Sets, Models and Proofs

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

2000

Contents

1 Sets

We shall assume that you have an idea of what a "set" is, and what a function between sets is. Let us recall a few 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 $x = y$. We use sometimes $f : X \rightarrowtail Y$ to indicate (or emphasize) that f is injective.

The function f is *surjective* (or onto) if every $y \in Y$ is equal to $f(x)$ for some $x \in X$; we denote this by $f : X \twoheadrightarrow Y$.

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}.

A set X is called a *subset* of a set Y, if every element of X is also an element of Y. We write: $X \subseteq Y$.

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.

Exercise 1 Prove:

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

b) if $f : X \rightarrowtail Y$ then f is a bijective function from X to the image of f.

The following sets will be taken for granted: 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.

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 sets:

- $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$, the *Cartesian product* of X and Y;
- $X + Y$ is the *disjoint sum* of X and Y, constructed as $\{(x, 0) \mid x \in X\} \cup \{(y, 1) \mid y \in Y\}$;
- 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 (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:

$$\begin{array}{ll}
\text{Type 1} & x_0 \xrightarrow{f} y_0 \xrightarrow{g} x_1 \xrightarrow{f} y_1 \to \ldots \\
\text{Type 2} & y_0 \xrightarrow{g} x_0 \xrightarrow{f} y_1 \xrightarrow{g} x_1 \to \ldots \\
\text{Type 3} & \ldots \to x_{-1} \xrightarrow{f} y_{-1} \xrightarrow{g} x_0 \xrightarrow{f} y_0 \to \ldots \\
\text{Type 4} & x_0 \xrightarrow{f} y_0 \to \ldots \to y_n \xrightarrow{g} x_0 \\
\text{Type 5} & y_0 \xrightarrow{g} x_0 \to \ldots \to x_n \xrightarrow{f} y_0
\end{array}$$

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; Types 4 and 5 are 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: $|X| \leq |Y|$ 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 1.2 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 $n \leq m$ 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 1.3 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:

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

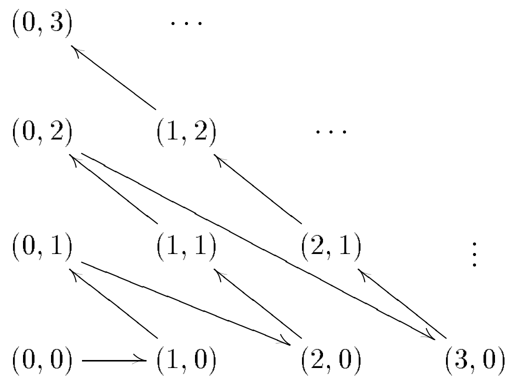
Therefore, $|\mathcal{P}(X)| = |\{0,1\}^X| = 2^{|X|}$.

Proposition 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 $f(0) = (0, 0)$, $f(1) = (0, 1)$, 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 1.4.

Proposition 1.5 *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 1.5 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 other assertion, 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

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

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

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

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

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

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

Example. This example illustrates the proof of 1.5 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 1.5.

Proposition 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 1.4). These are so-called *countable sets*. We make the following definition:

Definition 1.6 A set X is called *countable* if X is empty or if there is a surjective function $\mathbb{N} \twoheadrightarrow X$.

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 $f : \mathbb{N} \twoheadrightarrow X$ 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 $g(x)$?

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 $X + Y$.

An example of an *un*countable set is $2^{\mathbb{N}}$, as follows from proposition 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:

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

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

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 1.7 $|C| = |\mathbb{R}|$.

Proof. By 1.1, it suffices to prove thet $|C| \leq |\mathbb{R}|$ and $|\mathbb{R}| \leq |C|$. Since C is a subset of $\mathbb{R}$ we obviously have

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

There are many ways the prove the converse inequality. For example, each real number x is determined by the set of open intervals with rational end-points which contain x. This defines an injective function

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

Explicitly,

$$\psi(x) = \{(p, q) \in \mathbb{Q} \times \mathbb{Q} \mid p < x < q\}$$

Since $|\mathbb{Q}| = |\mathbb{N}|$, we see that $|\mathbb{Q} \times \mathbb{Q}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ (by proposition 1.4), so

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

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

Exercise 9 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.

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 usual axioms of Set Theory 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), and on the other, that its negation doesn't either (Cohen, 1966). 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 of Mathematics is a rule or principle that mathematicians use in constructing proofs, but which is itself often so clear that it needs no proof. An example is the principle of *induction* for natural numbers (see also the statements just before Proposition 1.22).

The Axiom of Choice is a principle of a slightly different nature, because it states the existence of a certain function, without defining it. Nonetheless it is often very useful in practice and it has been shown not to contradict the other axioms of Set Theory (this is another famous result of Gödel).

Informally, the Axiom of Choice states that given a collection of nonempty sets, there is a way to choose an element from each set in the collection. Here is a more precise formulation, seemingly much simpler.

Definition 1.8 The *Axiom of Choice* (AC) is the assertion that for every surjective function $f : X \twoheadrightarrow Y$ 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 1.8, 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 11), and
- Y is infinite (see Exercise 12)

But even in these circumstances the Axiom of Choice is not *always* necessary; for example, if, in definition 1.8, $X = \mathbb{N}$, we can simply define $s(y)$ as the *least* n such that $f(n) = y$ (this is the solution of Exercise 8i)).

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 1.9 *If X is an infinite set, there is an injective function $\mathbb{N} \to X$.*

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 $(x_0, \ldots, x_n)$ 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:

$$\begin{array}{rcl} f((x_0)) & = & * \\ f((x_0, \ldots, x_{n+1})) & = & (x_1, \ldots, x_n) \end{array}$$

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: for $n = 0$, let $g(n)$ be the element $x_0 \in X$ such that $s(*) = (x_0)$; if $g(0), \ldots, g(n)$ have been defined, let $g(n+1)$ be the element $x_{n+1} \in X$ such that

$$s((g(0), \ldots, g(n))) = (x_0, \ldots, x_{n+1})$$

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

Exercise 10 Use proposition 1.9 to show that if A is infinite and B is finite,

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

Exercise 11 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 12 Prove, without using AC, the *finite* Axiom of Choice, that is: if $f : X \twoheadrightarrow Y$ is surjective and Y is finite, f has a section.
[Hint: perform induction over the cardinality of Y]

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

Proposition 1.10 *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 is empty, the union is empty, hence countable. So let I be nonempty.

If $I' \subseteq I$ is the subset $\{i \in I \mid X_i \neq \emptyset\}$ then $\bigcup_{i \in I} X_i = \bigcup_{i \in I'} X_i$, so we may as well assume that X_i is nonempty for each $i \in I$.

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. ∎

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 A contains a convergent sequence.

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 1.11 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 1.12 *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 $\mathbb{R}$:

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

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.

1.3 Partially Ordered Sets and Zorn's Lemma

Zorn's Lemma 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 1.13 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).

Definition 1.14 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 $P = \{S \subseteq A \mid S \neq A\}$, 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

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

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 13 Suppose X and Y are sets. Let P consist of 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 $C = \{(A_i, f_i) \mid i \in I\}$ 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 1.15 *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 $1 \neq 0$. 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.

However, the argument fails if we drop the requirement that R has $1 \neq 0$. For example, we can turn every abelian group R into a ring by defining $rs = 0$ for all $r, s \in R$. Rings of this sort do not, in general, have maximal ideals. The reason is, that now every additive subgroup of R is an ideal, but the union of a chain of proper additive subgroups need not be a *proper* subgroup.

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

Proposition 1.16 *Zorn's Lemma implies the Axiom of Choice.*

In fact, Zorn's Lemma is *equivalent* to AC. For this and related facts, the interested reader is referred to an appendix to this chapter, section 1.5.

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 13. 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. ∎

Another important consequence of Zorn's Lemma is, 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 1.17 *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 1.5).

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 1.16: $(U, f, V) \leq (U', f', V')$ 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 $Y \cup \{y\}$ 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 $Y \to X$. ∎

It follows from Zorn's Lemma, via proposition 1.17, 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 1.4

Proposition 1.18 *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 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 1.9: 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 1.4), 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 10, there is a bijective function $\varphi : A \to X$. Combining f and φ we obtain a bijection between $A + A$ and A:

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

where ψ is the inverse of φ.

For ii): suppose that $|A| \leq |B|$. We have to show that $|A| + |B| = |B|$. Since $|A| \leq |B|$ there is an injective function $f : A \to B$ so we may as well suppose that A is a subset of B. Then $B \sim A + (B - A)$, and using i) (since A is assumed infinite), we have:

$$A + B \sim A + (A + (B - A)) \sim (A + A) + (B - A) \sim A + (B - A) \sim B$$

which shows that $|A| + |B| = |B|$ as required.

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 1.9 and 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 1.5 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 14 a) Let A and B be nonempty sets, at least one of them infinite. Show that

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

b) 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 $|A^*| = |A|$.

1.4 Well-Ordered Sets

Let $(L, \leq)$ be a poset (Definition 1.13). Recall that the order on L is *linear* if for all $x, y \in L$ we have $x \leq y$ or $y \leq x$; we call L a linear order.

Definition 1.19 A linear 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.

Let us see some examples.

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 1.22).

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.

Exercise 15 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 $x <_L x'$, or $x = x'$ and $y \leq_M y'$. Then $\leq$ well-orders $L \times M$.
The lexicographic order can be pictured as follows: view L as points on a line (since L is linearly ordered) and replace every point of L by a copy of M.

c) If $(L, \leq_L)$ and $(M, \leq_M)$ are two disjoint well-ordered sets, we can define an order on the sum $L + M$ as follows: for $x, y \in L + M$ 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 $L + M$.
This well-order on $L + M$ looks like putting M "on top of" L.

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

Proposition 1.20 *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 16 Prove Proposition 1.20. In one direction, you need to use the Axiom of Choice, in a way similar to the proof of Proposition 1.9

Exercise 17 A linear order $(X, \leq)$ is a well-order if and only if the following condition holds: for any subset S of X, if there is an $x \in X$ satisfying $x > s$ for every $s \in S$, then there is a least such x.

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 $\{y \in L \mid x < y\}$ 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 1.14) 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 1.21 *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*

$$\{y \in L \mid y < x\}$$

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 1.22 *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 $\{x \in L \,|\, x < l\} \subseteq S$, 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 18 Prove Proposition 1.22ii).

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 $\{f(k) \mid k \leq n\}$. 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* $\{f(y) \mid y < x\}$. There are various formulations. We prove one in the proposition below, and give others as exercises.

Proposition 1.23 *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*

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

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

Proof. Define a subset G of $L \times S$ (which will be the graph of the required function F) as follows:

$$\begin{array}{lll} (x, s) \in G & \text{iff} & \text{there is a function } f : \{y \in L \mid y < x\} \to S \text{ such that} \\ & & \text{(i)} \ \ \forall y < x\, f(y) = R(y, \{f(z) \mid z < y\}) \\ & & \text{(ii)} \ s = R(x, \{f(y) \mid y < x\}) \end{array}$$

Notice for later use that if f is such a function, then also $(y, f(y)) \in G$ for all $y < x$.

In order to see that G is the graph of a well-defined function F, we need to prove that for every $x \in L$ there is precisely one $s \in S$ with $(x, s) \in G$; in symbols $\forall x \exists! s\, (x, s) \in G$. This is easy to show by *induction* on L.

Indeed, suppose the assertion is true for all $y < x$, that is

$$\forall y < x \exists! t\, (y, t) \in G$$

(This is the "induction hypothesis"!). Then there is a unique function $f : \{y | y < x\} \to S$ such that

$$\forall y < x\, (y, f(y)) \in G$$

So if we let $s = R(x, \{f(y) \mid y < x\})$, the pair (x, s) belongs to G. This element is unique with this property, for if also $(x, s') \in G$ via a function

f' satisfying (i) and (ii) in the definition of G, we must have $f = f'$ by the uniqueness part of the induction hypothesis. Thus $s = s'$ since both satisfy (ii) for the same function $f = f'$. ∎

Exercise 19 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

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

ii) For any $\varepsilon_0 \in S$, any $R : \mathcal{P}(S) \to S$ and any $g : S \to S$ there is a unique function $F : L \to S$ such that

$$\begin{array}{rcll} F(0_L) & = & \varepsilon_0 & \\ F(l+1) & = & g(F(l)) & \text{if } l \text{ is not maximal in } L \\ F(x) & = & R(\{F(y) \mid y < x\}) & \text{if } l \text{ is a nonzero limit in } L \end{array}$$

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 19ii), $\varepsilon_0 = 0$, 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 1.27 below, and in the Appendix (1.5).

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

Definition 1.24 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 1.25 *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 $\{l' \in L \mid l' < l\}$.*

Proof. Suppose f and f' are two different embeddings: $L \to M$. Then $\{x \in L \mid f(x) \neq f'(x)\}$ 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 $y > x_0$ then $f'(y) > f'(x_0) > f(x_0)$. 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 $\{l' \in L \mid l' < l\}$ into L is the inclusion map, but l is not in the image of this map, so it is not an isomorphism. ∎

Corollary 1.26 *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 1.25 and the identical 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 1.27 *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 $M - (M \cap S)$, if this set is nonempty, and ∞ otherwise. The function R does not really depend on l, but that doesn't matter.

By proposition 1.23 there is a unique function $F : L \to M'$, such that

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

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 $\{x \in L \mid x < l_0\}$, in which case there is an embedding of M into L. ∎

Exercise 20 Let L be a well-order and $f : L \to L$ an injective, order-preserving map so $x < y$ implies $f(x) < f(y)$ for all $x, y \in L$.

Show that $x \leq f(x)$ for all $x \in L$.

Exercise 21 *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 three conditions are satisfied:*

i) *For each $x \in L$, $h(\{x\}) = x$*

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

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

iii) *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.

1.5 Appendix: Equivalents of the Axiom of Choice

In this section we collect some results which are not required reading for the course, but intended for the interested reader. Starting with a lemma that ensures the existence of "sufficiently large" well-ordered sets, we shall formulate yet another principle, Zermelo's *Well-Ordering Theorem* (1.29), and prove 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.

It should be noted (and emphasized) that the proof of the following lemma does *not* use the Axiom of Choice or Zorn's Lemma.

Lemma 1.28 (Hartog's 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 Proposition 1.25) 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 1.27, 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 a unique $m \in M$ such that L is isomorphic to the set $\downarrow(m) = \{m' \in M \mid m' < m\}$ with the restricted order from M.

Therefore, if we denote the $\cong$-equivalence class of L by $[L]$, the set $\{\alpha \in P/\cong \mid \alpha < [L]\}$ 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

$$L_W = \{l \in L \mid [{\downarrow}(l)] \in W\}$$

If L_W is empty, clearly $[L]$ is the least element of W. If Y_W is nonempty, then it has (as subset of the well-ordered set L) a least element l_W. But then $[{\downarrow}(l_W)]$ 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 1.25). ∎

The following consequence of the Axiom of Choice was discovered by E. Zermelo in 1904. We state it here as a "principle", because it is equivalent to AC, as we shall show.

Definition 1.29 The *Well-Ordering Theorem* is the statement that for every set X there exists a relation $\leq$ which well-orders X.

Remark. As said, Zermelo proved the Well-Ordering Theorem using the Axiom of Choice. 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.

Proposition 1.30 *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 Hartog's Lemma (1.28). 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 Hartog's 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 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 Hartog's Lemma.
The implication ii)⇒iii) was done in the proof of Proposition 1.17.
The implication iii)⇒iv) uses Hartog's Lemma once again. Let X be a set. According to Hartog's 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 $f : X \twoheadrightarrow Y$ 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. ∎

Remark 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 book by Rubin and Rubin, *Equivalents of the Axiom of Choice*. 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.

Exercise 22 Give a direct proof of the fact that Zorn's Lemma implies the Well-Ordering Theorem.
[*Hint: consider, for a set X, the poset P as defined in the proof of Proposition 1.28. Show that P satisfies the hypothesis of Zorn's Lemma, and therefore has a maximal element.*]

2 Models

2.1 Structure and Languages for the Real Numbers: 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 23 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 $x + y$, $x \cdot y$, 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 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

$$\forall x(\neg(x = 0) \rightarrow \exists y(x \cdot y = 1))$$

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:

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

[As an aside, we remark that also in $\mathbb{Q}$, the order is definable from the ring structure $0, 1; +, \cdot$. This, however, is rather involved, and depends on a classical result by Julia Robinson]

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 2.1 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 languages 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:

- An 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 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 2.3 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

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

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

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

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

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

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: *in formulas, a variable will always be either bound, or free, but not both; and if it is bound, it is only bound once.*

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 above 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 quantify over elements, not over subsets, or over sequences of elements. For example, suppose we consider the language of rings together with one extra 1-place relation symbol I. Such a 1-place relation will be interpreted as a subset of the structure, say a ring, we are talking about. Now we can express, in a formula, that I is an ideal:

$$\forall x \forall y \forall z (I(x) \wedge I(y) \wedge x + z = y \rightarrow I(z)) \wedge \forall x (I(x) \rightarrow \forall y I(x \cdot y))$$

and that I is a prime ideal:

$$\forall x \forall y (I(x \cdot y) \rightarrow (I(x) \vee I(y)))$$

but we cannot express that I is a maximal ideal.

It is possible to consider logics where such statements can be done: 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 2.4 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
$$f^M : M^n \to M$$
- 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 2.5 (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 2.6 (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 2.5, 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 2.6 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 24 Show that the following formulas are valid:

$$\begin{array}{l}
\varphi \leftrightarrow \neg\neg\varphi \\
\neg\varphi \leftrightarrow (\varphi \to \bot) \\
(\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi) \\
(\varphi \vee \psi) \leftrightarrow \neg(\neg\varphi \wedge \neg\psi) \\
(\varphi \wedge \psi) \leftrightarrow \neg(\neg\varphi \vee \neg\psi) \\
\exists x\varphi \leftrightarrow \neg\forall x\neg\varphi \\
\forall x\varphi \leftrightarrow \neg\exists x\neg\varphi
\end{array}$$

$$\begin{array}{l}
(\varphi \wedge (\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \chi)) \\
(\varphi \vee (\psi \wedge \chi)) \leftrightarrow ((\varphi \vee \psi) \wedge (\varphi \vee \chi)) \\
(\varphi \to (\psi \vee \chi)) \leftrightarrow ((\varphi \to \psi) \vee (\varphi \to \chi)) \\
(\varphi \to (\psi \wedge \chi)) \leftrightarrow ((\varphi \to \psi) \wedge (\varphi \to \chi))
\end{array}$$

In the following, assume that x does not occur in φ

$$\begin{array}{l}
(\varphi \to \exists x\psi) \leftrightarrow \exists x(\varphi \to \psi) \\
(\exists x\psi \to \varphi) \leftrightarrow \forall x(\psi \to \varphi) \\
(\forall x\psi \to \varphi) \leftrightarrow \exists x(\psi \to \varphi)
\end{array}$$

Exercise 25 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 26 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 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 27 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 28 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 equivalenc relation on M, etc.]

Exercise 29 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 30 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.

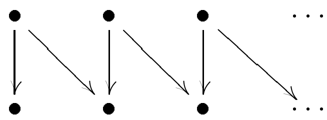
a) "Define" the numbers 0 and 1. That is, give L-formulas $\varphi_0(x)$ and $\varphi_1(x)$ with one free variable x, such that in both $\mathbb{Q}$ and $\mathbb{Z}$, $\varphi_i(a)$ is true exactly when $a = i$ $(i = 0, 1)$.

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

2.4 Examples of first order 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 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:

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

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

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

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!

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 31 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 discuss some first 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 if 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.

Exercise 32 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 2.7 (Compactness Theorem) *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 2.7 here, because it is a consequence of the Completeness Theorem (Theorem 3.6), which is proved in Chapter 3.

Exercise 33 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. Yet, there are still 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 34 Prove this.

Consequently, if T is the theory $\{\neg\phi_n \mid n \geq 1\}$, 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

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

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

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

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

Exercise 35 Conclude from this reasoning, that there can be no single sentence ϕ in the empty language, such that ϕ is true in exactly the infinite sets S.

Example 2. The language L_{grp} of groups has one constant e and one 1-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, 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:

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

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 36 Carry out the proof of the statement above.

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.

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:

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

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*.

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*.

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 $R \subseteq \mathbb{R}$.

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:

$$\{c > n \mid n \in \mathbb{N}\}$$

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, has developed into a subfield of Analysis; for a recent introduction, see the book *A Primer of Infinitesimal Analysis* by John Bell, Cambridge University Press 1998.

2.6 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 an L-formula ψ with at most the free variables $x_1, \ldots, x_n$ and which is moreover *quantifier-free* (meaning that in ψ no quantifiers occur), 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 $T \models \varphi \leftrightarrow \psi$.

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 37 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 2.8 *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 26 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. Our proof below is based on the book *Elements of Mathematical Logic* (Model Theory) by G. Kreisel and J.L. Krivine.

The language L is simply the language of commutative rings with 1, and T_{acf} has, besides the axioms for commutative rings with 1, the axioms:

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

where the last line describes an axiom for each $n \geq 1$ (so there are infinitely many axioms); and x^n abbreviates the term $\underbrace{x \cdot \cdots \cdot x}_{n}$.

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 $a, b_1, \ldots, b_n \in R$,

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

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

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

We need two preliminary lemmas.

Lemma 2.9 *Let $P(x, y_1, \ldots, y_n)$ and $Q(x, y_1, \ldots, y_n)$ be polynomials with coefficients in $\mathbb{Z}$. Then there is a quantifier-free L-formula $\varphi(y_1, \ldots, y_n)$ such that for every field K and elements $\xi_1, \ldots, \xi_n \in K$: $K \models \varphi(\xi_1, \ldots, \xi_n)$ if and only if, in the ring $K[x]$, the polynomial $P(x, \xi_1, \ldots, \xi_n)$ divides the polynomial $Q(x, \xi_1, \ldots, \xi_n)$.*

Proof. Let the degrees of P and Q in x be m and l, respectively, so that P and Q can be written as

$$\begin{aligned} P &= a_0 + a_1 x + \cdots + a_m x^m \\ Q &= b_0 + b_1 x + \cdots + b_l x^l \end{aligned}$$

where $a_0, \ldots, a_m, b_0, \ldots, b_l$ are polynomials in $y_1, \ldots, y_n$. We carry out an induction on $m + l$.

If $m + l = 0$ then in every field K, $P(x, \xi_1, \ldots, \xi_n)$ divides $Q(x, \xi_1, \ldots, \xi_n)$ if and only if either $a_0(\xi_1, \ldots, \xi_n) \neq 0$ or $b_0(\xi_1, \ldots, \xi_n) = 0$ (check this!), so we can take for φ the formula

$$\neg(a_0(y_1, \ldots, y_n) = 0) \vee b_0(y_1, \ldots, y_n) = 0$$

Now suppose $m + l = k$, and the lemma is proved for $m + l < k$. Distinguish cases as to whether $l < m$ or $l \geq m$.

If $l < m$, let P_1 be $a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$. By induction hypothesis, we have a quantifier-free formula ψ such that $K \models \psi(\xi_1, \ldots, \xi_n)$ if and only if $P_1(x, \xi_1, \ldots, \xi_n)$ divides $Q(x, \xi_1, \ldots, \xi_n)$. Now we can take for φ the formula:

$$(\psi(y_1, \ldots, y_n) \wedge a_m = 0) \vee (a_m \neq 0 \wedge \bigwedge_{i=0}^{l}(b_i = 0))$$

Check that this works!

If $l \geq m$, let again P_1 be $a_0 + \cdots + a_{m-1}x^{m-1}$ and put

$$Q_1 = a_m Q - b_l x^{l-m} P$$

Then the degree of Q_1 is at most $l-1$, so by induction hypothesis we have quantifier-free formulas ψ_1 and ψ_2 such that:

$$\begin{array}{lcl} K \models \psi_1(\xi_1, \ldots, \xi_n) & \Leftrightarrow & P_1(x, \xi_1, \ldots, \xi_n) \text{ divides } Q(x, \xi_1, \ldots, \xi_n) \\ K \models \psi_2(\xi_1, \ldots, \xi_n) & \Leftrightarrow & P(x, \xi_1, \ldots, \xi_n) \text{ divides } Q_1(x, \xi_1, \ldots, \xi_n) \end{array}$$

Now let $\varphi(y_1, \ldots, y_n)$ be the formula

$$(a_m = 0 \wedge \psi_1(y_1, \ldots, y_n)) \vee (a_m \neq 0 \wedge \psi_2(y_1, \ldots, y_n))$$

Again, check that this works! ∎

Another result that we need, is a cornerstone of commutative algebra (and algebraic geometry) and can be found, for example, in the book *Commutative Ring Theory* by Matsamura. We omit the proof.

Theorem 2.10 (Hilbert Nullstellensatz) *Let K be an algebraically closed field and I an ideal of the ring $K[X_1, \ldots, X_n]$. Denote by $V(I)$ the set*

$$\{(\xi_1, \ldots, \xi_n) \in K^n \mid \forall G \in I \, G(\xi_1, \ldots, \xi_n) = 0\}$$

Then for each $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, we have that $P(\xi_1, \ldots, \xi_n) = 0$ for all $(\xi_1, \ldots, \xi_n) \in V(I)$, if and only if there is a natural number n such that $P^n \in I$.

We are now ready to prove our quantifier elimination result.

Theorem 2.11 (Tarski) *T_{acf} admits elimination of quantifiers.*

Proof. By Lemma 2.8 and by the considerations following it, it suffices to look at formulas

$$\exists x(P_1(x) = 0 \wedge \cdots \wedge P_k(x) = 0 \wedge Q(x) \neq 0)$$

We distinguish cases and carry induction.

If $k = 0$ we have $\exists x Q(x) \neq 0$ where $Q(x) = b_0 + b_1 x + \cdots + b_l x^l$, and all b_i are polynomials in $y_1, \ldots, y_n$ with coefficients in $\mathbb{Z}$. Now every algebraically closed field is infinite, and a nonzero polynomial can have only finitely many roots, so $\exists x Q(x) \neq 0$ is T_{acf}-equivalent to the quantifier-free formula

$$b_0(y_1, \ldots, y_n) \neq 0 \vee \cdots \vee b_l(y_1, \ldots, y_n) \neq 0$$

If $k = 1$ we have $\exists x(P_1(x) = 0 \wedge Q(x) \neq 0)$. Now this is true for $\xi_1, \ldots, \xi_n$ in an algebraically closed field K, if and only if $Q(x, \xi_1, \ldots, \xi_n) \notin V(I)$ where I is the ideal generated by $P_1(x, \xi_1, \ldots, \xi_n)$. By Hilbert's Nullstellensatz (Theorem 2.10), this is the case iff for all N, $P_1(x, \xi_1, \ldots, \xi_n)$ is not a divisor of $Q(x, \xi_1, \ldots, \xi_n)^N$.

We use the fact that $K[x]$ is a unique factorization domain. P_1 is a divisor of Q^N for *some* N, iff every irreducible factor of P_1 divides Q; since the multiplicity of each irreducible factor in P_1 is at most the degree g of the polynomial $P_1(x, y_1, \ldots, y_n)$ in x, we see that if $P_1(x, \xi_1, \ldots, \xi_n)$ divides $Q(x, \xi_1, \ldots, \xi_n)^N$ for some N, then $P_1(x, \xi_1, \ldots, \xi_n)$ divides $Q(x, \xi_1, \ldots, \xi_n)^g$ (and the number g does not depend on the ξ's). By Lemma 2.9, this is equivalent to $K \models \psi(\xi_1, \ldots, \xi_n)$ for some quantifier-free ψ, so we can take $\neg\psi$ for our quantifier-free equivalent.

If $k > 1$, we may assume that the degree g_1 of P_1 in x is $\geq$ the degree g_2 of P_2. Let a_1 be the leading coefficient of P_1, so $P_1 = a_1 x^{g_1} + \cdots$, and let a_2 be the leading coefficient of P_2. Define:

$$\begin{aligned} P_1' &= a_2 P_1 - a_1 x^{g_1 - g_2} P_2 \\ P_2' &= P_2 - a_2 x^{g_2} \end{aligned}$$

Then, as is left for you to check, $\exists x(P_1 = 0 \wedge \cdots \wedge P_k = 0 \wedge Q \neq 0)$ is equivalent to

$$\begin{aligned} &(a_2 = 0 \wedge \exists x(P_1 = 0 \wedge P_2' = 0 \wedge \cdots \wedge P_k = 0 \wedge Q \neq 0)) \vee \\ &(a_2 \neq 0 \wedge \exists x(P_1' = 0 \wedge P_2 = 0 \wedge \cdots \wedge P_k = 0 \wedge Q \neq 0)) \end{aligned}$$

We have now obtained new simple formulas, but in each of them the sum of the degrees of the P_i has gone down by at least 1.

Eventually, we arrive at the case that $\sum_{i=1}^n g_i = 0$, which is essentially already treated. ∎

2.7 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 2.12 (Upwards 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 38 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 more involved. Before going into it, we introduce some terminology.

Definition 2.13 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 $x_1, \dots, x_n \in N$, $f^M(x_1, \dots, x_n)$ is an element of N, and equal to $f^N(x_1, \dots, x_n)$);
- $R^N = R^M \cap N^n$ for every n-place relation symbol R of L (this means that for $x_1, \dots, x_n \in N$, $(x_1, \dots, x_n) \in R^M$ if and only if $(x_1, \dots, x_n) \in R^M$).

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 39 Let $N \subseteq M$ be a substructure. Show that for every quantifier-free L-formula φ with variables $x_1, \dots, x_n$ and elements $m_1, \dots, m_n$ of N, we have

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

Exercise 40 Suppose N is a model of the L-theory T. Let T_N be the L_N-theory which has, besides the axioms for T, as axioms all quantifier-free L_N-sentences which are true in N. Show that a model of T_N is essentially the same thing as a model of T which contains N as a submodel.

If M is an L-structure and $N \subseteq M$ is a 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.

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 41 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

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

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

Definition 2.14 A substructure $N \subseteq M$ is called an *elementary substructure*, written $N \preceq M$, if the equivalence of Exercise 39 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 $M \preceq N$ 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 we wish to point out that the so-called *theory of dense linear orders without end-points*, of which both $\mathbb{Q}$ and $\mathbb{R}$ are models, has quantifier elimination. Hence the statement follows from the following exercise.

Exercise 42 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.

Exercise 43 Suppose N is an L-structure. Let $E(N)$ be the set of all L_N-sentences which are true in N. In analogy to Exercise 40, prove that a model of $E(N)$ is essentially the same thing as an L-structure M which contains N as elementary substructure.

Exercise 44 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]

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.

We obtain the following strengthening of Theorem 2.12.

Corollary 2.15 *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 2.12 to the theory $E(N)$ (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 $\|L\|$, by definition the cardinality of the set of L-formulas.

Exercise 45 Show that $\|L\| = |L|$ if L is infinite, and that $\|L\| = \omega$ if L is finite.

Theorem 2.16 (Downwards 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 $|N| = \|L\|$.*

Proof. We shall only prove the theorem for $\|L\| = \omega$ (so L 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. 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 41. 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 $f(m_1, \ldots, m_k) \in N_k \subseteq C_{k+1} \subseteq N$. And N is the union of a countable family of countable subsets of M, so N is countable.

It remains to prove that N is an elementary substructure of M. For this, we use the characterization given in Exercise 44. 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 44, N is an elementary substructure of M. ∎

We wrap up this section by putting together Corollary 2.15 and Theorem 2.16 to obtain the following useful conclusion:

Corollary 2.17 *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 2.15 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 extra constants from C. The injective function $C \to M'$ makes M' into an L_C-structure. Clearly $|C| \leq \|L_C\|$. Applying Theorem 2.16 with L_C in the place 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. ∎

2.8 Isomorphisms of L-structures; applications of the Löwenheim-Skolem Theorems

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 basis for V, then $|V| = |k| \times |B|$); 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.

Now 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 2.17 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). We feel that this should be impossible, and that we therefore always must have either $T_k^\infty \models \varphi$ or $T_k^\infty \models \neg\varphi$, in other words that the theory of infinite k-vector spaces is complete.

In fact, this reasoning is justified by the following general definition and subsequent exercise.

Definition 2.18 (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) $\beta(f^M(x_1, \dots, x_n)) = f^N(\beta(x_1), \dots, \beta(x_n))$ for every n-place function symbol f of L and every $x_1, \dots, x_n \in M$;

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

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 at least, as it should be, symmetric.

Exercise 46 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.

You should of course verify that an isomorphism of L_k-structures between two vector spaces is the same thing as an isomorphism of vector spaces; similarly, an isomorphism of L_{grp}-structures between groups is nothing but an isomorphism of groups; etcetera.

Definition 2.19 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 2.20 (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 47 Prove Theorem 2.20.

We conclude this chapter by giving an example of a theory which is ω-categorical; the theory of *dense linear order 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 2.21 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:

$$\begin{array}{rl}
\forall x \neg(x < x) & \text{irreflexivity} \\
\forall xyz(x < y \wedge y < z \to x < z) & \text{transitivity} \\
\forall xy(x < y \vee x = y \vee y < x) & \text{linearity} \\
\forall xy(x < y \to \exists z(x < z \wedge z < y)) & \text{density} \\
\forall x \exists yz(y < x \wedge x < z) & \text{no end points}
\end{array}$$

Theorem 2.22 (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 $M = \{m_0, m_1, \dots\}$ and $N = \{n_0, n_1, \dots\}$ 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:

$$\begin{tikzcd}
M_0 \arrow[r] \arrow[d, "\beta_0"'] & M_1 \arrow[r] \arrow[d, "\beta_1"'] & M_2 \arrow[d, "\beta_2"'] & \cdots \\
N_0 \arrow[r] & N_1 \arrow[r] & N_2 & \cdots
\end{tikzcd}$$

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, $\{m_0, \dots, m_k\} \subseteq M_k$ and $\{n_0, \dots, n_k\} \subseteq N_k$, 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 as 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 48 Show that the theory T_d is complete.

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, we have $M \models \phi$.

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 the lecture course in Recursion Theory for a precise meaning of this).

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*.

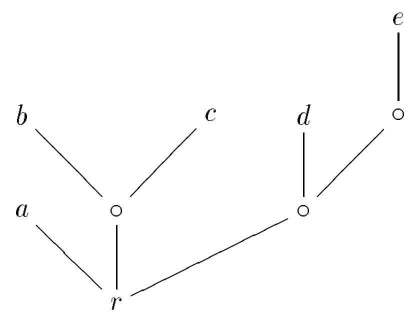
Definition 3.1 A *tree* is a partial order $(T, \leq)$ which has a least element, and is such that for every $x \in T$, the set

$$\downarrow(x) \equiv \{y \in T \mid y \leq x\}$$

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 49 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_1-*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.

Show that a finite tree is the same thing as a finite set V together with a connected T_1-hierarchy on V.

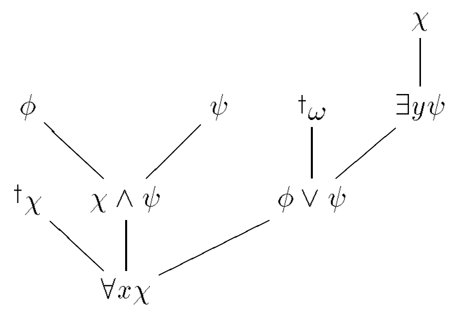
d) Let $\mathcal{B}$ be a set of finite trees such that for every finite tree there is exactly one element of $\mathcal{B}$ which is isomorphic to it. Let L be the language with one constant c and for every $n \in \mathbb{N}_{\geq 1}$ exactly one function symbol F_n of arity n. Show that $\mathcal{B}$ can be made into an L-structure such that for every other L-structure M and every $m \in M$, there is a unique function $f : \mathcal{B} \to M$ with the properties:

   i) $f(c) = m$, and

   ii) for all $n \in \mathbb{N}_{\geq 1}$ and every n-tuple $(b_1, \ldots, b_n)$ from $\mathcal{B}$,

$$f(F_n(b_1, \ldots, b_n)) = (F_n)^M(f(b_1), \ldots, f(b_n))$$

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 3.2 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 3.3 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 $x = r$, 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 50 Show that 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.

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, the reader is 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 3.3 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).

$\to I$ 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 $\Sigma(T'; \psi \to \varphi)$ is an element of T ($\to$-introduction).

$\to E$ Suppose T and S are elements of $\mathcal{P}$ with conclusions $\varphi \to \psi$ and φ, respectively. Then $\Sigma(T, S; \psi)$ is an element of $\mathcal{P}$ ($\to$-elimination).

$\neg I$ Suppose T is an element of $\mathcal{P}$ with conclusion $\perp$. 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 $\Sigma(T, S; \perp)$ is an element of $\mathcal{P}$ ($\neg$-elimination).

$\perp E$ Suppose T is an element of $\mathcal{P}$ with conclusion $\perp$. 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 $\mathcal{P}$ ($\perp$-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 φ, and u is a variable which doesn't occur in any unmarked assumption of T (and is not bound in φ). Then $\Sigma(T; \forall u\varphi)$ is an element of $\mathcal{P}$ ($\forall$-introduction).

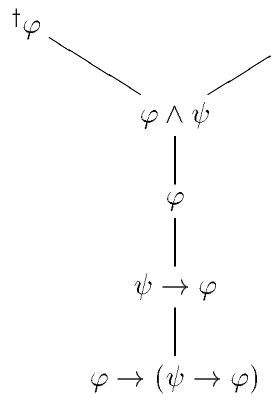
$\forall E$ Suppose T is an element of $\mathcal{P}$ with conclusion $\forall u\varphi$, and t is a term such that the substitution $\varphi[t/u]$ is defined. Then $\Sigma(T; \varphi[t/u])$ is an element of $\mathcal{P}$ ($\forall$-elimination).

$\exists I$ 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).

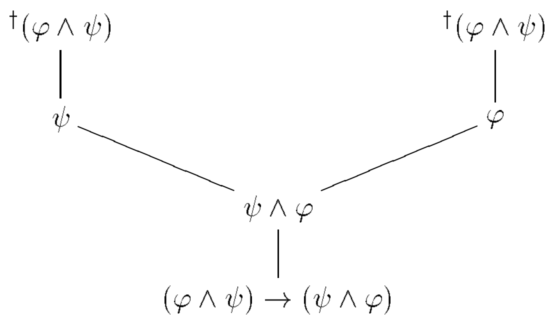
$\exists E$ Suppose T and S are elements of $\mathcal{P}$ with conclusions $\exists x\varphi$ and χ, respectively. Let u be a variable which doesn't occur in φ or χ, and is such that the only unmarked assumptions of S in which u occurs, are of the form $\varphi[u/x]$. Let V be the set of leaves of S 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)

$$\dfrac{\perp}{\varphi}$$

“Ex falso sequitur quodlibet”

d)

$$\dfrac{\dfrac{\dfrac{{}^{\dagger}(\neg(\varphi\wedge\psi)) \qquad \dfrac{\dfrac{\dfrac{{}^{\dagger}(\neg(\neg\varphi\vee\neg\psi)) \quad \dfrac{{}^{\dagger}(\neg\varphi)}{\neg\varphi\vee\neg\psi}}{\perp}}{\varphi} \qquad \dfrac{\dfrac{{}^{\dagger}(\neg(\neg\varphi\vee\neg\psi)) \quad \dfrac{{}^{\dagger}(\neg\psi)}{\neg\varphi\vee\neg\psi}}{\perp}}{\psi}}{\varphi\wedge\psi}}{\perp}}{\neg\varphi\vee\neg\psi}}{\neg(\varphi\wedge\psi)\to(\neg\varphi\vee\neg\psi)}$$

e)

$$\dfrac{\dfrac{{}^{\dagger}(\neg\varphi\vee\neg\psi) \qquad \dfrac{\dfrac{{}^{\dagger}(\neg\varphi) \quad \dfrac{{}^{\dagger}(\varphi\wedge\psi)}{\varphi}}{\perp}}{\neg(\varphi\wedge\psi)} \qquad \dfrac{\dfrac{{}^{\dagger}(\neg\psi) \quad \dfrac{{}^{\dagger}(\varphi\wedge\psi)}{\psi}}{\perp}}{\neg(\varphi\wedge\psi)}}{\neg(\varphi\wedge\psi)}}{(\neg\varphi\vee\neg\psi)\to\neg(\varphi\wedge\psi)}$$

Definition 3.4 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 51 (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

$$\begin{array}{c} {}^{\dagger}\varphi \\ | \\ \varphi \to \varphi \end{array}$$

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

$$\begin{array}{c} {}^{\dagger}\varphi \\ | \\ \to I \ \varphi \to \varphi \end{array}$$

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 3.3, 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:

$$\dfrac{{}^{\dagger}\varphi^1}{\varphi\to\varphi}\to I,1$$

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)

$$\dfrac{\dfrac{\dfrac{\dfrac{{}^{\dagger}\varphi^1 \qquad {}^{\dagger}\psi^2}{\varphi\wedge\psi}\wedge I}{\varphi}\wedge E}{\psi\to\varphi}\to I,2}{\varphi\to(\psi\to\varphi)}\to I,1$$

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)

$$\dfrac{\bot}{\varphi}\bot E$$

d)

$$\dfrac{\dfrac{\dfrac{{}^{\dagger}\neg(\varphi\wedge\psi)^4 \qquad \dfrac{\dfrac{\dfrac{{}^{\dagger}\neg(\neg\varphi\vee\neg\psi)^3 \qquad \dfrac{{}^{\dagger}\neg\varphi^1}{\neg\varphi\vee\neg\psi}\vee I}{\bot}\neg E}{\varphi}\bot E,1 \qquad \dfrac{\dfrac{{}^{\dagger}\neg(\neg\varphi\vee\neg\psi)^3 \qquad \dfrac{{}^{\dagger}\neg\psi^2}{\neg\varphi\vee\neg\psi}\vee I}{\bot}\neg E}{\psi}\bot E,2}{\varphi\wedge\psi}\wedge I}{\bot}\neg E}{\neg\varphi\vee\neg\psi}\bot E,3}{\neg(\varphi\wedge\psi)\to(\neg\varphi\vee\neg\psi)}\to I,4$$

e)

$$
\dfrac{{}^{\dagger}\neg\varphi\vee\neg\psi^{5} \qquad \dfrac{\dfrac{{}^{\dagger}\neg\varphi^{3} \qquad \dfrac{{}^{\dagger}\varphi\wedge\psi^{1}}{\varphi}\wedge E}{\bot}\neg E}{\neg(\varphi\wedge\psi)}\neg I,1 \qquad \dfrac{\dfrac{{}^{\dagger}\neg\psi^{4} \qquad \dfrac{{}^{\dagger}\varphi\wedge\psi^{2}}{\psi}\wedge E}{\bot}\neg E}{\neg(\varphi\wedge\psi)}\neg I,2}{\dfrac{\neg(\varphi\wedge\psi)}{(\neg\varphi\vee\neg\psi)\to\neg(\varphi\wedge\psi)}\to I,5}\vee E,3,4
$$

Some more examples:

f) A proof tree for $t = s \vdash s = t$:

$$
\dfrac{\dfrac{\forall x(x=x)}{t=t}\forall E \qquad t=s}{s=t}\text{Subst}
$$

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)

$$
\dfrac{\dfrac{\dfrac{\dfrac{{}^{\dagger}\neg\exists x\varphi(x)^{2} \qquad \dfrac{{}^{\dagger}\varphi(y)^{1}}{\exists x\varphi(x)}\exists I}{\bot}\neg E}{\neg\varphi(y)}\neg I,1}{\forall x\neg\varphi(x)}\forall I}{\neg\exists x\varphi(x)\to\forall x\neg\varphi(x)}\to I,2
$$

You should check why application of $\forall I$ is justified in this tree.

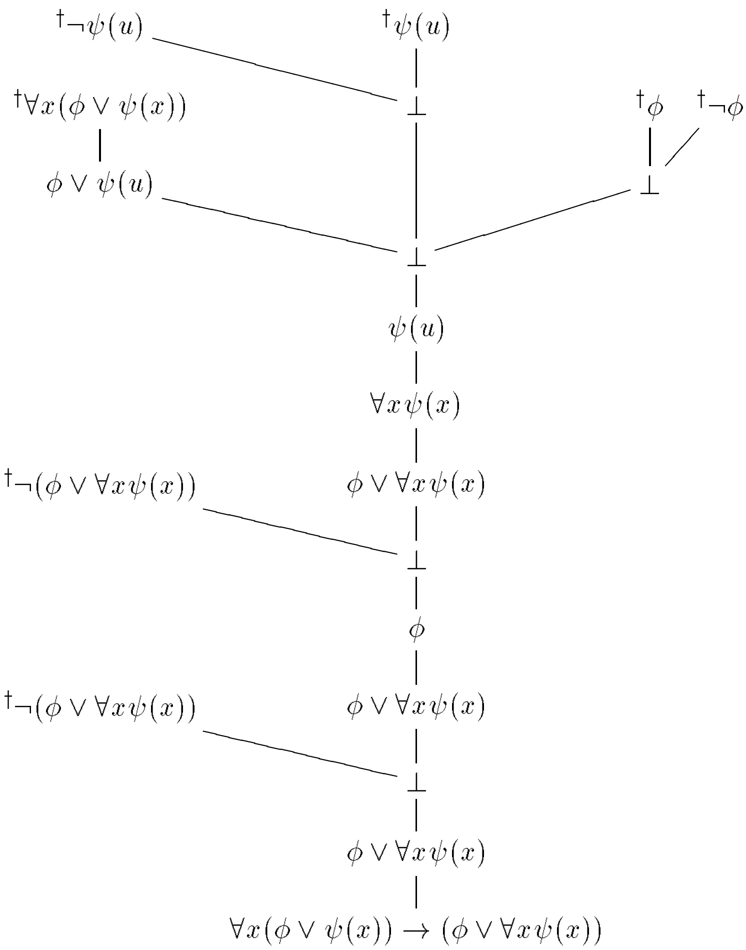
h) The following tree gives an example of the $\exists E$-construction:

$$
\dfrac{\dfrac{\dfrac{{}^{\dagger}\exists x\varphi(x)^{2} \qquad \dfrac{\dfrac{{}^{\dagger}\forall x\neg\varphi(x)^{3}}{\neg\varphi(y)}\forall E \qquad {}^{\dagger}\varphi(y)^{1}}{\bot}\neg E}{\bot}\exists E,1}{\neg\exists x\varphi(x)}\neg I,2}{\forall x\neg\varphi(x)\to\neg\exists x\varphi(x)}\to I,3
$$

i)

$$
\begin{prooftree}
\AxiomC{$^\dagger\neg\forall x\neg\varphi(x)^3$}
\AxiomC{$^\dagger\neg\exists x\varphi(x)^2$}
\AxiomC{$^\dagger\varphi(y)^1$}
\RightLabel{$\exists I$}
\UnaryInfC{$\exists x\varphi(x)$}
\RightLabel{$\neg E$}
\BinaryInfC{$\bot$}
\RightLabel{$\neg I, 1$}
\UnaryInfC{$\neg\varphi(y)$}
\RightLabel{$\forall I$}
\UnaryInfC{$\forall x\neg\varphi(x)$}
\RightLabel{$\neg E$}
\BinaryInfC{$\bot$}
\RightLabel{$\bot E, 2$}
\UnaryInfC{$\exists x\varphi(x)$}
\RightLabel{$\to I, 2$}
\UnaryInfC{$\neg\forall x\neg\varphi(x) \to \exists x\varphi(x)$}
\end{prooftree}
$$

j) The following tree is given in undecorated style; it is a good exercise to decorate it. It is assumed that the variable x does 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 $\phi_1 \rightarrow \phi_2$, transform the problem into $\Gamma \cup \{\phi_1\} \vdash \phi_2$;

If ϕ is a negation $\neg\psi$, transform into $\Gamma \cup \{\psi\} \vdash \perp$;

If ϕ is of form $\forall x \psi(x)$, transform into $\Gamma \vdash \psi(u)$;

In all other (non-obvious) cases, try $\Gamma \cup \{\neg\phi\} \vdash \bot$.

Exercise 52 Construct proof trees for the equivalences of Exercise 24. 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 tree φ and is closed under a number of constructions (definition 3.3), $\mathcal{P}$ is susceptible to proofs by *induction* over proof trees: if $\mathcal{A}$ is any set of labelled trees which contains 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 such that the conclusion of T is of the form $\varphi[c/u]$, where c is a constant that does not occur in any unmarked assumption of T, and v is a variable which doesn't occur anywhere in T, then replacing c by v throughout in T, results in a new proof tree.

In the proof of the Soundness Theorem (section 3.2 below) we shall also apply induction over proof trees.

Exercise 53 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) If $\varphi \in \Gamma$, then $\Gamma \vdash_H \varphi$;

ii) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \psi$ then $\Gamma \vdash_H (\varphi \wedge \psi)$, and conversely;

iii) if $\Gamma \vdash_H \varphi$ or $\Gamma \vdash_H \psi$, then $\Gamma \vdash_H (\varphi \vee \psi)$;

iv) if $\Gamma \cup \{\varphi\} \vdash_H \chi$ and $\Gamma \cup \{\psi\} \vdash_H \chi$, then $\Gamma \cup \{\varphi \vee \psi\} \vdash_H \chi$;

v) if $\Gamma \cup \{\varphi\} \vdash \bot$, then $\Gamma \vdash_H \neg\varphi$;

vi) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \neg\varphi$ then $\Gamma \vdash_H \bot$;

vii) if $\Gamma \cup \{\neg\varphi\} \vdash_H \bot$ then $\Gamma \vdash_H \varphi$;

viii) if $\Gamma \cup \{\varphi\} \vdash_H \psi$ then $\Gamma \vdash_H \varphi \to \psi$;

ix) if $\Gamma \vdash_H \varphi$ and $\Gamma \vdash_H \varphi \to \psi$ then $\Gamma \vdash_H \psi$;

x) if $\Gamma \vdash_H \psi(u)$ and u does not occur in Γ, then $\Gamma \vdash_H \forall x \psi(x)$;

xi) if $\Gamma \vdash_H \forall x \psi(x)$ then if $\psi[t/x]$ is defined, $\Gamma \vdash_H \psi[t/x]$;

xii) if $\psi[t/x]$ is defined and $\Gamma \vdash_H \psi[t/x]$, then $\Gamma \vdash_H \exists x \psi(x)$;

xiii) if $\Gamma \cup \{\psi(u)\} \vdash_H \chi$ and u does not occur in Γ or χ, then $\Gamma \cup \{\exists x \psi(x)\} \vdash_H \chi$.

Show that the relation $\Gamma \vdash_H \varphi$ coincides with the relation $\Gamma \vdash \varphi$ from Definition 3.4.

3.2 Soundness and Completeness

We compare the relation $\Gamma \vdash \phi$ from Definition 3.4 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 3.5 (Soundness Theorem) *If $\Gamma \vdash \phi$ then $\Gamma \models \phi$.*

Theorem 3.6 (Completeness Theorem; Gödel, 1930) *If $\Gamma \models \phi$ then $\Gamma \vdash \phi$.*

The Soundness Theorem follows easily from the following lemma:

Lemma 3.7 *Suppose T is an L-labelled proof tree with unmarked assumptions $\varphi_1, \dots, \varphi_n$ and conclusion ψ; let $u_1, \dots, u_k$ be a list of all variables that are free in at least one of $\varphi_1, \dots, \varphi_n, \psi$. Then for every L-structure M and any k-tuple $m_1, \dots, m_k$ of elements of M, we have:*

If for all i, $1 \leq i \leq n$, $M \models \varphi_i[m_1/u_1, \dots, m_k/u_k]$, then
$M \models \psi[m_1/u_1, \dots, m_k/u_k]$.

Exercise 54 Prove yourself, that Lemma 3.7 implies Theorem 3.5.

Proof. Lemma 3.7 is proved by a straightforward induction on proof trees: let $\mathcal{A}$ be the set of L-labelled 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 3.3. 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 $\to$-introduction from $S \in \mathcal{A}$; say S has conclusion ψ and T has conclusion $\phi \to \psi$. 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 $M \models (\phi \to \psi)[\vec{m}/\vec{u}]$. 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 $\exists x \varphi(x)$, the conclusion of S' is χ, and S' has possibly unmarked assumptions of form $\varphi[v/x]$ where v does not occur in any other unmarked assumption of S', nor in φ, nor in χ. Suppose that $M \models \psi[\vec{m}/\vec{u}]$ for each unmarked assumption ψ of S, and for each unmarked assumption ψ of S' distinct from $\varphi[v/x]$. Then $M \models (\exists x \varphi(x))[\vec{m}/\vec{u}]$ since $S \in \mathcal{A}$; say $M \models \varphi[\vec{m}/\vec{u}, p/x]$. Now it follows that, since also $S' \in \mathcal{A}$, $M \models \chi[\vec{m}/\vec{u}]$. Hence, $T \in \mathcal{A}$. ∎

Exercise 55 Supply yourself the induction step for the case of $\vee$-elimination, in the proof above.

For the proof of the Completeness Theorem (3.6), 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 56 Prove these facts.

Therefore, the statement of 3.6 reduces to the special case: if $\Gamma \models \bot$, then $\Gamma \vdash \bot$. We shall prove the contrapositive of this, viz.: if $\Gamma \not\vdash \bot$, 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 57 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 $\Gamma \nvdash \phi$, $\Gamma \cup \{\phi\}$ is a proper extension of Γ. Use maximality of Γ.

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 3.8 *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 $C/\sim$ 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

$$R^M = \{([c_1], \ldots, [c_n]) \mid \Gamma \vdash R(c_1, \ldots, c_n)\}$$

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.

Suppose $\phi \equiv \psi \vee \chi$. 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 $\Gamma \vdash \psi$, if and only if (by Exercise 57, since Γ is maximally formally consistent) $\Gamma \vdash \psi \vee \chi$.

The step for $\phi \equiv \neg\psi$ is similar, and the steps for $\wedge$ and $\rightarrow$ are left to you.

Now suppose $\phi \equiv \forall x \psi(x)$. We see that $\Gamma \models \phi$ 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 $\Gamma \vdash \exists x \neg\psi(x) \rightarrow \neg\psi(c)$. Then since $\Gamma \vdash \psi(c)$, we must have $\Gamma \vdash \neg\exists x \neg\psi(x)$. By one of the items of Exercise 52, $\Gamma \vdash \forall x \psi(x)$.

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 3.8 to Theorem 3.6.

Lemma 3.9 *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 3.9, let us wrap up the argument for Theorem 3.6 from it: given a formally consistent Γ, take Δ as in Lemma 3.9. By Lemma 3.8, 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 14a), $|C| = \omega \times |C|$; therefore, we can write C as a disjoint union:

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

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

$$F_n = \{\varphi(x) \mid \varphi(x) \text{ is an } L_n\text{-formula with one free variable } x\}$$

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

$$\Gamma_{n+1} = \Gamma_n \cup \{\exists x \varphi(x) \to \varphi(c_{\varphi(x)}) \mid \varphi(x) \in F_n\}$$

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

$$\Gamma_n \cup \{\exists x \varphi_i(x) \to \varphi_i(c_{\varphi_i(x)}) \mid 1 \leq i \leq m\} \vdash \phi$$

Combining Exercise 51 and the equivalences of Exercise 52, this is equivalent to (check!):

$$\Gamma_n \vdash \bigvee_{i=1}^{m} \neg(\exists x \varphi_i(x) \to \varphi(c_{\varphi_i(x)})) \vee \phi$$

Now the constants $c_{\varphi_i(x)}$ are not in L_n, hence don't occur in Γ_n. 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 consistent set of L'-sentences; this is done with the help of Zorn's Lemma (Definition 1.15).

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 $\Gamma \vdash \bot$ for some $\Gamma \in \mathcal{K}$ (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 3.10 (Compactness Theorem (2.7)) *If Γ is a set of L-sentences such that 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 58 Show that our proof of the Completeness Theorem has the corollary, that every consistent set of L-sentences has a model of cardinality at most $\|L\|$. Compare this to Theorem 2.16.

Exercise 59 (Skolem Functions) A *Skolem Theory* is a set of sentences δ, such that for every formula φ in the language under discussion, there is a function symbol F such that

$$\Delta \vdash \forall\vec{x}\,(\exists y\varphi(\vec{x}, y) \to \varphi(\vec{x}, F(\vec{x})))$$

Let Γ be a set of L-sentences. Show that there is an extension L' of L, and a Skolem theory Δ in L', which is conservative over Γ (recall that this means: if $\Delta \vdash \phi$ and ϕ is an L-sentence, then $\Gamma \vdash \phi$).

[Hint: 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*). 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 Completeness to conclude that Δ is conservative over Γ.]

Index