A Short Course on Mathematical Logic

Jouko Väänänen

December 28, 2018

Contents

Preface

This book is based on lectures the author has given in the Department of Mathematics and Statistics in the University of Helsinki during several decades. As the title reveals, this is a mathematics course, but it can also serve philosophy and computer science students. The presentation is self-contained, although the reader is assumed to be familiar with elementary set-theoretical notation and with proofs by induction.

The idea is to give basic completeness and incompleteness results in an unaffected and straightforward way without delving into all the elaboration that modern mathematical logic involves. There is a section "Further reading" guiding the reader to the rich literature on more advanced results.

I am indebted to the many students who have followed the course as well as to the teachers who have taught it in addition to myself, in particular Tapani Hyttinen, Åsa Hirvonen and Taneli Huuskonen. The book has existed as a manuscript in Finnish for a long time and all the members of the Helsinki Logic Group have greatly contributed to its final form. Each chapter ends with exercises. These exercises have been developed over the years by all members of the Helsinki Logic Group. Unfortunately I cannot give credit to their inventors because sufficient records have not been kept.

Helsinki 25.12.2016
Jouko Väänänen

Chapter 1

Introduction

The fundamental concepts of logic are

- *Sentence*, such as “Every non-negative number has a square root”.
- *Formula*, such as “The number x has a square root” or “x gets a higher salary than y”.
- *Model*, *structure*, such as the field of rational numbers, or a database.
- *Proof*, such as the proof of Fermat’s Last Theorem given by Andrew Wiles in 1994.
- *Truth*, such as “Every non-negative number has a square root” which is true in the field[1] of real numbers, but not in the field of rational numbers.

We will define the above fundamental concepts accurately—mathematically—and prove their basic properties:

- Easy property: Provable sentences are true in all models.
- A bit more difficult property: A sentence that is true in all models is provable.
- A difficult property: Many concepts that are important for mathematics are *incomplete* in the sense that when they are axiomatized, there are sentences that can neither be proved true nor be proved false.

The goal of this book is to prove these three properties. One may ask, is it not circular to prove something about provability, or establish truths about truth? The answer is “no”, but we have to proceed with care and avoid rushing to conclusions. We follow the path taken by Alfred Tarski: We assume mathematics, such as set theory, algebra, topology, measure theory, etc as the firm basis on which we base our investigation of logical concepts. Our results give us insights

[1] At this point it is not important to know what *fields* are.

into the nature and fundamental properties of the concepts of proof and truth. In this book we are not concerned with the question which naturally suggests itself, namely what is mathematics itself based on. We simply take the validity and consistency of mathematics as given. This may come as a disappointment to a reader who, like early researchers Gottlob Frege, Bertrand Russell, Rudolph Carnap and David Hilbert, hopes that logic can bring ultimate certainty to mathematics. The last result of this book, Gödel's Incompleteness Theorem from 1931, has inspired generations of mathematicians, logicians, philosophers, computer scientists and even general public, to contemplate whether mathematics is something that stands on its own feet and logic is just a tool to understand salient features of this edifice. Be it as it may, this book introduces the reader to this tool called logic.

Notation

We use ordinary set-theoretical notation such as

$$\{a_1, \ldots, a_n\}, A \cap B, A \cup B, A \setminus B, \emptyset.$$

The set $\{0, 1, 2, \ldots\}$ of natural numbers is denoted $\mathbb{N}$. The *ordered pair* of a and b is denoted $\langle a, b\rangle$. Ordered pairs satisfy

$$\langle a, b\rangle = \langle c, d\rangle \iff a = c \text{ and } b = d.$$

An ordered sequence is denoted $\langle a_1, \ldots, a_n\rangle$. It satisfies:

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \iff a_1 = b_1 \text{ and ... and } a_n = b_n.$$

The cartesian product $A \times A$ is denoted A^2 and n-fold product A^n.

A set is *finite* if it is of the form $\{a_1, \ldots, a_n\}$ for some natural number n, and otherwise infinite. A set is *countable* if it is of the form $\{a_n : n \in \mathbb{N}\}$, otherwise *uncountable*, and *countably infinite* if it is countable but not finite.

Chapter 2

Propositional logic

Propositional logic is the oldest and in many ways the simplest part of logic. Mathematically propositional logic is extremely elementary, but computationally it offers formidable challenges. The famous $P{=}NP$ problem[1] goes right to the heart of propositional logic. Computational properties of propositional logic are important because computers are built using electronic circuits based on propositional logic.

2.1 Propositional formulas

Propositional logic investigates logical properties of very simple but at the same time very exactly defined formulas. These formulas are called *propositional formulas*. They are built from so-called *proposition symbols* $p_0, p_1, \ldots$ by means of the *connectives*

$\neg$	*negation*
$\wedge$	*conjunction*
$\vee$	*disjunction*
$\rightarrow$	*implication*
$\leftrightarrow$	*equivalence*

In a mathematical investigation of propositional logic it is simplest to choose certain connectives as basic symbols in terms of which the others are defined. Following the Polish logician Jan Łukasiewicz (1878–1956) we choose negation and implication as the basic symbols, and define *propositional formulas* as follows:

Definition 2.1 (Propositional formulas) *(P1) Proposition symbols* $p_0, p_1, \ldots$ *are propositional formulas.*

(P2) If A *is a propositional formula, then so is* $\neg A$*.*

[1] This is the problem whether there is a polynomial $P(n)$ such that the validity of a propositional formula built up from n proposition symbols can be checked in $P(n)$ steps.

(P3) If A and B are propositional formulas, then so is $(A \to B)$.

Convention: The outermost parentheses of a formula need not be displayed.

Example 2.2 *The following are propositional formulas* $p_0, (p_0 \to p_0), (p_1 \to \neg(p_2 \to p_1)), (((p_0 \to p_1) \to \neg p_2) \to p_3)$.

A basic concept in propositional logic is *provability*, which we now define by first introducing the *axioms*:

Definition 2.3 (Provability) *The axioms of propositional logic are defined as follows:*

- *If A and B are propositional formulas, then*

  (A1) $(A \to (B \to A))$

  is an axiom.
- *If A and B are propositional formulas, then*

  (A2) $((\neg B \to \neg A) \to (A \to B))$

  is an axiom.
- *If A, B and C are propositional formulas, then*

  (A3) $(((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$

  is an axiom.

The set of propositional formulas provable *from a set S of propositional formulas is defined as follows:*

(T1) Every element of S is provable from S.

(T2) Every axiom is provable from S.

*(T3) If A and $(A \to B)$ are provable from S, then also B is provable from S. (*Modus Ponens *-rule)*

If A is provable from S, we write $S \vdash A$. If $\emptyset \vdash A$, we write $\vdash A$ and say that A is provable.

The idea of axiom (A1) is that if we know A to be true, the matter does not change[2] if we add a new assumption B. Axiom (A2) is called the *Law of Contraposition*. It encapsulates the idea of an *indirect proof*: If the denial of B contradicts A and we know A to be true, then B has to be true. Axiom (A3) is a kind of transitivity property of implication: If assuming A, C follows from B, then if in addition we know that B follows from A, then C follows from A.

[2] In the so called *non-monotonic reasoning* a new assumption may change some conclusions.

Example 2.4 *The following are provable propositional formulas*

$$
\begin{array}{l}
(p_0 \to (p_1 \to p_0)) \\
((\neg p_0 \to \neg p_1) \to (p_1 \to p_0)) \\
(((p_0 \to (p_1 \to p_0)) \to ((p_0 \to p_1) \to (p_0 \to p_0))) \\
((p_0 \to p_1) \to (p_0 \to p_0)).
\end{array}
$$

The last formula follows from the first and the third by Modus Ponens.

Example 2.5

$$
\begin{array}{l}
\{A, (A \to B)\} \vdash B \\
\{A\} \vdash (B \to A) \\
\{(\neg B \to \neg A)\} \vdash (A \to B) \\
\{(\neg B \to \neg A), A\} \vdash B \\
\{(A \to (B \to C))\} \vdash ((A \to B) \to (A \to C)) \\
\{(A \to (B \to C)), (A \to B)\} \vdash (A \to C) \\
\{(A \to (B \to C)), (A \to B), A\} \vdash C
\end{array}
$$

The definition of provability (Definition 2.3) is an example of an *inductive definition*. The basis of the induction are (T1) and (T2), while (T3) is the induction step. When we prove that a formula A is provable from a set S, we have to establish an induction from the axioms and elements of S to A. In practice this consists of writing down a list of formulas, one under another, with axioms or elements of S in the beginning, in each step following the Definition 2.3, until we reach A. Every step (i.e. row of the list) has to be either an axiom, an element of S, or follow from previous rows by Modus Ponens (MP). Such a list is called a *deduction*, a *derivation* or an *inference*. Building a deduction is not necessarily easy. Often one has to first decide on a strategy. Here is an example:

Theorem 2.6 $\vdash (A \to A)$

Proof. The idea is the following: By (A3),

$$((A \to (B \to A)) \to ((A \to B) \to (A \to A)))$$

is provable. On the other hand, $(A \to (B \to A))$ is provable, so MP gives

$$((A \to B) \to (A \to A)).$$

We would be done, if $(A \to B)$ were provable. So let us choose B so that $(A \to B)$ *is* provable. Choose $B = (A \to A)$. Thus we build the following list:

1.	$(A \to (B \to A))$	(A1)
2.	$((A \to (B \to A)) \to ((A \to B) \to (A \to A)))$	(A3)
3.	$((A \to B) \to (A \to A))$	MP 1,2
4.	$(A \to B)$	(A1)
5.	$(A \to A)$	MP 3,4

In the list we mention at the end of each row the reason why this row is there and why it abides by Definition 2.3. □

Theorem 2.7 $\vdash (\neg A \to (A \to B))$

Proof. Axiom (A1) gives

$$(\neg A \to (\neg B \to \neg A)),$$

which, when combined with axiom (A2)

$$((\neg B \to \neg A) \to (A \to B))$$

and axiom (A3) leads to the desired conclusion. For clarity we denote $C = (\neg B \to \neg A)$ and $D = (A \to B)$.

1.	$(C \to D)$	(A2)
2.	$((C \to D) \to (\neg A \to (C \to D)))$	(A1)
3.	$(\neg A \to (C \to D))$	MP 1,2
4.	$((\neg A \to (C \to D)) \to ((\neg A \to C) \to (\neg A \to D))$	(A3)
5.	$((\neg A \to C) \to (\neg A \to D))$	MP 3,4
6.	$(\neg A \to C)$	(A1)
7.	$(\neg A \to D)$	MP 5,6

□

We shall now prove a very useful general property of provable propositional formulas. It shows that the relationship between implication and provability is in harmony with our intuition.

Theorem 2.8 (Deduction Lemma) *If $S \cup \{A\} \vdash B$, then $S \vdash (A \to B)$ (and conversely).*

Proof. We use induction on provable formulas: (1) $B \in S$. Then $S \vdash B$. On the other hand $S \vdash (B \to (A \to B))$, so MP gives $S \vdash (A \to B)$. (2) $B = A$. By Theorem 2.6, $S \vdash (A \to B)$. (3) B is an axiom. Again $S \vdash B$, and as above $S \vdash (A \to B)$. (4) B has been obtained by MP from C and $(C \to B)$, for which the claim already holds, i.e. $S \vdash (A \to C)$ and $S \vdash (A \to (C \to B))$. By (A3), $S \vdash ((A \to (C \to B)) \to ((A \to C) \to (A \to B)))$, so we can use MP to obtain $S \vdash ((A \to C) \to (A \to B))$ and again with MP $S \vdash (A \to B)$. □

Lemma 2.9 *If $S \vdash A$ and $S \subseteq S'$, then $S' \vdash A$*

Proof. Problem 7. □

Lemma 2.10 $\vdash (A \to ((A \to B) \to B))$.

Proof. By MP, $\{A, (A \to B)\} \vdash B$. By the Deduction Lemma, $\{A\} \vdash ((A \to B) \to B)$, and further for the same reason, $\vdash (A \to ((A \to B) \to B))$. □

2.2 Truth-tables

All propositional formulas are not provable, for example the mere p_0, or $\neg(p_0 \to p_0)$. Moreover, deduction is consistent in the sense that there is no A for which

$$\vdash A \text{ and } \vdash \neg A.$$

A handy method for showing that something is not provable is a *valuation*, first introduced by Russell and Whitehead in their monumental Principia Mathematica [20]. The idea of a truth value is due to Gottlob Frege [7], though the concept was anticipated by George Boole [2] and Charles Peirce [15].

Definition 2.11 (Valuation) *A* valuation *is any function $v : \mathbb{N} \to \{0, 1\}$. If A is a propositional formula, then the* truth value *of A in the valuation v, $v(A)$, is defined as follows:*

$$\begin{aligned} v(p_n) = &\quad v(n) \\ v(\neg A) = &\quad \begin{cases} 0, & \textit{if } v(A) = 1 \\ 1, & \textit{if } v(A) = 0 \end{cases} \\ v((A \to B)) = &\quad \begin{cases} 0, & \textit{if } v(A) = 1 \textit{ and } v(B) = 0 \\ 1, & \textit{otherwise} \end{cases} \\ (= &\quad v(A) \cdot v(B) + 1 - v(A)\ ) \end{aligned}$$

A propositional formula A is a *tautology* if $v(A) = 1$ for all v. If A is a tautology for all $A \in S$, we write $v(S) = 1$. If $S = \emptyset$, we agree that $v(S) = 1$ for all v.

Example 2.12 *The formula $(p_n \to p_n)$ is a tautology, for $v((p_n \to p_n)) = 0$ only if $v(p_n) = 1$ and $v(p_n) = 0$, which is impossible. The formula $(p_n \to \neg p_n)$ is not a tautology, for if $v(n) = 1$ we obtain $v((p_n \to \neg p_n)) = 0$. The formula $(\neg\neg A \to A)$ is always a tautology, for $v((\neg\neg A \to A)) = 0$ only if $v(\neg\neg A) = 1 - (1 - v(A)) = v(A) = 1$ and $v(A) = 0$.*

Theorem 2.13 *All provable propositional formulas are tautologies.*

This follows from the more general observation:

Theorem 2.14 *If $v(S) = 1$ and $S \vdash A$, then $v(A) = 1$.*

Proof. We use induction on the structure of proofs: (1) $A \in S$. Now $v(A) = 1$, because $v(S) = 1$. (2) A is an axiom. We consider each axiom separately. If $v((A \to (B \to A))) = 0$, then $v(A) = 1$ and $v((B \to A)) = 0$, i.e. $v(A) = v(B) = 1$ and $v(A) = 0$, which is impossible. Therefore (A1) is a tautology. The case of the axioms (A2) and (A3) will be left as exercises (See Problem 10). (3) A follows by the rule MP from B and $(B \to A)$, which are assumed to be provable from S. By the Induction Hypothesis, $v(B) = 1$ and $v((B \to A)) = 1$. From this $v(A) = 1$ follows. $\square$

Example 2.15 *The propositional formula p_n is not provable, for $v(p_n) = 0$ when $v(n) = 0$. The propositional formula $(p_0 \to \neg p_0)$ is not provable (cf. example 2.12). The propositional formula $A = (p_0 \to (p_0 \to p_1))$ is not provable, for if $v(0) = 1$ and $v(1) = 0$, then $v(A) = 0$.*

Convention. We use the following shorthands:

$$\begin{array}{rcll}
(A \vee B) & = & (\neg A \to B) & \text{(disjunction)} \\
(A \wedge B) & = & \neg(A \to \neg B) & \text{(conjunction)} \\
(A \leftrightarrow B) & = & \neg((A \to B) \to \neg(B \to A)) & \text{(equivalence)}
\end{array}$$

Example 2.16
$$\begin{array}{rcl}
v((A \vee B)) & = & v(A) + v(B) - v(A) \cdot v(B) \\
v((A \wedge B)) & = & v(A) \cdot v(B) \\
v((A \leftrightarrow B)) & = & v((A \to B)) \cdot v((B \to A))
\end{array}$$

Example 2.17 *The following propositional formulas are tautologies*

$$\begin{array}{c}
((A \vee B) \leftrightarrow (B \vee A)) \\
((A \wedge B) \leftrightarrow (B \wedge A)) \\
((A \leftrightarrow B) \leftrightarrow (B \leftrightarrow A)) \\
(\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)) \\
(\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B))) \\
(\neg(A \to B) \leftrightarrow (A \wedge \neg B))) \\
(\neg\neg A \leftrightarrow A) \\
\neg(A \wedge \neg A) \\
(A \vee \neg A)
\end{array}$$

A method called the *truth table technique* was introduced independently by E. Post (1897—1954) [16] and L. Wittgenstein (1889—1951) [21] for the study of tautologies. The rows of the truth table list all relevant truth value combinations. If we investigate propositional formulas built from A and B, it suffices to know the truth values of A and B:

A	B	$(A \to B)$
1	1	1
1	0	0
0	1	1
0	0	1

A	B	$(A \leftrightarrow B)$
1	1	1
1	0	0
0	1	0
0	0	1

A	$\neg A$
1	0
0	1

A	B	$(A \wedge B)$
1	1	1
1	0	0
0	1	0
0	0	0

A	B	$(A \vee B)$
1	1	1
1	0	1
0	1	1
0	0	0

Example 2.18 *The truth table of the propositional formula* $(((A \to B) \wedge (B \to$

$C)) \to (A \to C))$ is:

A	B	C	$(((A$	$\to$	$B)$	$\wedge$	$(B$	$\to$	$C))$	$\to$	$(A$	$\to$	$C))$
1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1	0	0	1	1	0	0
1	0	1	1	0	0	0	0	1	1	1	1	1	1
1	0	0	1	0	0	0	0	1	0	1	1	0	0
0	1	1	0	1	1	1	1	1	1	1	0	1	1
0	1	0	0	1	1	0	1	0	0	1	0	1	0
0	0	1	0	1	0	1	0	1	1	1	0	1	1
0	0	0	0	1	0	1	0	1	0	1	0	1	0

The formula has truth value 1 *in each row. This shows that the propositional formula is a tautology.*

There are propositional formulas the form of which reveals that they are tautologies, such as $((A \wedge B) \to (A \vee C))$. It does not matter what A, B and C are. On the other hand, $((A \wedge B) \to (A \wedge C))$ is a tautology for some C (e.g. if $C = B$), but not for all C (e.g. if $A = p_0$, $B = p_1$ and $C = p_2$).

Example 2.19

A	B	$((A$	$\to$	$B)$	$\wedge$	$\neg$	$A)$	$\to$	$\neg$	B
1	1	1	1	1	0	0	1	1	0	1
1	0	1	0	0	0	0	1	1	1	0
0	1	0	1	1	1	1	0	0	0	1
0	0	0	1	0	1	1	0	1	1	0

We can see that the propositional formula in question gets the truth value 0 *when* $v(A) = 0$ *and* $v(B) = 1$*. This is possible e.g. if* $A = p_0$ *and* $B = p_1$*: let* $v(0) = 0$ *and* $v(1) = 1$.

Definition 2.20 (Consistency) *A set S of propositional formulas is* incon-sistent*, if there is A such that $S \vdash A$ and $S \vdash \neg A$. Otherwise S* consistent*. S is* complete *if it is consistent and for all propositional formulas A we have $S \vdash A$ or $S \vdash \neg A$*

Note: If $v(S) = 1$, then S is consistent.

Theorem 2.21 *The following conditions are equivalent:*

(1) *S is inconsistent.*
(2) *$S \vdash B$ for all B.*

Proof. Suppose $S \vdash A$ and $S \vdash \neg A$. Let B be arbitrary. By Theorem 2.7,

$$S \vdash \neg A \to (A \to B).$$

By using MP twice we obtain $S \vdash B$. On the other hand, assume (2). Then $S \vdash A$ and $S \vdash \neg A$ for any A, whence S is inconsistent. □

Theorem 2.22 *the following conditions are equivalent:*

(1) $S \vdash A$
(2) $S \cup \{\neg A\}$ *is inconsistent.*

Proof. If $S \vdash A$, then $S \cup \{\neg A\} \vdash A$ and $S \cup \{\neg A\} \vdash \neg A$, whence (2) follows. Assume then (2). We argue as follows:

1.	$S \cup \{\neg A\} \vdash \neg(\neg A \to A)$	Theorem 2.21
2.	$S \vdash \neg A \to \neg(\neg A \to A)$	Deduction Lemma, 1
3.	$S \vdash (\neg A \to \neg(\neg A \to A)) \to ((\neg A \to A) \to A)$	(A2)
4.	$S \vdash (\neg A \to A) \to A$	MP 2,3
5.	$S \cup \{\neg A\} \vdash A$	Theorem 2.21
6.	$S \vdash \neg A \to A$	Deduction Lemma, 5
7.	$S \vdash A$	MP 4,6

□

Theorem 2.23 *Let S be complete. Then*

(1) $S \vdash \neg A \Longleftrightarrow S \nvdash A$
(2) $S \vdash (A \to B) \Longleftrightarrow (S \nvdash A$ *or* $S \vdash B)$

Proof. (1) If $S \vdash \neg A$, then $S \nvdash A$ by consistency. If, on the other hand, $S \nvdash A$, then $S \vdash \neg A$ by completeness. (2) Suppose for a start $S \vdash (A \to B)$. If $S \vdash A$, then $S \vdash B$. Hence $S \nvdash A$ or $S \vdash B$. Suppose, on the other hand, $S \nvdash A$. Then by (1), $S \vdash \neg A$. Theorem 2.7 gives $S \vdash (A \to B)$. Suppose finally $S \vdash B$. By Axiom (A1) we have $S \vdash (A \to B)$. □

Theorem 2.24 *If $S \vdash A$, then there is a finite $S_A \subseteq S$ such that $S_A \vdash A$*

Proof. We use induction. (1) $A \in S$. Choose $S_A = \{A\}$. (2) A is an axiom. We choose $S_A = \emptyset$. (3) A follows by MP from propositional formulas B and $B \to A$. As an Induction Hypothesis we assume that the sets $S_B \subseteq S$ and $S_{B \to A} \subseteq S$ have already been found such that

$$S_B \vdash B \text{ and } S_{B \to A} \vdash B \to A.$$

Let $S_A = S_B \cup S_{B \to A}$. By MP we have $S_A \vdash A$. □

Theorem 2.25 (Chain Lemma) *If $S_0 \subseteq S_1 \subseteq \ldots$ are consistent sets of propositional formulas, then $S = \bigcup_{n=0}^{\infty} S_n$ is consistent.*

Proof. Let $S \vdash A$ and $S \vdash \neg A$. Choose finite $S' \subseteq S$ such that $S' \vdash A$ and $S' \vdash \neg A$ (Theorem 2.24). Let $n \in \mathbb{N}$ such that $S' \subseteq S_n$. Now $S_n \vdash A$ and $S_n \vdash \neg A$, contrary to our assumption. □

Theorem 2.26 (Lindenbaum's[3] Lemma) *If S is a consistent set of propositional formulas, then there is a complete $S' \supseteq S$.*

Proof. Let $A_0, A_1, \ldots$ be the sequence of all propositional formulas. Let $S_0 = S$. If S_n is defined, let S_{n+1} be obtained as follows:

Case 1 $S_n \vdash A_n$. Let $S_{n+1} = S_n \cup \{A_n\}$. If S_{n+1} is inconsistent, then $S_{n+1} \vdash \neg A_n$ by Theorem 2.24. By the Deduction Lemma, $S_n \vdash A_n \to \neg A_n$ and finally by MP, $S_n \vdash \neg A_n$, contrary to the assumption that S_n is known to be consistent. Therefore S_{n+1} is consistent.

Case 2 $S_n \nvdash A_n$. Let $S_{n+1} = S_n \cup \{\neg A_n\}$. If S_{n+1} is inconsistent then $S_n \vdash A_n$ by Theorem 2.22, contrary to our assumption. Therefore S_{n+1} is consistent.

Let $S' = \bigcup_{n=0}^{\infty} S_n$. By the Chain Lemma,a S' is consistent. Clearly S' is complete. $\square$

Theorem 2.27 *If S is a consistent set of propositional formulas, then there exists a valuation v such that $v(S) = 1$.*

Proof. By Lindenbaum's Lemma there is a complete $S' \supseteq S$. Let

$$v(n) = \begin{cases} 1 \text{ if } S' \vdash p_n \\ 0 \text{ if } S' \vdash \neg p_n. \end{cases}$$

We show that $v(A) = 1$ if and only if $S' \vdash A$. To show this, we use induction on A. (1) $A = p_n$. This follows from the definition of v. (2) $A = \neg B$. $v(\neg B) = 1$ if and only if $v(B) \neq 1$ if and only if $S' \nvdash B$ (by the Induction Hyp.) if and only if $S' \vdash \neg B$ (by Theorem 2.23). (3) $A = (B \to C)$. $v((B \to C)) = 1$ if and only if $v(B) \neq 1$ or $v(C) = 1$ if and only if $S' \nvdash B$ or $S' \vdash C$ (by the Induction Hyp.) if and only if $S' \vdash (B \to C)$ (by Theorem 2.23). The claim has been proved. Since $S \subseteq S'$, we obtain $v(S) = 1$. $\square$

The following important property of propositional logic was first proved[4] by Emil Post[5] in 1921. It shows that our axioms together with MP are sufficient. Any potential new axiom would be provable from the old ones.

Corollary 2.28 (Completeness Theorem) (1) *A is provable if and only if A is a tautology.*

(2) *$S \vdash A$ if and only if $v(A) = 1$ for all valuations for which $v(S) = 1$.*

Proof. (1) follows from (2) by the choice $S = \emptyset$. Thus we demonstrate only (2). If $S \vdash A$, then $v(A) = 1$ whenever $v(S) = 1$ by Theorem 2.14. If on the other hand $S \nvdash A$, then $S \cup \{\neg A\}$ is consistent by Theorem 2.22. By Theorem 2.27 there is v such that $v(S) = 1$ and $v(A) = 0$. $\square$

[3] Adolf Lindenbaum 1904—1941.

[4] It occurred in unpublished lectures of David Hilbert in Göttingen already in 1917, see [22].

[5] [16]

2.3 Problems

1. Which of the following are axioms of propositional logic (here A,B and C are arbitrary propositional formulas):
   (a) $(p_0 \to (p_1 \to p_2))$.
   (b) $((A \to B) \to (A \to (A \to B)))$.
   (c) $(p_0 \to (B \to C))$.
   (d) $((A \to B) \to A)$.
2. Give the deduction $\{A, (A \to C), (A \to (\neg B \to \neg C))\} \vdash B$.
3. Give the deduction $\{(C \to (B \to A)), (\neg B \to \neg C)\} \vdash (C \to A)$.
4. Show that $\vdash (A \to (A \vee B))$. You can use Theorems 2.6, 2.7, 2.8, 2.21 and 2.22, but not Corollary 2.28.
5. Give the deductions $\vdash (\neg\neg A \to A)$ and $\vdash (A \to \neg\neg A)$. You may use Theorems 2.6, 2.7, 2.8, 2.21 and 2.22.
6. Give the deduction $\vdash (A \to \neg\neg A)$. You may use Theorems 2.6, 2.7 and 2.8, but not Corollary 2.28. Investigating the proof of Theorem 2.22 may be helpful.
7. Show that if $S \vdash A$ and $S \subseteq S'$, then $S' \vdash A$ without using Corollary 2.28.
8. Show that the following are equivalent:
   (a) $S \vdash A$,
   (b) There is a finite sequence $(A_i)_{i \leq n}$ of propositional formulas such that
      i. $A_n = A$,
      ii. For each $i \leq n$, A_i is either an element of S, an axiom or obtained by MP from the formulas A_j, $j < i$.
9. Suppose A is a propositional formula and v and v' are valuations such that $v(n) = v'(n)$ whenever p_n occurs in A. Show that $v(A) = v'(A)$.
10. Prove that Axioms (A2) and (A3) are valid.
11. Show that $\{(p_0 \vee p_1)\} \nvdash (p_0 \to p_1)$.
12. Show that the propositional formula $(((p_0 \vee p_2) \wedge (p_1 \vee p_2)) \to ((p_0 \vee p_1) \wedge p_2))$ is not provable.
13. Show that the set $\{(p_{2n} \vee \neg p_{2n+1}) : n \in \mathbb{N}\}$ of propositional formulas is not complete.
14. Show that the set $\{(p_{2n} \wedge \neg p_{2n+1} : n \in \mathbb{N}\}$ is complete. You may use Corollary 2.28.

15. Give a set $S \neq \emptyset$ which has, for each $n \in \mathbb{N}$, a complete extension S_n, and moreover $S_n \neq S_m$ whenever $n \neq m$.

16. Show that if $\{(A \to B)\} \vdash (B \to A)$, then $\vdash (B \to A)$. You may use Corollary 2.28.

17. If A and B are finite words, then $l(A)$ stands for the number of left parentheses in A, $r(A)$ stands for the number of right parentheses in A, and AB stands for the word obtained by concatenating (i.e. writing first A and the immediately continuing with B). Prove that if A and B are words and AB is a propositional formula, then $l(B) \leq r(B)$.

Chapter 3

Structures

The concept of a structure is a basic one in mathematics. It emerged first in algebra in the form of groups, rings and fields in the nineteenth century and then expanded throughout mathematics in the early twentieth century. In logic the systematic study of structures started with the work of Alfred Tarski (1901-1983) in the 1930s but it existed in one form or another already in the works of Leopold Löwenheim, Thoralf Skolem and Kurt Gödel in the previous decade. The modern concept of a structure is based on (elementary) set theory.

3.1 Relations

A *binary relation* is any set of ordered pairs. If R is a binary relation, then the *domain* of R is the set $\mathrm{dom}(R) = \{x|$ there is y such that $\langle x, y\rangle \in R\}$. Respectively, the *range* of R is the set $\mathrm{ran}(R) = \{y|$ there is x such that $\langle x, y\rangle \in R\}$. Thus $R \subseteq \mathrm{dom}(R) \times \mathrm{ran}(R)$. An n-place relation is any set of ordered n-sequences.

A relation is

- *reflexive in* A if $\langle x, x\rangle \in R$ when $x \in A$
- *irreflexive in* A if $\langle x, x\rangle \notin R$ when $x \in A$
- *symmetric* if $\langle x, y\rangle \in R$ implies $\langle y, x\rangle \in R$
- *asymmetric* if $\langle x, y\rangle \in R$ implies $\langle y, x\rangle \notin R$
- *transitive* if $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$ imply $\langle x, z\rangle \in R$
- *intransitive* if $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$ imply $\langle x, z\rangle \notin R$
- *tricotomic in* A if for all $x, y \in A$ exactly one of the following holds $\langle x, y\rangle \in R$, $x = y$, $\langle y, x\rangle \in R$
- an *equivalence relation in* A if R is reflexive in A and symmetric and transitive.

- *a total order in* A if R is transitive and tricotomic in A.

If R is an equivalence relation in A, then we define for all $x \in A$

$$\begin{array}{rcl} [x] & = & \{y \in A | \langle x, y\rangle \in R\} \\ A/R & = & \{[x] | x \in A\}. \end{array}$$

A relation R is a *function* if for all $x \in \mathrm{dom}(R)$ there is exactly one y such that $\langle x, y\rangle \in R$. We then write $f(x) = y$. We write $f : A \to B$ if f is a function, $\mathrm{dom}(f) = A$ and $\mathrm{ran}(f) \subseteq B$. If in addition $\mathrm{ran}(f) = B$, then f is a *surjection*. If f is a function and for all $y \in \mathrm{ran}(f)$ there is exactly one x such that $\langle x, y\rangle \in f$, then f is an *injection*. $f : A \to B$ is a *bijection* if f is an injection and a surjection.

3.2 Structures

Structures a.k.a. *models*, our topic in this section, consist of a *domain* as well as relations and functions on the domain. The concept of a structure is very general covering e.g. all algebraic structures (groups, fields, etc) and also databases. It is perhaps surprising that one can say anything interesting about such a general concept. *Predicate logic*, to be defined in the next chapter, is ideal for expressing properties of structures while it itself has deep mathematical properties.

Definition 3.1 (Structure) *A* structure *is any set* $M \neq \emptyset$*, called the* domain*, or* universe*, of the structure, equipped with a finite*[1] *sequence of relations* $P_1, \ldots, P_n$*, functions* $f_1, \ldots, f_m$ *and constants* $c_1, \ldots, c_k$*. It is denoted*

$$\mathcal{M} = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k).$$

Example 3.2 (Algebraic structures) *The* group of integers *is the structure* $\mathbf{Z} = (\mathbb{Z}, +, 0)$*, where* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *is a function and 0 is a constant. Other algebraic examples of structures are* $\mathbf{Q} = (\mathbb{Q}, +, \cdot, 0, 1)$ *i.e. the field of rational numbers and* $\mathbf{R} = (\mathbb{R}, +, \cdot, 0, 1)$*, the field of real numbers.*

Example 3.3 (Unordered lists) *An unordered*[2] *binary list* 100110001 *can be thought of as an* unordered binary structure $(\{0, 1, \ldots, 8\}, \{0, 3, 4, 8\})$*, the universe of which is* $\{0, 1, \ldots, 8\}$*, with a* 1*—place (unary) relation (i.e. subset) {0,3,4,8}. The domain is set of bits and the subset tells which bits are ones. The given binary sequence can be, for example, a teacher's book-keeping about how many have passed a certain course. If book-keeping is maintained for several courses, several unary relations are needed. We then have an unordered binary table as, e.g., in Figure 3.1, which can also be represented pictorially as in Figure 3.2:*

[1] Sometimes we allow an infinite sequence of relations, functions and constants, but normally a finite number suffices.

[2] The list being unordered means that it can be written also as 111100000 or 010101010.

Student	Course 1	Course 2	Course 3
0	1	0	0
1	0	0	1
2	0	1	1
3	1	0	1
4	1	1	1
5	0	1	0
6	0	0	0
7	0	0	0
8	1	0	0

Figure 3.1:

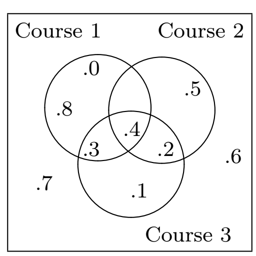


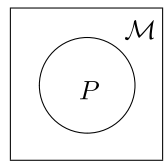
Figure 3.2:

The general form of a structure of this form is

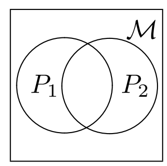
$$\mathcal{M} = (M, P_1, P_2, P_3),$$

where $P_1 \subseteq M, P_2 \subseteq M, P_3 \subseteq M$. Such a structure is called *monadic* (sometimes also *unary*). 1–place relations P_i can be one, two, three or more—however many, as long as they all are 1–place:

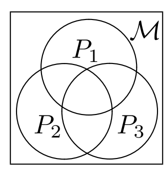
(M, P)



(M, P_1, P_2)



(M, P_1, P_2, P_3)



Example 3.4 (Total orders) *A structure* $(M, \lhd)$*, which consists of a universe* M *and a total order* $\lhd$ *on* M*, is called an* ordered set*. For example* $(\mathbb{N}, \lhd)$*, where* $\lhd = \{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} | n < m\}$*, and* $(\mathbb{Q}, \lhd)$*, where* $\lhd = \{\langle n, m\rangle \in \mathbb{Q} \times \mathbb{Q} | n < m\}$*, and* $(\{0, 1, 2\}, \lhd)$*, where* $\lhd = \{\langle 0, 2\rangle, \langle 2, 1\rangle, \langle 0, 1\rangle\}$.

Example 3.5 (Databases) *Consider the minuscule database*

name	*course*	*grade*
olga	ST	A
henry	MT	C
anna	MT	B
olga	RT	A

This can be construed as the structure (M, R)*, where* M *is the set*

$$\{\text{olga}, \text{henry}, \text{anna}, \text{ST}, \text{MT}, \text{RT}, A, B, C\}$$

and R *is the 3-place relation consisting of the triples* $\langle \text{olga}, \text{ST}, A\rangle$, $\langle \text{henry}, \text{MT}, A\rangle$, $\langle \text{anna}, \text{MT}, A\rangle$*, and* $\langle \text{olga}, \text{RT}, A\rangle$.

3.3 Vocabulary

In order to prove things about structures we have to agree upon a universal notation for structures. To this end we introduce the concept of a vocabulary.

Definition 3.6 (Vocabulary) *A* vocabulary *is set L of relation, function, and constant symbols. Relation and function symbols are associated with a so-called* arity-function $\#_L$ *which maps symbols to natural numbers.*

It does not matter what symbols we use for the elements of a vocabulary. Usually relation symbols are denoted R, function symbols f, and constant symbols c. A relation symbol $\mathrm{R} \in L$ is said to be a $\#_L(\mathrm{R})$–place or a $\#_L(\mathrm{R})$-ary relation symbol. A function symbol $\mathrm{f} \in L$ is said to be $\#_L(\mathrm{f})$–place or $\#_L(\mathrm{f})$–ary.

Definition 3.7 (L-structure) *If L is a vocabulary, then an L–structure is a pair*

$$\mathcal{M} = \langle M, \mathrm{Sat}_{\mathcal{M}} \rangle$$

where $\mathcal{M}$ is a non-empty set, and $\mathrm{Sat}_{\mathcal{M}}$ *is a function such that*

(1) $\mathrm{dom}(\mathrm{Sat}_{\mathcal{M}}) = L$
(2) $\mathrm{R} \in L \Longrightarrow \mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) \subseteq M^{\#_L(\mathrm{R})}$
(3) $\mathrm{f} \in L \Longrightarrow \mathrm{Sat}_{\mathcal{M}}(\mathrm{f}) : M^{\#_L(\mathrm{f})} \to M$
(2) $\mathrm{c} \in L \Longrightarrow \mathrm{Sat}_{\mathcal{M}}(\mathrm{c}) \in M$

Consider, for example, the structure

$$\mathcal{M} = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k).$$

An appropriate vocabulary for this structure is

$$L = \{\mathrm{R}_1, \ldots, \mathrm{R}_n, \mathrm{f}_1, \ldots, \mathrm{f}_m, \mathrm{c}_1, \ldots, \mathrm{c}_k\},$$

where $\#_L(\mathrm{R}_i)$ and $\#_L(\mathrm{f}_i)$ obey the arities in $\mathcal{M}$. Now $\mathcal{M}$ is the following L–structure $\mathcal{M} = \langle M, \mathrm{Sat}_{\mathcal{M}} \rangle$, where $\mathrm{Sat}_{\mathcal{M}}(\mathrm{R}_i) = P_i$, $\mathrm{Sat}_{\mathcal{M}}(\mathrm{f}_i) = f_i$, and $\mathrm{Sat}_{\mathcal{M}}(\mathrm{c}_i) = c_i$

Definition 3.8 (Reduct) *The* reduct *of an L–structure $\mathcal{M}$ to the vocabulary $L' \subseteq L$ is the L'–structure*

$$\mathcal{M} \restriction L' = \langle M, \mathrm{Sat}_{\mathcal{M}} \restriction L' \rangle.$$

Then $\mathcal{M}$ is an expansion *of $\mathcal{M}' \restriction L'$ to the vocabulary L.*

For example, (M, R_1), (M, R_2), (M, f), (M, R_1, f), (M, R_2, f),(M, R_1, R_2) and (M) are reducts of (M, R_1, R_2, f). Note that the last reduct is the reduct to the empty vocabulary.

3.4 Isomorphism

Definition 3.9 (Isomorphism) *L–structures*

$$\mathcal{M} = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k)$$

and

$$\mathcal{M}' = (M', P_1', \ldots, P_n', f_1', \ldots, f_m', c_1', \ldots, c_k')$$

are isomorphic, *if there is a bijection $\pi : M \to M'$ such that*

(1) $\langle a_1, \ldots, a_l \rangle \in P_i \iff \langle \pi(a_1), \ldots, \pi(a_l) \rangle \in P_i'$, *when* $1 \le i \le n$

(2) $f_i'(\pi(a_1), \ldots, \pi(a_l)) = \pi(f_i(a_1, \ldots, a_l))$, *when* $1 \le i \le m$

(3) $\pi(c_i) = c_i'$, *when* $1 \le i \le k$.

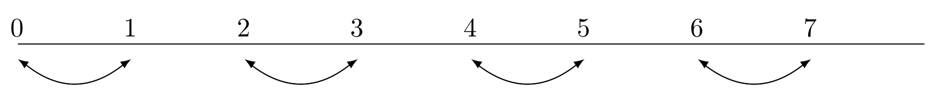
We then say that π is an isomorphism $\mathcal{M} \to \mathcal{M}'$, *in symbols $\pi : \mathcal{M} \cong \mathcal{M}'$. If additionally $\mathcal{M} = \mathcal{M}'$, then we say that π is an* automorphism *of the structure $\mathcal{M}$.*

The definition of an isomorphism may seem complicated but it simplifies in special cases, in particular when there are only few (or no) relations, functions and constants.

Example 3.10 *Consider the unary structures $\mathcal{M} = (\mathbb{N}, \{1, 3, 5, 7, \ldots\})$ and $\mathcal{M}' = (\mathbb{N}, \{0, 2, 4, 6, \ldots\})$. We show that the function $\pi : \mathbb{N} \to \mathbb{N}$,*

$$\pi(n) = \begin{cases} 2k+1 & \text{if } n = 2k \\ 2k & \text{if } n = 2k+1 \end{cases}$$

is an isomorphism $\mathcal{M} \to \mathcal{M}'$.



π is clearly a bijection $\mathbb{N} \to \mathbb{N}$. On the other hand, n is odd if and only if $\pi(n)$ is even. Thus π is an isomorphism. More generally, if

$$\begin{aligned} \mathcal{M} &= (M, P), \quad P \subseteq M \\ \mathcal{M}' &= (M', P'), \quad P' \subseteq M' \end{aligned}$$

then the bijection $\pi : M \to M'$ is an isomorphism, if and only if $a \in P \iff \pi(a) \in P'$, i.e. π has to map P onto P' and $M \setminus P$ onto $M' \setminus P'$. If M and M' are finite, then $\mathcal{M} \cong \mathcal{M}'$ if and only if P and P' have the same number of elements.

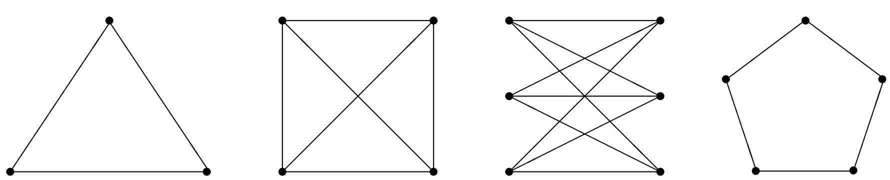
Example 3.11 *Unordered binary sequences are isomorphic if they have the same number of ones and zeros. Respectively, two binary tables (see Example 3.3) are isomorphic as binary structures if they have the same number of* *rows of each possible combination of ones and zeros:*

St.	*C1*	*C2*	*C3*	*St.*	*C1*	*C2*	*C3*
0	*1*	*0*	*0*	*0*	*0*	*0*	*1*
1	*0*	*0*	*1*	*1*	*1*	*0*	*0*
2	*0*	*1*	*1*	*2*	*0*	*1*	*1*
3	*1*	*0*	*1*	*3*	*1*	*1*	*1*
4	*1*	*1*	*1*	*4*	*0*	*1*	*0*
5	*0*	*1*	*0*	*5*	*1*	*0*	*1*
6	*0*	*0*	*0*	*6*	*0*	*0*	*0*
7	*0*	*0*	*0*	*7*	*1*	*0*	*0*
8	*1*	*0*	*0*	*8*	*0*	*0*	*0*

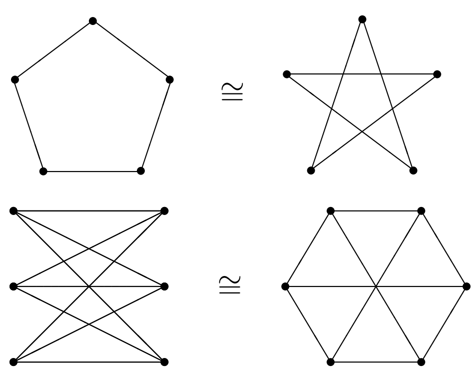
Two different but isomorphic copies of structures of this type can arise for example if the teacher accidentally forgets the order of the rows and has to renumber the rows.

Example 3.12 *The ordered sets* $\mathcal{M} = ((-\frac{\pi}{2}, \frac{\pi}{2}), <)$ *and* $\mathcal{M}' = (\mathbb{R}, <)$ *are isomorphic, as the mapping* $x \mapsto \tan(x)$ *reveals. On the other hand,* $([-\frac{\pi}{2}, \frac{\pi}{2}], <) \not\cong (\mathbb{R}, <)$*, as is easily observed by pondering where would an isomorphism map the boundary points* $-\frac{\pi}{2}$ *and* $\frac{\pi}{2}$*.*

Example 3.13 *A structure* (M, R) *is a* graph *if* $R \subseteq M^2$ *is symmetric and irreflexive. Examples of graphs:*

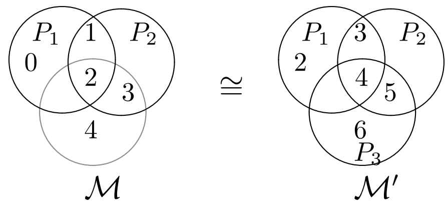


K_3 K_4 $K_{3,3}$ *pentagon*



Example 3.14 *The monadic structure* $\mathcal{M} = (\mathbb{N}, \{0,1,2\}, \{1,2,3\}), L = \{\mathrm{P}_1, \mathrm{P}_2\}$ *has an expansion which is isomorphic to*

$$\mathcal{M}' = (\mathbb{N}, \{2,3,4\}, \{3,4,5\}, \{4,5,6\}), L = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_3\}.$$



We add to the structure $\mathcal{M}$ the relation $\{2,3,4\}$. After this the mapping

$$\pi(n) = \begin{cases} n+2 & \text{if } n \leq 4 \\ 0 & \text{if } n = 5 \\ 1 & \text{if } n = 6 \\ n & \text{if } n > 6 \end{cases}$$

is an isomorphism between an expansion of $\mathcal{M}$ and $\mathcal{M}'$.

Example 3.15 *Let $L = \{\mathrm{P}, \mathrm{S}, \mathrm{L}\}$ (P="point", S="line", L="intersects"). This vocabulary is suitable for an investigation of geometry. Cartesian plane geometry is constituted by the L–structure $\mathcal{M} = (P \cup S, P, S, L)$, where*

$$\begin{array}{rcl} P & = & \text{points of the plane } \mathbb{R}^2 \\ S & = & \text{lines of the plane } \mathbb{R}^2 \\ L & = & \{\langle p, s\rangle \subseteq P \times S |\ \text{point } p \text{ is on line } s\}. \end{array}$$

So-called non-Euclidean geometries are very much like $\mathcal{M}$, but not isomorphic to it. A geometry not isomorphic to $\mathcal{M}$ is obtained also if we start with $\mathbb{R}^n$, $n > 2$, rather than $\mathbb{R}^2$.

Example 3.16 *Let $L = \{\mathrm{P}, \mathrm{J}, \varepsilon.\}$ If A is set, we obtain an L–structure*

$$\begin{array}{rcl} \mathcal{M} & = & (A \cup \mathcal{P}(A), A, J, \varepsilon) \\ P & = & A \\ J & = & \mathcal{P}(A) \\ \varepsilon & = & \{\langle x, y\rangle | x \in P, y \in J, x \in y\}. \end{array}$$

3.5 Problems

1. Let $L = \{\mathrm{P}\}$, where $\#_L(\mathrm{P}) = 1$. Give nine pairwise non-isomorphic L-structures with a domain consisting of exactly eight elements.
2. Prove that if $\mathcal{M} \cong \mathcal{M}'$ and $\mathcal{M}' \cong \mathcal{M}''$, then $\mathcal{M} \cong \mathcal{M}''$.
3. Are the structures $(\mathbb{R}, <)$ and $(\mathbb{R} \setminus \{0\}, <)$ isomorphic?
4. Let L be a vocabulary, $\mathcal{M}$ an L-structure, $L' \subseteq L$ and $\mathcal{M}'$ an L'-structure such that $\mathcal{M}\restriction L' \cong \mathcal{M}'$. Show that $\mathcal{M}'$ has an expansion $\mathcal{M}''$ such that $\mathcal{M} \cong \mathcal{M}''$.
5. Not so easy: Give a bijection $f : \mathbb{R} \to [0, 1)$.

Chapter 4

Predicate logic

Predicate logic is a mathematical tool for the study of structures. It turns out that properties of structures that are expressible in predicate logic have important common characteristics that turn out to be useful. One can think of predicate logic as a programming language for asking questions about structures.

As with programming languages, the definition of predicate logic is somewhat long and consists of many parts. The core of *predicate logic* consists of so-called *logical symbols*:

The *logical symbols* of predicate logic are:

variable symbols	$v_0, v_1, \ldots$
connectives	$\neg, \rightarrow$
a quantifier	$\forall$
parentheses	$($, $)$

If L is a vocabulary, then the set of *L-terms* is defined by the following inductive definition:

(1) Variable symbols v_n are L-terms.

(2) Constant symbols $\mathrm{c} \in L$ are L-terms.

(3) If $\mathrm{f} \in L, \#_L(\mathrm{f}) = n$ and $t_1, \ldots, t_n$ are L-terms, then $\mathrm{f}t_1 \ldots t_n$ is an L-term.

If a vocabulary L does not contain function symbols, then the only L-terms there are are the variable symbols and possible constant symbols. Condition (3), on the other hand, brings about the most complex L-terms.

Example 4.1 *Consider the vocabulary $L = \{+, 0\}$ of the structure (a group[1])*

$$\mathbf{Z} = (\mathbf{Z}, +, 0).$$

[1] A *group* is a structure $(G, +, 0)$, where the binary function $+$ and the constant 0 satisfy certain simple axioms, called the *group axioms*, reflecting the addition of integer (or rational, or real, or complex) numbers.

(The symbols + and 0 are here used in two different roles: as a function symbol and a constant symbol, and on the other hand as a function and a constant) Examples of L-terms are:

0
$v_0, v_1, v_2, \ldots$
$+t_0t_1$ *(e.g.* $+00, +v_0v_1$*)*
$++t_0t_1t_2$
$+++t_0t_1t_2t_3$

Essentially the L-terms are sums of variables and zeros.

Example 4.2 *Let us consider the vocabulary* $L = \{+, \cdot, 0, 1\}$ *of the structure (field[2])* $\mathbf{R} = (\mathbf{R}, +, \cdot, 0, 1)$*. Examples of L-terms are:*

0
1
$v_0, v_1, v_2, \ldots$
$+t_0t_1,\ \cdot t_0t_1$
$++t_0t_1\cdot t_2t_3,\ \cdot + t_0t_1 + t_2t_3$
$\cdot\cdot t_0t_1\cdot t_2t_3$

Essentially these are polynomials. We can say that terms are generalized polynomials.

Definition 4.3 (Assignment, value) *Let* $\mathcal{M}$ *be an L-structure. An* assignment *for* $\mathcal{M}$ *is any function* $s : \mathbb{N} \to M$*. The* value *of an L-term t in* $\mathcal{M}$ *under the assignment s,* $t^{\mathcal{M}}\langle s\rangle$*, is defined as follows:*

Case 1: $t = v_i$, $\quad t^{\mathcal{M}}\langle s\rangle = s(i)$
Case 2: $t = \mathrm{c}$, $\quad t^{\mathcal{M}}\langle s\rangle = \mathrm{Sat}_{\mathcal{M}}(\mathrm{c})$
Case 3: $t = \mathrm{f}_i t_1 \ldots t_n$, $\quad t^{\mathcal{M}}\langle s\rangle = \mathrm{Sat}_{\mathcal{M}}(\mathrm{f}_i)(t_1^{\mathcal{M}}\langle s\rangle, \ldots, t_n^{\mathcal{M}}\langle s\rangle)$.

Computing the value of a term is like computing the value of a polynomial when the values of the variables are given. Let $\mathcal{Z} = (\mathbf{Z}, +, 0)$ and $\mathcal{R} = (\mathbf{R}, +, \cdot, 0, 1)$. Then

$$\begin{aligned}
(++v_0v_1v_2)^{\mathcal{Z}}\langle s\rangle &= (+v_0v_1)^{\mathcal{Z}}\langle s\rangle + v_2^{\mathbf{Z}}\langle s\rangle \\
&= v_0^{\mathcal{Z}}\langle s\rangle + v_1^{\mathcal{Z}}\langle s\rangle + v_2^{\mathcal{Z}}\langle s\rangle \\
&= s(0) + s(1) + s(2) \\
(\cdot+v_0v_1v_2)^{\mathcal{R}}\langle s\rangle &= (+v_0v_1)^{\mathcal{R}}\langle s\rangle \cdot v_2^{\mathcal{R}}\langle s\rangle \\
&= (v_0^{\mathcal{R}}\langle s\rangle + v_1^{\mathcal{R}}\langle s\rangle) \cdot v_2^{\mathcal{R}}\langle s\rangle \\
&= (s(0) + s(1)) \cdot s(2)
\end{aligned}$$

[2] A *field* is a structure $(F, +, \cdot, 0, 1)$, where the binary functions $+$ and $\cdot$, together with the constants 0 and 1, satisfy certain simple axioms, called the *field axioms*, reflecting the addition and multiplication of rational (or real, or complex) numbers.

Lemma 4.4 *Let $\mathcal{M}$ and $\mathcal{M}'$ be L-structures and $\pi : M \cong M'$. Let $s : \mathbb{N} \to M$ and $s' : \mathbb{N} \to M'$ such that $s'(n) = \pi(s(n))$ for all $n \in \mathbb{N}$. Then $t^{\mathcal{M}'}\langle s'\rangle = \pi(t^{\mathcal{M}}\langle s\rangle)$ for all L-terms t.*

Proof. Problem 7. □

One of the most useful concepts in mathematics is the concept of an *equation*. Ever new methods are being developed for finding solutions of equations. The concept of an equation is important also in logic. In logic equations represent the simplest dependence between variables and constants. That is why equations are called *atomic formulas* in logic.

Definition 4.5 (Equation) *If L is vocabulary and t_1 and t_2 are L-terms, then*

$$\approx t_1 t_2$$

*is an L-**equation**[3].*

Examples of L-equations are:

$$\begin{array}{ll} \approx v_0 v_1 & \\ \approx +v_0 c v_0 & \#_L(+) = 2 \\ \approx \cdot v_0 v_1 + v_2 v_3 & \#_L(+) = \#_L(\cdot) = 2 \\ \approx \mathrm{fff} v_0 v_1 & \#_L(\mathrm{f}) = 1. \end{array}$$

The L-equation $\approx t_1 t_2$ is parsed such that one looks for the shortest term t_1 that follows the $\approx$-sign, and the rest constitutes the term t_2. Thus $\approx v_0 v_1 v_2$ is not an L-equation and $\approx \mathrm{ff} v_0 v_1 v_2 v_3$ is an L-equation only if $\#_L(\mathrm{f}) = 2$.

A typical problem in mathematics is to find the set of solutions of a given equation. Respectively we can define for any L-equation the set of assignments that "satisfy" it.

Definition 4.6 (Equation satisfaction) *Let L be a vocabulary, $\mathcal{M}$ an L-structure and $\approx t_1 t_2$ an L-equation. We define*

$$\mathrm{Sat}_{\mathcal{M}}(\approx t_1 t_2) = \{s | t_1^{\mathcal{M}}\langle s\rangle = t_2^{\mathcal{M}}\langle s\rangle\}.$$

This set consists of all assignments s that give the same value to t_1 and t_2, as in algebra the set of solutions of the equation $x^2 + 2x + 1 = y^3$ consists of all pairs $\langle a, b\rangle$ that give the same value to $a^2 + 2a + 1$ and b^3.

Examples:

$$\begin{array}{l} \mathrm{Sat}_{\mathcal{M}}(\approx v_0 v_1) = \{s | s(0) = s(1)\} \\ \mathrm{Sat}_{\mathcal{M}}(\approx v_0 \mathrm{c}) = \{s | s(0) = \mathrm{Sat}(\mathrm{c})\} \\ \mathrm{Sat}_{\mathbf{Z}}(\approx +v_0 v_1 v_2) = \{s | s(0) + s(1) = s(2)\} \\ \mathrm{Sat}_{\mathbf{R}}(\approx \cdot v_0 v_0 v_2) = \{s | s(0)^2 = s(1)\}. \end{array}$$

[3] This is often written $t_1 \approx t_2$. The reason to use the so-called *Polish notation* $\approx t_1 t_2$ is that it allows suppression of parentheses.

If $P(x)$ is a polynomial in x, it is easy to write down a term t, where x is denoted by v_0, such that $\mathrm{Sat}_{\mathbf{R}}(\approx tv_1) = \{s|P(s(0)) = s(1)\}$.

If we denote ${}^{\mathbb{N}}M = \{s|s : \mathbb{N} \to M\}$ then $\mathrm{Sat}_{\mathcal{M}}(\approx t_1t_2) \subseteq {}^{\mathbb{N}}M$. The bigger the set $\mathrm{Sat}_{\mathcal{M}}(\approx t_1t_2)$, the more solutions the equation $\approx t_1t_2$ has. A quite common extreme is the case $\mathrm{Sat}_{\mathcal{M}}(\approx t_1t_2) = {}^{\mathbb{N}}M$, i.e. the equation is satisfied by all values of the variables. Then the equation expresses a kind of universal law, such as $x+1 = 1+x$ in the group of integers and $(x+y)^2 = x^2+2xy+y^2$ in the field of real numbers. Another extreme is $\mathrm{Sat}_{\mathcal{M}}(\approx t_1t_2) = \emptyset$, i.e. the equation has no solution, as $x+x = 1$ in the group of integers or $x^2 = 2$ in the field of rational numbers.

We now move from equations to arbitrary formulas. Formulas can express more complicated situations than mere equations. We can use formulas to express conjunctions of equations, a.k.a. systems of equations, as well as inequations and inequalities.

Definition 4.7 (Formula) *Let L be a vocabulary. The set of* L-formulas *is defined as follows:*

1. *If t_1 and t_2 are L-terms, then $\approx t_1t_2$ is an L-formula.*
2. *If $\mathrm{R} \in L$, $\#_L(\mathrm{R}) = n$ and $t_1, \ldots, t_n$ are L-terms, then $\mathrm{R}t_1 \ldots t_n$ is an L-formula.*
3. *If φ and ψ are L-formulas and $n \in \mathbb{N}$ then $\neg\varphi, (\varphi \to \psi)$ and $\forall v_n\varphi$ are L-formulas.*

The formulas of the cases 1 and 2 are called *atomic formulas.*

Convention: We use the following shorthands:

$$
\begin{array}{rcll}
(\varphi \vee \psi) & = & (\neg\varphi \to \psi) & (\textit{disjunction}) \\
(\varphi \wedge \psi) & = & \neg(\varphi \to \neg\psi) & (\textit{conjunction}) \\
(\varphi \leftrightarrow \psi) & = & \neg((\varphi \to \psi) \to \neg(\psi \to \varphi)) & (\textit{equivalence}) \\
\exists v_n\varphi & = & \neg\forall v_n\neg\varphi & (\textit{existential quantifier}).
\end{array}
$$

The concept of a *solution set* $\mathrm{Sat}_{\mathcal{M}}(\approx t_1t_2)$ for equations generalizes to all formulas: we can associate to any L-formula φ in a canonical way a solution set $\mathrm{Sat}_{\mathcal{M}}(\varphi)$. To define this set we introduce the following notation: If $s : \mathbb{N} \to M, n \in \mathbb{N}$ and $a \in M$, then the assignment

$$s(a/n) \in {}^{\mathbb{N}}M$$

is defined as follows:

$$s(a/n)(i) = \begin{cases} a & \text{if } i = n \\ s(i) & \text{if } i \neq n. \end{cases}$$

Thus the assignment $s(a/m)$ is exactly the same assignment as s except that the value of $s(m)$ has been changed in $s(a/m)$ to the value a. This means that $s(a/m)(m) = a$ and for other i we have $s(a/m)(i) = s(i)$.

If $\mathcal{X} \subseteq {}^{\mathbb{N}}M$, Let

$$A_n(\mathcal{X}) = \{s | s(a/n) \in \mathcal{X} \text{ for all } a \in M\}.$$

Thus

$$s \in A_n(\mathcal{X}) \leftrightarrow \text{ for all } a \in M : s(a/n) \in \mathcal{X}.$$

This operation is used to define the solution set for quantified formulas.

The following definition, essentially due to Alfred Tarski, is perhaps the most important definition in this book. It establishes necessary and sufficient conditions for an assignment to "satisfy" a formula in a structure. Here "satisfaction" means that what the formula intuitively seems to say is actually the case. This is why the below definition is sometimes called the *Correspondence Theory of Truth*.

Definition 4.8 (Tarski's truth-definition) *If L is a vocabulary, φ is an L-formula and $\mathcal{M}$ is an L-structure, then $\mathrm{Sat}_{\mathcal{M}}(\varphi)$ is defined as follows:*

1. $\mathrm{Sat}_{\mathcal{M}}(\approx t_1 t_2) = \{s | t_1^{\mathcal{M}}\langle s \rangle = t_2^{\mathcal{M}}\langle s \rangle\}$
2. $\mathrm{Sat}_{\mathcal{M}}(\mathrm{R}t_1 \ldots t_n) = \{s | \langle t_1^{\mathcal{M}}\langle s \rangle, \ldots, t_n^{\mathcal{M}}\langle s \rangle\rangle \in \mathrm{R}^{\mathcal{M}}\}$
3. $\mathrm{Sat}_{\mathcal{M}}(\neg\varphi) = {}^{\mathbb{N}}M \setminus \mathrm{Sat}_{\mathcal{M}}(\varphi)$
4. $\mathrm{Sat}_{\mathcal{M}}((\varphi \to \psi)) = ({}^{\mathbb{N}}M \setminus \mathrm{Sat}_{\mathcal{M}}(\varphi)) \cup \mathrm{Sat}_{\mathcal{M}}(\psi)$
5. $\mathrm{Sat}_{\mathcal{M}}(\forall v_n \varphi) = A_n(\mathrm{Sat}_{\mathcal{M}}(\varphi))$.

$\mathrm{Sat}_{\mathcal{M}}(\varphi)$ *is the* interpretation *of the formula φ in the L-structure $\mathcal{M}$. We say that s* satisfies *φ in $\mathcal{M}$, $\mathcal{M} \models_s \varphi$, if $s \in \mathrm{Sat}_{\mathcal{M}}(\varphi)$. We say that $\mathcal{M}$* satisfies *φ, denoted $\mathcal{M} \models \varphi$, if $\mathrm{Sat}_{\mathcal{M}}(\varphi) = {}^{\mathbb{N}}M$, in which case we also say that φ is* true *in $\mathcal{M}$ and $\mathcal{M}$ is a* model *of φ.*

The interpretation of a formula φ in a structure $\mathcal{M}$ is a set of assignments, namely the set of those s that satisfy the formula. The bigger $\mathrm{Sat}_{\mathcal{M}}(\varphi)$ is, the more assignments satisfy the formula φ. On the other hand, it may happen that no s satisfies φ.

Example 4.9 *1.* $\mathrm{Sat}_{\mathcal{M}}((\varphi \wedge \psi)) = \mathrm{Sat}_{\mathcal{M}}(\varphi) \cap \mathrm{Sat}_{\mathcal{M}}(\psi)$.

2. $\mathrm{Sat}_{\mathcal{M}}(\exists v_n \varphi) = \{s | s(a/n) \in \mathrm{Sat}_{\mathcal{M}}(\varphi)$ *for some* $a \in M\}$.

Example 4.10 *Let $\mathcal{R} = (\mathbf{R}, +, \cdot, 0, 1)$. Now $s \in \mathrm{Sat}_{\mathcal{R}}(\exists v_0 \approx ++\cdot v_0 v_0 \cdot v_1 v_0 v_2 0)$ if there is $x \in \mathbf{R}$ such that $s(x/0) \in \mathrm{Sat}_{\mathcal{R}}(\approx ++\cdot v_0 v_0 \cdot v_1 v_0 v_2 0)$, i.e. there is $x \in \mathbf{R}$ such that $x^2 + s(1) \cdot x + s(2) = 0$, i.e. the equation $x^2 + s(1) \cdot x + s(2) = 0$ has a solution in the real numbers.*

Example 4.11 $L = \{\mathrm{f}\}, \#_L(\mathrm{f}) = 1, \mathcal{M} = (M, f)$. *Now f is an injection $M \to M$ if and only if $\mathrm{Sat}_{\mathcal{M}}(\forall v_0 \forall v_1 (\approx \mathrm{f}v_0 \mathrm{f}v_1 \to \approx v_0 v_1)) = {}^{\mathbb{N}}M$, and f is a surjection $M \to M$ if and only if $\mathrm{Sat}_{\mathcal{M}}(\forall v_0 \exists v_1 \approx \mathrm{f}v_1 v_0) = {}^{\mathbb{N}}M$.*

Example 4.12 *Let $L = \{+, 0\}$ and $\mathcal{Z} = (\mathbf{Z}, +, 0)$. The L-structure $\mathcal{Z}$ is a model of the following L-formulas:*

1. $\approx +v_0+v_1v_2++v_0v_1v_2$
2. $\approx +v_00v_0, \approx +0v_0v_0$
3. $\exists v_1(\approx +v_0v_10\wedge \approx +v_1v_00)$.

These so-called *group*[4] *axioms* are usually written in the following more familiar way:

$$x + (y + z) = (x + y) + z$$
$$x + 0 = x, 0 + x = x$$
$$\exists y(x + y = y + x = 0)$$

In algebra any L-structure that satisfies the group axioms is called a *group*. A colossal result of mathematical research has been the complete classification of all finite simple groups.

Example 4.13 Number theory *investigates arithmetic properties of the natural numbers* $0, 1, 2, 3, 4, \ldots$. *The so-called* standard model *of number theory is*

$$\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1).$$

Many properties of natural numbers can be expressed in predicate logic:

$s(0)$ *is even if*	$\mathcal{N} \models_s \exists v_1 \approx \cdot{+}11v_1v_0$
$s(0)$ *is prime if*	$\mathcal{N} \models_s \neg\exists v_1\exists v_2((\approx \cdot v_1v_2v_0 \wedge \neg \approx v_1v_0) \wedge \neg \approx v_11)$
$s(0)$ *is a square if*	$\mathcal{N} \models_s \exists v_1 \approx \cdot v_1v_1v_0$.

Definition 4.14 (Logical consequence) *An L-formula ψ is a* logical consequence *of an L-formula φ, in symbols $\varphi \models \psi$, if for all L-structures $\mathcal{M}$ and all $s : \mathbb{N} \to M$ the following holds: if $\mathcal{M} \models_s \varphi$ then $\mathcal{M} \models_s \psi$.*

The logical consequence $\varphi \models \psi$ means that whatever L-structure and whatever assignment we choose, if φ is satisfied, then also ψ is satisfied. This consequence is "logical" in the sense that it is immaterial which structure and which assignment we choose, i.e. ψ follows from φ merely because of its logical form. For example, if φ is the conjunction $(\psi \wedge \theta)$, then of course ψ follows from φ. Thanks to the quantifiers, logical consequence can, however, be extremely complicated. There is no mechanical method for deciding whether a given formula is a logical consequence of another. This is the famous *Church's Theorem* from 1936 [4].

Example 4.15 $\neg\forall v_n\varphi \models \exists v_n\neg\varphi$.

Proof. Suppose $s \in \mathrm{Sat}_{\mathcal{M}}(\neg\forall v_n\varphi)$. Hence $s \notin A_n(\mathrm{Sat}_{\mathcal{M}}(\varphi))$. Therefore there is $a \in M$ such that $s(a/n) \notin \mathrm{Sat}_{\mathcal{M}}(\varphi)$. Thus $\mathcal{M} \models_s \exists v_n\neg\varphi$. □

[4] See footnote on page 23.

Example 4.16 $\forall v_0 \exists v_1 \mathrm{R} v_0 v_1 \not\models \exists v_0 \forall v_1 \mathrm{R} v_0 v_1$.

Proof. Let $\mathcal{M} = (\mathbb{N}, <)$ and $s : \mathbb{N} \to \mathbb{N}$. $s(a/0)(a+1/1) \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R} v_0 v_1)$, whence $s(a/0) \in \mathrm{Sat}_{\mathcal{M}}(\exists v_1 \mathrm{R} v_0 v_1)$ for any $a \in \mathbb{N}$. Therefore $s \in \mathrm{Sat}_{\mathcal{M}}(\forall v_0 \exists v_1 \mathrm{R} v_0 v_1)$. On the other hand, if $s \in \mathrm{Sat}_{\mathcal{M}}(\exists v_0 \forall v_1 \mathrm{R} v_0 v_1)$ then there is $a \in \mathbb{N}$ such that $s(a/0) \in A_1(\mathrm{Sat}_{\mathcal{M}}(\mathrm{R} v_0 v_1))$. In particular $s(a/0)(a/1) \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R} v_0 v_1)$, a contradiction. Therefore $s \notin \mathrm{Sat}_{\mathcal{M}}(\exists v_0 \forall v_1 \mathrm{R} v_0 v_1)$. $\square$

Example 4.17 $\exists v_0 \forall v_1 \varphi \models \forall v_1 \exists v_0 \varphi$.

Proof. Let $\mathcal{M} \models_s \exists v_0 \forall v_1 \varphi$. Then for some $a \in M$ $\mathcal{M} \models_{s(a/0)} \forall v_1 \varphi$. Now we can prove $\mathcal{M} \models_s \forall v_1 \exists v_0 \varphi$. To this end, let $b \in M$ be arbitrary. We know that $\mathcal{M} \models_{s(a/0)(b/1)} \varphi$. But $s(a/0)(b/1) = s(b/1)(a/0)$, whence $\mathcal{M} \models_{s(b/1)} \exists v_0 \varphi$. As b was arbitrary, we have $\mathcal{M} \models_s \forall v_1 \exists v_0 \varphi$. $\square$

Example 4.18 $\forall v_0 (\mathrm{P} v_0 \vee \mathrm{Q} v_0) \not\models (\forall v_0 \mathrm{P} v_0 \vee \forall v_0 \mathrm{Q} v_0)$.

Proof. Let $\mathcal{M} = (\{0,1\}, \{0\}, \{1\})$, where $\mathrm{Sat}_{\mathcal{M}}(\mathrm{P}) = \{0\}$ and $\mathrm{Sat}_{\mathcal{M}}(\mathrm{Q}) = \{1\}$. Let $s : \mathbb{N} \to \{0,1\}$. If $a \in \{0,1\}$, then $a = 0$ or $a = 1$, whence $\mathcal{M} \models_{s(a/0)} (\mathrm{P} v_0 \vee \mathrm{Q} v_0)$. On the other hand $\mathcal{M} \not\models_s \forall v_0 \mathrm{P} v_0$, for $\mathcal{M} \not\models_{s(1/0)} \mathrm{P} v_0$. Similarily, $\mathcal{M} \not\models_s \forall v_0 \mathrm{Q} v_0$. Thus $\mathcal{M} \not\models_s (\forall v_0 \mathrm{P} v_0 \vee \forall v_0 \mathrm{Q} v_0)$. $\square$

Definition 4.19 (Validity) *An L-formula φ is* valid, *$\models \varphi$, if $\mathcal{M} \models_s \varphi$ holds for all L-structures $\mathcal{M}$ and for all $s : \mathbb{N} \to M$. Equivalently,* $\mathrm{Sat}_{\mathcal{M}}(\varphi) = {}^{\mathbb{N}}M$.

Validity is a special case of logical consequence. A valid formula follows logically from any other formula because it is always true. A valid formula expresses a general truth which does not depend on the structure or values of the variables. A valid formula is true merely because of its *form*. For example, $(\varphi \to \varphi)$ is valid, independently of what φ is. As in the case of logical consequence, it would be a mistake to conclude that validity is somehow a trivial property. Because of the aforementioned theorem of Church, validity cannot be checked mechanically. Valid formulas are not always as clear cases as $(\varphi \to \varphi)$. An implication $(\varphi \to \psi)$ may be valid for a deep mathematical reason. Let us think, for example, of number theory. Here φ may be the conjunction of the best known axioms for number theory. Then the question about the validity of $(\varphi \to \psi)$ is in principle (but not *in fact*[5]) as difficult to decide as the question of the truth of ψ in the standard model of number theory.

Example 4.20

1. *$\varphi \models \psi$ if and only if $\models (\varphi \to \psi)$*
2. *$\varphi \models (\psi \wedge \neg\psi)$ if and only if φ has no models if and only if $\varphi \models \psi$ for all ψ.*

[5] By Gödel's First Incompleteness Theorem (Theorem 5.32) every consistent mechanically given set of axioms of number theory can be associated with a truth that cannot be proved from the axioms.

4.1 Formulas

The variable v_0 occurs in the following two formulas

$$\mathrm{R}v_0v_1 \tag{4.1}$$

$$\forall v_0 \mathrm{R}v_0v_1 \tag{4.2}$$

The truth of formula (4.1) depends on the value of v_0, while the truth of (4.2) does not. Respectively, the value of

$$x^2 + y - 5 \tag{4.3}$$

depends on the value of x but the value of

$$\int_0^1 x^2 dx + y \tag{4.4}$$

does not. We say that v_0 occurs in (4.1) *free*, but in (4.2) it is *bound*. We now define the concepts of free and bound occurrence more exactly:

Definition 4.21 (Subformula) *A* subformula *of a formula is a part which itself is a formula. More exactly:*

1. *The only subformula of an atomic formula is the formula itself.*
2. *The subformulas of the formula $\neg\varphi$ are $\neg\varphi$ and subformulas of φ.*
3. *The subformulas of the formula $(\varphi \to \psi)$ are $(\varphi \to \psi)$, subformulas of φ and subformulas of ψ.*
4. *The subformulas of the formula $\forall v_n\varphi$ are $\forall v_n\varphi$ and subformulas of φ.*

Definition 4.22 (Bound and free variables) *An occurrence of a variable v_n in a formula is* bound *if it occurs in a subformula of the form $\forall v_n\psi$. Otherwise the occurrence is* free. *More exactly:*

1. *In an atomic formula all occurrences of variables are free.*
2. *The formula $\neg\varphi$ has the same occurrences of bound variables as φ.*
3. *An occurrence of a variable in $(\varphi \to \psi)$ is bound if it is a bound occurrence in φ or in ψ.*
4. *An occurrence of a variable v_m in $\forall v_n\varphi$ is bound, if it is a bound occurrence in φ or if $n = m$.*

Example 4.23 $(\forall \underset{b}{v_0} \mathrm{R}\underset{b}{v_0}\underset{f}{v_1} \to \forall \underset{b}{v_1}\mathrm{R}\underset{b}{v_1}\underset{f}{v_0})$, $b =$ *bound occurrence*
$\forall \underset{b}{v_0}(\mathrm{R}\underset{b}{v_0}\underset{f}{v_1} \to \forall \underset{b}{v_1}\mathrm{R}\underset{b}{v_1}\underset{b}{v_0})$, $f =$ *free occurrence*

The next theorem shows that whether an assignment s satisfies a formula φ or not depends only on the values $s(n)$ of the assignment on arguments n such that v_n occurs fee in φ. In particular, it depends only on $s(n)$ for such n that v_n overall occurs in φ. These facts are by no means surprising or deep. More interesting is *how* such facts can be proved. The proof is a typical induction argument.

Theorem 4.24 *Let L be a vocabulary, φ an L-formula and $\mathcal{M}$ an L-structure. Let s and s' be two assignment into $\mathcal{M}$ such that $s(n) = s'(n)$ whenever v_n occurrs free in φ. Then $\mathcal{M} \models_s \varphi \Longleftrightarrow \mathcal{M} \models_{s'} \varphi$.*

Proof. Let $\mathcal{E}$ be the set of those L-formulas φ for which the claim holds. We now show

1. Atomic L-formulas are in $\mathcal{E}$
2. $\varphi \in \mathcal{E} \Longrightarrow \neg\varphi \in \mathcal{E}$
3. $\varphi, \psi \in \mathcal{E} \Longrightarrow (\varphi \to \psi) \in \mathcal{E}$
4. $\varphi \in \mathcal{E}, n \in \mathbb{N} \Longrightarrow \forall v_n \varphi \in \mathcal{E}$

From these it follows that the claim holds for all L-formulas.

1. (a) $\approx t_1 t_2 \in \mathcal{E}$. It is easy to see (with a little inductive argument) that $t_i^{\mathcal{M}}\langle s\rangle = t_i^{\mathcal{M}}\langle s'\rangle$. Thus

$$\begin{aligned} \mathcal{M} \models_s \approx t_1 t_2 &\Longleftrightarrow t_1^{\mathcal{M}}\langle s\rangle = t_2^{\mathcal{M}}\langle s\rangle \\ &\Longleftrightarrow t_1^{\mathcal{M}}\langle s'\rangle = t_2^{\mathcal{M}}\langle s'\rangle \\ &\Longleftrightarrow \mathcal{M} \models_{s'} \approx t_1 t_2 \end{aligned}$$

   (b) $\mathrm{R}t_1 \dots t_n \in \mathcal{E}$:

$$\begin{aligned} \mathcal{M} \models_s \mathrm{R}t_1, \dots, t_n &\Longleftrightarrow \langle t_1^{\mathcal{M}}\langle s\rangle, \dots, t_n^{\mathcal{M}}\langle s\rangle\rangle \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) \\ &\underset{\text{as above}}{\Longleftrightarrow} \langle t_1^{\mathcal{M}}\langle s'\rangle, \dots, t_n^{\mathcal{M}}\langle s'\rangle\rangle \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) \\ &\Longleftrightarrow \mathcal{M} \models_{s'} \mathrm{R}t_1 \dots t_n. \end{aligned}$$

2. Suppose $\varphi \in \mathcal{E}$. Now

$$\begin{aligned} \mathcal{M} \models_s \neg\varphi &\Longleftrightarrow \mathcal{M} \not\models_s \varphi \underset{Ind.Hyp.}{\Longleftrightarrow} \mathcal{M} \not\models_{s'} \varphi \\ &\Longleftrightarrow \mathcal{M} \models_{s'} \neg\varphi. \end{aligned}$$

3. Suppose $\varphi, \psi \in \mathcal{E}$. As above, $(\varphi \to \psi) \in \mathcal{E}$.
4. Suppose $\varphi \in \mathcal{E}$ and $n \in \mathbb{N}$. We show that $\forall v_n \varphi \in \mathcal{E}$. To this end, let $s : \mathbb{N} \to M$ and $s' : \mathbb{N} \to M$ such that $s(i) = s'(i)$ whenever v_i occurs free in $\forall v_n \varphi$.

$$\begin{aligned} \mathcal{M} \models_s \forall v_n \varphi &\Longleftrightarrow \text{for all } a \in M : \mathcal{M} \models_{s(a/n)} \varphi \\ &\Longleftrightarrow^{6} \text{for all } a \in M : \mathcal{M} \models_{s'(a/n)} \varphi \\ &\Longleftrightarrow \mathcal{M} \models_{s'} \forall v_n \varphi. \end{aligned}$$

□

[6] Observe that $s(a/n)(i) = s'(a/n)(i)$ whenever v_i occurs free in φ, for if $i = n$, then $s(a/n)(i) = a = s'(a/n)(i)$. If on the other hand $i \neq n$, then v_i occurs free also in $\forall v_n \varphi$ and $s(a/n)(i) = s(i) = s'(i) = s'(a/n)(i)$, whence the Induction Hypothesis applies.

Theorem 4.25 *Let L and L' be vocabularies such that $L \subseteq L'$. Let φ be an L-formula and $\mathcal{M}$ an L'-structure. Let s be an assignment into M. Then $\mathcal{M} \models_s \varphi \iff \mathcal{M} \restriction L \models_s \varphi$.*

Proof. See Problem 8. □

Definition 4.26 (Sentence) *An L-formula is an L-*sentence*, if no variable occurs free in it.*

We have defined[7] $\mathcal{M} \models \varphi$ to mean that $\mathcal{M} \models_s \varphi$ for all $s : \mathbb{N} \to M$. If φ is an L-sentence, then Theorem 4.24 reveals that $\mathcal{M} \models_s \varphi$ for *all* $s : \mathbb{N} \to M$ if and only if $\mathcal{M} \models_s \varphi$ for *some* $s : \mathbb{N} \to M$. This shows that the truth of a sentence in a model is independent of the assignment.

The following theorem is fundamental and widely used. It shows that isomorphism preserves truth. In other words, it shows that with the sentences of predicate logic one cannot distinguish isomorphic structures from each other. This is in fact how it should be. Isomorphic structures are, from the point of view of logic, identical.

Theorem 4.27 (Isomorphism preserves truth) *Let $\mathcal{M}$ and $\mathcal{M}'$ be L-structures and $\pi : M \to M'$ an isomorphism. Then $\mathcal{M} \models_s \varphi \iff \mathcal{M}' \models_{\pi \circ s} \varphi$ for all L-formulas φ and assignments $s \in {}^{\mathbb{N}}M$.*

Proof. Let $\mathcal{E}$ be the set of those formulas φ for which: "for all $s \in {}^{\mathbb{N}}M$: $\mathcal{M} \models_s \varphi \iff \mathcal{M}' \models_{\pi \circ s} \varphi$". We show by induction that all formulas are in $\mathcal{E}$.

1. $\approx t_1 t_2 \in \mathcal{E}$, for:

$$\begin{aligned}
\mathcal{M} \models_s \approx t_1 t_2 &\iff t_1^{\mathcal{M}}\langle s\rangle = t_2^{\mathcal{M}}\langle s\rangle \text{ Definition 4.8} \\
&\iff \pi(t_1^{\mathcal{M}}\langle s\rangle) = \pi(t_2^{\mathcal{M}}\langle s\rangle) \text{ since } \pi \text{ is an injection} \\
&\iff t_1^{\mathcal{M}'}\langle \pi \circ s\rangle = t_2^{\mathcal{M}'}\langle \pi \circ s\rangle \text{ Lemma 4.4} \\
&\iff \mathcal{M}' \models_{\pi \circ s} \approx t_1 t_2 \text{ Definition 4.8}
\end{aligned}$$

2. $\mathrm{R} t_1 \dots t_n \in \mathcal{E}$, for:

$$\begin{aligned}
\mathcal{M} \models_s \mathrm{R} t_1 \dots t_n &\iff \langle t_1^{\mathcal{M}}\langle s\rangle, \dots, t_n^{\mathcal{M}}\langle s\rangle\rangle \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) \text{ Definition 4.8} \\
&\iff \langle \pi t_1^{\mathcal{M}}\langle s\rangle, \dots, \pi t_n^{\mathcal{M}}\langle s\rangle\rangle \in \mathrm{Sat}_{\mathcal{M}'}(\mathrm{R}) \text{ Definition 3.9} \\
&\iff \langle t_1^{\mathcal{M}'}\langle \pi \circ s\rangle, \dots, t_n^{\mathcal{M}'}\langle \pi \circ s\rangle\rangle \in \mathrm{Sat}_{\mathcal{M}'}(\mathrm{R}) \text{ By Lemma 4.4} \\
&\iff \mathcal{M}' \models_{\pi \circ s} \mathrm{R} t_1 \dots t_n \text{ Definition 4.8}
\end{aligned}$$

3. Suppose $\varphi \in \mathcal{E}$. We prove $\neg\varphi \in \mathcal{E}$.

$$\begin{aligned}
\mathcal{M} \models_s \neg\varphi &\iff \mathcal{M} \not\models_s \varphi \text{ Definition 4.8} \\
&\iff \mathcal{M}' \not\models_{\pi \circ s} \varphi, \text{ since } \varphi \in \mathcal{E} \\
&\iff \mathcal{M}' \models_{\pi \circ s} \neg\varphi \text{ Definition 4.8}
\end{aligned}$$

[7]Definition 4.8

4. Suppose $\varphi \in \mathcal{E}$ and $\psi \in \mathcal{E}$ and show $(\varphi \to \psi) \in \mathcal{E}$. Trivial!
5. Suppose $\varphi \in \mathcal{E}$ and $n \in \mathbb{N}$. We first observe: If $a \in M$, then

$$(\pi \circ s)(\pi(a)/n) = \pi \circ (s(a/n))) \tag{4.5}$$

$$\begin{array}{rcl}
\mathcal{M} \models_s \forall v_n \varphi & \Longleftrightarrow & \text{for all } a \in M \;\; \mathcal{M} \models_{s(a/n)} \varphi \\
& \underset{Ind.Hyp.}{\Longleftrightarrow} & \text{for all } a \in M \;\; \mathcal{M}' \models_{\pi\circ(s(a/n))} \varphi \\
& \underset{(4.5)}{\Longleftrightarrow} & \text{for all } a \in M \;\; \mathcal{M}' \models_{(\pi\circ s)(\pi(a)/n)} \varphi \\
& \underset{\pi \ surj.}{\Longleftrightarrow} & \text{for all } a' \in M' \;\; \mathcal{M}' \models_{(\pi\circ s)(a'/n)} \varphi \\
& \Longleftrightarrow & \mathcal{M}' \models_{\pi\circ s} \forall v_n \varphi
\end{array}$$

□

The next corollary is the main application of the above theorem: Isomorphic structures satisfy the same sentences.

Corollary 4.28 *If $\mathcal{M}$ and $\mathcal{M}'$ are L-structures and $\mathcal{M} \cong \mathcal{M}'$, then for all L-sentences φ: $\mathcal{M} \models \varphi \Longleftrightarrow \mathcal{M}' \models \varphi$*

Two structures need not be isomorphic for the same sentences to be true in them. We will see that there are infinite structures which satisfy exactly the same sentences and yet they are non-isomorphic. This fact is the reason for the following important definition:

Definition 4.29 (Elementary equivalence) *L-structures $\mathcal{M}$ and $\mathcal{M}'$ are* elementarily equivalent*, denoted $\mathcal{M} \equiv \mathcal{M}'$ if $\mathcal{M} \models \varphi \Longleftrightarrow \mathcal{M}' \models \varphi$ for all L-sentences φ.*

The message of Corollary 4.28 can now be written: $\mathcal{M} \cong \mathcal{M}'$ implies $\mathcal{M} \equiv \mathcal{M}'$.

Along with the concept of truth (Definition 4.8), the following concept is a very central one in logic.

Definition 4.30 (Definability) *Let $\mathcal{M}$ be an L-structure and $X \subseteq M^n$. We say that the relation X is* definable *in $\mathcal{M}$ if there is an L-formula φ such that*

$$\mathcal{M} \models_s \varphi \Longleftrightarrow \langle s(0), \ldots, s(n-1)\rangle \in X$$

for all $s : \mathbb{N} \to M$. We then say that φ defines *the relation X. An element $a \in M$ is* definable *in $\mathcal{M}$ if the 1-place relation $\{a\}$ is. A function $h : M^n \to M$ is* definable *in $\mathcal{M}$ if the $n+1$-place relation*

$$\{\langle a_0, \ldots, a_{n-1}, h(a_0, \ldots, a_{n-1})\rangle | a_0, \ldots, a_{n-1} \in M\}$$

is.

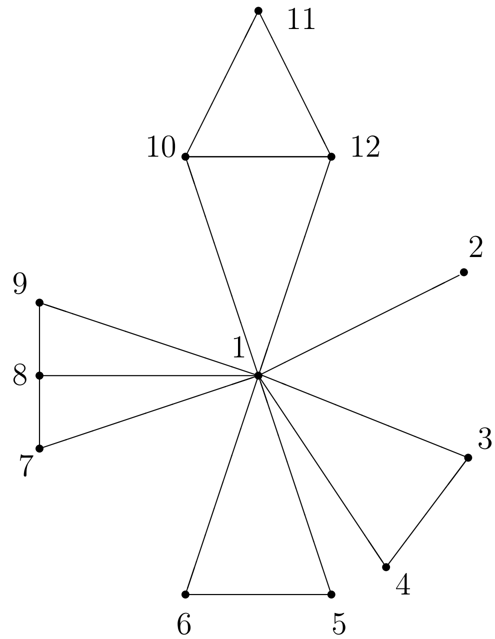


Figure 4.1: A graph.

We proved in Theorem 4.27 that isomorphisms preserve truth, and the analogous result for automorphisms is:

Theorem 4.31 (Automorphisms preserve definable relations) *Let $\mathcal{M}$ be an L-structure and the relation $X \subseteq M^n$ be definable in $\mathcal{M}$. If π is an automorphism of $\mathcal{M}$, then $\langle a_1, \ldots, a_n \rangle \in X \iff \langle \pi(a_1), \ldots, \pi(a_n) \rangle \in X$ for all $a_1, \ldots, a_n \in M$. A corresponding result holds for definable functions and elements.*

Proof. Let φ be an L-formula such that $\langle s(0), \ldots, s(n-1) \rangle \in X \iff \mathcal{M} \models_s \varphi$. Now

$$\begin{aligned} \langle s(0), \ldots, s(n-1) \rangle \in X &\iff \mathcal{M} \models_s \varphi \\ &\iff \mathcal{M} \models_{\pi \circ s} \varphi \text{ by Theorem 4.27} \\ &\iff \langle \pi(s(0)), \ldots, \pi(s(n-1)) \rangle \in X \end{aligned}$$

The claim follows upon choosing $s(i) = a_{i+1}$. □

Example 4.32 *Figure 4.1 is a* 12 *element graph* $\mathcal{G} = (G, R)$ *The element* 2 *is* *definable, for* $s(0) = 2 \iff \mathcal{G} \models_s \exists v_1 \forall v_2 (\mathrm{R} v_2 v_0 \to \approx v_2 v_1)$ *for all* s*. Let*

$$\begin{array}{lc} \theta_2 & \neg \approx v_1 v_2 \\ \theta_3 & ((\theta_2 \wedge \neg \approx v_1 v_3) \wedge \neg \approx v_2 v_3) \\ \theta_4 & (((\theta_3 \wedge \neg \approx v_1 v_4) \wedge \neg \approx v_2 v_4) \wedge \neg \approx v_3 v_4) \\ \vdots & \\ \theta_{n+1} & (\ldots(\theta_n \wedge \neg \approx v_1 v_{n+1}) \wedge \neg \approx v_2 v_{n+1}) \wedge \ldots \wedge \neg \approx v_n v_{n+1}) \end{array}$$

Thus θ_n says that $v_1, \ldots, v_n$ are distinct elements. Let ψ_n be the formula

$$\exists v_1 \ldots \exists v_n (\theta_n \wedge (\mathrm{R} v_0 v_1 \wedge \ldots \wedge \mathrm{R} v_0 v_n)).$$

Thus ψ_n says that v_0 has at least n neighbors. Let φ_n be the formula $(\psi_n \wedge \neg\psi_{n+1})$, which says that v_0 has exactly n neighbors.

The formula φ_2 defines the set $\{3, 4, 5, 6, 7, 9, 11\}$. The formula φ_3 defines the set $\{8, 10, 12\}$. The formula φ_{10} defines the element 1. The element 3 is not definable because

$$\pi(x) = \begin{cases} 4 & \text{if } x = 3 \\ 3 & \text{if } x = 4 \\ x & \text{otherwise} \end{cases}$$

is an automorphism of $\mathcal{G}$. In this way one can go through the entire graph and figure out which subsets are definable and which are not.

Example 4.33 *Every element of the structure* $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1)$ *is definable. The structure* $\mathcal{N}$ *does not have other automorphisms than the identity mapping. (Such structures are called* rigid*). Every element of* $\mathcal{Q} = (\mathbf{Q}, +, \cdot, 0, 1)$ *is definable. Every element of* $(\mathbb{N}, <)$ *is definable, but in the structure* $(\mathbf{Q}, <)$ no *element is definable.*

Example 4.34 *Let* $\mathcal{G}$ *be as in Example 4.32. In the structure* $\mathcal{G}' = (G, R, 3)$ *the element* 3 *has been given a name, for example* c_3*. Now the formula* $\approx v_0 \mathrm{c}_3$ *defines the element* 3 *in* $\mathcal{G}'$*. Recall that* 3 *was undefinable in* $\mathcal{G}$*. The element* 4 *is defined by the formula* $(\mathrm{R} v_0 \mathrm{c}_3 \wedge \neg\varphi_{10})$*. The sets* $\{3, 4\}$ *and* $\{5, 6\}$*, which were not definable in* $\mathcal{G}$*, are now definable in* $\mathcal{G}'$*.*

We shall now introduce a concept which is relevant only because we are using the same symbols for bound and free variables and this sometimes creates tricky situations. We have a formula, e.g. $\varphi = \exists v_2 (\mathrm{R} v_0 v_2 \wedge \mathrm{R} v_1 v_2)$ and we would like to have a formula φ' which says about v_0 and v_2 what φ says about v_0 and v_1. A direct substitution of v_2 to v_1 does not work for it yields $\exists v_2 (\mathrm{R} v_0 v_2 \wedge \mathrm{R} v_2 v_2)$ which has only v_0 free. We have to do something else.

Definition 4.35 (Free for) *The term* t *is* free for v_n *in* φ, $\mathrm{FVF}(t, v_n, \varphi)$*, if no occurrence of a variable in the term* t *will be a bound occurrence after the substitution of* t *to the free occurrences of* v_n *in* φ*.*

Here are some examples:

free	not free	for the variable	in the formula
v_2	v_1	v_0	$\exists v_1 \approx v_0 v_1$
$\mathrm{f}v_0$	$\mathrm{f}v_1$	v_0	$\exists v_1 \approx v_0 v_1$
v_0	-	v_1	$\mathrm{R}v_0 v_1$
$\mathrm{f}v_2 v_3$	$\mathrm{f}v_0 v_1$	v_2	$\exists v_0 \forall v_1 \approx \mathrm{f}v_0 v_1 v_2$
$\mathrm{f}v_0 v_1$	$\mathrm{f}v_3 v_4$	v_2	$\exists v_3 \forall v_4 \approx \mathrm{f}v_3 v_4 v_2$

Theorem 4.36 *for all t, v_n and φ there is φ^* such that $\models \varphi \leftrightarrow \varphi^*$ and $\mathrm{FVF}(t, v_n, \varphi^*)$.*

Proof. Problem 17. $\square$.

Theorem 4.37 (Substitution lemma) *Let be a L vocabulary, $\mathcal{M}$ an L-structure and $s : \mathbb{N} \to M$ an assignment.*

1. *Let t be an L-term in variables $v_0, \ldots, v_n$. Let $t_0, \ldots, t_n$ be L-terms. Let t' be obtained from t by replacing v_i by the term t_i for $i = 0, ..., n$. Then $(t')^{\mathcal{M}}\langle s\rangle = t^{\mathcal{M}}\langle s'\rangle$, where*

$$s'(i) = \begin{cases} t_i^{\mathcal{M}}\langle s\rangle & i \leq n \\ s(i) & i > n \end{cases}$$

2. *Let φ be an L-formula with $v_0, \ldots, v_n$ free. Let $t_0, \ldots, t_n$ be L-terms. Let φ' be obtained from φ by replacing v_i by t_i, in its free occurrences when $0 \leq i \leq n$. Suppose, that $\mathrm{FVF}(t_i, v_i, \varphi)$ for $0 \leq i \leq n$. Then*

$$\mathcal{M} \models_{s'} \varphi \Longleftrightarrow \mathcal{M} \models_s \varphi'$$

for s' as in 1 above.

Proof. Problems 18 and 19. $\square$

4.2 Identity

The simplest relation between variables is identity. It is particularly easy to see which formulas concerning identity are valid.

Lemma 4.38 *The following L-formulas are valid for all atomic L-formulas φ, all L-terms $t, t', t_1, \ldots, t_n, u_1, \ldots, u_n$ and all distinct natural numbers $m_1, ..., m_n$.*

1. $\approx tt$
2. $(\approx tt' \to \approx t't)$
3. $(((\approx t_1 u_1 \wedge ... \wedge \approx t_n u_n) \wedge \varphi') \to \varphi'')$

where φ' is obtained from φ by replacing each variable v_{m_i} by the term t_i, and φ'' respectively by replacing each variable v_{m_i} by the term u_i, for all $1 \leq i \leq n$.

Proof. Let $\mathcal{M}$ be an L-structure and $s : \mathbb{N} \to M$ and assignment. The claims 1 and 2 are trivial, so we focus on claim 3. Suppose

$$\mathcal{M} \models_s ((\approx t_1 u_1 \wedge ... \wedge \approx t_n u_n) \wedge \varphi')$$

Thus $t_i^{\mathcal{M}}\langle s\rangle = u_i^{\mathcal{M}}\langle s\rangle$ for $i = 1, \ldots, n$ and $\mathcal{M} \models_s \varphi'$. Let

$$s'(j) = \begin{cases} t_i^{\mathcal{M}}\langle s\rangle & j = m_i \\ s(j) & \text{otherwise} \end{cases}$$

and

$$s''(j) = \begin{cases} u_i^{\mathcal{M}}\langle s\rangle & j = m_i \\ s(j) & \text{otherwise.} \end{cases}$$

By Theorem 4.37

$$\begin{array}{ccc} \mathcal{M} \models_s \varphi' & \iff & \mathcal{M} \models_{s'} \varphi \\ \mathcal{M} \models_s \varphi'' & \iff & \mathcal{M} \models_{s''} \varphi \end{array}$$

Since now $s'(i) = s''(i)$ for all i, we obtain $\mathcal{M} \models_s \varphi' \iff \mathcal{M} \models_s \varphi''$. $\square$

Definition 4.39 (Identity axiom) *The formulas 1-3 of Lemma 4.38 are called* L-identity axioms.

Identity axioms are very simple, but sometimes one may need to be observant to recognise that a given formula is an identity axiom.

Example 4.40 *L-identity axioms:*

$$\approx v_0 v_0, \approx cc, \approx \mathrm{f} v_0 v_1 \mathrm{f} v_0 v_1$$

$$((\approx v_0 v_1 \wedge \mathrm{R} v_0) \to \mathrm{R} v_1)$$

$$((\approx v_0 v_1 \wedge \approx \mathrm{f} v_0 v_2) \to \approx \mathrm{f} v_1 v_2)$$

$$((\approx v_1 v_0 \wedge \approx v_1 v_2) \to \approx v_0 v_2).$$

4.3 Deduction

Deductions in predicate logic proceed very much as they do in propositional logic. The presence of the identity symbol and the quantifier symbol bring new axioms and a new rule in addition to Modus Ponens rule. We will eventually show that, just like propositional logic, also predicate logic permits a Completeness Theorem, implying that the given axioms and rules are indeed all that is needed.

Every predicate logic formula is either atomic, a negated formula, an implication, or a universally quantified formula. If atomic formulas and formulas starting with a universal quantifier are thought of as proposition symbols, the formulas of predicate logic are in fact propositional formulas. Therefore it makes sense to talk e.g. about the formulas $(\approx tt' \rightarrow \approx tt'), (\forall v_0\varphi \vee \neg\forall v_0\varphi)$ as tautologies. A formula φ being a tautology means thus that whichever valuation we use to associate atomic formulas and formulas starting with a universal quantifier with the numbers 0 and 1, then φ gets in this valuation the value 1. Note that $\exists v_0\varphi$ is a shorthand of $\neg\forall v_0\neg\varphi$. Thus $(\forall v_i\neg\varphi \vee \exists v_i\varphi), \neg(\forall v_i\neg\varphi \wedge \exists v_i\varphi)$ are tautologies.

A *deduction* is a sequence of formulas, where each member of the sequence is obtained from previous members by so-called rules of inference. Some members of the sequence have a special role. These are the the axioms of propositional logic, L-identity axioms, and so-called quantifier axioms:

Definition 4.41 (Quantifier axiom) *Suppose L is a vocabulary. L-formulas $(\forall v_j\psi \rightarrow \psi')$, where ψ' is obtained from ψ by substituting the term t to the free occurrences of v_j, assuming* $\mathrm{FVF}(t, v_j, \psi)$*, are called* L-quantifier axioms.

Lemma 4.42 *L-quantifier axioms are valid.*

Proof. Suppose $\mathcal{M} \models_s \forall v_j\psi$ and $\mathrm{FVF}(t, v_j, \psi)$. Thus $\mathcal{M} \models_{s(a/j)} \psi$, where $a = t^{\mathcal{M}}\langle s\rangle$. By Theorem 4.37, $\mathcal{M} \models_s \psi'$. Hence $\models \forall v_j\psi \rightarrow \psi'$.
□

Definition 4.43 (Deduction) *The L-*axioms *of predicate logic are the following:*

- *L-formulas that are axioms of propositional logic are L-axioms of predicate logic.*
- *L-identity axioms are L-axioms of predicate logic.*
- *L-quantifier axioms are L-axioms of predicate logic.*

The set of L-formulas that are provable *from a set Σ of L-formulas is defined as follows:*

(T1) Each member of Σ is provable from Σ.

(T2) Every L-axiom is provable from Σ.

(T3) Modus Ponens: If L-formulas φ and $(\varphi \rightarrow \psi)$ are provable from Σ, then also ψ is provable from Σ.

(T4) Universal generalisation*: If the L-formula $(\psi \rightarrow \theta)$ is provable from some $\Sigma' \subseteq \Sigma$ and v_j is a variable such that*

- *v_j does not occur free in ψ*
- *v_j does not occur free in the formulas of Σ'*

then $(\psi \to \forall v_j\theta)$ *is provable from* Σ.

If an L-formula φ *is provable from* Σ*, we write* $\Sigma \vdash \varphi$*. If* $\emptyset \vdash \varphi$*, we write* $\vdash \varphi$ *and say that* φ *is* provable.

The universal generalisation rule (T4) above requires that v_j does not occur free in the formulas of Σ' just as we assume v_j does not occur free in ψ. The following example shows that this is necessary.

Example 4.44 *In (T4) we have to assume that* v_j *does not occur free in* ψ*, because of examples such as* $\models (\mathrm{P}x \wedge \mathrm{R}x) \to \mathrm{R}x$ *but* $\not\models (\mathrm{P}x \wedge \mathrm{R}x) \to \forall x\mathrm{R}x$*. Respectively, we have to assume that* v_j *does not occur free in the formulas of* Σ*, because* $\{\mathrm{P}x \wedge \mathrm{R}x\} \models \mathrm{R}x$ *but* $\{\mathrm{P}x \wedge \mathrm{R}x\} \not\models \forall x\mathrm{R}x$*.*

Provability can be equivalently defined as follows:

Definition 4.45 (Deduction) *Let* L *be a vocabulary and* Σ *a set of* L*-formulas. A* deduction *from* Σ *is a sequence* $\langle\varphi_1, \ldots, \varphi_n\rangle$ *of* L*-formulas such that each* φ_i *satisfies one of the conditions:*

1. φ_i *is an element of* Σ
2. φ_i *is an axiom of propositional logic*
3. φ_i *is an L-identity axiom*
4. φ_i *is an L-quantifier axiom*
5. φ_i *is obtained by the* Modus Ponens*-rule from earlier ones, i.e. there are* $j, k < i$ *such that* $\varphi_j = (\varphi_k \to \varphi_i)$
6. φ_i *is obtained by the* universal generalisation*-rule from earlier ones, i.e.* $\varphi_i = (\psi \to \forall v_j\theta)$ *and there are* $k < i$ *and* $l_1, \ldots, l_m < k$ *such that*
    - $\varphi_k = (\psi \to \theta)$
    - v_j *does not occur free in* ψ
    - v_j *does not occur free in the formulas* $\{\varphi_{l_p}\}$*,* $p = 1, \ldots, k$*.*

Clearly, an L-formula φ is provable from Σ if and only if there is deduction $\langle\varphi_1 \ldots \varphi_n\rangle$ from Σ such that $\varphi_n = \varphi$.

Lemma 4.46 *If* φ *is provable from* Σ *and* $\Sigma \subseteq \Sigma'$*, then* φ *is provable from* Σ'*.*

Proof. See Problem 20. □

In propositional logic we showed that tautologies are provable. Therefore we can now accept any tautology as a step of a deduction.

Example 4.47 *Suppose, that* ψ' *is obtained from the formula* ψ *by substituting the term* t *to the free occurrences of the variable* v_j *and additionally* $\mathrm{FVF}(t, v_j, \psi)$ *holds. Then* $\vdash (\psi' \to \exists v_j\psi)$*:*

1.	$(\forall v_j\neg\psi \to \neg\psi')$	*L-quantifier axiom*
2.	$((\forall v_j\neg\psi \to \neg\psi') \to (\psi' \to \neg\forall v_j\neg\psi))$	*tautology*
3.	$(\psi' \to \exists v_j\psi)$	*MP 1,2*

Example 4.48 *Suppose $\Sigma \vdash (\psi \to \theta)$, where v_j does not occur free in θ or in the formulas of Σ. Then $\Sigma \vdash (\exists v_j \psi \to \theta)$.*

1.	$(\psi \to \theta)$	*by assumption*
2.	$((\psi \to \theta) \to (\neg\theta \to \neg\psi))$	*tautology*
3.	$(\neg\theta \to \neg\psi)$	*MP 1,2*
4.	$(\neg\theta \to \forall v_j \neg\psi)$	*universal generalisation 3*
5.	$((\neg\theta \to \forall v_j \neg\psi) \to (\neg\forall v_j \neg\psi \to \theta))$	*tautology*
6.	$(\exists v_j \psi \to \theta)$	*MP 4,5*

□

Example 4.49 $\{\mathrm{R}c, \forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)\} \vdash \mathrm{P}c$

1.	$(\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0) \to (\mathrm{R}c \to \mathrm{P}c))$	*quantifier axiom*
2.	$\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)$	*assumption*
3.	$(\mathrm{R}c \to \mathrm{P}c)$	*MP 1,2*
4.	$\mathrm{R}c$	*assumption*
5.	$\mathrm{P}c$	*MP 3,4*

□

Example 4.50 $\{\forall v_n \neg\varphi\} \vdash \neg\exists v_n \varphi$

1.	$(\forall v_n \neg\varphi \to \neg\neg\forall v_n \neg\varphi)$	*tautology*
2.	$\forall v_n \neg\varphi$	*assumption*
3.	$\neg \underbrace{\neg\forall v_n \neg\varphi}_{\exists v_n \varphi}$	*MP 1,2*

□

Example 4.51 $\{\exists v_n \neg\varphi\} \vdash \neg\forall v_n \varphi$

1.	$(\forall v_n \varphi \to \varphi)$	*quantifier axiom*
2.	$((\forall v_n \varphi \to \varphi) \to (\forall v_n \varphi \to \neg\neg\varphi))$	*tautology*
3.	$(\forall v_n \varphi \to \neg\neg\varphi)$	*MP 1,2*
4.	$(\forall v_n \varphi \to \forall v_n \neg\neg\varphi)$	*universal generalisation 3*
5.	$((\forall v_n \varphi \to \forall v_n \neg\neg\varphi) \to (\neg\forall v_n \neg\neg\varphi \to \neg\forall v_n \varphi))$	*tautology*
6.	$(\underbrace{\neg\forall v_n \neg\neg\varphi}_{\exists v_n \neg\varphi} \to \neg\forall v_n \varphi)$	*MP 5,6*
7.	$\exists v_n \neg\varphi$	*assumption*
8.	$\neg\forall v_n \varphi$	*MP 6,7*

□

Theorem 4.52 (Soundness Theorem) *If $\Sigma \vdash \varphi$, then $\Sigma \models \varphi$.*

Proof. Let $\langle \varphi_1, \ldots, \varphi_n \rangle$ be a deduction of a formula φ from $\Sigma' \subseteq \Sigma$. We prove by induction on n the following claim, from which $\Sigma \models \varphi$ follows:

Claim: $\Sigma' \models \varphi_i$.

1. φ_i is an element of Σ'. Clear.

2. φ_i is an axiom of propositional logic. Clear.
3. φ_i is an identity axiom. Lemma 4.38.
4. φ_i is a quantifier axiom. Lemma 4.42.
5. φ_i is obtained by Modus Ponens from φ_j and φ_k, where $\varphi_k = (\varphi_j \to \varphi_i)$. By the the Induction Hypothesis $\Sigma' \models \varphi_j$ and $\Sigma' \models \varphi_k$. Hence $\Sigma' \models \varphi_i$.
6. φ_i is obtained by the universal generalisation rule i.e. $\varphi_i = (\psi \to \forall v_k \theta)$ and $\varphi_j = (\psi \to \theta)$ for some $j < i$, and v_k is not free in ψ or in Σ'. We show $\Sigma' \vDash (\psi \to \forall v_k \theta)$. Let $\mathcal{M} \vDash_s \Sigma'$ and $\mathcal{M} \vDash_s \psi$. Let $a \in M$. By Theorem 4.24 $\mathcal{M} \vDash_{s(a/n)} \Sigma'$ and $\mathcal{M} \vDash_{s(a/n)} \psi$. By Induction Hypothesis $\Sigma' \vDash (\psi \to \theta)$, whence $\mathcal{M} \vDash_{s(a/n)} \theta$. We have proved $\mathcal{M} \vDash_s \forall v_k \theta$. $\square$

The Soundness Theorem 4.52 gives us a powerful method for showing that $\Sigma \nvdash \varphi$:

Corollary 4.53 *If $\Sigma \nvDash \varphi$, then $\Sigma \nvdash \varphi$.*

Example 4.54 $\{\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0), \mathrm{Pc}\} \nvdash \mathrm{R\,c}$.

Proof. Let $\mathcal{M} = (\{0\}, \mathrm{Sat}_{\mathcal{M}})$, where $\mathrm{Sat}_{\mathcal{M}}(\mathrm{c}) = 0$, $\mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) = \emptyset$ and $\mathrm{Sat}_{\mathcal{M}}(\mathrm{P}) = \{0\}$. Now $\mathcal{M} \vDash \forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)$ and $\mathcal{M} \vDash \mathrm{P\,c}$, but $\mathcal{M} \nvDash \mathrm{R\,c}$. $\square$

Example 4.55 $\{\forall v_0 \exists v_1 \mathrm{R}v_0 v_1, \forall v_1 \exists v_0 \mathrm{R}v_0 v_1\} \nvdash \exists v_0 \mathrm{R}v_0 v_0$

Proof. Let $\mathcal{M} = (\{0,1\}, \{\langle 0,1\rangle, \langle 1,0\rangle\})$. Now $\mathcal{M} \vDash \forall v_0 \exists v_1 \mathrm{R}v_0 v_1$, $\mathcal{M} \vDash \forall v_1 \exists v_0 \mathrm{R}v_0 v_1$, but $\mathcal{M} \nvDash \exists v_0 \mathrm{R}v_0 v_0$. $\square$

The following lemma shows that in certain situations a constant symbol can be replaced by a variable symbol. For example the following deduction of $(\mathrm{Rc} \to \exists v_0 \mathrm{R}v_0)$

(1)	$(\forall v_0 \neg \mathrm{R}v_0 \to \neg \mathrm{Rc})$	quantifier axiom
(2)	$((\forall v_0 \neg \mathrm{R}v_0 \to \neg \mathrm{Rc}) \to (\mathrm{Rc} \to \neg \forall v_0 \neg \mathrm{R}v_0))$	tautology
(3)	$(\mathrm{Rc} \to \neg \forall v_0 \neg \mathrm{R}v_0)$	MP 1,2
(4)	$(\mathrm{Rc} \to \exists v_0 \mathrm{R}v_0)$	shorthand

can be translated into a deduction of $(\mathrm{R}v_1 \to \exists v_0 \mathrm{R}v_0)$ by replacing c everywhere by v_1:

(1)	$(\forall v_0 \neg \mathrm{R}v_0 \to \neg \mathrm{R}v_1)$	quantifier axiom
(2)	$((\forall v_0 \neg \mathrm{R}v_0 \to \neg \mathrm{R}v_1) \to (\mathrm{R}v_1 \to \neg \forall v_0 \neg \mathrm{R}v_0))$	tautology
(3)	$(\mathrm{R}v_1 \to \neg \forall v_0 \neg \mathrm{R}v_0)$	MP 1,2
(4)	$(\mathrm{R}v_1 \to \exists v_0 \mathrm{R}v_0)$	shorthand

Convention: If φ is formula and t a term, then $\varphi(t/v_n)$ means a formula obtained from φ by replacing v_n in its free occurrences by the term t. Similarly, $t(t'/v_n)$ is the result of replacing v_n by t' everywhere in the term t.

The basic property of the formula $\varphi(t/v_n)$ is the following: Let us suppose $\mathrm{FVF}(t, v_n, \varphi)$. Theorem 4.37 gives $\mathcal{M} \models_s \varphi(t/v_n) \iff \mathcal{M} \models_{s(a/n)} \varphi$, where $a = t^{\mathcal{M}}\langle s\rangle$. In other words, if t is free for v_n in the formula φ, then to decide whether an assignment s satisfies the formula $\varphi(t/v_n)$ it suffices to compute the value a of t and decide whether $s(a/n)$ satisfies the formula φ.

Lemma 4.56 (Lemma on Constants) *Let L be a vocabulary, φ an L-formula, $n \in \mathbb{N}$, $c \notin L$ and Σ a set of L-formulas. If $\Sigma \vdash \varphi(\mathrm{c}/v_n)$ then there is $m \in \mathbb{N}$ such that $\Sigma \vdash \varphi(v_k/v_n)$ whenever $k \geq m$.*

Proof. Let $\langle \varphi_1, \ldots, \varphi_{n'}\rangle$ be a deduction of the formula $\varphi(\mathrm{c}/v_n)$ from Σ. Let $m \in \mathbb{N}$ be so big, that v_k does not occur at all in the formulas $\varphi_1, \ldots, \varphi_{n'}$ when $k \geq m$. Fix $k \geq m$. If θ is any formula, then let θ' be obtained from θ by replacing c everywhere by v_k. Since $\mathrm{c} \notin L$, we have $\theta' = \theta$ for all L-formulas θ. Since the formulas φ_i are $L \cup \{c\}$-formulas, the same does not hold for them.

Claim. $\langle \varphi'_1, \ldots, \varphi'_{n'}\rangle$ is a deduction from Σ

1. $\varphi_i \in \Sigma$: $\varphi'_i = \varphi_i$ whence $\varphi_i \in \Sigma$
2. φ_i tautology: Clearly φ'_i is a tautology
3. φ_i is an identity axiom. Clearly φ'_i is an identity axiom
4. φ_i is quantifier axiom $\forall v_j \psi \to \psi(t/v_j)$ where $\mathrm{FVF}(t, v_j, \psi)$. Let t' be the result of replacing c by v_k everywhere in the term t. Clearly also $\mathrm{FVF}(t', v_j, \psi')$, whence $\varphi'_i = \forall v_j \psi' \to \psi'(t'/v_j)$ is a quantifier axiom.
5. φ_i is obtained by MP from the formulas φ_j and $\varphi_k = (\varphi_j \to \varphi_i)$. Now φ'_i is obtained from the formulas φ'_j and $\varphi'_k = (\varphi'_j \to \varphi'_i)$ by MP.
6. $\varphi_i = (\psi \to \forall v_j \theta)$ is obtained by universal generalisation from the formula $\varphi_k = (\psi \to \theta)$ and v_j does not occur free in ψ. Now $\varphi'_k = (\psi' \to \theta')$, $\varphi'_i = (\psi' \to \forall v_j \theta')$ and v_j does not occur free in ψ', whence φ'_i is obtained by universal generalisation from φ'_k.

□

Theorem 4.57 (Deduction Lemma) *If $\Sigma \cup \{\psi\} \vdash \varphi$, then $\Sigma \vdash (\psi \to \varphi)$ (and conversely).*

Proof. Let $\varphi_1, \ldots, \varphi_n$ be a deduction of the formula φ from $\Sigma \cup \{\psi\}$.

Claim: $\Sigma \vdash (\psi \to \varphi_i)$ for all $i = 1 \ldots n$.

1. $\varphi_i \in \Sigma \cup \{\psi\}$. Clearly $\Sigma \vdash (\psi \to \varphi_i)$.
2. φ_i tautology. Clearly $\Sigma \vdash (\psi \to \varphi_i)$.
3. φ_i is an identity axiom. Clearly $\Sigma \vdash (\psi \to \varphi_i)$.
4. φ_i is a quantifier axiom. Clearly $\Sigma \vdash (\psi \to \varphi_i)$.
5. φ_i is obtained by MP from φ_j and φ_k, $\varphi_k = (\varphi_j \to \varphi_i)$. By using the tautology $((\psi \to \varphi_j) \to ((\psi \to \varphi_k) \to (\psi \to \varphi_i)))$ we see that $\Sigma \vdash (\psi \to \varphi_i)$.

6. φ_i is obtained by universal generalisation from φ_k, $\varphi_i = (\theta_1 \to \forall v_j \theta_2)$, $\varphi_k = (\theta_1 \to \theta_2)$ and v_j is not free in $\Sigma \cup \{\psi\} \cup \{\theta_1\}$. Now $\Sigma \vdash ((\psi \wedge \theta_1) \to \theta_2)$ and v_j is not free in $\Sigma \cup \{\psi \wedge \theta_1\}$. Therefore $\Sigma \vdash ((\psi \wedge \theta_1) \to \forall v_j \theta_2)$ from which $\Sigma \vdash (\psi \to \varphi_i)$ follows.

□

4.4 Theories

The word "theory" is used in logic simply for a set of sentences. Presumably the set is an *interesting* set of sentences rather than just a random set. However, for the purpose of developing the methodology of mathematical logic we allow theories to be quite arbitrary. Then we apply the methodology to interesting theories.

Definition 4.58 (Theory, model, consistency) *Let L be a vocabulary. An* L-theory *is any set Σ of L-sentences. An L-structure $\mathcal{M}$ is a* model *of the L-theory Σ if $\mathcal{M} \models \Sigma$. The theory Σ is* inconsistent *if there is an L-sentence φ such that $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$, otherwise* consistent*.*

An obvious sufficient condition for consistency is that the theory has a model:

Theorem 4.59 *If Σ has a model, then Σ is consistent.*

Proof. If $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$ then by the Soundness Theorem 4.52, Σ cannot have a model. □

We will show below (Theorem 4.71) that having a model is also a necessary condition for consistency.

An extreme example of a consistent theory is one directly built from a model:

Theorem 4.60 *Suppose L is a vocabulary and $\mathcal{M}$ is an L-structure. Then*

$$\mathrm{Th}(\mathcal{M}) = \{\varphi \mid \varphi \textit{ L-sentence and } \mathcal{M} \models \varphi\}$$

is a consistent L-theory.

Proof. Since trivially $\mathcal{M} \models \mathrm{Th}(\mathcal{M})$, we obtain $\mathcal{M} \models \varphi$, i.e. $\mathrm{Th}(\mathcal{M})$ has a model. □

Theorem 4.60 gives a wealth of consistent theories:

$\mathrm{Th}((\mathbb{N}, +, \cdot, 0, 1))$	the so-called *true arithmetic*
$\mathrm{Th}((\mathbf{R}, +, \cdot, 0, 1))$	the theory of the field of real numbers
$\mathrm{Th}((\mathbb{N}, S, 0))$	the theory of the *successor function*

Lemma 4.61 *If Σ is an inconsistent set of L-sentences, then there is a finite $\Sigma_0 \subseteq \Sigma$ such that Σ_0 is inconsistent.*

Proof. Suppose, that $\Sigma \vdash \varphi \wedge \neg\varphi$. Let $\varphi_1, \ldots, \varphi_n$ be a deduction of $\varphi \wedge \neg\varphi$ from Σ. Let $\Sigma_0 = \{\varphi_i | \varphi_i \in \Sigma\}$. Then $\varphi_1, \ldots, \varphi_n$ is a proof of $\varphi \wedge \neg\varphi$ from Σ_0. $\square$

Lemma 4.62 (Chain Lemma) *If $\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \ldots$ are consistent L-theories, then also $\bigcup_{n=0}^{\infty} \Sigma_n$ is consistent.*

Proof. Let $\Sigma' \subseteq \bigcup_{n=0}^{\infty} \Sigma_n$ finite. Then there is $m \in \mathbb{N}$ such that $\Sigma' \subseteq \Sigma_m$. Since Σ_m is consistent, also Σ' is consistent. $\square$

Lemma 4.63 *Let φ be a sentence. Then $\Sigma \cup \{\varphi\}$ is inconsistent if and only if $\Sigma \vdash \neg\varphi$.*

Proof. . We show first that if $\Sigma \cup \{\varphi\}$ is inconsistent, then $\Sigma \vdash \neg\varphi$. Let ψ be such that $\Sigma \cup \{\varphi\} \vdash (\psi \wedge \neg\psi)$. By the Deduction Lemma $\Sigma \vdash (\varphi \rightarrow (\psi \wedge \neg\psi))$. Note that the sentence $((\varphi \rightarrow (\psi \wedge \neg\psi)) \rightarrow \neg\varphi)$ is a tautology. Thus by MP, $\Sigma \vdash \neg\varphi$.

For the other direction, suppose that $\Sigma \vdash \neg\varphi$. Then $\Sigma \cup \{\varphi\} \vdash \neg\varphi$. The sentence $(\neg\varphi \rightarrow (\varphi \rightarrow (\varphi \wedge \neg\varphi)))$ is a tautology, whence MP gives $\Sigma \cup \{\varphi\} \vdash (\varphi \rightarrow (\varphi \wedge \neg\varphi))$, and further $\Sigma \cup \{\varphi\} \vdash (\varphi \wedge \neg\varphi)$. $\square$

Corollary 4.64 $\Sigma \cup \{\neg\varphi\}$ *is inconsistent if and only if* $\Sigma \vdash \varphi$. $\square$

Definition 4.65 (Completeness) *An L-theory Σ is* complete *if it is consistent and for all L-sentences φ we have*

$$\Sigma \vdash \varphi \text{ or } \Sigma \vdash \neg\varphi.$$

Example 4.66 $\mathrm{Th}(\mathcal{M})$ *is complete.*

Proof. If $\mathcal{M} \models \varphi$, then $\varphi \in \mathrm{Th}(\mathcal{M})$. If $\mathcal{M} \models \neg\varphi$, then $\neg\varphi \in \mathrm{Th}(\mathcal{M})$. $\square$

Theorem 4.67 (Lindenbaum Lemma) *Let L be a countable[8] vocabulary. If Σ is a consistent L-theory, then there is a complete L-theory Σ^* such that $\Sigma \subseteq \Sigma^*$.*

Proof. Since L is countable, we can list all L-sentences as follows: $\varphi_0, \varphi_1, \varphi_2, \ldots$. Define

$$\begin{aligned} \Sigma_0 &= \Sigma \\ \Sigma_{n+1} &= \begin{cases} \Sigma_n \cup \{\varphi_n\} & \text{if } \Sigma_n \vdash \varphi_n \\ \Sigma_n \cup \{\neg\varphi_n\} & \text{otherwise} \end{cases} \\ \Sigma^* &= \bigcup_{n=0}^{\infty} \Sigma_n \end{aligned}$$

[8] With the so-called *Axiom of Choice*—more exactly its equivalent form called *Zorn's Lemma*—the assumption of countability can be avoided.

Claim Σ_n is consistent for all n.

1. $n = 0$: $\Sigma_n = \Sigma$
2. Induction Hypothesis: Σ_n is consistent
3. $\Sigma_{n+1} = \Sigma \cup \{\varphi_n\}$ and $\Sigma_n \vdash \varphi_n$. If Σ_{n+1} were inconsistent then Lemma 4.63 would give $\Sigma_n \vdash \neg\varphi_n$. Since also $\Sigma_n \vdash \varphi_n$, it follows, that Σ_n is inconsistent, contrary to the Induction Hypothesis.
4. $\Sigma_{n+1} = \Sigma_n \cup \{\neg\varphi_n\}$ and $\Sigma_n \nvdash \varphi_n$. If Σ_{n+1} were inconsistent, then Corollary 4.64 would give $\Sigma_n \vdash \varphi_n$, contrary to our assumption. The claim is proved. By Lemma 4.62, Σ^* is consistent.

Claim Σ^* is complete.
If φ_n is an L-sentence, then $\varphi_n \in \Sigma_{n+1}$ or $\neg\varphi_n \in \Sigma_{n+1}$, whence the claim follows. $\square$

Theorem 4.68 *If Σ is a complete L-theory, then for all L-formulas φ and ψ the following holds:*

1. *$\Sigma \vdash \neg\varphi$ if and only if $\Sigma \nvdash \varphi$*
2. *$\Sigma \vdash (\varphi \to \psi)$ iff ($\Sigma \nvdash \varphi$ or $\Sigma \vdash \psi$)*

Proof. As in Theorem 2.23. $\square$

Lemma 4.69 *Let L be a vocabulary and Σ a consistent set of L-sentences. Let L' be a vocabulary such that $L' \setminus L$ contains infinitely many constant symbols. If $n \in \mathbb{N}$ and $\forall v_n\varphi$ is an L'-sentence, then there is a constant symbol $\mathrm{c} \in L' \setminus L$ such that $\Sigma \cup \{(\varphi(\mathrm{c}/v_n) \to \forall v_n\varphi)\}$ is consistent.*

Proof. Choose $\mathrm{c} \in L' \setminus L$ such that c does not occur in φ. If $\Sigma \cup \{(\varphi(\mathrm{c}/v_n) \to \forall v_n\varphi\})$ is inconsistent, then by Lemma 4.63, $\Sigma \vdash \neg(\varphi(\mathrm{c}/v_n) \to \forall v_n\varphi)$, whence it is easy to see that $\Sigma \vdash \varphi(\mathrm{c}/v_n)$ and $\Sigma \vdash \neg\forall v_n\varphi$. By the Lemma on Constants (Lemma 4.56), $\Sigma \vdash \varphi(v_m/v_n)$ for a suitably chosen $m \in \mathbb{N}$. By the universal generalisation Rule, $\Sigma \vdash \forall v_m\varphi(v_m/v_n)$ from which is follows easily that $\Sigma \vdash \forall v_n\varphi$. On the other hand, we just concluded that $\Sigma \vdash \neg\forall v_n\varphi$, contrary to our assumption that Σ is consistent. $\square$

Theorem 4.70 *Let L be a vocabulary and Σ a complete L-theory such that for all L-sentences $\forall v_n\varphi$ there is $c \in L$ such that $\Sigma \vdash (\varphi(\mathrm{c}/v_n) \to \forall v_n\varphi)$. Then there is an L-structure $\mathcal{M}$ such that for all L-sentences φ we have*

$$\mathcal{M} \models \varphi \text{ if and only if } \Sigma \vdash \varphi.$$

Proof. Let M_0 be the set of all L-*constant terms*. (Constant terms are terms that contain no variable symbols). Define in M_0

$$t \sim t' \iff \Sigma \vdash \approx tt'$$
$$[t] = \{t' \in M_0 \mid t \sim t'\}$$

Claim 1 $\sim$ is an equivalence relation in M_0.
Proof. Because of the identity axioms

1. $\Sigma \vdash \approx tt$ whence $t \sim t$.
2. if $t \sim t'$ and $t' \sim t''$, then $\Sigma \vdash \approx tt'$ and $\Sigma \vdash \approx t't''$ and therefore $\Sigma \vdash \approx tt''$ whence $t \sim t''$.
3. If $t \sim t'$, then $\Sigma \vdash \approx tt'$ whence $\Sigma \vdash \approx t't$ and therefore $t' \sim t$.

Claim 2 If $\mathrm{R} \in L$, $\#_L(\mathrm{R}) = n$, $t_1, \ldots, t_n$ are L-terms such that $\mathrm{R}t_1 \ldots t_n \in \Sigma$ and $t_1 \sim t_1', \ldots, t_n \sim t_n'$, then $\mathrm{R}t_1' \ldots t_n' \in \Sigma$, for the identity axioms give

$$\Sigma \vdash ((\approx t_1 t_1' \wedge \ldots \wedge \approx t_n t_n' \wedge \mathrm{R}t_1 \ldots t_n) \rightarrow \mathrm{R}t_1' \ldots t_n').$$

Claim 3 If $\mathrm{f} \in L, \#_L(\mathrm{f}) = n,$ and $t_1, \ldots, t_n, t_1', \ldots, t_n'$ are L-terms such that $t_1 \sim t_1', \ldots, t_n \sim t_n'$ then $\approx \mathrm{f}t_1 \ldots t_n \mathrm{f}t_1' \ldots t_n' \in \Sigma$.
Proof. Follows from the identity axioms.

Now we define an L-structure $\mathcal{M}$ as follows:

$$M = M_0/\sim = \{[t] \mid t \in M_0\}$$

$$\mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) = \{\langle [t_1], \ldots, [t_n] \rangle \mid \Sigma \vdash \mathrm{R}t_1 \ldots t_n\} \text{ when } \mathrm{R} \in L \text{ and } \#_L(\mathrm{R}) = n$$

$$\mathrm{Sat}_{\mathcal{M}}(\mathrm{f})([t_1], \ldots, [t_n]) = [\mathrm{f}t_1 ... t_n] \text{ when } \mathrm{f} \in L \text{ and } \#_L(\mathrm{f}) = n$$

$$\mathrm{Sat}_{\mathcal{M}}(c) = [c] \text{ when } c \in L$$

The Claims 1-3 guarantee that $\mathcal{M}$ is well-defined. We need to prove now $\mathcal{M} \models \Sigma$. This will follow if we prove:

Claim 4 For all L-terms $t_1, ..., t_n$ and L-formulas φ, with the free occurring variables $v_{k_1}, ..., v_{k_n}$, it holds that $t_i^{\mathcal{M}} = [t_i]$ and $\mathcal{M} \models \varphi(t_1/v_{k_1}, ..., t_n/v_{k_n}) \Longleftrightarrow \Sigma \vdash \varphi(t_1/v_{k_1}, ..., t_n/v_{k_n})$.

Proof. By definition $\mathrm{c}^{\mathcal{M}} = [c]$. Moreover, proceeding inductively,

$$\begin{aligned} (\mathrm{f}t_1 \ldots t_n)^{\mathcal{M}} &= \mathrm{Sat}_{\mathcal{M}}(\mathrm{f})(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}}) \\ &= \mathrm{Sat}_{\mathcal{M}}(\mathrm{f})([t_1], \ldots, [t_n]) = [\mathrm{f}t_1 ... t_n] \end{aligned}$$

Thus $t^{\mathcal{M}} = [t]$ for all t.
Now formulas:

1.

$$\begin{aligned}\mathcal{M} \models \approx t_1 t_2 &\iff t_1^{\mathcal{M}} = t_2^{\mathcal{M}}\\ &\iff [t_1] = [t_2]\\ &\iff t_1 \sim t_2\\ &\iff \Sigma \vdash \approx t_1 t_2\end{aligned}$$

2.

$$\begin{aligned}\mathcal{M} \models \mathrm{R}t_1 \dots t_n &\iff \langle t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}\rangle \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R})\\ &\iff \langle [t_1], \dots, [t_n]\rangle \in \mathrm{Sat}_{\mathcal{M}}(\mathrm{R})\\ &\iff \Sigma \vdash \mathrm{R}t_1 ... t_n\end{aligned}$$

3.

$$\begin{aligned}\mathcal{M} \models \neg\varphi &\iff \mathcal{M} \not\models \varphi\\ &\iff \Sigma \nvdash \varphi \text{ Induction Hyp.}\\ &\iff \Sigma \vdash \neg\varphi \text{ Theorem 4.68}\end{aligned}$$

4.

$$\begin{aligned}\mathcal{M} \models (\varphi \to \psi) &\iff \mathcal{M} \not\models \varphi \text{ or } \mathcal{M} \models \psi\\ &\iff \Sigma \nvdash \varphi \text{ or } \Sigma \vdash \psi \text{ Induction Hyp.}\\ &\iff \Sigma \vdash (\varphi \to \psi) \text{ Theorem 4.68}\end{aligned}$$

5. Suppose $\mathcal{M} \models \forall v_n\varphi$. There is c such that $\Sigma \vdash (\varphi(\mathrm{c}/v_n) \to \forall v_n\varphi)$. Clearly $\mathcal{M} \models \varphi(\mathrm{c}/v_n)$, whence by the Induction Hypothesis $\Sigma \vdash \varphi(\mathrm{c}/v_n)$. Now $\Sigma \vdash \forall v_n\varphi$ easily follows. Let conversely $\Sigma \vdash \forall v_n\varphi$. Clearly $\Sigma \vdash \varphi(\mathrm{c}/v_n)$ for all $\mathrm{c} \in L$. We show that $\mathcal{M} \models \forall v_n\varphi$ by going through all elements of the model $\mathcal{M}$. If $t \in M_0$, then by assumption there is $\mathrm{c} \in L$ such that

$$\Sigma \vdash (\neg \approx \mathrm{c}t \to \forall v_0 \neg \approx v_0 t).$$

On the other hand, if $\Sigma \vdash \forall v_0(\neg \approx v_0 t)$, then by the above, $\mathcal{M} \models \forall v_0(\neg \approx v_0 t)$, a contradiction. Thus $\Sigma \nvdash \forall v_0(\neg \approx v_0 t)$ and necessarily $\Sigma \vdash \approx \mathrm{c}t$ i.e. $t^{\mathcal{M}} = \mathrm{c}^{\mathcal{M}}$. Since $\mathcal{M} \models \varphi(\mathrm{c}/v_n)$, we get $\mathcal{M} \models \varphi(t/v_n)$. Thus $\mathcal{M} \models \forall v_n\varphi$.
□

We are ready to prove the famous Gödel[9] Completeness Theorem [8]:

Theorem 4.71 (Gödel's Completeness Theorem) *Suppose L is countable*[10]*, Σ is an L-theory and φ is an L-sentence. Then $\Sigma \vdash \varphi$ if and only if $\Sigma \models \varphi$. In particular, Σ is consistent if and only if Σ has a model.*

[9]Kurt Gödel 1906—1978.
[10]This is an unnecessary assumption but makes the proof easier.

Proof. If $\Sigma \vdash \varphi$ then $\Sigma \models \varphi$ by Theorem 4.52. Assume then $\Sigma \models \varphi$, but $\Sigma \not\vdash \varphi$. We obtain a contradiction by showing that $\Sigma \cup \{\neg\varphi\}$ has a model. Let $L' = L \cup \{\mathrm{c}_n \mid n \in \mathbb{N}\}$, where the constant symbols c_n are new i.e. not in L. We note that Σ, which is a an L-theory, is consistent also as an L'-theory (see Problem 28). By appealing repeatedly to Lemma 4.69 we obtain a consistent Σ_1 such that for all φ and $n \in \mathbb{N}$ there is $c \in L' \setminus L$ such that $(\varphi(\mathrm{c}/v_n) \to \forall v_n \varphi) \in \Sigma_1$. By Lindenbaum's Lemma there is a complete L'-theory $\Sigma^* \supseteq \Sigma_1$. By Theorem 4.70 Σ^* has a model $\mathcal{M}^*$. Let $\mathcal{M}$ be the reduct (see Definition 3.8) of the L'-structure $\mathcal{M}^*$ to the vocabulary L. Then $\mathcal{M} \models \Sigma$.
□

From the above proof we obtain the following Löwenheim[11]-Skolem[12] Theorem [12, 17]:

Theorem 4.72 (Löwenheim-Skolem Theorem) *If Σ is an L-theory which has a model, and L is countable, then Σ has a countable model.*

Theorem 4.71 has sweeping consequences:

- We can forget about deductions in predicate logic—it is enough to consider models and logical consequence defined by means of models.
- We can get new interesting models by simply constructing consistent theories.

An example of the use of interesting models arising from consistent theories is *non-standrad analysis.*

Theorem 4.73 (Compactness Theorem) *If Σ is set of L-formulas such that every finite $\Sigma_0 \subseteq \Sigma$ has a model, then Σ has a model.*

Proof. If Σ has no models, then Σ is by Theorem 4.71 inconsistent. By Lemma 4.61, Σ has a finite inconsistent subset Σ_0. But then Σ_0 has no models, contrary to our assumption. □

Example 4.74 *Let L be a countable vocabulary and Σ an L-theory such that if $\mathcal{M} \models \Sigma$, then M is finite. Then there is $n \in \mathbb{N}$ such that if $\mathcal{M} \models \Sigma$, then M has at $\leq n$ elements. Why? Suppose, that for every $n \in \mathbb{N}$ there is $\mathcal{M}_n \models \Sigma$ such that M_n has $> n$ elements. Let*

$$\varphi_n = \forall v_1 \ldots \forall v_n \exists v_{n+1}(\neg \approx v_{n+1}v_1 \wedge \ldots \wedge \neg \approx v_{n+1}v_n).$$

Thus $\mathcal{M}_n \models \Sigma \cup \{\varphi_m \mid m \leq n\}$. Let $\Sigma' = \Sigma \cup \{\varphi_m \mid m \in \mathbb{N}\}$. Now every finite subset of Σ' has a model. By the Compactness Theorem 4.73 the theory Σ' has a model $\mathcal{M}$. According to our assumption M is finite. On the other hand $\mathcal{M} \models \varphi_n$ for all $n \in \mathbb{N}$. This contradiction shows that the claim is true. □

[11]Leopold Löwenheim 1878—1957.
[12]Thoralf Skolem 1887—1963.

Example 4.75 *Let* $L = \{\oplus, \otimes, <, 0, 1\}$ *and* $\mathfrak{R} = \langle \mathbb{R}, \mathrm{Sat}_{\mathfrak{R}} \rangle$*, where* $\mathrm{Sat}_{\mathfrak{R}}(<) = \{\langle x, y \rangle \mid x < y\}$*,* $\mathrm{Sat}_{\mathfrak{R}}(\otimes)(x, y) = x \cdot y$*,* $\mathrm{Sat}_{\mathfrak{R}}(\oplus)(x, y) = x + y$*, and* $\mathrm{Sat}_{\mathfrak{R}}(0) = 0, \mathrm{Sat}_{\mathfrak{R}}(1) = 1$*. Let* $\Sigma = \mathrm{Th}(\mathfrak{R})$*.* Σ *has a model and* L *is countable, whence* Σ *has a countable model. In fact, the ordered field of* algebraic real numbers[13] *is a countable model of* Σ*.*

Theorem 4.76 *Let* L *be countable. An* L*-theory* Σ *is complete and closed under deduction (i.e. if* φ *is an* L*-sentence and* $\Sigma \vdash \varphi$*, then* $\varphi \in \Sigma$*) if and only if there is an* L*-structure* $\mathcal{M}$ *such that* $\Sigma = \mathrm{Th}(\mathcal{M})$*.*

Proof. Suppose, that Σ is complete and closed under deduction. Complete theories are assumed to be consistent, so the Completeness Theorem 4.71 gives Σ a model $\mathcal{M}$. If $\varphi \in \Sigma$, then $\varphi \in \mathrm{Th}(\mathcal{M})$. If on the other hand $\varphi \in \mathrm{Th}(\mathcal{M})$ and $\varphi \notin \Sigma$, then $\Sigma \nvdash \varphi$, whence $\Sigma \vdash \neg\varphi$ and therefore $\neg\varphi \in \Sigma$, whence $\neg\varphi \in \mathrm{Th}(\mathcal{M})$, a contradiction. Hence $\Sigma = \mathrm{Th}(\mathcal{M})$.

Conversely, let $\Sigma = \mathrm{Th}(\mathcal{M})$. Obviously Σ is closed under deduction. If φ is an L-sentence, then $\varphi \in \mathrm{Th}(\mathcal{M})$ or $\neg\varphi \in \mathrm{Th}(\mathcal{M})$, whence $\Sigma \vdash \varphi$ or $\Sigma \vdash \neg\varphi$. We have proved that Σ is complete. $\square$

Theorem 4.77 *A consistent* L*-theory* Σ *is complete if and only if all of its models are elementarily equivalent.*

Proof. Let Σ be complete and $\mathcal{M} \models \Sigma$, $\mathcal{M}' \models \Sigma$. If $\mathcal{M} \not\equiv \mathcal{M}'$, then there is an L-sentence φ such that $\mathcal{M} \models \varphi \not\Leftrightarrow \mathcal{M}' \models \varphi$. If $\Sigma \vdash \varphi$, then $\mathcal{M} \models \varphi$ and $\mathcal{M}' \models \varphi$. Otherwise $\Sigma \vdash \neg\varphi$, whence $\mathcal{M} \not\models \varphi$ and $\mathcal{M}' \not\models \varphi$. This contradiction shows that $\mathcal{M} \equiv \mathcal{M}'$.

Suppose Σ is incomplete. Thus there is an L-sentence φ such that $\Sigma \nvdash \varphi$ and $\Sigma \nvdash \neg\varphi$. By the Completeness Theorem 4.71, $\Sigma \not\models \varphi$ and $\Sigma \not\models \neg\varphi$. Thus there are $\mathcal{M} \models \Sigma \cup \{\neg\varphi\}$ and $\mathcal{M}' \models \Sigma \cup \{\varphi\}$. Hence $\mathcal{M} \not\equiv \mathcal{M}'$. $\square$

Definition 4.78 (Categoricity) *An* L*-theory is* $\aleph_0$-categorical[14]*, if its countably infinite models are all isomorphic.*

Theorem 4.79 (Łoś[15]-Vaught[16] Theorem) *Let* L *be countable and* Σ *a consistent* $\aleph_0$*-categorical* L*-theory without finite models. Then* Σ *is complete.*

Proof. Let $\mathcal{M} \models \Sigma$ and $\mathcal{M}' \models \Sigma$ (we use Theorem 4.77). Let $\Sigma_1 = \mathrm{Th}(\mathcal{M})$ and $\Sigma_2 = \mathrm{Th}(\mathcal{M}')$. By Theorem 4.72, the theory Σ_1 has a countably infinite model $\mathcal{M}_1$, and the theory Σ_2 has, likewise, a countably infinite model $\mathcal{M}_2$. By $\aleph_0$-categoricity, $\mathcal{M}_1 \cong \mathcal{M}_2$. By Corollary 4.28 $\mathcal{M}_1 \equiv \mathcal{M}_2$. Now $\mathcal{M} \equiv \mathcal{M}_1 \equiv \mathcal{M}_2 \equiv \mathcal{M}'$, whence $\mathcal{M} \equiv \mathcal{M}'$. $\square$

---

[13] A real number is *algebraic* is it is the root of a non-trivial polynomial with rational coefficients.

[14] $\aleph_0$ is read "aleph zero".

Example 4.80 *Let $L = \{\mathrm{R}\}$, where $\#_L(\mathrm{R}) = 1$. Let $\mathcal{M} = \langle \mathbb{R}, \mathrm{Sat}_{\mathcal{M}} \rangle$ and $\mathcal{M}' = \langle \mathbb{Q}, \mathrm{Sat}_{\mathcal{M}'} \rangle$, where $\mathrm{Sat}_{\mathcal{M}}(\mathrm{R}) = \mathbb{Q}$ and $\mathrm{Sat}_{\mathcal{M}'}(\mathrm{R}) = \mathbb{N}$. Clearly $\mathcal{M}_1 \not\cong \mathcal{M}_2$, since $\mathbb{R}$ is uncountable. But $\mathcal{M} \equiv \mathcal{M}'$, for both models are models of the $\aleph_0$-categorical theory Σ, where Σ consists of*

$$\begin{aligned}\forall v_0 \ldots \forall v_n \exists v_{n+1} \exists v_{n+2} [\neg \approx v_{n+1} v_0 \wedge \ldots \wedge \neg \approx v_{n+1} v_n \wedge \\ \neg \approx v_{n+2} v_0 \wedge \ldots \wedge \neg \approx v_{n+2} v_n \wedge \\ \mathrm{R} v_{n+1} \wedge \neg \mathrm{R} v_{n+2}],\end{aligned}$$

where $n \in \mathbb{N}$. Σ is $\aleph_0$-categorical, because in its countable models R and $-R$ are both countably infinite.

Dense linear order without end points DLO consists of the following sentences in the vocabulary $L = \{<\}$, $\#_L(<) = 2$: (for the sake of clarity we write $t < t'$ for $< tt'$):

$$\begin{aligned}&\forall v_0 \neg (v_0 < v_0) \\ &\forall v_0 \forall v_1 \forall v_2 ((v_0 < v_1 \wedge v_1 < v_2) \rightarrow v_0 < v_2) \\ &\forall v_0 \forall v_1 (v_0 < v_1 \vee \approx v_0 v_1 \vee v_1 < v_0) \\ &\forall v_0 (\exists v_1 (v_0 < v_1) \wedge \exists v_1 (v_1 < v_0)) \\ &\forall v_0 \forall v_1 \exists v_2 (v_0 < v_1 \rightarrow (v_0 < v_2 \wedge v_2 < v_1)\end{aligned}$$

Theorem 4.81 *The theory DLO is $\aleph_0$-categorical.*

Proof. Let $\mathcal{M}$ and $\mathcal{M}'$ be countable models of DLO. Let $M = \{d_n | n \in \mathbb{N}\}$ and $M' = \{d'_n | n \in \mathbb{N}\}$. Let $f_0 = \{\langle d_0, d'_0 \rangle\}$. Suppose, that

$$f_n = \{\langle x_0, y_0 \rangle, \ldots, \langle x_{2n}, y_{2n} \rangle\}$$

has been defined and

$$x_0 < x_1 < \ldots < x_{2n},\ y_0 <' y_1 <' \ldots <' y_{2n}$$

where $<$ refers to the relation $\mathrm{Sat}_{\mathcal{M}}(<)$ and $<'$ to the relation $\mathrm{Sat}_{\mathcal{M}'}(<)$. Let $d_m \in M \setminus \{x_0, \ldots, x_{2n}\}$ be such that m is minimal. Now either $d_m < x_0$ or $x_i < d_m < x_{i+1}$ for some $i < 2n$ or $x_{2n} < d_m$. In each case we can choose $y \in M' \setminus \{y_0, \ldots, y_{2n}\}$ such that respectively $y < y_0$ or $y_i < y < y_{i+1}$ or $y_{2n} < y$. We will map the element d_m to the element y. Now we search respectively for an element in M' and choose a pre-image x for it. Let $d'_k \in M' \setminus \{y_0, \ldots, y_{2n}, y\}$ be such that k is minimal. Choose $x \in M \setminus \{x_0, \ldots, x_{2n}, d_m\}$ as y above. Finally, let

$$f_{n+1} = f_n \cup \{\langle d_m, y \rangle, \langle x, d'_k \rangle\}.$$

Let

$$f = \bigcup_{n=0}^{\infty} f_n.$$

Now

$$d_n \in dom(f_n) \subseteq dom(f)$$
$$d'_n \in ran(f_n) \subseteq ran(f)$$

Clearly, $f : M \to M'$ is an isomorphism. □

Example 4.82 *The models* $\mathcal{M} = \langle \mathbf{R}, \mathrm{Sat}_{\mathcal{M}}(<)\rangle$ *and* $\mathcal{M}' = \langle \mathbf{Q}, \mathrm{Sat}_{\mathcal{M}}(<)\rangle$,

$$\mathrm{Sat}_{\mathcal{M}}(<) = \{\langle x, y\rangle \in \mathbf{R}^2 | x < y\}$$
$$\mathrm{Sat}_{\mathcal{M}}(<) = \{\langle x, y\rangle \in \mathbf{Q}^2 | x < y\}$$

of the theory DLO are by Theorem 4.81 and Theorem 4.79 elementarily equivalent: $\mathcal{M} \equiv \mathcal{M}'$.

4.5 Problems

1. Show that the sentence $(\forall v_0 \exists v_1(\mathrm{R}v_0v_1 \wedge \approx v_0v_1) \to \forall v_0 \mathrm{R}v_0v_0)$ is valid.

2. Decide whether $\models (\forall v_0 \exists v_1 \mathrm{R}v_0v_1 \to \exists v_1 \mathrm{R}v_1v_1)$?

3. Decide whether $\exists v_0 \forall v_1(\mathrm{R}v_0v_1 \to \mathrm{R}'v_0v_1) \models \exists v_0(\forall v_1 \mathrm{R}v_0v_1 \to \forall v_1 \mathrm{R}'v_0v_1)$?

4. Let φ be the formula $\forall v_0(\neg \approx v_0 \mathrm{f}v_0 \wedge \approx v_0 \mathrm{ff}v_0)$. Describe the models of φ and show that φ has infinitely many non-isomorphic models.

5. Prove the two claims of Example 4.9.

6. Prove the two claims of Example 4.20.

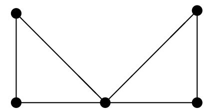
7. Let $\mathcal{M}$ and $\mathcal{M}'$ be L-structures and $\pi : \mathcal{M} \cong \mathcal{M}'$. Let $s : \mathbb{N} \to M$ and $s' : \mathbb{N} \to M'$ such that $s'(n) = \pi(s(n))$ for all $n \in \mathbb{N}$. Prove that $t^{\mathcal{M}'}\langle s'\rangle = \pi(t^{\mathcal{M}}\langle s\rangle)$ for all L-terms t.

8. Prove Theorem 4.25.

9. Let $\mathcal{M} = (\{0, 1, 2, 3, 4\}, P, Q)$, where $P = \{0, 1, 2\}$ and $Q = \{2, 3, 4\}$. What are the definable subsets of the structure $\mathcal{M}$? In each case give a formula that defines the subset or show that the subset is undefinable.

10. Prove that the class of subsets definable in a given $\mathcal{M}$ contains the empty set, the set M and is closed under union, intersection and complement (i.e. is a *Boolean algebra*).

11. List the definable subsets of the following graph. In each case give a formula that defines the subset or show that the subset is undefinable.



12. Show that every element of $\mathcal{Q} = (\mathbf{Q}, +, \cdot, 0, 1)$ is definable, but in the structure $(\mathbf{Q}, <)$ *no* element is definable.

13. Let $M = \{n \in \mathbb{N} : n < 10\}$ and $f : M \to M$ such that $f(x) = 5$ for all $x \in M$. What are the definable subsets of the structure (M, f)? In each case give a formula that defines the subset or show that the subset is undefinable.

14. Let $M = \{(n, m) \in \mathbb{N}^2 : m \leq n < 57\}$ and $E \subseteq M^2$ such that $((n, m), (k, l)) \in E$ if and only if $n = k$. What are the definable subsets of the structure (M, E)? In each case give a formula that defines the subset or show that the subset is undefinable.

15. Let $\mathbb{Q}$ be the set of rational numbers, $<$ the usual order of rational numbers, and $S : \mathbb{Q} \to \mathbb{Q}$ such that for all $x \in \mathbb{Q}$, $S(x) = x + 1$. Is

    (a) the element -5,

    (b) the element $1/3$

    definable in $(\mathbb{Q}, S, 0, <)$?

16. Let $\varphi = \forall v_0(\exists v_1 \mathrm{R} v_1 v_2 \to \forall v_2(\mathrm{R} v_1 v_2 \to \mathrm{R} v_0 v_2))$. Which of the following are true:

    (a) $\mathrm{FVF}(\mathrm{f} v_2 v_1, v_0, \varphi)$,

    (b) $\mathrm{FVF}(\mathrm{f} v_0 v_0, v_2, \varphi)$,

    (c) $\mathrm{FVF}(\mathrm{f} v_0 v_1, v_1, \varphi)$?

17. Prove that for all t, v_n and φ there exists φ^* such that $\models \varphi \leftrightarrow \varphi^*$ and $\mathrm{FVF}(t, v_n, \varphi^*)$.

18. Prove Theorem 4.37 part 1.

19. Prove Theorem 4.37 part 2.

20. Prove Lemma 4.46.

21. Give the deduction $\vdash (\forall v_0(\varphi \vee \psi) \to (\forall v_0 \varphi \vee \psi))$, when v_0 does not occur free in ψ.

22. Give the deduction $\{\forall v_0(\varphi \to \psi)\} \vdash (\exists v_0 \varphi \to \exists v_0 \psi)$.

23. Give the deduction $\{\forall v_0 \forall v_1 \approx v_0 v_1\} \vdash \exists v_0 \mathrm{P} v_0 \to \forall v_1 \mathrm{P} v_1$.

24. Give the deduction $\{\mathrm{R} c\} \vdash \forall v_0(\approx v_0 c \to \mathrm{R} v_0)$.

25. Give the deduction $\vdash (\forall v_0 \forall v_1(\varphi \wedge \psi) \to \forall v_0 \exists v_1 \varphi)$.

26. Let T be an L-theory, φ an L-formula and $c \notin L$. Show that if $T \vdash \varphi(\mathrm{c}/v_0)$ then $T \vdash \forall v_0 \varphi$.

27. Let T be an L-theory. Show that the following are equivalent:

    (i) For each L-sentence $\forall v_i \varphi$ there is a constant $c \in L$ for which $T \vdash \varphi(\mathrm{c}/v_i) \to \forall v_i \varphi$,

    (ii) For each L-sentence $\exists v_i \varphi$ there is a constant $c \in L$ for which $T \vdash \exists v_i \varphi \to \varphi(\mathrm{c}/v_i)$.

28. Suppose Σ is an L-theory. Let $L' = L \cup \{\mathrm{c}_n \mid n \in \mathbb{N}\}$, where the constant symbols c_n are new, i.e. not in L. Show (without using Theorem 4.71) that Σ is consistent also as an L'-theory. (Hint: If a contradiction were provable from Σ as an L'-theory, the Lemma on Constants 4.56 could used repeatedly to replace the new constants c_i by new variables.)

29. Let T be an L-theory such that in every L-structure some $\varphi \in T$ is true. Prove that there exist $n \in \mathbb{N}$ and $\varphi_0, ..., \varphi_n \in T$ such that $\vdash \varphi_0 \vee ... \vee \varphi_n$.

30. Let $L = \{\mathrm{c}_i \mid i \in \mathbb{N}\}$ and let T be an L-theory such that for each L-model $\mathcal{M}$ of T and every $a \in M$ there is $i \in \mathbb{N}$ such that $\mathrm{c}_i^{\mathcal{M}} = a$. Show that there is $n \in \mathbb{N}$ such that $T \vdash \bigvee_{k<m\leq n} \mathrm{c}_k = \mathrm{c}_m$, where $\bigvee_{k<m\leq n} \mathrm{c}_k = \mathrm{c}_m$ means the disjunction of the formulas $\mathrm{c}_k = \mathrm{c}_m$ for $k < m \leq n$.

31. Let $\mathcal{M} = (\{0, 1, 2\}, \{0\})$ be a $\{P\}$-structure. Find a $\{P\}$-sentence φ such that $\mathcal{M} \models \varphi$ and $\{\varphi\}$ is a complete theory.

32. Consider the $\{\mathrm{f}\}$-theory $T = \{\forall v_0(\neg \approx v_0 \mathrm{f} v_0 \wedge \approx v_0 \mathrm{ff} v_0)\}$. Describe the countably infinite models of T and show that T is not complete.

33. Suppose Σ is an L-theory and $L \subseteq L'$. Show that Σ is consistent also as an L'-theory. You may use Theorem 4.71.

34. Show that $\mathrm{Th}((\mathbb{N}, +, \cdot, 0, 1, <))$ is not $\aleph_0$-categorical.

35. Suppose that every finite subset of a theory T has a model with at least three elements. Prove that T itself has a model with at least three elements.

36. Let $\mathcal{M} = (\{0, 1\}, \{(0, 0), (0, 1), (1, 1)\})$ be a structure for the vocabulary $L = \{R\}$, $\#(R) = 2$. Find an L-sentence φ such that $\mathcal{M} \models \varphi$ and $\{\varphi\}$ is a complete theory.

37. Let L be a vocabulary and $\mathrm{c}_n \in L$ for $n \in \mathbb{N}$. Let T be an L-theory. Suppose that T has an infinite model $\mathcal{M}$. Prove that T has a model $\mathcal{N}$ with an element $a \in N$ such that $a \neq \mathrm{c}_n^{\mathcal{N}}$ for all $n \in \mathbb{N}$.

38. Let T_1 and T_2 theories such that $T_1 \cup T_2$ is inconsistent. Prove that there exists $\varphi_1, \ldots, \varphi_n \in T_1$ and $\psi_1, \ldots, \psi_n \in T_2$ such that

$$\varphi_1 \wedge \ldots \wedge \varphi_n \vdash \neg\psi_1 \vee \ldots \vee \neg\psi_n.$$

39. Suppose $L = \{P_1, \ldots, P_n\}$, where each P_i is 1-place. Denote $P_i^1 = P_i(v_0)$ and $P_i^1 = \neg P_i(v_0)$. If $\epsilon : \{1, \ldots, n\} \to \{0, 1\}$ then let $C_\epsilon = P_1^\epsilon \wedge \ldots \wedge P_n^{\epsilon(n)}$. Prove that finite L-structures $\mathcal{M}$ and $\mathcal{N}$ are isomorphic if and only if the sets $\{a \in M : \mathcal{M} \models_{s(a/0)} C_\epsilon$ for some $s\}$ and $\{a \in N : \mathcal{N} \models_{s(a/0)} C_\epsilon$ for some $s\}$ have the same number of elements for all $\epsilon : \{1, \ldots, n\} \to \{0, 1\}$.

Chapter 5

Incompleteness of number theory

By *number theory* we mean here arithmetic properties of the natural numbers $0, 1, 2, \ldots$. Arithmetic pertains to addition and multiplication. A surprisingly large portion of mathematics can be reduced to number theory. For example $\sqrt{2} > 1.414$ can be written in number theory as $\exists x(2 \cdot 10^6 = 1414^2 + x + 1)$. Statements about common transcendental functions such as $\sin(x)$, $\cos(x)$, $\ln(x)$, etc can be translated into number theory by means of Taylor series. It is an interesting fact that also the central concepts of logic, such as provability, consistency, validity, etc translate to the language of number theory. This is the topic of this section. After that it is possible to prove essential limitations on the scope of number theory.

Definition 5.1 (Number theory) *The vocabulary of* number theory *is*

$$L = \{\oplus, \otimes, 0, 1\}, \ \#_L(\oplus) = \#_L(\otimes) = 2.$$

Peano axioms *for number theory are*

(P1) $\forall v_0 \neg \approx \oplus v_0 1 0$

(P2) $\forall v_0 \forall v_1 (\approx \oplus v_0 1 \oplus v_1 1 \rightarrow \approx v_0 v_1)$

(P3) $\forall v_0 \approx \oplus v_0 0 v_0$

(P4) $\forall v_0 \forall v_1 \approx \oplus v_0 \oplus v_1 1 \oplus \oplus v_0 v_1 1$

(P5) $\forall v_0 \approx \otimes v_0 0 0$

(P6) $\forall v_0 \forall v_1 \approx \otimes v_0 \oplus v_1 1 \oplus \otimes v_0 v_1 v_0$

(P7) $\forall v_{n_0} \cdots \forall v_{n_k}((\varphi(0/v_0) \wedge \forall v_0(\varphi \rightarrow \varphi(\oplus v_0 1/v_0))) \rightarrow \forall v_0 \varphi)$ *(*Induction Schema*)*

where φ runs through all L-formulas and $v_{n_0} \ldots v_{n_k}$ are the variables other than v_0 that occur free in φ. We use P to denote the infinite set of Peano axioms. The standard model *of number theory is $\mathcal{N} = \langle \mathbb{N}, Sat_{\mathcal{N}} \rangle$, where*

$$Sat_{\mathcal{N}}(\oplus)(x, y) = x + y, \ Sat_{\mathcal{N}}(\otimes)(x, y) = x \cdot y$$

$$Sat_{\mathcal{N}}(0) = 0,\ \ Sat_{\mathcal{N}}(1) = 1$$

Theorem 5.2 $\mathcal{N} \models P$ *and* P *is therefore consistent.*

Proof. Only the Induction Schema requires consideration. Let φ be an L-formula with $v_0, v_{n_0}, \cdots, v_{n_k}$ free. Let $s : \mathbb{N} \to \mathbb{N}$. Let $X = \{i \in \mathbb{N} \mid \mathcal{N} \models_{s(i/0)} \varphi\}$. Suppose $\mathcal{N} \models_s (\varphi(0/v_0) \wedge \forall v_0(\varphi \to \varphi(\oplus v_0 1/v_0)))$. Thus $0 \in X$ and $i+1 \in X$ whenever $i \in X$. The ordinary induction principle of natural numbers implies that $X = \mathbb{N}$. Thus $\mathcal{N} \models_s \forall v_0 \varphi$. □

Note: We prove the above induction by means of induction. Isn't this blatantly circular? Yes, and therefore the above theorem is not particularly insightful. One may ask whether the consistency of P can be proved differently ("finitistically"), without assuming the existence of the model $\mathcal{N}$. *Kurt Gödel* proved in 1931 that P alone is not enough for proving the consistency of P (see Theorem 5.33). Thus something stronger than P has to be used. *Gerhard Gentzen* proved in 1943 that the consistency of P can be proved in an extension of P which has a stronger from of the Induction Schema, so-called transfinite induction up to the ordinal ϵ_0.

The important theorem below was proved by Thoralf Skolem[1] in 1933:

Theorem 5.3 (Skolem) *The theory* P *has models, that are not isomorphic to* $\mathcal{N}$.

Proof. Models of P that are not isomorphic to $\mathcal{N}$ are called *non-standard models*. Let $L' = \{\oplus,\ \otimes,\ 0,\ 1,\ c\}$, where c is a new constant symbol. Let Σ consist of P as well as

$$\neg \approx c0\ ,\ \neg \approx c1\ ,\ \neg \approx c \oplus 11, \neg \approx c \oplus \oplus 111\ ,\ \ldots$$

i.e. if we denote $\underline{n+1} = \oplus \underline{n} 1$ then $\Sigma = P \cup \{\neg \approx c\underline{n} \mid n \in \mathbb{N}\}$. If $\Sigma_0 \subseteq \Sigma$ is finite, then there is $k \in \mathbb{N}$ such that $\Sigma_0 \subseteq P \cup \{\neg \approx c\underline{n} \mid n \in \mathbb{N},\ n < k\}$. Let $\mathcal{N}'$ be the L'-structure $\langle \mathbb{N}, \mathrm{Sat}_{\mathcal{M}} \rangle$ which is otherwise as $\mathcal{N}$ (i.e. $\mathcal{N}' \restriction L = \mathcal{N}$) except $\mathrm{Sat}_{\mathcal{N}'}(c) = k$. Then $\mathcal{N}' \models \Sigma_0$. By the Compactness Theorem Σ has a model $\mathcal{M}' = \langle M', \mathrm{Sat}_{L'} \rangle$. In particular, if $\mathcal{M} = \mathcal{M}' \restriction L$, then $\mathcal{M} \models P$.

Claim $\mathcal{M} \ncong \mathcal{N}$

Proof. Suppose $\pi :\ \mathcal{M} \cong \mathcal{N}$. Let $m = \pi(\mathrm{Sat}_{\mathcal{M}'}(c))$. If $n \in \mathbb{N}$, then $\mathcal{M}' \models \neg \approx c\underline{n}$ whence, as π is an isomorphism, $m \neq \mathrm{Sat}_{\mathcal{N}}(\underline{n})$. But $\mathrm{Sat}_{\mathcal{N}}(\underline{n}) = n$ whence choosing $n = m$ leads to a contradiction. □

[1] Skolem's proof [18] was different from the modern proof we present here. The modern simple proof is based on the Compactness Theorem (Theorem 4.73), a consequence of Gödel's Completeness Theorem (Theorem 4.71). As Robert Vaught writes in [9, page 377], it is extraordinary that neither Skolem nor Gödel observed at the time that the existence of non-standrad models of P follows readily from Gödel's results of 1930-1931. Gödel himself points out that the existence follows from his Incompleteness Theorem (Theorem 5.32).

Theorem 5.4 $P \vdash \forall v_0 \approx \oplus 0 v_0 v_0$.

Proof. Thanks to the Completeness Theorem 4.71, it suffices to show $P \vDash \forall v_0 \approx \oplus 0 v_0 v_0$. To this end, let $\mathcal{M} = \langle M, \mathrm{Sat}_{\mathcal{M}} \rangle \vDash P$ and $s : \mathbb{N} \to M$. Let us denote $\mathrm{Sat}_{\mathcal{M}}(\oplus) = +'$, $\mathrm{Sat}_{\mathcal{M}}(\otimes) = \cdot'$, $\mathrm{Sat}_{\mathcal{M}}(0) = 0'$ and $\mathrm{Sat}_{\mathcal{M}}(1) = 1'$. We apply the Induction Schema to φ, which is the formula $\approx \oplus 0 v_0 v_0$. $\varphi(0/v_0)$ is the formula $\approx \oplus 000$. $\mathcal{M} \vDash_s \varphi(0/v_0)$ follows from Axiom (P3). Let then $a \in M$ and $\mathcal{M} \vDash_{s(a/0)} \varphi$. Thus $0' +' a = a$. $\varphi(\oplus v_0 1/v_0)$ is the formula $\approx \oplus 0 \oplus v_0 1 \oplus v_0 1$ whence $\mathcal{M} \vDash_{s(a/0)} \varphi(\oplus v_0 1/v_0)$ if $0' +' (a +' 1') = a +' 1'$. As $\mathcal{M} \vDash$ (P4), we have $0' +' (a +' 1') = (0' +' a) +' 1'$. By assumption, $0' +' a) = a$, whence $0' +' (a +' 1') = a +' 1'$. Since a was arbitrary, $\mathcal{M} \vDash \forall v_0[\varphi \to \varphi(\oplus v_0 1/v_0)]$ follows. Since $\mathcal{M} \vDash$ (P7), $\mathcal{M} \vDash \forall v_0 \varphi$ follows. □

Induction is a general method in number theory. Since P incorporates induction, at least in its simplest form, it is not at all easy to find sentences φ such that $\mathcal{N} \vDash \varphi$ but $P \nvDash \varphi$. Such φ however exist. Researchers try to find examples of such φ as close to mathematical practice as possible but so far all examples seem to arise somehow from logic (See, however [1, Ch. D8].) Kurt Gödel proved that the sentence φ, which says "P is consistent" has this property. We prove the slightly weaker claim that: $\{\varphi \mid P \vdash \varphi\}$ is an incomplete theory. To this end we now start an investigation of the definability of number theoretic functions.

5.1 Primitive recursive functions

Primitive recursive functions are functions, the value of which for any given arguments can be mechanically computed in finite time by means of a recurrence equation. Let us consider addition as an example:

$$\begin{aligned} x + 0 &= x \\ x + (y+1) &= (x+y) + 1. \end{aligned}$$

Or multiplication

$$\begin{aligned} x \cdot 0 &= 0 \\ x \cdot (y+1) &= (x \cdot y) + x. \end{aligned}$$

The general form of this kind of definition is:

$$\begin{aligned} f(x, 0) &= g(x) \\ f(x, y+1) &= h(y, f(x,y), x). \end{aligned}$$

Now we can compute $f(5,3)$ in a "recursive" way:

$$\begin{aligned} f(5,3) &= f(5,2+1) \\ &= h(2,f(5,2),5) \\ &= h(2,f(5,1+1),5) \\ &= h(2,h(1,f(5,1),5),5) \\ &= h(2,h(1,f(5,0+1),5),5) \\ &= h(2,h(1,h(0,f(5,0),5),5),5) \\ &= h(2,h(1,h(0,g(5),5),5),5) \end{aligned}$$

If for example $g(x) = x^2$ and $h(y,z,x) = y + z + x$, then

$$f(5,3) = h(2,h(1,h(0,g(5),5),5),5) = 2+1+0+25+5+5+5 = 43.$$

Recursively defined functions are examples of functions that are computable by a computer. On the other hand such functions can be defined in number theory.

Definition 5.5 (Primitive recursiveness) Primitive recursive *(p.r.) functions are defined as follows:*

(PR1) The zero function $Z(n) = 0$ is primitive recursive.

(PR2) The successor function $S(n) = n + 1$ is primitive recursive.

(PR3) The projection function $Pr^n_i(x_1, \ldots, x_n) = x_i$ is primitive recursive, when $1 \le i \le n$.

(PR4) If $f : \mathbb{N}^n \to \mathbb{N}$ and $g_i : \mathbb{N}^m \to \mathbb{N}$ are primitive recursive, when $1 \le i \le n$, then the composition

$$h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))$$

is primitive recursive.

(PR5) If $f : \mathbb{N}^n \to \mathbb{N}$ and $g : \mathbb{N}^{n+2} \to \mathbb{N}$ are primitive recursive, then the function obtained from them by recursion

$$\begin{cases} h(0, x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \\ h(y+1, x_1, \ldots, x_n) = g(y, h(y, x_1, \ldots, x_n), x_1, \ldots, x_n) \end{cases}$$

is primitive recursive. In the special case $n = 0$ the definition shrinks to

$$\begin{cases} h(0) = a \text{ (constant)} \\ h(y+1) = g(y, h(y)) \end{cases}$$

Example 5.6 1. *The* Identity function $id(x) = x$ *is primitive recursive, for* $id(x) = Pr^1_1(x)$

2. *If $f : \mathbb{N}^2 \to \mathbb{N}$ is primitive recursive, then $g(x,y) = f(y,x)$ is primitive recursive, for $g(x,y) = f(Pr_2^2(x,y),\ Pr_1^2(x,y))$.*

3. Addition $a(y,x) = y + x$ *is primitive recursive, for*

$$\begin{cases} a(0,x) = x = id(x) \\ a(y+1,x) = y + x + 1 = S(Pr_2^3(y, a(y,x), x)). \end{cases}$$

4. Multiplication $b(y,x) = y \cdot x$ *is primitive recursive, for*

$$\begin{cases} b(0,x) = 0 = Z(x) \\ b(y+1,x) = b(y,x) + x = a(Pr_2^3(y, b(y,x), x), Pr_3^3(y, b(y,x), x)). \end{cases}$$

5. Exponential function $c(y,x) = x^y$ *is primitive recursive. (Problem 1)*

6. Constant function $C_k(x) = k$ *is primitive recursive. (Problem 1)*

7. Bounded subtraction

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geq y \\ 0 & \text{if } x < y \end{cases}$$

is primitive recursive. (Problem 3)

Definition 5.7 (Primitive recursive relation) *A relation $R \subseteq \mathbb{N}^n$ is primitive recursive, if the characteristic function*

$$f_R(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } \langle x_1, \ldots, x_n \rangle \in R \\ 0, & \text{if } \langle x_1, \ldots, x_n \rangle \notin R \end{cases}$$

is primitive recursive.

Example 5.8 1. *The relation $R = \{0\}$ (i.e. the relation $x = 0$) is primitive recursive, for $f_R(x) = 1 \dot{-} x$.*

2. *The relation $R = \{x \in \mathbb{N} \mid x > 0\}$ is primitive recursive, as $f_R(x) = 1 \dot{-} (1 \dot{-} x)$. Denote $sg(x) = f_R(x)$.*

3. *If $R \subseteq \mathbb{N}^n$ and $S \subseteq \mathbb{N}^n$ are primitive recursive, then $\mathbb{N}^n \setminus R$, $R \cap S$ and $R \cup S$ are primitive recursive, since*

$$f_{\mathbb{N}^n \setminus R}(x_1, \ldots, x_n) = 1 \dot{-} f_R(x_1, \ldots, x_n),$$

$$f_{R \cap S}(x_1, \ldots, x_n) = f_R(x_1, \ldots, x_n) \cdot f_S(x_1, \ldots, x_n),$$

$$f_{R \cup S}(x_1, \ldots, x_n) = f_R(x_1, \ldots, x_n) + f_S(x_1, \ldots, x_n) \dot{-} f_R(x_1, \ldots, x_n) \cdot f_S(x_1, \ldots, x_n).$$

4. $R = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \leq y\}$ *is primitive recursive, since* $f_R(x, y) = 1 \dot{-} (x \dot{-} y)$.

5. $x = y \Leftrightarrow x \leq y$ *and* $y \leq x$ *whence* $x = y$ *is primitive recursive.*

6. $x < y \Leftrightarrow x \leq y$ *and* $x \neq y$ *whence* $x < y$ *is primitive recursive.*

7. *If* $R_i \subseteq \mathbb{N}^n,\ 1 \leq i \leq m$, *are primitive recursive and*

$$R_i \cap R_j = \varnothing \text{ when } i \neq j \text{ and } \bigcup_{i=1}^{m} R_i = \mathbb{N}^n$$

and functions $f_i : \mathbb{N}^n \to \mathbb{N},\ 1 \leq i \leq m$, *are primitive recursive, then the function*

$$h(x_1, \ldots, x_n) = \begin{cases} f_1(x_1, \ldots, x_n) & \text{if } R_1(x_1, \ldots, x_n) \\ \vdots & \\ f_m(x_1, \ldots, x_n) & \text{if } R_m(x_1, \ldots, x_n) \end{cases}$$

is primitive recursive, for

$$h(x_1, \ldots, x_n) = \sum_{i=1}^{m} f_i(x_1, \ldots, x_n) \cdot f_{R_i}(x_1, \ldots, x_n).$$

8. *If* $f : \mathbb{N}^{n+1} \to \mathbb{N}$ *is primitive recursive, then*

$$g(x_1, \ldots, x_n) = \prod_{i=0}^{x_1} f(i, x_1, \ldots, x_n)$$

and

$$h(x_1, \ldots, x_n) = \sum_{i=0}^{x_1} f(i, x_1, \ldots, x_n)$$

are primitive recursive, for if

$$\begin{cases} g'(0, x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n) \\ g'(y + 1, x_1, \ldots, x_n) = g'(y, x_1, \ldots, x_n) \cdot f(y + 1, x_1, \ldots, x_n) \end{cases}$$

then $g(x_1, \ldots, x_n) = g'(x_1, x_1, \ldots, x_n)$, *and if*

$$\begin{cases} h'(0, x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n) \\ h'(y + 1, x_1, \ldots, x_n) = h'(y, x_1, \ldots, x_n) + f(y + 1, x_1, \ldots, x_n) \end{cases}$$

then $h(x_1, \ldots, x_n) = h'(x_1, x_1, \ldots, x_n)$.

9. *If* $R \subseteq \mathbb{N}^{n+1}$ *is primitive recursive, then the relation*

$$S = \{\langle x_1, \dots, x_n\rangle \mid (\forall z \leq x_1)(\langle z, x_1, \dots, x_n\rangle \in R)\}$$

is primitive recursive, for $f_S(x_1, \dots, x_n) = \prod_{i=0}^{x_1} f_R(i, x_1, \dots, x_n)$. *Similarly,*

$$S = \{\langle x_1, \dots, x_n\rangle \mid (\exists z \leq x_1)(\langle z, x_1, \dots, x_n\rangle \in R)\}$$

is primitive recursive, for $f_S(x_1, \dots, x_n) = 1 \dot{-} (1 \dot{-} \sum_{i=0}^{x_1} f_R(i, x_1, \dots x_n))$.

10. *If* $R \subseteq \mathbb{N}^{n+1}$ *is primitive recursive and* $f : \mathbb{N}^n \to \mathbb{N}$ *is obtained by* bounded minimalisation *from* R, *i.e.*

$$f(x_1, \dots, x_n) = \begin{cases} \text{the least } z \leq x_1 \text{ such that } \langle z, x_1, \dots, x_n\rangle \in R, \\ \text{if there is such} \\ 0 \quad \text{otherwise} \end{cases}$$

then f *is primitive recursive, for if*

$$f'(0, x_1, \dots, x_n) = 0$$

$$f'(y+1, x_1, \dots, x_n) = \begin{cases} f'(y, x_1, \dots, x_n) & \text{if } (\exists u \leq y)(\langle u, x_1, \dots, x_n\rangle \in R) \\ y+1 & \text{if } \langle y+1, x_1, \dots, x_n\rangle \in R \text{ and} \\ & \quad \neg(\exists u \leq y)(\langle u, x_1, \dots, x_n\rangle \in R) \\ 0 & \text{otherwise} \end{cases}$$

then $f(x_1, \dots, x_n) = f'(x_1, x_1, \dots, x_n)$. *We then denote*

$$f(x_1, \dots, x_n) = \mu z \leq x_1 \langle z, x_1, \dots, x_n\rangle \in R.$$

11. *Let* $[x]$ *be the integer part of the real* x.

$f(x, y) = [x/y]$ *is primitive recursive, since*

$f(x, y) = (\mu z \leq x)(z \cdot y + y > x)$ *(We agree that* $[n/0] = 0$.*)*

$g(x) = [\sqrt{x}\ ]$ *is primitive recursive, since*

$g(x) = (\mu z \leq x)((z+1)^2 > x)$

$h(x) = [{}^2\log(x+1)]$ *is primitive recursive, since*

$h(x) = (\mu z \leq x)(2^{z+1} > x+1)$. □

What we call the *pairing function*, is the primitive recursive function

$$\pi(x, y) = \frac{1}{2}((x+y)^2 + 3x + y).$$

This is a bijection $\mathbb{N}^2 \to \mathbb{N}$ (Problem 5) whence we can define projection functions

$$\rho(z) = (\mu x \leq z)(\exists y \leq z)(\pi(x, y) = z)$$

$$\sigma(z) = (\mu y \leq z)(\exists x \leq z)(\pi(x, y) = z)$$

and

$$\rho(\pi(x, y)) = x, \ \sigma(\pi(x, y)) = y.$$

Thus $\pi(x, y)$ *codes* the numbers x and y into one number. The functions ρ and σ *decode* this code.

Now we need some elementary facts from number theory. For all $x \in \mathbb{N}$ and $y \in \mathbb{N} \setminus \{0\}$ there are unique $q \in \mathbb{N}$ and $r \in \mathbb{N}$ such that following *division algorithm* holds: $x = q \cdot y + r \ , \ r < y$. The number r is the *remainder*. We write r=$rm(x, y)$ and agree that $rm(x, 0) = x$ for all x. If $rm(x, y) = 0$, then y is a *factor* of x and we write $y \mid x \ , \ y$ *divides* x. We agree that $0 \nmid x$ for all $x \neq 0$. A natural number x is *prime*, $x \in Pr$, if its only factors are 1 and x and if additionally $x > 1$. The numbers x and y are *relative primes* if they have no other common factors than 1 and additionally $x, y > 1$. We then write $\langle x, y\rangle \in RP$.

Example 5.9 *The above fundamental concepts of number theory are all primitive recursive.*

1. *The remainder function $rm(x, y)$ is primitive recursive, since*

$$rm(x, y) = (\mu z \leq x)(\exists n \leq x)[(x = ny + z \textit{ and } z < y \textit{ and } y > 0)$$
$$\textit{or } (y = 0 \textit{ and } z = x)].$$

2. *The divisibility relation $y|x$ is primitive recursive, since $y|x \iff rm(x, y) = 0$.*

3. *The relation RP, i.e. "x and y are relative primes", is primitive recursive, since $\langle x, y\rangle \in RP \iff x > 1$ and $y > 1$ and not $(\exists n \leq x)(n \mid x$ and $n \mid y$ and $n > 1)$.*

4. *The set of primes Pr is primitive recursive, since $x \in Pr \iff x > 1$ and not $(\exists n \leq x)(n \mid x$ and $n > 1$ and $n < x)$.*

Let us denote consecutive primes as follows:

$$\begin{array}{lll} p_0 = 2 & p_3 = 7 & p_{100} = 547 \\ p_1 = 3 & p_4 = 11 & p_{101} = \cdots \\ p_2 = 5 & p_5 = 13 & \vdots \end{array}$$

One of the fundamental truths of mathematics is that every $m > 0$ can be expressed as a product of primes

$$m = 2^{a_0} \cdot 3^{a_1} \cdot \ \ldots \ \cdot p_k^{a_k},$$

where $a_k \neq 0$, except if $m = 1$ in which case $m = 2^0$. This is the *prime factorisation* of m. It can be generated simply by dividing the number m time after time, first by 2 as many times as the division is possible without remainder, then by 3, then by 5 etc. Because of the uniqueness of prime factorisation,

$$a_i = (\mu z \leq m)(p_i^z \mid m \text{ and } p_i^{z+1} \nmid m).$$

We use prime factorisation for coding an arbitrary sequence of numbers. In order that the length of the sequence becomes coded as well, we add 1 to all exponents. The *code* of a sequence $\langle a_0, \ldots, a_k \rangle$ is the number

$$m = 2^{a_0+1} \cdot 3^{a_1+1} \cdot \ \ldots \ \cdot p_k^{a_k+1}. \tag{5.1}$$

Conversely, if $m > 1$ is given, we denote:

$$\begin{aligned} k = \operatorname{len}(m) &= (\mu z \leq m)(p_{z+1} \nmid m) \\ a_i = (m)_i &= (\mu z \leq m)(p_i^{z+2} \nmid m). \end{aligned}$$

Thus, if $\langle a_0, \ldots, a_k \rangle \ \in \mathbb{N}^{k+1}$, then

$$\begin{aligned} k &= \operatorname{len}(2^{a_0+1} \cdot \ldots \cdot p_k^{a_k+1}) \\ a_i &= \ (2^{a_0+1} \cdot \ldots \cdot p_k^{a_k+1})_i. \end{aligned}$$

Now we can both *code* an arbitrary sequence $\langle a_0, \ldots, a_k \rangle$ into one number m and *decode* an arbitrary number $m > 0$ into a sequence $\langle (m)_0, ..., (m)_{\operatorname{len}(m)} \rangle$. Decoding a number is only meaningful if the number m is indeed of the form (5.1). As special cases we define $\operatorname{len}(1) = \operatorname{len}(0) = 0$ and $(m)_i = 0$ when $m = 0$ or $m = 1$.

Example 5.10 *The functions used in coding are all primitive recursive:*

1. The function $n \mapsto p_n$ is primitive recursive. (Problem 8).
2. The function $\operatorname{len}(x)$ is primitive recursive. Follows from 1.
3. The function $\langle x, y \rangle \mapsto (x)_y$ is primitive recursive. Follows from 1.

The class of primitive recursive functions is closed under much more complicated recursive definitions than Definition 5.5 (PR5). We use coding to prove this, and demonstrate the method first with the example of double recursion:

Lemma 5.11 (Double recursion) *Let*

$$\begin{cases} f_1(0, x) = g_1(x) \\ f_2(0, x) = g_2(x) \\ f_1(y+1, x) = h_1(y, f_1(y, x), f_2(y, x), x) \\ f_2(y+1, x) = h_2(y, f_1(y, x), f_2(y, x), x) \end{cases}$$

where g_1, g_2, h_1, h_2 are primitive recursive Then f_1 and f_2 are primitive recursive.

Proof. The following method is often useful: We define an *auxiliary function*

$$f^*(y,x) = 2^{f_1(y,x)+1} \cdot 3^{f_2(y,x)+1}$$

and show that f^* is primitive recursive. After that

$$\begin{aligned} f_1(y,x) &= (f^*(y,x))_0 \\ f_2(y,x) &= (f^*(y,x))_1 \end{aligned}$$

are seen to be primitive recursive. Rather than trying to show that the functions f_1 and f_2 are primitive recursive, we focus on the auxiliary function f^* and define the functions f_1 and f_2 in terms of that. For the function f^* we obtain the following equations:

$$\begin{aligned} f^*(0,x) &= 2^{g_1(x)+1} \cdot 3^{g_2(x)+1} \\ f^*(y+1,x) &= 2^{f_1(y+1,x)+1} \cdot 3^{f_2(y+1,x)+1} \\ &= 2^{h_1(y,f_1(y,x),f_2(y,x),x)+1} \cdot 3^{h_2(y,f_1(y,x),f_2(y,x),x)+1} \\ &= 2^{h_1(y,(f^*(y,x))_0,(f^*(y,x))_1,x)+1} \cdot 3^{h_2(y,(f^*(y,x))_0,(f^*(y,x))_1,x)+1} \end{aligned}$$

If we denote $g^*(x) = 2^{g_1(x)+1} \cdot 3^{g_2(x)+1}$ and

$$h^*(y,z,x) = 2^{h_1(x,(z)_0,(z)_1,x)+1} \cdot 3^{h_2(x,(z)_0,(z)_1,x)+1},$$

then g^* and h^* are primitive recursive and

$$\begin{aligned} f^*(0,x) &= g^*(x) \\ f^*(y+1,x) &= h^*(y,f^*(y,x),x) \end{aligned}$$

□

Another example of recursion that is not of the simple type of Definition 5.5 is the following:

$$\begin{cases} h(0,x) = f_1(x) \\ h(1,x) = f_2(x) \\ h(y+2,x) = g(y,h(y,x),h(y+1,x),x). \end{cases}$$

To calculate $h(y,x)$ in this example one has to calculate both $h(y-1,x)$ and $h(y-2,x)$, while in the ordinary recursion

$$\begin{cases} h(0,x) = f(x) \\ h(y+1,x) = g(y,h(y,x),x). \end{cases}$$

one has to calculate $h(y-1,x)$ only for calculating $h(y,x)$. Another possibility is that to calculate $h(y,x)$ one has to calculate $h([y/2],x)$. To deal with all examples of this type we prove a general result (Theorem 5.12). To this end, if $f(y, x_1, \ldots, x_n)$ is a function, then we define

$$\tilde{f}(y, x_1, \ldots, x_n) = \prod_{i=0}^{y} p_i^{f(i,x_1,\ldots,x_n)+1}$$

whence $f(i, x_1, \ldots, x_n) = (\tilde{f}(i, x_1, \ldots, x_n))_i$.
Note. If f is primitive recursive, then also $\tilde{f}$ is primitive recursive. If $\tilde{f}$ is primitive recursive, then so is f.

Theorem 5.12 *If*

$$\begin{cases} f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \\ f(y+1, x_1, \ldots, x_n) = h(y, \tilde{f}(y, x_1, \ldots, x_n), x_1, \ldots, x_n) \end{cases}$$

where g and h are primitive recursive, then f is primitive recursive.

Proof. It suffices to prove that $\tilde{f}$ is primitive recursive.

$$\begin{cases} \tilde{f}(0, x_1, \ldots, x_n) = 2^{g(x_1,\ldots,x_n)+1} \\ \tilde{f}(y+1, x_1, \ldots, x_n) = \tilde{f}(y, x_1, \ldots, x_n) \cdot p_{y+1}^{h(y,\tilde{f}(y,x_1,\ldots,x_n),x_1,\ldots,x_n)+1} \end{cases}$$

Example 5.13 *The* Fibonacci sequence *is defined as follows:* $a_0 = 0, a_1 = 1, a_{n+2} = a_n + a_{n+1}$. *The function $f(n) = a_n$ is primitive recursive, for $f(0) = 0$ and $f(n+1) = (\tilde{f}(n))_{n \dot{-} 1} + (\tilde{f}(n))_n + (1 \dot{-} n)$.*

5.2 Recursive functions

We have observed that the class of primitive recursive functions is closed under bounded minimalisation. Bounded minimalisation is a kind of search operation with a bound on how large numbers we have to go through. The class of recursive functions generalizes this to search without an upper bound, as long as we known in advance that a solution can be found. Emphasizing the difference may seem like splitting hairs, but in fact the class of recursive functions is much bigger than the class of primitive recursive functions.

Let $R \subseteq \mathbb{N}^{n+1}$ and $f : \mathbb{N}^n \to \mathbb{N}$. We say that f is obtained from R by *minimalisation* if

1. for all $x_1, \ldots, x_n \in \mathbb{N}$ there is y such that $\langle y, x_1, \ldots, x_n \rangle \in R$.
2. for all $x_1, \ldots, x_n \in \mathbb{N}$ we have $f(x_1, \ldots, x_n)$ is the least y such that $\langle y, x_1, \ldots, x_n \rangle \in R$.

Then we write

$$f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n \rangle \in R)$$

Definition 5.14 (Recursiveness) *The class of* recursive[2] functions *is defined as follows:*

1. *$S, Pr_i^n, +, \cdot, \dot{-}, x^y$ are recursive.*
2. *A function obtained from recursive functions by composition is recursive.*
3. *If $R \subseteq \mathbb{N}^{n+1}$ is a relation such that f_R is a recursive function (i.e. R is a* recursive relation*) and $f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n\rangle \in R)$ then f is recursive.*

We can immediately observe that the class of recursive relations includes the relations $x = y$, $x < y$ and $x \leq y$ and is closed under conjunction, disjunction and complement. Also restricted quantification preserves recursiveness:

$$(\forall z \leq y)(\langle z, x_1, \ldots, x_n\rangle \in R) \iff$$
$$(\mu z)(\langle z, x_1, \ldots, x_n\rangle \notin R \vee z = y+1) = y+1$$
$$(\exists z \leq y)(\langle z, x_1, \ldots, x_n\rangle \in R) \iff$$
$$(\mu z)(\langle z, x_1, \ldots, x_n\rangle \in R \vee z = y+1) \leq y$$

Thus also $rm(x, y)$, $\pi(x, y)$, $\rho(x, y)$ and $\sigma(x, y)$ are recursive.

Note. If $R = \{\langle y, x_1, \ldots, x_n\rangle \mid y = f(x_1, \ldots, x_n)\}$ is primitive recursive, then f is not necessarily primitive recursive, but it is recursive, since $f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n\rangle \in R)$.

Theorem 5.15 *If*

$$\begin{cases} f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \\ f(y+1, x_1, \ldots, x_n) = h(y, f(y, x_1, \ldots, x_n), x_1, \ldots, x_n) \end{cases}$$

where g and h are recursive, then f is recursive.

Proof. We commence with a proof that the function $n \mapsto p_n$ is recursive. We code a number n and a sequence $p_0, p_1, ..., p_n$ into one number z:

$$z = 2^0 \cdot 3^1 \cdot \ldots \cdot p_n^n.$$

Now $b = p_n$ satisfies

b is a prime

not $2|z$

If p and q are consecutive primes, $p < q \leq b$ and $i < n+1$, then

$p^i|z \iff q^{i+1}|z$

$b^n|z$ but not $b^{n+1}|z$

[2] Also known as *computable functions*.

Let R be the set of triples $\langle z, b, n\rangle$, where z b and n satisfy the above property. It is easy to see (by induction) that R is a recursive relation and that for all n there is one and only one z and one and only one b which satisfy the condition $\langle z, b, n\rangle \in R$. Now p_n is easy to compute from the number $(\mu z)(\exists y \leq z)R(z, y, n)$.

We now return to the original task and take advantage of the knowledge that the function $n \mapsto p_n$ is recursive: For given y and $\vec{x}$ we code the sequence $f(0, \vec{x}), f(1, \vec{x}), \ldots, f(y, \vec{x})$ into one number z:

$$z = 2^{f(0,\vec{x})+1} \cdot 3^{f(1,\vec{x})+1} \cdot \ldots \cdot {p_y}^{f(y,\vec{x})+1}$$

Now

$$\begin{aligned}
(z)_0 &= f(0, \vec{x}) \\
(z)_1 &= f(1, \vec{x}) \\
&\vdots \\
(z)_y &= f(y, \vec{x})
\end{aligned}$$

It is clear that

$$f(y, \vec{x}) = (\mu z((z)_0 = g(\vec{x}) \wedge \forall i < y((z)_{i+1} = h(i, (z)_i, \vec{x}))))_y.$$

Therefore f is recursive. $\square$

Theorem 5.15 holds also if the function x^y is left out from Definition 5.14, case 1. Then the above coding can be replaced by appeal to the so-called *Chinese Remainder Theorem.*

We have now seen that the class of recursive functions is closed under the same operations as the class of primitive recursive functions. In addition, recursiveness is preserved by unbounded minimalisation. In fact recursiveness is closed under much more complicated recursions than primitive recursiveness. The *Ackermann function*

$$\begin{array}{rcl}
A(0, x) & = & x + 1 \\
A(y + 1, 0) & = & A(y, 1) \\
A(y + 1, x + 1) & = & A(y, A(y + 1, x))
\end{array}$$

is an example of a recursive function that is not primitive recursive (Problems 15,)

According to the so-called *Church's Thesis* the class of recursive functions is exactly the same as the class of intuitively computable functions i.e. functions computable by a human following an algorithm. This thesis has a lot of evidence. All different attempts to define the concept of an intuitively computable function have turned out equivalent with recursiveness.

5.3 Definability in number theory

We prove in this section that recursive functions are definable in the standard model of number theory. For simplicity[3] we extend the vocabulary of number theory with a symbol for the exponential function: $L_{exp} = \{\oplus, \otimes, 0, 1, \underline{exp}\}$, where $\underline{exp}$ is a 2-place function symbol. Let $\mathcal{N}_{exp} = (\mathbb{N}, +, \cdot, 0, 1, exp)$, where $exp(n, m) = n^m$ and $exp(0, 0) = 1$.

Recall that a function $f : M^n \to M$ is said to be definable in a structure $\mathcal{M}$ (see Definition 4.30) if the relation

$$\{\langle x_1, \ldots, x_n, y\rangle | f(x_1, \ldots, x_n) = y\}$$

is definable in $\mathcal{M}$.

Theorem 5.16 *Let L vocabulary and $\mathcal{M}$ an L-structure. The class of functions definable in $\mathcal{M}$ is closed under composition: Let $f : M^n \to M$ and $g_i : M^m \to M$ $(1 \le i \le n)$ be definable. Then also $h : M^m \to M$,*

$$h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))$$

is definable.

Proof. Let φ be an L-formula such that

$$\mathcal{M} \models_s \varphi \iff f(s(0), \ldots, s(n-1)) = s(n)$$

and ψ_i L-formulas, $(1 \le i \le n)$, such that

$$\mathcal{M} \models_s \psi_i \iff g_i(s(0), \ldots, s(m-1)) = s(m).$$

In the formula φ the variable v_n is playing the role of the value of the function f when its arguments are $v_0, ..., v_{n-1}$. Respectively, in the formula ψ_i the variable v_m plays the role of the value of the function g_i when the arguments are $v_0, ..., v_{m-1}$. Now $h(a_0, ..., a_{m-1}) = a_m$ if and only if there are values $b_0, ..., b_n$ such that for all $i = 0, ..., n$ $g_i(a_0, ..., a_{m-1}) = b_i$ and additionally $f(b_0, ..., b_n) = a_m$. We now write the same, but using predicate logic. First we need some auxiliary variables that do not occur yet in these formulas. Let therefore k be greater than any j, for which v_j occurs in the formula $\varphi, \psi_1, \ldots, \psi_n$.

$$\begin{array}{rcl} h(s(0), \ldots, s(m-1)) & = & s(m) \\ & \iff & \\ \mathcal{M} & \models_s & \exists v_k \ldots \exists v_{k+n}(\varphi(v_k/v_0, \ldots, v_{k+n}/v_n) \wedge \\ & & \psi_1(v_k/v_m) \wedge \\ & & \psi_2(v_{k+1}/v_m) \wedge \ldots \\ & & \ldots \wedge \psi_n(v_{k+n-1}/v_m) \wedge \\ & & \approx v_{k+n}v_m) \end{array}$$

□

[3] This could be avoided if desired.

Theorem 5.17 *The class of functions and relations definable in the model $\mathcal{N}_{exp}$ is closed under minimalisation: If $R \subseteq \mathbb{N}^{n+1}$ is definable in $\mathcal{N}_{exp}$ and $f : \mathbb{N}^n \to \mathbb{N}$ such that*

$$f(x_1, \ldots, x_n) = \mu y(\langle x_1, \ldots, x_n, y\rangle \in R)$$

then f is definable in $\mathcal{N}_{exp}$.

Proof. Let φ be a formula of number theory such that

$$\mathcal{N}_{exp} \models_s \varphi \iff \langle s(0), \ldots, s(n)\rangle \in R$$

Let k be greater than any i, for which v_i occurs in φ. Now

$f(x_1, ..., x_n) = y \iff (\langle x_1, \ldots, x_n, y\rangle \in R$ and for all $z < y(\langle x_1, \ldots, x_n, z\rangle \notin R))$.

Therefore $f(s(0), \ldots, s(n-1)) = s(n) \iff \mathcal{N}_{exp} \models_s \varphi \wedge \forall v_k(\exists v_{k+1} \approx \oplus \oplus v_k v_{k+1} 1 v_n \to \neg\varphi(v_k/v_n))$. □

Theorem 5.18 *All recursive functions are definable in $\mathcal{N}_{exp}$.*

Proof. The starting functions Z, S, $+$, $\cdot$, Pr_i^n, $\dot{-}$ and m^n are clearly definable, whence the claim follows from Theorem 5.16 and Theorem 5.17. □

We now define *Gödel-numbering*. We associate terms and formulas of predicate logic with natural numbers in a certain simple manner. This makes it possible to apply number theory to terms and formulas. If w is a sequence (or a *word*)

$$w = w_0 \ldots w_k$$

built up from the symbols

$$0, 1, \oplus, \otimes, \underline{exp}, \approx, (,), \to, \neg, \forall, v_i,$$

then the *Gödel-number* of w is the natural number

$$\ulcorner w \urcorner = p_0{}^{\#(w_0)+1} \cdot \ldots \cdot p_k{}^{\#(w_k)+1}$$

where

$\#(0) = 0$	$\#(\approx) = 5$	$\#(\neg) = 9$
$\#(1) = 1$	$\#(() = 6$	$\#(\forall) = 10$
$\#(\oplus) = 2$	$\#()) = 7$	$\#(v_i) = 11 + i$
$\#(\otimes) = 3$	$\#(\to) = 8$	
$\#(\underline{exp}) = 4$		

For example

$$\ulcorner \approx v_0 v_1 \urcorner = 2^6 \cdot 3^{12} \cdot 5^{13} = 2767921875000000$$
$$\ulcorner \forall v_1 \approx \oplus v_0 v_1 v_2 \urcorner = 2^{11} \cdot 3^{13} \cdot 5^6 \cdot 7^3 \cdot 11^{12} \cdot 13^{13} \cdot 17^{14}$$
$$= 280079363569829269358223533191300819708709873301206889600000$$

Theorem 5.19 *The set* $\mathrm{Trm} = \{\ulcorner t \urcorner \mid t$ *is an* L_{exp}*-term*$\}$ *is primitive recursive.*

Proof. The following relations are primitive recursive:

$$\begin{array}{rcl} Zero(x) & \iff & x = \ulcorner 0 \urcorner \\ One(x) & \iff & x = \ulcorner 1 \urcorner \\ Variable(x) & \iff & x = \ulcorner v_i \urcorner \text{ for some } i \leq x \\ x * y = z & \iff & \mathrm{len}(z) = \mathrm{len}(x) + \mathrm{len}(y) + 1 \text{ and} \\ & & (\forall i \leq \mathrm{len}(x))((z)_i = (x)_i) \text{ and} \\ & & (\forall i \leq \mathrm{len}(y))((z)_{\mathrm{len}(x)+i+1} = (y)_i) \\ Sum(x,y,z) & \iff & z = \ulcorner \oplus \urcorner * x * y \\ Product(x,y,z) & \iff & z = \ulcorner \otimes \urcorner * x * y \\ Exp(x,y,z) & \iff & z = \ulcorner \underline{exp} \urcorner * x * y \end{array}$$

Here $x * y$ is an associative operation corresponding to *concatenation*[4] of words. We now show that f_{Trm} is a primitive recursive function. Note that $f_{\mathrm{Trm}}(z) = 1$ iff

$$\begin{array}{l} Zero(z) \vee One(z) \vee Variable(z) \vee \\ (\exists x \leq z)(\exists y \leq z)(Sum(x,y,z) \vee Product(x,y,z) \vee Exp(x,y,z)) \\ \wedge f_{\mathrm{Trm}}(x) = f_{\mathrm{Trm}}(y) = 1) \end{array}$$

If $x \leq z$, then $f_{\mathrm{Trm}}(x) = (\tilde{f}_{\mathrm{Trm}}(z))_x$. Thus $f_{\mathrm{Trm}}(z) = 1 \iff Zero(z)$ or $One(z)$ or $Variable(z)$ or $(\exists x < z)(\exists y < z)((Sum(x,y,z)$ or $Product(x,y,z)$ or $Exp(x,y,z))$ and $(\tilde{f}_{\mathrm{Trm}}(z))_x = (\tilde{f}_{\mathrm{Trm}}(z))_y = 1)$. The right hand side of the equivalence is:

$$\langle z - 1, \tilde{f}_{\mathrm{Trm}}(z-1) \rangle \in R$$

where R is primitive recursive, since x and y above can be chosen strictly smaller than z. Now we have

$$\begin{cases} f_{\mathrm{Trm}}(0) = 0 \\ f_{\mathrm{Trm}}(z+1) = f_R(z, \tilde{f}_{\mathrm{Trm}}(z)) \end{cases}$$

Hence f_{Trm} is primitive recursive □

Theorem 5.20 *The set* $\mathrm{Fml} = \{\ulcorner \varphi \urcorner \mid \varphi$ L_{exp}*-formula*$\}$ *is primitive recursive.*

Proof. See Problem 24. □

We now define a substitution operation which is purely number theoretic but in fact codes substitution among words. Let $Sub \subseteq \mathbb{N}^3$ be the relation

[4]Note that $2^{a_0+1} \cdot \ldots \cdot p_n^{a_n+1} * 2^{a_{n+1}+1} \cdot \ldots \cdot p_m^{a_{n+m+1}+1} = 2^{a_0+1} \cdot \ldots \cdot p_{n+m+1}^{a_{n+m+1}+1}$. For example $288 * 10800 = 2^5 \cdot 3^2 * 2^4 \cdot 3^3 \cdot 5^2 = 2^5 \cdot 3^2 \cdot 5^4 \cdot 7^3 \cdot 11^2 = 7470540000$.

$$\langle x,y,z\rangle \in Sub \iff \begin{array}{l}\text{there are words } w \text{ and } w' \text{ such that}\\ x=\ulcorner w\urcorner,\ y=\ulcorner w'\urcorner \text{ and } w' \text{ is obtained } w\\ \text{by replacing each } v_0 \text{ by the symbol } \underline{z},\end{array}$$

where $\underline{0}$ is the term 0 and $\underline{n+1}$ is the term $\underline{n}\oplus 1$.

Lemma 5.21 *The relation Sub is primitive recursive.*

Proof. Let $E \subseteq \mathbb{N}$ be the primitive recursive set

$$E = \{x \in \mathbb{N} | (\forall y \leq x)((x)_y \neq \#(v_0))\}$$

Now

$$\begin{array}{lll}\langle x,y,z\rangle \in Sub & \text{iff} & (x \in E \text{ and } x = y) \text{ or}\\ & & (\exists i < x)(\exists j < x)(\exists k < y)(\langle i,k,z\rangle \in Sub\\ & & \ \text{and } x = i * \ulcorner v_0\urcorner * j \text{ and } y = k * \ulcorner \underline{z}\urcorner * j\\ & & \ \text{and } j \in E)\end{array}$$

The function $z \mapsto \ulcorner \underline{z}\urcorner$ is clearly primitive recursive. Hence Sub is. □

Our goal now is to show that the property "φ is true" of a number theoretic sentence φ is not a definable property of the Gödel number of φ, and therefore also not a recursive property. In short, truth in number theory cannot be defined in a recursive way (see Corollary 5.24). Combined with Church's Thesis (see page 5.2) this means that the truth of number theoretic statements cannot be decided mechanically. This result of Gödel from 1931 caused an uproar which has not completely subsided.

Behind Gödel's result is the age-old *Liar Paradox.* A man says he is lying. Is he telling the truth? If he is, he is lying, whence he is telling the truth after all. So it cannot be that he is telling the truth. But that means he is lying i.e. what he says is true. Either way we end up in a contradiction. The same can be presented as follows: Consider the sentence

$$\text{The sentence (5.2) is not true.} \tag{5.2}$$

Is the sentence (5.2) true or not true? If it is true, it is not true. If it is not true, it is true. We cannot decide the truth of (5.2). From this it seems to follow that there is something wrong with the sentence (5.2).

Gödel's extraordinary achievement was to replace in this argument "not true" by "unprovable" and use Theorem 5.18 to show that the following sentence really exists:

$$\text{The sentence (5.3) is unprovable.} \tag{5.3}$$

Is the sentence (5.3) provable? If it is, it is by the Soundness Theorem true and hence unprovable. Hence (5.3) cannot be provable. But then (5.3) is true. We have an example of a true sentence that cannot be proved.

Gödel's proof is based on the so-called Gödel's Fixed-Point Theorem 5.22, which has the following idea: Consider a formula φ of number theory with one free variable v_0. The formula φ expresses some number theoretic property of the number v_0. But v_0 can have as its value the Gödel-number of a number theoretic formula ψ. Thus in this case φ expresses a property of the Gödel-number of ψ. The Fixed-Point Theorem says that ψ can be chosen in such a way that if v_0 is interpreted as the Gödel-number of ψ, then φ expresses exactly the property ψ. In other words, the sentence $\varphi(\underline{\ulcorner\psi\urcorner}/v_0)$ says the same thing as the sentence ψ, when $\underline{\ulcorner\psi\urcorner}$ connotes the constant term $\oplus ... \oplus 01$ ($\ulcorner\psi\urcorner$ $\oplus$-symbols).

Mathematics has many fixed-point theorems. For example the following: If f is a continuous function of the closed interval $[0,1]$ into itself, then there is a point x on the interval such that $f(x) = x$. One way of finding this x is to compute $f(0), f(f(0)), f(f(f(0))), ...$ It can be shown that this sequence converges to some point x on the interval. Then we use continuity to show that $f(x) = x$.

In logic one finds fixed points in principle in the same way, i.e. by iteration. Iteration may, however, lead to a sentence of infinite length. We can avoid arriving at an infinite sentence by utilizing *diagonalisation*, based on a substitution operation.

Theorem 5.22 (Gödel's Fixed-Point Theorem) *If φ is a formula of number, then there is formula ψ if number theory such that for all $s : \mathbb{N} \to \mathcal{N}_{exp}$.*

$$\mathcal{N}_{exp} \models_s \psi \Longleftrightarrow \mathcal{N}_{exp} \models_s \varphi(\underline{\ulcorner\psi\urcorner}/v_0)$$

and, in addition, the formulas ψ and $\varphi(\underline{\ulcorner\psi\urcorner}/v_0)$ have the same free variables.

Proof. Let σ be a formula for which

$$\langle s(0), s(1), s(2)\rangle \in Sub \Longleftrightarrow \mathcal{N}_{exp} \models_s \sigma$$

Remember: $\langle \ulcorner w\urcorner, \ulcorner w'\urcorner, z\rangle \in Sub \Longleftrightarrow w'$ is obtained by replacing every v_0 in w by the term $\underline{z}$. We may assume that v_0 does not occur bound in σ and neither does v_0 or v_1 in φ. Let θ be the formula

$$\exists v_1(\varphi(v_1/v_0) \wedge \sigma(v_0/v_2)).$$

It is worth noting that

$$\mathcal{N}_{exp} \models_{s(\ulcorner w\urcorner/0)} \theta \Longleftrightarrow \mathcal{N}_{exp} \models_{s(\ulcorner w'\urcorner/0)} \varphi,$$

where w' is obtained from w by replacing v_0 by the term $\underline{\ulcorner w\urcorner}$. Let $k = \ulcorner\theta\urcorner$ and

$\psi = \theta(\underline{k}/v_0)$. Now

$$\begin{aligned}
\mathcal{N}_{exp} \models_s \psi &\iff \mathcal{N}_{exp} \models_s \theta(\underline{k}/v_0) \\
&\iff \mathcal{N}_{exp} \models_{s(\ulcorner\theta\urcorner/0)} \theta \\
&\iff \mathcal{N}_{exp} \models_{s(\ulcorner w'\urcorner/0)} \varphi, \text{ where } w' \text{ is obtained from } \theta \\
&\qquad \text{by replacing } v_0 \text{ by the term } \underline{\ulcorner\theta\urcorner}(=\underline{k}) \\
&\iff \mathcal{N}_{exp} \models_{s(\ulcorner\psi\urcorner/0)} \varphi \\
&\iff \mathcal{N}_{exp} \models_s \varphi(\underline{\ulcorner\psi\urcorner}/v_0)
\end{aligned}$$

□

Theorem 5.23 (Tarski's Theorem) *The set*

$$\mathrm{Tr} = \{\ulcorner\psi\urcorner \mid \psi \textit{ is an } L_{exp}\textit{-sentence and } \mathcal{N}_{exp} \models \psi\}$$

is not definable in $\mathcal{N}_{exp}$.

Proof. Suppose that there is an L_{exp}-formula φ such that $s(0) \in \mathrm{Tr} \iff \mathcal{N}_{exp} \models_s \varphi$ [5]. By Gödel's Fixed-Point Theorem (5.22) there is an L_{exp}-formula ψ such that $\mathcal{N}_{exp} \models_s \psi \iff \mathcal{N}_{exp} \models_s \neg\varphi(\underline{\ulcorner\psi\urcorner}/v_0)$. Let $s(0) = \ulcorner\psi\urcorner$. Since ψ is an L_{exp}-sentence, we have

$$\begin{aligned}
\mathcal{N}_{exp} \models_s \psi &\iff \ulcorner\psi\urcorner \in \mathrm{Tr} \\
&\iff s(0) \in \mathrm{Tr} \\
&\iff \mathcal{N}_{exp} \models_s \varphi \\
&\iff \mathcal{N}_{exp} \models_s \varphi(\underline{\ulcorner\psi\urcorner}/v_0), \text{ since } s(0) = \ulcorner\psi\urcorner \\
&\iff \mathcal{N}_{exp} \not\models_s \psi,
\end{aligned}$$

a contradiction. □

Corollary 5.24 Tr *is not a recursive set.*

Proof. Theorem 5.18! □

5.4 Recursively enumerable sets

A recursive set is intuitively such a set of natural numbers that of any given number one can decide mechanically in finite time whether it belongs to the set or not. In other words, the characteristic function of a recursive set is

[5] We may assume that the only free variable of φ is v_0.

mechanically (algorithmically) computable. Recursively enumerable sets are such that we have again a mechanical algorithm for deciding whether a given number is in the set and the algorithm gives a positive answer if the number indeed is in the set, but if the number is not in the set the algorithm may keep computing for ever and we will never find the answer (unless we wait for an infinite amount of time). In other words, we can list the elements of a recursively enumerable set mechanically with an algorithm, but the numbers do not come in increasing order, so we may never know whether e.g. 15 pops up in the list after a long wait or never.

Definition 5.25 (Recursive enumerability) *A set $A \subseteq \mathbb{N}$ is* recursively enumerable[6] *(shorthand r.e.), if $A = \emptyset$ or there is a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that*

$$A = \{f(n) \mid n \in \mathbb{N}\}.$$

Note. The question $m \in A$? can be decided by computing $f(0), f(1), \ldots$ until $f(n) = m$, if $m \in A$. But if $m \notin A$, one has to compute infinitely many values $f(0), f(1), \ldots$ before the answer $m \notin A$ is settled.

Theorem 5.26 *Every recursive set is recursively enumerable.*

Proof. Let $A \neq \emptyset$ recursive i.e. f_A is a recursive function. Let $a \in A$ be arbitrary. Let

$$f(n) = \begin{cases} n, & \text{if } f_A(n) = 1 \\ a, & \text{if } f_A(n) = 0 \end{cases}$$

Now f is recursive and $A = \{f(n) \mid n \in \mathbb{N}\}$. □

Theorem 5.27 *Let $A \subseteq \mathbb{N}$. the following conditions are equivalent:*

(1) A is recursive.
(2) A and $\mathbb{N} \setminus A$ are recursively enumerable

Proof. (1) ⇒ (2) follows from from Theorem 5.26 because the complement of a recursive set is always recursive.
(2) ⇒ (1). Let for non-empty A

$$A = \{f(n) \mid n \in \mathbb{N}\}$$
$$\mathbb{N} \setminus A = \{g(n) \mid n \in \mathbb{N}\}$$

where f and g are recursive. If $h(n) = \mu m(f(m) = n \text{ or } g(m) = n)$ then h is recursive and $n \in A \iff f(h(n)) = n$, whence A is recursive. □

Theorem 5.28 *The class of recursively enumerable sets is closed under union and intersection.*

[6] Recursively enumerable sets are also called *computably enumerable*.

Proof. First:

Lemma 5.29 *A set $A \subseteq \mathbb{N}$ is recursively enumerable if and only if there is a recursive relation $R \subseteq \mathbb{N} \times \mathbb{N}$ such that*

$$(*) \qquad n \in A \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m\rangle \in R)$$

Proof. Let first $A \subseteq \mathbb{N}$ be non-empty recursively enumerable, e.g. $A = \{f(n) \mid n \in \mathbb{N}\}$, where f is recursive. Let $R = \{\langle n, m\rangle \mid f(m) = n\}$. Now R is recursive and $(*)$ holds. Let conversely R be recursive such that $(*)$ holds. Let $a \in A$ and

$$f(n) = \begin{cases} \rho(n) & \text{if } \langle \rho(n), \sigma(n)\rangle \in R \\ a & \text{otherwise} \end{cases}$$

Now f is recursive. If $n \in \mathbb{N}$ and $\langle \rho(n), \sigma(n)\rangle \in R$, then $\rho(n) \in A$ by $(*)$ i.e. $f(n) \in A$. If on the other hand $n \in A$ and $\langle n, m\rangle \in R$ then $n = f(\pi(n, m))$. Hence $A = \{f(n) \mid n \in \mathbb{N}\}$. □

Corollary Recursively enumerable sets are definable in $\mathcal{N}_{exp}$.

We return to the proof of Theorem 5.28. Let

$$n \in A \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m\rangle \in R)$$
$$n \in B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m\rangle \in R').$$

Then

$$n \in A \cup B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m\rangle \in R \;\text{ or }\; \langle n, m\rangle \in R')$$
$$n \in A \cap B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, \rho(m)\rangle \in R \;\text{ and }\; \langle n, \sigma(m)\rangle \in R').$$

□

Theorem 5.30 *The set*

$$\mathrm{Thm} = \{\ulcorner \varphi \urcorner \mid P \vdash \varphi,\ \varphi \textit{ a sentence of number theory } \}$$

is recursively enumerable.

Proof. Let Prf be the set of such numbers m, that $\langle (m)_0, (m)_1, ...(m)_{\mathrm{len}(m)}\rangle$ is a deduction.
Claim: Prf is primitive recursive
Proof. We make a sequence of observations, each one of which is provable by methods we have already introduced, albeit one has to carry out a lot of details:

(1^0) $\mathrm{PeAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ is a member of Peano's axioms $\}$ is p.r.
(2^0) $\mathrm{PrAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ is an axiom of propositional ogic $\}$ is p.r.
(3^0) $\mathrm{IdAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ is an L-identity axiom $\}$ is p.r.
(4^0) $\mathrm{QuAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ is an L-quantifier axiom $\}$ is p.r.
(5^0) $\mathrm{MP} = \{\langle\ulcorner\varphi\urcorner, \ulcorner(\varphi \to \psi)\urcorner, \ulcorner\psi\urcorner\rangle \mid \varphi, \psi$ are formulas of number theory $\}$ is p.r.
(6^0) $\mathrm{Ug} = \{\langle\ulcorner n, (\varphi \to \psi)\urcorner, \ulcorner(\varphi \to \forall v_j \psi)\urcorner\rangle \mid \varphi, \psi$ are formulas of number theory, $\langle (n)_0, \ldots, (n)_{\mathrm{len}(n)}\rangle = \langle\theta_0, \ldots, \theta_{\mathrm{len}(n)}\rangle$, and v_j does not occur free in $\varphi, \theta_0, \ldots,$ or $\theta_{\mathrm{len}(n)}$ is p.r.
(7^0) $\mathrm{Sen} = \{\ulcorner\varphi\urcorner \mid \varphi$ is a sentence of number theory $\}$ is p.r.

Now

$$\begin{aligned} m \in \mathrm{Prf} \iff\ & \forall i \le \mathrm{len}(m)((m)_i \in \mathrm{PeAx} \text{ or } (m)_i \in \mathrm{PrAx} \text{ tai } (m)_i \in \mathrm{IdAx} \\ & \text{tai } (m)_i \in \mathrm{QuAx} \text{ or} \\ & (\exists j \le i)(\exists k \le i)(\langle (m)_j, (m)_k, (m)_i\rangle \in \mathrm{MP}) \\ & \text{tai } (\exists n \le m)(\exists p \le m)(\exists j \le i)(\langle n, (m)_j, (m)_i\rangle \in \mathrm{Ug} \\ & \quad \text{and } (\forall s \le \mathrm{len}(n))(\exists t < i)((n)_s = (m)_t). \end{aligned}$$

Finally:

$$n \in \mathrm{Thm} \iff \exists m (m \in \mathrm{Prf} \text{ and } (m)_{\mathrm{len}(m)} = n \text{ and } n \in \mathrm{Sen}).$$

□

Corollary 5.31 (Gödel) *There is a sentence of number theory which is true but not provable from Peano's axioms.*

Proof. In Tarski's Theorem 5.23 we defined the set

$$\mathrm{Tr} = \{\ulcorner\varphi\urcorner \mid \mathcal{N}_{exp} \models \varphi,\ \varphi \text{ a sentence of number theory}\}$$

and showed that Tr is not definable in $\mathcal{N}_{exp}$. Therefore $\mathrm{Thm} \neq \mathrm{Tr}$. By the Soundness Theorem 4.52, $\mathrm{Thm} \subseteq \mathrm{Tr}$. Thus $\mathrm{Tr} \setminus \mathrm{Thm} \neq \emptyset$. □

Theorem 5.32 (Gödel's 1st Incompleteness Theorem) *Peano's axioms P are an incomplete theory i.e. there is a sentence φ of number theory such that $P \nvdash \varphi$ and $P \nvdash \neg\varphi$.*

Proof. By Corollary 5.31 there is a true sentence φ such that $P \nvdash \varphi$. If $P \vdash \neg\varphi$, then $\mathbb{N} \models \neg\varphi$ and φ is not true. Therefore $P \nvdash \neg\varphi$. □

It follows from Theorem 5.32 that P has two models $\mathcal{M}_1$ and $\mathcal{M}_2$ in one of which φ is true and in the other false. This means that models of P are not all elementarily equivalent. Hence non-standard models have number theoretic properties that the standard model $\mathcal{N}$ does not share.

In view of Theorem 14.6 there is a formula Bew of number theory with just v_0 free such that

$$s(0) \in \mathrm{Thm} \Longleftrightarrow \mathcal{N}_{exp} \models_s Bew$$

i.e. if φ is a sentence of number theory, then

$$P \vdash \varphi \Longleftrightarrow \mathcal{N}_{exp} \models Bew(\underline{\ulcorner\varphi\urcorner}/v_0).$$

By Gödel's Fixed-Point Theorem there is sentence ψ such that (letting $\varphi = \neg Bew$):

$$\mathcal{N}_{exp} \models \psi \Longleftrightarrow \mathcal{N}_{exp} \models \neg Bew(\ulcorner\psi\urcorner/v_0).$$

If $P \vdash \psi$, then $\mathcal{N}_{exp} \models Bew(\underline{\ulcorner\psi\urcorner}/v_0)$, whence $\mathcal{N}_{exp} \models \neg\psi$. On the other hand $P \vdash \psi$ implies $\mathcal{N}_{exp} \models \psi$, whence

$$P \vdash \psi \Longrightarrow \mathcal{N}_{exp} \models (\psi \wedge \neg\psi).$$

Therefore $P \nvdash \psi$ i.e. $\mathcal{N}_{exp} \models \neg Bew(\underline{\ulcorner\varphi\urcorner}/v_0)$ i.e. $\mathcal{N}_{exp} \models \psi$.

Hence ψ is an example of a true sentence which is not provable. Note that

$$\psi \text{ says "}\psi \text{ is not provable"}$$

i.e. ψ is a version of the Liar Paradox.

We know that P is consistent since $\mathcal{N}_{exp} \models P$. The consistency of P is equivalent to $P \nvdash \approx 0\,1$ (since $P \vdash [\varphi \wedge \neg\varphi] \leftrightarrow \approx 0\,1$, whatever the formula φ is). But

$$P \nvdash \approx 0\,1 \Longleftrightarrow \mathcal{N}_{exp} \models \neg Bew(\ulcorner \approx 0\,1\urcorner/v_0),$$

which is why we use a shorthand

$$Con(P)$$

of its own for $\neg Bew(\underline{\ulcorner \approx 0\,1\urcorner}/v_0)$.

Theorem 5.33 (Gödel's 2nd Incompleteness Theorem) *The consistency of Peano's axioms is not provable from Peano's axioms i.e. $Con(P)$ is a true sentence such that*

$$P \nvdash Con(P)$$

Proof. (Sketch) In this proof we assume that the usual definition of $\underline{exp}$ is included in P. Let ψ be as above. Now if $P \vdash \psi$, then $\mathcal{N}_{exp} \models Bew(\underline{\ulcorner\psi\urcorner}/v_0)$. Inspection of the proof of Theorem 5.30 indicates that $P \vdash \psi$ implies even $P \vdash Bew(\underline{\ulcorner\psi\urcorner}/v_0)$. Inspection of the proof of Gödel's Fixed-Point Theorem 5.22 indicates that even

$$P \vdash (\psi \leftrightarrow \neg Bew(\underline{\ulcorner\psi\urcorner}/v_0)).$$

Thus $P \vdash \psi$ implies $P \vdash \neg\psi$, i.e. $P \vdash \psi$ implies $P \vdash [\psi \wedge \neg\psi]$, i.e. $P \vdash \approx 01$, i.e. $\mathcal{N}_{exp} \models \neg Con(P)$. This entire inference can be carried out in P, which yields

$$P \vdash Bew(\underline{\ulcorner\psi\urcorner}/v_0) \to \neg Con(P)$$

i.e.

$$P \vdash Con(P) \to \neg Bew(\underline{\ulcorner \psi \urcorner}/v_0)$$

i.e.

$$P \vdash Con(P) \to \psi.$$

Thus if $P \vdash Con(P)$, then $P \vdash \psi$, contrary to $P \nvdash \psi$. $\square$

Gödel's 2nd Incompleteness Theorem holds for all axiom sets (theories) in mathematics as long as they are simple enough for the proof of Theorem 5.30 to go through and strong enough that basic facts of number theory can be proved. No such axiom system can prove its own consistency: This can be interpreted as saying that mathematics can never prove its own consistency.

Theorem 5.33 has the interesting consequence that P has a non-standrad model $\mathcal{M}$ for which $\mathcal{M} \models \neg Con(P)$ i.e. $\mathcal{M} \models Bew(\underline{\ulcorner \approx 01 \urcorner}/v_0)$. Thus there is an element t of $\mathcal{M}$ which satisfies in $\mathcal{M}$ all the conditions of being a deduction and the last element of the "deduction" t is ≈ 01. Loosely speaking, we can "prove" in $\mathcal{M}$ that $0 = 1$ but the "proof" is infinitely long.

5.5 Problems

1. Show that the functions $c(y, x) = x^y$ and $C_k(x) = k$, $k \in \mathbb{N}$, are primitive recursive.

2. Prove directly on the basis of Definition 5.5 that the function $f(n) = n \dot{-} 1$ is primitive recursive.

3. Prove directly on the basis of Definition 5.5 that bounded subtraction

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geq y \\ 0 & \text{if } x < y \end{cases}$$

is primitive recursive. Hint: You may find Problem 2 useful.

4. Prove directly on the basis of Definition 5.5, that if the function $f(n, m)$ is primitive recursive, then also the function $g(n, m) = f(f(0, m), f(1, n))$ is.

5. Show that function $\pi : \mathbb{N}^2 \to \mathbb{N}, \pi(x, y) = ((x + y)^2 + 3x + y)/2$ is a bijection.

6. Suppose R is a 1-place primitive recursive relation. Define $R_n = \{x \in R | x < n\}$. Show that $f : \mathbb{N} \to \mathbb{N}$ is primitive recursive when $f(n)$ is the number of the elements in the set R_n for all $n \in \mathbb{N}$.

7. Suppose that $f, g : \mathbb{N} \to \mathbb{N}$ are primitive recursive and $(g \circ f)(x) \geq x$ for all $x \in \mathbb{N}$. Show that the set $\{f(n)|n \in \mathbb{N}\}$ is primitive recursive.

8. Prove that the function $n \mapsto p_n$ is primitive recursive.

9. Show that an infinite set $R \subseteq \mathbb{N}$ is recursive if and only if there exists a strictly increasing recursive function $f : \mathbb{N} \to \mathbb{N}$ for which $R = \{f(n) \mid n \in \mathbb{N}\}$.

10. Let f be a recursive function such that $A = \{f(n) : n \in \mathbb{N}\}$ is non-recursive. Let $B = \{2^{f(2n)} : n \in \mathbb{N}\}$, $C = \{3^{f(2n+1)} : n \in \mathbb{N}\}$ Prove that at least one of the sets B and C is non-recursive.

11. Show that for all $a, b \in \mathbb{N}$ there is a finite $X_{ab} \subseteq \mathbb{N} \times \mathbb{N}$ such that:

    (i) $(a, b) \in X_{ab}$,

    (ii) If $(0, x + 1) \in X_{ab}$ then $(0, x) \in X_{ab}$,

    (iii) If $(y + 1, 0) \in X_{ab}$ then $(y, 1) \in X_{ab}$,

    (iv) If $(y+1, x+1) \in X_{ab}$ then $(y+1, x) \in X_{ab}$ and $(y, A(y+1, x)) \in X_{ab}$.

12. Not so easy: Show that the Ackermann function is recursive.

13. Show that $A(2, x) = 2x + 3$.

14. Prove that : $y + x < A(y, x) < A(y, x + 1) \leq A(y + 1, x)$.

15. Not so easy: Show that the Ackermann function is not primitive recursive. (Hint: Show that for every primitive recursive function $f(x_1, \ldots, x_n)$ there is a number a such that for all $x_1, \ldots, x_n$ we have $f(x_1, \ldots, x_n) < A(a, x_1 + \ldots + x_n)$.)

16. Let us call $R \subseteq \mathbb{N}$ *number theoretic* if it is definable in the model $\mathcal{N}_{exp}$. Suppose $R \subseteq \mathbb{N}^2$ is such that for all number theoretic $P \subseteq \mathbb{N}$ there is $m \in \mathbb{N}$ such that for all $x \in \mathbb{N}$: $x \in P$ if and only if $(x, m) \in R$. Show that R is not number theoretic.

17. Let n be the smallest number that cannot be defined with an English sentence which has at most one thousand letters. What can you say about the number n? What about the smallest natural number that cannot be defined with an L_{exp}-formula with at most one thousand symbols?

18. Prove that if a 2-place relation R is definable in $\mathcal{N}_{exp}$, then also the set $P = \{a + b : (a, b) \in R\}$ is definable in $\mathcal{N}_{exp}$.

19. A formula ψ of number theory is a fixed-point of a formula φ of number theory if for all $s : \mathbb{N} \to \mathcal{N}_{exp}$ we have $\mathcal{N}_{exp} \models_s \psi \iff \mathcal{N}_{exp} \models_s \varphi(\underline{\ulcorner\psi\urcorner}/v_0)$. Give an example of a fixed-point for the formula $\approx v_0v_0$. What about $\neg \approx v_0v_0$?

20. Suppose $f : \mathbb{N} \to \mathbb{N}$ is recursive. Show that there is an L_{exp}-sentence φ such that $\mathcal{N}_{exp} \models \varphi$ if and only if $f(\ulcorner\varphi\urcorner) = \ulcorner\varphi\urcorner$.

21. Give a function $f : \mathbb{N} \to \mathbb{N}$, which is not definable in $\mathcal{N}_{exp}$.

22. Define the class of *F-functions* as follows:

    (i) The functions Z, S, $+$ and Pr^n_m ovat F-functions,

    (ii) If $f : \mathbb{N} \to \mathbb{N}$ and $g_i : \mathbb{N} \to \mathbb{N}$, $1 \leq i \leq n$, are F-functions then also $h(x_1, ..., x_m) = f(g_1(x_1, ..., x_m), ..., g_n(x_1, ..., x_m))$ is an F-function.

    Show that multiplication is not an F-function (Hint: Investigate the growth rate of multiplication).

23. Show that the set $\{\ulcorner\varphi\urcorner : \mathcal{N}_{exp} \models \varphi, \varphi$ is an L_{exp}-atomic formula$\}$ is primitive recursive.

24. Show that the set $\{\ulcorner\varphi\urcorner : \mathcal{N}_{exp} \models \varphi, \varphi$ is an L_{exp}-formula$\}$ is primitive recursive.

25. A relation $R \subseteq \mathbb{N}^2$ is said to be *recursively enumerable* if the set $\{\pi(x, y) : R(x, y)\}$ is recursively enumerable. Prove that if $f : \mathbb{N} \to \mathbb{N}$ is a function, then the following conditions are equivalent:

    (a) f is recursive.

    (b) The relation $\{(n, f(n)) : n \in \mathbb{N}\}$ is recursive.

(c) The relation $\{(n, f(n)) : n \in \mathbb{N}\}$ is recursively enumerable.

26. Prove that if A and B are non-empty sets, then the following conditions are equivalent:

    (a) Both A and B are recursively enumerable sets.

    (b) $A \times B$ is a recursively enumerable relation.

27. Show that every infinite recursively enumerable contains an infinite recursive set.

28. Suppose $R \subseteq \mathbb{N}^3$ is a recursive relation. Show that the set

$$\{n \in \mathbb{N} : \forall z \leq n \exists y R(n, y, z)\}$$

is recursively enumerable.

29. Suppose the sets $A_n \subseteq \mathbb{N}$, $n \in \mathbb{N}$, are such that the set $\{\pi(m, n) : m \in A_n\}$ is recursively enumerable. Show that the *diagonal intersection*

$$\Delta_{n \in \mathbb{N}} A_n = \{m \in \mathbb{N} : m \in A_n \text{ kaikilla } n \leq m\}$$

is recursively enumerable.

30. Let $f : \mathbb{N} \to \mathbb{N}$ recursive and A is the set of $n \in \mathbb{N}$ for which there exists $> n$ such $m \in \mathbb{N}$ that $f(m) = n$. Show that A is recursively enumerable.

31. Suppose A and B are recursively enumerable sets. Show that the set of n such that $2n + 3m \in B$ for some $m \in A$, is recursively enumerable.

Chapter 6

Further reading

Good textbooks that are more or less similar to the current one, but are broader in scope, are [5] and [6]. A good overview of mathematical logic conveying the basics of the subject through to the 1960s is [14]. For later developments the reader is referred to [1]. For anyone interested in the early development of mathematical logic from Frege to Gödel the book [19] is invaluable.

The material presented above leads naturally to at least two directions of research. The first is *model theory* which aims at classifying models of a given first order theory, and at the same time aims at classifying theories according to what their models look like. Model theory originates in the work of Alfred Tarski and Abraham Robinson. It has developed into a rich and deep area of mathematics with close connections to both algebra and analysis. Recommendable model theory textbooks are [3] and [13].

Another direction of research that deserves to be mentioned is *set theory*. We have learnt above that there are number theoretic statements that the Peano axioms cannot decide. The same holds for the standard Zermelo-Fraenkel axiomatisation of set theory. But with set theory the situation is also a little different. It is not only that specifically drafted sentences can be undecided. There are statements arising directly from mathematical practice that are undecidable. The most notorious is the *Continuum Hypothesis*, the claim that every set of real numbers either permits an injection into natural numbers or surjection onto the real numbers. The proof that the Continuum Hypothesis is independent of the Zermelo-Fraenkel axioms of set theory is much more involved than the proof of Gödel's Incompleteness Theorem. The proof involves the concept of *forcing* introduced by Paul Cohen in 1962. During the last fifty years set theory has developed into a rich and deep field of mathematics. The independence phenomenon is just one feature of set theory. Other important topics are *large cardinals* and so-called *inner models*. Excellent textbooks on set theory are [10] and [11].

Bibliography

[1] *Handbook of mathematical logic.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. Edited by Jon Barwise, With the cooperation of H. J. Keisler, K. Kunen, Y. N. Moschovakis and A. S. Troelstra, Studies in Logic and the Foundations of Mathematics, Vol. 90. 57, 83

[2] George Boole. *An investigation of the laws of thought. On which are founded the mathematical theories of logic and probabilities. Reprint of the 1854 original.* Cambridge: Cambridge University Press, reprint of the 1854 original edition, 2009. 7

[3] C. C. Chang and H. J. Keisler. *Model theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, third edition, 1990. 83

[4] Alonzo Church. A note on the Entscheidungsproblem. *J. Symb. Log.*, 1:40–41, 1936. 28

[5] H.-D. Ebbinghaus, J. Flum, and W. Thomas. *Mathematical logic.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994. Translated from the German by Margit Meßmer. 83

[6] Herbert B. Enderton. *A mathematical introduction to logic.* Harcourt/Academic Press, Burlington, MA, second edition, 2001. 83

[7] Gottlob Frege. Über Sinn und Bedeutung. *Zeitschrift für Philosophie Und Philosophische Kritik*, 100(1):25–50, 1892. Eng. trans. in [**?**]. 7

[8] K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatsh. Math. Phys.*, 37:349–360, 1930. Engl. trans. [9, page 61]. 47

[9] Kurt Gödel. *Collected works. Vol. I.* The Clarendon Press, Oxford University Press, New York, 1986. Publications 1929–1936, With a preface by Solomon Feferman, Edited by Feferman, John W. Dawson, Jr., Warren Goldfarb, Charles Parsons and Robert M. Solovay. 56, 85

[10] Thomas Jech. *Set theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded. 83

[11] Kenneth Kunen. *Set theory*, volume 34 of *Studies in Logic (London)*. College Publications, London, 2011. 83

[12] L. Löwenheim. Über Möglichkeiten im Relativkalkül. *Math. Ann.*, 76:447–470, 1915. Eng. trans. [19, page 228]. 48

[13] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. An introduction. 83

[14] Andrzej Mostowski. Thirty years of foundational studies. Lectures on the development of mathematical logic and the study of the foundations of mathematics in 1930–1964. *Acta Philos. Fenn. Fasc.*, 17:1–180, 1965. 83

[15] C. S. Peirce. On the algebra of logic. A contribution to the philosophy of notation. *Am. J. Math.*, 7:180–202, 1885. 7

[16] Emil L. Post. Introduction to a general theory of elementary propositions. *American Journal of Mathematics*, 43(3):163–185, 1921. 8, 11

[17] Th. Skolem. Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen. Krist. Vid. Selsk. Skr. I, 1920, Nr. 4, 36 S (1922)., 1922. Eng. trans. in [**?**]. 48

[18] Th. Skolem. Über die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines endlichen Axiomensystems. Norsk Mat. Forenings Skr., II. Ser. No.1/12, 73-82 (1933), 1933. Eng. trans. [19, page 252]. 56

[19] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931.* Harvard University Press, Cambridge, Mass., 1967. 83, 86

[20] A. N. Whitehead and B. Russell. Principia Mathematica. Vol. I. Cambridge: University Press. xv, 666 S. 4° (1910)., 1910. 7

[21] L. Wittgenstein. Tractatus logico-philosophicus. With an introduction by B. Russell. New York: Harcourt, Brace & Co., 189 S. (1922)., 1922. 8

[22] Richard Zach. Completeness before post: Bernays, Hilbert, and the development of propositional logic. *The Bulletin of Symbolic Logic*, 5(3):331–366, 1999. 11

Index