA. This can be seen with the help of the Compactness Theorem: consider the language L, which is the language of PA together with one extra constant c. Let T be the L-theory which has all the axioms of PA, and moreover all the axioms:

$$\begin{array}{c} \neg(c=0) \\ \neg(c=1) \\ \neg(c=1+1) \\ \neg(c=(1+1)+1) \\ \vdots \end{array}$$

Suppose T' is a finite subtheory of T. Then T' contains only finitely many of these new axioms. Therefore, we can always make $\mathbb{N}$ into an L-structure which is a model of T', by picking a natural number for the interpretation of the constant c which is large enough.

Therefore, every finite subtheory T' of T is consistent; by the Compactness Theorem, T is consistent. So T has a model M. Then M is, in particular, a model of PA. One can show that in every model of PA, the interpretations of the closed terms

$$0, 1, 1+1, (1+1)+1, ((1+1)+1)+1, \ldots$$

are all distinct, so there is an injective function from $\mathbb{N}$ into M. Moreover, in M there is the element c^M which, since M is a model of T, must be distinct from $0^M, 1^M, (1+1)^M, \ldots$

The element c^M is called a *nonstandard number* and M is a *nonstandard model*.

Exercise 59

a) Prove that PA $\models \forall x(x = 0 \vee \exists y(x = y + 1))$

b) Let M be a nonstandard model of PA. Prove that M contains an infinite descending chain: there are elements $c_0, c_1, \ldots$ in M such that $c_0 > c_1 > \cdots$

The theory of models of PA is very interesting from the point of view of Model Theory, and also from the point of view of Gödel's famous *Incompleteness Theorems*. The book [17] gives an account of the model theory of PA; for an elementary exposition of the Incompleteness Theorems, see [24].

Another variation on the theme of the Compactness Theorem concerns well-orders.

Exercise 60 Let L be the language of orders, with just a 2-place relation symbol $<$ for "less than".

a) Give an L-sentence ϕ such that the models of ϕ are precisely the linear orders.

b) Show that there is no L-theory T such that the models of T are precisely the well-ordered sets.

[Hint: Suppose that such a theory T exists. Let L' be the language obtained from L by adding infinitely many new constants $c_1, c_2, \ldots$. Let T' be the L'-theory which contains T and a set of sentences saying that "$c_1 > c_2 > \cdots$ is an infinite descending chain" (recall Proposition 1.3.2). Use the Compactness Theorem to obtain a contradiction]

c) Use the technique of part b) (and the Hint there) to prove that for every infinite well-order M there is an L-structure M' such that the following hold:

   i) M and M' satisfy the same L-sentences

   ii) M' is not a well-order

Example 4. Consider the following language: the language $L_{\mathbb{R}}$ which has a constant r for every real number r, an n-place function symbol f for every function $f : \mathbb{R}^n \to \mathbb{R}$, and an n-place relation symbol R for every subset $R \subseteq \mathbb{R}^n$.

Clearly, interpreting everything by itself, $\mathbb{R}$ is an $L_{\mathbb{R}}$-structure. Let $T_{\mathbb{R}}$ be the set of all $L_{\mathbb{R}}$-sentences ϕ such that $\mathbb{R} \models \phi$. Then $\mathbb{R}$ is a model of $T_{\mathbb{R}}$.

Now just as in the previous example, we form a new language L out of $L_{\mathbb{R}}$ by adding one extra constant c, and we let T be the union of $T_{\mathbb{R}}$ with the set of new axioms:

$$\{c > n \,|\, n \in \mathbb{N}\}$$

And just as in the previous example, we see that every finite subtheory of T is consistent. Therefore by the Compactness Theorem, T has a model $\mathcal{R}$.

$\mathcal{R}$ is a model of $T_{\mathbb{R}}$, and there is an embedding of $\mathbb{R}$ into $\mathcal{R}$; but moreover, $\mathcal{R}$ contains the "infinite" element $c^{\mathcal{R}}$. $\mathcal{R}$ is a field, because the axioms for a field are true in $\mathbb{R}$ and hence form part of $T_{\mathbb{R}}$. Let $d \in \mathcal{R}$ be the multiplicative inverse of $c^{\mathcal{R}}$. Then in $\mathcal{R}$, d is greater than 0, yet it is smaller than $\frac{1}{n}$ for each n! d is called a *nonstandard element*. We say that $\mathcal{R}$ is a *model for nonstandard analysis*.

Using a model for nonstandard analysis allows one to define concepts of ordinary analysis without using the usual ε-δ definitions. For example, a function $f : \mathcal{R} \to \mathcal{R}$ is continuous at $x \in \mathcal{R}$ if and only if for each nonstandard element d, the element $|f(x+d)-f(x)|$ is at most nonstandard.

Moreover, a nonstandard element d is thought of as an "infinitesimal" element, and in a model of nonstandard analysis, the differential quotient $\frac{\mathrm{d}f}{\mathrm{d}x}$ is a "real" quotient (instead of a limit): one says that the function f is differentiable at x if and only if for any two nonstandard elements d and d', the expressions $\frac{f(x+d)-f(x)}{d}$ and $\frac{f(x+d')-f(x)}{d'}$ differ by at most a nonstandard element.

Nonstandard Analysis, originating in Logic and first developed by Abraham Robinson (see [22]), has developed into a subfield of Analysis; for a more recent introduction, see e.g. [12].

Here are some more exercises about the Compactness Theorem.

Exercise 61 For sets X, let us write '$|X|$ is divisible by 3' if either $|X|$ is finite and divisible by 3, or X is infinite. Prove that there is no sentence ϕ in the empty language, which expresses this property. [Hint: suppose such a sentence ϕ existed. Consider $\neg\phi$]

Exercise 62 Let L be an arbitrary language. A class $\mathcal{M}$ of L-structures

is called *elementary* if there is an L-theory T such that $\mathcal{M}$ is precisely the class of all models of T.

Suppose, that for such a class $\mathcal{M}$ we have that both $\mathcal{M}$ and its complement are elementary. Prove that there is an L-sentence ϕ such that $\mathcal{M}$ is precisely the class of all L-structures which satisfy ϕ.

Exercise 63 In this exercise we use the Compactness theorem to prove that every set X admits a linear order (that is, there is a linear order on X).

a) First prove this for every *finite* X, by induction on $|X|$.

b) Now let X be arbitrary. Let L be the language with one 2-place relation symbol $<$ and constants $\{c_x \mid x \in X\}$. The L-theory T has the following axioms:

$$\begin{array}{cl} \forall x \neg(x < x) & \\ \forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z) & \\ \forall x \forall y (x < y \vee x = y \vee y < x) & \\ \neg(c_x = c_y) & \text{for every pair } x \neq y \text{ of elements of } X \end{array}$$

Prove, using the Compactness Theorem, that T is consistent.

c) Let M be a model of T. Show that M induces a linear order on X.

Exercise 64 Let L be the language of rings and ϕ an L-sentence. Suppose that for every natural number n there is a prime number $p > n$ and a field F of characteristic p, such that $F \models \phi$. Show that there is a field K of characteristic 0 such that $K \models \phi$.

Exercise 65 (De Bruijn-Erdös) The result to be proved in this exercise was first published in [7]; evidently, the authors were unaware of the force of the Compactness Theorem at the time.
We consider *simple undirected graphs*: a simple undirected graph has edges just as the directed graphs of subsection 2.4.1, but now the edges have no direction. Moreover, a graph is simple if for any two vertices, there is at most one edge between them. In other words, a simple undirected graph is just a set with a symmetric binary relation.
Let (X, R) be such a simple undirected graph, and k a positive integer. A *k-colouring* of (X, R) is a function f from X to the set $\{1, \ldots, k\}$ such that whenever $x, y \in X$ and $R(x, y)$ holds, $f(x) \neq f(y)$ (note, that this implies that the relation R is irreflexive).
Prove (using the Compactness Theorem) the following statement: if every finite subgraph of (X, R) has a k-colouring, then (X, R) has a k-colouring.

2.6 Substructures and Elementary Substructures

Definition 2.6.1 (Isomorphism of L-structures) Let M and N be L-structures. An *isomorphism* from M to N is a bijective function $\beta : M \to N$ such that the following hold:

i) $\beta(c^M) = c^N$ for every constant c of L;

ii) $\beta(f^M(x_1, \ldots, x_n)) = f^N(\beta(x_1), \ldots, \beta(x_n))$ for every n-place function symbol f of L and every $x_1, \ldots, x_n \in M$;

iii) $(x_1, \ldots, x_n) \in R^M \Leftrightarrow (\beta(x_1), \ldots, \beta(x_n)) \in R^N$ for every n-place relation symbol of L and $x_1, \ldots, x_n \in M$.

We say that M and N are *isomorphic* if there is an isomorphism $\beta : M \to N$.

It is easy to see that if $\beta : M \to N$ is an isomorphism then so is $\beta^{-1} : N \to M$, so the relation of being isomorphic is symmetric.

Exercise 66 Let $\varphi(y_1, \ldots, y_n)$ be an L-formula and $x_1, \ldots, x_n \in M$. Suppose $\beta : M \to N$ is an isomorphism. Show that $M \models \varphi(x_1, \ldots, x_n)$ if and only if $N \models \varphi(\beta(x_1), \ldots, \beta(x_n))$. Conclude that isomorphic L-structures satisfy the same L-sentences.

Exercise 67 For a field k, let L_k be the language of k-vector spaces. Show that for k-vector spaces M and N, an L_k-isomorphism from M to N is the same thing as a bijective k-linear map. Show also that for two rings R and S, an L_{rings}-isomorphism from R to S is the same thing as a ring isomorphism. The same holds for graphs, groups, posets, etcetera.

Definition 2.6.2 Let M and N be structures for a language L. We say that N is a *substructure* of M, and write $N \subseteq M$, if N is a subset of M, and the following conditions are satisfied:

- $c^N = c^M$ for every constant c of L;
- $f^N : N^n \to N$ is the restriction of f^M to N^n for every n-place function symbol of L (this means that for all $x_1, \ldots, x_n \in N$, $f^M(x_1, \ldots, x_n)$ is an element of N, and equal to $f^N(x_1, \ldots, x_n)$);
- $R^N = R^M \cap N^n$ for every n-place relation symbol R of L (this means that for $x_1, \ldots, x_n \in N$, $(x_1, \ldots, x_n) \in R^M$ if and only if $(x_1, \ldots, x_n) \in R^N$).

When we are considering models M, N of an L-theory T, we also say that N is a *submodel* of M if N is a substructure of M.

Exercise 68 Let $N \subseteq M$ be a substructure. Show that for every quantifier-free L-formula (that is, a formula without quantifiers) φ with variables $x_1, \ldots, x_n$ and for every n-tuple $m_1, \ldots, m_n$ of elements of N, we have

$$N \models \varphi(m_1, \ldots, m_n) \text{ if and only if } M \models \varphi(m_1, \ldots, m_n)$$

Exercise 69 Let N be an L-structure. The *diagram* of N, $D(N)$, is the set of all quantifier-free L_N-sentences which are true in N.

a) Suppose M is a model of $D(N)$. Show that M has a substructure which is isomorphic to N.

b) Conversely, suppose that M is an L-structure such that N is isomorphic to a submodel of M. Show that M can be made into an L_N-structure which is a model of $D(N)$.

If M is an L-structure and $N \subseteq M$ is a nonempty subset which contains all the elements c^M and is closed under the functions f^M, there is a unique way of making N into a substructure of M, by defining

$$R^N = R^M \cap N^n$$

for each n-place relation symbol R of L. Therefore, we shall sometimes refer to the substructure determined by N, also by N.

Now suppose $\{N_i \mid i \in I\}$ is a family of subsets of M such that each N_i contains all the constants c^M and is closed under the functions f^M. Then this also holds for the intersection $\bigcap_{i \in I} N_i$. Therefore, if M is an L-structure and S is an arbitrary subset of M, there is a *least* substructure of M which contains S as a subset; we shall call this the substructure *generated by* S.

Exercise 70 a) Show that the substructure generated by S can also be constructed as the union of a chain of subsets of M, as follows. Let S_0 be the union of S and the set $\{c^M \mid c \text{ a constant of } L\}$. Suppose $S \subseteq S_0 \subseteq S_1 \subseteq \cdots \subseteq S_k$ have been constructed; let S_{k+1} be the union of S_k and the set

$$\{f^M(x_1, \ldots, x_n) \mid f \text{ an } n\text{-place function symbol of } L,\ x_1, \ldots, x_n \in S_k\}$$

b) Conclude that if the language L is countable and S is countable, the substructure generated by S is countable too.

c) More directly, the substructure generated by S is the set

$$\{t^M(s_1, \ldots, s_n) \mid t \text{ an } L\text{-term}, s_1, \ldots, s_n \in S\}$$

Definition 2.6.3 A substructure $N \subseteq M$ is called an *elementary substructure*, written $N \preceq M$, if the equivalence of Exercise 68 holds for *all* L-formulas φ. Equivalently, if for every sentence φ of L_N,

$$N \models \varphi \text{ if and only if } M \models \varphi$$

The notation $N \preceq M$ should not be confused with the same notation for embeddings between well-orders in Chapter 1.
The notion of "elementary substructure" means that, from the point of view of L, the elements of N have the same properties in N as in M. For example, consider $\mathbb{Q} \subseteq \mathbb{R}$ as a subring. Then this is *not* an elementary substructure, for 2 is a square in $\mathbb{R}$ but not in $\mathbb{Q}$. However, if we consider $\mathbb{Q}$ and $\mathbb{R}$ just as ordered structures (as structures for the language with just one binary relation symbol $<$), then $\mathbb{Q}$ is an elementary substructure of $\mathbb{R}$. We shall not prove this last fact here, but anticipating some definitions yet to come, we point out that the so-called *theory of dense linear orders without end-points* (see Definition 2.9.4 at the end of this chapter), of which both $\mathbb{Q}$ and $\mathbb{R}$ are models, has quantifier elimination (see the definition at the beginning of the next section). Hence the statement follows from exercise 73 below.

Exercise 71 Suppose N is an L-structure. The *elementary diagram* of N, $E(N)$, is the set of all L_N-sentences which are true in N. In analogy to Exercise 69, prove the following:

a) Suppose M is a model of $E(N)$. Show that M has an elementary substructure which is isomorphic to N.

b) Conversely, suppose that M is an L-structure such that N is isomorphic to an elementary submodel of M. Show that M can be made into an L_N-structure which is a model of $E(N)$.

The theory $E(N)$ is called the *elementary diagram* of N, and in the literature often denoted by $\mathrm{Diag}_{\mathrm{el}}(N)$.

Exercise 72 (Tarski-Vaught Test) Suppose $N \subseteq M$ is an L-substructure. Show that $N \preceq M$ if and only if the following condition holds: for every L_N-sentence of the form $\exists x \varphi$ which is true in M, there exists an $m \in N$ such that $M \models \varphi[m/x]$.
[Hint: use induction on L_N-sentences. Convince yourself that it suffices to consider the cases $\exists$, $\wedge$ and $\neg$]

Note, that if $N \preceq M$ then both structures satisfy in particular the same L-sentences; hence for every L-theory T, N is a model of T if and only if M is.

2.7 Quantifier Elimination

Let T be a theory in a language L. We say that T *admits elimination of quantifiers*, or *has quantifier elimination* if for every L-formula φ with free variables $x_1, \ldots, x_n$ there is a *quantifier-free* L-formula ψ with at most the free variables $x_1, \ldots, x_n$, such that

$$T \models \forall x_1 \cdots x_n(\varphi \leftrightarrow \psi)$$

We also say that φ and ψ are *T-equivalent*.

In particular, if φ is a sentence, there will be a quantifier-free L-sentence ψ such that $T \models \varphi \leftrightarrow \psi$.

Exercise 73 Suppose the theory T admits elimination of quantifiers. Then if $N \subseteq M$ is a substructure and N and M are models of T, N is an elementary substructure of M.

Applications of quantifier elimination often concern *completeness* of the theory T. We say that a theory T is *complete* if for every L-sentence φ, either $T \models \varphi$ or $T \models \neg\varphi$ holds. Clearly, if T admits quantifier elimination, then this has only to be checked for quantifier-free L-sentences.

Exercise 74 Show that T is complete if and only if any two models of T satisfy the same L-sentences.

The following lemma says that in order to check whether T has quantifier elimination, we may restrict ourselves to very simple formulas. Call a formula *simple* if it is of the form

$$\exists x(\psi_1 \wedge \cdots \wedge \psi_n \wedge \neg\chi_1 \wedge \cdots \wedge \neg\chi_m)$$

where $\psi_1, \ldots, \psi_n, \chi_1, \ldots, \chi_m$ are atomic formulas.

Lemma 2.7.1 *T admits elimination of quantifiers if and only if every simple formula is T-equivalent to a quantifier-free formula in at most the same free variables.*

Proof. Clearly, the given condition is necessary; to see that it is also sufficient, we argue by induction on φ to show that every φ is T-equivalent to a quantifier-free formula.

This is plainly true for atomic φ, and it is left to you to see that the set of formulas which are T-equivalent to a quantifier-free formula, is closed under the operations $\wedge$, $\vee$, $\rightarrow$ and $\neg$.

For the quantifier case, we use Exercise 43 which states that every quantifier-free formula is equivalent to a formula of the form

$$\psi_1 \vee \cdots \vee \psi_n$$

where each ψ_i is a conjunction of atomic formulas and negated atomic formulas. Hence, if φ is T-equivalent to a quantifier-free formula, it is T-equivalent to one in this form, whence $\exists x\varphi$ is equivalent to $(\exists x\psi_1) \vee \cdots \vee (\exists x\psi_n)$, that is: a disjunction of simple formulas. Now the condition in the lemma tells us that each of these is T-equivalent to a quantifier-free formula, and therefore so is $\exists x\varphi$.
For the case $\forall x\varphi$, one simply uses that this is equivalent to $\neg\exists x\neg\varphi$. ∎

In this section, by way of example we shall prove for one theory that it has quantifier elimination: the *theory of algebraically closed fields* T_{acf}. Recall that a field k is algebraically closed if every polynomial (which is not a constant different from 0) with coefficients in k has a root (a zero) in k. That this theory has quantifier elimination, was proved by Alfred Tarski in 1948.

Let us use L for the language L_{rings}: the language of commutative rings with 1. The L-theory T_{acf} has, besides the axioms for commutative rings with 1, the axioms:

$$\forall x(\neg(x = 0) \rightarrow \exists y(x{\cdot}y = 1))$$
$$\forall y_0 \cdots y_n((\textstyle\bigwedge_{i=0}^{n-1} y_i = 0 \wedge y_n \neq 0) \vee \exists x(y_0{\cdot}x^n + \cdots + y_{n-1}{\cdot}x + y_n = 0))$$

(here $y_n \neq 0$ abbreviates $\neg(y_n = 0)$, x^n abbreviates the term $\underbrace{x{\cdot}\cdots{\cdot}x}_{n \text{ times}}$, and $\bigwedge_{i=0}^{n-1} y_i = 0$ is short for $y_0 = 0 \wedge \cdots \wedge y_{n-1} = 0$)
The last line describes an axiom for each $n \geq 1$, so there are infinitely many axioms).
These axioms express that we have a field, in which every nonconstant polynomial has a root. In other words, an algebraically closed field.

Note that every term $t(x, y_1, \ldots, y_n)$ of L in variables $x, y_1, \ldots, y_n$ denotes a polynomial in the same variables, and coefficients in $\mathbb{N}$, so with every

atomic formula $t = s$ in these variables we can associate a polynomial P with coefficients in $\mathbb{Z}$, such that in every ring R and $a, b_1, \ldots, b_n \in R$,

$$R \models (t = s)(a, b_1, \ldots, b_n) \text{ iff } P(a, b_1, \ldots, b_n) = 0 \text{ in } R$$

Furthermore we notice that since every field is an integral domain, a conjunction $r_1 \neq 0 \wedge \cdots \wedge r_k \neq 0$ is equivalent to $r_1 \cdots r_k \neq 0$. So we can write every simple L-formula as

$$\exists x(P_1(x, y_1, \ldots, y_n) = 0 \wedge \cdots \wedge P_k(x, y_1, \ldots, y_n) = 0 \wedge Q(x, y_1, \ldots, y_n) \neq 0)$$

Definition 2.7.2 Let L be a language, Γ a set of L-formulas, M and N L-structures, $\vec{a} = a_1, \ldots, a_n$ and $\vec{b} = b_1, \ldots, b_n$ tuples of elements of M and N, respectively. Write $\vec{a} \equiv_\Gamma \vec{b}$ if for every formula $\phi(x_1, \ldots, x_n)$ from Γ we have:

$$M \models \phi(a_1, \ldots, a_n) \Leftrightarrow N \models \phi(b_1, \ldots, b_n)$$

We shall apply this for Γ the set of quantifier-free L-formulas and for Γ the set of simple L-formulas; and write $\vec{a} \equiv_{\text{qf}} \vec{b}$, $\vec{a} \equiv_{\text{simple}} \vec{b}$.

Lemma 2.7.3 *Let L be an arbitrary language. Suppose that an L-theory T has the following property:*

> Whenever M and N are models of T, and $\vec{a} = a_1, \ldots, a_n$, $\vec{b} = b_1, \ldots, b_n$ are tuples of elements of M and N, respectively, then $\vec{a} \equiv_{\text{qf}} \vec{b}$ implies $\vec{a} \equiv_{\text{simple}} \vec{b}$

Then T has quantifier elimination.

Proof. Assume that T has the property in the statement of the Lemma. By Lemma 2.7.1 we have to show that every simple L-formula is T-equivalent to a quantifier-free formula in the same free variables. So, let $\exists v \phi(v, \bar{w})$ be a simple formula, with $\vec{w} = w_1, \ldots, w_n$ the free variables. Let $\vec{c} = c_1, \ldots, c_n$ be new constants; we write $L_{\vec{c}}$ for $L \cup \{c_1, \ldots, c_n\}$.

Let Γ be the set of all quantifier-free L-formulas $\psi(\vec{w})$ such that

$$T \models (\exists v \phi(v, \vec{c})) \rightarrow \psi(\vec{c})$$

and write $\Gamma(\vec{c})$ for $\{\psi(\vec{c}) \,|\, \psi(\vec{w}) \in \Gamma\}$.

Claim 1 $T \cup \Gamma(\vec{c}) \models \exists v \phi(v, \vec{c})$

To prove Claim 1, suppose for a contradiction that M is a model of $T \cup \Gamma(\vec{c})$ and $M \models \neg \exists v \phi(v, \vec{c})$. Let Δ be the set of all quantifier-free $L_{\vec{c}}$-sentences which are true in M.

Claim 2 The theory $T \cup \Delta \cup \{\exists v \phi(v, \vec{c})\}$ is consistent.

Proof of Claim 2: suppose that this theory is inconsistent, then by the Compactness Theorem there are finitely many elements $\delta_1(\vec{c}), \ldots, \delta_k(\vec{c})$ of Δ such that

$$T \cup \{\delta_1(\vec{c}), \ldots, \delta_k(\vec{c})\} \cup \{\exists v \phi(v, \vec{c})\}$$

is inconsistent. This means that

$$T \models \exists v \phi(v, \vec{c}) \rightarrow \neg\delta_1(\vec{c}) \vee \cdots \vee \neg\delta_k(\vec{c})$$

and therefore by definition of Γ, that the formula $\neg\delta_1(\vec{w}) \vee \cdots \vee \neg\delta_k(\vec{w})$ is an element of Γ.

Now M is, by assumption, a model of $\Gamma(\vec{c})$ so we have

$$M \models \neg\delta_1(\vec{c}) \vee \cdots \vee \neg\delta_k(\vec{c})$$

On the other hand, the sentences $\delta_1(\vec{c}), \ldots, \delta_k(\vec{c})$ are elements of Δ and therefore true in M by definition of Δ. Clearly, we have a contradiction now, which proves Claim 2.

Having proved Claim 2, we return to the proof of Claim 1. By Claim 2, let N be a model of $T \cup \Delta \cup \{\exists v \phi(v, \vec{c})\}$.
Let $\vec{a} = \vec{c}^M$ and $\vec{b} = \vec{c}^N$. We have now, for every quantifier-free L-formula $\psi(\vec{w})$:

$$\begin{array}{rcl} M \models \psi(\vec{a}) & \Leftrightarrow & M \models \psi(\vec{c}) \\ & \Leftrightarrow & \psi(\vec{c}) \in \Delta \\ & \Leftrightarrow & N \models \psi(\vec{c}) \\ & \Leftrightarrow & N \models \psi(\vec{b}) \end{array}$$

We conclude that $\vec{a} \equiv_{\mathrm{qf}} \vec{b}$. However, $M \models \neg\exists v \phi(v, \vec{a})$ whereas $N \models \exists v \phi(v, \vec{b})$. Since $\exists v \phi(v, \vec{w})$ was assumed to be a simple formula, we see that $\vec{a} \not\equiv_{\mathrm{simple}} \vec{b}$.

But M and N are models of T. So we see that T does *not* have the property in the statement of the Lemma. This contradiction proves Claim 1.

Having proved Claim 1, we apply the Compactness Theorem once again, and see that there must be finitely many $\gamma_1(\vec{c}), \ldots, \gamma_m(\vec{c}) \in \Gamma(\vec{c})$ such that

$$T \models \bigwedge_{i=1}^{m} \gamma_i(\vec{c}) \rightarrow \exists v \phi(v, \vec{c})$$

Which means, since the constants $\vec{c}$ do not appear in T, that

$$T \models \forall \vec{w}(\bigwedge_{i=1}^{m} \gamma_i(\vec{w}) \rightarrow \exists v \phi(v, \vec{w}))$$

Since all γ_i are elements of Γ, we see that the formula $\exists v \phi(v, \vec{w})$ is T-equivalent to the quantifier-free formula $\bigwedge_{i=1}^{m} \gamma_i(\vec{w})$, and we are done. ∎

In order to prove that the theory T_{acf} has quantifier elimination, we need one ingredient from algebra:

Fact. For any field K there is an algebraically closed field $\overline{K}$, the *algebraic closure of* K, such that $K \subset \overline{K}$ and moreover, whenever K is embedded in an algebraically closed field L, there is a (non-unique) extension of this embedding to an embedding of $\overline{K}$ into L. In that case, the image of $\overline{K}$ in L consists precisely of those elements which are zeroes of polynomials with coefficients in K.

Theorem 2.7.4 (Tarski) *The theory T_{acf} has quantifier elimination.*

Proof. We wish to apply Lemma 2.7.3. Suppose K and K' are algebraically closed fields, $\vec{a} \in K$ and $\vec{b} \in K'$ are such that for every quantifier-free $L = L_{\text{rings}}$-formula $\psi(\vec{w})$ we have $K \models \psi(\vec{a})$ if and only if $K' \models \psi(\vec{b})$. Then the subring of K generated by $\vec{a}$ is isomorphic to the subring of K' generated by $\vec{b}$, so we may as well assume that $\vec{a} = \vec{b} \in K \cap K'$. Let $R \subset K \cap K'$ be the quotient field of the subring of $K \cap K'$ generated by $\vec{a}$.

Now let $\exists v \phi(v, \vec{w})$ be a simple L-formula, which we have seen may be taken to be of the form

$$\exists v(P_1(v, \vec{w}) = 0 \wedge \cdots \wedge P_k(v, \vec{w}) = 0 \wedge Q(v, \vec{w} \neq 0))$$

where $P_1, \ldots, P_k, Q$ are polynomials with coefficients in $\mathbb{Z}$. We have to prove: if $K \models \exists v \phi(v, \vec{a})$ then $K' \models \exists v \phi(v, \vec{a})$.

If all the polynomials $P_i(v, \vec{a})$ are identically zero, then this reduces to: if $K \models \exists v Q(v, \vec{a}) \neq 0$ then $K' \models \exists v Q(v, \vec{a}) \neq 0$. But if $K \models \exists v Q(v, \vec{a}) \neq 0$, then the polynomial $Q(v, \vec{a})$ is not identically zero, and has therefore only finitely many zeroes. On the other hand K', being algebraically closed, is infinite; hence $K' \models \exists v Q(v, \vec{a}) \neq 0$ as desired.

If not all polynomials P_i are identically zero, and $c \in K$ satisfies $K \models \phi(c, \vec{a})$, then c is algebraic over $\vec{a}$ and therefore an element of the algebraic closure of R. Since this algebraic closure embeds into K', we also have an element d of K' such that $K' \models \phi(d, \vec{a})$. We have verified the hypothesis of Lemma 2.7.3 and conclude that T_{acf} has quantifier elimination. ∎

Exercise 75 Let ϕ be the L_{rings}-sentence

$$\exists x(x^2 + 1 = 0 \wedge x + 1 \neq 0)$$

Give a quantifier-free L_{rings}-sentence ψ which is T_{acf}-equivalent to ϕ.

Exercise 76 Let K be an algebraically closed field, and $\phi(v)$ an L_{rings}-formula in one free variable v. Prove that the set $\{a \in K \mid K \models \phi(a)\}$ is either finite or cofinite.

In the book [20] you will find many more proofs of quantifier elimination for various theories.

Applications of Quantifier Elimination for T_{acf}

In this subsection we present a few mathematical applications of quantifier elimination for algebraically closed fields.

The theory T_{acf} is not complete, because it does not settle all quantifier-free sentences of L_{rings}: for example, the sentence $1 + 1 + 1 = 0$. However, once we specify the characteristic of the field, the theory becomes complete. Let ϕ_n be the sentence $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$. Define the following theories:
$T^p_{\text{acf}} = T_{\text{acf}} \cup \{\phi_p\}$ for a prime number p, is the theory of algebraically closed fields of characteristic p;
$T^0_{\text{acf}} = T_{\text{acf}} \cup \{\neg\phi_n \mid n > 0\}$ is the theory of algebraically closed fields of characteristic zero.

Then the theories T^p_{acf} and T^0_{acf} are complete, for by quantifier elimination we only have to look at quantifier-free sentences. These are combinations (using $\wedge$, $\vee$, $\neg$ and $\rightarrow$) of sentences $t = s$, with t and s closed terms. Then t and s represent elements of $\mathbb{Z}$, and $t = s$ is a consequence of T^p_{acf} precisely when their difference is a multiple of p. For characteristic 0: $t = s$ is a consequence of T^0_{acf} precisely when this sentence is true in $\mathbb{Z}$.

The completeness of these theories has the following consequence. We write $\mathbb{F}_p$ for the field of p elements, and $\overline{\mathbb{F}_p}$ for its algebraic closure. $\mathbb{C}$ is the field of complex numbers.

Lemma 2.7.5 *Let ϕ be a sentence of L_{rings}. The following assertions are equivalent:*

i) $\mathbb{C} \models \phi$

ii) There is a natural number m such that for all primes $p > m$, $\overline{\mathbb{F}_p} \models \phi$

Proof. $\mathbb{C}$ is an algebraically closed field of characteristic zero so if $\mathbb{C} \models \phi$ then by completeness of T^0_{acf}, $T^0_{\text{acf}} \models \phi$. By the Compactness Theorem, there is a number m such that $T_{\text{acf}} \cup \{\neg\phi_n \mid n \leq m\} \models \phi$. It follows that for every $p > m$, $\overline{\mathbb{F}_p} \models \phi$. This proves i)⇒ii); the converse implication is proved in the same way, considering $\neg\phi$ instead of ϕ. ∎

The following little theorem is a nice application of this lemma.

Theorem 2.7.6 *Let $F_1, \ldots, F_n$ be polynomials in n variables $Y_1, \ldots, Y_n$ and with complex coefficients. Consider the function $f : \mathbb{C}^n \to \mathbb{C}^n$ defined by*

$$f(z_1, \ldots, z_n) = (F_1(z_1, \ldots, z_n), \ldots, F_n(z_1, \ldots, z_n))$$

Then if f is injective, it is also surjective.

Proof. Convince yourself that for every natural number $d > 0$ there exists an L_{rings}-sentence Φ_d which expresses: "for every n-tuple of polynomials of degree $\leq d$, if the associated function f of n variables is injective, then it is surjective".

For an application of Lemma 2.7.5, we show that Φ_d is true in every field $\overline{\mathbb{F}_p}$. For suppose we have n polynomials $F_1, \ldots, F_n$ of degree $\leq d$ and coefficients in $\overline{\mathbb{F}_p}$, such that the function $f : (\overline{\mathbb{F}_p})^n \to (\overline{\mathbb{F}_p})^n$ is injective. Let $(x_1, \ldots, x_n) \in (\overline{\mathbb{F}_p})^n$. Let $a_1, \ldots, a_k$ be the list of coefficients which occur in the F_i. There is a least subfield F of $\overline{\mathbb{F}_p}$ which contains all x_i and all a_j. Then F is a finite extension of $\mathbb{F}_p$, hence finite. Moreover, f restricts to a function $F^n \to F^n$ which is still injective. But every injective function from a finite set to itself is also surjective. We conclude that $(x_1, \ldots, x_n)$ is in the image of f. Therefore, $\overline{\mathbb{F}_p} \models \Phi_d$.

By Lemma 2.7.5, $\mathbb{C} \models \Phi_d$, which proves the theorem. ∎

Another application of quantifier elimination for algebraically closed fields concerns a weak form of Hilbert's Nullstellensatz. We have to invoke a result from algebra.

Lemma 2.7.7 (Hilbert Basis Theorem) *For every field K, every ideal of the polynomial ring $K[X_1, \ldots, X_n]$ is finitely generated.*

Proof. See, e.g., [19]. ∎

Theorem 2.7.8 (Hilbert Nullstellensatz; weak form) *Suppose K is an algebraically closed field and $K[X_1, \ldots, X_n]$ the polynomial ring over K in n variables. Suppose I is an ideal in $K[X_1, \ldots, X_n]$. Then either $1 \in I$ or there are elements $a_1, \ldots, a_n$ in K such that $g(a_1, \ldots, a_n) = 0$ for every $g \in I$.*

Proof. Suppose $1 \notin I$. Then I is contained in a maximal ideal M of $K[X_1, \ldots, X_n]$. Let K' be the algebraic closure of the field $K[X_1, \ldots, X_n]/M$. In K', the elements $\overline{X_1}, \ldots, \overline{X_n}$ have the property that $g(\overline{X_1}, \ldots, \overline{X_n}) = 0$ for every $g \in I$.

Now K is a subring of K' and both are algebraically closed fields; by quantifier elimination, K is an elementary substructure of K'. It follows that for any *finite* number $g_1, \ldots, g_m$ of elements of I,

$$K \models \exists y_1 \cdots y_n (g_1(\vec{y}) = 0 \wedge \cdots \wedge g_m(\vec{y}) = 0)$$

But by the Hilbert Basis Theorem (Lemma 2.7.7) every ideal of $K[X_1, \ldots, X_n]$ is finitely generated, so we are done. ∎

In fact, there are many applications of Logic (Model Theory) to Algebra. For a modern introduction to this area see [5].

2.8 The Löwenheim-Skolem Theorems

The theorems in this section are about the question how "big" a model of a consistent first order L-theory T can be. Of course, it can happen that T contains a sentence which forces every model of T to have cardinality $\leq n$ for some $n \in \mathbb{N}$, as we have seen. It is also possible that a theory forces models to be at least as big as a given set C: if L has constants for each element of C, and the theory has axioms

$$\neg(c = d)$$

for each pair (c, d) of distinct constants.

The upshot of this section will be that this is basically all a theory can say; if there is an infinite model of T, there will, in general, be models of T of every infinite cardinality greater than a certain cardinal number associated with the language L.

Theorem 2.8.1 (Upward Löwenheim-Skolem Theorem) *Suppose T has an infinite model. Then for any set C there is a model M of T such that there is an injective function from C into M.*

Proof. Let L_C be the language L of the theory T, together with new constants c for every $c \in C$. We consider the L_C-theory T_C, which has all the axioms of T, together with the axioms

$$\neg(c = d)$$

for every pair of distinct elements c, d of C.

If M is a model of T_C, then M is a model of T, and moreover, the assignment $c \mapsto c^M$ specifies a function from C into M, which is injective since $M \models \neg(c = d)$ (which means $c^M \neq d^M$) whenever $c \neq d$. So all we have to do is show that T_C is consistent. This is done with the Compactness Theorem.

Let $T' \subseteq T_C$ be a finite subtheory. Then in T', only finitely many constants from C occur, say $c_1, \ldots, c_n$. Now by assumption T has an infinite model N; take n distinct elements $x_1, \ldots, x_n$ from N and make N into an L_C-structure by putting $(c_i)^N = x_i$ for $i = 1, \ldots, n$ and, for $c \neq c_1, \ldots, c_n$, let c^N be an arbitrary element of N.

Then N is an L_C-structure which is a model of T'. Hence, every finite subtheory T' of T_C has a model; so T_C has a model by the Compactness Theorem. ∎

The proof can be refined to obtain "large" models of T with certain extra properties. For example, if N is an infinite model of T and C is a set, there is a model M of T, such that C embeds into M and moreover, M satisfies exactly the same L-sentences as N.

Exercise 77 Prove this last statement.
[Hint: instead of T, use the set of L-sentences which are true in N]

Thus, we see that it is relatively easy to "enlarge" models; the construction of smaller ones is a bit more involved. First we prove the following strengthening of Theorem 2.8.1.

Corollary 2.8.2 *Let N be an infinite model of a theory T, and C an arbitrary set. Then there exists a model M of T which contains N as elementary substructure and allows an injective function: $C \to M$.*

Proof. Apply Theorem 2.8.1 to the theory $E(N)$ (see exercise 71) and note that $T \subseteq E(N)$. ∎

We state now the "downward Löwenheim-Skolem Theorem". Its formulation uses the notion of *cardinality of the language* L, notation $\|L\|$, which is by definition the cardinality of the set of L-formulas. Since L is also defined as a set (the set of all constants, function symbols and relation symbols), we also have the 'ordinary cardinality' $|L|$; the following exercise compares the two.

Exercise 78 Show that $\|L\| = |L|$ if L is infinite, and that $\|L\| = \omega$ if L is finite.

Theorem 2.8.3 (Downward Löwenheim-Skolem Theorem) *Let M be an infinite model of a theory T in a language L, and let $C \subseteq M$ be a subset with $|C| \leq \|L\|$. Then there is an elementary substructure $N \preceq M$ which contains C as a subset, and has the property that $|N| \leq \|L\|$.*

Proof. We shall only prove the theorem for $\|L\| = \omega$ (so L is a countable language). The general case is proved in essentially the same way, but managing the cardinalities becomes a bit more involved. So let $C \subseteq M$ be a countable subset. We assume that $C \neq \emptyset$; the case that $C = \emptyset$ is left to you.

The submodel N will be constructed as the union of a chain of countable subsets of M:

$$C = C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots$$

This chain is constructed inductively as follows: $C = C_0$ is given. Suppose we have constructed C_k (and it is part of the induction hypothesis that C_k is countable). Let N_k be the substructure of M generated by C_k. Then N_k is countable by Exercise 70. Now for each L-formula of the form $\exists x\varphi$ with free variables $y_1, \ldots, y_n$ and each n-tuple $m_1, \ldots, m_n$ of elements of N_k such that $M \models \exists x\varphi(x, m_1, \ldots, m_n)$, choose an element m of M such that $M \models \varphi(m, m_1, \ldots, m_n)$. Let C_{k+1} be N_k together with all elements m so chosen. Since N_k is countable and there are only countably many L-formulas, C_{k+1} is countable too. This completes the construction of the chain.

Let N be the union $\bigcup_{i=0}^{\infty} C_i$. Then N is a substructure of M, because N contains c^M for every constant c of L (check!), and if f is an n-place function symbol of L and $m_1, \ldots, m_n \in N$, then for some k already $m_1, \ldots, m_n \in C_k$, so $f^M(m_1, \ldots, m_n) \in N_k \subseteq C_{k+1} \subseteq N$. And N is the union of a countable family of countable subsets of M, so N is countable and infinite; so $|N| \leq \|L\|$ as desired.

It remains to prove that N is an elementary substructure of M. For this, we use the characterization given in Exercise 72. Suppose $\exists x\varphi(x, y_1, \ldots, y_n)$ is an L-formula and $m_1, \ldots, m_n \in N$ are such that $M \models \exists x\varphi(x, m_1, \ldots, m_n)$. Then there is a natural number k such that already $m_1, \ldots, m_n \in C_k$. By construction of C_{k+1}, there is $m \in C_{k+1}$ such that $M \models \varphi(m, m_1, \ldots, m_n)$; this m is also an element of N. By Exercise 72, N is an elementary substructure of M. ∎

We wrap up this section by putting together Corollary 2.8.2 and Theorem 2.8.3 to obtain the following useful conclusion:

Corollary 2.8.4 *Let M be an infinite model of an L-theory T, and let C be a set such that $|C| \geq \|L\|$. Then there is a model N of T such that $|N| = |C|$ and moreover N and M satisfy the same L-sentences.*

Proof. First we apply Corollary 2.8.2 to obtain a model M' which contains M as elementary substructure and allows an embedding $C \to M'$. Then M and M' satisfy the same L-sentences; in particular, M' is infinite.

Next, consider the language L_C which has an extra constant for every element of C. The injective function $C \to M'$ makes M' into an L_C-structure. Clearly $|C| \leq \|L_C\|$. Applying Theorem 2.8.3 with L_C in the role of L, we see that M' contains an elementary substructure N with $C \subseteq N$ and $|N| = |C|$. Then M and N satisfy the same L-sentences. ∎

2.9 Categorical Theories

Let us consider, for an example, the theory of k-vector spaces discussed in subsection 2.4.3.

If k is a finite field, any two k-vector spaces of the same cardinality are isomorphic as k-vector spaces, for if $|V| = |W|$ then any basis for V and any basis for W must have the same cardinality (if B is a finite basis for V, then $|V| = |k|^{|B|}$; if B is infinite, then $|V| = |B|$). And any bijection between bases extends uniquely to a k-linear map which is an isomorphism of k-vector spaces.

If k is infinite, this is no longer true: let $k = \mathbb{Q}$. The $\mathbb{Q}$-vector space $\mathbb{Q}[X]$ is countable and therefore of the same cardinality as $\mathbb{Q}$, but it has infinite dimension over $\mathbb{Q}$ and hence cannot be isomorphic to $\mathbb{Q}$ as vector space over itself.

However, it is true (and follows by much the same reasoning as for finite k) that if $|V| = |W| > |k|$, then V and W are isomorphic as k-vector spaces.

Let L_k be the language of k-vector spaces, and let T_k^∞ be the theory of infinite k-vector spaces. That is, T_k^∞ has the axioms for a k-vector space together with all the sentences $\neg\phi_n$ from Example 1 in section 2.5.

Theorem 2.9.1 *The theory T_k^∞ is complete.*

Proof. Suppose that $T_k^\infty \not\models \varphi$ and $T_k^\infty \not\models \neg\varphi$, for some L_k-sentence φ. Then there are infinite k-vector spaces V and W with $V \models \neg\varphi$ and $W \models \varphi$. But then, if C is any set such that $|C| > \|L_k\|$, Corollary 2.8.4 gives us k-vector spaces V' and W', such that:

i) V' satisfies the same L_k-sentences as V;

ii) W' satisfies the same L_k-sentences as W;

iii) $|V'| = |W'| = |C|$

Then as we have just argued, V' and W' must be isomorphic as k-vector spaces, yet $V' \models \neg\varphi$ by i), and $W' \models \varphi$ by ii). But this is clearly impossible, by exercises 66 and 67. ∎

Exercise 79 For another proof of the fact that T_k^∞ is complete: prove that T_k^∞ has quantifier elimination.

Definition 2.9.2 Let κ be a cardinal number. An L-theory T is called *κ-categorical* if for every pair M, N of models of T of cardinality κ, there is an isomorphism between M and N.

As we have seen, the theory of infinite k-vector spaces is κ-categorical if $\kappa > |k|$.

The following theorem generalizes the argument above that the theory T_k^∞ must be complete; its proof is therefore left as an exercise.

Theorem 2.9.3 (Łos-Vaught Test) *Suppose T is an L-theory which only has infinite models, and suppose T is κ-categorical for some $\kappa \geq \|L\|$. Then T is complete.*

Exercise 80 Prove Theorem 2.9.3.

We conclude this chapter by giving an example of a theory which is ω-categorical; the theory of *dense linear orders without end-points*. In this example it is not so much the result which is important, as the technique of the proof, which is known as Cantor's *back-and-forth argument*.

Definition 2.9.4 The theory T_d of dense linear orders without end-points is formulated in a language with just one binary relation symbol $<$, and has the following axioms:

$$\begin{aligned}
\forall x \neg(x < x) &\quad \text{irreflexivity}\\
\forall xyz(x < y \wedge y < z \rightarrow x < z) &\quad \text{transitivity}\\
\forall xy(x < y \vee x = y \vee y < x) &\quad \text{linearity}\\
\forall xy(x < y \rightarrow \exists z(x < z \wedge z < y)) &\quad \text{density}\\
\forall x \exists yz(y < x \wedge x < z) &\quad \text{no end points}
\end{aligned}$$

Theorem 2.9.5 (Cantor) *The theory T_d is ω-categorical.*

Proof. We have to show that any two countably infinite models M and N of T_d are isomorphic.

Start by choosing enumerations $M = \{m_0, m_1, \ldots\}$ and $N = \{n_0, n_1, \ldots\}$ of M and N.

We shall construct an isomorphism $\beta : M \to N$ as the union of a chain of order-preserving bijective functions between finite sets:

$$\begin{array}{ccccccc} M_0 & \longrightarrow & M_1 & \longrightarrow & M_2 & & \cdots \\ \downarrow{\scriptstyle \beta_0} & & \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} & & \\ N_0 & \longrightarrow & N_1 & \longrightarrow & N_2 & & \cdots \end{array}$$

such that the horizontal arrows are inclusions $M_k \subseteq M_{k+1}$, $N_k \subseteq N_{k+1}$, and β_k is the restriction of β_{k+1} to M_k. Moreover, we shall make sure that for each k, $\{m_0, \ldots, m_k\} \subseteq M_k$ and $\{n_0, \ldots, n_k\} \subseteq N_k$, so at the end we obtain a bijective function from M to N.

Let $M_0 = \{m_0\}$, $N_0 = \{n_0\}$ and β_0 the unique bijection.

Suppose $\beta_k : M_k \to N_k$ has been constructed, as order-preserving bijection. We construct M_{k+1}, N_{k+1} and β_{k+1} in two stages:

Stage 1. If $m_{k+1} \in M_k$, we do nothing in this stage and proceed to stage 2. If $m_{k+1} \notin M_k$ there are two possibilities:

- Either m_{k+1} lies below all elements of M_k, or above all these elements. In this case, we use the axiom "no end-points" to find an element $n \in N$ which has the same relative position with respect to N_k; we add m_{k+1} to M_k, n to N_k and put $\beta_{k+1}(m_{k+1}) = n$.

- m_{k+1} lies somewhere between the elements of M_k. Then by axiom "linearity" and the fact that M_k is finite, there is a greatest element $m_j \in M_k$ and a least $m_l \in M_k$ such that $m_j < m_{k+1} < m_l$. We use axiom "density" to pick an element n of N with $\beta_k(m_j) < n < \beta_k(m_l)$; we add m_{k+1} to M_k, n to N_k and put $\beta_{k+1}(m_{k+1}) = n$.

Stage 2. Here we do the symmetric thing with n_{k+1} and the inverse of the finite bijective function we have obtained after stage 1. After completing stage 2 we let $\beta_{k+1} : M_{k+1} \to N_{k+1}$ be the union of β_k and what we have added in stages 1 and 2.

This completes the construction of β_{k+1} and hence, inductively, of our chain of finite bijective, order-preserving functions. ∎

Exercise 81 Show that the theory T_d is complete.

Exercise 82 Use Lemma 2.7.3 to prove, that the theory T_d has quantifier elimination.

Exercise 83 Show that the theory T_d is *not* 2^ω-categorical.

Exercise 84 Use Theorem 2.9.5 for another proof that $\mathbb{R}$ is not countable.

Chapter 3

Proofs

In Chapter 2, we have introduced languages and formulas as mathematical objects: formulas are just certain finite sequences of elements of a certain set. Given a specific model, such formulas become mathematical statements via the definition of truth in that model.

In mathematical reasoning, one often observes that one statement "follows" from another, without reference to specific models or truth, as a purely "logical" inference. More generally, statements can be conjectures, assumptions or intermediate conclusions in a mathematical argument.

In this chapter we shall give a formal, abstract definition of a concept called 'proof'. A proof will be a finite object which has a number of *assumptions* which are formulas, and a *conclusion* which is a formula. Given a fixed language L, there will be a set of all proofs in L, and we shall be able to prove the *Completeness Theorem*:

> For a set Γ of L-sentences and an L-sentence ϕ, the relation $\Gamma \models \phi$ holds if and only if there exists a proof in L with conclusion ϕ and assumptions from the set Γ.

Recall that $\Gamma \models \phi$ was defined as: for every L-structure M which is a model of Γ, it holds that $M \models \phi$.

Therefore, the Completeness Theorem reduces a universal ("for all") statement about a large class of structures, to an existential ("there is") statement about one set (the set of proofs). Furthermore, we shall see that proofs are built up by rules that can be interpreted as elementary reasoning steps (we shall not go into the philosophical significance of this). Finally, we wish to remark that it can be effectively tested whether or not an object of appropriate kind is a 'proof', and that the set of all sentences ϕ such that

$\Gamma \models \phi$ can be effectively generated by a computer (we refer to a lecture course in Recursion Theory for a precise meaning of this, e.g. [4]).

Mathematicians who devised definitions of a notion of 'formal proof' include Frege, Russell and Hilbert; but by far the most influential one is due to Gerhard Gentzen (1909–1945). Gentzen gave in fact two widely used systems, of which we present the first below; this system was called by him 'natural deduction' (*Kalkül des natürlichen Schließens*,[9]). For biographical information on Gentzen, whose life was shaped to a great extent by the political developments in Germany during the period 1933–1945, see [21].

The Completeness Theorem was proved by Kurt Gödel in 1929 ([10]), but our proof below is based on that of Leon Henkin ([14]).

3.1 Proof Trees

In a well-structured mathematical argument, it is clear at every point what the conclusion reached so far is, what the current assumptions are and on which intermediate results each step depends.

We model this mathematically with the concept of a *tree*.

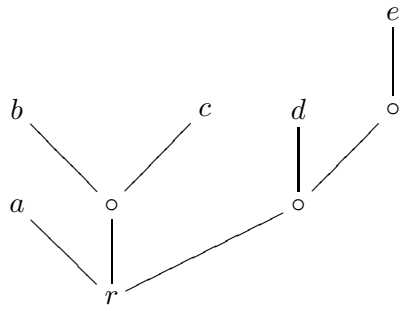
Definition 3.1.1 A *tree* is a partial order $(T, \leq)$ which has a least element, and is such that for every $x \in T$, the set

$$\downarrow(x) \;\equiv\; \{y \in T \,|\, y \leq x\}$$

is well-ordered by the relation $\leq$.

We shall only be concerned with *finite* trees; that is, finite posets T with least element, such that each $\downarrow(x)$ is linearly ordered.

This is an example of a tree:



We use the following dendrological language when dealing with trees: the least element is called the *root* (in the example above, the element marked

r), and the maximal elements are called the *leaves* (in the example, the elements marked a, b, c, d, e).

When we see a proof as a tree, the leaves are the places for the assumptions, and the root is the place for the conclusion. The information that the assumptions give, may be compared to the carbon dioxide in real trees, which finds its way from the leaves to the root.

The following exercise gives some alternative ways of characterizing trees.

Exercise 85 a) Show that a finite tree is the same thing as a finite sequence of nonempty finite sets and functions

$$A_n \to \cdots \to A_1 \to A_0$$

where A_0 is a one-element set.

b) Show that a finite tree is the same thing as a finite set V together with a function $f : V \to V$ which has the properties that f has exactly one fixed point $r = f(r)$, and there are no elements $x \neq r$ such that $x = f^n(x)$ for some $n \in \mathbb{N}$.

c) If V is a finite set, a *hierarchy* on V is a collection $\mathcal{C}$ of subsets of V, such that $V \in \mathcal{C}$, and for any two elements $C_1 \neq C_2$ of $\mathcal{C}$, we have $C_1 \subset C_2$ or $C_2 \subset C_1$ or $C_1 \cap C_2 = \emptyset$. Let us call $\mathcal{C}$ a T_0-*hierarchy* if for each $x, y \in V$ with $x \neq y$, there is $C \in \mathcal{C}$ such that either $x \in C$ and $y \notin C$, or $y \in C$ and $x \notin C$. Call $\mathcal{C}$ *connected* if there is an element $r \in V$ such that the only element $C \in \mathcal{C}$ such that $r \in C$, is V itself.

i) Show that if $\mathcal{C}$ is a connected T_0-hierarchy on V, then the relation

$$x \leq y \text{ if and only if for all } C \in \mathcal{C},\ x \in C \text{ implies } y \in C$$

defines a partial order on V which is a tree; and moreover, for every $x \in V$, the set $\{y \in V \,|\, x \leq y\}$ is an element of $\mathcal{C}$.

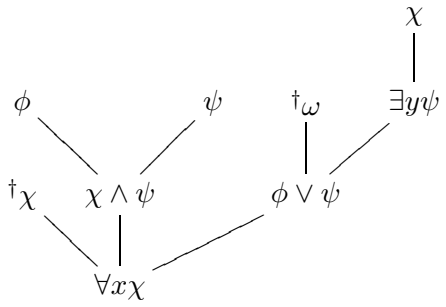
ii) Show also that if $\leq$ is a partial order on a finite set V which is a tree, then the set of subsets of V

$$\{\{y \in V \,|\, x \leq y\} \,|\, x \in V\}$$

is a connected T_0-hierarchy on V.

We shall be interested in L-*labelled* trees; that is: trees where the elements have 'names' which are L-formulas or formulas marked with a symbol †. For

example:



The following definition formalizes this:

Definition 3.1.2 Let L be a language. We fix an extra symbol †. A *marked* L-formula is a pair $(\dagger, \varphi)$; we shall write ${}^\dagger\varphi$ for $(\dagger, \varphi)$. Let $F(L)$ be the set of L-formulas, and let ${}^\dagger F(L)$ be the disjoint union of $F(L)$ and the set $\{\dagger\} \times F(L)$ of marked L-formulas.

An *L-labelled* tree is a finite tree T together with a function f from T to the set ${}^\dagger F(L)$, such that the only elements x of T such that $f(x)$ is a marked formula, are leaves of T.

The function f is called the *labelling function*, and $f(x)$ is called the *label* of x.

Among the L-labelled trees, we shall single out a set of 'proof trees'. The definition (Definition 3.1.3 below) uses the following two operations on L-labelled trees:

1). *Joining a number of labelled trees by adding a new root labelled ϕ*
Suppose we have a finite number of labelled trees $T_1, \ldots, T_k$ with labelling functions $f_1, \ldots, f_k$. Let T be the disjoint union $T_1 + \cdots + T_k$ together with a new element r, and ordered as follows: $x \leq y$ if and only if either $x = r$ or for some i, $x, y \in T_i$ and $x \leq y$ holds in T_i.

Let the labelling function f on T be such that it extends each f_i on T_i and has $f(r) = \phi$.

We denote this construction by $\Sigma(T_1, \ldots, T_k; \phi)$.

2). *Adding some markings*
Suppose T is a labelled tree with labelling function f. If V is a set of leaves of T, we may modify f to f' as follows: $f'(x) = f(x)$ if $x \notin V$ or $f(x)$ is a marked formula; otherwise, $f'(x) = (\dagger, f(x))$.

We denote this construction by $Mk(T; V)$.

Exercise 86 Show that, up to equivalence, every L-labelled tree can be constructed by a finite number of applications of these two constructions, starting from one element trees with unmarked labels.
Here we regard two L-labelled trees as equivalent if the underlying trees are isomorphic as partial orders, and they have the same labelling modulo this isomorphism.

For the rest of this section, we shall assume that we have a fixed language L which we won't mention (we say 'labelled' and 'formula' instead of 'L-labelled', 'L-formula' etc.). Let us also repeat that for us from now on, 'tree' means *finite* tree.

If T is a labelled tree with labelling function f, root r and leaves $a_1, \ldots, a_n$, we shall call the formula $f(r)$ (if it is a formula, that is: unmarked) the *conclusion* of T and the formulas $f(a_i)$ the *assumptions* of T. Assumptions of the form ${}^{\dagger}\varphi$ are called *eliminated assumptions*.

We can now give the promised definition of 'proof tree'. Instead of reading through the definition in one go, you are advised to work through a few clauses, and then have a look at the examples given after the definition; referring back to it when necessary.

Definition 3.1.3 The set $\mathcal{P}$ of *proof trees* is the smallest set of labelled trees, satisfying:

Ass For every formula φ, the tree with one element r and labelling function $f(r) = \varphi$, is an element of $\mathcal{P}$. Note that φ is both assumption and conclusion of this tree. We call this tree an *assumption tree*.

$\wedge I$ If T_1 and T_2 are elements of $\mathcal{P}$ with conclusions φ_1 and φ_2 respectively, then $\Sigma(T_1, T_2; \varphi_1 \wedge \varphi_2)$ is an element of $\mathcal{P}$. We say this tree was formed by $\wedge$-*introduction*.

$\wedge E$ If T is an element of $\mathcal{P}$ with conclusion $\phi \wedge \psi$ then both $\Sigma(T; \phi)$ and $\Sigma(T; \psi)$ are elements of $\mathcal{P}$. These are said to be formed by $\wedge$-*elimination*.

$\vee I$ If T is an element of $\mathcal{P}$ with conclusion φ, and ψ is any formula, then both $\Sigma(T; \varphi \vee \psi)$ and $\Sigma(T; \psi \vee \varphi)$ are elements of $\mathcal{P}$. We say these are formed by $\vee$-introduction.

$\vee E$ Suppose that T, S_1, S_2 are elements of $\mathcal{P}$ such that the conclusion of T is $\varphi \vee \psi$ and the conclusions of S_1 and S_2 are the same (say, χ). Let V_1

be the subset of the leaves of S_1 labelled φ, and let V_2 be the subset of the leaves of S_2 labelled ψ. Let $S_1' = Mk(S_1; V_1)$, $S_2' = Mk(S_2; V_2)$. Then $\Sigma(T, S_1', S_2'; \chi)$ is an element of $\mathcal{P}$ ($\vee$-elimination).

$\rightarrow I$ Suppose T is an element of $\mathcal{P}$ with conclusion φ, and let ψ be any formula. Let V be the subset of the set of leaves of T with label ψ, and $T' = Mk(T; V)$. Then $\Sigma(T'; \psi \rightarrow \varphi)$ is an element of $\mathcal{P}$ ($\rightarrow$-introduction).

$\rightarrow E$ Suppose T and S are elements of $\mathcal{P}$ with conclusions $\varphi \rightarrow \psi$ and φ, respectively. Then $\Sigma(T, S; \psi)$ is an element of $\mathcal{P}$ ($\rightarrow$-elimination).

$\neg I$ Suppose T is an element of $\mathcal{P}$ with conclusion $\bot$. Let φ be any formula, and V be the subset of the set of leaves of T labelled φ. Let $T' = Mk(T; V)$. Then $\Sigma(T'; \neg\varphi)$ is an element of $\mathcal{P}$ ($\neg$-introduction).

$\neg E$ Suppose T and S are elements of $\mathcal{P}$ with conclusions φ and $\neg\varphi$, respectively. Then $\Sigma(T, S; \bot)$ is an element of $\mathcal{P}$ ($\neg$-elimination).

$\bot E$ Suppose T is an element of $\mathcal{P}$ with conclusion $\bot$. Let φ be any formula, and V the subset of the set of leaves of T labelled $\neg\varphi$. Let $T' = Mk(T; V)$. Then $\Sigma(T'; \varphi)$ is an element of $\mathcal{P}$ ($\bot$-elimination; one also hears *reductio ad absurdum* or *proof by contradiction*).

Subst Suppose T and S are elements of $\mathcal{P}$ such that the conclusion of T is $\varphi[t/x]$ and the conclusion of S is $(t = s)$. Suppose furthermore that the substitutions $\varphi[t/x]$ and $\varphi[s/x]$ are defined (recall from Chapter 2: this means that no variable in t or s becomes bound in the substitution). Then $\Sigma(T, S; \varphi[s/x])$ is an element of $\mathcal{P}$ (Substitution).

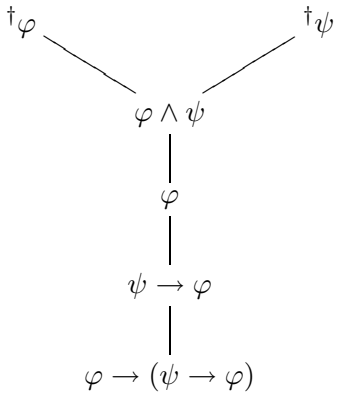
$\forall I$ Suppose T is an element of $\mathcal{P}$ with conclusion $\varphi[u/v]$, where u is a variable which does not occur in any unmarked assumption of T or in the formula $\forall v\varphi$ (and is not bound in φ). Then $\Sigma(T; \forall v\varphi)$ is an element of $\mathcal{P}$ ($\forall$-introduction).

$\forall E$ Suppose T is an element of $\mathcal{P}$ with conclusion $\forall u\varphi$, and t is a term such that the substitution $\varphi[t/u]$ is defined. Then $\Sigma(T; \varphi[t/u])$ is an element of $\mathcal{P}$ ($\forall$-elimination).

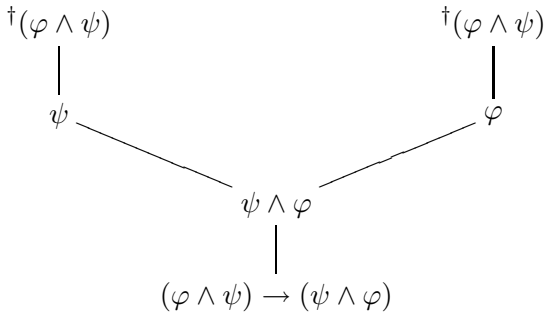
$\exists I$ Suppose T is an element of $\mathcal{P}$ with conclusion $\varphi[t/u]$, and suppose the substitution $\varphi[t/u]$ is defined. Then $\Sigma(T; \exists u\varphi)$ is an element of $\mathcal{P}$ ($\exists$-introduction).

$\exists E$ Suppose T and S are elements of $\mathcal{P}$ with conclusions $\exists x\varphi$ and χ, respectively. Let u be a variable which doesn't occur in φ or χ, and is such that the only unmarked assumptions of S in which u occurs, are of the form $\varphi[u/x]$. Let V be the set of leaves of S with label $\varphi[u/x]$, and $S' = Mk(S; V)$. Then $\Sigma(T, S'; \chi)$ is an element of $\mathcal{P}$ ($\exists$-elimination).

Examples. The following labelled trees are proof trees. Convince yourself of this, and find out at which stage labels have been marked:
a)

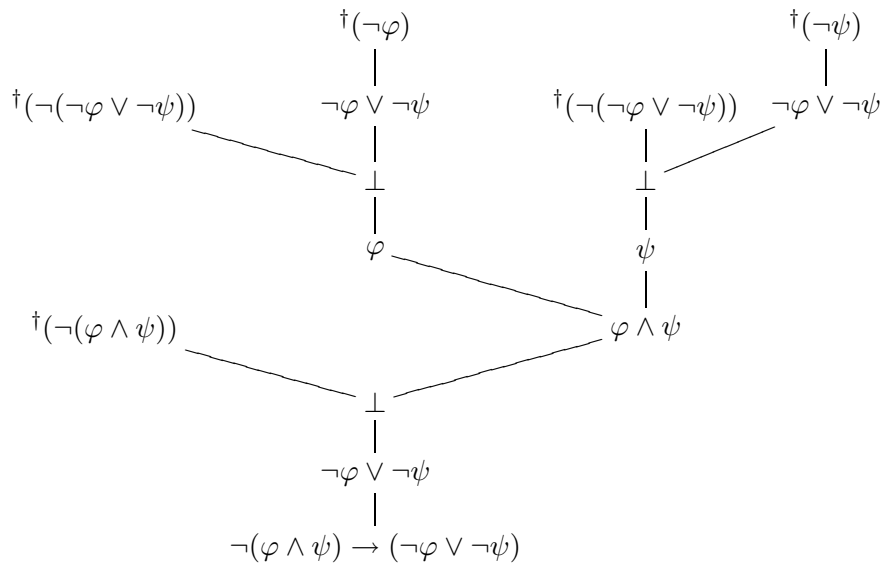


b)

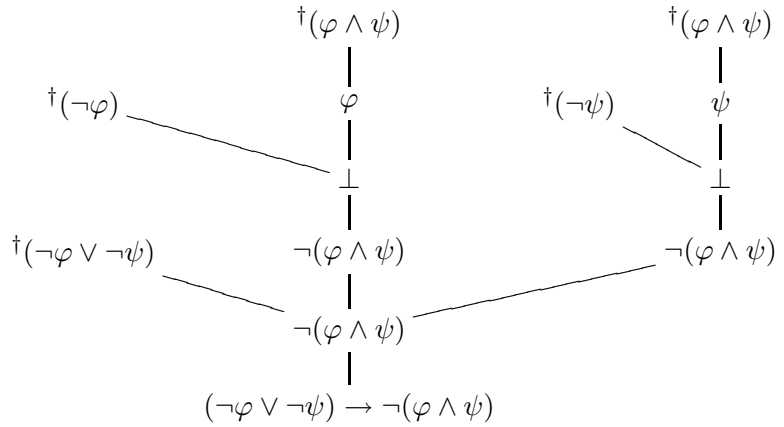


c)

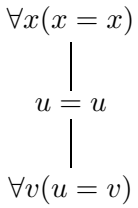
"Ex falso sequitur quodlibet"
d)



e)



f) The following "example" illustrates why, in formulating the rule $\forall I$, we have required that the variable u does not occur in the formula $\forall v\varphi$. For, let φ be the formula $u = v$. Consider that $(u = v)[u/v]$ is $u = u$, so were it not for this requirement, the following tree would be a valid proof tree:



Clearly, we would not like to accept this as a valid proof!

Definition 3.1.4 We define the relation

$$\Gamma \vdash \varphi$$

as: there is a proof tree with conclusion φ and whose unmarked assumptions are either elements of Γ or of the form $\forall x(x = x)$ for some variable x. We abbreviate $\{\varphi\} \vdash \psi$ as $\varphi \vdash \psi$, we write $\vdash \psi$ for $\emptyset \vdash \psi$, and $\Gamma, \varphi \vdash \psi$ for $\Gamma \cup \{\varphi\} \vdash \psi$.

Exercise 87 (Deduction Theorem) Prove, that the relation $\Gamma, \varphi \vdash \psi$ is equivalent to $\Gamma \vdash \varphi \to \psi$.

3.1.1 Variations and Examples

One variation in the notation of proof trees is, to write the name of each construction step next to the labels in the proof tree.

For example, the proof tree

$$\begin{array}{c} {}^{\dagger}\varphi \\ \vdots \\ \varphi \to \varphi \end{array}$$

is constructed from the assumption tree φ by $\to$-introduction (at which moment the assumption φ is marked). One could make this explicit by writing

$$\begin{array}{c} {}^{\dagger}\varphi \\ \vdots \\ \to I\, \varphi \to \varphi \end{array}$$

Another notational variation is one that is common in the literature: the ordering is indicated by horizontal bars instead of vertical or skew lines, and next to these bars, it is indicated by which of the constructions of Definition 3.1.3, the new tree results from the old one(s). Assumptions are numbered, such that different assumptions have different numbers, but distinct occurrences of the same assumption may get the same number. If, in the construction, assumptions are marked, this is indicated by their numbers next to the name of the construction.

In this style, the proof tree

$$\begin{array}{c} {\dagger}\varphi \\ | \\ \varphi \to \varphi \end{array}$$

looks as follows:

$$\frac{{\dagger}\varphi^1}{\varphi \to \varphi} \to I, 1$$

We shall call this a *decorated proof tree*. Although (or maybe: because!) they contain some redundant material, decorated proof trees are easier to read and better suited to practice the construction of proof trees.

In decorated style, examples a)–e) of the previous section are as follows:

a)

$$\dfrac{\dfrac{\dfrac{{\dagger}\varphi^1 \qquad {\dagger}\psi^2}{\varphi \wedge \psi} \wedge I}{\varphi} \wedge E}{\dfrac{\psi \to \varphi}{\varphi \to (\psi \to \varphi)} \to I, 2} \to I, 1$$

The assumption φ, numbered 1, gets marked when construction $\to I$ with number 1 is performed; etc.

b)

$$\dfrac{\dfrac{\dfrac{{\dagger}\varphi \wedge \psi^1}{\psi} \wedge E \qquad \dfrac{{\dagger}\varphi \wedge \psi^1}{\varphi} \wedge E}{\psi \wedge \varphi} \wedge I}{(\varphi \wedge \psi) \to (\psi \wedge \varphi)} \to I, 1$$

c)

$$\frac{\bot}{\varphi} \bot E$$

d)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\dagger\neg(\neg\varphi\vee\neg\psi)^3}\quad\dfrac{\dfrac{}{\dagger\neg\varphi^1}}{\neg\varphi\vee\neg\psi}\vee I}{\bot}\neg E}{\varphi}\bot E,1\quad\dfrac{\dfrac{\dfrac{}{\dagger\neg(\neg\varphi\vee\neg\psi)^3}\quad\dfrac{\dfrac{}{\dagger\neg\psi^2}}{\neg\varphi\vee\neg\psi}\vee I}{\bot}\neg E}{\psi}\bot E,2}{\varphi\wedge\psi}\wedge I}{\bot}\neg E}{\neg\varphi\vee\neg\psi}\bot E,3}{\neg(\varphi\wedge\psi)\to(\neg\varphi\vee\neg\psi)}\to I,4$$

e)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\dagger\neg\varphi\vee\neg\psi^5}\quad\dfrac{\dfrac{\dfrac{\dfrac{}{\dagger\neg\varphi^3}\quad\dfrac{\dfrac{}{\dagger\varphi\wedge\psi^1}}{\varphi}\wedge E}{\bot}\neg E}{\neg(\varphi\wedge\psi)}\neg I,1\quad\dfrac{\dfrac{\dfrac{}{\dagger\neg\psi^4}\quad\dfrac{\dfrac{}{\dagger\varphi\wedge\psi^2}}{\psi}\wedge E}{\bot}\neg E}{\neg(\varphi\wedge\psi)}\neg I,2}{\neg(\varphi\wedge\psi)}\vee E,3,4}{(\neg\varphi\vee\neg\psi)\to\neg(\varphi\wedge\psi)}\to I,5$$

Some more examples:

f) A proof tree for $t=s\vdash s=t$:

$$\dfrac{\dfrac{\dfrac{}{\forall x(x=x)}\forall E}{t=t}\quad t=s}{s=t}\text{ Subst}$$

The use of Subtitution is justified since $t=t$ is $(u=t)[t/u]$. Quite similarly, we have a proof tree for $\{t=s,s=r\}\vdash t=r$:

$$\dfrac{t=s\qquad s=r}{t=r}\text{ Subst}$$

g)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\dagger\neg\exists x\varphi(x)^2}\quad\dfrac{\dfrac{}{\dagger\varphi(y)^1}}{\exists x\varphi(x)}\exists I}{\bot}\neg E}{\neg\varphi(y)}\neg I,1}{\forall x\neg\varphi(x)}\forall I}{\neg\exists x\varphi(x)\to\forall x\neg\varphi(x)}\to I,2$$

You should check why application of $\forall I$ is justified in this tree.

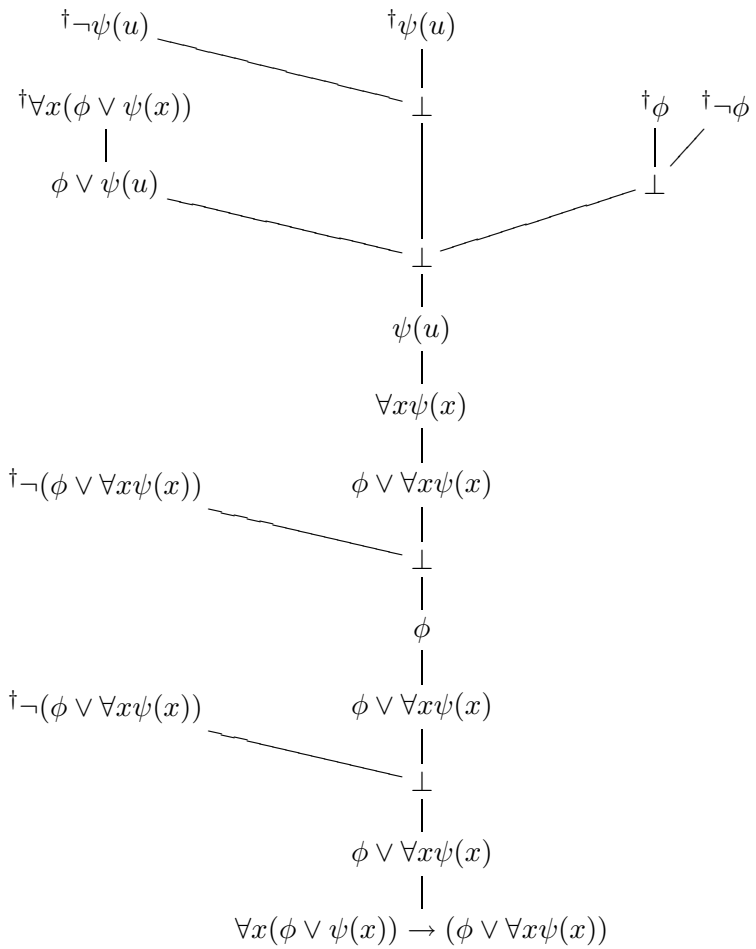
h) The following tree gives an example of the $\exists E$-construction:

$$\dfrac{\dfrac{\dfrac{{}^{\dagger}\exists x\varphi(x)^2 \qquad \dfrac{\dfrac{{}^{\dagger}\forall x\neg\varphi(x)^3}{\neg\varphi(y)}\,\forall E \qquad {}^{\dagger}\varphi(y)^1}{\bot}\,\neg E}{\bot}\,\exists E, 1}{\neg\exists x\varphi(x)}\,\neg I, 2}{\forall x\neg\varphi(x) \to \neg\exists x\varphi(x)}\,\to I, 3$$

i)

$$\dfrac{\dfrac{\dfrac{{}^{\dagger}\neg\forall x\neg\varphi(x)^3 \qquad \dfrac{\dfrac{\dfrac{{}^{\dagger}\neg\exists x\varphi(x)^2 \qquad \dfrac{{}^{\dagger}\varphi(y)^1}{\exists x\varphi(x)}\,\exists I}{\bot}\,\neg E}{\neg\varphi(y)}\,\neg I, 1}{\forall x\neg\varphi(x)}\,\forall I}{\bot}\,\neg E}{\exists x\varphi(x)}\,\bot E, 2}{\neg\forall x\neg\varphi(x) \to \exists x\varphi(x)}\,\to I, 2$$

j) The following tree is given in undecorated style; it is a good exercise to decorate it. It is assumed that the variables x and u do not occur in ϕ; check that without this condition, it is not a correct proof tree:



A bit of heuristics. When faced with the problem of constructing a proof tree which has a specified set of unmarked assumptions Γ and a prescribed conclusion ϕ (often formulated as: "construct a proof tree for $\Gamma \vdash \phi$"), it is advisable to use the following heuristics (but there is no guarantee that they work! Or that they produce the most efficient proof):

> If ϕ is a conjunction $\phi_1 \wedge \phi_2$, break up the problem into two problems $\Gamma \vdash \phi_1$ and $\Gamma \vdash \phi_2$;
>
> If ϕ is an implication $\phi_1 \to \phi_2$, transform the problem into $\Gamma \cup \{\phi_1\} \vdash \phi_2$;
>
> If ϕ is a negation $\neg\psi$, transform into $\Gamma \cup \{\psi\} \vdash \bot$;
>
> If ϕ is of form $\forall x\psi(x)$, transform into $\Gamma \vdash \psi(u)$;

If ϕ is a disjunction $\phi_1 \vee \phi_2$, one may try the transformation into $\Gamma \vdash \neg\phi_1 \to \phi_2$ or $\Gamma \vdash \neg\phi_2 \to \phi_1$;

In all other (non-obvious) cases, try $\Gamma \cup \{\neg\phi\} \vdash \bot$.

Exercise 88 Construct proof trees for the equivalences of Exercise 40. Recall that $\leftrightarrow$ is an abbreviation: for example, a proof tree for $\vdash (\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$ will be constructed out of two proof trees, one for $\{\varphi \to \psi\} \vdash \neg\varphi \vee \psi$, and one for $\{\neg\varphi \vee \psi\} \vdash \varphi \to \psi$, by applying $\to$- and $\wedge$-introduction.

3.1.2 Induction on Proof Trees

Since the set $\mathcal{P}$ of proof trees is defined as the *least* set of labelled trees which contains the assumption trees φ and is closed under a number of constructions (definition 3.1.3), $\mathcal{P}$ is susceptible to proofs by *induction* over proof trees: if $\mathcal{A}$ is any set of labelled trees which contains all φ and is closed under the constructions, then $\mathcal{A}$ contains $\mathcal{P}$ as a subset.

Some examples of properties of proof trees one can prove by this method:

1. No proof tree has a marked formula at the root.
2. In every proof tree T, for every $x \in T$ there are at most 3 elements of T directly above x (we say that every proof tree is a *ternary tree*).
3. If T is a proof tree for $\Gamma \vdash \varphi[c/u]$, where c is a constant that does not occur in Γ, and v is a variable which doesn't occur anywhere in T, then there is a proof tree for $\Gamma \vdash \varphi[v/u]$. It then follows by $\forall I$ that there is a proof tree for $\Gamma \vdash \forall u\varphi$.

Exercise 89 Carry out the proofs of these statements. For 3, prove the following: if T, c and v are as in the hypothesis, and $T[v/c]$ results from T by replacing c by v throughout, then $T[v/c]$ is also a proof tree, and is a proof tree for $\Gamma \vdash \varphi[v/u]$.

In the proof of the Soundness Theorem (section 3.2 below) we shall also apply induction over proof trees.

Exercise 90 Let $\Gamma \vdash_H \varphi$ be defined as the least relation between sets of L-formulas Γ and L-formulas φ, such that the following conditions are satisfied:

i) $\Gamma \vdash_H \forall x(x = x)$ always;

ii) If $\varphi \in \Gamma$, then $\Gamma \vdash_H \varphi$;

iii) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \psi$ then $\Gamma \vdash_H (\varphi \wedge \psi)$, and conversely;

iv) if $\Gamma \vdash_H \varphi$ or $\Gamma \vdash_H \psi$, then $\Gamma \vdash_H (\varphi \vee \psi)$;

v) if $\Gamma \cup \{\varphi\} \vdash_H \chi$ and $\Gamma \cup \{\psi\} \vdash_H \chi$, then $\Gamma \cup \{\varphi \vee \psi\} \vdash_H \chi$;

vi) if $\Gamma \cup \{\varphi\} \vdash_H \bot$, then $\Gamma \vdash_H \neg\varphi$;

vii) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \neg\varphi$ then $\Gamma \vdash_H \bot$;

viii) if $\Gamma \cup \{\neg\varphi\} \vdash_H \bot$ then $\Gamma \vdash_H \varphi$;

ix) if $\Gamma \cup \{\varphi\} \vdash_H \psi$ then $\Gamma \vdash_H \varphi \to \psi$;

x) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \varphi \to \psi$ then $\Gamma \vdash_H \psi$;

xi) if $\Gamma \vdash_H \psi(u)$ and u does not occur in Γ or in $\forall x\psi(x)$, then $\Gamma \vdash_H \forall x\psi(x)$;

xii) if $\Gamma \vdash_H \forall x\psi(x)$ then if $\psi[t/x]$ is defined, $\Gamma \vdash_H \psi[t/x]$;

xiii) if $\psi[t/x]$ is defined and $\Gamma \vdash_H \psi[t/x]$, then $\Gamma \vdash_H \exists x\psi(x)$;

xiv) if $\Gamma \cup \{\psi(u)\} \vdash_H \chi$ and u does not occur in Γ, χ or $\exists x\psi(x)$, then $\Gamma \cup \{\exists x\psi(x)\} \vdash_H \chi$;

xv) if the substitutions $\varphi[s/x]$ and $\varphi[t/x]$ are defined, $\Gamma \vdash_H \varphi[t/x]$ and $\Gamma \vdash_H t = s$, then $\Gamma \vdash_H \varphi[s/x]$.

Show that the relation $\Gamma \vdash_H \varphi$ coincides with the relation $\Gamma \vdash \varphi$ from Definition 3.1.4.

3.2 Soundness and Completeness

We compare the relation $\Gamma \vdash \phi$ from Definition 3.1.4 to the relation $\Gamma \models \phi$ from Chapter 2; recall that the latter means: in every model M of Γ, the sentence ϕ holds.

In this section we shall prove the following two theorems, for Γ a set of sentences, and ϕ a sentence:

Theorem 3.2.1 (Soundness Theorem) *If* $\Gamma \vdash \phi$ *then* $\Gamma \models \phi$.

Theorem 3.2.2 (Completeness Theorem; Gödel, 1929) *If* $\Gamma \models \phi$ *then* $\Gamma \vdash \phi$.

The Soundness Theorem follows easily from the following lemma:

Lemma 3.2.3 *Suppose T is an L-labelled proof tree with unmarked assumptions $\varphi_1, \ldots, \varphi_n$ and conclusion ψ; let $u_1, \ldots, u_k$ be a list of all variables that are free in at least one of $\varphi_1, \ldots, \varphi_n, \psi$. Then for every L-structure M and any k-tuple $m_1, \ldots, m_k$ of elements of M, we have:*

$$\begin{array}{c} \textit{If for all } i,\ 1 \leq i \leq n,\ M \models \varphi_i[m_1/u_1, \ldots, m_k/u_k], \textit{ then} \\ M \models \psi[m_1/u_1, \ldots, m_k/u_k]. \end{array}$$

Exercise 91 Prove yourself, that Lemma 3.2.3 implies Theorem 3.2.1.

Proof. Lemma 3.2.3 is proved by a straightforward induction on proof trees: let $\mathcal{A}$ be the set of L-labelled proof trees which satisfy the condition of the lemma, w.r.t. every L-structure M.

Clearly, $\mathcal{A}$ contains every assumption tree φ. Now we should show that $\mathcal{A}$ is closed under all the constructions of definition 3.1.3. In most cases, a quick inspection suffices. We shall treat a few cases, leaving the others for you to check.

Let us write $\varphi_i[\vec{m}/\vec{u}]$ for $\varphi_i[m_1/u_1, \ldots, m_k/u_k]$.

Suppose T is formed by $\rightarrow$-introduction from $S \in \mathcal{A}$; say S has conclusion ψ and T has conclusion $\phi \rightarrow \psi$. Suppose the unmarked assumptions of S other than ϕ, are $\varphi_1, \ldots, \varphi_n$, and let $u_1, \ldots, u_k$ be a list of variables as in the lemma, for S. Then if M is an L-structure and $m_1, \ldots, m_k \in M$, the induction hypothesis (viz., $S \in \mathcal{A}$) gives us that if $M \models \phi[\vec{m}/\vec{u}]$ and for all $i \leq n$, $M \models \varphi_i[\vec{m}/\vec{u}]$, then $M \models \psi[\vec{m}/\vec{u}]$. Then clearly, if $M \models \varphi_i[\vec{m}/\vec{u}]$ for each $i \leq n$, also $M \models (\phi \rightarrow \psi)[\vec{m}/\vec{u}]$. So $T \in \mathcal{A}$.

Suppose T is formed by $\forall$-introduction from $S \in \mathcal{A}$. Suppose S has unmarked assumptions $\varphi_1, \ldots, \varphi_n$ and conclusion $\psi(v)$, and v does not occur in $\varphi_1, \ldots, \varphi_n$. The induction hypothesis gives us that for any L-structure M and any tuple $\vec{m}, p$ from M, if for each $i \leq n$ $M \models \varphi_i[\vec{m}/\vec{u}]$ then $M \models \psi[\vec{m}/\vec{u}, p/v]$. Therefore, if for each $i \leq n$ $M \models \varphi_i[\vec{m}/\vec{u}]$, then for all $p \in M$, $M \models \psi[\vec{m}/\vec{u}, p/v]$; in other words $M \models (\forall x \psi[x/v])[\vec{m}/\vec{u}]$. Hence $T \in \mathcal{A}$.

Suppose T is formed by $\exists$-elimination from elements S, S' of $\mathcal{A}$. So the conclusion of S is $\exists v \phi$, the conclusion of S' is χ, and S' has possibly unmarked assumptions of form $\phi[w/x]$ where w does not occur in any other unmarked assumption of S', nor in ϕ, nor in χ. Let $\vec{u}$ be the list of free variables appearing in an unmarked assumption of T or in χ. Let $\vec{m}$ be a tuple of elements of M of the same length as $\vec{u}$.

Suppose that $M \models \varphi[\vec{m}/\vec{u}]$ for each unmarked assumption φ of T. We need to show that $M \models \chi[\vec{m}]$. A little care is needed, for when we wish to

apply the induction hypothesis to the trees S and S', we face the apparent problem that the formula $\exists v\phi$, which may not occur as unmarked assumption or as conclusion of T, may contain free variables $\vec{y}$ not among the $\vec{u}$. So let's write $\exists v\phi(\vec{u}, \vec{y}, v)$, displaying all the variables. Now the induction hypothesis for S tells us that for *every* tuple $\vec{n}$ of M of the same length as $\vec{y}$, $M \models \exists v\phi(\vec{m}, \vec{n}, v)$. Since M is nonempty, just pick any such tuple $\vec{n}_0$ from M. Then, choose $a \in M$ such that $M \models \phi(\vec{m}, \vec{n}_0, a)$. Now the induction hypothesis for S' (with the tuple $\vec{m}, \vec{n}_0, a$ for the variables $\vec{u}, \vec{y}, w$) tells us that $M \models \chi(\vec{m})$, as desired. ∎

Exercise 92 Supply yourself the induction step for the case of $\vee$-elimination, in the proof above.

For the proof of the Completeness Theorem (3.2.2), first we observe that $\Gamma \models \phi$ is equivalent to $\Gamma \cup \{\neg\phi\} \models \bot$, and that $\Gamma \vdash \phi$ is equivalent to $\Gamma \cup \{\neg\phi\} \vdash \bot$.

Exercise 93 Prove these facts.

Therefore, the statement of 3.2.2 reduces to the special case: if $\Gamma \models \bot$, then $\Gamma \vdash \bot$. We shall prove the contrapositive of this, viz.: if $\Gamma \nvdash \bot$, then Γ has a model.

Remark. As we have defined it in Chapter 2, "Γ is consistent" means "Γ has a model". In the literature, "Γ is consistent" is often defined as "$\Gamma \nvdash \bot$". By the Soundness and Completeness Theorems, the two definitions agree. But we haven't proved the Completeness Theorem yet. Therefore, we shall say that Γ is *formally consistent* if $\Gamma \nvdash \bot$.

A set Γ of L-sentences is said to be *maximally formally consistent* if Γ is formally consistent but no proper extension $\Gamma' \supset \Gamma$ is.

Exercise 94 Suppose Γ is a maximally formally consistent set of L-sentences. Show that for any two L-sentences ϕ and ψ it holds that $\Gamma \vdash \phi \vee \psi$ if and only if either $\Gamma \vdash \phi$ or $\Gamma \vdash \psi$.
[Hint: for the 'only if' direction, if $\Gamma \nvdash \phi$, then $\Gamma \cup \{\neg\phi\}$ is a formally consistent extension of Γ]
Prove also, that for any L-sentence ϕ, either $\phi \in \Gamma$ or $\neg\phi \in \Gamma$

We shall furthermore say that a set Γ of L-sentences *has enough constants*, if for every L-formula $\varphi(x)$ with one free variable x, there is a constant c such that

$$\Gamma \vdash \exists x\varphi(x) \to \varphi(c)$$

Lemma 3.2.4 *Let Γ be a maximally formally consistent set of L-sentences such that Γ has enough constants. Then Γ has a model.*

Proof. Let C be the set of constants of L. Then $C \neq \emptyset$ (why?). We put an equivalence relation $\sim$ on C by:

$$c \sim d \text{ if and only if } \Gamma \vdash (c = d)$$

It is easily verified (see Example f) of section 3.1.1) that $\sim$ is an equivalence relation. The set $M = C/\sim$ of equivalence classes is made into an L-structure as follows.

If F is an n-ary function symbol of L and $c_1, \ldots, c_n \in C$, then $\Gamma \vdash \exists x(F(c_1, \ldots, c_n) = x)$; since Γ has enough constants, there is a constant c such that $\Gamma \vdash F(c_1, \ldots, c_n) = c$; define F^M by $F^M([c_1], \ldots, [c_n]) = [c]$. This is independent of the choices for c and the representatives $c_1, \ldots, c_n$, for if $c_i \sim d_i$ for $i = 1, \ldots, n$ and $c \sim d$, we have easily $\Gamma \vdash F(d_1, \ldots, d_n) = d$ by a number of Substitution constructions on the corresponding proof trees.

Similarly, if R is an n-place relation symbol we put

$$R^M = \{([c_1], \ldots, [c_n]) \,|\, \Gamma \vdash R(c_1, \ldots, c_n)\}$$

and again one checks that this is well-defined.

Finally, if c is a constant of L we let $c^M = [c]$. This completes the definition of M as L-structure.

Now let t be a closed L-term. It is easily seen by induction on t that if c is a constant such that $\Gamma \vdash (t = c)$ (and such a constant exists, since Γ has enough constants), then $t^M = [c]$. Therefore, if s and t are closed L-terms, we have:

$$M \models (t = s) \text{ if and only if } \Gamma \vdash (t = s)$$

We shall now prove that for *every* L-sentence ϕ,

$$M \models \phi \text{ if and only if } \Gamma \vdash \phi$$

by induction on ϕ.

If ϕ is $R(c_1, \ldots, c_n)$, this holds by definition. Hence, since every closed term is equal to some constant as we have just seen, the claim also holds for sentences $R(t_1, \ldots, t_n)$ where the t_i are closed terms.

Suppose ϕ is $\psi \vee \chi$. Then $M \models \phi$ if and only if (by definition of $\models$) $M \models \psi$ or $M \models \chi$, if and only if (by induction hypothesis) $\Gamma \vdash \psi$ or $\Gamma \vdash \chi$, if and only if (by Exercise 94, since Γ is maximally formally consistent) $\Gamma \vdash \psi \vee \chi$. The step for $\neg\psi$ is similar, and the steps for $\wedge$ and $\rightarrow$ are left to you.

Now suppose ϕ is $\forall x\psi(x)$. We see that $M \models \phi$ is equivalent to: for all constants c of L, $M \models \psi(c)$. By induction hypothesis, this is equivalent to: for all constants c of L, $\Gamma \vdash \psi(c)$. This obviously follows from $\Gamma \vdash \forall x\psi(x)$. For the converse, using that Γ has enough constants, pick a c such that $\Gamma \vdash \exists x\neg\psi(x) \to \neg\psi(c)$. Then since $\Gamma \vdash \psi(c)$, we must have $\Gamma \vdash \neg\exists x\neg\psi(x)$. By one of the items of Exercise 88, $\Gamma \vdash \forall x\psi(x)$.
Again, the case for $\phi \equiv \exists x\psi(x)$ is similar, and omitted.

We see that M is a model of Γ, which was to be proved. ∎

The following lemma now links Lemma 3.2.4 to Theorem 3.2.2.

Lemma 3.2.5 *Let Γ be a formally consistent set of L-sentences. Then there is an extension L' of L by constants, and a set Δ of L'-sentences which extends Γ, is maximally formally consistent and has enough constants.*

Before proving Lemma 3.2.5, let us wrap up the argument for Theorem 3.2.2 from it: given a formally consistent Γ, take Δ as in Lemma 3.2.5. By Lemma 3.2.4, Δ has a model M. This is an L'-structure, but by restricting the interpretation to L it is also an L-structure. Since $\Gamma \subseteq \Delta$, the structure M is a model of Γ, as desired.

Proof. Fix a set C, disjoint from L, such that $|C| = \|L\| = \max(\omega, |L|)$. Then C is infinite, so by Exercise 19a), $|C| = \omega \times |C|$; therefore, we can write C as a disjoint union:

$$C = \bigcup_{n\in\mathbb{N}} C_n$$

such that for each $n \in \mathbb{N}$, $|C_n| = |C|$.

Let L_0 be L, and $L_{n+1} = L_n \cup C_n$, where the elements of C_n are new constants. By induction, one sees that $\|L_n\| = \|L\| = |C|$. It follows, that for each n, there is an injective function from the set

$$F_n = \{\varphi(x) \,|\, \varphi(x) \text{ is an } L_n\text{-formula with one free variable } x\}$$

to the set C_n; we denote this map by $\varphi(x) \mapsto c_{\varphi(x)}$.

We let L' be $\bigcup_{n\in\mathbb{N}} L_n$. We construct Γ' as $\bigcup_{n\in\mathbb{N}} \Gamma_n$, where $\Gamma_0 = \Gamma$ and

$$\Gamma_{n+1} = \Gamma_n \cup \{\exists x\varphi(x) \to \varphi(c_{\varphi(x)}) \,|\, \varphi(x) \in F_n\}$$

First, we prove the following fact:

(*) If $\Gamma_{n+1} \vdash \phi$, where ϕ is an L_n-sentence, then also $\Gamma_n \vdash \phi$ (We say that Γ_{n+1} is *conservative* over Γ_n).

Since every proof tree has only finitely many assumptions, we see that if $\Gamma_{n+1} \vdash \phi$ there are $\varphi_1(x), \ldots, \varphi_m(x) \in F_n$, such that

$$\Gamma_n \cup \{\exists x \varphi_i(x) \to \varphi_i(c_{\varphi_i(x)}) \,|\, 1 \leq i \leq m\} \vdash \phi$$

Combining Exercise 87 and the equivalences of Exercise 88, this is equivalent to (check!):

$$\Gamma_n \vdash \bigvee_{i=1}^{m} \neg(\exists x \varphi_i(x) \to \varphi_i(c_{\varphi_i(x)})) \vee \phi$$

Now the constants $c_{\varphi_i(x)}$ are not in L_n, hence don't occur in Γ_n or in ϕ. It follows from Example 3 in section 3.1.2, that

$$\Gamma_n \vdash \forall u_1 \cdots u_m [(\bigvee_{i=1}^{m} \neg(\exists x \varphi_i(x) \to \varphi_i(u_i)) \vee \phi]$$

By repeated use of $\vdash \forall x(\chi \vee \psi(x)) \to (\chi \vee \forall x \psi(x))$ (see Example j of section 3.1.1), and $\vdash \neg(\alpha \to \beta) \to (\alpha \wedge \neg\beta)$,

$$\Gamma_n \vdash \bigvee_{i=1}^{m} (\exists x \varphi_i(x) \wedge \forall u_i \neg \varphi_i(u_i)) \vee \phi$$

It follows, since $\vdash (\exists x \varphi_i(x) \wedge \forall u_i \neg \varphi_i(u_i)) \to \bot$ (check!), that $\Gamma_n \vdash \bot \vee \phi$ hence $\Gamma_n \vdash \phi$. This proves (*).

From (*) it follows that Γ' is formally consistent. For suppose $\Gamma' \vdash \bot$. Again using that every proof tree is finite, one finds that already $\Gamma_n \vdash \bot$ for some n; then by induction, using (*) one finds that $\Gamma \vdash \bot$ which contradicts the assumption that Γ is formally consistent.

It is easy to see that Γ' has enough constants; every formula contains only finitely many constants, so every L'-formula is an L_n-formula for some n. So a required constant for it will be in L_{n+1} by construction.

Now clearly, if a set of sentences has enough constants, then every bigger set also has enough constants. Therefore it suffices to show that Γ' can be extended to a maximally formally consistent set of L'-sentences; this is done with the help of Zorn's Lemma (Definition 1.2.8).

Let P be the set of those sets of L'-sentences that contain Γ' and are formally consistent; P is ordered by inclusion. P is nonempty, for $\Gamma' \in P$ as we have seen. If $\mathcal{K}$ is a chain in P then $\bigcup \mathcal{K}$ is formally consistent. Indeed, if $\bigcup \mathcal{K} \vdash \bot$ then already $Z \vdash \bot$ for some $Z \in \mathcal{K}$ (compare with the proof above that Γ' is formally consistent). By Zorn's Lemma, P has a maximal element Δ. Then Δ is maximally formally consistent, as is left for you to check; which finishes the proof. ∎

Corollary 3.2.6 (Compactness Theorem (2.5.1)) *If Γ is a set of sentences in a given language, and every finite subset of Γ has a model, then Γ has a model.*

Proof. Suppose Γ doesn't have a model. By the Completeness Theorem, $\Gamma \vdash \bot$. Then, as we have seen a few times before, already $\Gamma' \vdash \bot$ for some finite $\Gamma' \subseteq \Gamma$. But this contradicts the Soundness Theorem, because Γ' has a model by assumption. ∎

Exercise 95 Show that our proof of the Completeness Theorem has the corollary, that every formally consistent set of L-sentences has a model of cardinality at most $\|L\|$. Compare this to Theorem 2.8.3.

3.3 Skolem Functions

Definition 3.3.1 Let L be a language. A *Skolem Theory* is an L-theory Δ with the property that for every L-formula $\varphi(\vec{x}, y)$ with $n+1$ free variables, there is a function symbol F such that

$$\Delta \vdash \forall \vec{x}\,(\exists y \varphi(\vec{x}, y) \to \varphi(\vec{x}, F(\vec{x})))$$

In the case $n = 0$, we take this to mean that for $\varphi(y)$ there is a constant c such that $\Delta \vdash \exists y \varphi(y) \to \varphi(c)$.

Recall that if we have two languages $L \subseteq L'$ and two theories $T \subseteq T'$ such that T is an L-theory and T' is an L'-theory, T' is said to be *conservative over* T if every L-sentence which is a consequence of T' is already a consequence of T.

Exercise 96 Suppose that we have an infinite chain

$$L_1 \subseteq L_2 \subseteq \cdots$$

of languages, and also a chain

$$T_1 \subseteq T_2 \subseteq \cdots$$

of theories, such that for each n, T_n is an L_n-theory. Let $L = \bigcup_{n \geq 1} L_n$, and $T = \bigcup_{n \geq 1} T_n$. Then T is an L-theory.

Prove, that if T_{n+1} is conservative over T_n for each $n \geq 1$, then T is conservative over T_1.

Theorem 3.3.2 *Let Γ be an L-theory. Then there is an extension L' of L, and a Skolem theory Δ in L' extending Γ, which is conservative over Γ.*

Proof. First, we show the following: for every L-theory Γ there is an extension L' of L and an L'-theory Δ, such that $\Gamma \subseteq \Delta$, Δ is conservative over Γ and for every L-formula $\varphi(\vec{x}, y)$ with $n+1$ free variables, there is a function symbol F in L', such that

$$\Delta \vdash \forall \vec{x}\,(\exists y \varphi(\vec{x}, y) \to \varphi(\vec{x}, F(\vec{x})))$$

Let L' be the extension of L obtained in the following way: for every L-formula φ and every string $(x_1, \ldots, x_k, y) = (\vec{x}, y)$ of variables such that all free variables of φ occur in $\vec{x}, y$, add a k-ary function symbol $F^{\varphi}_{\vec{x},y}$. Let Δ be the set of L'-sentences defined as the union of Γ and the set of all L'-sentences of the form

$$\forall \vec{x}(\exists y \varphi \to \varphi[F^{\varphi}_{\vec{x},y}(\vec{x})/y])$$

where φ is an L-formula and $(\vec{x}, y)$ as above (the set Δ is said to be an extension of Γ by *Skolem functions*).

Exercise 97 Show that every model of Γ can be made into an L'-structure which is a model of Δ, by choosing appropriate functions as interpretations for the $F^{\varphi}_{\vec{x},y}$. Then use the Completeness Theorem to conclude that Δ is conservative over Γ.

In order to prove the theorem, we iterate this construction infinitely often: let $L_1 = L$, and $T_1 = \Gamma$. Suppose L_n and T_n have been defined; let L_{n+1} and T_{n+1} then be the extended language and the extended theory which are obtained from L_n and T_n by the construction above.

Finally, let $L' = \bigcup_{n \geq 1} L_n$ and $\Delta = \bigcup_{n \geq 1} T_n$. By Exercise 96, Δ is conservative over Γ. The proof that Δ is a Skolem theory is left to you. ∎

Exercise 98 Finish the proof of Theorem 3.3.2: prove that the constructed theory Δ is in fact a Skolem theory.

Exercise 99 Let Δ be a Skolem theory, $M \models \Delta$, and $X \subseteq M$. Let $\langle X \rangle$ be the substructure of M generated by X. Prove that $\langle X \rangle$ is an elementary substructure of M.

Exercise 100 Prove the following strengthening of the previous exercise: every Skolem theory has quantifier elimination.

Chapter 4

Sets Again

This short chapter aims to give you a nodding acquaintance with the *formal theory of sets*, which is accepted by most mathematicians as a foundation for mathematics.

Set theory, as we saw in the introduction to Chapter 1, was founded by Cantor. We have seen already many results by Cantor in these lecture notes: the Schröder-Cantor-Bernstein Theorem, the uncountability of $\mathbb{R}$, the diagonal argument, the Cantor Set, the notion of cardinal number and the Continuum Hypothesis, and in Chapter 2 the ω-categoricity of the theory of dense linear orders. The notion of 'ordinal number', which we shall see in this chapter, is also due to him and there is lots more.

Cantor was not a logician, and his idea of 'sets' was not very precise; basically, a set could be formed by grouping together all objects sharing a certain property. This approach was also taken by Frege, one of the first pioneers in logic.

However, there is a problem with this approach, which was pinpointed by Bertrand Russell in 1903 (this is the 'antinomy' we alluded to in the introduction to Chapter 2). Consider the set $\mathbb{N}$ of natural numbers. Clearly, $\mathbb{N}$ is not a natural number, so it is not an element of $\mathbb{N}$: $\mathbb{N} \notin \mathbb{N}$. Now, Russell continued, let us 'group together' into a set *all* those sets which are not elements of themselves: let

$$R = \{x \mid x \notin x\}$$

Suppose R is a set. Then the question as to whether or not $R \epsilon R$, makes sense. But by definition of R, we find that $R \epsilon R$ precisely when $R \notin R$! This is clearly a contradiction, which is known as "Russell's Paradox".[1]

[1] There is a real life version of the same paradox, about the "village barber, who shaves

4.1 The Axioms of ZF(C)

Mindful of Russell's paradox, Ernst Zermelo (1871–1953), whom we know from the Axiom of Choice and the Well-Ordering Theorem, formulated carefully a system of axioms for sets in [28] (1908). One of the basic ideas is that one can group together all objects *from a given set* which have a certain property, to form a new set: instead of allowing $\{x \mid P(x)\}$ to be a set, we declare that $\{x \in X \mid P(x)\}$ is always a set provided X is one (this is the Axiom Scheme of Separation below).

Zermelo's set theory (often denoted Z) is still an interesting object of study, but for mathematical purposes it is too weak, as was soon discovered. In 1922, the Axiom Scheme of Replacement was proposed by Fraenkel. The resulting system is called Zermelo-Fraenkel set theory, and denoted ZF. When the Axiom of Choice is added, we write ZFC.

The theory ZFC is formulated in the language $\{\epsilon\}$, where ϵ is a 2-place relation symbol expressing 'is an element of'. We only talk about sets and elementhood. What does it mean to say that this theory is a "foundation for mathematics"? It means that all constructions from the basic set theory we developed in Chapter 1 can be defined in ZFC, and that all sets and functions used in mathematics, can be regarded as elements of any model of ZFC. It is therefore possible to do as if every mathematical theorem is a theorem about sets.
We now list the axioms.

1) *Axiom of Extensionality*
$\forall x \forall y(\forall z(z \epsilon x \leftrightarrow z \epsilon y) \rightarrow x = y)$
Sets are equal if they have the same elements.

2) *Axiom of Pairing*
$\forall x \forall y \exists z \forall w(w \epsilon z \leftrightarrow (w = x \vee w = y))$
For each x and y, $\{x, y\}$ is a set.

3) *Axiom Scheme of Separation*
For every formula ϕ not containing the variable y, we have an axiom
$\forall x \exists y \forall w(w \epsilon y \leftrightarrow (w \epsilon x \wedge \phi))$
For each set x and property ϕ, $\{w \epsilon x \mid \phi\}$ is a set.

4) *Axiom of Union*
$\forall x \exists y \forall w(w \epsilon y \leftrightarrow \exists z(z \epsilon x \wedge w \epsilon z))$
For every set x, $\bigcup x$ (or $\bigcup_{z \epsilon x} z$) is a set.

---

every villager who does not shave himself". Does the barber shave himself?

5) *Axiom of Power Set*
$\forall x \exists y \forall w (w \epsilon y \leftrightarrow \forall z (z \epsilon w \rightarrow z \epsilon x))$
For every set x, $\mathcal{P}(x)$ is a set.

6) *Axiom of Infinity*
Since $\exists x (x = x)$ is a valid sentence, there is a set; if x is a set then by Separation there is a set $\{w \epsilon x \,|\, \bot\}$ which has no elements; and this set is unique, by Extensionality. We denote this empty set by $\emptyset$. Also, for any set x, we have a set $\{x\} = \{x, x\}$ by Pairing, and $x \cup \{x\} = \bigcup \{x, \{x\}\}$ using again Pairing, and Union. With these notations, the axiom of Infinity is now

$$\exists x (\emptyset \epsilon x \wedge \forall y (y \epsilon x \rightarrow (y \cup \{y\}) \epsilon x))$$

This will turn out to mean: "there is an infinite set".

7) *Axiom Scheme of Replacement*
For any formula ϕ which does not contain the variable y:

$$\forall a \exists b \forall c (\phi(a, c) \leftrightarrow c = b) \rightarrow$$
$$\forall x \exists y \forall v (v \epsilon x \rightarrow \exists u (u \epsilon y \wedge \phi(v, u)))$$

The premiss expresses that ϕ defines an operation F on sets. The axiom says that for any such operation F and any set x, there is a set y which contains $\{F(v) \,|\, v \epsilon x\}$ (it follows then by Separation, that in fact the latter is a set).

8) *Axiom of Regularity*
$\forall x (x \neq \emptyset \rightarrow \exists y (y \epsilon x \wedge \forall z \neg (z \epsilon y \wedge z \epsilon x)))$
Every nonempty set x has an element that is disjoint from x.

The regularity axiom (together with Pairing) implies that no set can be an element of itself, for if $x \epsilon x$ then the set $\{x\}$ does not contain an element disjoint from itself (check!). This has the following two consequences:

1) x is always a proper subset of $x \cup \{x\}$, so that any set satisfying the statement of the Axiom of Infinity is in fact infinite;

2) There can be no 'set of all sets', because such a set would be an element of itself. We see that the Russell paradox is resolved: the 'set' $R = \{x \,|\, x \notin x\}$ would have to be the set of all sets! Therefore, R is not a set.

Classes and Sets. A *class* is a collection of all sets satisfying a given property. For us, a class is given by a formula $\phi(x)$ with one free variable x. Such a class is a set, if $\exists y \forall x(\phi(x) \leftrightarrow x \epsilon y)$ holds. Note that, by Separation, every subclass of a set is a set.

Using Pairing, we have for each set x and each set y the set

$$\{\{x\}, \{x, y\}\}$$

which we denote (x, y) and call the *ordered pair* of x and y.

Exercise 101 Show:

a) $(x, y) = (u, v) \leftrightarrow x = u \wedge y = v$

b) $x \times y = \{(u, v) \mid u \epsilon x \wedge v \epsilon y\}$ is a set (Hint: use that for $u \epsilon x$ and $v \epsilon y$, (u, v) is a subset of $\mathcal{P}(x \cup y)$)

A *relation* from x to y is a subset of $x \times y$. Such a relation R is a *function* if $\forall u \epsilon x \exists v \epsilon y \forall w \epsilon y((u, w) \epsilon R \leftrightarrow v = w)$ holds.

Exercise 102 Show that for every two sets x and y, there is a set y^x of all functions from x to y.

The *Axiom of Choice* can now be formulated:

$$\forall x \forall y \forall f \epsilon y^x [\forall v \epsilon y \exists u \epsilon x((u, v) \epsilon f) \rightarrow \exists g \epsilon x^y \forall v \epsilon y \forall u \epsilon x((v, u) \epsilon g \rightarrow (u, v) \epsilon f)]$$

A *poset* is an ordered pair (x, r) such that $r \epsilon \mathcal{P}(x \times x)$ is a relation which partially orders x: i.e. $\forall u \epsilon x((u, u) \epsilon r)$ etcetera. Similarly, we can define the notions of a linear order and a well-order.

Exercise 103 Carry this out.

Remark on Notation. We have started to use a lot of symbols which are not part of the language $\{\epsilon\}$: $\mathcal{P}(x)$, $\bigcup x$, $\{y \epsilon x \mid \ldots\}$, etc. You should see these as abbreviations. Everything we express with these symbols can, equivalently, be said without them. For example if $\phi(v)$ is a formula then the expression $\phi(\mathcal{P}(x))$ is short for:

$$\exists y[\forall v(v \epsilon y \leftrightarrow \forall w(w \epsilon v \rightarrow w \epsilon x)) \wedge \phi(y)]$$

or equivalently

$$\forall y[\forall v(v \epsilon y \leftrightarrow \forall w(w \epsilon v \rightarrow w \epsilon x)) \rightarrow \phi(y)]$$

In principle, we could now translate every informal statement about sets in Chapter 1 into a formula of ZF, and prove it from the ZF-axioms by natural deduction trees. This is long and tedious, but possible. Let us here just stress these two points:

1) The theory ZF, augmented by the Axiom of Choice where necessary, suffices to prove all the theorems and propositions of Chapter 1.

2) Once one has formulated ZF as a first-order theory, the question whether or not a particular statement can be proved from it ($\mathrm{ZF} \vdash \phi$?) gets a precise mathematical meaning.

4.2 Ordinal numbers and Cardinal numbers

A set x is *transitive* if $\forall y \epsilon x \forall u \epsilon y (u \epsilon x)$ holds.

Exercise 104 Prove that x is transitive iff $\forall y \epsilon x (\mathcal{P}(y) \subset \mathcal{P}(x))$; and also that x is transitive iff $x \subset \mathcal{P}(x)$.

Examples. $\emptyset$ is transitive; $\{\emptyset\}$ too. $\{\{\emptyset\}\}$ is not transitive. If x and y are transitive, so is $x \cup y$, and if x is transitive, so is $x \cup \{x\}$.

A set x is an *ordinal number* (or just *ordinal*) if x is transitive and well-ordered by the relation ϵ. This means: x is an ordinal if the conditions

$$\forall y \epsilon x \forall v \epsilon y (v \epsilon x)$$
$$\forall y \subseteq x (y \neq \emptyset \rightarrow \exists v \epsilon y \forall w \epsilon y (v \neq w \rightarrow v \epsilon w))$$

hold.

Exercise 105 Check that these conditions indeed imply that ϵ is a linear order on x, and that it is a well-order.

Normally, we use Greek lower-case characters in the first half of the alphabet: α, β, γ,... for ordinals.

Theorem 4.2.1

a) $\emptyset$ *is an ordinal.*

b) *If* α *is an ordinal then every* $\beta \epsilon \alpha$ *is an ordinal.*

c) *If* α *and* β *are ordinals then* $\alpha \subsetneq \beta \rightarrow \alpha \epsilon \beta$.

d) *If* α *and* β *are ordinals then* $\alpha \subseteq \beta$ *or* $\beta \subseteq \alpha$.

Proof. a) is immediate and b) is left as an exercise.

For c), suppose $\alpha \subsetneq \beta$. Let γ be the ϵ-least element of $\beta - \alpha$. Then $\gamma \subseteq \alpha$. On the other hand, if $x \epsilon \alpha$ then $x = \gamma$ and $\gamma \epsilon x$ are impossible by definition of γ and the fact that α is transitive. Therefore, since β is an ordinal, $x \epsilon \gamma$ must hold. So $\alpha \subseteq \gamma$; hence $\alpha = \gamma$ and so $\alpha \epsilon \beta$, as required.

Part d) is proved by similar reasoning: suppose $\alpha \not\subseteq \beta$. Let γ be an ϵ-minimal element of $\alpha - \beta$. Then $\gamma \subseteq \beta$. If $\gamma = \beta$ then $\beta \epsilon \alpha$ hence $\beta \subsetneq \alpha$ by transitivity of α; if $\gamma \subsetneq \beta$ then $\gamma \epsilon \beta$ by c), which contradicts the choice of γ. ∎

Exercise 106 Prove part b) of Theorem 4.2.1. Prove also that if α and β are ordinals, then either $\alpha \epsilon \beta$, or $\alpha = \beta$, or $\beta \epsilon \alpha$ holds.

Let Ord be the class of ordinal numbers. For ordinals α, β we write $\alpha < \beta$ for $\alpha \epsilon \beta$. By Theorem 4.2.1, $<$ is a linear order on Ord. It is, actually, in a sense a well-order, as follows from the next theorem.

Theorem 4.2.2

a) Every nonempty subclass of Ord *has a $<$-least element; in fact, if C is a nonempty class of ordinals, then $\bigcap C$ belongs to C.*

b) For every set x of ordinals, $\bigcup x$ is an ordinal, and it is the least ordinal α such that $\beta \leq \alpha$ for all $\beta \epsilon x$.

c) For every ordinal α, $\alpha + 1 = \alpha \cup \{\alpha\}$ is an ordinal, and it is the least ordinal $> \alpha$.

Proof. For a), if C is defined by a formula $\phi(x)$ such that $\forall x(\phi(x) \rightarrow$ x is an ordinal) and x is such that $\phi(x)$ holds, then x is an ordinal and $x \cap C = \{y \epsilon x \mid \phi(y)\}$ is a set, a subset of x. If $x \cap C = \emptyset$, then x is the least element of C; otherwise, since x is an ordinal, $x \cap C$ has an ϵ-least element in x. We leave the details to you. ∎

Exercise 107 Fill in the details of the proof above for part a); prove yourself parts b) and c) of Theorem 4.2.2.

Theorem 4.2.2 suggests that, in analogy to Theorem 1.3.5, there might also be a principle of 'definition by recursion on Ord'. This is in fact the case, but requires a little care in formulating.

Recall (from the introduction to the axiom of Replacement) that a formula $\phi(x, y)$ defines an operation on sets if

$$\forall x \exists y \forall z(\phi(x, z) \leftrightarrow y = z)$$

holds. We say that $\phi(x,y)$ defines an operation on ordinals if

$$\forall x(x \in \text{Ord} \to \exists y \forall z(\phi(x,z) \leftrightarrow y = z))$$

holds, where '$x \in$ Ord' is the formula expressing that x is an ordinal.

Suppose $\phi(x,y)$ defines an operation on sets, which we call F. Then we use expressions like $\{F(x) \,|\, x \epsilon y\}$ as shorthand; if ψ is a formula, the expression $\psi(\{F(x) \,|\, x \epsilon y\})$ should be taken to mean

$$\exists z(\forall w(w \epsilon z \leftrightarrow \exists x(x \epsilon y \wedge \phi(x,w))) \wedge \psi(z))$$

Theorem 4.2.3 (Transfinite recursion on Ord) *For every operation F on sets there is a unique operation G on* Ord *such that for all ordinals α the following holds:*

$$G(\alpha) = F(\{G(\beta) \,|\, \beta \epsilon \alpha\})$$

Proof. Define G by the following formula $\psi(\alpha, x)$:

$$\psi(\alpha,x) \equiv \exists y \exists f \epsilon y^{\alpha} \left(\begin{array}{r} \forall \xi \epsilon \alpha(f(\xi) = F(\{f(\eta) \,|\, \eta \epsilon \xi\})) \wedge \\ x = F(\{f(\xi) \,|\, \xi \epsilon \alpha\}) \end{array} \right)$$

The proof that ψ defines an operation G on Ord with the stated property, is left to you. ∎

Examples of Ordinals. $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\} = \{0,1\}$, $3 = \{0,1,2\}$,... are ordinals. Let x be a set as postulated by the axiom of Infinity, so $\emptyset \epsilon x \wedge \forall y(y \epsilon x \to y \cup \{y\} \epsilon x)$. Let ω be the intersection of all subsets of x which contain $\emptyset$ and are closed under the operation $y \mapsto y \cup \{y\}$:

$$\omega = \{u \epsilon x \,|\, \forall r \epsilon \mathcal{P}(x)((\emptyset \epsilon r \wedge \forall v(v \epsilon r \to v \cup \{v\} \epsilon r)) \to u \epsilon r)\}$$

Then ω is an ordinal, the least infinite ordinal. We think of it as

$$\omega = \{0, 1, 2, \ldots\}$$

We have then, by 4.2.2c), also the ordinals $\omega{+}1$, $\omega{+}2$,.... One can show that there is a set of ordinals $\{\omega{+}n \,|\, n \epsilon \omega\}$ and hence an ordinal $\omega{+}\omega = \omega{\cdot}2$. Continuing, there is $\omega{\cdot}3$,... up to $\omega{\cdot}\omega = \omega^2$. Then, ω^3,...,ω^{ω},...,$\omega^{\omega^{\omega}}$,...,$\omega^{\omega^{\cdot^{\cdot}}}$. All these ordinals are countable!

Exercise 108 (Addition and Multiplication of ordinals) By transfinite recursion (4.2.3) we define operations of addition and multiplication on Ord, as follows:

$$\alpha + \beta = \left\{ \begin{array}{rl} \alpha & \text{if } \beta = 0 \\ \bigcup\{(\alpha + \gamma) + 1 \,|\, \gamma \epsilon \beta\} & \text{otherwise} \end{array} \right.$$

and

$$\alpha{\cdot}\beta = \begin{cases} 0 & \text{if } \beta = 0 \\ \bigcup\{(\alpha{\cdot}\gamma) + \alpha \,|\, \gamma \epsilon \beta\} & \text{else} \end{cases}$$

a) Show that $\gamma < \beta$ implies $\alpha + \gamma < \alpha + \beta$, and (if $\alpha \neq 0$) $\alpha{\cdot}\gamma < \alpha{\cdot}\beta$

b) Show: $0 + \beta = \beta$ and $0{\cdot}\beta = 0$

c) Show: $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ and $\alpha{\cdot}(\beta + 1) = (\alpha{\cdot}\beta) + \alpha$

d) Show that for any nonempty set of ordinals x,

$$\alpha + \bigcup x = \bigcup\{\alpha + \beta \,|\, \beta \epsilon x\}$$

e) Show that for $\alpha \neq 0$ and any set of ordinals x,

$$\alpha{\cdot}\bigcup x = \bigcup\{\alpha{\cdot}\beta \,|\, \beta \epsilon x\}$$

f) Show that $1 + \omega = \omega \neq \omega + 1$, and $2{\cdot}\omega = \omega \neq \omega{\cdot}2$

Theorem 4.2.4 *Every well-ordered set is isomorphic (as well-ordered set) to a unique ordinal number.*

Proof. Let $(X, <)$ be a well-ordered set. We use the principle of induction over X to show that for each $x \epsilon X$ there is a unique ordinal $F(x)$ such that $\{y \epsilon X \,|\, y < x\} \cong F(x)$. For successor elements $x{+}1$, let $F(x{+}1) = F(x){+}1 = F(x) \cup \{F(x)\}$; if l is a limit element, one proves that $\{F(x) \,|\, x < l\}$ is an ordinal which is isomorphic to $\{y \epsilon X \,|\, y < l\}$. Similarly now, $\{F(x) \,|\, x \epsilon X\}$ is an ordinal (it is a set by the Replacement axioms) which is isomorphic to $(X, <)$. ∎

Now recall Hartogs' Lemma, which states that for any set X there is a well-order $(W, <)$ such that W cannot be mapped injectively into X; by Theorem 4.2.4 there is an ordinal which cannot be mapped injectively into X, and by 4.2.2a), there is a least such ordinal. Taking $X = \omega$, we see that there is a *least uncountable ordinal*, which we denote by ω_1.

The ordinals $0, 1, 2, \ldots, \omega$ and ω_1 are examples of *cardinal numbers*. A cardinal number is an ordinal κ such that for every $\alpha \in \kappa$, there is no bijection between α and κ.

If one assumes the Axiom of Choice, every set X can be well-ordered and is therefore in bijective correspondence with an ordinal; taking the least such ordinal, one associates to every set X a unique cardinal number κ such that

there is a bijection between X and κ; we may write $|X|$ for κ. If we write 2^κ for $|\mathcal{P}(\kappa)|$ then the Continuum Hypothesis has a compact formulation: $2^\omega = \omega_1$.

Without the Axiom of Choice one can still formulate the Continuum Hypothesis but one can no longer prove that to every set corresponds a unique cardinal number as above.

There is a 1-1, surjective mapping from the class Ord of ordinals into the class of all infinite cardinal numbers, defined as follows: $\aleph_0$ (pronounce: "aleph–zero") is ω; if $\aleph_\alpha$ is defined, $\aleph_{\alpha+1}$ is the least cardinal number greater than $\aleph_\alpha$; if λ is a limit ordinal (that is, an ordinal not of the form $\alpha + 1$), then $\aleph_\lambda = \bigcup\{\aleph_\beta \,|\, \beta < \lambda\}$.

Exercise 109 Show that $\aleph_\alpha$ is a cardinal for each α. Show also that for each infinite cardinal κ there is a unique ordinal α such that $\kappa = \aleph_\alpha$.

One can prove, without the Axiom of Choice, that $|\aleph_\alpha \times \aleph_\alpha| = \aleph_\alpha$ for each α. You should compare this to Proposition 1.18.

4.3 The real numbers

The real numbers are constructed as follows. From ω, construct $\mathbb{Z}$ as the set of equivalence classes of $\omega \times \omega$ under the equivalence relation: $(n, m) \sim (k, l)$ iff $n + l = m + k$. There are then well-defined operations of addition and multiplication on $\mathbb{Z}$. Define an equivalence relation on the set of those pairs (k, l) of elements of $\mathbb{Z}$ such that $l \neq 0$, by putting $(k, l) \sim (r, s)$ iff $ks = lr$. The set of equivalence classes is $\mathbb{Q}$, the set of rational numbers. $\mathbb{Q}$ is an *ordered field*, that is a field with a linear order $<$ such that

i) $r > s \rightarrow r + t > s + t$

ii) $r > s > 0, t > 0 \rightarrow rt > st$

hold.

A *Dedekind cut* in $\mathbb{Q}$ is a nonempty subset $A \subset \mathbb{Q}$ such that:

i) $a \epsilon A, a' < a \rightarrow a' \epsilon A$

ii) $\mathbb{Q} - A \neq \emptyset$

iii) $\forall a \epsilon A \exists b \epsilon A (a < b)$

$\mathbb{R}$ is the set of Dedekind cuts in $\mathbb{Q}$, ordered by inclusion. $\mathbb{Q}$ is included in $\mathbb{R}$ via the embedding $\iota : q \mapsto \{r \epsilon \mathbb{Q} \,|\, r < q\}$.

Exercise 110 Show that there are operations $+, \cdot$ on $\mathbb{R}$, making $\mathbb{R}$ into an ordered field which extends the ordered field $\mathbb{Q}$.

Suppose $\mathcal{A}$ is a set of elements of $\mathbb{R}$ which is bounded. Then $\bigcup \mathcal{A}$ is an element of $\mathbb{R}$; the least upper bound of $\mathcal{A}$. So $\mathbb{R}$ is complete. Moreover, $\mathbb{Q}$ is dense in $\mathbb{R}$: if $A, B \in \mathbb{R}$ and $A \subsetneq B$, there is a $q \epsilon \mathbb{Q}$ such that $A \subsetneq \iota(q) \subsetneq B$. From this, it follows that $\mathbb{R}$ is a so-called *Archimedean ordered field*: that is, an ordered field such that for each a there is a natural number n such that $a < \iota(n)$. The following theorem, stated without proof (but the proof is not hard) characterizes the real numbers up to isomorphism.

Theorem 4.3.1 *There exists, up to order-isomorphism, exactly one complete Archimedean ordered field, the field of real numbers.*

Bibliography

[1] G. Cantor. Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen. *J. Reine Angew. Math.*, 77:258–262, 1874.

[2] Paul J. Cohen. The independence of the continuum hypothesis. *Proc.Nat.Acad.Sci.U.S.A.*, 50:1143–1148, 1963.

[3] Paul J. Cohen. Independence results in set theory. In *Theory of Models*, pages 39–54. North-Holland, 1965.

[4] N.J. Cutland. *Computability*. Cambridge University Press, 1980.

[5] M. Messmer D. Marker and A. Pillay. *Model Theory of Fields*, volume 5 of *Lecture Notes in Logic*. Association for Symbolic Logic, 2002. second edition.

[6] Joseph W. Dauben. *Georg Cantor*. Princeton University Press, 1990.

[7] N.G. de Bruijn and P. Erdös. A colour problem for infinite graphs and a problem in the theory of relations. *Indagationes Mathematicae*, 13:369–373, 1951.

[8] S. Feferman. Some applications of the notions of forcing and generic sets. *Fundamenta Mathematicae*, 56:325–345, 1964.

[9] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 1934.

[10] K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatsh.Math.Phys.*, 37:349–360, 1930.

[11] K. Gödel. *The Consistency of the Continuum Hypothesis*, volume 3 of *Annals of Mathematics Studies*. Princeton University Press, 1940.

[12] Robert Goldblatt. *Lectures on the Hyperreals – an Introduction to Nonstandard Analysis*, volume 188 of *Graduate Texts in Mathematics*. Springer Verlag, 1998.

[13] Friedrich Hartogs. Über das Problem der Wohlordnung. *Mathematische Annalen*, 76:436–443, 1915.

[14] L. Henkin. The completeness of the first-order functional calculus. *Journal of Symbolic Logic*, 14:159–166, 1949.

[15] Ioan James. *Remarkable Mathematicians*. Cambridge University Press, 2003.

[16] Th.J. Jech. *The Axiom of Choice*, volume 75 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1973. Reprinted by Dover, New York, 2008.

[17] R. Kaye. *Models of Peano Arithmetic*, volume 15 of *Oxford Logic Guides*. Oxford University Press, Oxford, 1991.

[18] J.L. Kelley. The Tychonoff product theorem implies the axiom of choice. *Fundamenta Mathematicae*, 37:75–76, 1950.

[19] S Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer Verlag, 2002.

[20] D. Marker. *Model Theory–an Introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 2002.

[21] Eckart Menzler-Trott. *Logic's lost genius: the life of Gerhard Gentzen*, volume 33 of *History of Mathematics*. American Mathematical Society and London Mathematical Society, 2007.

[22] Abraham Robinson. *Non-standard Analysis*. North-Holland, 1966.

[23] Herman Rubin and Jean E. Rubin. *Equivalents of the Axiom of Choice*, volume 116 of *Studies in Logic*. North-Holland, 1985.

[24] P. Smith. *An Introduction to Gödel's Theorems*. Cambridge University Press, 2009. Fourth printing with corrections.

[25] E. Specker. Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom). *Zeitschr.Math.Logik u. Grindl.d.Math.*, 3(3):173–210, 1957.

[26] Alfred Tarski. Der Wahrheitsbegriff in den formalisierten Sprachen. *Studia Philosophica*, 1:261–405, 1935.

[27] E. Zermelo. Beweis, daß jede Menge wohlgeordnet werden kann. *Mathematische Annalen*, 59:514–516, 1904.

[28] E. Zermelo. Untersuchungen über die Grundlagen der Mengenlehre. *Mathematische Annalen*, 65:261–281, 1908.

Index