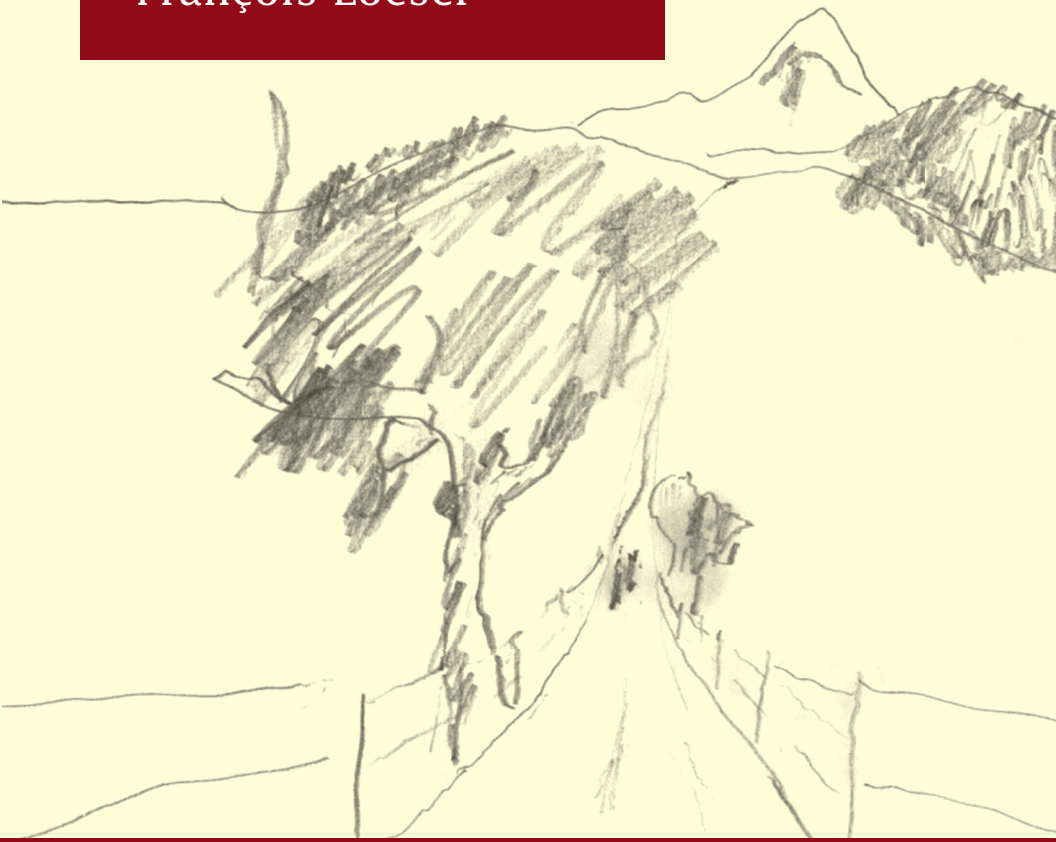
STUDENT MATHEMATICAL LIBRARY
Volume 89

A First Journey through Logic

Martin Hils
François Loeser



AMS American Mathematical Society

A First Journey through Logic

10.1090/stml/089

STUDENT MATHEMATICAL LIBRARY
Volume 89

A First Journey through Logic

Martin Hils
François Loeser

AMS American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 03-01.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-89

Library of Congress Cataloging-in-Publication Data

Names: Hils, Martin, 1973- author. | Loeser, François, author.

Title: A first journey through logic / Martin Hils, François Loeser.

Description: Providence, Rhode Island : American Mathematical Society, [2019] | Series: Student mathematical library ; volume 89 | Includes bibliographical references and index.

Identifiers: LCCN 2019014487 | ISBN 9781470452728 (alk. paper)

Subjects: LCSH: Logic, Symbolic and mathematical–Textbooks. | Mathematics–Textbooks. | AMS: Mathematical logic and foundations – Instructional exposition (textbooks, tutorial papers, etc.). msc Classification:

LCC QA9 .H52445 2019 | DDC 511.3–dc23

LC record available at https://lccn.loc.gov/2019014487

10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

Contents

Introduction

The aim of this book, which originates from a course that we taught successively at École Normale Supérieure (FL in 2007-2010 and MH in 2010-2013), is to present a broad panorama of Mathematical Logic to students who feel curious about this field but have no intent to specialize in it. As a consequence we have deliberately chosen not to write another comprehensive textbook, of which there already exist quite a few excellent ones, but instead to deliver a slim text which provides direct routes to some significant results of general interest.

Our point of view is to treat Logic on an equal footing to any other topic in the mathematical curriculum. Since one does not have to define natural numbers when teaching Number Theory, or sets when teaching Analysis, why should we in a Logic course? For this reason we start the book with a presentation of naive Set Theory, that is, the theory of sets that mathematicians use on a daily basis. It is only in the last chapter that we discuss the Zermelo-Fraenkel axioms, which in fact most mathematicians who are not Set Theorists or teaching a logic course are not so familiar with.

In each chapter we have tried to present at least a few juicy highlights, outside Logic whenever possible, either in the main text, or as exercises or appendices. We consider exercises as an essential component of the book, and we encourage the reader to work them out thoroughly;

they should be seen not only as a tool to check that the course is correctly assimilated, but also as a way to provide an opening to additional topics of interest.

The book is organized as follows. In the first chapter, in addition to the basic theory of ordinal and cardinal numbers, we cover more exotic topics like Goodstein sequences, infinite combinatorics (clubs and Solovay's Theorem) and Hindman's Theorem (a striking result in additive combinatorics). In Chapter 2 we introduce First-order Logic and formal proofs. We prove Gödel Completeness via Henkin witnesses. Craig Interpolation and Beth Definability are treated in exercises. The next chapter delves deeper inside Model Theory, with detailed coverage of Quantifier Elimination. In particular we prove Quantifier Elimination for algebraically closed fields, which allows one to state and prove the Lefschetz Principle in Algebraic Geometry and Ax's Theorem on surjectivity of injective polynomial mappings. Chapter 4 is devoted to basic Recursion Theory and culminates with the existence of universal recursive functions, undecidability of the Halting Problem and Rice's Theorem. In Chapter 5 we prove the classical undecidability and incompleteness results of Tarski and Church and provide a complete proof of Gödel's Second Incompleteness Theorem which we found in Martin Ziegler's book [**13**]. We also present, as an exercise, a theorem of Tennenbaum about the inexistence of non-standard countable recursive models of Peano. Finally in Chapter 6 we develop Axiomatic Set Theory, including the Reflection Principle and some proofs of independence and relative consistency.

This book is intended towards advanced undergraduate students, graduate students at any stage, or working mathematicians, who seek a first exposure to core material of mathematical logic and some of its applications. Prerequisites are minimal: besides familiarity with abstract reasoning and basic mathematical concepts, some acquaintance with General Topology and Algebra, especially Field Theory, is required at various places.

For the interested reader, here are a few suggestions for further reading, providing more comprehensive and advanced material, ordered by increasing difficulty:

Model Theory: The books by Marker [**8**], Poizat [**9**] and Tent-Ziegler [**12**].

Set Theory: The books by Krivine [**6**], Kunen [**7**] and Jech [**5**].

Recursion Theory: The books by Cooper [**1**], Rogers [**10**] and Soare [**11**].

Acknowledgements
We heartfully thank the following colleagues and friends who encouraged us in the project of transforming our notes into a book and/or helped us immensely in improving the text: Martin Bays, Antoine Chambert-Loir, Zoé Chatzidakis, Artem Chernikov, Raf Cluckers, Arthur Forey, Franziska Jahnke, Silvain Rideau, Pierre Simon. Moreover, we thank Christian Maurer who provided the drawing for the book cover.

During the preparation of this book the first author was partially supported by ANR through ValCoMo (ANR-13-BS01-0006) and by DFG through SFB 878 and the second author was partially supported by ANR through Défigéo (ANR-15-CE40-0008) and by the Institut Universitaire de France.

10.1090/stml/089/01

Chapter 1

Counting to Infinity

Introduction

The general purpose of this chapter is to provide tools for comparing sizes of infinities. To this aim we develop in 1.3-1.6 the notion of *ordinals* which constitute a natural infinite extension of natural numbers. Ordinals classify well-ordered sets and are a natural device for using transfinite induction. A fundamental and very useful fact is that ordinals are endowed with arithmetic operations extending those of natural numbers, even though some classical properties do not extend (for instance addition of ordinals is no longer commutative).

Building on the notion of ordinals, we develop in 1.7-1.10 the concept of *cardinals*, which is the right notion to compare the size of sets. Unlike the case of ordinals, one needs to assume the validity of the Axiom of Choice (which we discuss in 1.7) to develop a full fledged theory of cardinals. In the last sections of this chapter, we study cardinal arithmetic, which appears to have a much richer theory of exponentation than ordinal arithmetic.

1.1. Naive Set Theory

In this chapter we shall use the notions of *set* and *natural number* in the same way as in any mathematical textbook, that is, in a naive sense,

without further questioning. It is only in the last chapter that we shall introduce the classical ZFC system of axioms of Zermelo-Fraenkel (plus the Axiom of Choice). We shall see that the notions and results of this first chapter remain valid in the more formal *axiomatic Set Theory*, using only the axioms of ZFC. We shall thus develop Cantor's theory of ordinal and cardinal numbers from this naive point of view.

When A and B are sets, we denote by $A \cup B$, $A \cap B$ and by $A \setminus B$ their set-theoretic *union*, *intersection* and *difference*, respectively. More generally, if I is a set and $(A_i)_{i \in I}$ is a family of sets indexed by I, we denote its union by $\bigcup_{i \in I} A_i$ and its intersection by $\bigcap_{i \in I} A_i$; thus we have $x \in \bigcup_{i \in I} A_i$ if and only $x \in A_i$ for some $i \in I$ and $x \in \bigcap_{i \in I} A_i$ if and only $x \in A_i$ for every $i \in I$.

We write $A \subseteq B$ if A is a *subset* of B, and $A \subset B$ if A is a *proper subset* of B. The *power set* of A is denoted by $\mathcal{P}(A)$. It is the set of subsets of A; thus $C \in \mathcal{P}(A)$ if and only if $C \subseteq A$.

We denote by $\mathbb{N}$ the set $\{0, 1, 2, ...\}$ of natural numbers, and we write $\mathbb{N}^*$ for $\mathbb{N} \setminus \{0\}$.

We will make constant use of the *extensionality principle* according to which two sets containing the same elements are equal.

We shall also make use of the *comprehension principle* which states that given a set A and a property P of sets, there exists a set whose elements are exactly those elements of A that satisfy property P. We defer to Section 6.2 for a more precise formulation.

1.2. The Cantor and Cantor-Bernstein Theorems

The existence of an injective, surjective or bijective function between two sets may be seen as a way to compare their "size". We start with two results going in that direction.

Theorem 1.2.1 (Cantor). *Let A be a set. There is no surjection $A \to \mathcal{P}(A)$.*

Proof. Let $f : A \to \mathcal{P}(A)$ be a map. Consider the set

$$B = \{x \in A \mid x \notin f(x)\}.$$

For every $x \in A$ with $f(x) = B$, we have $x \in B$ if and only if $x \notin B$. Hence B does not belong to the image of f. □

Theorem 1.2.2 (Cantor-Bernstein). *Let A and B be sets, and let $f : A \to B$ and $g : B \to A$ be injective maps. Then there exists a bijection $h : B \to A$.*

Proof. We may assume A is a subset of B and f is the inclusion map. Indeed, one may replace A by $f(A)$ and g by $f \circ g$. Now set $C = \{g^n(x) \mid n \in \mathbb{N},\ x \in B \setminus A\}$. Define a map $h : B \to A$ by $h(c) = g(c)$ when $c \in C$ and $h(x) = x$ when $x \in B \setminus C$. The map h is surjective: indeed, any $x \in A \cap C$ is of the form $x = g(y)$ for some $y \in C$ and for any $x \in A \setminus C$, $x = h(x)$. It is also clearly injective. □

Definition. Let X and Y be sets. One says that X and Y are *equinumerous*, and writes $X \sim Y$, if there exists a bijection between X and Y; one says X is *subnumerous* to Y, and writes $X \preccurlyeq Y$, if there exists an injection $X \to Y$.

Using this terminology, the Cantor-Bernstein Theorem may be restated as: if $X \preccurlyeq Y$ and $Y \preccurlyeq X$, then $X \sim Y$.

1.3. Orders

This section and the next one are devoted to preliminary results on ordered sets that are needed to develop the theory of ordinals.

Definition. A *partial order* $<$ on a set X is a binary relation (that is, given by a subset of $X \times X$) which is *transitive* (if $x < y$ and $y < z$ then $x < z$) and *antireflexive* ($x \not< x$). If furthermore, for every $x, y \in X$ one has $x < y$, $x = y$ or $y < x$, one says $<$ is a *total order*.

One writes $x \leq y$ to mean $x < y$ or $x = y$, $x > y$ for $y < x$, and $x \geq y$ for $y \leq x$.

If $Y \subseteq X$, $y \in Y$ is a *smallest element* if for every y' in Y, $y \leq y'$. It is a *minimal element* if for every y' in Y, $y' \not< y$. One similarly defines a *largest element* and a *maximal element*. A *lower bound* of Y is an element of X which is $\leq$ all elements in Y. An *infimum* of Y is a largest element in the set of lower bounds of Y. One similarly defines the notion of *upper bound* and *supremum*.

Note that in a partial order, if $a \leq b$ and $b \leq a$ then $a = b$. Thus smallest and largest elements are unique, which is in general not the case for minimal or maximal elements.

Remark 1.3.1. If $<$ is a partial order, $\leq$ is a *reflexive* relation ($x \leq x$ for every $x \in X$), transitive and *antisymmetric* (if $x \leq y$ and $y \leq x$ then $x = y$).

Conversely, if $\leq$ is a binary relation on a set X which is reflexive, transitive and antisymmetric then the relation $<$ defined by $x < y :\Leftrightarrow (x \leq y \text{ and } x \neq y)$ is a partial order on X.

Proof. Exercise. □

Definition.

(1) Let $<$ be a partial order on X. We say $<$ is *well-founded* if any non-empty subset of X contains a minimal element.

(2) A *well-order* is a well-founded total order.

Remark 1.3.2. Let $<$ be a partial order on X.

(1) The map $a \mapsto X_{\leq a} = \{x \in X \mid x \leq a\}$ identifies $(X, <)$ with a subset Y of $\mathcal{P}(X)$ endowed with the partial order induced by $\subset$.

(2) $<$ is well-founded if and only if there is no infinite decreasing sequence in X.

(3) $<$ is a well-order if and only if every non-empty subset of X contains a smallest element.

Proof. The proofs of (1) and (3) are left as exercises.

Let us prove (2). If $(X, <)$ is not well-founded, there exists a subset $\emptyset \neq Y \subseteq X$ without minimal element. By induction on $n \in \mathbb{N}$ one may construct $y_n \in Y$ such that $y_{n+1} < y_n$. Conversely, if $(y_n)_{n\in\mathbb{N}}$ is a decreasing sequence, it is clear that $Y = \{y_n \mid n \in \mathbb{N}\}$ does not contain a minimal element. □

Example 1.3.3.

(1) The usual order $<$ on $\mathbb{Z}$ is a non-well-founded total order. Its restriction to $\mathbb{N}$ is a well-order.

(2) For every set X, the relation $\subset$ is a partial order on $\mathcal{P}(X)$ which is well-founded if and only if X is finite.[1]

(3) The restriction of a partial order (resp. total, well-founded) on X to $Y \subseteq X$ is a partial order (resp. total, well-founded) on Y.

1.4. Operations on Orders

Definition. Let X and Y be partially ordered sets.

(1) The *ordered sum* of X and Y, denoted by $X + Y$, is the partially ordered set consisting of pairs $(x, 0)$ with $x \in X$ and $(y, 1)$ with $y \in Y$, the order being defined as follows: $(a, i) < (b, j)$ if $i < j$ or if $i = j$ and $a < b$.

(2) The *reverse lexicographic product* of X and Y is defined by endowing the cartesian product $X \times Y$ with the order: $(x, y) < (x', y')$ if $y < y'$ or if $y = y'$ and $x < x'$. It is still denoted by $X \times Y$.

By an *isomorphism* between two partially ordered sets X and Y we mean a bijection f between X and Y such that for any $x, x' \in X$ one has $x < x'$ if and only if $f(x) < f(x')$.

Lemma 1.4.1.

(1) *The ordered sum of total orders* (*resp. well-founded partial orders*) *is a total order* (*resp. well-founded*).

(2) *The reverse lexicographic product of two total orders* (*resp. well-founded partial orders*) *is a total order* (*resp. well-founded*).

(3) *Let X, Y and Z be partially ordered. We have the following canonical isomorphisms of partially ordered sets:*
   (a) $(X + Y) + Z \cong X + (Y + Z)$.
   (b) $(X \times Y) \times Z \cong X \times (Y \times Z)$.
   (c) $X \times (Y + Z) \cong (X \times Y) + (X \times Z)$.

Proof. The only non-trivial point to check is that the reverse lexicographic product of two well-founded partially ordered sets is well-founded.

[1] By a *finite* set we mean a set into which $\mathbb{N}$ does not inject.

Let X and Y be two well-founded partially ordered sets. Let Z be a non-empty subset of $X \times Y$. We denote by $\pi : X \times Y \to Y$ the projection on the second factor. The order on Y being well-founded, there exists a minimal element y_0 in $\pi(Z) \subseteq Y$. Since the order on X is well-founded, there is a minimal element x_0 in the (non-empty) set $Z_{y_0} = \{x \in X \mid (x, y_0) \in Z\}$. It is clear that (x_0, y_0) is minimal in Z. □

Definition. Let X and Y be totally ordered sets. We assume that X admits a smallest element 0. One defines the partially ordered set $X^{(Y)}$ as follows. As a set, it is the set of functions from Y to X with finite support, that is, the subset of the set X^Y of all functions $Y \to X$ consisting of functions $f : Y \to X$ such that

$$\mathrm{supp}(f) := \{y \in Y \mid f(y) \neq 0\}$$

is finite. One sets $f < g$ if there exists $y \in Y$ such that $f(y) < g(y)$ and $f(y') = g(y')$ for every $y' > y$.

Proposition 1.4.2. *Let X, Y and Z be totally ordered sets, and assume that X admits a smallest element* 0.

(1) *The relation $<$ defines a total order on $X^{(Y)}$ which is well-founded when the orders on X and Y are both well-founded.*

(2) *There are canonical isomorphisms of totally ordered sets $X^{(Y+Z)} \cong X^{(Y)} \times X^{(Z)}$ and $X^{(Y \times Z)} \cong \left(X^{(Y)}\right)^{(Z)}$.*

Proof. The only non-trivial point to check is that if X and Y are well-ordered, then $X^{(Y)}$ is well-founded. Let Z be a non-empty subset of $X^{(Y)}$. Let us prove that Z contains a smallest element. If the constant function with value 0 belongs to Z, there is nothing to prove. Hence, we may assume $\mathrm{supp}(f) \neq \emptyset$ for every $f \in Z$. Let

$$Y_1 = \{s_1(f) \mid f \in Z\},$$

where $s_1(f) = \max(\mathrm{supp}(f))$. Let y_1 be the smallest element of Y_1, and set $Z_1' = \{f \in Z \mid s_1(f) = y_1\}$. The set Z_1' is an *initial segment* of Z, in other words $f < g$ for every $f \in Z_1'$ and $g \in Z \setminus Z_1'$. Let x_1 be the smallest element of $\{f(y_1) \mid f \in Z_1'\}$. We set

$$Z_1 = \{f \in Z_1' \mid f(y_1) = x_1\}.$$

The set Z_1 is an initial segment of Z_1'. If Z_1 contains the function with constant value 0 outside $\{y_1\}$, we are done. Otherwise, we have $\mathrm{supp}(f) \setminus \{y_1\} \neq \emptyset$ for every $f \in Z_1$. Let $Y_2 = \{s_2(f) \mid f \in Z_1\}$, where $s_2(f) = \max(\mathrm{supp}(f) \setminus \{y_1\})$. Let y_2 be the smallest element of Y_2, and x_2 the smallest element of $\{f(y_2) \mid f \in Z_1 \text{ and } y_2 = s_2(f)\}$. We set $Z_2 = \{f \in Z_1 \mid s_2(f) = y_2 \text{ and } f(y_2) = x_2\}$. It is an initial segment of Z_1. If Z_2 contains the function with constant value 0 outside $\{y_1, y_2\}$, we are done, otherwise one continues in the same way, constructing Y_3, y_3, Z_3', x_3, Z_3 and so on. Since the sequence (y_i) is strictly decreasing in Y, this process stops after a finite number of steps. □

1.5. Ordinal Numbers

A set X is said to be *transitive* if for all $x \in X$ and $y \in x$ one has $y \in X$. This is equivalent to $x \in X \Rightarrow x \subseteq X$.

Definition. A set X is an *ordinal* if it is transitive and if the relation $\{(x, y) \in X \times X \mid x \in y\}$ on X defines a well-order on X.

Proposition 1.5.1. *Let α and β be ordinals.*

(1) *$\emptyset$ is an ordinal.*

(2) *If $\alpha \neq \emptyset$, then $\emptyset \in \alpha$.*

(3) *$\alpha \notin \alpha$.*

(4) *If $x \in \alpha$, then $x = S_{<x} := \{y \in \alpha \mid y < x\}$.*

(5) *If $x \in \alpha$, then x is an ordinal.*

(6) *$\beta \subseteq \alpha$ if and only if $\beta \in \alpha$ or $\beta = \alpha$.*

(7) *$x := \alpha \cup \{\alpha\}$ is an ordinal, denoted by α^+.*

Proof. (1) is clear. For (2), one considers $x \in \alpha$ minimal. If $y \in x$, then $y \in \alpha$ by transitivity of α, and x would not be minimal. In (3), by antireflexivity, we have $x \notin x$ for every $x \in \alpha$. Thus $\alpha \in \alpha$ implies $\alpha \notin \alpha$. (4) follows from the fact that $<$ is given by $\in$. To prove (5), note that $\in$ restricts to a well-order on x, since $x \subseteq \alpha$. Furthermore, $x = S_{<x}$ is transitive, since $z \in y \in x \Rightarrow z < x \Rightarrow z \in S_{<x}$.

To prove the 'only if' part in (6), let us assume that $\beta \subset \alpha$. Let x be minimal in $\alpha \setminus \beta$. Clearly $\beta \supseteq S_{<x}$ by minimality. Furthermore, if

$y \in \beta$, then $y \in x$ since otherwise $x \in y$ and $x \in \beta$. Hence $\beta = S_{<x} = x \in \alpha$. The other implication in (6) is clear, and the verification of (7) is immediate. □

Proposition 1.5.2. *Let X be a non-empty set of ordinals. Then $\bigcap_{\alpha\in X} \alpha$ is a smallest element of X.*

Proof. The intersection of a family of transitive sets is transitive, and the restriction of a well-order to a subset is a well-order. Hence $\beta = \bigcap_{\alpha\in X} \alpha$ is an ordinal. We have $\beta \subseteq \alpha$ for every $\alpha \in X$. If $\beta \notin X$, then $\beta \in \alpha$ for every $\alpha \in X$, by Proposition 1.5.1(6). It follows that $\beta \in \beta$, which is absurd. □

Theorem 1.5.3. *Let α and β be ordinals. Exactly one of the following properties holds:*

$$(1)\ \alpha \in \beta, \qquad (2)\ \alpha = \beta, \qquad (3)\ \beta \in \alpha.$$

Proof. One sets $X = \{\alpha, \beta\}$, and one applies Proposition 1.5.2. If $\alpha \cap \beta = \alpha$, then $\alpha \subseteq \beta$, hence $\alpha = \beta$ or $\alpha \in \beta$ by Proposition 1.5.1(6). Similarly, if $\alpha \cap \beta = \beta$, then $\alpha = \beta$ or $\beta \in \alpha$. The fact that these properties are mutually exclusive follows from the axioms of a partial order. □

Notation. From now on, we shall write $\alpha < \beta$ for $\alpha \in \beta$, and $\alpha \leq \beta$ for $\alpha \subseteq \beta$, when α and β are ordinals.

Proposition 1.5.4. *Let X be a set of ordinals. Then $b = \bigcup_{\alpha\in X} \alpha$ is an ordinal. Furthermore, if γ is an ordinal with $\gamma < b$, there exists $\alpha \in X$ such that $\gamma \in \alpha$. We shall also write $b = \sup_{\alpha\in X} \alpha$.*

Proof. The set b being the union of transitive sets, it is transitive. Furthermore, b contains only ordinals. By Theorem 1.5.3, $\in$ induces a total order on b. If $\emptyset \neq Z \subseteq b$, then $\bigcap_{\alpha\in Z} \alpha$ is a smallest element of Z by Proposition 1.5.2. This shows that the order given by $\in$ on b is well-founded. □

An ordinal of the form α^+ is called *a successor ordinal*. It is clear that α^+ is the smallest ordinal $> \alpha$.

Definition. A *limit ordinal* is a non-empty ordinal which is not a successor.

Proposition 1.5.5. *For an ordinal $\lambda \neq \emptyset$, the following conditions are equivalent:*

(1) *λ is a limit ordinal;*

(2) *$\lambda = \bigcup_{\alpha<\lambda} \alpha$.*

Proof. (1)⇒(2). Let $\beta = \bigcup_{\alpha<\lambda} \alpha$ and λ a limit. It is clear that $\beta \subseteq \lambda$. Conversely, assume $\alpha < \lambda$. Then $\alpha^+ \leq \lambda$ and it follows that $\alpha^+ < \lambda$ since λ is a limit ordinal. The statement follows, since $\alpha \in \alpha^+ \subseteq \beta$.

(2)⇒(1). If $\lambda = \gamma^+$, then $\bigcup_{\alpha<\lambda} \alpha = \bigcup_{\alpha\leq\gamma} \alpha = \gamma < \lambda$. □

Example 1.5.6.

(1) One can recover the *natural numbers as ordinals* as follows. One sets $\underline{0} := \emptyset$, and inductively $\underline{n+1} := \underline{n}^+$ for $n \in \mathbb{N}$. For instance $\underline{1} = \{\emptyset\}$, $\underline{2} = \{\underline{0}, \underline{1}\} = \{\emptyset, \{\emptyset\}\}$, $\underline{3} = \{\underline{0}, \underline{1}, \underline{2}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

One proves by induction that $\underline{n}$ is an ordinal for every natural number n. We shall often identify $\underline{n}$ and n.

(2) One sets $\omega := \bigcup_{n\in\mathbb{N}} \underline{n}$. It is an ordinal by Proposition 1.5.4.

Definition. One says that an ordinal is *finite* if it is not a limit and none of its elements is a limit.

Proposition 1.5.7.

(1) *ω is the set of finite ordinals.*

(2) *ω is the smallest limit ordinal.*

Proof. One proves first, by induction on $n \in \mathbb{N}$, that all elements of ω are finite ordinals. Furthermore, $\alpha < \omega$ implies $\alpha^+ < \omega$. This proves (2). If $\alpha \notin \omega$, then $\omega \leq \alpha$, so either $\alpha = \omega$ or $\omega \in \alpha$. In both cases, α is not finite. This proves (1). □

Lemma 1.5.8. *Let $f : \alpha \to \alpha'$ be a strictly increasing map between two ordinals. Then $f(\beta) \geq \beta$ for every $\beta \in \alpha$. In particular, $\alpha \leq \alpha'$, and if f is an isomorphism of ordered sets, then $\alpha = \alpha'$ and f is equal to the identity.*

Proof. If there exists $\beta \in \alpha$ with $f(\beta) < \beta$, we consider β_0 minimal with that property. Since f is strictly increasing, we have $f(f(\beta_0)) < f(\beta_0)$, which contradicts minimality.

The statement about an isomorphism f follows by applying the result to f as well as to f^{-1}. □

Theorem 1.5.9 (Classification of well-orders by ordinals)**.** *Every well-ordered set X is isomorphic, as an ordered set, to some ordinal. Furthermore, the ordinal and the isomorphism are both unique.*

Proof. Uniqueness follows from Lemma 1.5.8. To prove existence, let us first note that for every $x \in X$, any isomorphism between $S_{<x}$ and an ordinal α can be extended to an isomorphism between $S_{\leq x} = S_{<x} \cup \{x\}$ and α^+. Let

$$Y = \{y \in X \mid \text{ there exists } f : S_{\leq y} \cong \alpha \text{ for some ordinal } \alpha\}.$$

By uniqueness, for $y \in Y$, the ordinal $\alpha = \alpha(y)$ and the isomorphism $f = f_y$ are unique. Let us prove $Y = X$. Otherwise, there would exist $x \in X$ minimal in $X \setminus Y$. For $y < x$ we have an isomorphism $f_y : S_{\leq y} \cong \alpha(y)$. Furthermore, these isomorphisms form a coherent family in the sense that for every $y' < y < x$ we have $f_y \restriction_{S_{\leq y'}} = f_{y'}$. (To see this, note that an initial segment of an ordinal is an ordinal.) We set

$$\alpha = \sup_{y<x} \alpha(y) \text{ and } f : S_{<x} \to \alpha,\ f(y) := f_y(y).$$

It is clear that f is well defined and induces an isomorphism of ordered sets between $S_{<x}$ and α. By the observation made at the beginning, f may be extended to an isomorphism between $S_{\leq x}$ and α^+, which leads to a contradiction. So we have $Y = X$. To conclude, one uses the same kind of argument, setting $\alpha(X) := \sup_{x \in X} \alpha(x)$ and $f : X \cong \alpha(X)$, $x \mapsto f_x(x)$. □

Remark 1.5.10 (Transfinite induction)**.** Let P be a property of ordinals. One assumes:

- $\emptyset$ satisfies P;
- for every ordinal α: if α satisfies P, then α^+ satisfies P;
- for every limit ordinal λ: if every $\alpha < \lambda$ satisfies P, then λ satisfies P.

Then every ordinal satisfies P.

1.6. Ordinal Arithmetic

If α and β are ordinals, by Theorem 1.5.9 there is a unique ordinal isomorphic to the ordered sum of α and β, which one denotes by $\alpha+\beta$. One similarly defines $\alpha\beta$ as the unique ordinal isomorphic to the reverse lexicographic product $\alpha\times\beta$ and α^β as the unique ordinal isomorphic to the ordered set $\alpha^{(\beta)}$. Note that 0^β has still to be defined: one sets $0^0 := 1$ and $0^\beta := 0$ for every $\beta > 0$.

Proposition 1.6.1 (Ordinal addition)**.** *Let α, β and γ be ordinals.*

(1) $\alpha + 0 = 0 + \alpha = \alpha$.

(2) $\alpha + 1 = \alpha^+$.

(3) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, *in particular* $\alpha + \beta^+ = (\alpha + \beta)^+$.

(4) $\alpha < \beta$ *if and only if there exists an ordinal* $\delta > 0$ *such that* $\beta = \alpha + \delta$.

(5) *If* $\beta < \gamma$, *then* $\alpha + \beta < \alpha + \gamma$ *for every* α. *In particular, one may simplify on the left:* $\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$.

(6) *If* λ *is a limit, then* $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$ (*continuity*).

(7) $1 + \alpha = \alpha + 1$ *when* α *is finite, otherwise* $1 + \alpha = \alpha$.

Proof. (1) and (2) are clear, and (3) follows from Lemma 1.4.1. For the non-trivial implication in (4), one easily checks that the ordinal δ isomorphic to the well-ordered set $\beta \setminus \alpha$ does the job.

(5) If $\beta < \gamma$, by (2) and (4) one has $\gamma = \beta+\delta$, hence $\alpha+\gamma = (\alpha+\beta)+\delta$, for some $\delta > 0$.

(6) $\alpha + \lambda \geq \sup_{\beta<\lambda}(\alpha + \beta)$ follows from (5). Conversely, suppose $\alpha \leq \mu < \alpha + \lambda$. Then $\mu = \alpha + \delta$ for some δ with $0 \leq \delta < \lambda$. Since λ is a limit, one has $\delta^+ < \lambda$, hence $\mu < \alpha + \delta^+ \leq \sup_{\beta<\lambda}(\alpha + \beta)$.

(7) One proves by induction on $n \in \mathbb{N}$ that $1 + n = n + 1$. By (6) we have $1 + \omega = \omega$. Finally, $\alpha \geq \omega$ can be written as $\alpha = \omega + \beta$, hence $1 + \alpha = 1 + \omega + \beta = \omega + \beta = \alpha$. □

From now on, we shall allow the omission of parentheses, using the convention that exponentiation ties are stronger than multiplication and

that multiplication ties are stronger than addition. For instance, one should read $\alpha\beta + \gamma$ as $(\alpha\beta) + \gamma$, and $\gamma\alpha^\beta$ as $\gamma\left(\alpha^\beta\right)$.

Proposition 1.6.2 (Ordinal multiplication)**.** *Let α, β, γ be ordinals.*

(1) $\alpha 0 = 0\alpha = 0$.

(2) $\alpha 1 = 1\alpha = \alpha$.

(3) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(4) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$, *in particular* $\alpha\beta^+ = \alpha\beta + \alpha$.

(5) $2\omega = \omega < \omega 2 = \omega + \omega$.

(6) *Assume $\alpha \neq 0$. If $\beta < \gamma$, then $\alpha\beta < \alpha\gamma$. In particular, one may simplify on the left: $\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma$.*

(7) *If λ is a limit ordinal, then $\alpha\lambda = \sup_{\beta<\lambda} \alpha\beta$ (continuity).*

Proof. (1) and (2) are clear, (3) and (4) follow from Lemma 1.4.1. For (6), it suffices to note that if $\beta < \gamma$ then $\gamma = \beta + \delta$ for some $\delta > 0$, hence $\alpha\gamma = \alpha\beta + \alpha\delta$ by (4) from which it follows that $\alpha\gamma > \alpha\beta$.

(7) One may assume $\alpha \neq 0$. Let λ be a limit ordinal. The inequality $\alpha\lambda \geq \sup_{\beta<\lambda} \alpha\beta =: \delta$ follows from (6). Conversely, let $\gamma < \alpha\lambda$. Euclidean division, proved in the next lemma, provides a pair of ordinals (ρ, μ) such that $\gamma = \alpha\mu + \rho$, with $\rho < \alpha$. Since $\mu < \lambda$ by (6), we have $\mu^+ < \lambda$ because λ is a limit ordinal, hence $\gamma = \alpha\mu + \rho < \alpha\mu + \alpha = \alpha\mu^+ \leq \delta$. In (5), $2\omega = \omega$ follows from (7), the other statements being clear. □

Lemma 1.6.3 (Euclidean division)**.** *Let α and β be ordinals, with $\alpha \neq 0$. Then there exists a unique pair of ordinals (ρ, μ) such that $\rho < \alpha$ and $\beta = \alpha\mu + \rho$.*

Proof. Uniqueness: Assume $\alpha\mu + \rho = \alpha\mu' + \rho'$ with $\rho, \rho' < \alpha$. If $\mu < \mu'$, then $\alpha\mu + \rho < \alpha\mu^+ \leq \alpha\mu' \leq \alpha\mu' + \rho'$, which is absurd. Hence $\mu = \mu'$ by symmetry, and one obtains $\rho = \rho'$ after simplifying.

Existence: When $\beta = 0$ there is nothing to prove. Assume $\beta \neq 0$. The mapping $f_0 : \beta \to \alpha \times \beta$, $x \mapsto (0, x)$ is strictly increasing, hence $\beta \leq \alpha\beta$ by Lemma 1.5.8. If $\beta = \alpha\beta$, one sets $\mu = \beta$ and $\rho = 0$. Otherwise, we have $\beta \in \alpha\beta$. Let f be the unique isomorphism of ordered sets between $\alpha\beta$ and $\alpha \times \beta$. One sets $(\rho, \mu) = f(\beta)$. Since $S_{<(\rho,\mu)} \cong (\alpha \times \mu) + \rho$ it follows that $\beta = \alpha\mu + \rho$. □

Note that we have only used properties (1)–(4) and (6) from Proposition 1.6.2 in our proof of Euclidean division, thus avoiding circularity.

Proposition 1.6.4 (Ordinal exponentiation)**.** *Let α, β, γ be ordinals.*

(1) *For every α, we have $\alpha^0 = 1$, $\alpha^1 = \alpha$ and $1^\alpha = 1$. If $\alpha \neq 0$, then $0^\alpha = 0$.*

(2) $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$, *in particular* $\alpha^{\beta^+} = \alpha^\beta \alpha$.

(3) $\left(\alpha^\beta\right)^\gamma = \alpha^{\beta\gamma}$.

(4) *If $\alpha > 1$ and $\beta < \gamma$, then $\alpha^\beta < \alpha^\gamma$.*

(5) *If λ is a limit ordinal and $\alpha \neq 0$, then $\alpha^\lambda = \sup_{\beta<\lambda} \alpha^\beta$ (continuity).*

Proof. (1) is checked directly, and statements (2) and (3) follow from Proposition 1.4.2.

(4) $\beta < \gamma \Rightarrow \gamma = \beta + \delta$ for some $\delta > 0$. Hence $\alpha^\gamma = \alpha^{\beta+\delta} = \alpha^\beta \alpha^\delta$. But $\alpha^\delta > 1$ since as a set $\alpha^{(\delta)}$ contains at least two elements. It follows that $\alpha^\gamma > \alpha^\beta$ by Proposition 1.6.2(6).

Let us prove the non-trivial inequality in (5). Let $f \in \alpha^{(\lambda)}$. One may assume f is not the constant function with value 0. Then $s_1(f) < \lambda$, and hence $\beta = s_1(f)^+ < \lambda$, which proves there exists a strictly increasing function $S_{\leq f} \to \alpha^{(\beta)}$. One concludes by Lemma 1.5.8. □

Remark 1.6.5. The following formulas would allow us to define ordinal addition, multiplication and exponentiation by transfinite induction:

- $\alpha + 0 = \alpha$, $\alpha + \beta^+ = (\alpha + \beta)^+$, and $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$ for λ a limit ordinal.
- $\alpha 0 = 0$, $\alpha\beta^+ = \alpha\beta + \alpha$, and $\alpha\lambda = \sup_{\beta<\lambda}(\alpha\beta)$ for λ a limit ordinal.
- Assume $\alpha \neq 0$. Then one has $\alpha^0 = 1$, $\alpha^{\beta^+} = \alpha^\beta \alpha$, and $\alpha^\lambda = \sup_{\beta<\lambda}\left(\alpha^\beta\right)$ for λ a limit ordinal.

1.7. The Axiom of Choice

Given a family of sets $(X_i)_{i\in I}$, one defines their *product* as

$$\prod_{i\in I} X_i = \left\{ f : I \to \bigcup_{i\in I} X_i \;\middle|\; f(i) \in X_i \text{ for all } i \in I \right\}.$$

Definition. The *Axiom of Choice* (AC) states that the product of a family of non-empty sets is non-empty: if $X_i \neq \emptyset$ for all $i \in I$, then $\prod_{i\in I} X_i \neq \emptyset$.

In the Zermelo-Fraenkel system of axioms ZF, (AC) is equivalent to *Zorn's Lemma* and also to *Zermelo's Theorem*. We shall prove these equivalences in the last chapter of this book, and accept them for the moment.

Definition. A partially ordered set X is *inductive* if any totally ordered subset $Y \subseteq X$ admits an upper bound in X. (In particular, such an X is non-empty).

Zorn's Lemma. Every inductive partially ordered set admits a maximal element.

Zermelo's Theorem (Wohlordnungssatz)**.** Every set can be well-ordered.

1.8. Cardinal Numbers

We now assume, until the end of the penultimate chapter, that the Axiom of Choice holds.

Definition. An ordinal is a *cardinal* if it is not equinumerous to a smaller ordinal.

Example 1.8.1.

(1) Any finite ordinal is a cardinal.

(2) The ordinal ω is a cardinal. When considered as a cardinal it will be denoted by $\aleph_0$.

(3) If α is an infinite ordinal, then α^+ is not a cardinal. (Indeed, α^+ and α are equinumerous.)

Proposition 1.8.2. *Any set X is equinumerous to a unique cardinal, denoted by* $\mathrm{card}(X)$.

Proof. By Zermelo's Theorem and Theorem 1.5.9, X is equinumerous to an ordinal α. Let $\beta \leq \alpha$ be minimal such that β is equinumerous to α. Then β is a cardinal and is in bijection with X. Uniqueness is clear. □

Proposition 1.8.3. *Let X and Y be sets and assume that X is non-empty. The following statements are equivalent:*

(1) $\mathrm{card}(X) \leq \mathrm{card}(Y)$.

(2) *There exists an injective map $X \to Y$.*

(3) *There exists a surjective map $Y \to X$.*

Proof. (1)⇒(2) is easy.

(2)⇒(3): Let $f : X \to Y$ be an injective map. As X is non-empty, one may fix $x_0 \in X$. One defines a surjective map $g : Y \to X$ by setting $g(y) := x_0$ if $y \notin \mathrm{im}(f) = \{f(x) \mid x \in X\}$, and $g(y) := f^{-1}(y)$ otherwise.

(3)⇒(1): If there exists a surjective map $Y \to X$, then there exists a surjection $g : \lambda = \mathrm{card}(Y) \to \kappa = \mathrm{card}(X)$. The map f sending $\alpha \in \kappa$ to the minimal $\beta \in \lambda$ such that $g(\beta) = \alpha$ provides an injection $\kappa \to \lambda$. In particular, κ is in bijection with some ordinal $\gamma \leq \lambda$. (One takes γ as the unique ordinal which is isomorphic to the well-order induced on $\mathrm{im}(f)$.) □

Definition. A set X is said to be *countable* if $\mathrm{card}(X) \leq \aleph_0$, and *finite* if $\mathrm{card}(X) < \aleph_0$.

Proposition 1.8.4. *Let X be a set of cardinals. Then $\lambda = \sup_{\kappa \in X} \kappa$ is a cardinal.*

Proof. If $\alpha < \lambda$, then $\alpha < \kappa$ for some $\kappa \in X$. Since κ is a cardinal, we have $\kappa = \mathrm{card}(\kappa) \leq \mathrm{card}(\lambda)$, and hence $\alpha < \mathrm{card}(\lambda)$. This proves that λ is not equinumerous to some smaller ordinal. □

Notation. From now on, κ, λ, etc. will denote cardinals.

There is no largest cardinal. Indeed, if κ is a cardinal, then $\lambda := \mathrm{card}(\mathcal{P}(\kappa)) > \kappa$ by Cantor's Theorem. In particular, the set of all cardinals $\leq \lambda$ that are $> \kappa$ is non-empty. We denote by κ^+ its smallest element, called the *cardinal successor* of κ. To avoid confusion, from now on the ordinal successor of α will be denoted by $\alpha + 1$.

Definition. The $\aleph$-*hierarchy* assigns to any ordinal a cardinal as follows:

- $\aleph_0 := \omega$.
- $\aleph_{\alpha+1} := \aleph_\alpha^+$.
- $\aleph_\alpha := \sup_{\beta<\alpha} \aleph_\beta$, if α is a limit ordinal.

By transfinite induction, one proves that $\alpha < \beta \Rightarrow \aleph_\alpha < \aleph_\beta$. In combination with the next result, it follows that the $\aleph$-hierarchy provides a strictly increasing enumeration of the infinite cardinals by the ordinals.

Proposition 1.8.5. *Every infinite cardinal is of the form $\aleph_\alpha$ for some α.*

Proof. Let κ be an infinite cardinal. The function $\beta \mapsto \aleph_\beta$ is strictly increasing on $\kappa + 1$, and it takes its values in $\aleph_{\kappa+1}$. Thus $\aleph_\kappa \geq \kappa$ by Lemma 1.5.8, and hence $\aleph_{\kappa+1} > \kappa$. Let $\alpha \leq \kappa + 1$ be minimal with $\aleph_\alpha > \kappa$. Since $\kappa \geq \aleph_0$, we have $\alpha > 0$. If α were a limit ordinal, by definition we would have $\kappa \in \bigcup_{\beta<\alpha} \aleph_\beta$, and hence $\kappa \in \aleph_\beta$ for some $\beta < \alpha$, which would contradict the minimality of α. Thus $\alpha = \beta + 1$ and also $\aleph_\beta \leq \kappa < \aleph_{\beta+1} = \aleph_\beta^+$. Since $\aleph_\beta^+$ is the cardinal successor of $\aleph_\beta$, necessarily $\aleph_\beta = \kappa$. □

1.9. Operations on Cardinals

If X and Y are sets, one denotes by $X + Y$ their disjoint union, by $X \times Y$ their cartesian product and by X^Y the set of maps from Y to X. If κ and λ are cardinals, one denotes by $\kappa + \lambda$ the cardinal of their disjoint union, by $\kappa\lambda$ the cardinal of their cartesian product and by κ^λ the cardinal of the set of maps from λ to κ. These operations are respectively called *cardinal addition*, *cardinal multiplication* and *cardinal exponentiation*.

They should not be confused with the corresponding ordinal operations. For instance $2^\omega = \omega = \aleph_0 < 2^{\aleph_0}$; also $\aleph_0 2 = \aleph_0$, but $\omega < \omega 2$. It is clear that on finite cardinals all of these operations correspond to the usual arithmetic operations. Note that $\mathrm{card}(X+Y) = \mathrm{card}(X) + \mathrm{card}(Y)$, $\mathrm{card}(X \times Y) = \mathrm{card}(X)\mathrm{card}(Y)$ and $\mathrm{card}(X^Y) = \mathrm{card}(X)^{\mathrm{card}(Y)}$.

The proof of the following statements is immediate, using Proposition 1.8.3.

Proposition 1.9.1. *Let κ, λ and μ be cardinals.*

(1) *Cardinal addition and multiplication are commutative and associative, multiplication is distributive with respect to addition, $\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$, $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$ and $(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$.*

(2) *If $\kappa \leq \lambda$, then $\kappa + \mu \leq \lambda + \mu$, $\kappa\mu \leq \lambda\mu$ and $\kappa^\mu \leq \lambda^\mu$ (when $\kappa > 0$) and $\mu^\kappa \leq \mu^\lambda$ (when $\mu > 0$).* □

Proposition 1.9.2. *One has* $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

Proof. There is an injection $h : 2^{\aleph_0} \to \mathbb{R}$ sending a sequence $(a_i)_{i\in\mathbb{N}}$ to the sum $\sum_i a_i 2^{-i}$ if the support of the sequence is infinite, and to $2 + \sum_i a_i 2^{-i}$ otherwise. This proves that $2^{\aleph_0} \leq \mathrm{card}(\mathbb{R})$. On the other hand, the image of h contains the interval $(0, 1)$ which is equinumerous to $\mathbb{R}$ (for instance via $x \mapsto 1/\pi \arctan(x) + 1/2$); hence $\mathrm{card}(\mathbb{R}) \leq 2^{\aleph_0}$. □

Proposition 1.9.3 (Hessenberg's Theorem)**.** *For every infinite cardinal κ, one has $\kappa\kappa = \kappa$.*

Proof. By induction on α, we will prove that $\aleph_\alpha \aleph_\alpha = \aleph_\alpha$.

For $\alpha = 0$ this is clear. Indeed, the mapping $\alpha_2 : \mathbb{N}^2 \to \mathbb{N}$ defined by $\alpha_2(m, n) := 1/2(m + n + 1)(m + n) + n$ is bijective.

Let us now assume $\aleph_\beta \aleph_\beta = \aleph_\beta$ for every $\beta < \alpha$. One endows $\aleph_\alpha \times \aleph_\alpha$ with the following order:

$$\begin{aligned}(\beta, \gamma) < (\beta', \gamma') \text{ if } &\max(\beta, \gamma) < \max(\beta', \gamma'), \text{ or}\\ &\text{if } \max(\beta, \gamma) = \max(\beta', \gamma') \text{ and } \beta < \beta', \text{ or}\\ &\text{if } \max(\beta, \gamma) = \max(\beta', \gamma'), \beta = \beta' \text{ and } \gamma < \gamma'.\end{aligned}$$

One checks easily that this is a well-order. Furthermore, for every $\delta < \aleph_\alpha$, the set $\delta \times \delta$ is an initial segment for $<$. By Theorem 1.5.9, there is a unique isomorphism of ordered sets $f : \varepsilon \to \aleph_\alpha \times \aleph_\alpha$ with ε an ordinal.

Assume $\varepsilon > \aleph_\alpha$. Then $\aleph_\alpha \in \varepsilon$ and $f(\aleph_\alpha) = (\beta_0, \gamma_0) \in \aleph_\alpha \times \aleph_\alpha$. Set $\delta_0 := \max(\beta_0, \gamma_0) + 1$. Since no infinite successor ordinal is a cardinal (by Example 1.8.1), we have $\delta_0 < \aleph_\alpha$ and the restriction of f to $\aleph_\alpha$ is an injective map from $\aleph_\alpha$ to $\delta_0 \times \delta_0$, a set of cardinality

$$\mathrm{card}(\delta_0 \times \delta_0) = \mathrm{card}(\delta_0) \leq \delta_0 < \aleph_\alpha$$

by the induction hypothesis. This is a contradiction, and thus one has $\aleph_\alpha \aleph_\alpha \leq \aleph_\alpha$.

The inequality in the other direction is clear. □

Example 1.9.4. Let $\mathcal{T}$ be the set of all open subsets of $\mathbb{R}$. Then $\mathrm{card}(\mathcal{T}) = 2^{\aleph_0}$.

Proof. The mapping assigning to a real number $r \in \mathbb{R}$ the open interval $(r, +\infty)$ defines an injection from $\mathbb{R}$ to $\mathcal{T}$, which proves that $\mathrm{card}(\mathcal{T}) \geq 2^{\aleph_0}$.

Conversely, note that every open subset of $\mathbb{R}$ is a union of intervals of the form $(q, q + q')$, with $q \in \mathbb{Q}$ and $q' \in \mathbb{Q}_{>0}$. The mapping sending $Y \subseteq \mathbb{Q} \times \mathbb{Q}_{>0}$ to $\bigcup_{(q,q') \in Y} (q, q + q')$ provides a surjection of $\mathcal{P}(\mathbb{Q} \times \mathbb{Q}_{>0})$ to $\mathcal{T}$. Since $\mathbb{Q} \times \mathbb{Q}_{>0}$ is countable, one deduces that $2^{\aleph_0} \geq \mathrm{card}(\mathcal{T})$. □

Proposition 1.9.5.

(1) *Let X and Y be non-empty sets and assume that at least one of them is infinite. Then*

$$\mathrm{card}(X \cup Y) = \mathrm{card}(X \times Y) = \max(\mathrm{card}(X), \mathrm{card}(Y)).$$

(2) *Let $\kappa \geq \aleph_0$ and $\lambda > 0$ be cardinals. Then $\kappa + \lambda = \kappa\lambda = \max(\kappa, \lambda)$.*

(3) *Let $(X_i)_{i \in I}$ be a family of sets with at least one X_i infinite. Then*

$$(*) \qquad \mathrm{card}\left(\bigcup_{i \in I} X_i \right) \leq \sup\left(\{\mathrm{card}(X_i) \mid i \in I\} \cup \{\mathrm{card}(I)\} \right).$$

(In particular, a countable union of countable sets is countable.) If furthermore the sets X_i are all non-empty and mutually disjoint, then equality holds in $(*)$.

Proof. (1) Let $\kappa = \max(\mathrm{card}(X), \mathrm{card}(Y))$. We have

$$\kappa \leq \mathrm{card}(X \cup Y) \leq \kappa + \kappa = 2\kappa \leq \kappa\kappa$$

and $\kappa \leq \mathrm{card}(X \times Y) \leq \kappa\kappa$. One concludes by Hessenberg's Theorem.

(2) is a special case of (1).

(3) Let $X = \{(x_i, i) \mid x_i \in X_i \text{ for some } i \in I\}$ be the disjoint union of the sets X_i. There is a canonical surjection $X \to \bigcup_{i\in I} X_i$, hence it suffices to prove that

$$\operatorname{card}(X) \leq \sup\left(\{\operatorname{card}(X_i) \mid i \in I\} \cup \{\operatorname{card}(I)\}\right).$$

Let $\kappa = \sup\{\operatorname{card}(X_i) \mid i \in I\}$, and let Y_i be the set of injective maps $X_i \to \kappa$. Since the sets Y_i are all non-empty, by the Axiom of Choice there exists some $f = (f_i)_{i\in I} \in \prod_{i\in I} Y_i$. Consider $g : X \to \kappa \times I$, defined by $g((x_i, i)) := (f_i(x_i), i)$. The function g is injective, hence $\operatorname{card}(X) \leq \kappa \operatorname{card}(I) = \max(\kappa, \operatorname{card}(I))$. The equality statement is clear. □

It follows from the preceding proposition that cardinal addition and multiplication is quite trivial for infinite cardinals. The situation for cardinal exponentiation is very different. In fact, the ZFC axioms are far from completely determining the values of cardinal exponentiation. For instance they do not allow to settle the continuum hypothesis:

Definition.

- The *Continuum Hypothesis* (CH) is the statement $2^{\aleph_0} = \aleph_1$.
- The *Generalized Continuum Hypothesis* (GCH) is the statement $2^\kappa = \kappa^+$ for every infinite cardinal κ.

If $(\kappa_i)_{i\in I}$ is a family of cardinals, we shall denote by $\sum_{i\in I} \kappa_i$ the cardinal of the disjoint union of the κ_i, and by $\prod_{i\in I} \kappa_i$ the cardinal of the product of the family.

Theorem 1.9.6 (König's Theorem)**.** *Let $(\kappa_i)_{i\in I}$ and $(\lambda_i)_{i\in I}$ be families of cardinals with $\kappa_i < \lambda_i$ for every i. Then $\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i$.*

Proof. Let $f : \sum_{i\in I} \kappa_i \to \prod_{i\in I} \lambda_i$. For every i, f induces a mapping $f_i : \kappa_i \to \lambda_i$ given by the ith component of the restriction of f to κ_i. Since $\kappa_i < \lambda_i$, the set $B_i := \lambda_i \setminus \operatorname{im}(f_i)$ is non-empty for every i. By (AC) there exists some $b \in \prod_{i\in I} B_i \subseteq \prod_{i\in I} \lambda_i$. Clearly $b \notin \operatorname{im}(f)$. □

1.10. Cofinality

In this section we shall use the notion of cofinality to prove for instance that $2^{\aleph_0} \neq \aleph_\omega$.

Definition.

- Let X be a totally ordered set. We say that a subset $Y \subseteq X$ is *cofinal* in X if Y is not bounded in X, that is, if for any $x \in X$ there exists $y \in Y$ such that $x \leq y$. We say that a function $f : Z \to X$ is *cofinal* if $\mathrm{im}(f)$ is cofinal in X.
- The *cofinality* of an ordinal α, denoted by $\mathrm{cof}(\alpha)$, is the smallest ordinal β such that there exists a cofinal function $\beta \to \alpha$.

Example 1.10.1.

(1) $\mathrm{cof}(0) = 0$.

(2) $\mathrm{cof}(\alpha + 1) = 1$ for any ordinal α.

(3) $\mathrm{cof}(\omega) = \omega$.

Proposition 1.10.2. *Let α be an ordinal.*

(1) $\mathrm{cof}(\alpha) \leq \alpha$.

(2) $\mathrm{cof}(\alpha)$ *is a cardinal.*

(3) $\mathrm{cof}(\alpha)$ *is the smallest ordinal β such that there exists a cofinal and strictly increasing map $\beta \to \alpha$.*

(4) $\mathrm{cof}(\mathrm{cof}(\alpha)) = \mathrm{cof}(\alpha)$.

Proof. (1) is clear, and (2) follows from the fact that any ordinal β is in bijection with $\mathrm{card}(\beta) \leq \beta$.

(3) It is enough to provide some $\beta \leq \mathrm{cof}(\alpha)$ and a cofinal and strictly increasing map $\beta \to \alpha$. By hypothesis, there exists a cofinal map $h : \mathrm{cof}(\alpha) \to \alpha$. Let us define

$$X = \{x \in \mathrm{cof}(\alpha) \mid h(y) < h(x) \text{ for every } y < x\}.$$

The set $h(X) = \{h(x) \mid x \in X\}$ is cofinal in α. Indeed, let $\gamma < \alpha$. By the cofinality of h, there exists $y \in \mathrm{cof}(\alpha)$ such that $h(y) \geq \gamma$. When y is minimal with this property, we have $y \in X$.

Since $(X, <) \cong (\beta, \in)$ for some $\beta \leq \mathrm{cof}(\alpha)$, we are done, because the restriction of h to X is cofinal and strictly increasing.

(4) $\mathrm{cof}(\mathrm{cof}(\alpha)) \leq \mathrm{cof}(\alpha)$ follows from part (1). For the inequality in the other direction, let us consider the cofinal and strictly increasing functions $f : \mathrm{cof}(\mathrm{cof}(\alpha)) \to \mathrm{cof}(\alpha)$ and $g : \mathrm{cof}(\alpha) \to \alpha$, which are

possible by (3). Then the function $g \circ f : \mathrm{cof}(\mathrm{cof}(\alpha)) \to \alpha$ is cofinal, and hence $\mathrm{cof}(\alpha) \leq \mathrm{cof}(\mathrm{cof}(\alpha))$. □

We shall say that an infinite cardinal κ is *regular* if $\mathrm{cof}(\kappa) = \kappa$, and *singular* if $\mathrm{cof}(\kappa) < \kappa$.

Proposition 1.10.3. *Any infinite cardinal which is a successor is regular. In particular $\aleph_1$ is regular.*

Proof. Let $\kappa = \aleph_{\beta+1} = \aleph_\beta^+$. Note that for a limit ordinal α, a subset $X \subseteq \alpha$ is cofinal if and only if $\alpha = \bigcup_{\gamma \in X} \gamma$. (This follows from Proposition 1.5.5.) Consider a function $f : \lambda \to \kappa$ for some $\lambda < \kappa$. Then $\lambda \leq \aleph_\beta$ and it follows from Proposition 1.9.5(3) that $\mathrm{card}\left(\bigcup_{\beta<\lambda} f(\beta)\right) \leq \sup(\{\mathrm{card}(f(\beta)) \mid \beta < \lambda\} \cup \{\lambda\}) \leq \aleph_\beta$. Hence f is not cofinal. □

Proposition 1.10.4. *If λ is a limit ordinal, then* $\mathrm{cof}(\aleph_\lambda) = \mathrm{cof}(\lambda)$.

Proof. If $f : \alpha \to \lambda$ is cofinal, then $\tilde{f} : \alpha \to \aleph_\lambda$, $\beta \mapsto \aleph_{f(\beta)}$ is cofinal too, since $\aleph_\lambda = \bigcup_{\gamma<\lambda} \aleph_\gamma$ by definition. This proves $\mathrm{cof}(\aleph_\lambda) \leq \mathrm{cof}(\lambda)$. Conversely, let $g : \alpha \to \aleph_\lambda$ be cofinal. The map $\tilde{g} : \alpha \to \lambda$, defined by $\tilde{g}(\beta) = 0$ if $g(\beta)$ is finite, and $\tilde{g}(\beta) = \gamma$ if $\mathrm{card}(g(\beta)) = \aleph_\gamma$, is cofinal. □

Proposition 1.10.5. *Let $\kappa \geq 2$ and $\lambda \geq \aleph_0$ be cardinals. Then* $\mathrm{cof}\left(\kappa^\lambda\right) > \lambda$.

Proof. Consider a map $f : \alpha \to \kappa^\lambda$, with α some ordinal $\leq \lambda$. Since $f(\beta) < \kappa^\lambda$ for every $\beta < \alpha$, it follows from König's Theorem that

$$\mathrm{card}\left(\bigcup_{\beta<\alpha} f(\beta)\right) \leq \sum_{\beta<\alpha} \mathrm{card}(f(\beta)) < \prod_{\beta<\alpha} \left(\kappa^\lambda\right) = \kappa^{\lambda \cdot \mathrm{card}(\alpha)} \leq \kappa^\lambda.$$

Hence f is not cofinal. □

Corollary 1.10.6. $2^{\aleph_0} \neq \aleph_\omega$.

Proof. We have $\mathrm{cof}(\aleph_\omega) = \mathrm{cof}(\omega) = \omega = \aleph_0 < \mathrm{cof}\left(2^{\aleph_0}\right)$. □

1.11. Exercises

Exercise 1.11.1.

(1) Prove that an ordinal α is a limit if and only if there is an ordinal $\beta \neq 0$ such that $\alpha = \omega\beta$.

(2) Prove that $\omega^2 = \omega\omega$ is not of the form $\delta + \omega$.

Exercise 1.11.2 (Cantor normal form)**.** Let α be an ordinal > 1.

(1) Prove that $\alpha^\gamma \geq \gamma$ for any ordinal γ. (Is there any example with $\alpha^\gamma = \gamma$?)

(2) Let β be an ordinal > 0. Prove that there exists an ordinal γ such that $\alpha^\gamma \leq \beta < \alpha^{\gamma^+}$.

(3) Deduce that any ordinal β can be expanded in basis α: there exists a finite sequence of ordinals $\beta_1 > ... > \beta_n \geq 0$ and ordinals k_i with $0 < k_i < \alpha$ such that

$$\beta = \alpha^{\beta_1} k_1 + ... + \alpha^{\beta_n} k_n.$$

Furthermore the natural number n and the sequences (β_i) and (k_i) are unique.

The expansion into basis ω is called the *Cantor normal form*.

Exercise 1.11.3 (Goodstein sequences)**.** Let n, p be natural numbers, with $p \geq 2$. Let us define the iterated expansion of n in basis p as follows: first expand n in basis p (for instance if $n = 35$, $p = 2$, one has $35 = 2^5 + 2 + 1$). Then, expand the exponents in basis p and so on, so that all numbers occurring are $< p$. For instance the iterated expansion of 35 in basis 2 is $35 = 2^{2^2+1} + 2 + 1$.

For $q \geq p \geq 2$, one defines a function $f_{p,q} : \mathbb{N} \to \mathbb{N}$ as follows. Let n be a natural number. Then $f_{p,q}(n)$ is obtained by replacing all occurrences of p in the iterated expansion of n in basis p by q. One similarly defines ordinal valued functions $f_{p,\omega}$ by replacing all occurrences of p by ω (when $p > 2$, one writes the coefficients at the right of the p^n). For instance, $f_{2,3}(35) = 3^{3^3+1}+3+1 = 59053$ and $f_{3,\omega}(35) = f_{3,\omega}(3^3+3\cdot 2+2) = \omega^\omega + \omega \cdot 2 + 2$.

(1) Prove that $f_{q,r} \circ f_{p,q} = f_{p,r}$ for any $\omega \geq r > q > p \geq 2$.

(2) Prove that the functions $f_{p,\omega}$ are strictly increasing.

For any $a \in \mathbb{N}$, the *Goodstein sequence* attached to a is the sequence $(g_n(a))_{n\geq 2}$ defined by $g_2(a) := a$ and

$$g_{n+1}(a) = \begin{cases} f_{n,n+1}(g_n(a)) - 1 & \text{if } g_n(a) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

For $a = 5$, one has for instance $g_2(5) = 5$, $g_3(5) = 3^3 + 1 - 1 = 27$, $g_4(5) = 4^4 - 1 = 255$, and $g_5(5) = 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 3 - 1 = 467$.

(3) Let a be a natural number. Study the monotonicity of the sequence $f_{p,\omega}(g_p(a))$.

(4) Prove that for any $a \in \mathbb{N}$ there exists $s(a) \in \mathbb{N}$ such that $g_n(a) = 0$ when $n \geq s(a)$.

Exercise 1.11.4 (The order topology)**.** On any totally ordered set X, one may define a topology, the *order topology*, generated by the open intervals, that is, by the sets of the form $(-\infty, b) = \{x \in X \mid x < b\}$, $(a, b) = \{x \in X \mid a < x < b\}$ or (a, ∞), for $a, b \in X$.

(1) Prove that for any X, the order topology is Hausdorff.

(2) Let α and β be ordinals endowed with the order topology. Prove the following statements:
   (a) α is discrete if and only if $\alpha \leq \omega$.
   (b) α is compact if and only if α is not a limit ordinal.
   (c) Suppose $f : \alpha \to \beta$ is a weakly increasing function, that is, $x \leq y \Rightarrow f(x) \leq f(y)$. Then f is continuous if and only if, for any limit $\lambda \in \alpha$, $f(\lambda) = \sup_{\gamma<\lambda} f(\gamma)$.

Exercise 1.11.5 (Ulam's Theorem)**.** An *Ulam matrix* is a family of subsets $U_{\alpha,n}$ of $\aleph_1$, $\alpha < \aleph_1$, $n < \omega$, such that

- for any $n < \omega$ and $\alpha, \beta < \aleph_1$ with $\alpha \neq \beta$, $U_{\alpha,n} \cap U_{\beta,n} = \emptyset$;
- for any $\alpha < \aleph_1$, the set $\aleph_1 \setminus \bigcup_{n<\omega} U_{\alpha,n}$ is at most countable.

(1) For any $\xi < \aleph_1$, let $f_\xi : \omega \to \aleph_1$ such that $\xi \subseteq \mathrm{im}(f_\xi)$. Set

$$U_{\alpha,n} = \{\xi < \aleph_1 \mid f_\xi(n) = \alpha\}.$$

Prove that $(U_{\alpha,n})$ is an Ulam matrix.

(2) Let $\mu : \mathcal{P}(\aleph_1) \to [0,1]$ be a σ-additive measure on $\aleph_1$, that is, $\mu(\bigcup_{n<\omega} A_n) = \sum_{n<\omega} \mu(A_n)$ for all families $(A_n)_{n<\omega}$ of pairwise disjoint subsets of $\aleph_1$. Prove that if $\mu(\{\alpha\}) = 0$ for every $\alpha < \aleph_1$, then μ is identically zero.

Exercise 1.11.6 (Closed unbounded sets)**.** Let $\kappa > \aleph_0$ be a regular cardinal. A set $C \subseteq \kappa$ is said to be a *club* (closed unbounded) if it is closed and cofinal, that is, if it is cofinal in κ and for any non-empty subset $A \subseteq C$, $\sup A \in C \cup \{\kappa\}$. A subset $S \subseteq \kappa$ is called *stationary* if $S \cap C \neq \emptyset$ for any club $C \subseteq \kappa$.

(1) Let $\lambda < \kappa$ and $(C_i)_{i<\lambda}$ be a family of clubs. Prove that $\bigcap_{i<\lambda} C_i$ is a club.

(2) Let $(C_i)_{i<\kappa}$ be a family of clubs. Prove that the diagonal intersection $\triangle_{i<\kappa} C_i := \{\alpha < \kappa \mid \alpha \in \bigcap_{i<\alpha} C_i\}$ is a club.

(3) (Fodor's Lemma) Let $S \subseteq \kappa$ be a stationary set and suppose $f : S \to \kappa$ is a *regressive* map (that is, such that $f(\alpha) < \alpha$ for any $\alpha \in S$). Prove that there exists a stationary set $T \subseteq S$ such that f is constant on T.

(4) (Solovay's Theorem for $\aleph_1$) Let $\kappa = \aleph_1$, and let $S \subseteq \aleph_1$ be a stationary set. Prove that S can be written as the union of $\aleph_1$ pairwise disjoint stationary sets.

[Hint: For any limit ordinal $\alpha \in S$, write $\alpha = \sup_{n<\omega} a_n^\alpha$. Use this to define a regressive function to which one may apply Fodor's Lemma.]

Exercise 1.11.7 (Solovay's Theorem)**.** Let $\kappa > \aleph_0$ be a regular cardinal. The aim of this exercise is to prove Solovay's Theorem: *Any stationary set $S \subseteq \kappa$ can be written as the union of κ pairwise disjoint stationary sets.*

(1) For a cardinal $\lambda < \kappa$, let $E^\kappa_\lambda = \{\alpha < \kappa \mid \mathrm{cof}(\alpha) = \lambda\}$. Prove Solovay's Theorem when $S \subseteq E^\kappa_\omega$.

(2) Prove Solovay's Theorem when $S \subseteq \{\alpha < \kappa \mid \mathrm{cof}(\alpha) < \alpha\}$.

(3) Assume S is a set of regular cardinals. Prove that

$$T = \{\alpha \in S \mid S \cap \alpha \text{ is not stationary in } \alpha\}$$

is stationary.

[Hint: Prove it by contradiction after noticing that if C is a club, the set $C' \subseteq C$ of limits of points of C is still a club.]

(4) Prove Solovay's Theorem in the general case.

[Hint: Prove it is enough to consider the case when S is a set of regular cardinals. For $\alpha \in T$, consider a strictly increasing sequence $(a^\alpha_\xi : \xi < \kappa)$ with limit α such that $a^\alpha_\xi \notin S$. Then adapt the proof of (1).]

Exercise 1.11.8 (Filters and ultrafilters)**.** Let X be a non-empty set. A *filter* on X is a set $F \subseteq \mathcal{P}(X)$ such that

(i) $X \in F, \emptyset \notin F$,

(ii) if $A, B \in F$, then $A \cap B \in F$, and

(iii) if $A \in F$ and $A \subseteq B$, then $B \in F$.

A set $\mathcal{B}$ of non-empty subsets of X is a *filter basis* on X if for any $A, B \in \mathcal{B}$ there is $C \in \mathcal{B}$ such that $C \subseteq A \cap B$.

(1) Prove that any filter basis $\mathcal{B}$ is contained in a minimal filter with respect to inclusion, denoted by $F_{\mathcal{B}}$.

(2) Let J be a set and let I be the set of finite subsets of J. For any $i \in I$, set $I_i = \{j \in I \mid i \subseteq j\}$. Prove that the set $\mathcal{B}$ whose elements are the sets I_i, $i \in I$, is a filter basis on I.

(3) Prove that when X is infinite, the set of subsets of X whose complement in X is finite is a filter. This filter is called the *Fréchet filter*.

(4) An *ultrafilter* is a filter which is maximal with respect to inclusion. Prove that a filter F on a non-empty set X is an ultrafilter if and only if for any $A \subseteq X$, either A or $X \setminus A$ belongs to F.

(5) Prove that for any $x \in X$, the set $U_x = \{Y \subseteq X \mid x \in Y\}$ is an ultrafilter on X. Such an ultrafilter is called *principal*.

(6) Prove that an ultrafilter is principal if and only if it contains a finite set as an element. Deduce that when X is finite, any ultrafilter on X is principal, and when X is infinite, an ultrafilter U is non-principal if and only if it contains the Fréchet filter as a subset.

(7) Prove that any filter is contained in some ultrafilter. In particular, on any infinite set there exists a non-principal ultrafilter.

Exercise 1.11.9 (Hausdorff's Theorem)**.** The aim of this exercise is to prove the following result due to Hausdorff: *On an infinite set X of cardinality κ, there exist $2^{(2^\kappa)}$ distinct ultrafilters.*

(1) A family F of subsets of X is said to be *free* if whenever $A_1, \ldots, A_n, B_1, \ldots, B_m$ are distinct elements of F, then $A_1 \cap \cdots \cap A_n \cap (X \setminus B_1) \cap \cdots \cap (X \setminus B_m)$ is non-empty. Prove that Hausdorff's Theorem is a consequence of the following statement: there exists a free family of cardinality 2^κ.

(2) Consider the set Y consisting of pairs $(F, (P_1, \ldots, P_n))$ with F a finite subset of X and $(P_1, \ldots, P_n)$ a finite sequence of of subsets of F. What is the cardinality of Y?

(3) To any $A \in \mathcal{P}(X)$ we assign a subset A' of $X \cup Y$ as follows:
- if $x \in X$, then $x \in A'$ if and only if $x \in A$;
- if $y \in Y$ and $y = (F, (P_1, \ldots, P_n))$, then $y \in A'$ if and only if $A \cap F$ is one of the P_i's.

Prove that the set of the A' for $A \subseteq X$ is a free family (on $X \cup Y$).

(4) Conclude Hausdorff's Theorem.

Exercise 1.11.10 (The continuum hypothesis for closed subsets of $\mathbb{R}$)**.** The aim of this exercise is to prove that the continuum hypothesis holds for closed subsets of the real line (Cantor's Theorem), that is, if $F \subseteq \mathbb{R}$ is closed, then either F is countable or $\mathrm{card}(F) = 2^{\aleph_0}$.

Let $F \subseteq \mathbb{R}$ be a closed subset such that $\mathrm{card}(F) > \aleph_0$.

(1) Let C be the set of $x \in F$ such that there is an open set $\Omega \subseteq \mathbb{R}$ which contains x and satisfies $\mathrm{card}(\Omega \cap F) \leq \aleph_0$. Set $F' := F \setminus C$.

Prove the following properties:
(a) C is countable,
(b) F' is a closed subset of $\mathbb{R}$, and
(c) any non-empty open subset of F' is uncountable.

(2) Let I be an open interval such that $I \cap F' \neq \emptyset$.

Prove that for any $\epsilon > 0$ there are open intervals I_0 and I_1 of length at most ϵ such that $I_i \cap F' \neq \emptyset$ and $\overline{I_i} \subseteq I$ for $i = 0, 1$ and such that $\overline{I_0} \cap \overline{I_1} = \emptyset$. (Here, $\overline{J}$ denotes the closure of J.)

(3) Prove that there is an injection of $2^{\aleph_0}$ into F'.

(4) Prove Cantor's Theorem.

Exercise 1.11.11. A *tree* is a partial order $(T, <_T)$ such that for every $t \in T$, the set

$$\hat{t} := \{s \in T \mid s <_T t\}$$

is well-ordered. If T has a smallest element, it is called the *root* of T.

The *height* of $t \in T$ is defined as the unique ordinal isomorphic to $(\hat{t}, <_T)$ and denoted by $\mathrm{ht}(t)$. Finally, $\mathrm{ht}(T) := \sup\{\mathrm{ht}(t) + 1 \mid t \in T\}$ is the *height* of T. For an ordinal α one sets $T(\alpha) = \{t \in T \mid \mathrm{ht}(t) = \alpha\}$.

A *branch* in a tree $(T, <_T)$ is a totally ordered subset which is maximal with respect to inclusion. It is called *cofinal* in T if it non-trivially intersects any level $T(\alpha)$ for $\alpha < \mathrm{ht}(T)$.

Prove König's Lemma: If T is a tree of height ω such that $T(n)$ is finite for every $n \in \omega$, then T contains a cofinal branch.

Exercise 1.11.12.

(1) For $\alpha \in \aleph_1$, let Y_α be the set of strictly increasing non-cofinal maps from α to $\mathbb{Q}$. For $\beta < \alpha$, denote by $\rho^\alpha_\beta : Y_\alpha \to Y_\beta$ the (surjective) restriction map. Prove that there are countable subsets $X_\alpha \subseteq Y_\alpha$ such that for any $\alpha > \beta$, the following properties hold:
   (a) $\rho^\alpha_\beta(X_\alpha) = X_\beta$.
   (b) For any $f \in X_\beta$, any upper bound $q \in \mathbb{Q}$ of $\mathrm{im}(f)$ and any $\epsilon > 0$ there is $g \in X_\alpha$ with $\rho^\alpha_\beta(g) = f$ such that $\mathrm{im}(g)$ is bounded above by $q + \epsilon$.

(2) Let $\varprojlim_{\alpha \in \aleph_1} X_\alpha$ be the set of all $f = (f_\alpha) \in \prod_{\alpha \in \aleph_1} X_\alpha$ such that $\rho^\alpha_\beta(f_\alpha) = f_\beta$ for all $\beta < \alpha$. Prove that $\varprojlim_{\alpha \in \aleph_1} X_\alpha = \emptyset$.

(3) Deduce Aronszajn's Theorem: *There is an* Aronszajn tree*, that is, a tree T of height $\aleph_1$ with $T(\alpha)$ countable for all $\alpha < \aleph_1$ such that T does not admit a cofinal branch.*

1.12. Appendix: Hindman's Theorem

In this appendix we shall freely use the material on ultrafilters treated in Exercise 1.11.8. Let E be a non-empty set and $\mathcal{U}(E)$ the set of all ultrafilters on E. When E is infinite, there exist non-principal ultrafilters on E.

For a subset $A \subseteq E$, set $\langle A\rangle = \{U \in \mathcal{U}(E) \mid A \in U\}$.

Lemma 1.12.1. *The sets $\langle A\rangle$, for $\emptyset \neq A \subseteq E$, form a basis of open sets for a compact Hausdorff topology on $\mathcal{U}(E)$.*

Proof. We have $\langle A_1\rangle \cap \cdots \cap \langle A_n\rangle = \langle A_1 \cap \cdots \cap A_n\rangle$, which proves that the sets $\langle A\rangle$ form a basis of open sets for some topology. Furthermore, $\langle E \setminus A\rangle = \mathcal{U}(E) \setminus \langle A\rangle$, thus $\langle A\rangle$ is open and closed. In particular, the topology is Hausdorff.

Consider a covering $\bigcup_{i\in I} \Omega_i$ of $\mathcal{U}(E)$ by open subsets. To prove the existence of $I_0 \subseteq I$ finite such that $\bigcup_{i\in I_0} \Omega_i = \mathcal{U}(E)$ we may assume $\Omega_i = \langle A_i\rangle$ for any $i \in I$. If for some finite $I_0 \subseteq I$ one has $\bigcup_{i\in I_0} A_i = E$, we are done, since then $\bigcup_{i\in I_0} \langle A_i\rangle = \mathcal{U}(E)$. Otherwise, the set

$$\mathcal{B} = \left\{ \bigcap_{i\in I_0} E \setminus A_i \mid I_0 \subseteq I \text{ finite} \right\}$$

is a filter basis and is contained in some ultrafilter U on E by Exercise 1.11.8, which contradicts $\bigcup_{i\in I} \Omega_i = \mathcal{U}(E)$. □

Now consider $\mathcal{U}(\mathbb{N}^*)$. Let $k \in \mathbb{N}^*$, $A \subseteq \mathbb{N}^*$ and $U \in \mathcal{U}(\mathbb{N}^*)$. One sets $A - k := \mathbb{N}^* \cap \{a - k \mid a \in A\}$ and

$$A_U := \{k \in \mathbb{N}^* \mid A - k \in U\}.$$

Lemma 1.12.2. *For any $U \in \mathcal{U}(\mathbb{N}^*)$ and every $A, B \subseteq \mathbb{N}^*$, one has $\mathbb{N}^*_U = \mathbb{N}^*$, $(A \cap B)_U = A_U \cap B_U$ and $(\mathbb{N}^* \setminus A)_U = \mathbb{N}^* \setminus A_U$.*

Proof. These properties are easy consequences of the fact that for $k \in \mathbb{N}^*$ one has $\mathbb{N}^* - k = \mathbb{N}^*$, $(A-k)\cap(B-k) = A\cap B - k$ and $(\mathbb{N}^* \setminus A) - k = \mathbb{N}^* \setminus (A - k)$. The details are left as an exercise. □

For $U, V \in \mathcal{U}(\mathbb{N}^*)$, one sets $U \oplus V := \{A \subseteq \mathbb{N}^* \mid A_U \in V\}$.

Lemma 1.12.3.

(1) *For any $U, V \in \mathcal{U}(\mathbb{N}^*)$, $U \oplus V \in \mathcal{U}(\mathbb{N}^*)$.*

(2) *$\oplus$ is associative.*

(3) *For fixed U, the function $f_U : \mathcal{U}(\mathbb{N}^*) \to \mathcal{U}(\mathbb{N}^*)$, $V \mapsto U \oplus V$, is continuous.*

Proof. (1) It is clear that $\mathbb{N}^* \in U \oplus V$, and that for any $A \in U \oplus V$ and $A \subseteq B$ one has $B \in U \oplus V$. Stability of $U \oplus V$ under intersection and the fact that $A \in U \oplus V$ if and only if $\mathbb{N}^* \setminus A \notin U \oplus V$ are consequences of Lemma 1.12.2.

(2) One has $(A - k)_U = A_U - k$ (exercise). From this, one may deduce that $(A_U)_V = A_{U \oplus V}$. Indeed, for $l \in \mathbb{N}^*$, one has

$$\begin{aligned} l \in (A_U)_V &\Leftrightarrow A_U - l \in V \Leftrightarrow (A - l)_U \in V \\ &\Leftrightarrow A - l \in U \oplus V \Leftrightarrow l \in A_{U \oplus V}. \end{aligned}$$

If $U, V, W \in \mathcal{U}(\mathbb{N}^*)$, we deduce that

$$\begin{aligned} A \in U \oplus (V \oplus W) &\Leftrightarrow A_U \in V \oplus W \\ &\Leftrightarrow (A_U)_V = A_{U \oplus V} \in W \Leftrightarrow A \in (U \oplus V) \oplus W, \end{aligned}$$

which proves associativity of $\oplus$.

(3) Let $A \subseteq \mathbb{N}^*$. Continuity of f_U follows from the following:

$$\begin{aligned} f_U^{-1}(\langle A \rangle) &= \{V \in \mathcal{U}(\mathbb{N}^*) \mid A \in U \oplus V\} \\ &= \{V \in \mathcal{U}(\mathbb{N}^*) \mid A_U \in V\} = \langle A_U \rangle. \end{aligned}$$

□

We shall say an ultrafilter U on $\mathbb{N}^*$ is *idempotent* if $U \oplus U = U$.

Proposition 1.12.4. *There exists an idempotent ultrafilter in $\mathcal{U}(\mathbb{N}^*)$.*

Remark 1.12.5. For $m, n \in \mathbb{N}^*$, one can easily check that the sum of the corresponding principal ultrafilters is given by $U_m \oplus U_n = U_{m+n}$. In particular no principal ultrafilter is idempotent. □

Proof of Proposition 1.12.4. One considers the set

$$\mathbb{A} := \{\mathcal{A} \subseteq \mathcal{U}(\mathbb{N}^*) \mid \mathcal{A} \text{ is a non-empty closed set with } \mathcal{A} \oplus \mathcal{A} \subseteq \mathcal{A}\}.$$

The set $\mathbb{A}$ is non-empty since it contains $\mathcal{U}(\mathbb{N}^*)$. Furthermore the partial order on $\mathbb{A}$ given by $\supseteq$ is inductive. This follows from the fact that a

subset of a compact Hausdorff space is closed if and only if it is compact. Thus, if $(\mathcal{A}_i)_{i\in I}$ is a totally ordered subset of $\mathbb{A}$, then $\bigcap_{i\in I}\mathcal{A}_i \in \mathbb{A}$. By Zorn's Lemma, there exists $\mathcal{B} \in \mathbb{A}$ which is minimal for inclusion.

Let $U \in \mathcal{B}$. We shall prove that $U \oplus U = U$.

First, we consider $\mathcal{B}' := U \oplus \mathcal{B} \subseteq \mathcal{B}$. Since f_U is continuous, the set $\mathcal{B}' = f_U(\mathcal{B})$ is compact (hence closed). Furthermore, if $V_1, V_2 \in \mathcal{B}$, one has $(U \oplus V_1) \oplus (U \oplus V_2) = U \oplus W$ for some $W \in \mathcal{B}$, since $\mathcal{B} \oplus \mathcal{B} \subseteq \mathcal{B}$. This proves that $\mathcal{B}' \oplus \mathcal{B}' \subseteq \mathcal{B}'$. Hence we have $\mathcal{B}' \in \mathbb{A}$, and thus $\mathcal{B}' = \mathcal{B}$ by minimality of $\mathcal{B}$. In particular, there exists $V' \in \mathcal{B}$ such that $U \oplus V' = U$.

Set $\mathcal{V}' = \{V' \in \mathcal{B} \mid U \oplus V' = U\}$. By continuity of the map f_U, $\mathcal{V}' = f_U^{-1}(\{U\}) \cap \mathcal{B}$ is closed, and we just proved it is non-empty. If $V', V'' \in \mathcal{V}'$, then $U \oplus (V' \oplus V'') = (U \oplus V') \oplus V'' = U \oplus V'' = U$. Thus $\mathcal{V}'$ is closed under $\oplus$ and it belongs to $\mathbb{A}$. It follows that $\mathcal{V}' = \mathcal{B}$ by minimality of $\mathcal{B}$. In particular, $U \in \mathcal{V}'$, hence $U \oplus U = U$. □

For a subset $A \subseteq \mathbb{N}^*$, one denotes by

$$\Sigma_A := \left\{ \sum_{k\in A_0} k \mid A_0 \subseteq A \text{ finite} \right\}$$

the set of finite sums of distinct elements of A.

Theorem 1.12.6 (Hindman's Theorem)**.** *Let $\chi : \mathbb{N}^* \to \{1, \dots, n\}$ be any function. Then there exists $B \subseteq \mathbb{N}^*$ infinite such that χ is constant on Σ_B.*

Proof. Let $U = U \oplus U \in \mathcal{U}(\mathbb{N}^*)$ be an idempotent ultrafilter as provided by Proposition 1.12.4. There then exists a unique $i_0 \leq n$ such that $\chi^{-1}(i_0) \in U$. Set $A := \chi^{-1}(i_0)$. We will prove the existence of an infinite set $B \subseteq A$ such that $\Sigma_B \subseteq A$, which will complete the proof.

As $U = U \oplus U$, for any $C \in U$ one has $C_U \in U$, hence $C \cap C_U \in U$. In particular, $C \cap C_U$ is infinite. Furthermore, for any $k \in C \cap C_U$ one has $(C - k) \cap C \in U$.

By induction on $n \in \mathbb{N}$, one defines a decreasing sequence $(A^n)_{n\in\mathbb{N}}$ in U and a strictly increasing sequence of integers $(k_n)_{n\in\mathbb{N}}$ as follows. One sets $A^0 := A$ and one chooses $k_0 \in A^0 \cap A^0_U$. Assuming A^n and k_n already constructed, one sets $A^{n+1} := (A^n - k_n) \cap A^n \in U$, and one

chooses some $k_{n+1} > k_n$ such that $k_{n+1} \in A^{n+1} \cap A_U^{n+1}$. This is possible since $A^{n+1} \cap A_U^{n+1}$ is infinite.

Now $B = \{k_n \mid n \in \mathbb{N}\}$ is an infinite subset of A. Let I be a finite nonempty subset of $\mathbb{N}$. We now prove by induction on $\mathrm{card}(I)$ that $\sum_{i\in I} k_i \in A^{\min I}$. If I is a singleton, this is clear. Assume now that $\mathrm{card}(I) = m+1$ for some $m > 0$ and let $i_0 < ... < i_m$ be the elements of I. By induction we know that

$$k_{i_1} + ... + k_{i_m} \in A^{i_1} \subseteq A^{i_0+1} = A^{i_0} \cap (A^{i_0} - k_{i_0}).$$

It follows that $k_{i_0} + ... + k_{i_m} \in A^{i_0}$ as claimed. We have thus proved that $\Sigma_B \subseteq A$. □

10.1090/stml/089/02

Chapter 2

First-order Logic

Introduction

This chapter introduces the basics of *first-order logic*. First-order logic is a standard way to formalize mathematics. For instance Peano arithmetic and Zermelo-Fraenkel set theory formalize respectively number theory and set theory. In a given formal language, one can define the basic notions of variables, terms and formulas. One can also define formal logical deduction rules that allow one to deduce new statements from a given set of axioms via a formal proof. This corresponds to the *syntactic* side of formal logic, where constructions are purely symbolic and no specific interpretation or meaning is given to the symbols.

On the other hand, *structures* for a given language are sets where it is possible to interpret terms and formulas. In particular, one can give a meaning to the *validity* of a formula with no free variables in a structure. This is the *semantic* side.

The main result in this chapter is Gödel's Completeness Theorem which states that a formula with no free variables can be formally deduced from a given set of axioms if and only if it is valid in every structure satisfying these axioms. This particularly remarkable result shows that the syntactic and semantic viewpoints are equivalent. It also provides an a posteriori justification for our choice of syntax.

2.1. Languages and Structures

Statements in first-order logic are sequences of symbols describing properties of certain structures. For instance the statement given by

$$\forall x(x > 0 \to \exists y\, y \cdot y = x)$$

is satisfied in some ordered field if and only if every positive element is a square. It holds in the ordered field of real numbers, that is, in the structure $\mathfrak{R} = \langle \mathbb{R}; 0, 1, +, -, \cdot, < \rangle$, and it does not hold in the ordered field of rational numbers.

We will see that this statement can be expressed in first-order logic. However, other properties of ordered field, like being *complete* (any bounded non-empty subset admits a supremum) or *archimedean* (for every $x > 0$ there exists $n \in \mathbb{N}$ such that $nx > 1$), cannot be expressed as statements in first-order logic.

Definition. A (*first-order*) *language* is a set of symbols $\mathcal{L}$ composed of two disjoint subsets:

(1) The first part (common to all languages) consists of auxiliary symbols "(" and ")" together with the following *logical symbols:*

the set of *variables*	$\mathcal{V} = \{v_n \mid n \in \mathbb{N}\}$
the *equality symbol*	$=$ ("equals")
connectives	$\neg$ (negation, "not"), and
	$\wedge$ (conjunction, "and")
the *existential quantifier*	$\exists$ ("there exists")

(2) The second part, called the *signature* of $\mathcal{L}$ and denoted by $\sigma^{\mathcal{L}}$, consists of the *non-logical symbols* of $\mathcal{L}$. It consists of
- a set of *constant symbols* $\mathcal{C}^{\mathcal{L}}$;
- a sequence of sets $\mathcal{F}_n^{\mathcal{L}}$, $n \in \mathbb{N}^*$, where elements of $\mathcal{F}_n^{\mathcal{L}}$ are called *n-ary function symbols*;
- a sequence of sets $\mathcal{R}_n^{\mathcal{L}}$, $n \in \mathbb{N}^*$, where elements of $\mathcal{R}_n^{\mathcal{L}}$ are called *n-ary relation symbols* (or *n-ary predicates*).

The language $\mathcal{L}$ is given by the (disjoint) union of these sets of symbols.

Let us note that a language is always infinite. The first part being common to all languages, we shall make the abuse of notation of identifying $\mathcal{L}$ and $\sigma^{\mathcal{L}}$.

Example 2.1.1.

$\mathcal{L}_\emptyset = \emptyset$	The empty language.
$\mathcal{L}_{ring} = \{\underline{0}, \underline{1}, +, -, \cdot\}$	The ring language (with 1).
$\mathcal{L}_{ord} = \{<\}$	The order language.
$\mathcal{L}_{o.ring} = \mathcal{L}_{ring} \cup \mathcal{L}_{ord}$	The ordered ring language.
$\mathcal{L}_{ar} = \{\underline{0}, S, +, \cdot, <\}$	The language of arithmetic.
$\mathcal{L}_{set} = \{\in\}$	The language of set theory.

In these examples, $\underline{0}$ and $\underline{1}$ are constant symbols, $-$ and S unary function symbols, $+$ and $\cdot$ binary function symbols, and $<$ and $\in$ binary relation symbols.

Definition. Let $\mathcal{L}$ be a first-order language. An *$\mathcal{L}$-structure* $\mathfrak{A}$ consists of a non-empty set A (called the *base set* of $\mathfrak{A}$) together with an element $c^{\mathfrak{A}} \in A$ for each $c \in \mathcal{C}^{\mathcal{L}}$, a function $f^{\mathfrak{A}} : A^n \to A$ for each $f \in \mathcal{F}_n^{\mathcal{L}}$ and a subset $R^{\mathfrak{A}} \subseteq A^n$ for each $R \in \mathcal{R}_n^{\mathcal{L}}$. We write $\mathfrak{A} = \langle A; (Z^{\mathfrak{A}})_{Z \in \sigma^{\mathcal{L}}} \rangle$.

$Z^{\mathfrak{A}}$ is called the *interpretation* of the symbol $Z \in \sigma^{\mathcal{L}}$ in the structure $\mathfrak{A}$.

Example 2.1.2.

(1) $\mathfrak{N} = \langle \mathbb{N}; 0, S, +, \cdot, < \rangle$ is an $\mathcal{L}_{ar}$-structure, with S the successor function assigning $x + 1$ to x, and the other symbols having their usual interpretation.

(2) $\mathfrak{C} = \langle \mathbb{C}; 0, 1, +, -, \cdot \rangle$, the field of complex numbers, is an $\mathcal{L}_{ring}$-structure.

(3) $\mathfrak{R} = \langle \mathbb{R}; 0, 1, +, -, \cdot, < \rangle$, the ordered field of real numbers, is an $\mathcal{L}_{o.ring}$-structure.

Definition. We say that two $\mathcal{L}$-structures $\mathfrak{A}$ and $\mathfrak{B}$ are *isomorphic*, $\mathfrak{A} \cong \mathfrak{B}$, if there exists an *isomorphism* $F : \mathfrak{A} \cong \mathfrak{B}$, that is, a bijection $F : A \to B$ between the base sets of $\mathfrak{A}$ and $\mathfrak{B}$ which commutes with the interpretations of the symbols in $\sigma^{\mathcal{L}}$, that is,

- $F(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$ for every constant symbol $c \in \mathcal{C}^{\mathcal{L}}$,
- $F(f^{\mathfrak{A}}(a_1, \dots, a_n)) = f^{\mathfrak{B}}(F(a_1), \dots, F(a_n))$ for every function symbol $f \in \mathcal{F}_n^{\mathcal{L}}$ and every tuple $(a_1, \dots, a_n) \in A^n$,
- $(a_1, \dots, a_n) \in R^{\mathfrak{A}} \iff (F(a_1), \dots, F(a_n)) \in R^{\mathfrak{B}}$ for every predicate $R \in \mathcal{R}_n^{\mathcal{L}}$ and every tuple $(a_1, \dots, a_n) \in A^n$.

2.2. Terms and Formulas

A *word* over a set (alphabet) E is a finite string $w = a_0 a_1 \cdots a_{k-1}$ with $a_i \in E$ for every i. We call k the *length* of w, and we denote by E^* the set of words over E.[1]

Definition. Let $\mathcal{L}$ be a language. The set $\mathcal{T}^{\mathcal{L}}$ of $\mathcal{L}$-terms is the smallest subset D of $\mathcal{L}^*$ containing the variables and the constant symbols such that if $f \in \mathcal{F}_n^{\mathcal{L}}$ and $t_1, \dots, t_n \in D$, then $f t_1 \cdots t_n \in D$.

It is easy to see that $\mathcal{T}^{\mathcal{L}} = \bigcup_{n\in\mathbb{N}} \mathcal{T}_n^{\mathcal{L}}$, where $\mathcal{T}_0^{\mathcal{L}} = \mathcal{C}^{\mathcal{L}} \cup \mathcal{V}^{\mathcal{L}}$ and, inductively,

$$\mathcal{T}_{n+1}^{\mathcal{L}} = \mathcal{T}_n^{\mathcal{L}} \cup \{f t_1 \cdots t_k \mid k \in \mathbb{N}^*, f \in \mathcal{F}_k^{\mathcal{L}} \text{ and } t_1, \dots, t_k \in \mathcal{T}_n^{\mathcal{L}}\}.$$

Proposition 2.2.1 (Unique reading of terms)**.** *Any term $t \in \mathcal{T}^{\mathcal{L}}$ satisfies one and only one of the following:*

(1) *t is a variable.*

(2) *t is a constant symbol.*

(3) *There exists a unique integer $n \geq 1$, a unique n-ary function symbol f and a unique sequence $(t_1, \dots, t_n)$ of terms such that $t = f t_1 \cdots t_n$.*

Proof. Exercise. (One first proves by induction on the length of terms that no proper initial segment of a term is a term.) □

Notation. For ease of reading, from now on we shall often write $f(t_1, \dots, t_n)$ instead of $f t_1 \cdots t_n$. When f is binary, we sometimes write $t_1 f t_2$ instead of $f t_1 t_2$. For instance, $(x + y) \cdot z$ means $\cdot + xyz$.

The *height* $\mathrm{ht}(t)$ of a term t is defined as the least natural number k such that $t \in \mathcal{T}_k^{\mathcal{L}}$. It follows from the unique reading property for terms that $\mathrm{ht}(f(t_1 \cdots t_n)) = 1 + \max(\mathrm{ht}(t_i))$. This will allow us to give definitions by induction on the height of terms.

Definition. An *atomic $\mathcal{L}$-formula* is

- either a word of the form $t_1 = t_2$, where t_1, t_2 are $\mathcal{L}$-terms,

[1] We will continue to write $\mathbb{N}^*$ for the set of non-zero natural numbers. As we will never use $\mathbb{N}$ as an alphabet, this should not cause any ambiguity.

- or a word of the form $Rt_1 \cdots t_n$, where $R \in \mathcal{R}_n^{\mathcal{L}}$ and all the t_i are $\mathcal{L}$-terms.

The set $\mathrm{Fml}^{\mathcal{L}}$ of *$\mathcal{L}$-formulas* is the smallest subset D of $\mathcal{L}^*$ that contains all atomic $\mathcal{L}$-formulas and such that if $x \in \mathcal{V}$ and $\varphi, \psi \in D$, then $\neg\varphi$, $(\varphi \wedge \psi)$ and $\exists x\varphi$ are all in D.

It is easy to see that $\mathrm{Fml}^{\mathcal{L}} = \bigcup_{n\in\mathbb{N}} \mathrm{Fml}_n^{\mathcal{L}}$, where $\mathrm{Fml}_0^{\mathcal{L}}$ is the set of atomic formulas, and, inductively,

$$\mathrm{Fml}_{n+1}^{\mathcal{L}} = \mathrm{Fml}_n^{\mathcal{L}} \cup \{\neg\varphi \mid \varphi \in \mathrm{Fml}_n^{\mathcal{L}}\} \cup \{(\varphi \wedge \psi) \mid \varphi, \psi \in \mathrm{Fml}_n^{\mathcal{L}}\}$$
$$\cup \{\exists x\varphi \mid x \in \mathcal{V} \text{ and } \varphi \in \mathrm{Fml}_n^{\mathcal{L}}\}.$$

Proposition 2.2.2 (Unique reading of formulas)**.** *Any $\mathcal{L}$-formula φ satisfies one and only one of the following:*

(1) *φ is an atomic formula.*

(2) *φ is equal to $\neg\psi$ for some unique $\mathcal{L}$-formula ψ.*

(3) *φ is equal to $(\psi \wedge \chi)$ for some unique $\mathcal{L}$-formulas ψ and χ.*

(4) *φ is equal to $\exists x\psi$ for some unique variable x and some unique $\mathcal{L}$-formula ψ.*

Proof. Exercise. (One first proves by induction on the length of formulas that no proper initial segment of a formula is a formula.) □

If φ is a formula, its *height* $\mathrm{ht}(\varphi)$ is defined as the least natural number k such that $\varphi \in \mathrm{Fml}_k^{\mathcal{L}}$. It follows from the unique reading property for formulas that $\mathrm{ht}((\varphi \wedge \psi)) = 1 + \max(\mathrm{ht}(\varphi), \mathrm{ht}(\psi))$ and $\mathrm{ht}(\exists x\varphi) = \mathrm{ht}(\neg\varphi) = 1 + \mathrm{ht}(\varphi)$. This will allow us to give definitions by induction on the height of formulas.

Definition.

(1) Let v_k be a variable. One defines, by induction on the height of a formula φ, the notion of a *free occurrence* of v_k in φ:
   - If φ is atomic, all occurrences of v_k in φ are free.
   - If φ is equal to $\neg\psi$, the free occurences of v_k in φ are those in ψ.
   - If φ is equal to $(\psi \wedge \chi)$, the free occurrences of v_k in φ are those in ψ and those in χ.

- If φ is equal to $\exists v_l \psi$ and $l \neq k$, the free occurrences of v_k in φ are those in ψ.
- If φ is equal to $\exists v_k \psi$, no occurrence of v_k in φ is free.

(2) Occurrences of v_k in φ which are not free are called *bound*.

(3) The *free variables of* φ are those having at least one free occurrence in φ. One denotes by $\mathrm{Free}(\varphi)$ as the set of free variables of φ.

(4) A *sentence* is a formula with no free variable.

Example. If φ is the formula $(\exists v_0\, v_0 < v_1 \wedge v_0 = v_1)$, the first two occurrences of v_0 are bound, and the third is free. All occurrences of v_1 in φ are free, thus $\mathrm{Free}(\varphi) = \{v_0, v_1\}$.

Notation. We will use the following abbreviations:

$(\varphi \vee \psi)$ for $\neg(\neg\varphi \wedge \neg\psi)$	(*disjunction*)
$(\varphi \to \psi)$ for $\neg(\varphi \wedge \neg\psi)$	(*implication*)
$(\varphi \leftrightarrow \psi)$ for $((\varphi \to \psi) \wedge (\psi \to \varphi))$	(*equivalence*)
$\forall x \varphi$ for $\neg\exists x \neg\varphi$	(*universal quantifier*).

We shall write $\exists x_1, \ldots, x_n$ instead of $\exists x_1 \cdots \exists x_n$ (similarly for the universal quantifier), $R(t_1, \ldots, t_n)$ instead of $Rt_1 \cdots t_n$, and sometimes $t_1 R t_2$ instead of $Rt_1 t_2$.

We shall write $(\varphi_0 \wedge \cdots \wedge \varphi_n)$ or sometimes $\bigwedge_{i=0}^{n} \varphi_i$ instead of $(\cdots((\varphi_0 \wedge \varphi_1) \wedge \varphi_2) \wedge \ldots \wedge \varphi_n)$, similarly for $\vee$ instead of $\wedge$.

Finally, to ease the reading of formulas, we shall sometimes add parentheses, or we will omit them. In this case, we shall read formulas according to the convention that symbols from $\{\neg, \exists, \forall\}$ bind the strongest, followed by $\wedge$, then $\vee$, and that symbols from $\{\to, \leftrightarrow\}$ bind the weakest.

Thus, for instance $\forall x \varphi \wedge \psi \to \chi$ shall mean $((\forall x \varphi \wedge \psi) \to \chi)$, that is, $\neg((\forall x \varphi \wedge \psi) \wedge \neg\chi)$, and so finally $\neg((\neg\exists x \neg\varphi \wedge \psi) \wedge \neg\chi)$.

Example. The field axioms can be expressed as first-order sentences in $\mathcal{L}_{ring}$:

(1) $\forall x\, x + \underline{0} = x$.

(2) $\forall x, y\, x + y = y + x$.

(3) $\forall x\, (-x) + x = \underline{0}$.

(4) $\forall x, y, z\,(x + y) + z = x + (y + z)$.

(5) $\forall x\, x \cdot \underline{1} = x$.

(6) $\forall x, y\, x \cdot y = y \cdot x$.

(7) $\forall x, y, z\,(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(8) $\forall x, y, z\, x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

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

(10) $\neg \underline{0} = \underline{1}$.

2.3. Semantics

We now explain how to interpret formulas in a given structure.

Definition. Let $\mathfrak{A}$ be an $\mathcal{L}$-structure.

(1) An *assignment* (*with values in* $\mathfrak{A}$) is a function $\alpha : \mathcal{V} \to A$ from the set of variables to the base set of $\mathfrak{A}$.

(2) If α is an assignment and t is an $\mathcal{L}$-term, one defines $t^{\mathfrak{A}}[\alpha]$, by induction on $\mathrm{ht}(t)$, in the following way:
- $v_i^{\mathfrak{A}}[\alpha] = \alpha(v_i)$ (for $v_i \in \mathcal{V}$) and $c^{\mathfrak{A}}[\alpha] = c^{\mathfrak{A}}$ (for $c \in \mathcal{C}^{\mathcal{L}}$),
- $f(t_1, \dots, t_n)^{\mathfrak{A}}[\alpha] = f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[\alpha], \dots, t_n^{\mathfrak{A}}[\alpha])$.

The proof of the following lemma is clear.

Lemma 2.3.1. *If two assignments α and β coincide on all variables having an occurrence in t, then $t^{\mathfrak{A}}[\alpha] = t^{\mathfrak{A}}[\beta]$.* □

Notation. If t is a term, we shall sometimes denote it by $t(x_1, \dots, x_n)$ if the variables x_i are distinct and all variables having at least one occurrence in t belong to the x_i.

If a term $t(x_1, \dots, x_n)$ and elements $a_1, \dots, a_n \in A$ are given, one defines $t^{\mathfrak{A}}[a_1, \dots, a_n]$ by $t^{\mathfrak{A}}[\alpha]$ with α an assignment with $\alpha(x_i) = a_i$ for all i, which is well defined by the previous lemma.

Definition (Satisfaction of a formula)**.** Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. By induction on the height of a formula φ, we now define for any assignment α the relation $\mathfrak{A} \vDash \varphi[\alpha]$ which will be read "φ is satisfied in $\mathfrak{A}$ by α":

$$\begin{aligned}
\mathfrak{A} \vDash t_1 = t_2[\alpha] &\quad :\Longleftrightarrow\quad t_1^{\mathfrak{A}}[\alpha] = t_2^{\mathfrak{A}}[\alpha] \\
\mathfrak{A} \vDash Rt_1 \cdots t_n[\alpha] &\quad :\Longleftrightarrow\quad (t_1^{\mathfrak{A}}[\alpha], \dots, t_n^{\mathfrak{A}}[\alpha]) \in R^{\mathfrak{A}} \\
\mathfrak{A} \vDash \neg\psi[\alpha] &\quad :\Longleftrightarrow\quad \mathfrak{A} \nvDash \psi[\alpha] \text{ (that is, not } \mathfrak{A} \vDash \psi[\alpha]) \\
\mathfrak{A} \vDash (\psi \wedge \chi)[\alpha] &\quad :\Longleftrightarrow\quad \mathfrak{A} \vDash \psi[\alpha] \text{ and } \mathfrak{A} \vDash \chi[\alpha] \\
\mathfrak{A} \vDash \exists x\psi[\alpha] &\quad :\Longleftrightarrow\quad \text{there exists } a \in A \text{ with } \mathfrak{A} \vDash \psi[\alpha_{a/x}].
\end{aligned}$$

Here, $\alpha_{a/x}$ denotes the assignment defined by $\alpha_{a/x}(x) = a$ and $\alpha_{a/x}(y) = \alpha(y)$ for $y \neq x$.

Proposition 2.3.2. *If two assignments α and β coincide on* Free(φ)*, then one has $\mathfrak{A} \vDash \varphi[\alpha]$ if and only if $\mathfrak{A} \vDash \varphi[\beta]$.*

Proof. By induction on ht(φ). The case of atomic formulas follows from Lemma 2.3.1. In the induction step, only the case where φ is equal to $\exists x\psi$ deserves an argument. If $\mathfrak{A} \vDash \varphi[\alpha]$, there exists $a \in A$ such that $\mathfrak{A} \vDash \psi[\alpha_{a/x}]$. Any variable $y \neq x$ that is free in ψ is also free in φ. Hence $\mathfrak{A} \vDash \psi[\beta_{a/x}]$ by the induction hypothesis, and so $\mathfrak{A} \vDash \varphi[\beta]$. □

Notation. A formula φ shall sometimes be denoted by $\varphi(x_1, \dots, x_n)$ if the variables x_i are distinct and all free variables in φ belong to the x_i.

If a formula $\varphi(x_1, \dots, x_n)$ and elements $a_1, \dots, a_n \in A$ are given, one defines $\mathfrak{A} \vDash \varphi[a_1, \dots, a_n]$ by $\mathfrak{A} \vDash \varphi[\alpha]$, where α is an assignment with $\alpha(x_i) = a_i$, which is well defined by the previous proposition.

Thus, $\varphi(x_1, \dots, x_n)$ defines an n-ary relation on the structure $\mathfrak{A}$, given by $\varphi[\mathfrak{A}] := \{(a_1, \dots, a_n) \in A^n \mid \mathfrak{A} \vDash \varphi[a_1, \dots, a_n]\}$.

In particular, when φ is a sentence, the relation

$$\mathfrak{A} \vDash \varphi$$

can be interpreted as "φ is *satisfied* (or *true*) in $\mathfrak{A}$" or "$\mathfrak{A}$ is a *model* of φ".

Example. An $\mathcal{L}_{ring}$-structure $\langle K; 0, 1, +, -, \cdot\rangle$ is a field if and only if it satisfies the field axioms (1)–(10) given previously.

Definition. Let $\mathfrak{A}$ be a structure and $D \subseteq A^n$.

- The set D is called $\emptyset$-*definable* in $\mathfrak{A}$ if $D = \varphi[\mathfrak{A}]$ for some formula $\varphi(x_1, \dots, x_n)$.
- Let $B \subseteq A$ be a parameter set. Then D is called B-*definable* in $\mathfrak{A}$ if there exist a formula $\varphi(x_1, \dots, x_n, y_1, \dots, y_m)$ and $\overline{b} \in B^m$ such

that D is equal to the set

$$\varphi[\mathfrak{A}, \overline{b}] := \{\overline{a} \in A^n \mid \mathfrak{A} \vDash \varphi[a_1, \dots, a_n, b_1, \dots, b_m]\}.$$

Exercise 2.3.3.

(1) Let $\mathfrak{A}$ be an $\mathcal{L}$-structure and B a non-empy subset of A containing the interpretations $c^{\mathfrak{A}}$ of all constants in $\mathcal{L}$ and which is closed under all operations $f^{\mathfrak{A}}$. Restricting the interpretations of all symbols from the set A to B one obtains an $\mathcal{L}$-structure $\mathfrak{B}$, called *substructure* of $\mathfrak{A}$. We shall write $\mathfrak{B} \subseteq \mathfrak{A}$ when $\mathfrak{B}$ is a substructure of $\mathfrak{A}$.

Prove that the intersection of a family of substructures of $\mathfrak{A}$ is either a substructure or empty. Deduce that any non-empty subset X of A is contained in a smallest substructure of $\mathfrak{A}$, called the *substructure generated by* X and denoted by $\langle X \rangle_{\mathfrak{A}}$. Prove that the base set of $\langle X \rangle_{\mathfrak{A}}$ is given by

$$\left\{ t^{\mathfrak{A}}[\alpha] \mid t \in \mathcal{T}^{\mathcal{L}} \text{ and } \alpha : \mathcal{V} \to X \right\}.$$

(2) Let $\mathfrak{A} = \langle A; 0, 1, +, -, \cdot \rangle$ be an $\mathcal{L}_{ring}$-structure. One assumes that $\mathfrak{A}$ is a ring. Prove that the substructure generated by a subset X of A is the subring generated by X.

2.4. Substitution

The aim of this section is to provide a satisfactory notion for the substitution in a formula φ of a variable x by a term s, in such a way that the expected semantical properties (cf. Proposition 2.4.2) are satisfied.

One might simply decide to replace every free occurrence of x in φ by s, but it might then happen that some variable in s becomes bound by a quantifier in the resulting formula. This could have unpleasant consequences, as for the formula $\varphi(v_0)$ given by $\exists v_1 \neg v_1 = v_0$, with $x = v_0$ and $s = v_1$, for which one would get the formula $\exists v_1 \neg v_1 = v_1$ which is satisfied in no structure, while as soon as $\mathfrak{A}$ contains at least two distinct elements, $\mathfrak{A} \vDash \varphi[a]$ for any $a \in A$.

The following somewhat more complicated definition remedies this issue.

Definition. Let $x_0, \dots, x_r$ be distinct variables and $s_0, \dots, s_r$ be terms. One defines the *similtaneous substitution* of the x_i by the s_i as follows.

(1) Let t be a term. Then $t_{s_0/x_0,\dots,s_r/x_r} = t_{\overline{s}/\overline{x}}$ is the word obtained by "simulatenously replacing all occurrences of x_i in t by s_i", that is, one sets
- $x_{\overline{s}/\overline{x}} = \begin{cases} x & \text{if } x \neq x_0, \dots, x \neq x_r, \\ s_i & \text{if } x = x_i, \end{cases}$
- $c_{\overline{s}/\overline{x}} = c$,
- $[f t^1 \cdots t^n]_{\overline{s}/\overline{x}} = f t^1_{\overline{s}/\overline{x}} \cdots t^n_{\overline{s}/\overline{x}}$, inductively.

(2) By induction on the height of a formula, one sets
- $[t = t']_{\overline{s}/\overline{x}}$ equal to $t_{\overline{s}/\overline{x}} = t'_{\overline{s}/\overline{x}}$,
- $[Rt^1 \cdots t^n]_{\overline{s}/\overline{x}}$ equal to $R t^1_{\overline{s}/\overline{x}} \cdots t^n_{\overline{s}/\overline{x}}$,
- $[\neg\psi]_{\overline{s}/\overline{x}}$ equal to $\neg[\psi]_{\overline{s}/\overline{x}}$, and finally
- $(\psi \wedge \chi)_{\overline{s}/\overline{x}}$ equal to $(\psi_{\overline{s}/\overline{x}} \wedge \chi_{\overline{s}/\overline{x}})$.
- Let $x_{i_1}, \dots, x_{i_k}$ $(i_1 < \dots < i_k)$ be those variables among $x_0, \dots, x_r$ that are free in $\exists x\psi$. (In particular one has $x \neq x_{i_1}, \dots, x \neq x_{i_k}$.)
  If x has no occurrence in any of $s_{i_1}, \dots, s_{i_k}$, one sets

  $$[\exists x\psi]_{\overline{s}/\overline{x}} \text{ equal to } \exists x[\psi]_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k}}.$$

  If x has some occurrence in one of $s_{i_1}, \dots, s_{i_k}$, one sets

(∗) $$[\exists x\psi]_{\overline{s}/\overline{x}} \text{ equal to } \exists u[\psi]_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k},u/x},$$

  where u is the first variable appearing in the enumeration $v_0, v_1, v_2, \dots$ which does not occur in any of the words $\exists x\psi, s_{i_1}, \dots, s_{i_k}$.

Exercise 2.4.1. Prove the following by induction on height:

(1) If t is a term, then $t_{\overline{s}/\overline{x}}$ is a term.

(2) If φ is a formula, then $\varphi_{\overline{s}/\overline{x}}$ is a formula. Moreover, one has $\mathrm{ht}(\varphi_{\overline{s}/\overline{x}}) = \mathrm{ht}(\varphi)$.

Let $x_0, \dots, x_r$ be distinct variables, α an assignment with values in $\mathfrak{A}$ and $a_0, \dots, a_r$ elements of A. One defines the assignment $\alpha_{a_0/x_0,\dots,a_r/x_r} = \alpha_{\overline{a}/\overline{x}}$ by $\alpha_{\overline{a}/\overline{x}}(x_i) = a_i$ and $\alpha_{\overline{a}/\overline{x}}(y) = \alpha(y)$ if $y \neq x_i$ for every i.

Proposition 2.4.2 (Substitution Lemma)**.** *Let $x_0, \dots, x_r$ be distinct variables, $s_0, \dots, s_r$ terms and α an assignment with values in $\mathfrak{A}$.*

(1) *For every term t one has $t^{\mathfrak{A}}_{\overline{s}/\overline{x}}[\alpha] = t^{\mathfrak{A}}\left[\alpha_{s_0^{\mathfrak{A}}[\alpha]/x_0,\dots,s_r^{\mathfrak{A}}[\alpha]/x_r}\right]$.*

(2) *For every formula φ one has*

$$\mathfrak{A} \vDash \varphi_{\overline{s}/\overline{x}}[\alpha] \text{ if and only if } \mathfrak{A} \vDash \varphi\left[\alpha_{s_0^{\mathfrak{A}}[\alpha]/x_0,\dots,s_r^{\mathfrak{A}}[\alpha]/x_r}\right].$$

Proof. (1) is easy. One proves (2) by induction on the height of φ, the only non-trivial case being when φ is of the form $\exists x\psi$. As in the definition of $[\exists x\psi]_{\overline{s}/\overline{x}}$, one denotes by $x_{i_1}, \dots, x_{i_k}$ the variables that are exactly those among the x_i which are free in $\exists x\psi$. Assume first that x occurs in one of the terms $s_{i_1}, \dots, s_{i_k}$, and let u be the variable chosen as in $(*)$. Then

$$\begin{aligned}
&\mathfrak{A} \vDash [\exists x\psi]_{\overline{s}/\overline{x}}[\alpha] \iff \mathfrak{A} \vDash \exists u[\psi]_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k},u/x}[\alpha] \\
\iff &\text{there exists } a \in A \text{ such that } \mathfrak{A} \vDash \psi_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k},u/x}[\alpha_{a/u}] \\
\iff &\text{(by the induction hypothesis) there exists } a \in A \text{ such that} \\
&\mathfrak{A} \vDash \psi[\alpha_{s_{i_1}^{\mathfrak{A}}[\alpha_{a/u}]/x_{i_1},\dots,s_{i_k}^{\mathfrak{A}}[\alpha_{a/u}]/x_{i_k},u^{\mathfrak{A}}[\alpha_{a/u}]/x}] \\
\iff &\text{there exists } a \in A \text{ such that } \mathfrak{A} \vDash \psi[\alpha_{s_{i_1}^{\mathfrak{A}}[\alpha]/x_{i_1},\dots,s_{i_k}^{\mathfrak{A}}[\alpha]/x_{i_k},a/x}] \\
&\text{(by Lemma 2.3.1, since } u \text{ does not occur in any of the } s_{i_j}) \\
\iff &\mathfrak{A} \vDash \exists x\psi[\alpha_{s_{i_1}^{\mathfrak{A}}[\alpha]/x_{i_1},\dots,s_{i_k}^{\mathfrak{A}}[\alpha]/x_{i_k}}] \\
\iff &\mathfrak{A} \vDash \exists x\psi[\alpha_{s_0^{\mathfrak{A}}[\alpha]/x_0,\dots,s_r^{\mathfrak{A}}[\alpha]/x_r}].
\end{aligned}$$

The last equivalence follows from Proposition 2.3.2, since the assignments $\alpha_{s_{i_1}^{\mathfrak{A}}[\alpha]/x_{i_1},\dots,s_{i_k}^{\mathfrak{A}}[\alpha]/x_{i_k}}$ and $\alpha_{s_0^{\mathfrak{A}}[\alpha]/x_0,\dots,s_r^{\mathfrak{A}}[\alpha]/x_r}$ coincide on the set $\mathrm{Free}(\exists x\psi)$.

Assume now that the variable x has no occurrence in any of the terms $s_{i_1}, \dots, s_{i_k}$. Then

$$\begin{aligned}
&\mathfrak{A} \vDash [\exists x\psi]_{\overline{s}/\overline{x}}[\alpha] \iff \mathfrak{A} \vDash \exists x[\psi]_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k}}[\alpha] \\
\iff &\text{there exists } a \in A \text{ with } \mathfrak{A} \vDash \psi_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k}}[\alpha_{a/x}] \\
\iff &\text{(by the induction hypothesis and since } x \neq x_{i_1}, \dots, x \neq x_{i_k}) \\
&\text{there exists } a \in A \text{ with } \mathfrak{A} \vDash \psi[\alpha_{s^{\mathfrak{A}}_{i_1}[\alpha_{a/x}]/x_{i_1},\dots,s^{\mathfrak{A}}_{i_k}[\alpha_{a/x}]/x_{i_k},a/x}] \\
\iff &\mathfrak{A} \vDash \exists x\psi[\alpha_{s^{\mathfrak{A}}_{i_1}[\alpha]/x_{i_1},\dots,s^{\mathfrak{A}}_{i_k}[\alpha]/x_{i_k}}] \\
\iff &\mathfrak{A} \vDash \exists x\psi[\alpha_{s^{\mathfrak{A}}_0[\alpha]/x_0,\dots,s^{\mathfrak{A}}_r[\alpha]/x_r}].
\end{aligned}$$

□

Example 2.4.3.

(1) Let $\varphi(v_0)$ be the formula $\exists v_1 \neg v_1 = v_0$, and let $s = v_1$. Then φ_{s/v_0} is equal to $\exists v_2[\neg v_1 = v_0]_{v_1/v_0,v_2/v_1}$, that is, to $\exists v_2 \neg v_2 = v_1$.

(2) Let φ be a formula and $x_1, \dots, x_n$ be distinct variables. One assumes that $s_1, \dots, s_n$ do not contain any variables having an occurrence in φ. Then $\varphi_{\overline{s}/\overline{x}}$ is the word obtained by simultaneously replacing every free occurrence of x_i by s_i.

We prove this by induction on $\mathrm{ht}(\varphi)$, the only non-trivial case being when φ is of the form $\exists x\psi$. Let $i_1 < \dots < i_k$ be chosen as in the definition of $\varphi_{\overline{s}/\overline{x}}$. By assumption, x has no occurrence in any of $s_{i_1}, \dots, s_{i_k}$, and so by definition $[\exists x\psi]_{\overline{s}/\overline{x}}$ equals $\exists x\psi_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k}}$. As the s_{i_j} do not contain any variables occurring in ψ, $\psi_{s_{i_1}/x_{i_1},\dots,s_{i_k}/x_{i_k}}$ is inductively given by simultaneously replacing every free occurrence of x_{i_j} by s_{i_j}, for $j = 1, \dots, k$. This proves the result.

Lemma 2.4.4. *If y is a variable with no occurrence in φ, then $\left[\varphi_{y/x}\right]_{x/y}$ is equal to φ.*

Proof. The proof is by induction on $\mathrm{ht}(\varphi)$, the only non-trivial case being when φ is of the form $\exists z\psi$. If x is not free in φ, then $\left[\varphi_{y/x}\right]_{x/y}$ equals $\varphi_{x/y}$ by Example 2.4.3(2), and so is equal to φ by definition, as y does not occur in φ at all. We may thus assume that x is free in $\exists z\psi$, so in particular $z \neq x$ and $z \neq y$. Hence by definition $\left[[\exists z\psi]_{y/x}\right]_{x/y}$ is equal to

$\left[\exists z[\psi]_{y/x}\right]_{x/y}$, which is equal to $\exists z\left[[\psi]_{y/x}\right]_{x/y}$. But $\left[\psi_{y/x}\right]_{x/y}$ equals ψ by the induction hypothesis. □

Notation. Let $s_1, \dots, s_n$ be terms. If $t(x_1, \dots, x_n)$ is a term, we shall often write $t(s_1, \dots, s_n)$ for $t_{s_1/x_1,\dots,s_n/x_n}$, and $\varphi(s_1, \dots, s_n)$ instead of $\varphi_{s_1/x_1,\dots,s_n/x_n}$ if φ is a formula of the form $\varphi(x_1, \dots, x_n)$.

2.5. Universally Valid Formulas

Definition. An $\mathcal{L}$-formula φ is called *universally valid*, written $\models \varphi$, if it is satisfied in every $\mathcal{L}$-structure $\mathfrak{A}$ and for any assignment α with values in $\mathfrak{A}$, that is, if $\mathfrak{A} \models \varphi[\alpha]$ for every $\mathfrak{A}$ and every α.

Remark 2.5.1. The formula $\varphi(x_1, \dots, x_n)$ is universally valid if and only if the sentence $\forall x_1, \dots, x_n \varphi$ is universally valid.

We call $\forall x_1, \dots, x_n \varphi$ a *universal closure of* φ. We will write $\mathfrak{A} \models \varphi$ for $\mathfrak{A} \models \forall x_1, \dots, x_n \varphi$.

Example.

(1) $\exists x\, x = x$ is universally valid. (By definition, a structure is non-empty!)

(2) Let φ and ψ be $\mathcal{L}$-formulas. Then $(\varphi \to (\psi \to \varphi))$ is universally valid.

The fact that we do not mention the language $\mathcal{L}$ in the notation $\models \varphi$ is justified by the next lemma. First some terminology.

Definition. Let $\mathcal{L} \subseteq \mathcal{L}'$ be two languages. If $\mathfrak{A}' = \langle A; (Z^{\mathfrak{A}'})_{Z \in \sigma^{\mathcal{L}'}} \rangle$ is an $\mathcal{L}'$-structure, we set $\mathfrak{A} := \mathfrak{A}' \restriction_{\mathcal{L}} := \langle A; (Z^{\mathfrak{A}'})_{Z \in \sigma^{\mathcal{L}}} \rangle$, the *reduct of* $\mathfrak{A}'$ *to* $\mathcal{L} \subseteq \mathcal{L}'$. The structure $\mathfrak{A}'$ is called an *expansion of* $\mathfrak{A}$ *to* $\mathcal{L}'$.

Lemma 2.5.2. *Let φ be an $\mathcal{L}$-formula and $\mathcal{L}' \supseteq \mathcal{L}$. Then φ is universally valid as an $\mathcal{L}$-formula if and only if it is universally valid as an $\mathcal{L}'$-formula.*

Proof. One may identify assignments with values in $\mathfrak{A}$ and those with values in $\mathfrak{A}'$, and one has $\mathfrak{A}' \models \varphi[\alpha] \iff \mathfrak{A} \models \varphi[\alpha]$ for any assignment α. Thus it suffices to prove that any $\mathcal{L}$-structure $\mathfrak{A}$ has an expansion to some $\mathcal{L}'$-structure, which is clear. □

We now specify a framework for formulas like $(\varphi \to (\psi \to \varphi))$ which are always satisfied independently of the truth values of φ and of ψ, namely *propositional calculus*.

One fixes a set $\mathcal{P} = \{p_i \mid i \in \mathbb{N}\}$, where the p_i are called *propositional variables* (they will take only "true" or "false" as values).

Propositional calculus formulas are defined as words over the alphabet $\mathcal{P} \cup \{\neg, \wedge, (,)\}$, formed according to the following rules:

- p_i is a formula for any i;
- if F and G are formulas, then $\neg F$ and $(F \wedge G)$ are formulas, too.

Let $\mathrm{Fml}_{\mathcal{P}}$ denote the set of propositional calculus formulas. As before we introduce the abbreviations $\vee$, $\to$ and $\leftrightarrow$.

One identifies $\mathbb{Z}/2 = \{0, 1\}$ with {"false", "true"}, by assigning 0 to "false" and 1 to "true". An *assignment* is a function $\delta : \mathcal{P} \to \{0, 1\}$.

Any assignment δ induces a function $\delta^* : \mathrm{Fml}_{\mathcal{P}} \to \{0, 1\}$ defined by $\delta^*(p_i) = \delta(p_i)$, $\delta^*(\neg F) = 1 - \delta^*(F)$ and $\delta^*((F \wedge G)) = \delta^*(F) \cdot \delta^*(G)$, inductively. If $\delta^*(F) = 1$, we also write $\delta \vDash F$.

One writes $F = F(q_1, \dots, q_n)$ if the q_i are distinct variables and all variables occurring in F belong to the q_i.

Exercise 2.5.3. For any function $g : \{0, 1\}^n \to \{0, 1\}$ there exists a propositional calculus formula $F(p_1, \dots, p_n)$ such that, for any assignment δ, one has $\delta^*(F) = g(\delta(p_1), \dots, \delta(p_n))$.

Definition.

(1) One says that a formula $F \in \mathrm{Fml}_{\mathcal{P}}$ is a *tautology for the propositional calculus* if $\delta \vDash F$ for any assignment δ. This can be rephrased by saying that $F = F(q_1, \dots, q_n)$ is true for any choice of truth values for the q_i.

(2) An $\mathcal{L}$-formula φ is a *tautology for the predicate calculus* if there exists $F = F(q_1, \dots, q_n)$ a tautology for the propositional calculus and $\mathcal{L}$-formulas $\psi_1, \dots, \psi_n$ such that φ equals $F_{\psi_1/q_1, \dots, \psi_n/q_n}$ (the word obtained by replacing the variables q_i by ψ_i).

Lemma 2.5.4. *Tautologies for the predicate calculus are universally valid formulas.*

Proof. Clear. □

Lemma 2.5.5 (Equality axioms)**.** *The following sentences are universally valid:*

- $\forall v_0\, v_0 = v_0$ (*reflexivity,* E1)
- $\forall v_0, v_1 (v_0 = v_1 \to v_1 = v_0)$ (*symmetry,* E2)
- $\forall v_0, v_1, v_2 ((v_0 = v_1 \wedge v_1 = v_2) \to v_0 = v_2)$ (*transitivity,* E3)
- $\forall v_1, \dots, v_{2n} \left(\bigwedge_{i=1}^{n} v_i = v_{i+n} \to f v_1 \cdots v_n = f v_{n+1} \cdots v_{2n}\right)$ *for any* $f \in \mathcal{F}_n^{\mathcal{L}}$ (*congruence for functions,* E4)
- $\forall v_1, \dots, v_{2n} (\left(\bigwedge_{i=1}^{n} v_i = v_{i+n} \wedge R v_1 \cdots v_n\right) \to R v_{n+1} \cdots v_{2n}\big)$ *for any* $R \in \mathcal{R}_n^{\mathcal{L}}$ (*congruence for relations,* E5)*.*

Proof. Clear. □

Remark. The sentences (E1-E5) express that $=$ is a *congruence relation*, that is, an equivalence relation compatible with the functions and the relations of the language.

Lemma 2.5.6 (Quantifier axioms)**.** *Let φ and ψ be $\mathcal{L}$-formulas.*

(1) *For every variable x which is not free in φ, the formula*

(Q1) $$\forall x (\varphi \to \psi) \to (\varphi \to \forall x \psi)$$

is univerally valid.

(2) *For every variable x and every term t, the formula*

(Q2) $$\varphi_{t/x} \to \exists x \varphi$$

is universally valid.

(3) *For every variable x the formula*

(Q3) $$\exists x \varphi \leftrightarrow \neg \forall x \neg \varphi$$

is universally valid.

Proof. (2) follows easily from the Substitution Lemma (Proposition 2.4.2), and (3) is clear.

We will now prove (1). Suppose that $x \notin \mathrm{Free}(\varphi)$, and that $\mathfrak{A} \vDash \forall x (\varphi \to \psi)[\alpha]$, that is, $\mathfrak{A} \vDash \neg \exists x (\varphi \wedge \neg \psi)[\alpha]$, from which we infer $\mathfrak{A} \vDash (\neg \varphi \vee \psi)[\alpha_{a/x}]$ for any $a \in A$. We have to prove that $\mathfrak{A} \vDash (\varphi \to \forall x \psi)[\alpha]$,

and for this we may assume that $\mathfrak{A} \models \varphi[\alpha]$. But then $\mathfrak{A} \models \varphi[\alpha_{a/x}]$ by Proposition 2.3.2, as $x \notin \text{Free}(\varphi)$, and so $\mathfrak{A} \models \psi[\alpha_{a/x}]$. Since $a \in A$ was arbitrary, $\mathfrak{A} \models \forall x\, \psi[\alpha]$ follows. □

Remark. The restriction on the variable x in (Q1) is necessary, as shown by the following example. Let both φ and ψ be equal to the formula $x = c$, where c is a constant symbol. Then $\models \forall x(\varphi \to \psi)$, but in any structure $\mathfrak{A}$ with a base set that contains at least 2 elements, one has $\mathfrak{A} \not\models \forall x\,(\varphi \to \forall x\, \psi)$.

Definition. An $\mathcal{L}$-*theory* is a set of $\mathcal{L}$-sentences.

Let T be an $\mathcal{L}$-theory.

- One says that the $\mathcal{L}$-structure $\mathfrak{A}$ is a *model of* T, which we denote by $\mathfrak{A} \models T$, if $\mathfrak{A} \models \varphi$ for any $\varphi \in T$.
- A sentence (or more generally a formula) φ is a *logical consequence* of T, denoted by $T \models \varphi$, if for any $\mathcal{L}$-structure $\mathfrak{A}$ which is a model of T we have $\mathfrak{A} \models \varphi$ (that is, in case of a formula $\varphi(x_1, \dots, x_n)$, we require $\mathfrak{A} \models \forall x_1, \dots, x_n\, \varphi$).

By the proof of Lemma 2.5.2, the fact that $T \models \varphi$ is independent of the language $\mathcal{L}$.

2.6. Formal Proofs and Gödel's Completeness Theorem

In this section we will prove Gödel's Completeness Theorem, which states that any universally valid $\mathcal{L}$-formula may be obtained using a finite deduction (a formal proof). This fundamental result establishes a perfect correspondence between semantic truth and syntactic provability in first-order logic.

We will start by formalizing the notion of proof.

By the *logical axioms* we mean:

- predicate calculus tautologies,
- the equality axioms (E1-E5) from Lemma 2.5.5,
- the quantifier axioms (Q1-Q3) from Lemma 2.5.6.

There will be two *deduction rules*:

- (MP) Modus Ponens: From φ and $\varphi \to \psi$, one can deduce ψ.
- Generalization: From φ, one can deduce $\forall x\, \varphi$ (x any variable).

Definition.

(1) Let φ be an $\mathcal{L}$-formula and T be an $\mathcal{L}$-theory. A *formal proof of φ in T* is a finite sequence of $\mathcal{L}$-formulas $(\varphi_0, \dots, \varphi_n)$ with φ_n equal to φ such that, for every $i \leq n$, either $\varphi_i \in T$, or φ_i is a logical axiom, or it can be deduced by (MP) from some φ_j and φ_k with $j, k < i$, or it can be obtained by generalization from a formula φ_j with $j < i$.

(2) One says that φ is *provable in T*, denoted by $T \vdash_{\mathcal{L}} \varphi$, if there exists a formal proof of φ in T. We write $\vdash_{\mathcal{L}} \varphi$ if φ is provable in the empty theory.

A priori, $\vdash_{\mathcal{L}}$ depends on the language $\mathcal{L}$ in which the formula φ and the theory T are considered, since if $\mathcal{L}' \supseteq \mathcal{L}$, there are more $\mathcal{L}'$-proofs than $\mathcal{L}$-proofs. However we shall see that $T \models \varphi$ if and only if $T \vdash_{\mathcal{L}} \varphi$, which shows in particular that the provability of a formula is independent of the language.

In the sequel, we shall consider proofs $(\varphi_0, \dots, \varphi_n)$ in which formulas φ_i whose provability has been previously established will be considered as axioms. It is always possible to transform such a proof into a formal proof; it is enough to replace φ_i by a formal proof of φ_i.

Example 2.6.1.

(1) If φ and ψ are $\mathcal{L}$-sentences, then $\{\varphi, \psi\} \vdash_{\mathcal{L}} \varphi \wedge \psi$.

Now let φ be an $\mathcal{L}$-formula, x, y variables and t an $\mathcal{L}$-term. Then we have the following:

(2) $\vdash_{\mathcal{L}} \forall x\, \varphi \to \varphi_{t/x}$.

(3) If y does not occur in φ, then $\vdash_{\mathcal{L}} \forall y\, \varphi_{y/x} \to \forall x\, \varphi$.

(4) $\vdash_{\mathcal{L}} \forall x\, \varphi \to \varphi$.

Proof. (1) From φ and the tautology $\varphi \to (\psi \to (\varphi \wedge \psi))$ one deduces $\psi \to (\varphi \wedge \psi)$ by (MP), from which one deduces $\varphi \wedge \psi$, using ψ and applying (MP) again.

(2) Here is a formal proof of $\forall x\,\varphi \to \varphi_{t/x}$ (recall that by definition $\forall x\,\varphi$ is the formula $\neg\exists x\neg\varphi$):

φ_0 equals $(\neg\varphi_{t/x} \to \exists x\,\neg\varphi)$	(Q2)
φ_1 equals $(\neg\varphi_{t/x} \to \exists x\,\neg\varphi) \to (\neg\exists x\,\neg\varphi \to \varphi_{t/x})$	(tautology)
φ_2 equals $\forall x\,\varphi \to \varphi_{t/x}$	(MP).

(3) The formula $\forall y\,\varphi_{y/x} \to \left[\varphi_{y/x}\right]_{x/y}$ is an instance of (2). Since $\left[\varphi_{y/x}\right]_{x/y}$ equals φ by Lemma 2.4.4, we get $\forall x\,(\forall y\,\varphi_{y/x} \to \varphi)$ by generalization, from which we conclude by the quantifier axiom (Q1) and (MP).

(4) is a special case of (2), since φ is equal to $\varphi_{x/x}$. □

Lemma 2.6.2 (Soundness)**.** *Let T be an $\mathcal{L}$-theory and φ an $\mathcal{L}$-formula. Then*

$$T \vdash_{\mathcal{L}} \varphi \Rightarrow T \vDash \varphi.$$

Proof. The logical axioms are universally valid by Lemma 2.5.4, Lemma 2.5.5 and Lemma 2.5.6. Clearly, if $T \vDash \varphi$ and $T \vDash \varphi \to \psi$, then $T \vDash \psi$. It is also easy to see that $T \vDash \varphi$ implies $T \vDash \forall x\,\varphi$. By induction on the length of a formal proof, we are done. □

Definition. Let T be an $\mathcal{L}$-theory.

- T is *inconsistent* if there exists an $\mathcal{L}$-sentence φ such that $T \vdash_{\mathcal{L}} \varphi$ and $T \vdash_{\mathcal{L}} \neg\varphi$.
- T is *consistent* if it is not inconsistent.
- T is *complete* if it is consistent and for any $\mathcal{L}$-sentence φ either $T \vdash_{\mathcal{L}} \varphi$ or $T \vdash_{\mathcal{L}} \neg\varphi$.

Example 2.6.3.

(1) Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. Then the set

$$\mathrm{Th}(\mathfrak{A}) := \{\varphi \text{ is } \mathcal{L}\text{-sentence} \mid \mathfrak{A} \vDash \varphi\}$$

is a theory, called the *theory of* $\mathfrak{A}$. It is a complete theory (its consistency follows from Lemma 2.6.2).

(2) The theory of algebraically closed fields is the $\mathcal{L}_{ring}$-theory ACF which is composed of the field axioms together with a sentence χ_n for any $n \geq 1$ expressing that any polynomial of degree n has a root. For instance, the formula χ_n given by $\forall z_0,\ldots,z_{n-1}\exists x(x^n +$

$z_{n-1}x^{n-1}+...+z_0 = 0$) works; that formula can be rewritten in $\mathcal{L}_{ring}$.

Remark 2.6.4.

(1) An $\mathcal{L}$-theory T is inconsistent if and only if $T \vdash_{\mathcal{L}} \varphi$ for any $\mathcal{L}$-formula φ.

(2) If $T \vdash_{\mathcal{L}} \varphi$, there exists $T_0 \subseteq T$ finite such that $T_0 \vdash_{\mathcal{L}} \varphi$.

Proof. Exercise. □

Corollary 2.6.5.

(1) *Let T be an $\mathcal{L}$-theory such that all finite subsets of T are consistent. Then T is consistent, too.*

(2) *Let $(T_i)_{i\in I}$ be a family of consistent $\mathcal{L}$-theories, with $T_i \subseteq T_j$ or $T_j \subseteq T_i$ for any $i, j \in I$. Then $T = \bigcup_{i\in I} T_i$ is consistent, too.* □

Lemma 2.6.6 (Deduction Lemma)**.** *Let χ be an $\mathcal{L}$-sentence, T an $\mathcal{L}$-theory and φ an $\mathcal{L}$-formula. Then*

$$T \cup \{\chi\} \vdash_{\mathcal{L}} \varphi \text{ if and only if } T \vdash_{\mathcal{L}} \chi \to \varphi.$$

Proof. It is clear that $T \vdash_{\mathcal{L}} \chi \to \varphi$ implies that $T\cup\{\chi\} \vdash_{\mathcal{L}} \varphi$. Conversely, let $(\varphi_0, ..., \varphi_n)$ be a formal proof of φ in $T\cup\{\chi\}$. By induction on i, we shall prove that $T \vdash_{\mathcal{L}} (\chi \to \varphi_i)$. If φ_i equals χ, this is clear, and if $T \vdash_{\mathcal{L}} \varphi_i$, it follows from (MP) and the fact that $(\varphi_i \to (\chi \to \varphi_i))$ is a tautology. This implies that $T \vdash_{\mathcal{L}} (\chi \to \varphi_i)$ when φ_i is a logical axiom or an element of T.

If φ_i is deduced by (MP) applied to φ_j and φ_k for $j, k < i$, so φ_k equals $\varphi_j \to \varphi_i$, it is enough to use (MP) together with the fact that $((\chi \to \varphi_j) \wedge (\chi \to (\varphi_j \to \varphi_i)) \to (\chi \to \varphi_i))$ is a tautology.

Finally, if φ_i is obtained by generalization from φ_j for $j < i$, so φ_i equals $\forall x\varphi_j$, we have $T \vdash_{\mathcal{L}} \chi \to \varphi_j$ by induction, from which we deduce $T \vdash_{\mathcal{L}} \forall x\,(\chi \to \varphi_j)$ by generalization. Now, χ being a sentence, the formula $\forall x\,(\chi \to \varphi) \to (\chi \to \forall x\,\varphi)$ is a quantifier axiom, so we conclude that $T \vdash_{\mathcal{L}} \chi \to \forall x\,\varphi$ by (MP). □

Corollary 2.6.7. *Let T be an $\mathcal{L}$-theory and φ an $\mathcal{L}$-sentence. Then $T \vdash_{\mathcal{L}} \varphi$ if and only if $T \cup \{\neg\varphi\}$ is inconsistent.*

Proof. The 'only if' part is clear. Conversely, if $T \cup \{\neg\varphi\}$ is inconsistent, then $T \cup \{\neg\varphi\} \vdash_{\mathcal{L}} \varphi$ by Remark 2.6.4(1). It follows from the Deduction Lemma that $T \vdash_{\mathcal{L}} \neg\varphi \to \varphi$. Since $(\neg\varphi \to \varphi) \to \varphi$ is a tautology, we conclude by (MP). □

Lemma 2.6.8 (Simulation of constants by variables)**.** *Let ψ be an $\mathcal{L}$-formula, T an $\mathcal{L}$-theory, and let C be a set of constant symbols such that $\mathcal{L} \cap C = \emptyset$.*

(a) *Let x be a variable and $c \in C$. The following are equivalent:*
   (1) $T \vdash_{\mathcal{L}} \psi$,
   (2) $T \vdash_{\mathcal{L}\cup\{c\}} \psi_{c/x}$,
   (3) $T \vdash_{\mathcal{L}\cup\{c\}} \psi$.

(b) *One has $T \vdash_{\mathcal{L}} \psi$ if and only if $T \vdash_{\mathcal{L}\cup C} \psi$.*

Proof. For ease of notation we shall assume $T = \emptyset$; the proof for general T is just the same. Let us start by proving (a).

(1)⇒(3) is clear since any $\mathcal{L}$-proof is an $\mathcal{L} \cup \{c\}$-proof.

(3)⇒(2). If $\vdash_{\mathcal{L}\cup\{c\}} \psi$, then generalization yields $\vdash_{\mathcal{L}\cup\{c\}} \forall x\psi$. Using Example 2.6.1(2) and (MP), one deduces $\vdash_{\mathcal{L}\cup\{c\}} \psi_{c/x}$.

(2)⇒(1). For $\tilde{\varphi}$ an $\mathcal{L} \cup \{c\}$-formula and y a variable not occurring in $\tilde{\varphi}$, we denote by φ and also by $\tilde{\varphi}_{y/c}$ the word obtained by substituting every occurrence of c in $\tilde{\varphi}$ by y.

Let $\tilde{\varphi}, \tilde{\psi}$ and $\tilde{\chi}$ be $\mathcal{L} \cup \{c\}$-formulas with no occurrence of y. Then the following statements hold:

(i) φ is an $\mathcal{L}$-formula.

(ii) $\varphi_{c/y}$ is equal to $\tilde{\varphi}$.

(iii) If $\tilde{\varphi}$ is an equality axiom (respectively a tautology or a quantifier axiom), then φ is so, too.

(iv) If $\tilde{\varphi}$ is obtained using (MP) from $\tilde{\psi}$ and $\tilde{\chi}$, then φ is obtained using (MP) from ψ and χ.

(v) If $\tilde{\varphi}$ is obtained using generalization from $\tilde{\psi}$, then φ is obtained using generalization from ψ.

One proves (i) by induction on the height of φ, and (ii) follows from Example 2.4.3(2). The statements (iv) and (v) are immediate, and also

the case of an equality axiom, a tautology or an instance of (Q1) or (Q3) in (iii). It remains to check the case of an instance of (Q2) in (iii): If $\tilde{\varphi}$ is of the form $(\tilde{\delta}_{t/x} \to \exists x \tilde{\delta})$, one has to prove that the formula φ, which is given by $([\tilde{\delta}_{t/x}]_{y/c} \to \exists x [\tilde{\delta}]_{y/c})$, is an instance of (Q2). This follows from the fact that $[\tilde{\delta}_{t/x}]_{y/c}$ and $[\tilde{\delta}_{y/c}]_{t_{y/c}/x}$ are equal, which is proved by induction on height.

Now, let $(\tilde{\varphi}^0, \dots, \tilde{\varphi}^m)$ be a formal proof of $\psi_{c/x}$ in the language $\mathcal{L} \cup \{c\}$. Choose a variable y not occurring in any of $\tilde{\varphi}^0, \dots, \tilde{\varphi}^m$ and such that $y \neq x$.

One deduces from (i)-(v) that $(\varphi^0, \dots, \varphi^m)$ is a formal proof in the language $\mathcal{L}$ of $\left[\psi_{c/x}\right]_{y/c}$, which is equal to $\psi_{y/x}$ by Example 2.4.3(2).

By generalization one gets $\vdash_{\mathcal{L}} \forall y\, \psi_{y/x}$. Using Example 2.6.1(3,4) and (MP), one gets $\vdash_{\mathcal{L}} \psi$, which completes the proof of (2)⇒(1).

Item (b) is a direct consequence of (a). Indeed, as any $\mathcal{L} \cup C$-proof involves only a finite number of elements of C, one may assume that C is finite. One concludes by induction on the cardinality of C, using (1)⇔(3). □

Lemma 2.6.9. *Let T be an $\mathcal{L}$-theory, $\varphi(x)$ an $\mathcal{L}$-formula and $c \in \mathcal{L}$ a constant symbol not occurring in $T \cup \{\varphi(x)\}$. Assume that T is consistent. Then $T \cup \{\exists x \varphi \to \varphi_{c/x}\}$ is a consistent $\mathcal{L}$-theory.*

Proof. If the conclusion does not hold, then $T \vdash_{\mathcal{L}} \exists x\, \varphi \wedge \neg \varphi_{c/x}$ by Corollary 2.6.7. In particular, $T \vdash_{\mathcal{L}} \exists x\, \varphi$, and, by Lemma 2.6.8(a), $T \vdash_{\mathcal{L}} \neg \varphi$, so $T \vdash_{\mathcal{L}} \forall x \neg \varphi$ by generalization. Using the quantifier axiom (Q3) and (MP), it follows that T is inconsistent. □

Theorem 2.6.10 (Gödel's Completeness Theorem)**.** *Let T be an $\mathcal{L}$-theory and φ an $\mathcal{L}$-sentence. Then $T \vDash \varphi$ if and only if $T \vdash_{\mathcal{L}} \varphi$.*

Remark. Since $\vDash$ does not depend on the language $\mathcal{L}$, a posteriori $\vdash_{\mathcal{L}}$ does not depend on $\mathcal{L}$ either. Thus, once Gödel's Completeness Theorem is proved, we shall write $\vdash$ instead of $\vdash_{\mathcal{L}}$.

Proof. $T \vdash_{\mathcal{L}} \varphi \Rightarrow T \vDash \varphi$. This is the easy direction in Gödel's theorem and it expresses that our notion of formal proof is sound. It holds by Lemma 2.6.2.

$T \models \varphi \Rightarrow T \vdash_{\mathcal{L}} \varphi$. This is the non-trivial direction. It will follow from the next theorem, which is an existence statement for models. In fact, as

$$T \not\models \varphi \iff T \cup \{\neg\varphi\} \text{ has a model} \qquad \text{(by definition) and}$$
$$T \not\vdash_{\mathcal{L}} \varphi \iff T \cup \{\neg\varphi\} \text{ is consistent} \qquad \text{(by Corollary 2.6.7),}$$

this theorem is equivalent to the Completeness Theorem. □

Theorem 2.6.11. *A theory has a model if and only if it is consistent.*

Proof. The easy direction was already proved. To prove that any consistent theory T has a model, we will start by constructing an expansion T^+ of T in some language $\mathcal{L}^+ \supseteq \mathcal{L}$ which has better properties. Let us begin with a definition.

Definition. Let $\mathcal{L}$ be a language and C a set of constant symbols with $\mathcal{L} \cap C = \emptyset$. One says that an $\mathcal{L} \cup C$-theory T^+ *admits Henkin witnesses in* C if for any $\mathcal{L} \cup C$-formula $\varphi(x)$ there exists $c \in C$ such that $\exists x\varphi \to \varphi_{c/x} \in T^+$.

If $\mathfrak{A}$ is an $\mathcal{L}$-structure and $A = \{a_c \mid c \in C\}$ is an enumeration (possibily non-injective) of its base set by C, one denotes by $\mathfrak{A}^+$ the $\mathcal{L} \cup C$-structure obtained from $\mathfrak{A}$ by interpreting c by a_c. Then $\mathrm{Th}(\mathfrak{A}^+)$ is a complete theory which admits Henkin witnesses in C. In fact, any complete theory which admits Henkin witnesses in C is of this form:

Proposition 2.6.12. *Any complete $\mathcal{L} \cup C$-theory T^+ which admits Henkin witnesses in C has a model $\mathfrak{A}^+$ consisting of constants of C, that is, with a base set of the form $A^+ = \{c^{\mathfrak{A}^+} \mid c \in C\}$.*

Proof of Proposition 2.6.12. We observe that replacing T^+ by the set of $\mathcal{L} \cup C$-sentences φ such that $T^+ \vdash_{\mathcal{L}\cup C} \varphi$ does not change the assumptions. We may thus assume that T^+ is *deductively closed*, that is, $T^+ \vdash_{\mathcal{L}\cup C} \varphi$ if and only if $\varphi \in T^+$.

Note that it follows from the equality axioms that the binary relation $c \sim d :\iff c = d \in T^+$ on C is an equivalence relation. We set $a_c := c/\!\sim$ and $A^+ := \{a_c \mid c \in C\}$. Then $A^+ \neq \emptyset$, as clearly $C \neq \emptyset$. Let us define an $\mathcal{L} \cup C$-structure $\mathfrak{A}^+$ on A^+ as follows:

- For d a constant symbol, we set $d^{\mathfrak{A}^+} := a_c$ if $c = d \in T^+$, where $c \in C$. Note that such a c always exists. Indeed, $d = d \to \exists x\, x = d \in T^+$ by (Q2), thus $\exists x\, x = d \in T^+$ by (MP); since T^+ admits Henkin witnesses in C, there exists $c \in C$ such that $\exists x\, x = d \to c = d \in T^+$, whence $c = d \in T^+$ by (MP). Furthermore by the equality axioms $d^{\mathfrak{A}^+}$ does not depend on the choice of c.
- For $R \in \mathcal{R}_n^{\mathcal{L}}$ we set

  $$(a_{c_1}, \dots, a_{c_n}) \in R^{\mathfrak{A}^+} : \iff Rc_1 \cdots c_n \in T^+.$$

  This is well defined by the equality axioms (E5).
- For $f \in \mathcal{F}_n^{\mathcal{L}}$ we set

  $$f^{\mathfrak{A}^+}(a_{c_1}, \dots, a_{c_n}) = a_{c_0} : \iff fc_1 \cdots c_n = c_0 \in T^+.$$

  This is well defined by the equality axioms (E4). By an argument similar to the one given for constants one proves that $f^{\mathfrak{A}^+}$ is defined everywhere as a function.

The following statements then hold:

(I) If t is an $\mathcal{L} \cup C$-term without variables and $c \in C$, then

$$t^{\mathfrak{A}^+} = a_c \iff t = c \in T^+.$$

(II) Let ψ be an $\mathcal{L} \cup C$-sentence. Then $\mathfrak{A}^+ \vDash \psi \iff \psi \in T^+$.

One proves (I) by induction on $\mathrm{ht}(t)$, using the equality axioms.

To prove (II), first recall that $\mathrm{ht}(\psi) = \mathrm{ht}(\psi_{\overline{s}/\overline{x}})$ (cf. Exercise 2.4.1). One argues by induction on $\mathrm{ht}(\psi)$.

If ψ is of the form $t_1 = t_2$, then (II) follows from (I). If ψ is of the form $Rt_1 \cdots t_n$, one chooses $c_i \in C$ such that $t_i^{\mathfrak{A}^+} = a_{c_i}$. Since $t_i = c_i \in T^+$, one has $\mathfrak{A}^+ \vDash \psi \iff Rc_1 \cdots c_n \in T^+ \iff \psi \in T^+$. The first equivalence follows from the definition of $\mathfrak{A}^+$, the second from (E5).

If ψ is equal to $(\varphi_1 \wedge \varphi_2)$ it is clear that (II) for ψ follows from (II) for both φ_1 and φ_2. If ψ is equal to $\neg\varphi$, one has

$$\mathfrak{A}^+ \vDash \psi \iff \mathfrak{A}^+ \nvDash \varphi \iff \varphi \notin T^+ \iff \psi \in T^+,$$

since T^+ is complete and deductively closed by hypothesis.

Finally, suppose that ψ is equal to $\exists x\varphi$. Let us note that $\psi \in T^+$ if and only if there exists $c \in C$ such that $\varphi_{c/x} \in T^+$. Indeed, since T^+ admits Henkin witnesses in C, the 'only if' part holds. For the 'if' part, it is enough to use (Q2), (MP) and the fact that T^+ is deductively closed. One may now conclude as follows:

$$\begin{aligned} \mathfrak{A}^+ \vDash \psi &\iff \mathfrak{A}^+ \vDash \varphi[a_c] \text{ for some } c \in C \\ \text{(Substitution Lemma)} &\iff \mathfrak{A}^+ \vDash \varphi_{c/x} \text{ for some } c \in C \\ \text{(Induction Hypothesis)} &\iff \varphi_{c/x} \in T^+ \text{ for some } c \in C \\ &\iff \psi \in T^+. \end{aligned}$$

Thus $\mathfrak{A}^+$ is a model of T^+ consisting of constants in C. □

The following lemma will be enough to conclude the proof of Theorem 2.6.11, because if $\mathfrak{A}^+$ is a model of the $\mathcal{L}^+ = \mathcal{L} \cup C$-theory T^+ with $T^+ \supseteq T$, then the reduct of $\mathfrak{A}^+$ to the language $\mathcal{L}$ is a model of T. □

Lemma 2.6.13. *For any consistent $\mathcal{L}$-theory T there exists a set of constant symbols C disjoint from $\mathcal{L}$ such that if $\mathcal{L}^+$ denotes the language $\mathcal{L} \cup C$, then there exists a complete $\mathcal{L}^+$-theory T^+ containing T that admits Henkin witnesses in C.*

Proof. To any $\mathcal{L}$-formula with a free variable $\varphi(x)$ one assigns a new constant symbol c_φ. Let C_1 be the set of all c_φ. One sets $\mathcal{L}_1 = \mathcal{L} \cup C_1$ and

$$T_1 := \widetilde{T} := T \cup \{\exists x\varphi \to \varphi_{c_\varphi/x} \mid \varphi(x) \in \mathrm{Fml}^{\mathcal{L}}\}.$$

Let us prove that the theory T_1 is consistent. Since a theory is consistent if and only if any finite subset is consistent, it suffices to prove that the theory $\widetilde{T}' = T \cup \{\exists x_i \varphi^i \to \varphi^i_{c_{\varphi^i}/x_i}\}$ is consistent for any finite set of formulas $\{\varphi^1, \dots, \varphi^n\}$. The theory T being consistent as an $\mathcal{L}_1$-theory by Lemma 2.6.8(b), this follows from Lemma 2.6.9, by induction on n.

We iterate that construction, with C_2 a set of new constant symbols, $\mathcal{L}_2 := \mathcal{L}_1 \cup C_2$ and the $\mathcal{L}_2$-theory $T_2 := \widetilde{T_1}$. By the argument just given, T_2 is consistent. By induction, T_n being constructed, it gives rise to a set of new constant symbols C_{n+1}. One sets $\mathcal{L}_{n+1} = \mathcal{L}_n \cup C_{n+1}$, and the $\mathcal{L}_{n+1}$-theory $T_{n+1} := \widetilde{T_n}$ is consistent. Set $C := \bigcup_{n\in\mathbb{N}} C_n$ and $\mathcal{L}^+ := \mathcal{L} \cup C$. Thus $(T_n)_{n\in\mathbb{N}}$ is an increasing sequence of consistent $\mathcal{L}^+$-theories.

The $\mathcal{L}^+$-theory $T' := \bigcup_{n\in\mathbb{N}} T_n$ is then consistent by Corollary 2.6.5. By construction, it admits Henkin witnesses in C.

Since any $\mathcal{L}^+$-theory S' containing T' still admits Henkin witnesses in C, it suffices to prove that any consistent $\mathcal{L}^+$-theory is contained in some complete $\mathcal{L}^+$-theory. This follows from Zorn's Lemma. Indeed, the set

$$\mathcal{S} = \{S' \supseteq T' \mid S' \text{ is a consistent } \mathcal{L}^+\text{-theory}\}$$

is non-empty and partially ordered under inclusion. As the union of a chain of consistent theories is still consistent by Corollary 2.6.5, this ordering is inductive. Hence, by Zorn's Lemma, there exists a maximal element in $\mathcal{S}$, that is, there exists an $\mathcal{L}^+$-theory $T^+ \supseteq T'$ which is maximal consistent. Let φ be some $\mathcal{L}^+$-sentence. If $T^+ \nvdash_{\mathcal{L}^+} \varphi$, the $\mathcal{L}^+$-theory $T^+ \cup \{\neg\varphi\}$ is consistent by Corollary 2.6.7. One deduces that $\neg\varphi \in T^+$ by maximality, hence T^+ is complete, which finishes the proof.

When $\mathcal{L}$ is countable, one can provide a more direct construction for the theory in the lemma that we shall now sketch. One fixes a set $C = \{c_n \mid n \in \mathbb{N}\}$ of new constant symbols and one enumerates the set of $\mathcal{L} \cup C$-sentences via $\varphi_0, \varphi_1, \varphi_2, \ldots$. By induction, one constructs an increasing sequence $(T_n)_{n\in\mathbb{N}}$ of consistent $\mathcal{L} \cup C$-theories with the following properties:

- $T_0 = T$, and $T_n \setminus T$ is finite for any $n \in \mathbb{N}$;
- $\varphi_n \in T_{n+1}$ or $\neg\varphi_n \in T_{n+1}$;
- if φ_n is of the form $\exists x\psi \in T_{n+1}$, then there exists $c \in C$ such that $\psi_{c/x} \in T_{n+1}$.

Once such a sequence $(T_n)_{n\in\mathbb{N}}$ is constructed, it is enough to set $T^+ := \bigcup_{n\in\mathbb{N}} T_n$. Then T^+ is a complete theory by construction, and it admits Henkin witnesses in C. To prove the latter, consider some $\mathcal{L}\cup C$-formula $\psi(x)$. Then there exists some $n \in \mathbb{N}$ such that $\exists x\psi$ is equal to φ_n. If $\varphi_n \in T^+$, then by construction $\psi_{c/x} \in T^+$ for some $c \in C$, hence $\exists x\psi \to \psi_{c/x} \in T^+$. Otherwise, one has $\neg\exists x\psi \in T^+$, hence $\exists x\psi \to \psi_{c/x} \in T^+$ for any c.

Assume T_n is constructed. If $T_n \cup \{\varphi_n\}$ is consistent, one sets ψ_n equal to φ_n. Otherwise, ψ_n is set equal to $\neg\varphi_n$. In both cases, the theory $T_n \cup \{\psi_n\}$ is consistent. If ψ_n is not of the form $\exists x\chi$, one sets $T_{n+1} := T_n \cup \{\psi_n\}$.

Otherwise, let m be minimal such that c_m has no occurrence in T_n (such an m exists since $T_n \setminus T$ is finite). One sets $T_{n+1} := T_n \cup \{\psi_n, \chi_{c_m/x}\}$. The theory T_{n+1} is consistent by Lemma 2.6.9. □

2.7. Exercises

Exercise 2.7.1 (Compactness in propositional logic)**.** Let $\mathrm{Fml}_{\mathcal{P}}$ be the set of propositional formulas over an infinite set $\mathcal{P}$ of propositional variables. A set $\Sigma \subseteq \mathrm{Fml}_{\mathcal{P}}$ is called *satisfiable* if there is an assignment $\delta : \mathcal{P} \to \{0,1\}$ such that $\delta^*(F) = 1$ for all $F \in \Sigma$; it is called *finitely satisfiable* if every finite subset $\Sigma_0 \subseteq \Sigma$ is satisfiable.

The aim of this exercise is to prove the following result (Compactness Theorem in propositional logic): *A set $\Sigma \subseteq \mathrm{Fml}_{\mathcal{P}}$ of propositional formulas is satisfiable if and only if it is finitely satisfiable.*

(1) Prove the theorem in the special case when Σ is *complete*, that is, when for every $p \in \mathcal{P}$ one has $p \in \Sigma$ or $\neg p \in \Sigma$.

(2) Prove that every finitely satisfiable set of propositional formulas is contained in a finitely satisfiable set which is complete.

(3) Conclude.

Application 1. Let k be a natural number. A graph $\mathcal{G} = (G, E)$ is said to be *k-colorable* if there is a coloring of its set of vertices G with k colors such that any two vertices which are connected by an edge have different colors. Prove that a graph $\mathcal{G}$ is k-colorable if and only if every finite subgraph of $\mathcal{G}$ is k-colorable.

Application 2. For $n \in \mathbb{N}$ and a set A let $\mathcal{P}_n(A)$ be the set of n-element subsets of A.

(a) Prove Ramsey's Theorem (infinite version): *For any natural numbers n, k and any $f : \mathcal{P}_n(\mathbb{N}) \to \{0, 1, \dots, k-1\}$ there is an infinite subset A of $\mathbb{N}$ such that the restriction of f to $\mathcal{P}_n(A)$ is constant.*
[Hint: Argue by induction on $n \in \mathbb{N}$. Given some function $f : \mathcal{P}_{n+1}(\mathbb{N}) \to \{0, 1, \dots, k-1\}$ and some natural number a, consider the induced map f_a on $\mathcal{P}_n(\mathbb{N} \setminus \{a\})$ defined by $f_a(S) = f(S \cup \{a\})$. Inductively construct an increasing sequence $0 = a_0 < a_1 < a_2 < \cdots$ in $\mathbb{N}$ and a sequence of infinite sets $\mathbb{N} = X_0 \supsetneq X_1 \supsetneq$

$X_2 \supsetneq \cdots$ such that for every i one has $a_i \in X_i$, $X_{i+1} \cap [0, a_i] = \emptyset$ and f_{a_i} is constant on $\mathcal{P}_n(X_{i+1})$.]

(b) Deduce Ramsey's Theorem (finite version): *For any natural numbers m, n, k there is a natural number N such that for any function $f : \mathcal{P}_n(\{0, 1, \dots, N-1\}) \to \{0, 1, \dots, k-1\}$ there is an m-element subset $A \subseteq \{0, 1, \dots, N-1\}$ such that the restriction of f to $\mathcal{P}_n(A)$ is constant.*

Exercise 2.7.2 (Resolution in propositional logic)**.** We keep the context of the previous exercise. Let $F, G \in \mathrm{Fml}_{\mathcal{P}}$. We say that F and G are *logically equivalent* if $(F \leftrightarrow G)$ is a tautology. A *literal* is a formula of the form p or $\neg p$ for some $p \in \mathcal{P}$; a *clause* is a disjunction of literals. By convention, the empty clause, denoted by $\square$, is a formula which is always false.

Observe that any formula F is logically equivalent to a conjunction of clauses.

- If a literal L occurs more than once in a clause C, a clause D obtained by deleting one occurrence of L in C is called a *simplification* of C.
- Given clauses $C = C_1 \vee p \vee C_2$ and $D = D_1 \vee \neg p \vee D_2$, where $p \in \mathcal{P}$, we say that $E = C_1 \vee C_2 \vee D_1 \vee D_2$ is obtained from C and D by the *cut rule*.
- A *resolution sequence* from a set of clauses $\mathcal{C}$ is a finite sequence of clauses $(C_0, \dots, C_n)$ such that for any $i \leq n$ either $C_i \in \mathcal{C}$, or C_i is a simplification of C_j for some $j < i$, or there exist $j, k < i$ such that C_i is obtained from C_j and C_k by the cut rule.

  We say $\mathcal{C}$ is *refutable* if there is a resolution sequence from $\mathcal{C}$ ending in $\square$.

The aim of this exercise is to prove that a set of clauses is satisfiable if and only if it may not be refuted.

(1) Prove that the resolution method is sound: if a set of clauses may be refuted, then it is unsatisfiable.

(2) Observe that a clause C is a tautology if and only if there is a propositional variable p such that C contains the literals p and $\neg p$.

(3) Let $\mathcal{C}$ be a set of clauses and $p \in \mathcal{P}$. If C is a clause, let $C_{p=0}$ be the clause obtained from C by deleting all literals which are equal to p. Consider

$$\mathcal{C}_{p=0} = \{C_{p=0} \mid C \text{ does not contain the literal } \neg p\}.$$

Similarly define $C_{p=1}$ and $\mathcal{C}_{p=1}$, interchanging the roles of $\neg p$ and p.

(a) Prove that $\mathcal{C}$ is satisfiable if and only if $\mathcal{C}_{p=0}$ or $\mathcal{C}_{p=1}$ is satisfiable.

(b) Prove that $\mathcal{C}_{p=0}$ is refutable if and only if there is a resolution sequence from $\mathcal{C}$ ending in $\square$ or in p.

(c) Prove that $\mathcal{C}$ is refutable if and only if both $\mathcal{C}_{p=0}$ and $\mathcal{C}_{p=1}$ are refutable.

(4) Prove that the resolution method is complete: if a set of clauses is not satisfiable, it may be refuted.

[Hint: Prove the result for finite sets of clauses by induction on the number of variables, and then use compactness (cf. Exercise 2.7.1) to deduce the general case from this.]

Exercise 2.7.3 (Interpolation). Let φ be an $\mathcal{L}_1$-sentence and let ψ be an $\mathcal{L}_2$-sentence such that $\models \varphi \to \psi$. Set $\mathcal{L}_0 := \mathcal{L}_1 \cap \mathcal{L}_2$. The aim of this exercise is to prove Craig's Interpolation Theorem: *There exists an $\mathcal{L}_0$-sentence θ such that $\models \varphi \to \theta$ and $\models \theta \to \psi$.*

We may assume that $\mathcal{L}_1$ and $\mathcal{L}_2$ are countable. Assume for contradiction that no such θ exists. Let C be a countably infinite set of new constant symbols and set $\mathcal{L}_i^+ = \mathcal{L}_i \cup C$, for $i \in \{0, 1, 2\}$. For an $\mathcal{L}_1^+$-theory T and an $\mathcal{L}_2^+$-theory U we say that the pair (T, U) is *inseparable* if there is no $\mathcal{L}_0^+$-sentence θ such that $T \models \theta$ and $U \models \neg\theta$.

(1) Prove that the pair $(\{\varphi\}, \{\neg\psi\})$ is inseparable.

(2) Prove that if (T, U) is inseparable and χ is an $\mathcal{L}_1^+$-sentence, then either $(T \cup \{\chi\}, U)$ or $(T \cup \{\neg\chi\}, U)$ is inseparable.

(3) Construct an increasing chain of finite $\mathcal{L}_1^+$-theories $(T_n)_{n\in\mathbb{N}}$ with $T_0 = \{\varphi\}$ and an increasing chain of finite $\mathcal{L}_2^+$-theories $(U_n)_{n\in\mathbb{N}}$ with $U_0 = \{\neg\psi\}$ such that, letting $T_\omega = \bigcup_{n\in\mathbb{N}} T_n$ and $U_\omega = \bigcup_{n\in\mathbb{N}} U_n$, the following conditions hold:

(i) T_ω is a complete deductively closed $\mathcal{L}_1^+$-theory which admits Henkin witnesses in C,
(ii) U_ω is a complete deductively closed $\mathcal{L}_2^+$-theory which admits Henkin witnesses in C, and
(iii) the pair (T_ω, U_ω) is inseparable.

Moreover, deduce from (i)-(iii) that $T_\omega \cap U_\omega$ is a complete $\mathcal{L}_0^+$-theory which admits Henkin witnesses in C.

(4) Prove that $T_\omega \cup U_\omega$ has a model, and conclude Craig's Interpolation Theorem.

(5) Deduce Robinson's Consistency Theorem: *If T_i are consistent $\mathcal{L}_i$-theories for $i = 1, 2$ such that $T_0 = T_1 \cap T_2$ is a complete $\mathcal{L}_0$-theory, then $T_1 \cup T_2$ is consistent.*

Exercise 2.7.4 (Beth Definability)**.** Let $\mathcal{L}$ be a first-order language and $R \notin \mathcal{L}$ an n-ary relation symbol. Let T be an $\mathcal{L} \cup \{R\}$-theory.

- We say T *implicitly defines* R if for any $\mathcal{L}$-structure $\mathfrak{M}$ with base set M and any n-ary relations $R_1, R_2 \subseteq M^n$ such that $\langle \mathfrak{M}, R_1 \rangle$ and $\langle \mathfrak{M}, R_2 \rangle$ are both models of T, one has $R_1 = R_2$.
- We say that T *explicitly defines* R if there is an $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$ such that $T \models \forall \overline{x}(R(\overline{x}) \leftrightarrow \varphi(\overline{x}))$.

The aim of this exercise is to prove Beth's Definability Theorem: *The theory T implicitly defines the relation R if and only if it explicitly defines R.*

(1) Prove that if T explicitly defines R, then it implicitly defines R.

(2) Assume that T implicitly defines R. Let R' be a new n-ary relation symbol and $c_1, \dots, c_n$ new pairwise distinct constant symbols.
   (a) Let T' be the theory obtained from T by replacing every occurrence of R by R'. Observe that
   $$T \cup T' \models R(c_1, \dots, c_n) \to R'(c_1, \dots, c_n).$$
   (b) Prove that there is a finite conjunction φ of sentences in T such that
   $$\varphi \wedge R(c_1, \dots, c_n) \models \varphi' \to R'(c_1, \dots, c_n),$$

where φ' is the formula obtained from φ by replacing every occurrence of R by R'.

(c) Prove that T explicitly defines R.

[Hint: Use Craig's Interpolation Theorem (see Exercise 2.7.3).]

Exercise 2.7.5. If w is a word over the alphabet Σ, a *subword* of w is a word u such that $w = w_1 u w_2$ for certain words w_1, w_2.

By induction on the height of a formula φ, one defines the set $\mathrm{Sub}(\varphi)$ of all *subformulas* of φ as a subset of the set of its subwords. If φ is atomic, then $\mathrm{Sub}(\varphi) := \{\varphi\}$; if φ equals $\neg\psi$ or $\exists v_i \psi$, then $\mathrm{Sub}(\varphi) := \mathrm{Sub}(\psi) \cup \{\varphi\}$; finally, if φ equals $(\psi_1 \wedge \psi_2)$, then $\mathrm{Sub}(\varphi) := \mathrm{Sub}(\psi_1) \cup \mathrm{Sub}(\psi_2) \cup \{\varphi\}$.

Now let T be an $\mathcal{L}$-theory. Two $\mathcal{L}$-formulas $\varphi_1(\overline{x})$ and $\varphi_2(\overline{x})$ are said to be *equivalent in* T if $T \vDash \forall x_1, \dots, x_n(\varphi_1 \leftrightarrow \varphi_2)$. They are called *logically equivalent* if they are equivalent in the empty theory.

Assume that $\varphi(\overline{x})$ is an $\mathcal{L}$-formula and that $\psi(y_1, \dots, y_m)$ is a subformula of φ. Let ψ' be equivalent in T to ψ, and assume that $\mathrm{Free}(\psi) = \mathrm{Free}(\psi') = \{y_1, \dots, y_m\}$. Let $\varphi'(\overline{x})$ be the formula one obtains when one replaces the subformula ψ in φ by ψ'. Show that $\varphi(\overline{x})$ and $\varphi'(\overline{x})$ are then equivalent in T.

Exercise 2.7.6 (Herbrand normal form)**.** Let $\mathcal{L}$ be a language. A formula φ is said to be in *prenex normal form* if it is of the form

$$Q_1 x_1 \dots Q_m x_m \varphi_0,$$

where $Q_i \in \{\exists, \forall\}$ for $1 \leq i \leq m$ and φ_0 is a quantifier-free formula. It is called *existential* if it is in prenex normal form and does not contain any universal quantifier.

(1) Prove that for every $\mathcal{L}$-formula $\varphi(\overline{x})$ there is an $\mathcal{L}$-formula $\psi(\overline{x})$ in prenex normal form which is logically equivalent to $\varphi(\overline{x})$, that is, such that $\vDash \forall \overline{x}(\varphi \leftrightarrow \psi)$.

The language $\mathcal{L}^{\mathcal{H}}$ is obtained from $\mathcal{L}$ by adding, for every $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$ with n free variables, a function symbol f_φ of arity n. If $\varphi(x_1, \dots, x_n)$ is an $\mathcal{L}$-formula in prenex normal form, one defines its Herbrand form $\varphi^{\mathcal{H}}(x_1, \dots, x_n)$ by induction on the length of φ:

- if $\varphi(x_1, \dots, x_n)$ is quantifier-free, one sets $\varphi^{\mathcal{H}}(x_1, \dots, x_n)$ equal to $\varphi(x_1, \dots, x_n)$;
- if $\varphi(x_1, \dots, x_n)$ is of the form $\exists y \psi(y, x_1, \dots, x_n)$, one sets $\varphi^{\mathcal{H}}(x_1, \dots, x_n)$ equal to $\exists y \psi^{\mathcal{H}}(y, x_1, \dots, x_n)$;
- if $\varphi(x_1, \dots, x_n)$ is of the form $\forall y \psi(y, x_1, \dots, x_n)$, one sets $\varphi^{\mathcal{H}}(x_1, \dots, x_n)$ equal to $\psi^{\mathcal{H}}\big(f_\varphi(x_1, \dots, x_n), x_1, \dots, x_n\big)$.

(2) Let φ be in prenex normal form. Prove that $\varphi \vdash \varphi^{\mathcal{H}}$.

(3) Prove that for every $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$ in prenex normal form and for every $\mathcal{L}$-structure $\mathfrak{M}$, there is an $\mathcal{L}^{\mathcal{H}}$-expansion $\mathfrak{M}^{\mathcal{H}}$ of $\mathfrak{M}$ such that for every $(a_1, \dots, a_n) \in M^n$, if $\mathfrak{M} \not\models \varphi[a_1, \dots, a_n]$ then $\mathfrak{M}^{\mathcal{H}} \not\models \varphi^{\mathcal{H}}[a_1, \dots, a_n]$.

(4) Let φ be an $\mathcal{L}$-sentence in prenex normal form. Prove that $\vdash \varphi^{\mathcal{H}}$ if and only if $\vdash \varphi$. In other words, there is an explicit recipe to construct an existential sentence in an expansion of the language which is universally valid if and only if the original sentence is universally valid.

Exercise 2.7.7. Let $\mathcal{L}$ be a first-order language containing at least one constant symbol, and let φ be an existential $\mathcal{L}$-sentence, given by $\exists x_1, \dots, x_n \psi$, with $\psi(x_1, \dots, x_n)$ a quantifier-free formula. Prove that $\vdash \varphi$ if and only if there are $m > 0$ and $\mathcal{L}$-terms $(t_i^j)_{1 \le i \le n, 1 \le j \le m}$ not containing any variable such that

$$\vdash \bigvee_{1 \le j \le m} \psi(t_1^j, \dots, t_n^j).$$

Exercise 2.7.8 (Omitting Types Theorem)**.** Let T be an $\mathcal{L}$-theory and $\pi = \pi(v_1, \dots, v_n)$ a set of $\mathcal{L}$-formulas such that the free variables of the formulas in π belong to $\{v_1, \dots, v_n\}$. One says π is a *partial n-type* (*in* T) if for any finite subset $\{\varphi_1, \dots, \varphi_k\}$ of π, the theory $T \cup \{\exists \overline{v} \bigwedge_{i=1}^{k} \varphi_i\}$ is consistent.

- One says a model $\mathfrak{M}$ of T *realizes* π if there exists $\overline{a} \in M^n$ such that $\mathfrak{M} \models \varphi[\overline{a}]$ for any $\varphi \in \pi$; otherwise, one says that $\mathfrak{M}$ *omits* π.

- π is called *isolated* if there exists a formula $\varphi(v_1, \dots, v_n)$ with $T \cup \{\exists \overline{v} \varphi\}$ consistent such that $T \vdash \forall \overline{v}(\varphi \to \psi)$ for any formula $\psi \in \pi$.

The aim of this exercise is to prove the following result, which is called the Omitting Types Theorem: *Let $\mathcal{L}$ be countable and T a consistent $\mathcal{L}$-theory. One assumes that, for $j \in \mathbb{N}$, $\pi_j = \pi(v_1, \dots, v_{n_j})$ is a non-isolated partial type. Then there exists a countable model of T that omits all the π_j.*

We consider T and $(\pi_j)_{j \in \mathbb{N}}$ as in the statement of the theorem. Let $C = \{c_i \mid i \in \mathbb{N}\}$ be a set of new pairwise distinct constant symbols and set $\mathcal{L}^* = \mathcal{L} \cup C$.

(1) Let $\psi(v_0)$ be an $\mathcal{L}^*$-formula, and let $T' \supseteq T$ be a consistent $\mathcal{L}^*$-theory such that $T' \setminus T$ is finite. Prove that there exists $c \in C$ such that $T'' = T' \cup \{\exists v_0 \psi \to \psi(c)\}$ is consistent.

(2) Let $\overline{c} = (c_{i_1}, \dots, c_{i_{n_j}})$ be some n_j-tuple of distinct elements of C, and let $T' \supseteq T$ be a consistent $\mathcal{L}^*$-theory with $T' \setminus T$ finite. Prove that there exists $\varphi(v_1, \dots, v_{n_j}) \in \pi_j$ such that $T'' = T' \cup \{\neg\varphi(\overline{c})\}$ is consistent.

[Hint: Use that, up to logical equivalence, T' is given by $T \cup \{\chi(\overline{c}, \overline{d})\}$, where $\chi(v_1, \dots, v_{n_j}, \overline{y})$ is some $\mathcal{L}$-formula and $\overline{d}$ a tuple of constant symbols in C disjoint from $\overline{c}$.]

(3) Prove that there exists a consistent $\mathcal{L}^*$-theory $T^* \supseteq T$ satisfying the following properties:
   (H) For every $\mathcal{L}^*$-formula $\psi(v_0)$ there exists some $c \in C$ not appearing in ψ such that $\exists v_0 \psi \to \psi(c) \in T^*$.
   (O) For any $j \in \mathbb{N}$ and any n_j-tuple $(c_{i_1}, \dots, c_{i_{n_j}})$ of distinct elements of C there exists a formula $\varphi(\overline{v}) \in \pi_j$ such that $\neg\varphi(c_{i_1}, \dots, c_{i_{n_j}}) \in T^*$.

   [Hint: Using suitable enumerations, construct T^* as the union of an increasing chain $(T_n)_{n \in \mathbb{N}}$ with $T_0 = T$ and $T_n \setminus T$ finite for every n.]

(4) Let T^* be a consistent $\mathcal{L}^*$-theory satisfying (H). Prove that for any $i \in \mathbb{N}$, the set $X_i = \{j \in \mathbb{N} \mid T^* \vdash c_i = c_j\}$ is infinite.

(5) Conclude the Omitting Types Theorem.

10.1090/stml/089/03

Chapter 3

First Steps in Model Theory

Introduction

First-order model theory deals with the relationship between theories in a first-order language and their models. It provides a way to treat problems from other areas of mathematics (like algebra or combinatorics) with tools from mathematical logic. First-order logic has a rather limited expressive power: we will see for instance that an infinite structure is never determined, up to isomorphism, by its first-order theory (Corollary 3.2.4). In fact this apparent weakness is a strength and a reason for its efficiency. As we will see it is sometimes quite useful to be able to switch from one model of a theory to another.

One of the main themes of this chapter is quantifier elimination, which in concrete examples often yields a particularly simple description of all definable sets in models of the theory under consideration. In Theorem 3.4.4 we provide a very useful semantical criterion for a formula to be equivalent to a quantifier-free formula in a given theory (a syntactic condition). This applies in particular to the theory of algebraically closed fields which is studied in 3.5, and other examples are considered in exercises. As a remarkable consequence of this study, we provide a statement and a proof of the Lefschetz principle from algebraic

geometry (Theorem 3.5.5) which allows us to transfer results from algebraically closed fields of characteristic zero to algebraically closed fields of sufficiently large characteristic. A beautiful application is provided by Ax's Theorem (Theorem 3.6.3) stating that injective complex polynomial mappings are always surjective, which is proved by reduction to finite fields.

3.1. Some Fundamental Theorems

Theorem 3.1.1 (Compactness Theorem)**.** *Let T be a theory such that any finite subset of T has a model. Then T has a model.*

Proof. The theory T is consistent if and only if any finite subset of T is consistent. Thus the statement follows from Theorem 2.6.11. □

Remark. Our proof of the Compactness Theorem uses Gödel's Completeness Theorem. For a more direct semantical proof, see Exercise 3.7.5.

Exercise. Fix a language $\mathcal{L}$ and denote by X the set of $\mathcal{L}$-theories T which are complete and closed under deduction. One may define a topology on X in the following way. For φ an $\mathcal{L}$-sentence, one sets $\langle\varphi\rangle := \{T \in X \mid \varphi \in T\}$, and one considers the topology generated by the family of all $\langle\varphi\rangle$. Prove:

(1) $\langle\varphi \wedge \psi\rangle = \langle\varphi\rangle \cap \langle\psi\rangle$ and $\langle\neg\varphi\rangle = X \setminus \langle\varphi\rangle$. In particular the sets $\langle\varphi\rangle$ form a basis of clopen subsets.

(2) The space X is compact and Hausdorff.

Definition. Let $\mathfrak{M}$ and $\mathfrak{N}$ be $\mathcal{L}$-structures.

(1) We say that $\mathfrak{M}$ and $\mathfrak{N}$ are *elementarily equivalent* if they satisfy the same $\mathcal{L}$-sentences, that is, if $\mathrm{Th}(\mathfrak{M}) = \mathrm{Th}(\mathfrak{N})$. This is denoted by $\mathfrak{M} \equiv \mathfrak{N}$.

(2) Assume that $\mathfrak{M} \subseteq \mathfrak{N}$. We say that $\mathfrak{M}$ is an *elementary substructure* of $\mathfrak{N}$ (and $\mathfrak{N}$ is called an *elementary extension* of $\mathfrak{M}$) if for every $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$ and every tuple $\overline{a} = (a_1, \dots, a_n) \in M^n$ we have $\mathfrak{M} \models \varphi[\overline{a}]$ if and only if $\mathfrak{N} \models \varphi[\overline{a}]$. This is denoted by $\mathfrak{M} \preccurlyeq \mathfrak{N}$.

Remark.

(1) If $\mathfrak{M} \preccurlyeq \mathfrak{N}$, then $\mathfrak{M} \equiv \mathfrak{N}$.

(2) If $\mathfrak{M} \cong \mathfrak{N}$, then $\mathfrak{M} \equiv \mathfrak{N}$. □

The following example shows that if $\mathfrak{M} \subseteq \mathfrak{N}$ and $\mathfrak{M} \equiv \mathfrak{N}$ it is not always the case that $\mathfrak{M} \preccurlyeq \mathfrak{N}$.

Example. One considers the two $\mathcal{L}_{ord}$-structures $\mathfrak{N} := \langle \mathbb{N}; < \rangle$ and $\mathfrak{M} := \langle \mathbb{N}^*; < \rangle$. One has $\mathfrak{M} \subseteq \mathfrak{N}$ and $\mathfrak{M} \cong \mathfrak{N}$, in particular $\mathfrak{M} \equiv \mathfrak{N}$. On the other hand the extension $\mathfrak{M} \subseteq \mathfrak{N}$ is not elementary, since $\mathfrak{M} \models \neg \exists x\, x < 1$ and $\mathfrak{N} \models \exists x\, x < 1$.

Theorem 3.1.2 (Tarski-Vaught Test)**.** *Let $\mathfrak{M}$ and $\mathfrak{N}$ be $\mathcal{L}$-structures with $\mathfrak{M} \subseteq \mathfrak{N}$. Assume that for any $\mathcal{L}$-formula $\varphi(x_0, \dots, x_n)$ and any tuple $\overline{a} = (a_1, \dots, a_n) \in M^n$, if there exists $b_0 \in N$ such that $\mathfrak{N} \models \varphi[b_0, \overline{a}]$, then there exists $a_0 \in M$ such that $\mathfrak{N} \models \varphi[a_0, \overline{a}]$. Then $\mathfrak{M} \preccurlyeq \mathfrak{N}$.*

Proof. By induction on $\mathrm{ht}(\varphi(x_1, \dots, x_n))$ one proves that for any $\overline{a} \in M^n$ one has $\mathfrak{M} \models \varphi[\overline{a}] \iff \mathfrak{N} \models \varphi[\overline{a}]$.

When φ is atomic, this is clear since $\mathfrak{M}$ is a substructure of $\mathfrak{N}$. The case of logical connectives is also clear.

Assume now that $\varphi(x_1, \dots, x_n)$ is equal to $\exists x_0 \psi(x_0, \dots, x_n)$. (As x_0 is not free in φ, we may assume that $x_0 \neq x_i$ for $i = 1, \dots, n$.) Let $\overline{a} = (a_1, \dots, a_n) \in M^n$. Then

$$\begin{aligned} \mathfrak{M} \models \varphi[\overline{a}] &\iff \text{there exists } a_0 \in M \text{ such that } \mathfrak{M} \models \psi[a_0, \overline{a}] \\ &\iff \text{there exists } a_0 \in M \text{ such that } \mathfrak{N} \models \psi[a_0, \overline{a}] \\ &\iff \text{there exists } b_0 \in N \text{ such that } \mathfrak{N} \models \psi[b_0, \overline{a}] \\ &\iff \mathfrak{N} \models \varphi[\overline{a}], \end{aligned}$$

where the second equivalence follows from the induction hypothesis and the third one from the hypothesis of the theorem. □

Notation. For a language $\mathcal{L}$ we set $\mathrm{card}(\mathcal{L}) = \mathrm{card}(\mathrm{Fml}^{\mathcal{L}})$.

Note that $\mathrm{card}(\mathcal{L}) \geq \mathrm{card}(\mathcal{T}^{\mathcal{L}})$.

Theorem 3.1.3 (Downward Löwenheim-Skolem Theorem)**.** *Let $\mathfrak{M}$ be an $\mathcal{L}$-structure and $A \subseteq M$. Assume that* $\mathrm{card}(M) \geq \mathrm{card}(\mathcal{L})$*. Then there exists an elementary substructure $\mathfrak{M}_0$ of $\mathfrak{M}$ containing A which is of cardinality* $\sup(\mathrm{card}(A), \mathrm{card}(\mathcal{L}))$.

Proof. Up to enlarging the subset A if necessary, we may assume that $\mathrm{card}(A) \geq \mathrm{card}(\mathcal{L})$.

In this proof, when $\emptyset \neq B \subseteq M$, we denote by $\widetilde{B} \subseteq M$ the base set of $\langle B \rangle_{\mathfrak{M}}$, the substructure generated by B. By Exercise 2.3.3 we have

$$\widetilde{B} = \{t^{\mathfrak{M}}[b_1, \dots, b_n] \mid t = t(x_1, \dots, x_n) \in \mathcal{T}^{\mathcal{L}},\ b_1, \dots, b_n \in B\}.$$

In particular, if $\mathrm{card}(B) \geq \mathrm{card}(\mathcal{L})$, then $\mathrm{card}(B) = \mathrm{card}(\widetilde{B})$, since there exists a surjection from $\mathcal{T}^{\mathcal{L}} \times \bigcup_{n\in\mathbb{N}} B^n$ onto $\widetilde{B}$.

Let $\mathfrak{A}_0 := \langle A \rangle_{\mathfrak{M}}$ and $A_0 := \widetilde{A}$. Assuming $A_i \subseteq M$ is already defined, one constructs A_{i+1} as follows. For any $\mathcal{L}$-formula $\varphi(x_0, \dots, x_n)$ and any n-tuple $\overline{a} \in A_i^n$, if $\mathfrak{M} \vDash \varphi[b_0, \overline{a}]$ for some $b_0 \in M$, one chooses $c(\varphi, \overline{a}) \in M$ such that $\mathfrak{M} \vDash \varphi[c(\varphi, \overline{a}), \overline{a}]$. One sets

$$B_{i+1} := A_i \cup \{c(\varphi, \overline{a}) \mid \varphi(x_0, \dots, x_n) \in \mathrm{Fml}^{\mathcal{L}}, a_1, \dots, a_n \in A_i\}$$

and $A_{i+1} := \widetilde{B_{i+1}}$, the base set of $\mathfrak{A}_{i+1} = \langle B_{i+1} \rangle_{\mathfrak{M}}$.

Let $M_0 := \bigcup_{i\in\mathbb{N}} A_i$. Then M_0 (is non-empty and) contains $c^{\mathfrak{M}}$ for any $c \in \mathcal{C}^{\mathcal{L}}$ and is closed under $f^{\mathfrak{M}}$ for any $f \in \mathcal{F}^{\mathcal{L}}$. It is thus the base set of a substructure $\mathfrak{M}_0$ of $\mathfrak{M}$.

Let $\varphi(x_0, \dots, x_n)$ be a formula, $\overline{a} \in M_0^n$ and $b_0 \in M$ such that $\mathfrak{M} \vDash \varphi[b_0, \overline{a}]$. There exists $N \in \mathbb{N}$ such that $a_1, \dots, a_n \in A_N$. By the construction of A_{N+1} there exists $c_0 \in A_{N+1} \subseteq M_0$ such that $\mathfrak{M} \vDash \varphi[c_0, \overline{a}]$. Hence $\mathfrak{M}_0 \preccurlyeq \mathfrak{M}$ by the Tarski-Vaught Test. It is clear that $\mathrm{card}(M_0) = \mathrm{card}(A)$. □

Example 3.1.4. Let $\mathfrak{R} = \langle \mathbb{R}; 0, 1, +, -, \cdot, < \rangle$ be the ordered field of real numbers.

(1) There exists $\mathfrak{R}' \equiv \mathfrak{R}$ with $\mathfrak{R}'$ non-archimedean, that is, containing an element $\varepsilon > 0$ such that $n \cdot \varepsilon = \underbrace{\varepsilon + \dots + \varepsilon}_{n \text{ times}} < 1$ for any $n \in \mathbb{N}$. Such an ε is called *infinitesimal*.

(2) There exists $\mathfrak{R}' \preccurlyeq \mathfrak{R}$ such that $\mathfrak{R}'$ is not complete.

Proof. (1) Let c be a new constant symbol and $\mathcal{L} := \mathcal{L}_{o.ring} \cup \{c\}$. Let φ_n be the formula $\underbrace{c + \dots + c}_{n \text{ times}} < 1$. One considers the $\mathcal{L}$-theory

$$T := \mathrm{Th}(\mathfrak{R}) \cup \{0 < c\} \cup \{\varphi_n \mid n \in \mathbb{N}\}.$$

For any finite $T_0 \subseteq T$ there exists $N \in \mathbb{N}$ such that $\varphi_m \notin T_0$ for any $m \geq N$. The expansion of $\mathfrak{R}$ to $\mathcal{L}$ obtained by interpreting c by $1/N \in \mathbb{R}$ is thus a model of T_0. By compactness, it follows that T has a model $\mathfrak{R}'$. The element $\varepsilon = c^{\mathfrak{R}'}$ is infinitesimal, hence $\mathfrak{R}'$ is non-archimedean.

(2) By the Downward Löwenheim-Skolem Theorem (for $A = \emptyset$), there exists $\mathfrak{R}' \preccurlyeq \mathfrak{R}$ with a countable base set $\mathbb{R}'$. Since $\mathfrak{R}'$ is a field, $\mathbb{Q} \subseteq \mathbb{R}'$. Take $r \in \mathbb{R} \setminus \mathbb{R}'$. Then the set $\{r' \in \mathbb{R}' \mid r' < r\}$ has no supremum in $\mathbb{R}'$, since $\mathbb{R}'$ is dense in $\mathbb{R}$. □

Remark. One may prove that $\langle \mathbb{R}_{alg}; +, -, 0, 1, \cdot, < \rangle \preccurlyeq \mathfrak{R}$, where $\mathbb{R}_{alg} = \{r \in \mathbb{R} \mid \text{there exists } 0 \neq p(X) \in \mathbb{Q}[X] \text{ such that } p(r) = 0\}$.

Remark. Suppose that $\mathfrak{M} \preccurlyeq \mathfrak{M}'$ and $D \subseteq M^n$ is a definable set (with parameters). Then D extends canonically to a definable set $D' \subseteq M'^n$ in $\mathfrak{M}'$, such that $D' \cap M^n = D$. Indeed, if $D = \varphi[\mathfrak{M}, \overline{b}]$ for some formula $\varphi(\overline{x}, \overline{y})$ and tuple $\overline{b}$ from $\mathfrak{M}$, then $D' = \varphi[\mathfrak{M}', \overline{b}]$ has the desired property, and it is independent of the choice of φ and $\overline{b}$.

Definition. Let $\mathcal{P}$ be a property that an $\mathcal{L}$-structure may or may not satisfy. We say that $\mathcal{P}$ is *axiomatizable* (resp. *finitely axiomatizable*) if there exists an $\mathcal{L}$-theory T (resp. an $\mathcal{L}$-sentence φ) such that for any $\mathcal{L}$-structure $\mathfrak{M}$, the property $\mathcal{P}$ is satisfied by $\mathfrak{M}$ if and only if $\mathfrak{M} \models T$ (resp. $\mathfrak{M} \models \varphi$). In this case one says that T (resp. φ) *axiomatizes* the property $\mathcal{P}$.

Proposition 3.1.5. *Let $\mathcal{P}$ be a property that an $\mathcal{L}$-structure may or may not satisfy. Then $\mathcal{P}$ is finitely axiomatizable if and only if $\mathcal{P}$ and its negation are both axiomatizable.*

Proof. If φ axiomatizes $\mathcal{P}$, then $\neg\varphi$ axiomatizes its negation. Conversely, assume that T axiomatizes $\mathcal{P}$ and that T' axiomatizes the negation of $\mathcal{P}$. The theory $T \cup T'$ being inconsistent, there exist $\varphi_1, \ldots, \varphi_n \in T$, $\varphi'_1, \ldots, \varphi'_m \in T'$ such that $\{\varphi_1, \ldots, \varphi_n, \varphi'_1, \ldots, \varphi'_m\}$ is inconsistent. Hence

$$\mathfrak{M} \models T \Rightarrow \mathfrak{M} \models \bigwedge_{i=1}^{n} \varphi_i \Rightarrow \mathfrak{M} \not\models \bigwedge_{i=1}^{m} \varphi'_i \Rightarrow \mathfrak{M} \not\models T' \Rightarrow \mathfrak{M} \models T,$$

showing that the sentence $\bigwedge_{i=1}^{n} \varphi_i$ is a finite axiomatization of $\mathcal{P}$. □

Example 3.1.6.

(1) For any prime number p, fields of characteristic p are finitely axiomatizable in the language $\mathcal{L}_{ring}$.

(2) Fields of characteristic 0 are axiomatizable in $\mathcal{L}_{ring}$, but are not finitely axiomatizable. Indeed, if a sentence φ_0 were a finite axiomatization, it would be a consequence of the theory $\varphi_{field} \cup \{\neg \underbrace{1 + \ldots + 1}_{p \text{ times}} = 0 \mid p \text{ prime}\}$, and then

$$\varphi_{fields} \cup \{\neg \underbrace{1 + \ldots + 1}_{p \text{ times}} = 0 \mid p \text{ prime and } p < N\} \vdash \varphi_0$$

for some $N \in \mathbb{N}$. This would lead to a contradiction, since there exist fields of characteristic $p > N$.

(3) Archimedean ordered fields are not axiomatizable (cf. Example 3.1.4(1)).

(4) Complete ordered fields are not axiomatizable (cf. Example 3.1.4(2)).

The last two examples make more precise what we said at the beginning of Chapter 2.

3.2. The Diagram Method

In practice, one often wishes to construct a model of some theory which contains a given structure as a substructure or as an elementary substructure. In this section, we will see that these properties may be encoded in suitable theories.

Let $\mathfrak{M}$ be an $\mathcal{L}$-structure. We consider the language $\mathcal{L}_M$ obtained by adding to $\mathcal{L}$ a new constant symbol c_m for each element m of M. The structure $\mathfrak{M}$ admits a natural expansion to the language $\mathcal{L}_M$, by interpreting c_m by m. We denote $\mathfrak{M}^*$ the corresponding $\mathcal{L}_M$-structure.

By abuse of notation, we shall sometimes identify m and c_m in what follows. This will not cause any trouble, because of the Substitution Lemma (Proposition 2.4.2).

Definition.

(1) The *complete diagram* of $\mathfrak{M}$, denoted by $D(\mathfrak{M})$, is defined as $\mathrm{Th}(\mathfrak{M}^*)$. It is the set of $\mathcal{L}_M$-sentences $\varphi(c_{m_1}, \ldots, c_{m_n})$, where

$\varphi(x_1, \dots, x_n)$ is an $\mathcal{L}$-formula and $\overline{m} \in M^n$ is such that $\mathfrak{M} \models \varphi[m_1, \dots, m_n]$.

(2) The *simple diagram* of $\mathfrak{M}$, denoted by $\Delta(\mathfrak{M})$, consists of all $\mathcal{L}_M$-sentences $\varphi(c_{m_1}, \dots, c_{m_n})$, where $\varphi(x_1, \dots, x_n)$ is a quantifier-free $\mathcal{L}$-formula and $\overline{m} \in M^n$ is a tuple such that $\mathfrak{M} \models \varphi[m_1, \dots, m_n]$.

Proposition 3.2.1. *Reducts to the language $\mathcal{L}$ of models of $D(\mathfrak{M})$ correspond, up to $\mathcal{L}$-isomorphism, to elementary extensions of $\mathfrak{M}$.*

Proof. Let $\mathfrak{N}' \models D(\mathfrak{M})$ and $\mathfrak{N} := \mathfrak{N}' \restriction_{\mathcal{L}}$ be its $\mathcal{L}$-reduct. The map $m \mapsto c_m^{\mathfrak{N}'}$ provides an isomorphism between $\mathfrak{M}$ and an elementary substructure of $\mathfrak{N}$.

Conversely, if $\mathfrak{M} \preccurlyeq \mathfrak{N}$, we consider the $\mathcal{L}_M$-expansion $\mathfrak{N}'$ of $\mathfrak{N}$ obtained by interpreting c_m by m. We will prove that $\mathfrak{N}' \models D(\mathfrak{M})$. For this, let $\varphi(c_{m_1}, \dots, c_{m_n}) \in D(\mathfrak{M})$. By definition, this means that $\mathfrak{M} \models \varphi[m_1, \dots, m_n]$, so $\mathfrak{N} \models \varphi[m_1, \dots, m_n]$ by elementarity, and finally $\mathfrak{N}' \models \varphi(c_{m_1}, \dots, c_{m_n})$ by the Substitution Lemma. □

Proposition 3.2.2. *Reducts to the language $\mathcal{L}$ of models of $\Delta(\mathfrak{M})$ correspond, up to $\mathcal{L}$-isomorphism, to extensions of $\mathfrak{M}$.*

Proof. Similar to the previous proof. □

Theorem 3.2.3 (Upward Löwenheim-Skolem Theorem)**.** *Let $\mathfrak{M}$ be an infinite $\mathcal{L}$-structure for some language $\mathcal{L}$, and let κ be a cardinal such that $\kappa \geq \sup(\mathrm{card}(M), \mathrm{card}(\mathcal{L}))$. Then there exists an elementary extension of $\mathfrak{M}$ which is of cardinality κ.*

Proof. It is enough to construct an elementary extension $\mathfrak{N}$ of $\mathfrak{M}$ of cardinality $\geq \kappa$, and to apply the Downward Löwenheim-Skolem Theorem to a subset $A \subseteq N$ of cardinality κ containing M.

For any $i \in \kappa$, let c_i be a new constant symbol. Consider the language $\widetilde{\mathcal{L}} := \mathcal{L}_M \cup \{c_i \mid i \in \kappa\}$ and the $\widetilde{\mathcal{L}}$-theory

$$\widetilde{T} := D(\mathfrak{M}) \cup \{\neg c_i = c_j \mid i < j < \kappa\}.$$

Then $\widetilde{T}$ is finitely satisfiable. Indeed, if $\widetilde{T}_0$ is a finite subset of $\widetilde{T}$, interpreting the new constant symbols $c_{i_1}, \dots, c_{i_n}$ occurring in $\widetilde{T}_0$ by distinct elements of M one gets an expansion of $\mathfrak{M}^*$ which is a model of $\widetilde{T}_0$. (This

is possible since M is infinite.) By compactness, one gets a model $\widetilde{\mathfrak{N}} \models \widetilde{T}$ whose $\mathcal{L}$-reduct $\mathfrak{N}$ is an elementary extension of $\mathfrak{M}$ (by Proposition 3.2.1) of cardinality $\geq \kappa$, since it contains the elements $c_i^{\widetilde{\mathfrak{N}}}$, for $i \in \kappa$, which are pairwise distinct. □

Corollary 3.2.4. *Let T be a theory having an infinite model. Then T has a model of cardinality κ for any $\kappa \geq \mathrm{card}(\mathcal{L})$.* □

Exercise 3.2.5. Let $\mathcal{L}$ be a finite language (that is, a language the signature of which is finite), and let $\mathfrak{M}$ be a finite $\mathcal{L}$-structure.

(1) Prove that there exists an $\mathcal{L}_M$-sentence $\varphi \in \Delta(\mathfrak{M})$ such that $\vdash \varphi \to \varphi'$ for any $\varphi' \in \Delta(\mathfrak{M})$.

(2) Deduce that if $\mathfrak{N} \equiv \mathfrak{M}$, then $\mathfrak{N} \cong \mathfrak{M}$.

(3) (More difficult.) Let $\mathfrak{M}'$ be a finite $\mathcal{L}'$-structure, with $\mathcal{L}'$ not necessarily finite. Prove that $\mathfrak{N}' \equiv \mathfrak{M}' \Rightarrow \mathfrak{N}' \cong \mathfrak{M}'$.

3.3. Expansions by Definition

It is often useful to enrich the language by symbols for definable relations, functions or constants. We will describe in this section how this may be done formally.

Notation. $\exists!\, x\psi$ ("there exists a unique x such that ψ") is an abbreviation for $\exists x(\psi \wedge \forall x'(\psi_{x'/x} \to x = x'))$, with x' a variable which is distinct from x.

Definition. Let T be an $\mathcal{L}$-theory and let $\mathcal{L}' \supseteq \mathcal{L}$. Assume that there are

- for any n-ary relation symbol $R \in \mathcal{L}' \setminus \mathcal{L}$ an $\mathcal{L}$-formula $\varphi_R(x_1, \dots, x_n)$,
- for any n-ary function symbol $f \in \mathcal{L}' \setminus \mathcal{L}$ an $\mathcal{L}$-formula $\varphi_f(x_0, x_1, \dots, x_n)$ such that $T \models \forall x_1, \dots, x_n \exists!\, x_0\, \varphi_f$,
- for any constant symbol $c \in \mathcal{L}' \setminus \mathcal{L}$ an $\mathcal{L}$-formula $\varphi_c(x_0)$ such that $T \models \exists!\, x_0\, \varphi_c$.

Then the $\mathcal{L}'$-theory T' given by T together with

- an axiom $\forall x_1, \dots, x_n(\varphi_R(x_1, \dots, x_n) \leftrightarrow Rx_1 \cdots x_n)$ for any relation symbol $R \in \mathcal{L}' \setminus \mathcal{L}$,

- an axiom $\forall x_1, \dots, x_n \, \varphi_f(f(x_1, \dots, x_n), x_1, \dots, x_n)$ for any function symbol $f \in \mathcal{L}' \setminus \mathcal{L}$,
- an axiom $\varphi_c(c)$ for any constant symbol $c \in \mathcal{L}' \setminus \mathcal{L}$

is called an *expansion by definition* of T.

Recall that two formulas $\varphi_1(x_1, \dots, x_n)$ and $\varphi_2(x_1, \dots, x_n)$ are called *equivalent in the theory* T if $T \vDash \forall x_1, \dots, x_n(\varphi_1 \leftrightarrow \varphi_2)$, and that they are called *logically equivalent* if they are equivalent in the empty theory (cf. Exercise 2.7.5).

Lemma 3.3.1. *Any formula is logically equivalent to a formula with all terms of height* ≤ 1.

Proof. For φ a formula, let $M(\varphi)$ be the maximal height of a term in φ. The proof will be by induction on $(M(\varphi), \mathrm{ht}(\varphi))$ with lexicographic order. The only non-trivial case is that of an atomic formula φ, say of the form $Rt_1 \cdots t_n$. To simplify notations, we assume that $\mathrm{ht}(t_i) > 1$ for $i = 1, \dots, m$ and $\mathrm{ht}(t_i) \leq 1$ for $i > m$. For $i = 1, \dots, m$, let $t_i = f_i(s_{i,1}, \dots, s_{i,k_i})$. One chooses new variables $y_{i,j}$, for $i = 1, \dots, m$ and $1 \leq j \leq k_i$. If $\overline{y}_i := (y_{i,1}, \dots, y_{i,k_i})$, then φ is logically equivalent to the formula ψ given by

$$\exists \overline{y}_1, \dots, \overline{y}_m \left(Rf_1(\overline{y}_1) \cdots f_m(\overline{y}_m) t_{m+1} \cdots t_n \wedge \bigwedge_{i,j} y_{i,j} = s_{i,j} \right)$$

and which satisfies $M(\psi) < M(\varphi)$. The case where φ is given by $t_1 = t_2$ is similar. □

Definition. Let T be an $\mathcal{L}$-theory and $T' \supseteq T$ an $\mathcal{L}'$-theory for some language $\mathcal{L}' \supseteq \mathcal{L}$. One says that T' is a *conservative expansion* of T if for any $\mathcal{L}$-sentence ψ one has $T \vDash \psi$ if and only if $T' \vDash \psi$.

Proposition 3.3.2. *Let T' be an expansion by definition of T. Then the expansion $T' \supseteq T$ is conservative. Furthermore, any $\mathcal{L}'$-formula ψ' is equivalent in T' to an $\mathcal{L}$-formula ψ.*

Proof. Any model $\mathfrak{M}$ of T has an $\mathcal{L}'$-expansion (in fact unique) to a model $\mathfrak{M}'$ of T'. For a relation symbol $R \in \mathcal{L}' \setminus \mathcal{L}$, we may and need to define $R^{\mathfrak{M}'} = \varphi_R[\mathfrak{M}]$ (cf. Exercise 2.7.4(1)). For a new function symbol f, this amounts to defining $f^{\mathfrak{M}'}(a_1, \dots, a_n) = a_0$ if $\mathfrak{M} \vDash \varphi_f[a_0, a_1, \dots, a_n]$.

The case of a new constant symbol is similar. It follows that $T' \supseteq T$ is conservative.

In order to show that any $\mathcal{L}'$-formula is equivalent in T' to an $\mathcal{L}$-formula, for simplicity we treat the case where $\mathcal{L}' = \mathcal{L} \cup \{f\}$ for an n-ary function symbol f. The general case is proved in a similar way.

First let ψ' be an atomic $\mathcal{L}'$-formula containing only terms of height ≤ 1, say ψ' equals $Rt_1 \cdots t_m$. Assume for simplicity that for $i = 1, \ldots, k$ one has $t_i = f(s_1^i, \ldots, s_n^i)$ and that f does not appear in t_i for $i > k$. The terms s_j^i have height 0, and thus are $\mathcal{L}$-terms. Let $z_1, \ldots, z_k$ be new variables. Then the $\mathcal{L}$-formula

$$\exists z_1, \ldots, z_k \left(Rz_1 \cdots z_k t_{k+1} \cdots t_m \wedge \bigwedge_{i=1}^{k} \varphi_f(z_i, s_1^i, \ldots, s_n^i) \right)$$

is equivalent in T' to ψ'. If ψ' equals $t_1 = t_2$, the argument is the same.

Now let ψ' be an arbitrary $\mathcal{L}'$-formula. By Lemma 3.3.1, we may assume that all terms occurring in ψ' have height at most 1. For any atomic subformula χ' of ψ', one chooses an equivalent $\mathcal{L}$-formula χ. (We just constructed such a formula.) One then defines ψ as the $\mathcal{L}$-formula obtained by replacing any atomic subformula χ' of ψ' by the corresponding $\mathcal{L}$-formula χ. It is a general fact that replacing subformulas by equivalent ones produces an equivalent formula. (This is proved in Exercise 2.7.5, where the notion of a subformula is also defined). □

Example 3.3.3.

(1) Let $T' = \mathrm{Th}(\mathfrak{R})$ be the theory of the ordered field of real numbers and T the theory of the (pure) field of real numbers. Since in $\mathbb{R}$ we have $r < s$ if and only if there exists $t \neq 0$ such that $t^2 = s - r$, T' is an expansion by definition of T.

(2) Let T be the $\mathcal{L}_{ord}$-theory of total orders without endpoints, and let T' be the $\mathcal{L}_{o.ring}$-theory of ordered fields. Then T' is a non-conservative expansion of T, since for example $T' \models \forall x, y(x < y \rightarrow \exists z(x < z \wedge z < y))$, that is, the order in any ordered field is dense (as any bounded interval has a midpoint), whereas this is not a logical consequence of T.

(3) Let $T = \mathrm{Th}(\langle \aleph_1; < \rangle)$. Then ω is a definable constant in T, that is, there is a formula $\varphi(x_0)$ such that $T \models \exists!\, x_0 \varphi$ and $\langle \aleph_1; < \rangle \models$

$\varphi[\omega]$. Indeed, the set of limit ordinals is defined by the formula

$$\exists y\, y < x \wedge \forall y \exists z (y < x \to y < z \wedge z < x)$$

which we denote by $\mathrm{Lim}(x)$, and it suffices to set $\varphi(x_0)$ equal to the formula $\mathrm{Lim}(x_0) \wedge \forall y(\mathrm{Lim}(y) \to \neg y < x_0)$.

Exercise 3.3.4. Let $T \subseteq T'$ be theories in languages $\mathcal{L}$ and $\mathcal{L}' \supseteq \mathcal{L}$, respectively. Prove that T' is equivalent to an expansion by definition of T if and only if every model of T admits a unique expansion to a model of T'.

3.4. Quantifier Elimination

Using induction on height, it is easy to check that every formula φ is logically equivalent to a formula ψ which is in *prenex form*, that is, of the form $Q_1 x_1 \cdots Q_n x_n \chi$, with χ quantifier-free and $Q_i \in \{\exists, \forall\}$ for all i. In general, the number of alternations of quantifiers $\exists$ and $\forall$ provides a good indication about the complexity of the formula φ (and of the set defined by φ in a given structure). In concrete examples, sets defined by a quantifier-free formula are usually easier to handle than those defined by an arbitrary formula. For this reason, quantifier elimination results are very useful and often open the way for a deeper understanding of the theory under consideration.

We shall start with the following important technical result.

Theorem 3.4.1. *Let T be an $\mathcal{L}$-theory, $n \geq 1$ a natural number and $\varphi(x_1, \ldots, x_n)$ an $\mathcal{L}$-formula. The following properties are equivalent:*

(1) *There is a quantifier-free $\mathcal{L}$-formula $\psi(x_1, \ldots, x_n)$ such that φ and ψ are equivalent in T.*

(2) *Let $\mathfrak{M}$ and $\mathfrak{N}$ be models of T and let $\mathfrak{A}$ be a common substructure of $\mathfrak{M}$ and $\mathfrak{N}$. Then for any $\overline{a} \in A^n$ one has $\mathfrak{M} \vDash \varphi[\overline{a}] \iff \mathfrak{N} \vDash \varphi[\overline{a}]$.*

Remark 3.4.2. When $n = 0$ and φ is a sentence, one may consider φ as $\varphi(x)$ and apply the theorem to $\varphi(x)$ to find a quantifier-free formula $\psi(x)$ which is equivalent to $\varphi(x)$ in T. For instance, the theorem $\exists y y = y$ of T is equivalent in T to the formula $x = x$.

Note that if the language $\mathcal{L}$ does not contain a constant symbol, there is no quantifier-free $\mathcal{L}$-sentence. In this case, when we assert the existence of a quantifier-free *formula* ψ equivalent to a *sentence* φ in what follows, we will allow that ψ has one free variable.

Proof of Theorem 3.4.1. (1)⇒(2). We first observe that if $\mathfrak{A} \subseteq \mathfrak{B}$, $\psi(x_1, \dots, x_n)$ is a quantifier-free formula and $\overline{a} \in A^n$, then one has $\mathfrak{A} \models \psi[\overline{a}] \iff \mathfrak{B} \models \psi[\overline{a}]$. Thus, if $\mathfrak{M}$ et $\mathfrak{N}$ are models of T having $\mathfrak{A}$ as a common substructure and if $\varphi(x_1, \dots, x_n)$ is equivalent in T to the quantifier-free formula $\psi(x_1, \dots, x_n)$, then for $\overline{a} \in A^n$ one has

$$\mathfrak{M} \models \varphi[\overline{a}] \iff \mathfrak{M} \models \psi[\overline{a}] \iff \mathfrak{A} \models \psi[\overline{a}] \iff \mathfrak{N} \models \psi[\overline{a}] \iff \mathfrak{N} \models \varphi[\overline{a}].$$

(2)⇒(1). We consider the set of formulas

$$\Gamma(\overline{x}) := \{\chi(x_1, \dots, x_n) \text{ quantifier-free} \mid T \models \forall x_1, \dots, x_n(\varphi \to \chi)\}.$$

We choose new pairwise distinct constants $c_1, \dots, c_n$, and we consider the theory $\Gamma(\overline{c}) := \{\chi(c_1, \dots, c_n) \mid \chi \in \Gamma(\overline{x})\}$ in the augmented language $\mathcal{L}' = \mathcal{L} \cup \{c_1, \dots, c_n\}$. We now prove that

$$(*) \qquad T \cup \Gamma(\overline{c}) \models \varphi(\overline{c}).$$

If $(*)$ did not hold, one could find $\mathfrak{M}' \models T \cup \Gamma(\overline{c}) \cup \{\neg\varphi(\overline{c})\}$. Let $\mathfrak{A}' := \langle c_1^{\mathfrak{M}'}, \dots, c_n^{\mathfrak{M}'} \rangle_{\mathfrak{M}'} = \langle A; \dots \rangle$ be the substructure generated by the elements $c_i^{\mathfrak{M}'}$ in $\mathfrak{M}'$. Observe that $\Gamma(\overline{c}) \subseteq \Delta(\mathfrak{A}')$. Let us prove that

$$\Sigma := T \cup \Delta(\mathfrak{A}') \cup \{\varphi(\overline{c})\}$$

has a model.

Otherwise, $T \cup \Delta(\mathfrak{A}') \models \neg\varphi(\overline{c})$. Since any element of A can be written as an $\mathcal{L}'$-term, if one denotes by $\Delta_{\overline{c}}(\mathfrak{A}')$ the set of quantifier-free $\mathcal{L}'$-sentences in $\Delta(\mathfrak{A}')$, then $T \cup \Delta(\mathfrak{A}')$ is a conservative expansion of $T \cup \Delta_{\overline{c}}(\mathfrak{A}')$ by Proposition 3.3.2. In particular,

$$T \cup \Delta_{\overline{c}}(\mathfrak{A}') \models \neg\varphi(\overline{c}).$$

Hence there exist quantifier-free $\mathcal{L}$-formulas $\xi_1(\overline{x}), \dots, \xi_k(\overline{x})$ such that

$$T \models \bigwedge_{i=1}^{k} \xi_i(\overline{c}) \to \neg\varphi(\overline{c}) \qquad \text{and} \qquad \Delta(\mathfrak{A}') \models \bigwedge_{i=1}^{k} \xi_i(\overline{c}) =: \xi(\overline{c}).$$

Since the constant symbols c_i do not appear in T, or in $\varphi(\overline{x})$ or $\xi(\overline{x})$, one deduces (for instance by Lemma 2.6.8) that

$$T \models \forall \overline{x}(\xi(\overline{x}) \to \neg\varphi(\overline{x}))$$

and then $T \models \forall \overline{x}(\varphi(\overline{x}) \to \neg\xi(\overline{x}))$. By definition it follows that $\neg\xi(\overline{x}) \in \Gamma(\overline{x})$ and $\neg\xi(\overline{c}) \in \Gamma(\overline{c})$, hence $\neg\xi(\overline{c}) \in \Delta(\mathfrak{A}')$, which provides a contradiction.

Hence Σ has a model $\mathfrak{N}^*$, and the $\mathcal{L}$-reduct $\mathfrak{N}$ of $\mathfrak{N}^*$ contains an isomorphic copy $\mathfrak{B}'$ of $\mathfrak{A}'$ as a substructure by Proposition 3.2.2. Up to identifying $\mathfrak{B}'$ and $\mathfrak{A}'$, we have constructed two models $\mathfrak{M} = \mathfrak{M}' \restriction_{\mathcal{L}}$ and $\mathfrak{N}$ of T containing a common substructure $\mathfrak{A} = \mathfrak{A}' \restriction_{\mathcal{L}}$ such that, if one sets $a_i = c_i^{\mathfrak{M}'}$, then $\mathfrak{N} \models \varphi[\overline{a}]$ and $\mathfrak{M} \models \neg\varphi[\overline{a}]$, which contradicts (2). We have thus proved $(*)$.

By compactness there exist $\zeta_1(\overline{c}), \ldots, \zeta_m(\overline{c}) \in \Gamma(\overline{c})$ such that

$$T \models \bigwedge_{i=1}^{m} \zeta_i(\overline{c}) \to \varphi(\overline{c}).$$

As above, this implies that $T \models \forall \overline{x}\left(\bigwedge_{i=1}^{m} \zeta_i(\overline{x}) \to \varphi(\overline{x})\right)$. Since for all i we have $T \models \forall \overline{x}(\varphi \to \zeta_i)$, we infer that $T \models \forall \overline{x}\left(\bigwedge_{i=1}^{m} \zeta_i(\overline{x}) \leftrightarrow \varphi(\overline{x})\right)$, with $\bigwedge_{i=1}^{m} \zeta_i(\overline{x})$ a quantifier-free $\mathcal{L}$-formula. □

Definition. Let T be an $\mathcal{L}$-theory. One says that T admits *quantifier elimination* (in the language $\mathcal{L}$) if every $\mathcal{L}$-formula φ is equivalent in T to a quantifier-free $\mathcal{L}$-formula.

Lemma 3.4.3. *Assume that for every quantifier-free formula φ and any variable x there exists a quantifier-free formula ψ such that $\exists x\varphi$ and ψ are equivalent in T. Then T admits quantifier elimination.*

Proof. Let ψ and ψ' be two formulas which are equivalent in T, which we denote by $\psi \sim_T \psi'$. Since $\neg\psi \sim_T \neg\psi'$, $\exists x\psi \sim_T \exists x\psi'$ and $\chi \wedge \psi \sim_T \chi \wedge \psi'$ for any formula χ, we can argue by induction on the height of the formula, and the statement follows, by considering only formulas in prenex form and eliminating one quantifier at the time. □

Theorem 3.4.4. *Let T be an $\mathcal{L}$-theory. One assumes that for any pair of models $\mathfrak{M}$ and $\mathfrak{N}$ of T, for any common substructure $\mathfrak{A}$ of $\mathfrak{M}$ and $\mathfrak{N}$ and for*

any quantifier-free formula $\varphi(x_0, \dots, x_n)$, if there exist $\overline{a} \in A^n$ and $b_0 \in M$ such that $\mathfrak{M} \models \varphi[b_0, \overline{a}]$, then there exists $c_0 \in N$ such that $\mathfrak{N} \models \varphi[c_0, \overline{a}]$.

Then T admits quantifier elimination.

Remark. The converse of this statement is clear: any theory which admits quantifier elimination satisfies the hypothesis of the theorem.

Proof of Theorem 3.4.4. Let $\mathfrak{A} \subseteq \mathfrak{M}, \mathfrak{N} \models T$. Let φ be a quantifier-free formula and let χ be $\exists x_0 \varphi$. By hypothesis, we have $\mathfrak{M} \models \chi[\overline{a}] \iff \mathfrak{N} \models \chi[\overline{a}]$ for every $\overline{a} \in A^n$. It follows from Theorem 3.4.1 that χ is equivalent in T to a quantifier-free formula, which is enough to conclude by Lemma 3.4.3. □

Proposition 3.4.5. *Let T be a theory which admits quantifier elimination.*

(1) *Let $\mathfrak{M}$ and $\mathfrak{N}$ be models of T with a common substructure. Then $\mathfrak{M} \equiv \mathfrak{N}$.*

(2) *Let $\mathfrak{M}$ and $\mathfrak{N}$ be models of T. If $\mathfrak{M} \subseteq \mathfrak{N}$, then $\mathfrak{M} \preccurlyeq \mathfrak{N}$.*

Proof. (1) This is a special case of the easy implication in Theorem 3.4.1. Indeed, any sentence φ is equivalent in T to a quantifier-free formula $\psi(x)$. Let $\mathfrak{A}$ be a common substructure of $\mathfrak{M}$ and $\mathfrak{N}$. For any $a \in A$, one then has

$$\begin{aligned} \mathfrak{M} \models \varphi \iff \mathfrak{M} \models \psi[a] &\iff \mathfrak{A} \models \psi[a] \\ &\iff \mathfrak{N} \models \psi[a] \iff \mathfrak{N} \models \varphi. \end{aligned}$$

(2) This is a direct consequence of Theorem 3.4.1. □

3.5. Algebraically Closed Fields

In this section we treat an important and particularly nice example of a theory from algebra, namely the $\mathcal{L}_{ring}$-theory ACF of algebraically closed fields (see Example 2.6.3).

Let A be a subring of a field K. An element of K is said to be *algebraic over A* if it is the root of a non-zero polynomial with coefficients in A. If A is an integral domain, an *algebraic closure of A* is an algebraically closed field K containing A such that any element of K is algebraic over A.

In the following fact we list some results from field theory which we will need in this and the next section.

Fact 3.5.1. *Let A be an integral domain.*

(1) *There exists an algebraic closure of A.*

(2) *If K and K' are algebraic closures of A, then there exists an isomorphism $f : K \cong K'$ such that $f \restriction_A = \mathrm{id}_A$.*

(3) *Assume A is a subring of an algebraically closed field L. Then the subfield $A_L^{alg} = \{b \in L \mid b \text{ is algebraic over } A\}$ is an algebraic closure of A.*

(4) *Let $\mathbb{F}_p^{alg}$ be an algebraic closure of the field with p elements $\mathbb{F}_p$. Then $\mathbb{F}_p^{alg}$ is an increasing union of finite subfields F_N, $N \in \mathbb{N}$. More precisely, for any integer $k \geq 1$, the set of roots of the polynomial $X^{p^k} - X$ in $\mathbb{F}_p^{alg}$ is a subfield $\mathbb{F}_{p^k}$ (with p^k elements), and $\bigcup_{k\in\mathbb{N}} \mathbb{F}_{p^k} = \mathbb{F}_p^{alg}$. Since furthermore $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^l}$ when $k \mid l$, it is enough to take $F_N := \mathbb{F}_{p^{N!}}$.*

(5) *Any algebraically closed field is infinite.*

(6) *Let $K \subseteq L$ be a field extension with K an algebraically closed field, and let $b \in L \setminus K$. Then b is not algebraic over K.*

Theorem 3.5.2 (Chevalley-Tarski)**.** *The theory* ACF *admits quantifier elimination.*

Proof. First observe that a substructure of a field in $\mathcal{L}_{ring}$ is nothing but a subring. By Theorem 3.4.4 it is thus enough to prove that if K and L are algebraically closed fields, A is a common subring, and $\varphi(x_0, \dots, x_n)$ is a quantifier-free formula, then for any $\overline{a} \in A^n$, if there exists $b \in L$ such that $L \models \varphi[b, \overline{a}]$ then there exists $c \in K$ such that $K \models \varphi[c, \overline{a}]$.

By Fact 3.5.1, K and L contain algebraic closures F_K and F_L of A that are isomorphic via an isomorphism inducing the identity on A. Enlarging A if necessary, we may thus assume that A is an algebraically closed field and even that $A = K \subseteq L$.

The formula φ is logically equivalent to a formula of the form $\bigvee_i \bigwedge_j \chi_{i,j}$, with each $\chi_{i,j}(x_0, \dots, x_n)$ either atomic or the negation of an atomic formula. If $L \models \varphi[b, \overline{a}]$, there exists i such that

$L \models \bigwedge_j \chi_{i,j}[b, \overline{a}]$. It is thus enough to consider the case where φ is a conjunction of atomic formulas and negations of atomic formulas. In the theory of fields, any atomic formula is equivalent to $P(\overline{x}) = 0$ for some polynomial $P(\overline{x})$ with integer coefficients. We may therefore assume that $\varphi(\overline{x})$ is of the form

$$\bigwedge_{i=1}^{n} P_i(\overline{x}) = 0 \wedge \bigwedge_{i=1}^{m} \neg Q_i(\overline{x}) = 0.$$

If one of the $P_i(x_0, a_1, \dots, a_n) \in K[x_0]$ is a non-zero polynomial, then b is algebraic over K, which implies that $b \in K$ and we are done.

Thus we may assume that φ equals $\bigwedge_{i=1}^{m} \neg Q_i(\overline{x}) = 0$. By the existence of b, each polynomial $Q_i(x_0, \overline{a}) \in K[x_0]$ is non-zero, and hence has only a finite number of roots. The field K is infinite, since it is algebraically closed, so there exists $c \in K$ such that $K \models \varphi[c, \overline{a}]$. □

Corollary 3.5.3. *In $K \models$ ACF, the definable sets* (*with parameters*) *are precisely the* constructible *sets, that is, sets given by boolean combinations of polynomial equations with coefficients from K.* □

Let p be a prime number or $p = 0$. We denote by ACF_p the theory of algebraically closed fields of characteristic p.

Theorem 3.5.4. *Let p be a prime number or $p = 0$. The theory ACF_p is complete.*

Proof. Any field of characteristic $p > 0$ contains $\mathbb{F}_p$ as a subfield. If K and L are algebraically closed fields of characteristic p, then $K \equiv L$ by Theorem 3.5.2 and Proposition 3.4.5(1), which proves that ACF_p is complete.

For ACF_0, the argument is the same, replacing $\mathbb{F}_p$ by $\mathbb{Q}$. □

Theorem 3.5.5 (Lefschetz Principle)**.** *Let φ be an $\mathcal{L}_{ring}$-sentence. The following conditions are equivalent:*

(1) $\mathbb{C} \models \varphi$.

(2) *There exists an algebraically closed field of characteristic 0 in which φ is satisfied.*

(3) *Any algebraically closed field of characteristic 0 satisfies φ.*

(4) *There exists $N \in \mathbb{N}$ such that φ is satisfied in any algebraically closed field of characteristic $p > N$.*

(5) *There exists an infinite set of prime numbers $\mathcal{P}$ such that for any $p \in \mathcal{P}$ there exists an algebraically closed field of characteristic p in which φ is satisfied.*

Proof. (1) $\iff$ (2) $\iff$ (3) follows from Theorem 3.5.4.

(3)$\Rightarrow$(4). Note that ACF_0 is equal to $\mathrm{ACF} \cup \{\chi_p \mid p \text{ prime}\}$, where χ_p expresses that $p = 1 + \cdots + 1$ is different from 0. If $\mathrm{ACF}_0 \vDash \varphi$, by compactness there exists a finite subset Δ of ACF_0 such that $\Delta \vDash \varphi$. But Δ contains only a finite set of sentences χ_p. Thus, there exists $N \in \mathbb{N}$ such that $K \vDash \Delta$ for any algebraically closed field K of characteristic $p > N$. For such a field K, one has $K \vDash \varphi$.

(4)$\Rightarrow$(5) is clear.

(5)$\Rightarrow$(3). For $p \in \mathcal{P}$, let $K_p \vDash \mathrm{ACF}_p$ such that $K_p \vDash \varphi$. If $\mathrm{ACF}_0 \nvDash \varphi$, then $\mathrm{ACF}_0 \vDash \neg\varphi$ by completeness. By the implication (3)$\Rightarrow$(4), there exists $N \in \mathbb{N}$ such that $\neg\varphi$ is satisfied in any algebraically closed field of characteristic $p > N$. This forces $\mathcal{P}$ to be finite, a contradiction. □

Theorem 3.5.6 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field and $P_1(\overline{x}), \ldots, P_m(\overline{x}) \in K[x_1, \ldots, x_n]$. If the system of polynomial equations $P_1(\overline{x}) = P_2(\overline{x}) = \ldots = P_m(\overline{x}) = 0$ has a solution in some field $L \supseteq K$, then it already has a solution in K.*

Proof. Let $L \supseteq K$ and $\overline{a} \in L^n$ be such that $P_1(\overline{a}) = \ldots = P_m(\overline{a}) = 0$. Up to enlarging L if necessary, we may assume that L is algebraically closed. Since ACF admits quantifier elimination, we have $K \preccurlyeq L$ by Proposition 3.4.5.

We now choose $\mathcal{L}_{ring}$-terms $F_i(\overline{x}, \overline{z_i})$ and tuples $\overline{b}_i$ in K such that $P_i(\overline{x}) = F_i(\overline{x}, \overline{b}_i)$. Then $L \vDash \exists\overline{x} \bigwedge F_i(\overline{x}, \overline{b}_i) = 0$, and therefore $K \vDash \exists\overline{x} \bigwedge F_i(\overline{x}, \overline{b}_i) = 0$, since $K \preccurlyeq L$. □

3.6. Ax's Theorem

A chain of $\mathcal{L}$-structures is a sequence $(\mathfrak{M}_i)_{i\in\mathbb{N}}$ of $\mathcal{L}$-structures such that $\mathfrak{M}_i \subseteq \mathfrak{M}_{i+1}$ for any i.

If $(\mathfrak{M}_i)_{i\in\mathbb{N}}$ is such a chain, there exists a unique $\mathcal{L}$-structure $\mathfrak{M}$ with base set $M = \bigcup_{i\in\mathbb{N}} M_i$ such that $\mathfrak{M}_i \subseteq \mathfrak{M}$ for any i. Indeed, the only way to interpret the language symbols is to set $c^{\mathfrak{M}} = c^{\mathfrak{M}_0}$, $f^{\mathfrak{M}} = \bigcup_{i\in\mathbb{N}} f^{\mathfrak{M}_i}$ and $R^{\mathfrak{M}} = \bigcup_{i\in\mathbb{N}} R^{\mathfrak{M}_i}$, which is clearly well defined. The $\mathcal{L}$-structure $\mathfrak{M}$ obtained that way is denoted by $\bigcup_{i\in\mathbb{N}} \mathfrak{M}_i$.

Definition. A formula of the form $\forall x_1, \dots, x_n \exists y_1, \dots, y_m \varphi$, with φ quantifier-free and $m, n \geq 0$, is called a $\forall\exists$-*formula*.

Lemma 3.6.1 (Preservation of $\forall\exists$-sentences under unions of chains)**.** *Let ψ be a $\forall\exists$-sentence in $\mathcal{L}$ and $(\mathfrak{M}_i)_{i\in\mathbb{N}}$ a chain of $\mathcal{L}$-structures such that $\mathfrak{M}_i \models \psi$ for any i. Then $\mathfrak{M} = \bigcup_{i\in\mathbb{N}} \mathfrak{M}_i \models \psi$.*

Proof. Let ψ be the sentence $\forall x_1, \dots, x_n \exists y_1, \dots, y_m \varphi(\overline{x}, \overline{y})$ with φ quantifier-free. We have to prove that $\mathfrak{M} \models \exists y_1, \dots, y_m \varphi[\overline{a}, \overline{y}]$ for any $\overline{a} \in M^n$. Since the sequence of base sets $(M_i)_{i\in\mathbb{N}}$ is increasing, there exists $k \in \mathbb{N}$ such that $\overline{a} \in M_k^n$. Hence there exist $b_1, \dots, b_m \in M_k$ such that $\mathfrak{M}_k \models \varphi[\overline{a}, \overline{b}]$, as $\mathfrak{M}_k \models \psi$. One deduces that $\mathfrak{M} \models \varphi[\overline{a}, \overline{b}]$, since φ is quantifier-free and $\mathfrak{M}_k$ is a substructure of $\mathfrak{M}$. □

Remark. It will be proved in Exercise 3.7.11 that a sentence is preserved under unions of chains if and only if it is logically equivalent to a $\forall\exists$-sentence.

Proposition 3.6.2. *Let φ be a $\forall\exists$-sentence in the language $\mathcal{L}_{ring}$ which is satisfied in every finite field. Then* ACF $\models \varphi$. *In particular φ is satisfied in $\mathbb{C}$.*

Proof. As recalled in Fact 3.5.1(4), $\mathbb{F}_p^{alg}$ is the union of a chain of finite fields. So it follows from Lemma 3.6.1 that one has $\mathbb{F}_p^{alg} \models \varphi$ for every prime p. The statement is now a consequence of the Lefschetz Principle. □

Theorem 3.6.3 (Ax's Theorem)**.** *Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial mapping, that is, of the form $f = (f_1, \dots, f_n)$ with $f_i \in \mathbb{C}[x_1, \dots, x_n]$ polynomials. If f is injective, then f is surjective.*

Proof. There exist $\mathcal{L}_{ring}$-terms — which can be interpreted as polynomials with integer coefficients — $P_{n,d}(\overline{z}, \overline{x})$ such that, for any field K, any polynomial $g(\overline{x}) \in K[x_1, \dots, x_n]$ of degree $\leq d$ may be written as

$P_{n,d}(\overline{a},\overline{x})$ for some tuple $\overline{a}$ of elements of K. The following sentence $\psi_{n,d}$ is $\forall\exists$ and expresses that any injective polynomial function $f : K^n \to K^n$, with all polynomials f_i of degree at most d, is surjective:

$$\forall \overline{z}_1, \dots, \overline{z}_n, \overline{u}\, \exists \overline{x}, \overline{x}' \left[\left(\bigwedge_{i=1}^{n} P_{n,d}(\overline{z}_i, \overline{x}) = u_i \right) \vee \left(\bigwedge_{i=1}^{n} P_{n,d}(\overline{z}_i, \overline{x}) = P_{n,d}(\overline{z}_i, \overline{x}') \wedge \neg \bigwedge_{i=1}^{n} x_i = x_i' \right) \right].$$

Since $\psi_{n,d}$ is satisfied in every finite field, it follows from Proposition 3.6.2 that ACF $\vDash \psi_{d,n}$, so in particular $\mathbb{C} \vDash \psi_{d,n}$. □

3.7. Exercises

Exercise 3.7.1. Let $\mathfrak{M}_1$ and $\mathfrak{M}_2$ be two $\mathcal{L}$-structures. Prove that $\mathfrak{M}_1 \equiv \mathfrak{M}_2$ if and only there exist $\mathfrak{N}_1, \mathfrak{N}_2$ and $\mathfrak{P}$ such that $\mathfrak{M}_i \cong \mathfrak{N}_i$ and $\mathfrak{N}_i \preccurlyeq \mathfrak{P}$ for $i = 1, 2$.

Exercise 3.7.2. Let $T = \mathrm{Th}(\mathfrak{N})$, where $\mathfrak{N}$ denotes the $\mathcal{L}_{ar}$-structure $\langle \mathbb{N}; S, 0, +, \cdot, < \rangle$. Prove that there exists $\mathfrak{N}' \vDash T$ such that N' contains a non-standard prime number, that is, an element p' such that one has $\mathfrak{N}' \vDash \forall x (\exists y\, x \cdot y = p' \to (x = 1 \vee x = p'))$ and $\mathfrak{N}' \vDash (\underbrace{S \cdots S}_{n \text{ times}} 0) < p'$ for any $n \in \mathbb{N}$.

Exercise 3.7.3. Prove that any theory T admits an expansion by definition that admits quantifier elimination.

Exercise 3.7.4 (Vaught's Criterion)**.** Let $\mathcal{L}$ be a first-order language and κ an infinite cardinal. An $\mathcal{L}$-theory T is said to be *κ-categorical* if all its models of cardinality κ are isomorphic.

We assume that κ is larger than or equal to the cardinality of $\mathcal{L}$.

(1) Let T be an $\mathcal{L}$-theory. Prove that any infinite model of T is elementarily equivalent to a model of T of cardinality κ.

(2) Prove that if a consistent theory T is κ-categorical and has no finite model then it is complete.

Exercise 3.7.5. Let $\mathcal{L}$ be a first-order language, and let I be a non-empty set. Let $(\mathfrak{M}_i)_{i\in I}$ be a family of $\mathcal{L}$-structures. Finally, let U be an ultrafilter on I. (We refer to Exercise 1.11.8 for the notion of an ultrafilter.) If M_i is the underlying set of $\mathfrak{M}_i$, we consider the following equivalence relation on $\prod_I M_i$: $(a_i) \equiv_U (b_i)$ if and only if $\{i \in I \mid a_i = b_i\} \in U$. We denote by M_U the set of equivalence classes and by $\pi : \prod_I M_i \to M_U$ the canonical projection.

(1) Prove that $\equiv_U$ is indeed an equivalence relation.

(2) Prove that M_U admits a unique $\mathcal{L}$-structure $\mathfrak{M}_U$ such that for every atomic $\mathcal{L}$-formula $\varphi(x^1, \cdots, x^n)$ and every tuple $(a^1, \cdots, a^n) \in (\prod_I M_i)^n$ one has

$$\mathfrak{M}_U \vDash \varphi[\pi(a^1), \cdots, \pi(a^n)]$$

if and only if the set of i such that $\mathfrak{M}_i \vDash \varphi[a_i^1, \cdots, a_i^n]$ is in U. The structure $\mathfrak{M}_U$ is called the *ultraproduct* of the $\mathfrak{M}_i$ with respect to U. It is denoted by $\prod_U \mathfrak{M}_i$.

(3) Prove Łoś's Theorem: *For every formula $\varphi(x^1, \cdots, x^n)$ and every tuple $(a^1, \cdots, a^n) \in (\prod_I M_i)^n$, one has*

$$\mathfrak{M}_U \vDash \varphi[\pi(a^1), \cdots, \pi(a^n)]$$

if and only if $\{i \in I \mid \mathfrak{M}_i \vDash \varphi[a_i^1, \cdots, a_i^n]\} \in U$.

(4) Use Łoś's Theorem to give a direct proof of the Compactness Theorem (Theorem 3.1.1).
[Hint: For a theory T, let I be the set of all finite subsets of T. Show that there is an ultrafilter U on I which contains $A_{T_0} := \{T_1 \in I \mid T_1 \supseteq T_0\}$ for every $T_0 \in I$. Prove that if $\mathfrak{M}_{T_0} \vDash T_0$ for every T_0, then $\prod_U \mathfrak{M}_{T_0}$ is a model of T.]

(5) Let P be the set of prime numbers, and let U be a non-principal ultrafilter on P. We work in $\mathcal{L}_{ring}$, and we consider the family $(\mathbb{F}_p)_{p\in P}$ of fields with p elements and their ultraproduct $\mathbb{F}_U$ with respect to U. Observe that $\mathbb{F}_U$ is a field. Determine its characteristic.

(6) Let $(\mathfrak{M}_i)_{i\in\mathbb{N}}$ be a family of infinite well-orderings, considered in $\mathcal{L}_{ord}$. Let U be a non-principal ultrafilter on $\mathbb{N}$, and let $\mathfrak{M}_U$ be the ultraproduct of the $\mathfrak{M}_i$ with respect to U.

Prove that there is a strictly decreasing sequence in $\mathfrak{M}_U$ of length $\aleph_1$. In particular, $\mathfrak{M}_U$ is not a well-ordering.

Exercise 3.7.6.

(1) We denote by DLO the $\mathcal{L}_{ord}$-theory of dense total orderings without endpoints.
   (a) Let $\mathfrak{M}, \mathfrak{M}'$ be models of DLO and let $\mathfrak{A} \subseteq \mathfrak{M}$, $\mathfrak{A}' \subseteq \mathfrak{M}'$ be finite substructures. Assume that $f : \mathfrak{A} \cong \mathfrak{A}'$ is an $\mathcal{L}_{ord}$-isomorphism and $b \in M$. Prove that f can be extended to an isomorphism with domain $A \cup \{b\}$ and image contained in M'.
   (b) Deduce that DLO admits quantifier elimination and is complete.
   (c) Prove that DLO is $\aleph_0$-categorical.
   (d) (More difficult.) Prove that for every cardinal $\kappa > \aleph_0$, the theory DLO is not κ-categorical.

(2) Let $\mathcal{L}' = \mathcal{L}_{ord} \cup \{c_i \mid i \in \mathbb{N}\}$, with $\{c_i \mid i \in \mathbb{N}\}$ a set of constant symbols. Let DLO$'$ be the $\mathcal{L}'$-theory obtained by adding to DLO the axioms $c_i < c_j$ for any $i, j \in \mathbb{N}$ with $i < j$.
   (a) Prove that DLO$'$ is a complete theory.
   (b) Prove that the theory DLO$'$ has exactly three countable models up to isomorphism.

Exercise 3.7.7. Let T be the $\mathcal{L}_{ord}$-theory of total discrete orders without endpoints, that is, totally ordered sets such that any element has an (immediate) predecessor and an (immediate) successor. Observe that $\langle \mathbb{Z}; < \rangle \models T$.

(1) Prove that T does not admit quantifier elimination.

(2) Write an $\mathcal{L}_{ord}$-formula which defines the graph of the successor function in any model of T. Let T' be the definitional expansion of T in the language $\mathcal{L}' = \{<, S\}$, where S corresponds to the successor function. Prove that T' admits quantifier elimination and is complete.

(3) Deduce that T is complete.

Exercise 3.7.8. Let $m \neq n$ be natural numbers. Prove that there is an $\mathcal{L}_{ord}$-sentence which is true in $\langle \omega \cdot m, < \rangle$ and false in $\langle \omega \cdot n, < \rangle$. Is there an $\mathcal{L}_{ord}$-sentence which is true in $\langle \omega^m, < \rangle$ and false in $\langle \omega^n, < \rangle$?

Exercise 3.7.9. In this exercise, we consider the theory of the structure $\mathfrak{M}_0 := \langle \mathbb{Q}; 0, +, < \rangle$. Recall that an *ordered abelian group* is an abelian group A endowed with a compatible total ordering ($a < b$ implies $a+c < b+c$ for any $a, b, c \in A$). We shall deal with ordered abelian groups in the language $\mathcal{L}_{\mathrm{OAG}} := \{0, +, <\}$, and we denote by OAG the corresponding theory.

Let DOAG be the theory of non-trivial divisible ordered abelian groups. It is obtained by adding to OAG the following axioms:

(i) $\exists x\, x \neq 0$ and

(ii) an axiom of the form $\forall x \exists y\ \underbrace{y + \cdots + y}_{n \text{ times}} = x$ for any integer $n \geq 1$.

Observe that $\mathfrak{M}_0 \models \mathrm{DOAG}$.

(1) Prove that if $\langle D; 0, +, < \rangle \models \mathrm{DOAG}$, then $\langle D; < \rangle \models \mathrm{DLO}$. (See Exercise 3.7.6 for the theory DLO.)

(2) Prove that if $\langle A; 0, +, < \rangle \models \mathrm{OAG}$, then $\langle A; 0, + \rangle$ is torsion-free, that is, if $na = 0$ for $a \in A$ and $n \in \mathbb{N}^*$, then $a = 0$.

(3) Let $\mathfrak{D} \models \mathrm{DOAG}$ and let $\mathfrak{A} = \langle A; 0, +, < \rangle \subseteq \mathfrak{D}$. We denote by $\mathrm{div}_{\mathfrak{D}}(\mathfrak{A})$ the substructure with base set

$$\{d \in D \mid \exists n \geq 1 \text{ and } a \in A \text{ such that } a + n \cdot d \in A\}.$$

Prove that if $\mathfrak{D}, \mathfrak{D}' \models \mathrm{DOAG}$ and $\mathfrak{A} \subseteq \mathfrak{D}$, $\mathfrak{A}' \subseteq \mathfrak{D}'$, then every isomorphism $f : \mathfrak{A} \cong \mathfrak{A}'$ extends uniquely to an isomorphism $\tilde{f} : \mathrm{div}_{\mathfrak{D}}(\mathfrak{A}) \cong \mathrm{div}_{\mathfrak{D}'}(\mathfrak{A}')$.

(4) Prove that DOAG is complete and admits quantifier elimination.

(5) Deduce that if $\mathfrak{D} \models \mathrm{DOAG}$ and $\varphi(x)$ is any $(\mathcal{L}_{\mathrm{OAG}})_D$-formula, then the subset of D defined by $\varphi(x)$ is a finite union of open intervals and singletons.

Exercise 3.7.10 (Embedding Theorem)**.** Given languages $\mathcal{L}' \subseteq \mathcal{L}$ and an $\mathcal{L}$-theory T, we denote by $T'_\forall$ (or by $T_\forall$ in case $\mathcal{L} = \mathcal{L}'$) the theory of

all universal $\mathcal{L}'$-sentences (that is, sentences of the form $\forall x_1, \dots, x_n \psi$ for ψ quantifier-free) which are consequences of T.

(1) Prove the Embedding Theorem: *An $\mathcal{L}'$-structure $\mathfrak{M}'$ embeds into the $\mathcal{L}'$-reduct of a model of T if and only if $\mathfrak{M}' \models T'_\forall$.*
[Hint: Use the diagram method to establish the non-trivial implication.]

(2) Application. A group G is called *left-orderable* if there exists a total order $<$ on G such that for all elements x, y, g from G, $x < y$ entails $g \cdot x < g \cdot y$. Now let $\mathcal{L}_{gp} = \{e, \cdot, (\cdot)^{-1}\}$ be the language of groups.
   (a) Prove that the class of left-orderable groups may be axiomatized by a universal $\mathcal{L}_{gp}$-theory.
   (b) Give an explicit (universal) axiomatzation in the case of commutative groups.

(3) (a) Prove the Preservation Theorem for universal theories: *T may be axiomatzed by universal sentences if and only if it is preserved under substructures, that is, any substructure of a model of T is a model of T.*
   (b) Let T be the theory of fields in $\mathcal{L}_{ring}$. Determine the models of $T_\forall$.

Exercise 3.7.11 (Preservation Theorem for $\forall\exists$-theories)**.** The aim of this exercise is to prove that the following conditions (i) and (ii) are equivalent for a theory T (Chang-Łoś-Suszko Theorem):

(i) *T is preserved under unions of chains, that is, if $(\mathfrak{M}_i)_{i\in\mathbb{N}}$ is a chain of $\mathcal{L}$-structures such that $\mathfrak{M}_i \models T$ for all i, then $\bigcup_{i\in\mathbb{N}} \mathfrak{M}_i \models T$.*

(ii) *T may be axiomatzed by $\forall\exists$-sentences.*

(1) Observe that (ii)$\Rightarrow$(i).

(2) Let $\mathfrak{M} \subseteq \mathfrak{N}$. We say that $\mathfrak{M}$ is *1-elementary* in $\mathfrak{N}$ and we write $\mathfrak{M} \preccurlyeq_1 \mathfrak{N}$, if for any existential formula $\varphi(x_1, \dots, x_n)$ and any $\overline{a} \in M^n$ one has $\mathfrak{M} \models \varphi[a_1, \dots, a_n]$ if and only if $\mathfrak{N} \models \varphi[a_1, \dots, a_n]$. (The same is then true for universal formulas as well. Why?)
   Prove that if $\mathfrak{M} \preccurlyeq_1 \mathfrak{N}$, then there is $\mathfrak{M}' \supseteq \mathfrak{N}$ such that $\mathfrak{M} \preccurlyeq \mathfrak{M}'$.

[Hint: Use the Embedding Theorem from Exercise 3.7.10.]

(3) Let T be a theory which is preserved under unions of chains. One sets

$$T_{\forall\exists} = \{\varphi \mid \varphi \text{ is a } \forall\exists\text{-sentence in } \mathcal{L} \text{ such that } T \models \varphi\}.$$

Prove that every model of $T_{\forall\exists}$ admits a 1-elementary extension which is a model of T.

(4) Prove that (i)⇒(ii) and conclude.

(5) Prove that a sentence φ is preserved by unions of chains if and only if it is logically equivalent to a $\forall\exists$-sentence.

Exercise 3.7.12 (Indiscernible Sequences)**.** Let $\mathfrak{M}$ be an $\mathcal{L}$-structure, and let $(I, <)$ be an infinite totally ordered set. The *Ehrenfeucht-Mostowski type* of a sequence $\overline{a} = (a_i)_{i\in I}$ in M is given by $\mathrm{EM}(\overline{a}) = (\mathrm{EM}_n(\overline{a}))_{n\geq 1}$, where for each $n \geq 1$, $\mathrm{EM}_n(\overline{a})$ denotes the set of $\mathcal{L}$-formulas $\varphi(x_1, \dots, x_n)$ with $\mathfrak{M} \models \varphi[a_{i_1}, \dots, a_{i_n}]$ for all $i_1 < \cdots < i_n$ in I. We call $\overline{a}$ *indiscernible* if for any $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$, either $\varphi \in \mathrm{EM}_n(\overline{a})$ or $\neg\varphi \in \mathrm{EM}_n(\overline{a})$, that is, if one has

$$(*) \qquad \mathfrak{M} \models \varphi[a_{i_1}, \dots, a_{i_n}] \text{ if and only if } \mathfrak{M} \models \varphi[a_{j_1}, \dots, a_{j_n}]$$

for all $i_1 < \dots < i_n$ and $j_1 < \dots < j_n$ from I.

Now let $(J, <)$ be an infinite totally ordered set and $\overline{b} = (b_j)_{j\in J}$ an arbitrary sequence in M. Prove that there exists $\mathfrak{N} \succcurlyeq \mathfrak{M}$ containing an indiscernible sequence $(a_i)_{i\in I}$ such that $\mathrm{EM}_n(\overline{a}) \supseteq \mathrm{EM}_n(\overline{b})$ for all integers $n \geq 1$.

[Hint: Use Ramsey's Theorem (cf. Exercise 2.7.1) to prove that for any finite set of formulas Φ, there exists an infinite subset J' of J such that the equivalence $(*)$ holds for all finite subtuples of $\overline{b}$ indexed by increasing sequences of elements in J' and all formulas from Φ.]

10.1090/stml/089/04

Chapter 4

Recursive Functions

Introduction

In this chapter, we will develop a theory of 'computable' functions and sets of natural numbers that will play a fundamental role in the study of incompleteness of Peano arithmetic that will be undertaken in the next chapter. The basic building block of computability is provided by the notion of *primitive recursive functions* which we introduce in 4.1. Unfortunately this notion is too restrictive since, as the example of the Ackermann function shows (4.2), some obviously computable functions do not belong to this class. A satisfactory definition of computable functions is provided by the notion of general recursive functions which is introduced in 4.3.

Another natural candidate for the class of computable functions are the functions which are computable by a Turing machine that we introduce in 4.4. It is a fundamental result that the two notions coincide: a function is recursive if and only if it is Turing computable. One advantage of Turing computability is that it easily yields the existence of *universal* recursive functions that play a major role in the theory.

We conclude this chapter with the study of *recursively enumerable* sets (4.6). These are sets of natural numbers for which there exists an algorithm that enumerates their members. A set is recursive if and only it

is recursively enumerable and its complement is also recursively enumerable. However not all recursively enumerable sets are recursive, which leads to several negative results like the undecidability of the Halting Problem or Rice's Theorem.

4.1. Primitive Recursive Functions

Notation. For $n \in \mathbb{N}$, we set $\mathcal{F}_n := \{f : \mathbb{N}^n \to \mathbb{N}\}$. Moreover, we set $\mathcal{F} := \bigcup_{n\in\mathbb{N}} \mathcal{F}_n$. The function $f \in \mathcal{F}_n$ which to $(x_1, \dots, x_n)$ associates $f(x_1, \dots, x_n) \in \mathbb{N}$ will sometimes be denoted by

$$f = \lambda x_1 \cdots x_n . f(x_1, \dots, x_n).$$

Definition. The set of *primitive recursive* functions is the smallest subset E of $\mathcal{F}$ which satisfies the following properties:

(R0) E contains the following *basic functions*:
- $S = \lambda x.x + 1$ (the *successor function*),
- the 0-ary (constant) function C_0^0 equal to 0, that is, $C_0^0 = \lambda.0$,
- for any $n \in \mathbb{N}^*$ and any $1 \le i \le n$ the projection P_i^n on the ith coordinate, that is, $P_i^n = \lambda x_1 \cdots x_n . x_i$.

(R1) E is stable under *composition*: if $f_1, \dots, f_n \in \mathcal{F}_p \cap E$ and $h \in \mathcal{F}_n \cap E$, then $g = h(f_1, \dots, f_n) \in E$.

(R2) E is stable under *recursion*: if $g \in \mathcal{F}_n \cap E$ and $h \in \mathcal{F}_{n+2} \cap E$, then the function f defined by

$$f(x_1, \dots, x_n, 0) := g(x_1, \dots, x_n),$$
$$f(x_1, \dots, x_n, y+1) := h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y))$$

is also in E.

We observe that the constant functions $C_k^n = \lambda x_1 \cdots x_n . k$ are primitive recursive for any $k, n \in \mathbb{N}$. (Note that the function C_0^1 is obtained by recursion from $g = C_0^0$ and $h = P_2^2$.)

If $X \subseteq \mathbb{N}^n$, its *characteristic function* is denoted by $\mathbb{1}_X$, that is,

$$\mathbb{1}_X(x_1, \dots, x_n) = \begin{cases} 1 & \text{if } (x_1, \dots, x_n) \in X; \\ 0 & \text{else.} \end{cases}$$

Lemma 4.1.1. *The functions $\lambda xy.x+y$, $\lambda xy.x\cdot y$, $\lambda xy.x^y$, $\lambda x.x!$, $\lambda xy.x\dot{-}y$ and $\mathbb{1}_{\mathbb{N}^*}$ are primitive recursive. Here, $x\dot{-}y := x-y$ if $x \geq y$, and $x\dot{-}y := 0$, else.*

Proof. The addition $f = \lambda xy.x+y$ is obtained by recursion from $g = P_1^1$ and $h = S \circ P_3^3$, as $x+0 = x$ and $x+(y+1) = S(x+y)$.

The other functions are easily obtained as well. Let us give the argument for $\lambda xy.x\dot{-}y$ and $\mathbb{1}_{\mathbb{N}^*}$. One first constructs $\lambda y.y\dot{-}1$ by recursion, via $0\dot{-}1 = 0$, $(y+1)\dot{-}1 = y$. One may then define $x\dot{-}0 = x$, $x\dot{-}(y+1) = (x\dot{-}y)\dot{-}1$. Finally, $\mathbb{1}_{\mathbb{N}^*}(x) = 1\dot{-}(1\dot{-}x)$. □

Definition. A subset X of $\mathbb{N}^n$ is called *primitive recursive* if its characteristic function $\mathbb{1}_X$ is primitive recursive.

Lemma 4.1.2.

(1) *The set of primitive recursive functions is stable under a permutation of variables.*

(2) *If $X \subseteq \mathbb{N}^n$ is primitive recursive and if $f_1, \dots, f_n \in \mathcal{F}_p$ are primitive recursive, then the set*

$$Y = \{(x_1, \dots, x_p) \in \mathbb{N}^p \mid (f_1(\overline{x}), \dots, f_n(\overline{x})) \in X\}$$

is primitive recursive.

(3) *The set of primitive recursive subsets of $\mathbb{N}^n$ contains $\emptyset$ and $\mathbb{N}^n$, and it is stable under $\cup$, $\cap$ and passage to the complement (so under boolean combinations).*

(4) *The set $\{(x,y) \mid x < y\} \subseteq \mathbb{N}^2$ is primitive recursive.*

(5) (*Definition by cases.*) *Let $\mathbb{N}^n = A_1 \dot{\cup} \dots \dot{\cup} A_k$ be a partition of $\mathbb{N}^n$ into finitely many primitive recursive sets A_i, and let $f_1, \dots, f_k \in \mathcal{F}_n$ be primitive recursive. Then the function f, defined by $f(\overline{x}) = f_i(\overline{x})$ if $\overline{x} \in A_i$, is primitive recursive. In particular, the functions $\lambda x_1 \cdots x_n.\max(x_i)$ and $\lambda x_1 \cdots x_n.\min(x_i)$ are primitive recursive.*

(6) (*Bounded sums and products.*) *If $f \in \mathcal{F}_{n+1}$ is primitive recursive, so are the following functions:*

$$\lambda x_1 \cdots x_n y. \sum_{t=0}^{y} f(\overline{x}, t) \text{ and } \lambda x_1 \cdots x_n y. \prod_{t=0}^{y} f(\overline{x}, t).$$

(7) (*Bounded μ-operator.*) *Let $X \subseteq \mathbb{N}^{n+1}$ be primitive recursive. Then $f \in \mathcal{F}_{n+1}$, $f(\overline{x}, z) = (\mu t \leq z)\big((\overline{x}, t) \in X\big)$, defined by*

$$f(\overline{x}, z) := \begin{cases} 0 & \text{if there is no } t \leq z \text{ with } (\overline{x}, t) \in X; \\ t_0 & \text{if } t_0 \text{ is the smallest natural number} \\ & t \leq z \text{ such that } (\overline{x}, t) \in X \end{cases}$$

is a primitive recursive function.

(8) (*Bounded quantification.*) *If $X \subseteq \mathbb{N}^{n+1}$ is a primitive recursive set, so are the sets*

$$X_e = \{(x_1, \dots, x_n, z) \in \mathbb{N}^{n+1} \mid (\exists t \leq z)\,(\overline{x}, t) \in X\} \text{ and}$$
$$X_a = \{(x_1, \dots, x_n, z) \in \mathbb{N}^{n+1} \mid (\forall t \leq z)\,(\overline{x}, t) \in X\}.$$

Proof. Part (1) is clear, and (2) follows from $\mathbb{1}_Y = \mathbb{1}_X(f_1, \dots, f_n)$.

(3) One has $\mathbb{1}_{\mathbb{N}^n \setminus X} = 1 \dot{-} \mathbb{1}_X$ and $\mathbb{1}_{X \cap Y} = \mathbb{1}_X \cdot \mathbb{1}_Y$.

(4) One has $\mathbb{1}_<(x, y) = \mathbb{1}_{\mathbb{N}^*}(y \dot{-} x)$.

(5) One has $f = \mathbb{1}_{A_1} f_1 + \dots + \mathbb{1}_{A_k} f_k$.

(6) is proved by recursion.

(7) Given $X \subseteq \mathbb{N}^{n+1}$, one has $f(\overline{x}, 0) = 0$,

$$f(\overline{x}, z+1) = \begin{cases} f(\overline{x}, z) & \text{if } \sum_{t=0}^{z} \mathbb{1}_X(\overline{x}, t) \geq 1; \\ z+1 & \text{if } \sum_{t=0}^{z} \mathbb{1}_X(\overline{x}, t) = 0 \text{ and } (\overline{x}, z+1) \in X; \\ 0 & \text{else.} \end{cases}$$

Thus f is primitive recursive (by recursion and definition by cases).

(8) Passing to the complement, it is enough to treat the first case. One has $\mathbb{1}_{X_e}(\overline{x}, z) = 1$ if $\sum_{t=0}^{z} \mathbb{1}_X(\overline{x}, t) \geq 1$, and $\mathbb{1}_{X_e}(\overline{x}, z) = 0$, else. □

Example 4.1.3.

(1) Let $q : \mathbb{N}^2 \to \mathbb{N}$ be the function which to (x, y) associates the integer part of x/y if $y \neq 0$, and 0 else. Then q is primitive recursive. [Indeed, $q(x, y) = (\mu t \leq x)((t + 1) \cdot y > x)$.]

(2) $\{(x, y) \in \mathbb{N}^2 : y \mid x\}$ is a primitive recursive set. [Indeed, one has $y \mid x \iff \exists z z \cdot y = x \iff x = q(x, y) \cdot y$.]

(3) The set P of prime numbers is primitive recursive. [Indeed, $x \in P \iff x \geq 2 \wedge (\forall y \leq x)\ (y \mid x \to (y = 1 \vee y = x))$. By the closure properties stated in Lemma 4.1.2, P is thus primitive recursive.]

(4) The function π, which to x associates the $(x+1)$th prime number, is primitive recursive. [Indeed, one has $\pi(0) = 2$, $\pi(x + 1) = (\mu z \leq \pi(x)! + 1)\,(z > \pi(x) \wedge z \in P)$.]

(5) A primitive recursive bijection between $\mathbb{N}^2$ and $\mathbb{N}$ is given by the function $\alpha_2 = \lambda xy.\frac{1}{2}(x + y + 1)(x + y) + x$. Moreover, there are primitive recursive functions $\beta_1^2, \beta_2^2 \in \mathcal{F}_1$ such that $\alpha_2(\beta_1^2, \beta_2^2) = \mathrm{id}_{\mathbb{N}}$. [Indeed, as $\alpha_2(x, y) \geq \min(x, y)$, one has $\beta_1^2(x) = (\mu z \leq x)(\exists t \leq x)(\alpha_2(z, t) = x))$, and similarly for the function β_2^2.]

By induction on $p \geq 2$, one defines a primitive recursive bijection $\alpha_p : \mathbb{N}^p \to \mathbb{N}$ whose inverse has primitive recursive components $\beta_1^p, \ldots, \beta_p^p$. For this, it suffices to set $\alpha_{p+1}(x_1, \ldots, x_{p+1}) = \alpha_p(x_1, \ldots, x_{p-1}, \alpha_2(x_p, x_{p+1}))$.

If $(x_0, \ldots, x_{n-1})$ is a finite sequence of natural numbers, we define its *Gödel number* as

$$\langle x_0, \ldots, x_{n-1} \rangle := \pi(0)^{x_0} \cdot \ldots \cdot \pi(n-2)^{x_{n-2}} \cdot \pi(n-1)^{x_{n-1}+1} - 1.$$

Lemma 4.1.4. *The map $\langle\ \rangle$ defines a bijection between the set of finite sequences of natural numbers and the set of natural numbers $\mathbb{N}$. It satisfies the following properties:*

(1) *The binary* component *function $(x)_i$, defined by*

$$(\langle x_0, \ldots, x_{n-1} \rangle)_i = \begin{cases} x_i & \text{if } i < n, \\ 0 & \text{else,} \end{cases}$$

is primitve recursive.

(2) *The* length *function, given by* $\lg(\langle x_0, \dots, x_{n-1}\rangle) = n$, *is primitive recursive.*

(3) *For any* $n \in \mathbb{N}$, $\langle\ \rangle \restriction_{\mathbb{N}^n} : \mathbb{N}^n \to \mathbb{N}$ *is primitive recursive.*

(4) $\lg(x) \leq x$ *for any* x, *and if* $x > 0$, *then* $(x)_i < x$ *for any* i.

Proof. Part (4) is clear, and (3) follows from Example 4.1.3.

(2) One has $\lg(x) = (\mu y \leq x)\,[(\forall z \leq x)\,(y \leq z \to \pi(z) \nmid (x+1))]$ if $x > 0$ and $\lg(0) = 0$, so lg is primitive recursive by Lemma 4.1.2.

(1) The description

$$(x)_i = \begin{cases} 0 & \text{if } i \geq \lg(x), \\ (\mu y \leq x)\,(\pi(i)^{y+2} \nmid (x+1)) & \text{if } i+1 = \lg(x), \\ (\mu y \leq x)\,(\pi(i)^{y+1} \nmid (x+1)) & \text{if } i+1 < \lg(x) \end{cases}$$

of the component function yields its primitive recursiveness. □

4.2. The Ackermann Function

We now define the *Ackermann function* $\xi \in \mathcal{F}_2$, a function which is computable in the intuitive sense but which turns out to be non-primitive recursive:

- $\xi(0, x) := 2^x$,
- $\xi(y, 0) := 1$,
- $\xi(y+1, x+1) := \xi(y, \xi(y+1, x))$.

This function is well-defined and may be computed in a finite number of steps (exercise; it suffices to consider the lexicographic order on $\mathbb{N}^2$).

We will also write $\xi_n(x)$ for $\xi(n, x)$, and ξ_n^k for $\underbrace{\xi_n \circ \dots \circ \xi_n}_{k \text{ times}}$.

Lemma 4.2.1.

(1) $\xi_n(x) > x$ *for all* $n, x \in \mathbb{N}$.

(2) ξ_n *is strictly increasing for all* $n \in \mathbb{N}$.

(3) $\xi_{n+1}(x) \geq \xi_n(x)$ *for all* $n, x \in \mathbb{N}$.

(4) ξ_n^k *is strictly increasing for all* $k, n \in \mathbb{N}$.

(5) $\xi_n^k(x) < \xi_n^{k+1}(x)$ *for all* $k, n, x \in \mathbb{N}$.

(6) $\xi_m^k(x) \leq \xi_n^k(x)$ *for all* $k, m, n, x \in \mathbb{N}$ *with* $m \leq n$.

(7) $\xi_n^k(x) \leq \xi_{n+1}(x+k)$ *for all* $k, n, x \in \mathbb{N}$.

Proof. We prove (1) and (2) simultaneously by induction on n. The case $n = 0$ is clear. Suppose now that (1) and (2) hold for n. By the induction hypothesis, one has $\xi_{n+1}(x+1) = \xi_n(\xi_{n+1}(x)) > \xi_{n+1}(x)$, showing that (2) holds for $n+1$. As $\xi_{n+1}(0) = 1$ by definition, (1) follows from (2).

(3) $\xi_{n+1}(0) = \xi_n(0)$, and $\xi_{n+1}(x+1) = \xi_n(\underbrace{\xi_{n+1}(x)}_{\geq x+1}) \geq \xi_n(x+1)$ by (1) and (2).

(4), (5) and (6) are clear.

(7) This is proved by induction on k, the case $k = 0$ being clear. Now suppose that the result holds for k. Using (3), one then has $\xi_n^{k+1}(x) = \xi_n(\xi_n^k(x)) \leq \xi_n(\xi_{n+1}(x+k)) = \xi_{n+1}(x+k+1)$. □

Definition. We say that a function $f \in \mathcal{F}_1$ *dominates* the function $g \in \mathcal{F}_n$ if there exists $N \in \mathbb{N}$ such that for all $\overline{x} \in \mathbb{N}^n$ one has $g(\overline{x}) \leq f(\max(x_1, \ldots, x_n, N))$.

Note that if f is strictly increasing, then f dominates g if and only if $g(\overline{x}) \leq f(\max(x_1, \ldots, x_n))$ except for a finite number of n-tuples.

We denote by $\mathcal{C}_n$ the set of functions in $\mathcal{F}$ which are dominated by at least one of the functions ξ_n^k, where $k \in \mathbb{N}$.

Lemma 4.2.2.

(1) $\mathcal{C}_n \subseteq \mathcal{C}_m$ *for any* $n \leq m$.

(2) $\mathcal{C}_0$ *contains the basic functions* $(S, C_0^0$ *and all the projections* $P_i^n)$ *as well as the functions* $\lambda xy.x + y$, $\lambda x.k \cdot x$ *(for fixed* k*) and* $\lambda x_1 \ldots x_n.\max(x_1, \ldots, x_n)$.

(3) $\mathcal{C}_n$ *is stable under composition.*

(4) *If* $g \in \mathcal{F}_p \cap \mathcal{C}_n$ *and* $h \in \mathcal{F}_{p+2} \cap \mathcal{C}_n$*, then the function* f *defined by recursion from* g *and* h *is in* $\mathcal{C}_{n+1}$.

In particular, the set $\mathcal{C} = \bigcup_{n \in \mathbb{N}} \mathcal{C}_n$ *contains all primitive recursive functions.*

Proof. (1) and (2) are clear.

(3) Suppose that $f_1, \dots, f_m \in \mathcal{F}_p \cap \mathcal{C}_n$ and $g \in \mathcal{F}_m \cap \mathcal{C}_n$ are given. There exist natural numbers $N, N_1, \dots, N_m, k, k_1, \dots, k_m$ such that $g(\overline{y}) \leq \xi_n^k(\max(y_1, \dots, y_m, N))$ for every $\overline{y} \in \mathbb{N}^m$ and, for any $i \in \{1, \dots, m\}$ and $\overline{x} \in \mathbb{N}^p$, $f_i(\overline{x}) \leq \xi_n^{k_i}(\max(x_1, \dots, x_p, N_i))$. Set $M = \max(N, N_1, \dots, N_m)$ and $l = \max(k_1, \dots, k_m)$. Now let $\overline{x} \in \mathbb{N}^p$. Setting $M_{\overline{x}} := \max(x_1, \dots, x_p, M)$, one then has

$$g(f_1(\overline{x}), \dots, f_m(\overline{x})) \leq \xi_n^k(\xi_n^l(M_{\overline{x}})) = \xi_n^{k+l}(M_{\overline{x}}).$$

(4) By definition of the recursion, one has $f(\overline{x}, 0) = g(\overline{x})$ and $f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$. By assumption, there exist natural numbers k_1, N_1, k_2, N_2 such that $g(\overline{x}) \leq \xi_n^{k_1}(\max(x_1, \dots, x_p, N_1))$ and $h(\overline{x}, y, t) \leq \xi_n^{k_2}(\max(x_1, \dots, x_p, y, t, N_2))$. Using induction on y, one easily obtains that

$$(*) \qquad f(\overline{x}, y) \leq \xi_n^{k_1 + yk_2}(\max(x_1, \dots, x_p, y, N_1, N_2)).$$

Applying Lemma 4.2.1(7), one deduces from $(*)$ that

$$f(\overline{x}, y) \leq \underbrace{\xi_{n+1}(\max(x_1, \dots, x_p, y, N_1, N_2) + k_1 + k_2 y)}_{\text{a composition of functions in } \mathcal{C}_{n+1}},$$

whence the result by (3). □

Theorem 4.2.3. *The Ackermann function is not primitive recursive.*

Proof. Suppose, for contradiction, that ξ is primitive recursive. Then $\lambda x.\xi(x, 2x)$ is primitive recursive, too, and so, by Lemma 4.2.2, there exist $k, n, N \in \mathbb{N}$ such that $\xi(x, 2x) \leq \xi_n^k(x)$ for all $x > N$. By Lemma 4.2.1(7) it follows that $\xi_x(2x) \leq \xi_{n+1}(x + k)$ for all $x > N$. For $x > \max(k, n+1)$, this is a contradiction. □

Remark. An easy induction on n shows that all the functions ξ_n are primitive recursive.

4.3. Partial Recursive Functions

The existence of the Ackermann function — computable in the intuitive sense but not primitive recursive — shows that we ought to enlarge the

class of functions we are considering. For technical reasons it is moreover convenient to pass to partial functions.

By definition, a *partial function* from $\mathbb{N}^n$ to $\mathbb{N}$ is a pair (A, f), with $A \subseteq \mathbb{N}^n$ and $f : A \to \mathbb{N}$. The set A is called the *domain* (of definition) of f and denoted by $\mathrm{dom}(f)$. We write $\mathcal{F}_n^*$ for the set of such pairs, and $\mathcal{F}^* = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n^*$. Most of the time, we will write f instead of (A, f).

Definition. The set of *partial recursive functions* is the smallest subset E of $\mathcal{F}^*$ which satisfies the following properties (R0)*-(R3)*:

(R0)* E contains the basic functions (S, C_0^0 and all the projections P_i^n).

(R1)* E is stable under composition (of partial functions): Given partial functions $f_1, \dots, f_n \in \mathcal{F}_m^* \cap E$ and $h \in \mathcal{F}_n^* \cap E$, then $g = h(f_1, \dots, f_n) \in E$, where g is the partial function which to $\overline{x}$ assigns $h(f_1(\overline{x}), \dots, f_n(\overline{x}))$ if $\overline{x} \in \mathrm{dom}(f_i)$ for all i and $(f_1(\overline{x}), \dots, f_n(\overline{x})) \in \mathrm{dom}(h)$. Otherwise, g is not defined for $\overline{x}$.

(R2)* E is stable under recursion (of partial functions): Given $g \in \mathcal{F}_p^* \cap E$ and $h \in \mathcal{F}_{p+2}^* \cap E$, then $f \in E$, where
- $f(\overline{x}, 0) = g(\overline{x})$ if $\overline{x} \in \mathrm{dom}(g)$, and otherwise f is not defined for $(\overline{x}, 0)$;
- $f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$ if f is defined for $(\overline{x}, y)$ (this property is defined simultaneously by recursion on y) and if $(\overline{x}, y, f(\overline{x}, y)) \in \mathrm{dom}(h)$, and otherwise f is not defined for $(\overline{x}, y+1)$.

(R3)* E is stable under the *μ-operator*: Given $f \in \mathcal{F}_{n+1}^* \cap E$, then $g \in E$, where $g \in \mathcal{F}_n^*, g(\overline{x}) = \mu y\big(f(\overline{x}, y) = 0\big)$ is the partial function defined as follows:
- if there is z such that $f(\overline{x}, z) = 0$ and $(\overline{x}, z') \in \mathrm{dom}(f)$ for all $z' \leq z$, then $g(\overline{x})$ is the minimal such z;
- otherwise, g is not defined for $\overline{x}$.

A partial function $f \in \mathcal{F}_n^*$ is *total* if $\mathrm{dom}(f) = \mathbb{N}^n$. A (*total*) *recursive function* is a total function which is partial recursive.

The following operation is reserved for total functions.

Let $f \in \mathcal{F}_{n+1}$ be a total function. Assume that f satisfies

$$\forall x_1, \dots, x_n \exists y f(\overline{x}, y) = 0.$$

Then we say that the (total) function $g = \lambda \overline{x}.\mu y \big(f(\overline{x}, y) = 0\big)$ is obtained from f by the *total μ-operator*.

We say that a set of total functions satisfies property (R3) if it is stable under the total μ-operator.

Exercise 4.3.1. Prove that the Ackermann function is recursive. (See also Proposition 4.5.4.)

4.4. Turing Computable Functions

Turing machines provide a way to make precise the notion of a function which is 'computable by a machine'.

Definition. A *Turing machine* $\mathcal{M}$ is given by the following data:

- A finite number (≥ 1) of *tapes* $B_1, B_2, \dots$ placed horizontally, each bounded on the left and unbounded on the right; each tape is divided into squares which are numbered by $\mathbb{N}^*$ from left to right. The tapes are arranged in such a way that the squares with the same number lie on the same vertical line.
- A *read-write head* which may read, erase and write symbols on the tape squares (one symbol per square). The head moves horizontally and is placed, at any moment, over one vertical column, and it manipulates all squares of this column simultaneously.

  The set of symbols is given by $S = \{\$, |, b\}$ (b is called the *blank* symbol).

Here are the data which are specific to $\mathcal{M}$:

- $n = n(\mathcal{M}) \in \mathbb{N}^*$ (the number of tapes).
- A finite set Q of *states*. There are two (distinct) distinguished states in Q: q_i (the *initial* state) and q_f (the *final* state).
- A function $M : S^n \times Q \to S^n \times Q \times \{-1, 0, 1\}$, the *transition function* of $\mathcal{M}$.

A description of the way the machine $\mathcal{M}$ operates:

- At every instant (point in time) $t \in \mathbb{N}$, $\mathcal{M}$ is in one of the states from Q.
- $\mathcal{M}$ operates at every instant by changing states, erasing and writing symbols on the tapes and moving its head.

The way $\mathcal{M}$ operates is subject to the following rules:

(1) At the instant $t = 0$, $\mathcal{M}$ is in the initial state, and its head is placed over the squares number 1.

(2) At every instant t, $\mathcal{M}$ reads the symbols $(s_1, \dots, s_n) \in S^n$ written in front of its head, and the transition function M describes what $\mathcal{M}$ is supposed to do. If $\mathcal{M}$ is in state q and reads $(s_1, \dots, s_n)$, and if $M(\overline{s}, q) = (\overline{s'}, q', \varepsilon)$, then the head erases $\overline{s}$, writes $\overline{s'}$, moves by ε horizontally, and $\mathcal{M}$ changes its state to q', then passes to the instant $t + 1$.

(3) $\mathcal{M}$ stops to operate if it attains the final state.

Correct input:

- At the instant $t = 0$, \$ is written in the tape squares number 1, and only there.
- On each square a symbol from S is written, and only finitely many symbols are non-blank.

(These conditions then remain satisfied during the whole computation).

Constraints:

- For any $\overline{s} \in S^n$, one has $M(\overline{s}, e_f) = (\overline{s}, e_f, 0)$.
- The head cannot erase the symbol \$ (which marks the beginning of the tape) or overwrite a symbol different from \$ with \$:
  - For any $q \in Q$, $M((\$, \dots, \$), q) = ((\$, \dots, \$), q', \varepsilon)$ for some $\varepsilon \in \{0, 1\}$;
  - if $\overline{s} \neq (\$, \dots, \$)$, then $M(\overline{s}, q) = (\overline{s'}, q', \varepsilon)$ with $s'_i \neq \$$ for all i.

Remark. A Turing machine is *deterministic*, that is, every step in the computation follows in a unique way from the preceding one, and one

may thus predict for every instant t the position of the head, the state of the machine and the content of the tape squares.

Definition.

(1) A tape *represents* (at a given instant) the natural number m if what is written on it equals $(\$, \underbrace{|, \dots, |}_{m \text{ times}}, b, \dots, b, \dots)$.

(2) A Turing machine $\mathcal{M}$ *computes* $f \in \mathcal{F}_p^*$ if $n(\mathcal{M}) \geq p+1$ and if for all $\overline{m} \in \mathbb{N}^p$, when $\mathcal{M}$ starts operating with the input where for $i = 1, \dots, p$, the tape B_i represents m_i and, for $i > p$, the tape B_i represents 0, then
   - if $\overline{m} \in \mathrm{dom}(f)$, then $\mathcal{M}$ stops after some finite time, and its tapes successively represent the natural numbers $(m_1, \dots, m_p, f(\overline{m}), 0, \dots, 0)$ (in this order);
   - if $\overline{m} \notin \mathrm{dom}(f)$, $\mathcal{M}$ either never stops, that is, q_f is never attained, or $\mathcal{M}$ stops after some finite time, but when it stops there is no $n \in \mathbb{N}$ such that the tapes of the machine $\mathcal{M}$ successively represent the natural numbers $(m_1, \dots, m_p, n, 0, \dots, 0)$.

(3) The partial function f is *Turing computable* if there is a Turing machine $\mathcal{M}$ which computes f.

Remarks.

(1) There are many variants of the model of a Turing machine (one may for example work with tapes which are unbounded on the left and on the right), all leading to the same notion of Turing computability.

(2) Using unary code to represent natural numbers is of course very inefficient, but it suffices for our purposes, since we are not concerned with practical feasibility or complexity issues in this book.

Lemma 4.4.1. *The basic functions (S, C_0^0 and the projections P_i^n) are Turing computable.*

Proof. C_0^0 is computed by a Turing machine $\mathcal{M}$ with one tape, a set of states $Q = \{q_i, q_f\}$, and with a transition function $M(\$, q_i) = (\$, q_f, 0)$.

(Here, and in what follows, we only give the relevant part of the transition function M.)

P_i^n is computed by $\mathcal{M}$ with $n+1$ tapes, a set of states $Q = \{q_i, q_f\}$, and with a transition function $M(\$, \dots, \$, q_i) = (\$, \dots, \$, q_i, +1)$ and

$$M(s_1, \dots, s_n, b, q_i) = \begin{cases} (s_1, \dots, s_n, |, e_i, +1) & \text{if } s_i = |, \\ (s_1, \dots, s_n, b, q_f, 0) & \text{if } s_i = b. \end{cases}$$

The successor function S is computed by a Turing machine $\mathcal{M}$ with two tapes, a set of states $Q = \{q_i, q_f\}$, and with a transition function $M(\$, \$, q_i) = (\$, \$, q_i, +1), M(|, b, q_i) = (|, |, q_i, +1)$ and finally $M(b, b, q_i) = (b, |, q_f, 0)$. □

Lemma 4.4.2. *The set of partial Turing computable functions is stable under composition.*

Proof. Let $f_1, \dots, f_n \in \mathcal{F}_p^*$ and $g \in \mathcal{F}_n^*$ be Turing computable, and let $h = g(f_1, \dots, f_n)$.

By assumption there exist $\mathcal{M}_i$, $1 \leq i \leq n$, where $\mathcal{M}_i$ is a Turing machine with $p_i \geq p+1$ tapes and a set of states Q_i which computes f_i, as well as a Turing machine $\mathcal{M}'$ with $n' \geq n+1$ tapes and a set of states Q' which computes g.

Let $\mathcal{M}$ be a Turing machine with $p+(n'-n)+\sum_{i=1}^n (p_i - p)$ tapes and a set of states $Q = \{q_d, q_c\} \dot{\cup} Q' \dot{\cup} \dot{\bigcup}_i Q_i$. The initial state of $\mathcal{M}$ corresponds to that of $\mathcal{M}_1$, and its final state to that of $\mathcal{M}'$.

The machine $\mathcal{M}$ operates as follows (the precise description of the transitifion function of $\mathcal{M}$ is left as an exercise):

If $(m_1, \dots, m_p, 0, \dots, 0)$ are represented on the tapes, $\mathcal{M}$ starts to compute $f_1(m_1, \dots, m_p)$ as $\mathcal{M}_1$ would do, using the states in $Q_1 \setminus \{q_f^1\}$ and $(p_1 - p)$ auxiliary tapes (all different from B_{p+1}). In state q_f^1, it returns to the beginning of the tapes, then passes to state $q_i^2 \in Q_2$ and computes $f_2(\overline{m})$, using the states in $Q_2 \setminus \{q_f^2\}$ and $(p_2 - p)$ auxiliary tapes (all different from B_{p+1} and from the previous auxiliary tapes). In this way, $\mathcal{M}$ successively computes $f_1(\overline{m}), \dots, f_n(\overline{m})$. Once $f_n(\overline{m})$ has been computed, $\mathcal{M}$ passes to the initial state of $\mathcal{M}'$ and computes $h(f_1(\overline{m}), \dots, f_n(\overline{m}))$ as $\mathcal{M}'$ would do, using Q' and $n'-n$ auxiliary tapes (distinct from B_{p+1}). For

this computation, it uses the tapes on which are represented the $f_i(\overline{m})$ as input tapes and B_{p+1} as an output tape. Renumbering the tapes, the transition function of $\mathcal{M}$ may thus be established using the transition functions of $\mathcal{M}_1$,...,$\mathcal{M}_n$ and $\mathcal{M}'$.

Once $h(f_1(\overline{m}), \dots, f_n(\overline{m}))$ is computed, instead of passing to the final state of $\mathcal{M}'$, $\mathcal{M}$ passes to state q_d which serves to move its head to the beginning of the tapes. Then, in state q_c, it 'clears' the tapes on which are represented the $f_i(\overline{m})$, and finally it passes to the final state. □

Lemma 4.4.3. *The set of partial Turing computable functions is stable under the μ-operator.*

Proof. The easy proof is left as an exercise. □

Lemma 4.4.4. *The set of partial Turing computable functions is stable under recursion.*

Proof. Suppose that $g \in \mathcal{F}_p^*$ is computed by the Turing machine $\mathcal{M}$ with $p+1+k$ tapes and a set of states Q, and that $h \in \mathcal{F}_{p+2}^*$ is computed by $\mathcal{M}'$ with $p+3+k'$ tapes and a set of states Q'. Let $f \in \mathcal{F}_{p+1}^*$ be the partial function defined by recursion from g and h, that is, $f(\overline{x}, 0) = g(\overline{x})$ and $f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$.

We now give an informal description of a Turing machine $\mathcal{N}$ which computes f: $\mathcal{N}$ has $p+4+k+k'$ tapes, and its set of states is given by $Q \dot{\cup} Q'$ plus a couple of auxiliary states, with $q_i^{\mathcal{N}} = q_i^{\mathcal{M}}$ and $q_f^{\mathcal{N}} = q_f^{\mathcal{M}'}$.

On input $(m_1, \dots, m_{p+1})$, $\mathcal{N}$ operates as follows:

(1) Compute $g(m_1, \dots, m_p)$ with input tapes $B_1, \dots, B_p$, an output tape B_{p+2} and auxiliary tapes $B_{p+5}, \dots, B_{p+4+k}$, operating as $\mathcal{M}$ would do, up to renumbering the tapes.

(2) Compare m_{p+1} and the natural number y which is represented on B_{p+3} (note that during the whole computation, B_{p+3} will represent a natural number $\leq m_{p+1}$):
- if $m_{p+1} = y$, then go to step (5);
- if $m_{p+1} > y$, then go to step (3).

(3) Compute $h(m_1, \dots, m_p, y, f(\overline{x}, y)) = f(\overline{x}, y+1)$ as $\mathcal{M}'$ would do, with input tapes $B_1, \dots, B_p, B_{p+3}, B_{p+2}$, an output tape B_{p+4} and the last k' tapes as auxiliary tapes.

(4) Copy the content of B_{p+4} onto tape B_{p+2}, then clear tape B_{p+4} and increment the content of B_{p+3} by one, that is, pass from y to $y+1$. Then go back to step (2).

(5) Clear tape B_{p+3} and stop. □

Theorem 4.4.5. *Every partial recursive function is Turing computable.*

Proof. It is enough to combine the four preceding lemmas. □

In order to establish the converse of Theorem 4.4.5, we ought to code Turing machines and the way they operate.

Coding of Turing machines. We identify the set $S = \{b, \$, |\}$ with $\{0,1,2\}$, via $0 \leftrightarrow b$, $1 \leftrightarrow \$$ and $2 \leftrightarrow |$. We code a sequence $(s_i)_{i\leq n}$ of symbols in S, or a sequence $(s_i)_{i\in\mathbb{N}}$ with $s_i = 0$ for almost all i, by $\Gamma((s_i)) = \sum_{i\geq 0} s_i 3^i \in \mathbb{N}$.

Let $\mathcal{M}$ be a Turing machine. Then $\mathcal{M}$ is given by:

- $n = n(\mathcal{M}) \geq 1$, the number of tapes of $\mathcal{M}$.
- The set of states Q. We will suppose that $Q = \{0, \dots, m\}$ (thus, $m \geq 1$ equals $\mathrm{card}(Q) - 1$), with $q_i = 0$ and $q_f = 1$.
- The transition function $M : S^n \times Q \to S^n \times Q \times \{-1, 0, 1\}$.

To code the transition function M, if $\rho = (s_1, \dots, s_n, q) \in S^n \times Q$ and $M(\rho) = (t_1, \dots, t_n, q', \varepsilon)$, we set

$$r_1(\rho) = \alpha_2(\Gamma(s_1, \dots, s_n), q)$$

and

$$r_2(\rho) = \alpha_3(\Gamma(t_1, \dots, t_n), q', \varepsilon + 1),$$

and then

$$\ulcorner M \urcorner = \prod_{\rho \in S^n \times Q} \pi(r_1(\rho))^{r_2(\rho)}.$$

To decode, we will use the following function $\delta \in \mathcal{F}_2$, defined by $\delta(i,x) := (\mu z \leq x)\left(\pi(i)^{z+1} \nmid x\right)$. We then have

$$\delta(\alpha_2(\Gamma(s_1, \dots, s_n), q), \ulcorner M \urcorner) = \alpha_3(\Gamma(t_1, \dots, t_n), q', \varepsilon + 1).$$

Finally, we define the *index* of $\mathcal{M}$ as $\ulcorner \mathcal{M} \urcorner = \alpha_3(n, m, \ulcorner M \urcorner)$.

Lemma 4.4.6. *For any $p \geq 0$, the set*

$$I_p = \{\ulcorner \mathcal{M} \urcorner \mid \mathcal{M} \text{ is a Turing machine with at least } p+1 \text{ tapes}\}$$

is primitive recursive.

Proof. It is easy to see that one may recognize in a primitive recursive way if the constraints on the transition function are met. The details are left as an exercise. □

A *configuration* $C = C(t)$ of $\mathcal{M}$ (at an instant t) is a sequence $(s_i)_i \in S^{\mathbb{N}}$ such that s_{nv+w} equals the symbol which is written on the $(v+1)$th square of tape B_{w+1}. (We suppose that there is only a finite number of non-blank symbols and that \$ is written at the beginning of the tapes and only there.)

We code the configuration C by $\Gamma(C) := \Gamma((s_i))$. To decode, we will use the function

$$\eta(\Gamma(C), u, v, n) = r\left(q(\Gamma(C), 3^{n(u \dot{-} 1)+(v \dot{-} 1)}), 3\right)$$

(here, q denotes the result of the division with remainder, and r denotes the remainder), which gives the symbol s which is written on the uth square of tape B_v. If $\sigma = (s_1, \ldots, s_n)$ is the sequence of symbols written on the squares of number u, then $\Gamma(\sigma) = \varepsilon(\Gamma(C), u, n)$, where $\varepsilon(x, y, z) = r\left(q(x, 3^{z(y \dot{-} 1)}), 3^z\right)$.

The *situation* $\mathrm{Sit} = \mathrm{Sit}(t)$ *of* $\mathcal{M}$ (at an instant t) is given by $(q, k, C(t))$, where q denotes the state of $\mathcal{M}$ at the instant t, k the number of squares in front of which is placed the head at the instant t and $C(t)$ the configuration at the instant t. We code the situation via $\Gamma(\mathrm{Sit}(t)) = \alpha_3(q, k, \Gamma(C(t)))$.

Lemma 4.4.7. *Let $p \geq 0$. There exists a primitive recursive function $g^p \in \mathcal{F}_2$ such that the following properties hold:*

- *$g^p(i, x) = 0$ if $i \notin I_p$;*
- *if $i = \ulcorner \mathcal{M} \urcorner$ and x is the code of the situation of $\mathcal{M}$ at the instant t, then $g^p(i, x)$ is the code of the situation of $\mathcal{M}$ at the instant $t+1$.*

Proof. We suppose that $i = \ulcorner \mathcal{M} \urcorner \in I_p$. Then

- the current state of $\mathcal{M}$ is $\beta_1^3(x) = q$,

- the number of squares which are currently observed is $\beta_2^3(x) = k$,
- the code of the current configuration $C(t)$ of the machine $\mathcal{M}$ is $\beta_3^3(x) = \Gamma(C(t))$,
- the number of tapes of $\mathcal{M}$ is given by $\beta_1^3(i) = n$,
- the number of states of $\mathcal{M}$ minus 1 is given by $\beta_2^3(i) = m$,
- the code of the transition function is given by $\beta_3^3(i) = \ulcorner M \urcorner$,
- the code of the sequence of symbols read by the head at the instant t is given by

$$\varepsilon\left(\Gamma(C(t)), k, n\right) = \varepsilon\left(\beta_3^3(x), \beta_2^3(x), \beta_1^3(i)\right) =: c.$$

If x is not the code of a situation, we set $g^p(i, x) = 0$. This is the case if $\beta_1^3(x) > m$ or $\beta_2^3(x) = 0$ or if $\beta_3^3(x)$ is not the code of a configuration with \$ at the beginning of the tapes and only there (the last condition may be expressed in a primitive recursive way, using the functions ε and η).

Otherwise, let $\delta := \delta\left(\alpha_2(c, q), \ulcorner M \urcorner\right)$. Then $c' = \beta_1^3(\delta)$ is the code of the sequence of symbols written in the place where was previously written the sequence coded by c. We may set $g^p(i, x) = \alpha_3\left(q', k', \Gamma(C')\right)$, where

$$\Gamma(C') = \left(\Gamma(C) + 3^{n(k \dot{-} 1)} \cdot c'\right) \dot{-} \left(3^{n(k \dot{-} 1)} \cdot c\right)$$

is the code of the configuration of the machine $\mathcal{M}$ at the instant $t + 1$, $q' = \beta_2^3(\delta)$ is the state of $\mathcal{M}$, and where $k' = \left(\beta_2^3(x) + \beta_3^3(\delta)\right) \dot{-} 1$ is the number of squares which are observed by the head of $\mathcal{M}$ at the instant $t + 1$. □

One defines a function $\mathrm{ST}^p \in \mathcal{F}_{p+2}$ as follows:

- $\mathrm{ST}^p(i, t, \overline{x}) = 0$, if $i \notin I_p$;
- otherwise, $\mathrm{ST}^p(i, t, \overline{x})$ is the code $\Gamma(\mathrm{Sit}(t))$ of the situation at the instant t of the machine $\mathcal{M}$ of index i which has started to operate at the instant $t = 0$ with the following configuration: on $B_1, \ldots, B_p$ are represented the natural numbers $x_1, \ldots, x_p$, and the other tapes represent 0.

Theorem 4.4.8. *The function* ST^p *is primitive recursive for any* $p \geq 0$.

Proof. The function $\lambda i\overline{x}.\mathrm{ST}^p(i,0,\overline{x})$ is primitive recursive. (This is easy to see and is left as an exercise.)

Moreover, one has $\mathrm{ST}^p(i,t+1,\overline{x}) = g^p\left(i,\mathrm{ST}^p(i,t,\overline{x})\right)$, so the result follows by Lemma 4.4.7. □

An *output configuration for* $\overline{x} = (x_1,\dots,x_p) \in \mathbb{N}^p$ is a configuration where the tapes $B_1,\dots,B_p$ represent $x_1,\dots,x_p$, the tape B_{p+1} represents a natural number and where the other tapes represent 0.

For $p \geq 0$, we define a set $E^p \subseteq \mathbb{N}^{p+2}$ as follows:

$$(i,c,\overline{x}) \in E^p \;:\Longleftrightarrow\; \begin{cases} i \in I_p \text{ and } c \text{ is the code of an} \\ \text{output configuration for } \overline{x}. \end{cases}$$

It is easy to see that E^p is a primitive recursive set. (In order to express for example that B_{p+1} represents a natural number, observe that one may bound the universal quantifier in the formula $\forall z(\eta(c,z,p+1,n) = 2 \wedge z \geq 3 \to \eta(c,z\dot{-}1,p+1,n) = 2)$ by c. The details are left as an exercise.)

We now define sets $B^p \subseteq \mathbb{N}^{p+2}$ and $C^p \subseteq \mathbb{N}^{p+3}$ as follows:

$$(i,t,\overline{x}) \in B^p \;:\Longleftrightarrow\; \begin{cases} \beta_1^3\left(\mathrm{ST}^p(i,t,\overline{x})\right) = 1 \text{ and} \\ (i,\beta_3^3(\mathrm{ST}^p(i,t,\overline{x})),\overline{x}) \in E^p. \end{cases}$$

(This expresses that at the instant t, the machine of index i is in the final state, and its configuration is an output configuration for $\overline{x}$.)

$$(i,y,t,\overline{x}) \in C^p \;:\Longleftrightarrow\; \begin{cases} (i,t,\overline{x}) \in B^p \text{ and} \\ y \text{ is represented on } B_{p+1}. \end{cases}$$

The sets B^p and C^p are primitive recursive.

Now let $f \in \mathcal{F}_p^*$ be a partial Turing computable function. Choose a Turing machine $\mathcal{M}$ which computes f, and set $i = \ulcorner\mathcal{M}\urcorner$. One may define the partial function $T_{\mathcal{M}}$ (which gives the computing time) as

$$T_{\mathcal{M}}(\overline{x}) := \mu t\left((i,t,\overline{x}) \in B^p\right).$$

One then gets

$$(*) \qquad f(\overline{x}) = \big(\mu y \leq T_{\mathcal{M}}(\overline{x})\big)\big((i,y,T_{\mathcal{M}}(\overline{x}),\overline{x}) \in C^p\big).$$

The description $(*)$ is called the *Kleene normal form* of f.

In particular, we have proved the following two results.

Theorem 4.4.9. *Every partial Turing computable function is recursive.* □

Proposition 4.4.10.

(1) *If f is a total Turing computable function which may be computed in a primitive recursive time, then f is primitive recursive.*

(2) *The set of partial recursive functions is the smallest subset of $\mathcal{F}^*$ which contains the primitive recursive functions and which is stable under composition and under application of the μ-operator.*

(3) *The set of total recursive functions is the smallest subset of $\mathcal{F}$ which contains the primitive recursive functions and which is stable under composition and under application of the total μ-operator. In other words, every total recursive function may be obtained by a finite number of applications of the rules* (R0)-(R3). □

Let us observe that our arguments to prove that every Turing computable function is recursive are not specific to Turing machines. This justifies the following thesis.

Church's Thesis. Every function which is computable (in the intuitive sense) is recursive.

4.5. Universal Functions

It suffices to vary the index of the Turing machine in order to obtain a universal function. Let us first define a function $T^p \in \mathcal{F}^*_{p+1}$ as follows:

- if $i \notin I_p$, then $T^p(i, \overline{x})$ is not defined;
- if $i \in I_p$, then $T^p(i, \overline{x}) = \mu t \left[(i, t, \overline{x}) \in B^p\right]$.

We may now define a partial recursive function $\varphi^p \in \mathcal{F}^*_{p+1}$, via

$$\varphi^p(i, \overline{x}) = \mu y \left[(i, y, T^p(i, \overline{x}), \overline{x}) \in C^p\right].$$

We set $\varphi^p_i = \lambda \overline{x}.\varphi^p(i, \overline{x})$.

Proposition 4.5.1. *φ^p is a* universal *partial recursive function, that is, every partial recursive function in p variables is of the form φ_i^p for a suitable natural number i.* □

Theorem 4.5.2 (s-m-n Theorem)**.** *For any pair of natural numbers m and n there is a primitive recursive function $s_n^m \in \mathcal{F}_{n+1}$ such that for all $i \in \mathbb{N}, \overline{x} \in \mathbb{N}^n$ and $\overline{y} \in \mathbb{N}^m$ one has*

$$\varphi_i^{n+m}(\overline{x}, \overline{y}) = \varphi_{s_n^m(i,\overline{x})}^m(\overline{y}).$$

Proof. Let $\mathcal{M}$ be a Turing machine with at least $m + n + 1$ tapes. Given $(a_1, \dots, a_n) \in \mathbb{N}^n$, consider the Turing machine $\mathcal{M}'$ which operates as follows:

(1) It writes $a_1, \dots, a_n$ on the tapes $B_{m+2}, \dots, B_{m+n+1}$.

(2) It then operates as $\mathcal{M}$, up to permutation of the tapes, and it writes the result on the tape B_{m+1}.

(3) It then clears the tapes $B_{m+2}, \dots, B_{m+n+1}$, and finally it stops.

It is clear that there is a primitive recursive function $g \in \mathcal{F}_{n+1}$ which computes the code $\ulcorner \mathcal{M}' \urcorner \in I_m$ from $\ulcorner \mathcal{M} \urcorner$ and $a_1, \dots, a_n$, that is, $g(\ulcorner \mathcal{M} \urcorner, a_1, \dots, a_n) = \ulcorner \mathcal{M}' \urcorner$ and $g(i, \overline{a}) = 0$ if $i \notin I_{m+n}$. We may thus set $s_n^m = g$. □

Theorem 4.5.3 (Kleene's Fixed Point Theorem)**.** *Suppose $m \in \mathbb{N}^*$ and $\alpha \in \mathcal{F}_1$ is a total recursive function. Then there exists $i \in \mathbb{N}$ such that $\varphi_i^m = \varphi_{\alpha(i)}^m$.*

Proof. Consider $g = \lambda y x_1 \dots x_m . \varphi^m(\alpha(s_1^m(y, y)), x_1, \dots, x_m)$. By universality (Proposition 4.5.1), one has $g = \varphi_a^{m+1}$ for some index $a \in \mathbb{N}$. One gets

$$\varphi_{\alpha(s_1^m(y,y))}^m(\overline{x}) = \varphi_a^{m+1}(y, \overline{x}) = \varphi_{s_1^m(a,y)}^m(\overline{x}).$$

Setting $i := s_1^m(a, a)$, one obtains $\varphi_{\alpha(i)}^m = \varphi_i^m$. □

The Fixed Point Theorem provides an elegant argument to establish the following result (cf. Exercise 4.3.1).

Proposition 4.5.4. *The Ackermann function ξ is recursive.*

Proof. Define a partial recursive function $\theta \in \mathcal{F}_3^*$ as follows:

- $\theta(i,y,x) = 2^x$ if $y = 0$;
- $\theta(i,y,x) = 1$ if $x = 0$;
- $\theta(i,y,x) = \varphi^2(i, y\dot{-}1, \varphi^2(i,y,x\dot{-}1))$ otherwise.

By universality, there exists $a \in \mathbb{N}$ such that $\theta = \varphi^3_a$. By the s-m-n Theorem, this yields

$$\theta(i,y,x) = \varphi^2_{s^2_1(a,i)}(y,x).$$

Set $\alpha = \lambda i.s^2_1(a,i)$. By Kleene's Fixed Point Theorem (Theorem 4.5.3) there exists $i_0 \in \mathbb{N}$ such that $\varphi^2_{i_0} = \varphi^2_{\alpha(i_0)}$. The function $\varphi^2_{i_0}$ is recursive and satisfies the relations which define the Ackermann function. Indeed, for $y, x \in \mathbb{N}^*$, one has

$$\begin{aligned}\varphi^2_{i_0}(y,x) &= \theta(i_0,y,x)\\ &= \varphi^2(i_0, y-1, \varphi^2(i_0,y,x-1)) = \varphi^2_{i_0}(y-1, \varphi^2_{i_0}(y,x-1)).\end{aligned}$$

Finally, note that the totality of the function $\varphi^2_{i_0}$ follows by induction as well. □

4.6. Recursively Enumerable Sets

Definition. A set of natural numbers $X \subseteq \mathbb{N}^n$ is called *recursively enumerable* if there is a recursive set $Y \subseteq \mathbb{N}^{n+1}$ such that $X = \pi(Y)$, where π denotes the projection on the first n coordinates.

Remark. Every recursive set is recursively enumerable. □

Proposition 4.6.1. *The set of recursively enumerable sets is stable under intersection, union, projection and bounded universal quantification. Moreover, if $f_1, \dots, f_n \in \mathcal{F}_m$ are recursive and $X \subseteq \mathbb{N}^n$ is recursively enumerable, then $\{\overline{x} \in \mathbb{N}^m \mid (f_1(\overline{x}), \dots, f_m(\overline{x})) \in X\}$ is recursively enumerable.*

Proof. We say that an n-ary relation $R(x_1, \dots, x_n)$ on $\mathbb{N}$ is recursively enumerable if there exists an $n+1$-ary recursive relation $\widetilde{R}(\overline{x}, y)$ on $\mathbb{N}$ such that $R(\overline{x}) \iff \exists y \widetilde{R}(\overline{x}, y)$ holds in $\mathbb{N}$. In what follows, all equivalences are meant to be in $\mathbb{N}$.

Now assume that $R(\overline{x})$ and $S(\overline{x})$ are n-ary recursively enumerable relations. Choose recursive relations $\widetilde{R}(\overline{x}, y)$ and $\widetilde{S}(\overline{x}, y)$ such that $R(\overline{x}) \iff$

$\exists y\widetilde{R}(\overline{x}, y)$ and $S(\overline{x}) \iff \exists y\widetilde{S}(\overline{x}, y)$. We then have the following equivalences:

$$\begin{aligned} R(\overline{x}) \vee S(\overline{x}) &\iff \exists y \left(\widetilde{R}(\overline{x}, y) \vee \widetilde{S}(\overline{x}, y)\right). \\ R(\overline{x}) \wedge S(\overline{x}) &\iff \exists y \left(\widetilde{R}(\overline{x}, \beta_1^2(y)) \wedge \widetilde{S}(\overline{x}, \beta_2^2(y))\right). \\ \exists z R(\overline{y}, z) &\iff \exists z \exists u \widetilde{R}(\overline{y}, z, u) \iff \exists s \widetilde{R}(\overline{y}, \beta_1^2(s), \beta_2^2(s)). \end{aligned}$$

Moreover, $(\forall z \leq w)\, R(\overline{x}, z)$ is equivalent to $(\forall z \leq w)\, \exists y\, \widetilde{R}(\overline{x}, z, y)$, which in turn is equivalent to $\exists s\, (\forall z \leq w)\, \widetilde{R}(\overline{x}, z, (s)_z)$, where $(s)_z$ denotes the component function from Lemma 4.1.4.

Finally, suppose that $f_1, \dots, f_n \in \mathcal{F}_m$ are recursive functions. Then $R(f_1(\overline{x}), \dots, f_n(\overline{x}))$ is equivalent to $\exists y \widetilde{R}(f_1(\overline{x}), \dots, f_n(\overline{x}), y)$, which proves the moreover part. □

Theorem 4.6.2. *For $X \subseteq \mathbb{N}^n$, the following are equivalent:*

(1) *X is recursively enumerable.*

(2) *X is empty or it is the image of a function $f = (f_1, \dots, f_n) : \mathbb{N} \to \mathbb{N}^n$, where $f_1, \dots, f_n \in \mathcal{F}_1$ are (total) recursive.*

(3) *$X = \mathrm{dom}(g)$ for a partial recursive function $g \in \mathcal{F}_n^*$.*

(4) *There exists a primitive recursive set $Y \subseteq \mathbb{N}^{n+1}$ such that $X = \pi(Y)$.*

Proof. We may assume $n = 1$. Indeed, we may identify $\mathbb{N}^n$ and $\mathbb{N}$ using the bijection α_n, as α_n as well as the component functions β_i^n of α_n^{-1} are primitive recursive.

(1)⇒(2): Let $r \in X$ and let $Y \subseteq \mathbb{N}^2$ be recursive such that $X = P_1^2(Y)$. Then $X = \mathrm{im}(f)$, where $f \in \mathcal{F}_1$ is defined as follows:

$$f(z) := \begin{cases} \beta_1^2(z) & \text{if } (\beta_1^2(z), \beta_2^2(z)) \in Y, \\ r & \text{else.} \end{cases}$$

(2)⇒(3): If $f \in \mathcal{F}_1$ is a recursive function, we define $g = \lambda x.\mu t(x = f(t))$. Then g is a partial recursive function and $\mathrm{dom}(g) = \mathrm{im}(f)$. Moreover, $\emptyset = \mathrm{dom}(g)$ for $g = \lambda x.\mu t(x > x)$.

(3)⇒(4): Let $g \in \mathcal{F}_1^*$ be a partial recursive function such that $X = \mathrm{dom}(g)$. By universality there is $i_0 \in \mathbb{N}$ with $g = \varphi^1_{i_0}$, that is,

$$X = \{x \in \mathbb{N} \mid \exists t \left[(i_0, t, x) \in B^1\right]\}.$$

This proves (4), as B^1 is primitive recursive.

(4)⇒(1): Trivial. □

Remark. Given that (1) and (4) are equivalent, the proof of the implication (1)⇒(2) actually shows that one may suppose in (2) that the functions $f_1, \ldots, f_n$ are primitive recursive.

Corollary 4.6.3. *The set* $U = \mathrm{dom}(\varphi^n) \subseteq \mathbb{N}^{n+1}$ *is* universal recursively enumerable *in the following sense: U is recursively enumerable and every recursively enumerable set* $X \subseteq \mathbb{N}^n$ *is of the form* $U_e = \{\overline{x} \mid (e, \overline{x}) \in U\}$ *for some* $e \in \mathbb{N}$. □

Theorem 4.6.4 (Theorem of the Complement)**.** *A set* $X \subseteq \mathbb{N}^n$ *is recursive if and only if both X and* $\mathbb{N}^n \setminus X$ *are recursively enumerable.*

Proof. "⇒" is clear. To prove "⇐", assume that $X \subseteq \mathbb{N}^n$ is such that there are recursive subsets Y and Y' of $\mathbb{N}^{n+1}$ with $X = \pi(Y)$ and $\mathbb{N}^n \setminus X = \pi(Y')$. Then $\mathbb{1}_X(\overline{z}) = \mathbb{1}_Y(\overline{z}, \mu t[(\overline{z}, t) \in Y \cup Y'])$. □

Theorem 4.6.5. *The set* $\mathrm{dom}(\varphi^1)$ *is not recursive. In particular, there exists a recursively enumerable non-recursive set.*

Proof. We will prove that the domain of the function $g = \lambda x.\varphi^1(x, x)$ is not recursive. (In other words, one may not decide if a Turing machine stops when operating on its own code.)

Let $D = \mathbb{N} \setminus \mathrm{dom}(g)$. If D were recursively enumerable, then $D = \mathrm{dom}(\varphi^1_{i_0})$ for some $i_0 \in \mathbb{N}$ by Corollary 4.6.3. In particular, we would get $i_0 \in D$ if and only if $\varphi^1(i_0, i_0)$ is defined. But this is absurd, since the definition of g implies that $i_0 \in D$ if and only if $\varphi^1(i_0, i_0)$ is not defined. □

The *Halting Problem* HALT is defined as the set

$$\{i \in I_1 \mid \mathcal{M} \text{ of index } i \text{ halts when operating on the empty input}\}.$$

A slight variation of our argument in the previous proof yields the following.

Theorem 4.6.6 (Undecidability of the Halting Problem)**.** *The set* HALT *is not recursive.*

Proof. Suppose for contradiction that HALT is recursive. It is easy to see that $I_s = \mathrm{dom}\big(\lambda x.\varphi^1(x,0)\big)$ is then recursive as well, where I_s is by definition the set of indices of Turing machines which halt in an output configuration for the input 0 when operating on the empty input. Indeed, if $i \in \mathrm{HALT}$, then $i \in I_s$ if and only if

$$\Big(i, \beta_3^3(\mathrm{ST}^1(i, \mu t[\beta_1^3(\mathrm{ST}^1(i,t,0)) = 1], 0)), 0\Big) \in E^1.$$

Now choose a recursively enumerable non-recursive set $A \subseteq \mathbb{N}$ (which exists by Theorem 4.6.5). Let $\mathcal{M}$ be a Turing machine which computes a function $f \in \mathcal{F}_2^*$ with $\mathrm{dom}(f) = A \times \{0\}$. Let i_0 be the index of $\mathcal{M}$. Then $A = \{n \in \mathbb{N} \mid s_1^1(i_0, n) \in I_s\}$, and so A is recursive, contradicting our assumption. □

Theorem 4.6.7 (Rice's Theorem)**.** *Let $\mathcal{X}$ be a set of partial recursive functions in one variable. Suppose that $\mathcal{X}$ is neither empty nor equal to the set of all partial recursive functions in one variable. Then $I = \{i \in \mathbb{N} \mid \varphi_i^1 \in \mathcal{X}\}$ is not recursive.*

Proof. Passing to the complement if necessary, we may assume that the function with empty domain is in $\mathcal{X}$. Choose $j \in \mathbb{N} \setminus I$, and consider the function $\psi(x,y,z) = \big(\varphi^1(j,z) + \varphi^1(x,y)\big) \dot{-} \varphi^1(x,y)$. Letting $\psi_{x,y} = \lambda z.\psi(x,y,z)$, we get

$$\psi_{x,y} \in \mathcal{X} \iff (x,y) \notin \mathrm{dom}(\varphi^1) = U.$$

We have $\psi = \varphi_{i_0}^3$ for a natural number i_0, so $\psi_{x,y} = \varphi^1_{s_2^1(i_0,x,y)}$ by the s-m-n Theorem. Consider $h = \lambda xy.s_2^1(i_0,x,y)$, which is a recursive function. Then

$$(x,y) \in \mathbb{N}^2 \setminus U \iff h(x,y) \in I.$$

As $\mathbb{N}^2 \setminus U$ is not recursive by Theorem 4.6.4 (and the Theorem of the Complement), I is not recursive either. □

Example 4.6.8.

(1) Let $f \in \mathcal{F}_1^*$ be some partial recursive function. Then the set $\{i \in \mathbb{N} \mid \psi_i^1 = f\}$ is not recursive.

(2) The set $\{(i,j) \in \mathbb{N}^2 \mid \varphi_i^1 = \varphi_j^1\} \subseteq \mathbb{N}^2$ is not recursive.

(3) The set of indices of total (recursive) functions is not recursive.

4.7. Elimination of Recursion

The following elementary result is crucial for the next chapter, since it shows that the recursive functions are definable in the language of arithmetic $\mathcal{L}_{ar}$.

Theorem 4.7.1 (Elimination of Recursion)**.** *The set of total recursive functions is the smallest subset of $\mathcal{F}$ which contains the basic functions C_0^0, S, P_i^n, $+$, $\cdot$, $\mathbb{1}_=$ and $\mathbb{1}_<$, and which is stable under composition and the total μ-operator.*

Let E be the smallest subset of $\mathcal{F}$ which contains the basic functions $C_0^0, S, P_i^n, +, \cdot, \mathbb{1}_=$ and $\mathbb{1}_<$, and which is stable under composition and the total μ-operator. We will temporarily (until Theorem 4.7.1 is proven) say that a function is #-recursive if it is in E, and that a set X is #-recursive if $\mathbb{1}_X \in E$. We will first prove a lemma.

Lemma 4.7.2 (Gödel's β-function)**.**

(1) *The function $\lambda xy.x \dot{-} y$ is #-recursive.*

(2) *The collection of #-recursive sets is stable under boolean combinations and bounded quantification.*

(3) *The set $\{(x,y,z) \in \mathbb{N}^3 \mid x \equiv y \mod z\}$ is #-recursive.*

(4) *The collection of #-recursive functions is stable under definition by cases (see Lemma 4.1.2(5)), if both the functions and the sets of the partition are #-recursive.*

(5) *There exists a #-recursive function $\beta \in \mathcal{F}_3$ (called* Gödel's β-function*) such that for any finite sequence of natural numbers $(c_0, \ldots, c_{n-1})$ there are $a, b \in \mathbb{N}$ with $\beta(a,b,i) = c_i$ for $i = 0, \ldots, n-1$.*

Proof. (1) One has $x \dot{-} y = \mu z\,(x < (y + z) + 1)$.

(2) One has $\mathbb{1}_{X^c} = 1 \dot{-} \mathbb{1}_X$ and $\mathbb{1}_{X \cap Y} = \mathbb{1}_X \cdot \mathbb{1}_Y$, which establishes stability under boolean combinations. Now suppose that $X \subseteq \mathbb{N}^{n+1}$ is a

#-recursive set. Define a function $f \in \mathcal{F}_{n+1}$,

$$f(\overline{x}, z) := \mu y \big((\overline{x}, y) \in X \text{ or } y = z + 1\big).$$

As the condition in parentheses may be expressed by a condition of the form $g(\overline{x}, y, z) = 0$ for some #-recursive function g, it follows that f is #-recursive. Stability under bounded existential quantification follows from the equivalence $(\exists y \leq z)\,(\overline{x}, y) \in X \iff f(\overline{x}, z) < z + 1$. For $\forall y \leq z$, the same follows by passing to the complement. This finishes the proof of (2).

(3) One has the following equivalence:

$$x \equiv y \mod z \iff (\exists w \leq x + y)\big(x = y + w \cdot z \vee y = x + w \cdot z\big).$$

(4) Let $\mathbb{N}^n = A_1 \dot\cup \ldots \dot\cup A_k$ be a partition with A_i #-recursive for all i, and let $f_1, \ldots, f_k \in \mathcal{F}_n$ be #-recursive functions. Then $\sum_{i=1}^{k} \mathbb{1}_{A_i} \cdot f_i$ is #-recursive.

(5) Set $\beta(a, b, i) := \mu z\,[z \equiv a \mod ((i + 1)b + 1)]$. By what we have seen, β is #-recursive. Now let $c_0, \ldots, c_{n-1}$ be given, and let $b \in \mathbb{N}$ be such that b is divisible by $n!$ and $b > c_i$ for all i. Then $b+1, 2b+1, 3b+1, \ldots, nb+1$ is a sequence of coprime integers. Indeed, if a prime p divides $ib + 1$ and $jb + 1$ for some $1 \leq i < j \leq n$, then $p \nmid b$ and $p \mid b(i - j)$. Thus $p \mid (i - j)$. Since $(i - j) \mid n!$, this is absurd.

By the Chinese Remainder Theorem there exists $a \in \mathbb{N}$ such that for all $i = 0, \ldots, n - 1$ one has $a \equiv c_i \mod ((i + 1)b + 1)$. As $c_i < (i + 1)b + 1$ for all i, c_i is the smallest natural number z such that $z \equiv a \mod ((i + 1)b + 1)$. □

Proof of Theorem 4.7.1. By Proposition 4.4.10(3) it is enough to prove that the collection E of #-recursive functions is stable under recursion. Let $g \in \mathcal{F}_n$ and $h \in \mathcal{F}_{n+2}$ be #-recursive functions, and let $f \in \mathcal{F}_{n+1}$ be the function obtained by recursion from g and h. Consider the set

$$\begin{aligned} Z := \{(\overline{x}, y, a, b) \in \mathbb{N}^{n+3} \mid\ & \beta(a, b, 0) = g(\overline{x}) \\ & \text{and } (\forall i \leq y)\,\beta(a, b, i + 1) = h(\overline{x}, i, \beta(a, b, i))\}, \end{aligned}$$

which is #-recursive by Lemma 4.7.2. Moreover, the key property of β shows that for any $(\overline{x}, y) \in \mathbb{N}^{n+1}$ there are $a, b \in \mathbb{N}$ such that $(\overline{x}, y, a, b) \in$

Z. Thus, $e = \lambda\overline{x}y.\mu s\big[(\exists a \leq s)(\exists b \leq s)(\overline{x}, y, a, b) \in Z\big]$ is a #-recursive function. Finally, $f(\overline{x}, y)$ equals

$$\mu z\big[(\exists a \leq e(\overline{x}, y))(\exists b \leq e(\overline{x}, y))\big((\overline{x}, y, a, b) \in Z \text{ and } z = \beta(a, b, y)\big)\big],$$

proving that f is #-recursive. □

4.8. Exercises

Exercise 4.8.1. Describe a Turing machine which computes the addition function $\lambda xy.x + y$.

Exercise 4.8.2. Let p and q be prime numbers. Then q is called *p-Mersenne* if $q = \frac{p^n-1}{p-1}$ for some $n \in \mathbb{N}$. Prove that the following set is primitive recursive:

$$\{N \in \mathbb{N} \mid \text{ there is a prime } p \text{ such that } N \text{ is a } p\text{-Mersenne prime}\}.$$

Exercise 4.8.3. The Fibonacci function $\mathrm{fib} \in \mathcal{F}_1$ is defined via $\mathrm{fib}(0) := 0$, $\mathrm{fib}(1) := 1$, and $\mathrm{fib}(n+2) := \mathrm{fib}(n+1) + \mathrm{fib}(n)$ for all $n \in \mathbb{N}$. Prove that fib is primitive recursive.

Exercise 4.8.4 (Kalmár elementary functions)**.** The set of *elementary* (*recursive*) *functions* is the smallest subset E of $\mathcal{F}$ which satisfies the following properties:

- E contains C_0^0, the projections P_i^n for all $1 \leq i \leq n$, the addition, the multiplication and $\mathbb{1}_=$;
- if $g \in \mathcal{F}_k \cap E$ and $f_1, \ldots, f_k \in \mathcal{F}_n \cap E$, then $g(f_1, \ldots, f_k) \in E$;
- if $f \in \mathcal{F}_{n+1} \cap E$, then the bounded sum

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

and the bounded product

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

are in E, too.

(1) Prove that for all n, k, the constant function C_k^n is elementary.

(2) Call a subset $A \subseteq \mathbb{N}^n$ elementary if $\mathbb{1}_A$ is elementary. Prove that $\{0\} \subseteq \mathbb{N}$ is elementary, and that the set of elementary subsets of $\mathbb{N}^n$ is stable under Boolean combinations.

(3) Prove that the exponential function $\exp = \lambda xy.x^y$ is elementary.

(4) We now define a function $T \in \mathcal{F}_2$, setting $T(m,0) = m$ and $T(m,n+1) = \exp(2, T(m,n))$. For a natural number n, let $T_n = \lambda x.T(x,n)$.
   (a) Prove that T is primitive recursive.
   (b) Prove that T_n is strictly increasing for all n and that, for fixed m, the function $(m,n) \mapsto T(m,n)$ is strictly increasing in n.
   (c) Prove that for every elementary function f, there exists $n \in \mathbb{N}$ such that f is dominated by T_n.
   (d) Prove that T is not elementary.

Exercise 4.8.5.

(1) Let $f \in \mathcal{F}_1$ be an increasing recursive function. Prove that $\mathrm{im}(f)$ is recursive.

(2) Conversely, prove that any infinite recursive subset of $\mathbb{N}$ is the image of a strictly increasing unary recursive function.

(3) Prove that every infinite recursively enumerable set contains an infinite recursive set.

Exercise 4.8.6 (A primitive recursive bijection whose inverse is not primitive recursive)**.**

(1) Prove that the set of recursive bijections between $\mathbb{N}$ and $\mathbb{N}$ forms a group.

(2) Prove that for every Turing machine $\mathcal{M}$ which computes a total function, the graph of the computing time function $T_{\mathcal{M}}$ is primitive recursive.

(3) Prove that $f \in \mathcal{F}_n$ is primitive recursive if and only if its graph is primitive recursive and f is bounded from above by a primitive recursive function.

(4) Let $g \in \mathcal{F}_1$ be strictly increasing. Prove that the graph of g is primitive recursive if and only if $\mathrm{im}(g)$ is primitive recursive.

(5) Let $f \in \mathcal{F}_1$ be a recursive function which is not primitive recursive, and let $\mathcal{M}$ be a Turing machine computing f.
   (a) Let $g_0 \in \mathcal{F}_1$ be defined by
   $$g_0(x) = \sup\{T_{\mathcal{M}}(y) \mid y \leq x\} + 2x.$$
   Prove that g_0 is recursive, but not primitive recursive, and that the graph and the image of g_0 are primitive recursive sets.
   (b) Let $g_1 \in \mathcal{F}_1$ be a strictly increasing function such that $\mathrm{im}(g_1) = \mathbb{N} \setminus \mathrm{im}(g_0)$. Consider the function $h \in \mathcal{F}_1$ given by $h(2x) = g_0(x)$, $h(2x+1) = g_1(x)$. Prove that h is bijective, recursive, but not primitive recursive, and that h^{-1} is primitive recursive.

Exercise 4.8.7 (Existence of recursively inseparable recursively enumerable sets)**.**

(1) For a natural number $k \in \mathbb{N}$, denote by Z_k the set of all $n \in \mathbb{N}$ such that $n \in \mathrm{dom}(\varphi^1_n)$ and $\varphi^1_n(n) = k$. Prove that Z_k is recursively enumerable.

(2) Deduce from this that there exist recursively enumerable sets $A, B \subseteq \mathbb{N}$ with $A \cap B = \emptyset$ such that there is no recursive set $C \subseteq \mathbb{N}$ with $A \subseteq C$ and $C \cap B = \emptyset$.

(3) Prove that there is a partial recursive unary function which cannot be extended to a total recursive function.

Exercise 4.8.8. Prove that there are primitive recursive functions $s_1, s_2 \in \mathcal{F}_1$ such that whenever φ^2_i is bijective, the components of its inverse are given by $\varphi^1_{s_1(i)}$ and $\varphi^1_{s_2(i)}$.

10.1090/stml/089/05

Chapter 5

Models of Arithmetic and Limitation Theorems

Introduction

Our aim in this chapter is to study models of Peano arithmetic. We start by describing a way to encode formulas and proofs in a finite signature in a recursive way. This applies in particular to weak Peano arithmetic PA_0 and full Peano arithmetic PA which we introduce in 5.3. A key result is the Representability Theorem 5.3.5 which asserts that total recursive functions are represented by Σ_1-formulas. Using the diagonal argument (Proposition 5.4.1), we prove the theorem of Tarski on the non-definability of truth (Theorem 5.4.3) and the theorem of Church on the undecidability of arithmetic (Theorem 5.4.5).

In the Section 5.5 we prove Gödel's First Incompleteness Theorem. The last two sections are devoted to a complete proof of Gödel's celebrated second incompleteness theorem. This requires full Peano arithmetic PA contrary to the previous results for which only weak Peano arithmetic PA_0 was needed. A key ingredient is the definability of satisfiability for Σ_1-formulas which is proved in Proposition 5.6.1.

5.1. Coding Formulas and Proofs

Let $\sigma^{\mathcal{L}} = \{\lambda_1, \dots, \lambda_l\}$ be a finite signature. We assign to each symbol s of $\mathcal{L}$ its *Gödel number* $\ulcorner s \urcorner$ as follows: to $=, \wedge, \neg, (,), \exists$ one assigns $\langle 0,0\rangle, \langle 0,1\rangle, \dots, \langle 0,5\rangle$, to λ_i one assigns $\langle 0, i+5\rangle$, and to v_i ($i \in \mathbb{N}$) one assigns $\langle 1, i\rangle$.

To a word $m = s_1 \cdots s_n$ on the alphabet $\mathcal{L}$ we assign the *Gödel number*

$$\#m = \langle \ulcorner s_1 \urcorner, \dots, \ulcorner s_n \urcorner \rangle.$$

This coding is clearly injective.

Lemma 5.1.1. *The following sets are primitive recursive:*

(1) $\mathrm{Term} = \{\#t \mid t \text{ is an } \mathcal{L}\text{-term}\}$.

(2) $\mathrm{Form} = \{\#\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-formula}\}$.

(3) $\{(\#t, n) \mid t \in \mathcal{T}^{\mathcal{L}} \text{ and } v_n \text{ has an occurrence in } t\}$ *as well as* $\{(\#t, n) \mid t \in \mathcal{T}^{\mathcal{L}} \text{ and } v_n \text{ has no occurrence in } t\}$.

(4) $\{(\#\varphi, n) \mid \varphi \in \mathrm{Fml}^{\mathcal{L}} \text{ and } v_n \text{ has an occurrence in } \varphi\}$, *and similarly for* 'has no occurrence', 'has at least one free occurrence', 'has no free occurrence', 'has at least one bound occurrence' *and* 'has no bound occurrence' *instead of* 'has an occurrence'.

(5) $\{\#\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence}\}$.

Proof. We use properties of the coding function $\langle \dots \rangle$ for finite sequences (cf. Lemma 4.1.4) and the primitive recursive decoding function in two arguments $\lambda x i.(x)_i$. In particular, we use the inequality $n = \mathrm{lg}(\langle s_0, \dots, s_{n-1}\rangle) \leq \langle s_0, \dots, s_{n-1}\rangle$.

By unique reading properties, we may not only argue by induction on length, but also on height of terms and formulas. For instance, if x is the code of a word m starting with '(', then x is the code of a formula if and only if there exist $y_1, y_2 < x$ such that $y_i = \#\varphi_i$ for some formulas φ_1, φ_2 such that m is the word $(\varphi_1 \wedge \varphi_2)$. The details are left as an exercise. □

Recall that we have defined substitution in terms and formulas. If $x_1, \dots, x_n$ are n pairwise distinct variables, and $s_1, \dots, s_n$ are terms, we defined $t_{\overline{s}/\overline{x}}$ and $\varphi_{\overline{s}/\overline{x}}$ (see Section 2.4). One easily proves that the functions $S_t : \mathbb{N}^3 \to \mathbb{N}$ and $S_f : \mathbb{N}^3 \to \mathbb{N}$ are primitive recursive, where S_t is the

function assigning to (a, b, c) the integer $\#t_{\overline{s}/v_{i_1},\dots,v_{i_n}}$ if $a = \langle i_1, \dots, i_n\rangle$ is the code of a sequence of pairwise distinct natural numbers, $b = \#t \in$ Term and $c = \langle \#s_1, \dots, \#s_n\rangle$, with $\#s_i \in$ Term for any i, and 0 otherwise.

The function S_f is defined in a similar way: to

$$(a, b, c) = (\langle i_1, \dots, i_n\rangle, \#\varphi, \langle \#s_1, \dots, \#s_n\rangle)$$

one assigns

$$S_f(a, b, c) = \#\varphi_{\overline{s}/v_{i_1},\dots,v_{i_n}}.$$

In particular, one obtains the following statement:

Lemma 5.1.2. *There exist primitive recursive functions* Subst_t *and* Subst_f *in* $\mathcal{F}_3$ *such that, for any* n*, if* s *and* t *are terms and* φ *is a formula, then*

$$\mathrm{Subst}_t(n, \#s, \#t) = \#t_{s/v_n} \quad \textit{and} \quad \mathrm{Subst}_f(n, \#s, \#\varphi) = \#\varphi_{s/v_n}. \quad \square$$

Similarly, one encodes formulas from propositional calculus, via $F \mapsto \#F \in \mathbb{N}$, with $F \in \mathrm{Fml}_{\mathcal{P}}$.

Lemma 5.1.3. *The set* Taut *of codes of tautologies for the predicate calculus is primitive recursive.*

Proof. One checks directly that

- the set $\mathrm{Form}_{\mathcal{P}} = \{\#F \mid F \in \mathrm{Fml}_{\mathcal{P}}\}$ is primitive recursive;
- the function assigning to (d, x) the truth value (0 or 1) of the formula $F = F[p_0, \dots, p_{n-1}]$ for the distribution of truth values $d = \langle d_0, \dots, d_{n-1}\rangle$, with d the code of a length n sequence of 0's and 1's, and $x = \#F$ the code of $F \in \mathrm{Fml}_{\mathcal{P}}$ containing only propositional variables p_i with $i \leq n - 1$, and 0 otherwise, is primitive recursive;
- the set $\mathrm{Taut}_{\mathcal{P}} = \{\#F \mid F \text{ is a tautology}\}$ is primitive recursive;
- there exists a primitive recursive function assigning to the pair $(\langle \#\varphi_0, \dots \#\varphi_{n-1}\rangle, \#F)$ the natural number $\#F_{\overline{\varphi}/\overline{p}}$ if $F = F[p_0, \dots, p_{n-1}]$.

This is enough to get the result. $\square$

Similarly one checks that the set of codes of the equality axioms is primitive recursive and also the set of codes of the quantifier axioms (taking into account Lemma 5.1.2). We have thus proved the following statement.

Theorem 5.1.4. *The set* Ax *of codes $\#\varphi$ of logical axioms φ of $\mathcal{L}$ is primitive recursive.* □

Coding formal proofs. We encode a finite sequence of $\mathcal{L}$-formulas $d = (\varphi_0, \dots, \varphi_{n-1})$ by $\#\#d = \langle \#\varphi_0, \dots, \#\varphi_{n-1} \rangle$.

Lemma 5.1.5. *The set*

$$\mathrm{Prf} = \{(\#\#d, \#\varphi) \mid d \text{ is a formal proof of } \varphi\}$$

is primitive recursive.

Proof. Given (x, y), one first checks if $y \in \mathrm{Form}$, that is, if $y = \#\varphi$ for some $\mathcal{L}$-formula φ. If yes, it suffices to decode and to test whether all components of x are codes of $\mathcal{L}$-formulas φ_i, the last one being equal to φ, and whether for every i, either φ_i is a logical axiom (which is a primitive recursive property by Theorem 5.1.4) or it can be obtained using deduction rules from previous formulas. □

Proposition 5.1.6. *The set $U = \{\#\varphi \mid \vdash \varphi\}$ is recursively enumerable.*

Proof. We have $n \in U \Leftrightarrow \exists d\, (d, n) \in \mathrm{Prf}$. □

5.2. Decidable Theories

Let T be an $\mathcal{L}$-theory. We denote by $\mathrm{Thm}(T) = \{\varphi\ \mathcal{L}\text{-sentence} \mid T \vdash \varphi\}$ the deductive closure of T.

Definition. Let T be an $\mathcal{L}$-theory.

(1) T is called *recursive* if $\{\#\varphi \mid \varphi \in T\}$ is a recursive set.

(2) T is called *recursively* (or *effectively*) *axiomatizable* if there exists a recursive $\mathcal{L}$-theory T' such that $\mathrm{Thm}(T) = \mathrm{Thm}(T')$.

(3) T is called *decidable* if the set $\#\mathrm{Thm}(T) = \{\#\varphi \mid T \vdash \varphi\}$ is recursive.

If T is an $\mathcal{L}$-theory, one sets

$$\mathrm{Prf}(T) = \{(\#\#d, \#\varphi) \mid \ d \text{ is a proof of } \varphi \text{ in } T\}.$$

Lemma 5.2.1. *If T is recursive, then the set* $\mathrm{Prf}(T)$ *is recursive.*

Proof. Exercise. □

Theorem 5.2.2. *If T is effectively axiomatizable, then* $\#\mathrm{Thm}(T)$ *is recursively enumerable.*

Proof. Let T_0 be a recursive theory such that $\mathrm{Thm}(T) = \mathrm{Thm}(T_0)$.

We have $\varphi \in \mathrm{Thm}(T)$ if and only if φ is an $\mathcal{L}$-sentence and there exists a proof of φ in T_0. One concludes by Lemma 5.1.1(5) in combination with Lemma 5.2.1. □

Remark 5.2.3. The converse of Theorem 5.2.2 holds, too.

Proof. Assume the set $\#\mathrm{Thm}(T)$ is recursively enumerable. There then exists a recursive function $f \in \mathcal{F}_1$ such that

$$\#\mathrm{Thm}(T) = \{f(i) = \#\varphi_i \mid i \in \mathbb{N}\}.$$

The function g which to n assigns $\#\bigwedge_{i=0}^{n} \varphi_i$ is recursive and we have $g(n) \geq n$ for every n. Its image is therefore a recursive set. Since $\{\bigwedge_{i=0}^{n} \varphi_i \mid n \in \mathbb{N}\}$ is an axiomatization of $\mathrm{Thm}(T)$, this finishes the proof. □

Theorem 5.2.4. *Assume T is effectively axiomatizable and complete. Then T is decidable.*

Proof. By Theorem 5.2.2, we already know that $\#\mathrm{Thm}(T)$ is recursively enumerable. Its complement $\mathbb{N} \setminus \#\mathrm{Thm}(T)$ is the union of $\{\#\varphi \mid \neg\varphi \in \mathrm{Thm}(T)\}$ and $\{x \mid x \text{ is not the code of an } \mathcal{L}\text{-sentence}\}$. The former set is recursively enumerable since $\#\varphi \mapsto \#\neg\varphi$ is given by a (primitive) recursive function, while the latter one is primitive recursive by Lemma 5.1.1(5). One concludes by Theorem 4.6.4. □

Example 5.2.5.

(1) Any finitely axiomatizable theory is effectively axiomatizable.

(2) ACF_p, p prime or 0, is decidable.
[Indeed, the axiomatization is clearly recursive, and one concludes by combining Theorem 3.5.4 (ACF_p is complete) with Theorem 5.2.4.]

(3) ACF is decidable.
[Indeed, as ACF is effectively axiomatizable, it suffices to prove that $X = \{\#\varphi \mid \varphi \text{ is a sentence and } \mathrm{ACF} \not\models \varphi\}$ is a recursively enumerable set. But one has $\mathrm{ACF} \not\models \varphi$ if and only if there exists p prime such that $\mathrm{ACF}_p \models \neg\varphi$, as follows from the Lefschetz principle, which is equivalent to $\mathrm{ACF} \models \chi_p \to \neg\varphi$, where χ_p is the formula $\underbrace{1 + \cdots + 1}_{p \text{ times}} = 0$.

It follows that $\#\varphi \in X$ if and only if there exists a prime p and y such that $\big(y, \#(\chi_p \to \neg\varphi)\big) \in \mathrm{Prf}(\mathrm{ACF})$. Since the mapping $(p, \#\varphi) \mapsto \#(\chi_p \to \neg\varphi)$ is (primitive) recursive, one concludes that X is recursively enumerable.]

(4) The theory of the ordered field of real numbers $\mathcal{R}$ is decidable (this is a result of Tarski).
[Since it is complete, it suffices by Theorem 5.2.4 to give an effective axiomatization of $\mathrm{Th}(\mathcal{R})$. One can prove that any ordered field $\langle K; +, -, 0, 1, \cdot, < \rangle$ satisfying the intermediate value property for polynomial functions (that is, if $P(X) \in K[X]$ and $a, b \in K$ with $a < b$ and $P(a) \cdot P(b) < 0$, there exists $c \in K$ such that $a < c < b$ and $P(c) = 0$) is elementarily equivalent to $\mathcal{R}$. To prove this, one shows that the theory we just described admits quantifier elimination in the language of ordered rings, for which we refer to [**12**].]

Exercise 5.2.6. If T is decidable and $\varphi_0, \ldots, \varphi_{n-1}$ are $\mathcal{L}$-sentences, then $T \cup \{\varphi_0, \ldots, \varphi_{n-1}\}$ is decidable.

5.3. Peano Arithmetic

We shall work in the language of arithmetic $\mathcal{L}_{ar} = \{0, S, +, \cdot, <\}$. In any $\mathcal{L}_{ar}$-structure, for any $n \in \mathbb{N}$, one defines by induction $\underline{n}$, setting $\underline{0} = 0$ and $\underline{n+1} = S(\underline{n})$.

Definition.

(1) The set of *weak Peano axioms* is the finite set PA_0 consisting of the following 8 axioms:
- (A1) $\forall v_0\, \neg Sv_0 = 0$.
- (A2) $\forall v_0\, \exists v_1 (\neg v_0 = 0 \to Sv_1 = v_0)$.
- (A3) $\forall v_0 \forall v_1\, (Sv_0 = Sv_1 \to v_0 = v_1)$.
- (A4) $\forall v_0\, v_0 + 0 = v_0$.
- (A5) $\forall v_0 \forall v_1\, v_0 + Sv_1 = S(v_0 + v_1)$.
- (A6) $\forall v_0\, v_0 \cdot 0 = 0$.
- (A7) $\forall v_0 \forall v_1\, v_0 \cdot Sv_1 = (v_0 \cdot v_1) + v_0$.
- (A8) $\forall v_0 \forall v_1\, (v_0 < v_1 \leftrightarrow (\exists v_2 v_2 + v_0 = v_1 \wedge \neg v_0 = v_1))$.

(2) The set of *Peano axioms* is the infinite set PA consisting of PA_0, and for each $\mathcal{L}_{ar}$-formula $\varphi(v_0, \dots, v_n)$ of the following axiom of induction (where $\overline{v} = (v_1, \dots, v_n)$):

$$\forall v_1 \forall v_2 \cdots \forall v_n([\varphi(0, \overline{v}) \wedge \forall v_0(\varphi(v_0, \overline{v}) \to \varphi(Sv_0, \overline{v}))] \to \forall v_0 \varphi(v_0, \overline{v})).$$

Remark 5.3.1.

(1) One has $\mathfrak{N}_{\mathrm{st}} := \langle \mathbb{N}; 0, \mathit{succ}, +, \cdot, < \rangle \vDash \mathrm{PA}$.

(2) PA_0 is an expansion by definition of the $\mathcal{L}_{ar} \setminus \{<\}$-theory (A1)-(A7). (This is a consequence of (A8).)

(3) PA_0 is a quite weak theory. One may construct models in which addition (or multiplication) is not commutative or associative; also, there are models in which $<$ does not define a total order.

(4) An element in a model of PA_0 is called *non-standard* if it is different from the interpretation of $\underline{n}$ for any $n \in \mathbb{N}$. By compactness, there exist models of PA (and thus of PA_0) containing non-standard elements.

Definition. Let $\mathfrak{M} \subseteq \mathfrak{M}'$ be $\mathcal{L}_{ar}$-structures. One says that $\mathfrak{M}$ is an *initial segment* of $\mathfrak{M}'$ if the following two conditions hold:

- For all $a' \in M'$ and all $a \in M$ such that $\mathfrak{M}' \vDash a' < a$ one has $a' \in M$.
- For all $a' \in M' \setminus M$ and all $a \in M$ one has $\mathfrak{M}' \vDash a < a'$.

Lemma 5.3.2. *Let $\mathfrak{M} \vDash \mathrm{PA}_0$. Then $N = \{\underline{n}^{\mathfrak{M}} \mid n \in \mathbb{N}\}$ is the base set of a substructure of $\mathfrak{M}$ which is isomorphic to $\mathfrak{N}_{\mathrm{st}}$ and an initial segment of $\mathfrak{M}$.*

Proof. Let $\mathfrak{M} \vDash \mathrm{PA}_0$. One proves:

(i) For any $m, n \in \mathbb{N}$ one has $\mathrm{PA}_0 \vDash \underline{m} + \underline{n} = \underline{m+n}$.
This is proved by (naive) induction on $n \in \mathbb{N}$, using (A4) and (A5).

(ii) For any $m, n \in \mathbb{N}$ one has $\mathrm{PA}_0 \vDash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$.
This is proved by induction on n, using (A6), (A7) and (i).

(iii) $\mathrm{PA}_0 \vDash \forall x \forall y (x < y \leftrightarrow Sx < Sy)$.
Indeed, if $a, b, c \in M$, one has the following equivalences:

$$\mathfrak{M} \vDash c + a = b \wedge \neg a = b \overset{(A3)}{\iff} \mathfrak{M} \vDash S(c+a) = Sb \wedge \neg Sa = Sb$$
$$\overset{(A5)}{\iff} \mathfrak{M} \vDash c + Sa = Sb \wedge \neg Sa = Sb.$$

The statement thus follows from (A8).

(iv) For any $n \in \mathbb{N}$ one has $\mathrm{PA}_0 \vDash \forall x (x < \underline{n} \leftrightarrow \bigvee_{i=0}^{n-1} x = \underline{i})$.
This is proved by induction on n. If $\mathfrak{M} \vDash c < 0$ for some $c \in M$, then (in $\mathfrak{M}$) $a + c = 0$ for some $a \in M$ and $c \neq 0$ by (A8), hence $c = Sd$ for some d by (A2), and by (A5) one infers that $0 = a + Sd = S(a+d)$, which contradicts (A1). This proves the case $n = 0$. For the induction step $n \mapsto n+1$, one uses (iii) together with the fact that $0 < c$ for any $c \neq 0$ (a consequence of (A4) and (A8)).

(v) Let $c \in M \setminus N$ and $n \in \mathbb{N}$. Then $\mathfrak{M} \vDash \underline{n} < c$.
This is proved by induction on n, the case $n = 0$ being clear. For the induction step $n \mapsto n+1$, note that $c = Sd$ for some $d \notin N$. Hence $\mathfrak{M} \vDash \underline{n} < d$, which proves $\mathfrak{M} \vDash \underline{n+1} < c$, using (iii).

This concludes the proof. □

Up to naming elements of $\mathbb{N}$ by constants (which is irrelevant since any element of $\mathbb{N}$ is the interpretation of a term), we have in particular proved that if $\mathfrak{M} \models \mathrm{PA}_0$, then $\mathfrak{M} \models \Delta(\mathfrak{N}_{\mathrm{st}})$.

Definition.

(1) The set of Σ_1*-formulas* is the smallest set of $\mathcal{L}_{ar}$-formulas containing the quantifier-free formulas and which is stable under $\wedge$, $\vee$, existential quantification $\exists x$ and *bounded universal quantification* ($\forall x < t$), with t a term not depending on the variable x. Here, $(\forall x < t)\,\varphi$ is defined as $\forall x(x < t \to \varphi)$.

(2) The set of *strict* Σ_1*-formulas* is the smallest set of $\mathcal{L}_{ar}$-formulas containing the formulas $0 = x$, $Sx = y$, $x + y = z$, $x \cdot y = z$, $x = y$, $\neg x = y$, $x < y$, $\neg x < y$ and which is stable under $\wedge$, $\vee$, $\exists x$ and, assuming that x and y are two distinct variables, under $\forall x < y$.

Lemma 5.3.3.

(1) *Any* Σ_1*-formula is equivalent to a strict* Σ_1*-formula.*

(2) *If* φ *is a* Σ_1*-formula, then any formula* $\varphi_{\overline{s}/\overline{x}}$ *obtained by substitution is a* Σ_1*-formula, too.*

Proof. Proceeding as in the proof of Lemma 3.3.1 one may eliminate complex terms by using existential quantifiers. For instance, the formula $x \cdot Sy = 0$ is equivalent to $\exists u \exists v(Sy = u \wedge x \cdot u = v \wedge 0 = v)$. The second statement is clear. □

Proposition 5.3.4. *Any* Σ_1*-sentence satisfied in* $\mathfrak{N}_{\mathrm{st}}$ *is a theorem of* PA_0.

Proof. By Lemma 5.3.3, it is enough to prove that for any strict Σ_1-formula $\varphi(x_1, \dots, x_n)$ and any $m_1, \dots, m_n \in \mathbb{N}$ we have

$$\mathfrak{N}_{\mathrm{st}} \models \varphi[m_1, \dots, m_n] \Rightarrow \mathrm{PA}_0 \vdash \varphi(\underline{m_1}, \dots, \underline{m_n}).$$

We shall prove this by induction on the height of the formula starting from the case when φ is a quantifier-free formula, which follows from Lemma 5.3.2.

Assume now that the statement holds for $\varphi(x_0, \dots, x_n)$ and for $\psi(x_0, \dots, x_n)$. Clearly it then also holds for $\varphi \wedge \psi$ and $\varphi \vee \psi$. We now prove that it holds for $\exists x_0 \varphi(x_0, \dots, x_n)$. If $\mathfrak{N}_{\mathrm{st}} \models \exists x_0 \varphi[m_1, \dots, m_n]$, then

there exists $m_0 \in \mathbb{N}$ such that $\mathfrak{N}_{\mathrm{st}} \vDash \varphi[m_0, \dots, m_n]$, which implies $\mathrm{PA}_0 \vDash \varphi(\underline{m_0}, \dots, \underline{m_n})$ by the induction hypothesis; hence $\mathrm{PA}_0 \vDash \exists x_0 \varphi(\underline{m_1}, \dots, \underline{m_n})$.

Finally, if $\mathfrak{N}_{\mathrm{st}} \vDash (\forall x_0 < x_1)\varphi[m_1, \dots, m_n]$, then by definition of $\forall x_0 < x_1$ one has $\mathfrak{N}_{\mathrm{st}} \vDash \varphi[m_0, m_1, \dots, m_n]$ for any $m_0 < m_1$. By the induction hypothesis, we then have $\mathrm{PA}_0 \vDash \varphi(\underline{m_0}, \dots, \underline{m_n})$ for any $m_0 < m_1$. By (iv) in the proof of Lemma 5.3.2, one deduces $\mathrm{PA}_0 \vDash (\forall x_0 < x_1)\varphi(\underline{m_1}, \dots, \underline{m_n})$. □

Definition.

(1) Let $f \in \mathcal{F}_p$. One says that the formula $\varphi(x_1, \dots, x_{p+1})$ *represents* f if for any $n_1, \dots, n_p \in \mathbb{N}$ one has

$$\mathrm{PA}_0 \vDash \forall y \Big(\varphi(\underline{n_1}, \dots, \underline{n_p}, y) \leftrightarrow y = \underline{f(n_1, \dots, n_p)} \Big).$$

(2) Let $A \subseteq \mathbb{N}^p$. One says that $\varphi(x_1, \dots, x_p)$ *represents* A if for any $n_1, \dots, n_p \in \mathbb{N}$ one has

$$\overline{n} \in A \Rightarrow \mathrm{PA}_0 \vDash \varphi(\underline{n_1}, \dots, \underline{n_p})$$

and

$$\overline{n} \notin A \Rightarrow \mathrm{PA}_0 \vDash \neg\varphi(\underline{n_1}, \dots, \underline{n_p}).$$

Remark. If $\varphi(x_1, \dots, x_p)$ represents A, then $\mathbb{1}_A$ is represented by the formula $(\varphi(\overline{x}) \wedge x_{p+1} = \underline{1}) \vee (\neg\varphi(\overline{x}) \wedge x_{p+1} = 0)$. Conversely, if $\psi(\overline{x}, x_{p+1})$ represents $\mathbb{1}_A$, then $\psi(\overline{x}, \underline{1})$ represents A. □

Theorem 5.3.5 (Representability Theorem)**.** *Every total recursive function is represented by a Σ_1-formula.*

Proof. Let $\mathcal{S}$ be the set of total functions that are represented by a Σ_1-formula. By Theorem 4.7.1, it is enough to establish the following three facts:

(i) The basic functions $S, P_i^n, C_0^0, +, \cdot, \mathbb{1}_=$ and $\mathbb{1}_<$ are in $\mathcal{S}$.

(ii) $\mathcal{S}$ is stable under composition.

(iii) $\mathcal{S}$ is stable under the total μ-operator.

Item (i) is clear, since the basic functions are all represented by quantifier-free formulas (which are Σ_1 by definition).

If $f_1, \dots, f_p \in \mathcal{F}_m$ are represented by the formulas $\varphi_1, \dots, \varphi_p$ and if $g \in \mathcal{F}_p$ is represented by ψ, then $h = g(f_1, \dots, f_p) \in \mathcal{F}_m$ is represented by

$$\exists y_1, \dots, \exists y_p \bigwedge_{i=1}^{p} \varphi_i(\overline{x}, y_i) \wedge \psi(y_1, \dots, y_p, x_{m+1}).$$

In particular, this proves (ii).

Finally, let $f \in \mathcal{F}_{p+1} \in \mathcal{S}$, and let $g \in \mathcal{F}_p$ be the function obtained from f by the total μ-operator, that is, $g(\overline{x}) = \mu y\,(f(\overline{x}, y) = 0)$. Let $A = \{(\overline{x}, y) \mid f(\overline{x}, y) = 0\} \subseteq \mathbb{N}^{p+1}$. Applying (i) and (ii), we get $\mathbb{1}_A = \lambda \overline{x} y. \mathbb{1}_{=}(f(\overline{x}, y), 0) \in \mathcal{S}$. Choose a Σ_1-formula $\varphi(\overline{x}, y, z)$ representing $\mathbb{1}_A$. Then the function g is represented by the Σ_1-formula $\psi(\overline{x}, y)$ given by $\varphi(\overline{x}, y, \underline{1}) \wedge (\forall y' < y)\, \varphi(\overline{x}, y', 0)$. This proves (iii). □

Corollary 5.3.6. *A subset $A \subseteq \mathbb{N}^n$ is recursively enumerable if and only if there exists a Σ_1-formula defining A in the structure $\mathfrak{N}_{\mathrm{st}}$.*

Proof. Any subset defined by a quantifier-free formula is (primitive) recursive, hence a subset defined by a Σ_1-formula is recursively enumerable by the closure properties of recursively enumerable sets, their stability under existential quantification (that is, under projection), bounded universal quantification, intersection and union (Proposition 4.6.1).

Conversely, since any recursively enumerable set is the projection of a recursive set, it is enough to prove that any recursive set is defined by a Σ_1-formula, which follows from the Representability Theorem. □

Proposition 5.3.7. *Let $\mathfrak{M}$ be a model of* PA. *Then the following properties are satisfied in $\mathfrak{M}$:*

(1) *$+$ and $\cdot$ are commutative and associative.*

(2) *$\cdot$ is distributive with respect to $+$.*

(3) *$<$ defines a total order, compatible with $+$ (if $a < b$, then $a + c < b + c$) and with multiplication with a non-zero element (if $a < b$ and $c \neq 0$, then $a \cdot c < b \cdot c$); 0 is the minimal element for this order, and for any a, Sa is the immediate successor of a.*

(4) *Any element is regular for addition* ($a+c = b+c \Rightarrow a = b$)*, and any non-zero element is regular for multiplication* (*if* $a \cdot c = b \cdot c$ *and* $c \neq 0$*, then* $a = b$).

Proof. All these properties are easily proved using the induction axioms of PA. As examples, let us provide the arguments for associativity and commutativity of addition. The proof of the remaining properties is similar.

Associativity of addition.

Let $\varphi(x, y, z)$ be the formula $x+(y+z) = (x+y)+z$. In $\mathfrak{M}$, we have $a+(b+0) = a+b = (a+b)+0$ by (A4), and hence $\mathfrak{M} \vDash \forall x, y\, \varphi(x, y, 0)$. If $a, b, c \in M$ verify $(a+b)+c = a+(b+c)$, then

$$\begin{aligned} a+(b+Sc) = a+S(b+c) &= S(a+(b+c)) \\ &= S((a+b)+c) = (a+b)+Sc \end{aligned}$$

by (A5), whence $\mathfrak{M} \vDash \forall x, y, z\, (\varphi(x, y, z) \rightarrow \varphi(x, y, Sz))$. The induction axiom for φ implies that $\mathfrak{M} \vDash \forall x, y, z\, \varphi(x, y, z)$.

Commutativity of addition.

One checks the following properties:

(i) $\mathfrak{M} \vDash \forall x\, 0 + x = x$ (by induction, using (A4) and (A5)).

(ii) $\mathfrak{M} \vDash \forall x\, \underline{1} + x = Sx$ (by induction, using (i) and (A5)).

(iii) $\mathfrak{M} \vDash \forall x, y\, x + y = y + x$ (by induction, using (i), (ii) and associativity of addition). □

Remark. By Proposition 5.3.7, PA suffices for the purposes of basic number theory. However, as we will see later in this chapter, PA is not a complete theory. Concrete mathematical statements independent from PA are not so easy to provide, but it is known that for instance Goodstein's theorem from Exercise 1.11.3 is such an example.

Lemma 5.3.8 (Overspill)**.** *Let* $\mathfrak{M}$ *be a non-standard model of* PA (*that is, a model containing a non-standard element*) *and let* $\varphi(x)$ *be an* $\mathcal{L}_{ar}$*-formula. If* $\mathfrak{M} \vDash \varphi(\underline{n})$ *for every* $n \in \mathbb{N}$*, then there exists* $c \in M$ *non-standard such that* $\mathfrak{M} \vDash \varphi[c]$.

Proof. Otherwise, φ would be satisfied precisely by the standard elements, yielding $\mathfrak{M} \vDash \varphi(0)$ and $\mathfrak{M} \vDash \forall x(\varphi(x) \to \varphi(Sx))$. But then $\mathfrak{M} \vDash \forall x\, \varphi(x)$, which is a contradiction since $\mathfrak{M}$ contains non-standard elements by hypothesis. □

5.4. The Theorems of Tarski and Church

We fix a primitive recursive function subst $\in \mathcal{F}_2$ such that if $\varphi(v)$ is any $\mathcal{L}_{ar}$-formula with one free variable v and $n \in \mathbb{N}$, then one has $\text{subst}(\#\varphi, n) = \#\varphi(\underline{n})$. Note that such a function subst clearly exists.

By the Representability Theorem, we may choose a Σ_1-formula $G(x, y, z)$ representing subst. Given a formula $\varphi(v)$ with one free variable v, we consider the formula

$$H_\varphi(x) := \exists z\,(G(x, x, z) \wedge \varphi(z)),$$

and we set $n_\varphi := \#\neg H_\varphi$ and $\Delta_\varphi := \neg H_\varphi(\underline{n_\varphi})$.

Proposition 5.4.1 (The Diagonal Argument)**.** *Let $\varphi(v)$ be a formula with one free variable, in the language $\mathcal{L}_{ar}$. Then*

$$\text{PA}_0 \vdash \varphi(\underline{\#\Delta_\varphi}) \leftrightarrow \neg\Delta_\varphi.$$

Proof. Let $\mathfrak{M}$ be a model of PA_0. Since by the above definitions $\text{subst}(n_\varphi, n_\varphi) = \text{subst}(\#\neg H_\varphi, n_\varphi) = \#\Delta_\varphi$, we have

$$(*) \qquad \mathfrak{M} \vDash \forall z \left(G(\underline{n_\varphi}, \underline{n_\varphi}, z) \leftrightarrow z = \underline{\#\Delta_\varphi} \right),$$

and thus

$$\mathfrak{M} \vDash \varphi(\underline{\#\Delta_\varphi}) \Leftrightarrow \mathfrak{M} \vDash \underbrace{\exists z \left(G(\underline{n_\varphi}, \underline{n_\varphi}, z) \wedge \varphi(z) \right)}_{H_\varphi(\underline{n_\varphi})} \Leftrightarrow \mathfrak{M} \vDash \neg\Delta_\varphi$$

by $(*)$ and by the definition of Δ_φ, respectively. □

Corollary 5.4.2 (Fixed Point Theorem)**.** *Let $\varphi(v)$ be an $\mathcal{L}_{ar}$-formula with one free variable. Then there exists an $\mathcal{L}_{ar}$-sentence ψ such that*

$$\text{PA}_0 \vdash \varphi(\underline{\#\psi}) \leftrightarrow \psi.$$

Proof. One may take $\Delta_{\neg\varphi}$ as ψ and use the Diagonal Argument. □

Theorem 5.4.3 (Tarski's Theorem on the Non-definability of Truth)**.** *Let $\mathfrak{M} \models \mathrm{PA}_0$. Then there is no $\mathcal{L}_{ar}$-formula $S(v)$ with one free variable such that for any $\mathcal{L}_{ar}$-sentence ψ one has $\mathfrak{M} \models \psi$ if and only if $\mathfrak{M} \models S(\underline{\#\psi})$.*

Proof. Assume S is such a formula. By Proposition 5.4.1 one has $\mathrm{PA}_0 \vdash S(\underline{\#\Delta_S}) \leftrightarrow \neg\Delta_S$. In particular, $\mathfrak{M} \models S(\underline{\#\Delta_S}) \leftrightarrow \neg\Delta_S$, which is absurd in view of the property satisfied by S. □

Corollary 5.4.4. *There is no $\mathcal{L}_{ar}$-formula $S_{\mathfrak{N}_{\mathrm{st}}}(v)$ such that for any $\mathcal{L}_{ar}$-sentence ψ one has $\mathfrak{N}_{\mathrm{st}} \models \psi$ if and only if $\mathfrak{N}_{\mathrm{st}} \models S_{\mathfrak{N}_{\mathrm{st}}}(\underline{\#\psi})$. In particular,* $\mathrm{Th}(\mathfrak{N}_{\mathrm{st}})$ *is undecidable.*

Proof. The first part is a special case of Theorem 5.4.3. Assume now, for contradiction, that $T = \mathrm{Th}(\mathfrak{N}_{\mathrm{st}})$ is decidable. This means that $\#\mathrm{Thm}(T)$ is a recursive set and thus representable by a Σ_1-formula $\varphi(v)$ by Theorem 5.3.5. For any $\mathcal{L}_{ar}$-sentence ψ we then have $\mathfrak{N}_{\mathrm{st}} \models \psi$ if and only if $\mathfrak{N}_{\mathrm{st}} \models \varphi(\underline{\#\psi})$, contradicting the first part. □

Theorem 5.4.5 (Church's Theorem)**.** *Let $T \supseteq \mathrm{PA}_0$ be a consistent $\mathcal{L}_{ar}$-theory. Then T is undecidable.*

Proof. Otherwise, $\#\mathrm{Thm}(T)$ would be a recursive set, and there would exist, by the Representability Theorem, a formula $\tau(v)$ representing $\#\mathrm{Thm}(T)$. Applying Proposition 5.4.1 we would get

$$T \vdash \Delta_\tau \Leftrightarrow \#\Delta_\tau \in \#\mathrm{Thm}(T) \Leftrightarrow \mathrm{PA}_0 \vdash \tau(\underline{\#\Delta_\tau}) \Leftrightarrow \mathrm{PA}_0 \vdash \neg\Delta_\tau,$$

which is absurd, since by assumption T is a consistent theory with $T \supseteq \mathrm{PA}_0$. □

Church's Theorem yields undecidability of the Predicate Calculus:

Corollary 5.4.6 (Church)**.** *There exists a finite language $\mathcal{L}$ such that $U = \{\#\varphi \mid \varphi$ is a universally valid $\mathcal{L}$-formula$\}$ is not recursive.*

Proof. Let $\mathcal{L} = \mathcal{L}_{ar}$. Assume U is recursive. Then, as a formula φ is universally valid if and only if a universal closure of φ is, the empty $\mathcal{L}_{ar}$-theory is decidable. Since PA_0 is a finite theory, PA_0 would then

be decidable by Exercise 5.2.6, contradicting the Theorem of Church. Indeed,

$$\varphi \in \mathrm{Thm}(\mathrm{PA}_0) \Leftrightarrow \mathrm{PA}_0 \vdash \varphi \Leftrightarrow \vdash \underbrace{\bigwedge_{i=1}^{8} A_i \to \varphi}_{\psi_\varphi} \Leftrightarrow \psi_\varphi \in \mathrm{Thm}(\emptyset). \quad \square$$

Remark. One can prove that the corollary already holds for $\mathcal{L}$ consisting only of a binary relation symbol, that is, $\mathcal{L}_{set} = \{\in\}$. Examples of simpler languages for which this no longer holds are discussed in Exercise 5.8.3.

5.5. Gödel's First Incompleteness Theorem

From Church's Theorem we may now derive Gödel's First Incompleteness Theorem, which Gödel had proved prior to Church's work.

Theorem 5.5.1 (Gödel's First Incompleteness Theorem)**.** *Let T be a consistent and recursive $\mathcal{L}_{ar}$-theory such that $T \supseteq \mathrm{PA}_0$. Then T is not complete.*

Proof. If T were complete, it would be decidable by Theorem 5.2.4, contradicting Church's Theorem. $\square$

In the remainder of this section, we shall keep the hypotheses of Theorem 5.5.1, namely $T \supseteq \mathrm{PA}_0$ is consistent and recursive. We will now present an improvement of Theorem 5.5.1, due to Rosser, providing an explicit sentence ψ such that neither $T \vdash \psi$ nor $T \vdash \neg\psi$.

We recall that the set

$$\mathrm{Prf}(T) = \{(\#\varphi, \#\#d) \mid d \text{ is a formal proof of } \varphi \text{ in } T\}$$

is recursive. By the Representability Theorem, there exists a Σ_1-formula $P_T(x, y)$ representing $\mathrm{Prf}(T) \subseteq \mathbb{N}^2$.

Let $\mathrm{Neg} : \mathbb{N} \to \mathbb{N}$ be a primitive recursive function such that $\mathrm{Neg}(\#\varphi) = \#\neg\varphi$ and $\mathrm{Neg}(x) = 0$ if x is not the code of a formula. Fix a Σ_1-formula $\nu(x, y)$ representing Neg. We set

$$P_T^R(x, y) := P_T(x, y) \wedge \neg(\exists z \leq y)\exists u(P_T(u, z) \wedge \nu(x, u)).$$

Let $h_T^R(x) := \exists y P_T^R(x, y)$, and $\Delta_T^R := \Delta_{h_T^R}$.

Theorem 5.5.2 (Rosser's Variant of the First Incompleteness Theorem)**.** *Let $T \supseteq \mathrm{PA}_0$ be consistent and recursive. Then $T \nvdash \Delta_T^R$ and $T \nvdash \neg\Delta_T^R$.*

Proof. We set $\Delta := \Delta_T^R$ and $m := \#\Delta$. By the Diagonal Argument (Proposition 5.4.1), we have

$$(\dagger) \qquad \mathrm{PA}_0 \vdash \exists y P_T^R(\underline{m}, y) \leftrightarrow \neg\Delta.$$

Assume $T \vdash \Delta$. Then there exists a proof of Δ in T, thus there exists $p \in \mathbb{N}$ such that $(m, p) \in \mathrm{Prf}(T)$, whence $\mathrm{PA}_0 \vdash P_T(\underline{m}, \underline{p})$. Since T is consistent, for any $p' \in \mathbb{N}$ we have $\mathrm{PA}_0 \vdash \neg\exists u \left(\nu(\underline{m}, u) \wedge P_T(u, \underline{p'})\right)$. It is enough to note that $\mathrm{PA}_0 \vdash (x \leq \underline{p} \leftrightarrow \bigvee_{i=0}^{p} x = \underline{i})$ to deduce that $\mathrm{PA}_0 \vdash P_T^R(\underline{m}, \underline{p})$. By (†), we have $\mathrm{PA}_0 \vdash \neg\Delta$, and hence $T \vdash \neg\Delta$ (since $T \supseteq \mathrm{PA}_0$). This is a contradiction.

Assume $T \vdash \neg\Delta$. Then there exists a natural number p such that $\mathrm{PA}_0 \vdash P_T(\underline{\#\neg\Delta}, \underline{p})$. Since T is consistent, for any $p' \in \mathbb{N}$ we have $\mathrm{PA}_0 \vdash \neg P_T(\underline{m}, \underline{p'})$. It follows that $\mathrm{PA}_0 \vdash \neg\exists y P_T^R(\underline{m}, y)$, since $\mathfrak{N}_{\mathrm{st}}$ is an initial segment of any model of PA_0 by Lemma 5.3.2. By (†), we have $\mathrm{PA}_0 \vdash \Delta$, and hence $T \vdash \Delta$, which is a contradiction. □

Remark. Let $T \supseteq \mathrm{PA}_0$ be a consistant and recursive $\mathcal{L}_{ar}$-theory. Let $h_T(x) := \exists y P_T(x, y)$ and $\Delta_T := \Delta_{h_T}$. Then $T \nvdash \Delta_T$.

Proof. The proof is similar to that of Theorem 5.5.2 and left as an exercise. □

5.6. Definability of Satisfiability for Σ_1-formulas

By Tarski's result (Theorem 5.4.3), there is no formula expressing satisfiability for all arithmetical sentences. However, if one restricts to Σ_1-sentences, one has the following representability result:

Proposition 5.6.1. *There exists a Σ_1-formula $\mathrm{Sat}_{\Sigma_1}(v)$ such that for any Σ_1-sentence φ one has*

$$\mathrm{PA} \vdash \varphi \leftrightarrow \mathrm{Sat}_{\Sigma_1}(\underline{\#\varphi}).$$

Before we give a proof the proposition, we prove a result which guarantees that various arguments involving coding may be carried out in any model of PA.

Lemma 5.6.2. *Let $f \in \mathcal{F}_n$ be a primitive recursive function. Then there is a Σ_1-formula $\chi_f(x_1 \dots, x_n, y)$ representing f such that*

$$\mathrm{PA} \vdash \forall x_1, \dots, x_n \exists! \, y \chi_f.$$

Proof. We say that function $f \in \mathcal{F}$ is *provably total* Σ_1 if the conclusion of the lemma holds for f. We will only sketch the argument and leave the (rather tedious) details to the reader.

Claim 1. *Gödel's β-function $\beta \in \mathcal{F}_3$ is provably total Σ_1.*

Recall that $\beta(x_1, x_2, x_3) = \mu z \, [z \equiv x_1 \mod (x_2(x_3 + 1) + 1)]$. One checks that the formula $\chi_\beta(x_1, x_2, x_3, y)$ given by

$$(*) \qquad y < x_2(x_3 + 1) + 1 \wedge \exists v \, x_1 = x_0 + v((x_3 + 1) + 1)$$

is a Σ_1-formula which represents β and defines a total function in any model of PA. This proves Claim 1.

Claim 2. *Let $\mathfrak{M}$ be a model of* PA*, $\gamma(x, y)$ an $\mathcal{L}_{ar}$-formula with parameters from M and $i \in M$ such that $\mathfrak{M} \models (\forall j < i) \exists! \, y \gamma(j, y)$. Then there are $a, b \in M$ such that $\mathfrak{M} \models (\forall j < i) \forall y (\chi_\beta(a, b, j, y) \leftrightarrow \gamma(j, y))$, with χ_β as in $(*)$.*

This holds in $\mathfrak{N}_{\mathrm{st}}$ by Lemma 4.7.2(5). If it did not hold in $\mathfrak{M}$, there would be a minimal i_0 where it fails. The proof that if it holds for $i_0 - 1$, then it holds for i_0 only uses basic number theory and may thus be carried out in $\mathfrak{M} \models \mathrm{PA}$. Thus, a minimal counter-example cannot exist, proving Claim 2.

Claim 3. *The set of provably total Σ_1-functions contains the basic functions $(S, P_i^n$ and $C_0^0)$, and it is stable under composition and recursion.*

The statements about the basic functions and composition are clear. To prove stability under recursion, suppose $f \in \mathcal{F}_{n+1}$ is defined by recursion using $g \in \mathcal{F}_n$ and $h \in \mathcal{F}_{n+2}$, and that $\psi(x_1, \dots, x_n, y)$ is a Σ_1-formula representing g which defines a total function in any model of PA, and similarly $\theta(x_1, \dots, x_{n+2}, y)$ for h. Using Claim 2, one may then construct

a Σ_1-formula $\varphi(x_1, \dots, x_{n+1}, y)$ representing f which defines a total function in any model of PA, by coding the computation of f as in the proof of Theorem 4.7.1. □

Remark 5.6.3. Consider the expansion by definitions of PA given by adding new symbols for the functions defined by the formulas χ_f as in Lemma 5.6.2. By the proofs of Lemma 3.3.1 and Proposition 3.3.2, noting in addition that the formula $\neg\chi_f(\overline{x}, y)$ is equivalent in PA to the Σ_1-formula $\exists z(\chi_f(\overline{x}, z) \wedge y \neq z)$, it follows from Lemma 5.6.2 that every Σ_1-formula in the expansion is equivalent to a Σ_1-formula in $\mathcal{L}_{ar}$. Below, we will construct Σ_1-formulas through this process. Abusing notation, we will use the same letter f for the function symbol and for the corresponding primitive recursive function.

We will in particular use the binary function $(x)_i$ to decode sequences in $\mathfrak{M} \models$ PA which are of 'finite' length in the sense of $\mathfrak{M}$.

Proof of Proposition 5.6.1. By Lemma 5.3.3 any Σ_1-formula φ is logically equivalent to a strict Σ_1-formula. It follows from the proof of that lemma that there exists a primitive recursive function f such that, for any Σ_1-formula φ, $f(\#\varphi)$ is the Gödel number of a strict Σ_1-formula logically equivalent to φ. It is thus enough to prove the existence of a Σ_1-formula $S'(v)$ such that for any strict Σ_1-sentence φ, one has PA $\vdash \varphi \leftrightarrow S'(\underline{\#\varphi})$.

By a *certificate* of a strict Σ_1-formula φ we shall mean a finite sequence $(\varphi_1, \dots, \varphi_n)$ of strict Σ_1-formulas with φ_n equal to φ and a finite sequence $(s^1, \dots, s^n)$ of finite sequences of natural numbers $s^m = (s_0^m, \dots, s_{\alpha(m)-1}^m)$ such that the following conditions hold:

(i) All free variables of φ_m belong to $v_0, \dots, v_{\alpha(m)-1}$.

(ii) If φ_m is the formula $0 = v_i$ then $0 = s_i^m$.

(iii) If φ_m is the formula $S(v_i) = v_j$ then $s_i^m + 1 = s_j^m$.

(iv) If φ_m is the formula $v_i + v_j = v_k$ then $s_i^m + s_j^m = s_k^m$.

(v) If φ_m is the formula $v_i \cdot v_j = v_k$ then $s_i^m s_j^m = s_k^m$.

(vi) If φ_m is the formula $v_i = v_j$ then $s_i^m = s_j^m$.

(vii) If φ_m is the formula $\neg v_i = v_j$ then $s_i^m \neq s_j^m$.

(viii) If φ_m is the formula $v_i < v_j$ then $s_i^m < s_j^m$.

(ix) If φ_m is the formula $\neg v_i < v_j$ then $s_i^m \not< s_j^m$.

(x) If φ_m is the formula $\varphi' \wedge \varphi''$ then $\exists m', m'' < m$ such that φ' equals $\varphi_{m'}$, φ'' equals $\varphi_{m''}$ and $s^m = s^{m'} = s^{m''}$.

(xi) If φ_m is the formula $\varphi' \vee \varphi''$ then $\exists m' < m$ such that φ' equals $\varphi_{m'}$ and $s^m = s^{m'}$, or $\exists m'' < m$ such that φ'' equals $\varphi_{m''}$ and $s^m = s^{m''}$.

(xii) If φ_m is the formula $\exists v_i \varphi'$ then $\exists m' < m$ such that φ' equals $\varphi_{m'}$ and $s_k^{m'} = s_k^m$, $\forall k < \min(\alpha(m), \alpha(m'))$, $k \neq i$.

(xiii) If φ_m is the formula $(\forall v_i < v_j)\, \varphi'$ then $\forall a < s_j^m\ \exists m' < m$ such that φ' equals $\varphi_{m'}$, $s_i^{m'} = a$ and such that $s_k^{m'} = s_k^m$, $\forall k < \min(\alpha(m), \alpha(m'))$, $k \neq i$.

This notion of certificate makes sense in any model $\mathfrak{M}$ of PA and one has

$$\mathfrak{M} \vDash \text{“}\varphi \text{ has a certificate”} \text{ if and only if } \mathfrak{M} \vDash \varphi.$$

This is checked by induction on $\#\varphi$ in the model $\mathfrak{M}$ (it is crucial here that $\mathfrak{M}$ is a model of PA and not only of PA_0).

Furthermore, one may express the existence of a certificate for φ in $\mathfrak{M}$ by a Σ_1-formula in the Gödel number of φ. More precisely, there exists a Σ_1-formula $S'(v)$, such that in any model $\mathfrak{M}$ of PA, for any code $\#\varphi$ of a 'strict Σ_1-formula' (even non-standard), $\mathfrak{M} \vDash S'(\#\varphi)$ if and only if $\mathfrak{M} \vDash$ “φ has a certificate”. One constructs $S'(v)$ by coding conditions (i)-(xiii) that are clearly expressed by Σ_1-conditions. The equivalence between $\mathfrak{M} \vDash S'(\#\varphi)$ and $\mathfrak{M} \vDash$ “φ has a certificate” is checked by induction on $\#\varphi$ in the model $\mathfrak{M}$. Here again it is important that $\mathfrak{M}$ is a model of PA. □

5.7. Gödel's Second Incompleteness Theorem

Let T be a recursive $\mathcal{L}_{ar}$-theory containing PA. To state and to prove the Second Incompleteness Theorem, we will explicitly construct a specific formula expressing that a sentence is provable.

We consider Σ_1-formulas $\mathrm{Sen}(v)$, $\mathrm{Ax}_T(v)$, $\mathrm{MP}(v_0, v_1, v_2)$ as well as $\mathrm{Gen}(v_0, v_1)$ representing respectively the set of Gödel numbers of sentences, the union of the sets of Gödel numbers of logical axioms and of those of T, the set of triples $(\#\varphi, \#\psi, \#\delta)$ with φ, ψ and δ formulas such

that δ is obtained from φ and ψ by modus ponens, and the set of pairs $(\#\varphi, \#\psi)$ with φ and ψ such that ψ is obtained from φ by generalization.

We shall also use Gödel's β-function to code sequences. We consider the following formula $B(a, b, n)$:

$$\forall i < n\Big[\mathrm{Ax}_T(\beta(a,b,i)) \vee (\exists j, k < i)\,\mathrm{MP}(\beta(a,b,j), \beta(a,b,k), \beta(a,b,i)) \\ \vee (\exists j < i)\,\mathrm{Gen}(\beta(a,b,j), \beta(a,b,i))\Big].$$

The formula $\mathrm{Pr}_T(m)$ given by

$$\mathrm{Sen}(m) \wedge \exists a, b, n(\beta(a,b,n) = m \wedge B(a,b,n+1))$$

expresses that m is the Gödel number of a sentence having a formal proof in T. If φ is a sentence, $T \vdash \varphi$ if and only if $\mathfrak{N}_{\mathrm{st}} \vDash \mathrm{Pr}_T(\underline{\#\varphi})$. In particular, if φ is a Σ_1-sentence, $\mathfrak{N}_{\mathrm{st}} \vDash \varphi \implies \mathfrak{N}_{\mathrm{st}} \vDash \mathrm{Pr}_T(\underline{\#\varphi})$. In order for this property to hold in any model of PA, we are led to consider the following variants of B and Pr_T.

One defines the formula $\widetilde{B}(a, b, n)$ by

$$\forall i < n\Big[\mathrm{Ax}_T(\beta(a,b,i)) \vee (\exists j, k < i)\,\mathrm{MP}(\beta(a,b,j), \beta(a,b,k), \beta(a,b,i)) \\ \vee (\exists j < i)\,\mathrm{Gen}(\beta(a,b,j), \beta(a,b,i)) \vee \mathrm{Sat}_{\Sigma_1}(\beta(a,b,i))\Big]$$

and $\widetilde{\mathrm{Pr}}_T(m)$ by

$$\mathrm{Sen}(m) \wedge \exists a, b, n(\beta(a,b,n) = m \wedge \widetilde{B}(a,b,n+1)).$$

Finally, if φ is a sentence we write $\Box_T\varphi$ for $\widetilde{\mathrm{Pr}}_T(\underline{\#\varphi})$.

By construction the following properties hold:

Proposition 5.7.1.

(1) *If φ is a Σ_1-sentence,*

$$\mathrm{PA} \vdash \varphi \to \Box_T\varphi.$$

(2) *For any sentence ψ,*

$$\mathfrak{N}_{\mathrm{st}} \vDash \Box_T\psi \iff T \vdash \psi.$$

Proof. Let φ be a Σ_1-sentence and let $\mathfrak{M}$ be a model of PA. By Proposition 5.6.1, if $\mathfrak{M} \vDash \varphi$, it follows that $\mathfrak{M} \vDash \mathrm{Sat}_{\Sigma_1}(\underline{\#\varphi})$, and hence also $\mathfrak{M} \vDash \Box_T\varphi$. This proves (1).

Note that if φ is a Σ_1-sentence which is true in $\mathfrak{N}_{\mathrm{st}}$, then $T \vdash \varphi$. Part (2) thus follows from the construction of $\widetilde{\mathrm{Pr}}_T(m)$. □

Proposition 5.7.2. *Let φ and ψ be sentences. The operator $\Box_T$ satisfies the following properties (Loeb's axioms):*

(L1) $T \vdash \varphi \implies T \vdash \Box_T\varphi$.

(L2) $T \vdash (\Box_T\varphi \wedge \Box_T(\varphi \to \psi)) \to \Box_T\psi$.

(L3) $T \vdash \Box_T\varphi \to \Box_T\Box_T\varphi$.

Proof. (L1) By Proposition 5.7.1(2), if $T \vdash \varphi$, then $\mathfrak{N}_{\mathrm{st}} \vDash \Box_T\varphi$. Since $\widetilde{\mathrm{Pr}}_T$ is Σ_1, it follows that $\Box_T\varphi$ is satisfied in any model of PA_0, so in particular in any model of T.

(L2) Arguing in an arbitrary model of PA, it follows from modus ponens that $\mathrm{PA} \vdash (\Box_T\varphi \wedge \Box_T(\varphi \to \psi)) \to \Box_T\psi$, which implies (L2).

(L3) is a special case of (1) in Proposition 5.7.1 since $\Box_T\varphi$ is a Σ_1-sentence and $T \supseteq \mathrm{PA}$. □

Corollary 5.7.3. *Let φ and ψ be sentences. If $T \vdash \varphi \to \psi$, then $T \vdash \Box_T\varphi \to \Box_T\psi$.*

Proof. Assume $T \vdash \varphi \to \psi$. Then, by (L1), $T \vdash \Box_T(\varphi \to \psi)$. It follows that $T \vdash \Box_T\varphi \to (\Box_T\varphi \wedge \Box_T(\varphi \to \psi))$. By (L2) one deduces that $T \vdash \Box_T\varphi \to \Box_T\psi$. □

Theorem 5.7.4. *Let T be a recursive $\mathcal{L}_{ar}$-theory containing* PA. *Let φ be a sentence. Then*

$$T \vdash \Box_T(\Box_T\varphi \to \varphi) \to \Box_T\varphi.$$

Proof. There exists a formula $F(x)$ such that for any sentence θ, $F(\underline{\#\theta})$ is equal to the sentence $\Box_T\theta \to \varphi$. By Corollary 5.4.2, there exists a sentence ψ such that

$$(*) \qquad T \vdash \psi \leftrightarrow (\Box_T\psi \to \varphi).$$

In particular,

$$T \vdash \psi \to (\Box_T\psi \to \varphi);$$

hence, by Corollary 5.7.3,

$$T \vdash \Box_T \psi \to \Box_T(\Box_T \psi \to \varphi).$$

It follows from (L3) that

$$T \vdash \Box_T \psi \to (\Box_T \Box_T \psi \wedge \Box_T(\Box_T \psi \to \varphi)).$$

Since by (L2)

$$T \vdash (\Box_T \Box_T \psi \wedge \Box_T(\Box_T \psi \to \varphi)) \to \Box_T \varphi,$$

one deduces that

$$(**) \qquad T \vdash \Box_T \psi \to \Box_T \varphi.$$

From $(**)$ one gets that

$$T \vdash (\Box_T \varphi \to \varphi) \to (\Box_T \psi \to \varphi),$$

thus by $(*)$ it follows that

$$T \vdash (\Box_T \varphi \to \varphi) \to \psi.$$

By Corollary 5.7.3 one infers that

$$T \vdash \Box_T(\Box_T \varphi \to \varphi) \to \Box_T \psi,$$

and using $(**)$ one deduces that

$$T \vdash \Box_T(\Box_T \varphi \to \varphi) \to \Box_T \varphi,$$

which ends the proof. □

Corollary 5.7.5. *If $T \vdash \Box_T \varphi \to \varphi$, then $T \vdash \Box_T \varphi$.*

Proof. Indeed, if $T \vdash \Box_T \varphi \to \varphi$, then it follows from (L1) that $T \vdash \Box_T(\Box_T \varphi \to \varphi)$, so we may conclude by Theorem 5.7.4. □

Since $\Box_T \varphi \to \varphi$ is logically equivalent to $\neg \Box_T \varphi \vee \varphi$, we obtain the following corollary.

Corollary 5.7.6. *If $T \vdash \neg \Box_T \varphi$, then $T \vdash \Box_T \varphi$.* □

This corollary implies in particular the following famous result.

Theorem 5.7.7 (Gödel's Second Incompleteness Theorem)**.** *Let T be a recursive $\mathcal{L}_{ar}$-theory containing* PA*. Then if T is consistent, for any sentence φ, $T \nvdash \neg \Box_T \varphi$. In particular, let $\mathrm{Con}_T = \neg \Box_T(0 = 1)$, the sentence expressing the consistency of T. Then $T \nvdash \mathrm{Con}_T$.* □

5.8. Exercises

Exercise 5.8.1 (Presburger arithmetic)**.** We consider the language $\mathcal{L}_{\mathrm{Pres}} = \{0, +, <, 1, \equiv_n, n \geq 1\}$, where $\equiv_n$ is a binary relation for all n. *Presburger arithmetic* is the $\mathcal{L}_{\mathrm{Pres}}$-theory T_{Pres} which is given by the following axioms:

- the axioms of ordered abelian groups (cf. Exercise 3.7.9);
- an axiom stating that 1 is the smallest positive element;
- for any $n \geq 1$, an axiom φ_n of the form

$$\forall x, y\, (x \equiv_n y \leftrightarrow \exists z\, x + nz = y)$$

  and an axiom ψ_n of the form

$$\forall x \bigvee_{i=0}^{n-1} x \equiv_n \underbrace{1 + \cdots + 1}_{i \text{ times}}.$$

(1) Observe that $\mathcal{Z} = \langle \mathbb{Z}; 0, 1, +, <, \equiv_n \rangle \vDash T_{\mathrm{Pres}}$, where all symbols have their usual interpretation in the integers.

(2) Prove that T_{Pres} eliminates quantifiers and is complete.

(3) Deduce that T_{Pres} is decidable.

Exercise 5.8.2.

(1) Let $\Phi = \{\#\varphi \mid \varphi \text{ is a satisfiable } \mathcal{L}_{ar}\text{-sentence}\}$. Prove that Φ is not recursively enumerable.

(2) Let Φ_m be the set of codes $\#\varphi$ of $\mathcal{L}_{ar}$-sentences φ satisfiable by an $\mathcal{L}_{ar}$-structure of domain $\{0, \ldots, m-1\}$, with $m \geq 1$ an integer. Prove that Φ_m is primitive recursive.

(3) One considers the set Φ_{fin} of codes $\#\varphi$ of $\mathcal{L}_{ar}$-sentences φ satisfiable by a finite $\mathcal{L}_{ar}$-structure. Using the previous question and an appropriate coding, prove that Φ_{fin} is recursively enumerable.

Exercise 5.8.3. Let $\mathcal{L} = \{P, c\}$, with P a unary predicate and c a constant.

(1) Determine all countable $\mathcal{L}$-structures up to isomorphism.

(2) Deduce that two $\mathcal{L}$-structures $\mathfrak{M}$ and $\mathfrak{N}$ are elementarily equivalent precisely if the following two conditions hold:

- $\mathfrak{M} \vDash Pc$ if and only if $\mathfrak{N} \vDash Pc$, and
- $\mathfrak{M} \vDash \exists^{\geq k} x\, Qx$ if and only if $\mathfrak{N} \vDash \exists^{\geq k} x\, Qx$, for any $k \in \mathbb{N}$ and any $Q \in \{P, \neg P\}$.

(3) Prove that an $\mathcal{L}$-sentence φ is universally valid if and only if $\mathfrak{M} \vDash \varphi$ for any finite $\mathcal{L}$-structure. Deduce that the empty $\mathcal{L}$-theory is decidable.

Exercise 5.8.4. The aim of this exercise is to prove that there is a total recursive function which is not provably total Σ_1 (see p. 135 for the definition).

(1) Prove that there is a partial recursive function $h \in \mathcal{F}_2^*$ with the following properties:
- if $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $n \in \mathbb{N}$ is such that there exists $m \in \mathbb{N}$ with $\mathrm{PA} \vdash \varphi(\underline{n}, \underline{m})$, then $\mathrm{PA} \vdash \varphi\left(\underline{n}, \underline{h(a,n)}\right)$;
- if $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $n \in \mathbb{N}$ is such that there does not exist $m \in \mathbb{N}$ with $\mathrm{PA} \vdash \varphi(\underline{n}, \underline{m})$, then $(a, n) \notin \mathrm{dom}(h)$;
- otherwise, $h(a, n) = 0$.

(2) Choose $h \in \mathcal{F}_2^*$ as above, and define $g \in \mathcal{F}_3$ as follows:
- if $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $b = \#\#d$ for a formal proof d of $\forall v_0 \exists! \, v_1 \varphi(v_0, v_1)$ in PA, then $g(a, b, n) = h(a, n)$;
- otherwise $g(a, b, n) = 0$.

Prove that g is total recursive, and that it is *universal provably total* Σ_1 in the following sense: a function $f \in \mathcal{F}_1$ is provably total Σ_1 if and only if there are $a, b \in \mathbb{N}$ such that $f = \lambda n.g(a, b, n)$.

(3) Conclude.

Exercise 5.8.5 (End Extensions in Peano Arithmetic)**.** In this exercise, we shall use the Omitting Types Theorem as proved in Exercise 2.7.8. The aim is to prove the following result, due to MacDowell and Specker:

Let $\mathfrak{M}$ be a countable model of PA*. Then there exists a proper elementary extension $\mathfrak{N} \succcurlyeq \mathfrak{M}$ such that $\mathfrak{N}$ is an* end extension *of $\mathfrak{M}$: for any $m \in M$ and every $n \in N \setminus M$ we have $\mathfrak{N} \vDash m < n$.*

(1) Let $\mathfrak{M} \models \mathrm{PA}$. Prove that the *pigeonhole principle* holds in $\mathfrak{M}$: for any $\mathcal{L}_{ar}(M)$-formula $\theta(v, z)$ and any $a \in M$ we have

$$\mathfrak{M} \models [\forall x(\exists z > x)(\exists v < a)\theta(v, z)] \to (\exists v < a)\forall x(\exists z > x)\theta(v, z).$$

(2) Let $\mathfrak{M} \models \mathrm{PA}$. Let c be a constant symbol which is not in $\mathcal{L}_{ar}(M)$, and set $\mathcal{L} = \mathcal{L}_{ar}(M) \cup \{c\}$. We now consider the $\mathcal{L}$-theory $T := D(\mathfrak{M}) \cup \{c > m \mid m \in M\}$, where $D(\mathfrak{M})$ is the complete diagram of $\mathfrak{M}$ (cf. Section 3.2).
   (a) Check that T is consistent.
   (b) Let $a \in M$ and let $\theta(v, z)$ be an $\mathcal{L}$-formula such that $T \vdash \forall v(\theta(v, c) \to v < a)$ and such that $T \cup \{\exists v \theta(v, c)\}$ is consistent.
   Prove that there exists $m \in M$ with $m < a$ and such that $\mathfrak{M} \models \forall x(\exists z > x)\theta(m, z)$.
   (c) Let $a \in M$ be a non-standard element. Consider the set of formulas

$$\pi_a(v) := \{v < a\} \cup \{v \neq m \mid m \in M\}.$$

   Prove that π_a is a non-isolated partial 1-type in T.

(3) Conclude.

Exercise 5.8.6 (Tenenbaum's Theorem)**.** Let $\mathfrak{M}$ be a non-standard model of PA and let $\eta(x, y)$ be an $\mathcal{L}_{ar}$-formula with two free variables. Denote by $S_\eta(\mathfrak{M})$ the set of $A \subseteq \mathbb{N}$ such that there is $a \in M$ with

$$A = \{n \in \mathbb{N} \mid \mathfrak{M} \models \eta(\underline{n}, a)\}.$$

Denote by $S(\mathfrak{M})$ the union of all $S_\eta(\mathfrak{M})$, where η runs over the set of $\mathcal{L}_{ar}$-formulas with two free variables.

(1) Let $\eta_0(x, y)$ be an $\mathcal{L}_{ar}$-formula such that for any pair of disjoint finite subsets A and B of $\mathbb{N}$, the sentence

$$\exists x \left(\bigwedge_{i \in A} \eta_0(\underline{i}, x) \wedge \bigwedge_{j \in B} \neg \eta_0(\underline{j}, x) \right)$$

is provable in PA. Prove that $S_{\eta_0}(\mathfrak{M}) = S(\mathfrak{M})$.
[Hint: Use overspill in $\mathfrak{M}$.]

(2) Prove that there is a Σ_1-formula η_0 with two free variables such that for all $n \in \mathbb{N}$ the sentence

$$\eta_0(\underline{n}, x) \leftrightarrow \exists y(\underline{\pi(n)} \cdot y = x)$$

is provable in PA. Here, $\pi(n)$ denotes the $(n+1)$th prime number. Prove that $S_{\eta_0}(\mathfrak{M}) = S(\mathfrak{M})$.

(3) Let A and B be two disjoint recursively enumerable subsets of $\mathbb{N}$.

(a) The set of Δ_0-*formulas* is defined as the smallest set of $\mathcal{L}_{ar}$-formulas containing the atomic formulas and which is stable under $\wedge$, $\neg$ and under *bounded quantification* $(\exists x < t)$ and $(\forall x < t)$, with t a term not depending on the variable x.
Observe that there are Δ_0-formulas $\alpha(x, y)$ and $\beta(x, y)$ such that in $\mathfrak{N}_{\mathrm{st}}$, A is defined by $\exists y \alpha(x, y)$ and B by $\exists y \beta(x, y)$.

(b) Prove that for any $k \in \mathbb{N}$,

$$\mathfrak{M} \models (\forall x, y, z < \underline{k})\, \neg(\alpha(x, y) \wedge \beta(x, z)),$$

and that there is $\zeta \in M$ non-standard such that

$$\mathfrak{M} \models (\forall x, y, z < \zeta)\, \neg(\alpha(x, y) \wedge \beta(x, z)).$$

(c) Consider A and B as in Exercise 4.8.7 (that is, infinite and recursively inseparable) to deduce that $S(\mathfrak{M})$ contains a non-recursive set.

(4) If M is countable and $h : \mathbb{N} \to M$ is a bijection, one may transport the $\mathcal{L}_{ar}$-structure of $\mathfrak{M}$ via h^{-1} on $\mathbb{N}$, defining $x +' y := h^{-1}(h(x) + h(y))$, $x \cdot' y := h^{-1}(h(x) \cdot h(y))$, etc.

We now assume that the structure $\mathfrak{M}$ is *recursive*, that is, there exists a bijection h as above such that $+'$ and $\cdot'$ are recursive functions.

(a) For any fixed integer $c \in \mathbb{N}$, prove that the function $f : \mathbb{N}^2 \to \mathbb{N}$ given by $f(n, m) = 1$ if $\underbrace{m +' \cdots +' m}_{\pi(n) \text{ times}} = c$ and $f(n, m) = 0$ otherwise, is recursive.

(b) Deduce from this that $S(\mathfrak{M})$ does only contain recursive sets.

(c) Deduce Tenenbaum's Theorem:
There is no recursive non-standard model of PA.

10.1090/stml/089/06

Chapter 6

Axiomatic Set Theory

Introduction

In this final chapter, we will formalize set theory within the first-order logic framework we have developed in former chapters. The language of set theory $\mathcal{L}_\in$ has only one non-logical symbol, the binary relation symbol $\in$. We start by discussing in detail the Zermelo-Fraenkel axioms and the Axiom of Choice. In 6.3 we are finally in a position to prove the equivalence of the Axiom of Choice, of Zorn's Lemma and the existence of well-orderings.

Section 6.4 is devoted to the Axiom of Foundation and its connection with the von Neumann hierarchy. We are then able to prove some independence and relative consistency results in 6.5, like the relative consistency of the Axiom of Foundation or the relative consistency of the negation of the existence of inaccessible cardinals. In the final section we discuss a few famous independence and relative consistency results whose proofs are outside the scope of this book, like the independence of the continuum hypothesis.

6.1. The Framework

We will work in the language $\mathcal{L}_\in$, and we will consider $\mathcal{L}_\in$-structures $\mathcal{U} = \langle U; \in \rangle$ (where $\mathcal{U}$ will be called a *universe of sets*).

We call a *set* any element of U. The universe U itself is a set in the naive sense. The membership relation between two sets is given by the relation symbol $\in$.

In this way we may form the language $\mathcal{L}_{\in,U}$ (a set in the naive sense).

Definition. A naive subset D of U is a *class* if there is an $\mathcal{L}_{\in,U}$-formula $\varphi(x)$ such that $D = \varphi[\mathcal{U}]$.

Note that any set a defines a class C_a, which is given by the formula $\varphi(x)$ equal to $x \in a$. By the Extensionality Axiom (which is not yet defined!), two sets a and b are equal if and only if $C_a = C_b$.

By abuse of notation, we sometimes use $\in$ to denote membership (in the naive sense) in a class, writing $c \in D$ instead of $\mathcal{U} \vDash \varphi[c]$, where $D = \varphi[\mathcal{U}]$. This should not create any confusion.

6.2. The Zermelo-Fraenkel Axioms

Definition.

(1) The *Zermelo-Fraenkel axiom system, denoted by* ZF, is given by the following list of axioms: Extensionality, Comprehension Scheme, Pairing, Union, Power Set, Replacement Scheme, Infinity, Foundation.

(2) If one adds the the Axiom of Choice (AC) to ZF, one obtains the *axiom system* ZFC.

Remark. Some authors do not include the Axiom of Foundation in the axiom system ZF.

We will now discuss the axioms in detail.

Extensionality Axiom. $\forall x, y\,(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y)$.

It expresses that two sets having the same elements are equal.

Notation. We write $x \subseteq y$ as an abbreviation for $\forall z(z \in x \rightarrow z \in y)$.

The Extensionality Axiom is then equivalent to the following sentence: $\forall x, y\,(x \subseteq y \wedge y \subseteq x \rightarrow x = y)$.

Comprehension Axiom Scheme. For any formula $\varphi(v_0, \dots, v_n)$ in the language $\mathcal{L}_\in$, one puts an axiom of the form

$$\forall v_1, \dots, v_{n+1} \exists v_{n+2} \forall v_0 \, (v_0 \in v_{n+2} \leftrightarrow (v_0 \in v_{n+1} \wedge \varphi(v_0, \dots, v_n))) \, .$$

It expresses that if a is a set and D is a class, then the class $\{b \in a \mid b \in D\}$ is given by a set. We will sometimes denote this set by $a \cap D$.

Here are some easy consequences of the axioms stated so far:

- If a and b are two sets, then one may form their intersection $a \cap b = \{c \in a \mid c \in b\}$ and, in a similar way, their difference $a \setminus b = \{c \in a \mid c \notin b\}$.
- One obtains the existence of the empty set, denoted by $\emptyset$. Indeed, let a be an arbitrary set. Then $\emptyset = \{c \in a \mid \neg c = c\}$. The uniqueness of $\emptyset$ follows from Extensionality.
- If $a \neq \emptyset$ is a set, one obtains the existence of $\bigcap_{b \in a} b$ (as a set). To see this, choose an arbitrary $b_0 \in a$, and observe that $\bigcap_{b \in a} b = \{c \in b_0 \mid \forall x (x \in a \to c \in x)\}$.

Remark 6.2.1. Comprehension implies that there is no set containing all sets. Indeed, suppose for contradiction that $\mathcal{U} \vDash \forall z \, z \in a$ for some $a \in U$. By Comprehension there is a set b such that $\mathcal{U} \vDash \forall z (z \in b \leftrightarrow z \notin z)$, so in particular $b \in b$ if and only if $b \notin b$. This contradiction is Russell's Antinomy, and it shows that a cannot exist.

Pairing Axiom. $\forall y_1, y_2 \exists x \forall z \, (z \in x \leftrightarrow (z = y_1 \vee z = y_2))$.

It expresses that if a and b are two sets, then $\{a, b\}$ is a set.

Definition. The *ordered pair* (also called *Kuratowski pair*) of two sets a and b is the set $(a, b) := \{\{a\}, \{a, b\}\}$.

Lemma 6.2.2. *With the axioms stated so far, we have:*

(1) *The collection of ordered pairs forms a class. Moreover, there is an $\mathcal{L}_\in$-formula $\varphi(x, y)$ such that $\mathcal{U} \vDash \varphi[a, b]$ if and only if a is an ordered pair of the form $a = (b, c)$. The analogous fact holds for the second coordinate.*

(2) *One has $(b, c) = (b', c')$ if and only if $b = b'$ and $c = c'$.*

Proof. Exercise. □

Union Axiom. $\forall y \exists x \forall z\,(z \in x \leftrightarrow \exists w(z \in w \wedge w \in y))$.

It expresses that for every set a, the following class is given by a set: $\bigcup a := \{z \mid \exists w(z \in w \wedge w \in a)\}$.

Note that, by combining the Pairing Axiom and the Union Axiom, one gets that the union $a \cup b$ of two sets a and b is given by a set.

Power Set Axiom. $\forall y \exists x \forall z (z \in x \leftrightarrow z \subseteq y)$.

It postulates the existence of the set of subsets of a set, that is, for any set a the class $\mathcal{P}(a) = \{b \mid b \subseteq a\}$ is given by a set.

Lemma 6.2.3. *The axioms stated so far imply the existence of the cartesian product of two sets a and b: $a \times b = \{(x, y) \mid x \in a \wedge y \in b\}$ is a set.*

Proof. If $x \in a$ and $y \in b$, then one has $\{x\}, \{x, y\} \in \mathcal{P}(a \cup b)$, whence $(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b))$. One may conclude by Comprehension, using Lemma 6.2.2. □

One may also define triples $(x, y, z) := ((x, y), z)$ and more generally n-tuples, via $(x_1, \dots, x_{n+1}) := ((x_1, \dots, x_n), x_{n+1})$, inductively. One obtains $a \times b \times c$, and more generally $a_1 \times \cdots \times a_n$.

Definition.

- A (*binary*) *relation* R is a set of ordered pairs. One sets $\mathrm{dom}(R) := \{x \mid \exists y (x, y) \in R\}$, called the *domain* of R, and $\mathrm{im}(R) := \{y \mid \exists x (x, y) \in R\}$, called the *image* of R.
- A *function* f is a relation which is unique on the right, that is, which satisfies $\forall x, y, z\,((x, y) \in f \wedge (x, z) \in f \to y = z)$.

Remark.

- Note that if R is a relation, then $\mathrm{dom}(R)$ and $\mathrm{im}(R)$ are sets. Indeed, for $(x, y) \in R$ one has $x, y \in \bigcup(\bigcup R)$.
- By definition, a function is identified with its graph.

Notation. When f is a function, we usually write $f(x) = y$ instead of $(x, y) \in f$. Sometimes, for $x \notin \mathrm{dom}(f)$, we set $f(x) := \emptyset$. If $a = \mathrm{dom}(f)$ and $\mathrm{im}(f) \subseteq b$, we write $f : a \to b$.

Lemma 6.2.4. *Let a and b be two sets. With the axioms we have stated so far, one then gets the following:*

(1) $\{R \mid R$ *is a relation with* $\mathrm{dom}(R) \subseteq a$ *and* $\mathrm{im}(R) \subseteq b\}$ *is a set.*

(2) $\{f \mid f : a \to b\}$ *is a set.*

(3) *The collection of functions forms a class. We denote by* $\mathrm{Fn}(x)$ *an* $\mathcal{L}_\in$*-formula which defines this class.*

Proof. Exercise. □

A *family of sets*, indexed by the set I, is a function f with $\mathrm{dom}(f) = I$. One usually writes $(a_i)_{i\in I}$ for such a family, where $a_i = f(i)$.

Remark. If $(a_i)_{i\in I}$ is a family of sets with non-empty index set I, then the class $\prod_{i\in I} a_i := \{g : I \to \bigcup_{i\in I} a_i \mid \forall z(z \in I \to g(z) \in z)\}$ is given by a set. □

Definition. We say that $F \subseteq U^2$ is a *functional class* if there is an $\mathcal{L}_{\in,U}$-formula $\varphi(x, y)$ which defines F such that

$$\mathcal{U} \vDash \forall x, y_1, y_2\, (\varphi(x, y_1) \wedge \varphi(x, y_2) \to y_1 = y_2)\,.$$

The class $\mathrm{Dom}(F)$ defined by $\exists y\varphi$ is called the *Domain* of F, and the class $\mathrm{Im}(F)$ defined by $\exists x\varphi$ is called the *Image* of F.

Note that a functional class gives rise to a function in the naive sense, with domain $\mathrm{Dom}(F)$. One may also consider functional classes which correspond to naive functions between a class $D \subseteq U^n$ and U that are definable in $\mathcal{L}_{\in,U}$.

Replacement Axiom Scheme. For each formula $\varphi(x, y, v_1, \ldots, v_n)$ in the language $\mathcal{L}_\in$, one puts an axiom of the form

$$\forall v_0, v_1, \ldots, v_n[\forall x, y_1, y_2(\varphi(x, y_1, \overline{v}) \wedge \varphi(x, y_2, \overline{v}) \to y_1 = y_2) \\ \to \exists v_{n+1} \forall y(y \in v_{n+1} \leftrightarrow \exists x(x \in v_0 \wedge \varphi(x, y, \overline{v})))].$$

It expresses that if $F \subseteq U^2$ is a functional class and a is a set, then $F[a] := \{z \mid \exists u(u \in a \wedge (u, z) \in F)\}$ is a set. (It is obtained by 'replacing' every element of a by its image under F.)

The axioms stated so far are not independent. Indeed:

Lemma 6.2.5.

(1) *The Replacement Axiom Scheme implies the Comprehension Axiom Scheme.*

(2) *The Pairing Axiom is a consequence of the other axioms stated so far.*

Proof. Let $\varphi(x)$ be given. Let $F(x, y)$ be the formula $(x = y \wedge \varphi(x))$. Then $\{x \in a \mid \varphi(x)\} = F[a]$, proving (1).

To prove (2), suppose that a and b are two sets. Observe that $\emptyset \in \mathcal{P}(\emptyset) = \{\emptyset\}$, so in particular $\emptyset \neq \mathcal{P}(\emptyset)$. Let $F(x, y)$ be the formula $((x = \emptyset \wedge y = a) \vee (x = \mathcal{P}(\emptyset) \wedge y = b))$. This is a functional class, and for $c = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \mathcal{P}(\emptyset)\}$, one gets $F[c] = \{a, b\}$. □

Remark. We may work in an expansion by definition and use for example relation symbols $x \subseteq y$ (binary) and $f : x \to y$ (ternary), function symbols $x \cup y$, $x \cap y$, $x \setminus y$, $\bigcup y$, $\mathcal{P}(y)$, $\{x, y\}$, (x, y), $x \times y$, $\mathrm{dom}(R)$, $\mathrm{im}(R)$, the constant symbol $\emptyset$, etc., in the Comprehension and Replacement schemes. By Proposition 3.3.2, this does not change anything.

Recall that a set x is an *ordinal* if it is a transitive set such that $\in \restriction_{x \times x}$ defines a well-order on x, that is, a total order which is well-founded. (Well-foundedness may be expressed by the following formula: $\forall y(y \in \mathcal{P}(x) \wedge \neg y = \emptyset \to \exists z(z \in y \wedge z \cap y = \emptyset))$.) Let $\mathrm{Ord}(x)$ be an $\mathcal{L}_\in$-formula which defines the class of ordinals (in all models of the axioms stated so far). We then get a formula

$$\mathrm{Card}(x) := \mathrm{Ord}(x) \wedge \forall y(y \in x \to \text{‘there is no surjective’ } f : y \to x)$$

which defines the class of cardinals.

Notation. In what follows, we will use α, β, γ, etc., to denote only ordinals. For instance, we will write $\forall \gamma \varphi$ instead of $\forall \gamma(\mathrm{Ord}(\gamma) \to \varphi)$.

Axiom of Infinity (AI). $\exists x(\emptyset \in x \wedge \forall z(z \in x \to z \cup \{z\} \in x))$.

It postulates the existence of a set which contains $\emptyset$ and is stable under the ‘successor’ function.

Let a be a set as postulated by (AI). Applying Comprehension if necessary, we may assume that a is a set of ordinals. Let α be the least ordinal such that $\alpha \notin a$. By construction, $\emptyset \in \alpha$ and α is stable under the successor function, so α is a limit ordinal.

We let $\mathrm{Lim}(x)$ be a formula which defines the class of all limit ordinals. By what we have just seen, limit ordinals exist. One denotes by ω the smallest limit ordinal.

Axiom of Foundation (AF). $\forall x(\neg x = \emptyset \to \exists z(z \in x \wedge z \cap x = \emptyset))$.

Observe that (AF), together with the Pairing Axiom, implies that no set a contains itself as an element, since otherwise $\{a\}$ would contradict (AF).

Notation. We denote by ZF^- the axioms of ZF without (AF), and by ZFC^- the axioms of ZFC without (AF).

Remark 6.2.6.

(1) In any model of ZF^-, the ordinals satisfy the same properties as we have seen in Chapter 1. Similarly for the cardinals in models of ZFC^-.

(2) The class of ordinals is not a set. Indeed, if Ord were given by the set a, then a would be transitive and well-ordered by $\in$, so an ordinal and thus $a \in a$. But $a \notin a$ for all ordinals by Proposition 1.6.1.

Similarly, Card is not a set. Indeed, if it were given by the set a, then Ord would be given by the set $\bigcup a$.

Lemma 6.2.7 (Transfinite induction). *Let $\mathcal{U} \vDash \mathrm{ZF}^-$, and let $\varphi(x)$ be an $\mathcal{L}_{\in,U}$-formula. Then $\mathcal{U}$ satisfies the following induction property:*

$$\varphi(0) \wedge \forall\gamma(\varphi(\gamma) \to \varphi(\gamma+1)) \\ \wedge \forall\gamma[(\mathrm{Lim}(\gamma) \wedge \forall\delta(\delta < \gamma \to \varphi(\delta))) \to \varphi(\gamma)] \to \forall\gamma\varphi(\gamma).$$

Proof. If $\mathcal{U}$ satisfies

$$\varphi(0) \wedge \forall\gamma(\varphi(\gamma) \to \varphi(\gamma+1)) \wedge \forall\gamma[(\mathrm{Lim}(\gamma) \wedge \forall\delta(\delta < \gamma \to \varphi(\delta))) \to \varphi(\gamma)]$$

and $\mathcal{U} \vDash \neg\varphi[\alpha]$ for some ordinal α, it is enough to choose a minimal such α to get a contradiction. □

Theorem 6.2.8 (Definition by transfinite recursion)**.** *Let $\mathcal{U} \models \mathrm{ZF}^-$, and let G be a functional class with $\mathrm{Dom}(G) = U^{n+1}$. Then there is a unique functional class F with $\mathrm{Dom}(F) = U^n \times \mathrm{Ord}$ such that one has $F(\overline{w}, \alpha) = G(\overline{w}, F \restriction_{\{\overline{w}\}\times\alpha})$ for every tuple of sets $\overline{w}$ and every ordinal α.*

Proof. The key idea is to approximate F by functions. We prove first that for every $\overline{w}$ and every ordinal β there is a unique function $f_{\overline{w},\beta}$ with domain β such that $f_{\overline{w},\beta}(\alpha) = G(\overline{w}, \{\overline{w}\} \times f_{\overline{w},\beta} \restriction_\alpha)$ for all $\alpha < \beta$. The uniqueness is clear by transfinite induction.

Fix $\overline{w}$. To establish existence, let us prove by induction on β that there is a function $f_{\overline{w},\beta}$ with domain β such that

$$(*)_{\overline{w},\beta} \qquad \forall\alpha\big(\alpha < \beta \to f_{\overline{w},\beta}(\alpha) = G(\overline{w}, \{\overline{w}\} \times f_{\overline{w},\beta} \restriction_\alpha)\big).$$

If $\beta = 0$, set $f_{\overline{w},\beta} = \emptyset$.

If $\beta = \beta' + 1$ and $f_{\overline{w},\beta'}$ is a function which satisfies $(*)_{\overline{w},\beta'}$, one may simply set $f_{\overline{w},\beta} = f_{\overline{w},\beta'} \cup \{(\beta', G(\overline{w}, \{\overline{w}\} \times f_{\overline{w},\beta'}))\}$.

Finally, if β is a limit ordinal, we consider the set $X_{\overline{w},\beta}$ of all functions f such that there exists $\beta' < \beta$ with $\mathrm{dom}(f) = \beta'$ and f satisfies $(*)_{\overline{w},\beta'}$. By Replacement and uniqueness, $X_{\overline{w},\beta}$ is indeed a set. Then, again by uniqueness, $\bigcup_{f' \in X_{\overline{w},\beta}} f'$ is a function, and it clearly satisfies $(*)_{\overline{w},\beta}$.

We may now set $(\overline{w}, \beta, y) \in F :\Leftrightarrow$ for any function f with domain $\beta + 1$ satisfying $(*)_{\overline{w},\beta+1}$ one has $f(\beta) = y$. □

Example 6.2.9 (Applications of transfinite recursion)**.**

(1) The operations of ordinal arithmetic (ordinal addition, multiplication and exponentiation) may be defined by transfinite recursion (see Remark 1.6.5).

(2) The $\aleph$-hierarchy of infinite cardinals is given by a functional class $\aleph : \mathrm{Ord} \to \mathrm{Card}$. Indeed, it is sufficient to apply Theorem 6.2.8 to the functional class $G : U \to U$ defined as follows:
   - $G(0) = \omega$.
   - If $f : \alpha \to \beta$ for two ordinals α, β, then $G(f)$ equals the least cardinal κ such that $\kappa > f(\alpha')$ for every $\alpha' < \alpha$.
   - Finally, if x is not a function between two ordinals, then $G(x) = \emptyset$.

(3) The *von Neumann hierarchy*. By transfinite recursion, one defines a functional class $\alpha \mapsto V_\alpha$ as follows:
- $V_0 = \emptyset$.
- $V_{\alpha+1} = \mathcal{P}(V_\alpha)$.
- $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ for λ a limit ordinal.

Proposition 6.2.10 (ZF^-)**.** *The ordinal ω endowed with the ordinal operations (addition, multiplication and the successor function), with $0 = \emptyset$ and $<$ given by $\in$, is a model of* PA.

Proof. Exercise. □

6.3. The Axiom of Choice

Axiom of Choice (AC).

$$\forall f[(\mathrm{Fn}(f) \wedge \emptyset \notin \mathrm{im}(f)) \to \exists g\,(\mathrm{Fn}(g) \wedge \mathrm{dom}(g) = \mathrm{dom}(f) \wedge \forall x(x \in \mathrm{dom}(g) \to g(x) \in f(x)))].$$

It expresses that the product of a family of non-empty sets is non-empty.

Definition. Let a be a set. A *choice function* on a is a function $h : \mathcal{P}(a)' := \mathcal{P}(a) \setminus \{\emptyset\} \to a$ such that $h(A) \in A$ for all $A \in \mathcal{P}(a)'$.

Proposition 6.3.1. (AC) *is equivalent to the existence of a choice function on every set a.*

Proof. Suppose (AC). For any set a, we then have $\prod_{A\in\mathcal{P}(a)'} A \neq \emptyset$. Any element of this product is a choice function on a.

Conversely, let $(a_i)_{i\in I}$ be a family of sets with $a_i \neq \emptyset$ for all $i \in I$. Let $a = \bigcup_{i\in I} a_i$ and $h : \mathcal{P}(a)' \to a$ be a choice function on a. Then $h \circ f \in \prod_{i\in I} a_i$, where $f : I \to \mathcal{P}(a)'$, $f(i) := a_i$. □

Theorem 6.3.2. *The following are equivalent in the theory* ZF^-*:*

(1) (AC).

(2) *Zorn's Lemma.*

(3) *Zermelo's Theorem* (*Wohlordnungssatz*).

Proof. (1)⇒(2): By way of contradiction, let us suppose that $\langle X, < \rangle$ is an inductive partial order without maximal element. We consider the set

$$\mathcal{T} = \{T \in \mathcal{P}(X) \mid T \text{ is totally ordered by } <\}.$$

As X is inductive and there is no maximal element in X, for any $T \in \mathcal{T}$, the set $B(T) := \{x \in X \mid x > t \ \forall t \in T\}$ is non-empty. By (AC), there is a function $b : \mathcal{T} \to X$ such that $b(T) \in B(T)$ for any $T \in \mathcal{T}$.

Let G be the following functional class:

- if g is a function with $\mathrm{dom}(g) \in \mathrm{Ord}$ and $\mathrm{im}(g) \in \mathcal{T}$, then $G(g) = b(\mathrm{im}(g))$;
- $G(g) = \emptyset$, otherwise.

Applying Theorem 6.2.8, we obtain a functional class F with $\mathrm{Dom}(F) = \mathrm{Ord}$ such that $F(\alpha) = G(F \restriction_\alpha)$ for every ordinal α. One shows easily by induction that $F(\alpha) \in X$ for every α and that

$$\alpha < \beta \Rightarrow F(\alpha) < F(\beta).$$

In particular, F is injective as a naive function. The class F^{-1}, defined by $(x, \alpha) \in F^{-1} :\Leftrightarrow (\alpha, x) \in F$, is thus a functional class. We have $F^{-1}[X] = \mathrm{Ord}$, so Ord is a set by the Replacement Axiom Scheme. This contradicts Remark 6.2.6(2).

(2)⇒(3): Let a be a set. We have to show that a admits a well-order. Consider $X := \{(b, R) \mid b \in \mathcal{P}(a) \text{ and } R \text{ is a well-order on } b\}$. It is easy to see that X is a set (exercise).

On X, we define a partial order as follows:

$$(b, R) \leq (b', R') \ :\Leftrightarrow \ b \text{ is an initial segment of } (b', R') \text{ and } R' \restriction_b = R.$$

This partial order is inductive. Indeed, if $(b_i, R_i)_{i \in I}$ is a totally ordered subset of X, then $(b, R) := (\bigcup_{i \in I} b_i, \bigcup_{i \in I} R_i)$ is an upper bound of this subset. By Zorn's Lemma, there is an element $(\tilde{b}, \tilde{R}) \in X$ which is maximal for $\leq$. If $\tilde{b} \neq a$, there exists $y \in a \setminus \tilde{b}$. We set $b' = \tilde{b} \cup \{y\}$ and $R' := \tilde{R} \cup \{(x, y) \mid x \in \tilde{b}\}$. It is then clear that R' is a well-order on b' which prolongates the one on $\tilde{b}$, contradicting the maximality of $(\tilde{b}, \tilde{R})$.

(3)⇒(1): Let a be a set. By hypothesis, a may be well-ordered, say by $<$. The function $f : \mathcal{P}(a)' \to a$ which associates to any non-empty

subset of a its smallest element is a choice function on a. We conclude by Proposition 6.3.1. □

Remark 6.3.3 (Skolem's Paradox)**.** If ZFC is consistent, it has a (necessarily infinite) model. Since $\mathcal{L}_\in$ is countable, ZFC thus admits a countable model $\mathfrak{M}$ by the Downward Löwenheim-Skolem Theorem. But there exist uncountable sets in $\mathfrak{M}$, for example $\aleph_1$ or $\mathbb{R}$.

Explanation: The notion of 'countability' depends on the model of ZFC one works in, so it is relative. Being countable in the sense of $\mathfrak{M}$ and being countable in the sense of the (naive) ground model of set theory in the metatheory is not the same thing. Moreover, the base set M of $\mathfrak{M}$ is a set from the naive point of view, and a proper class from the point of view of $\mathfrak{M}$.

More generally, the notion of cardinality depends on the model. For instance, the set of natural numbers $\mathbb{N}$ and the set of real numbers $\mathbb{R}$ (both taken in the sense of $\mathfrak{M}$) are both countable from the point of view of the underlying naive ground model. But the bijection between these two sets which exists as a naive set is not even represented by a functional class in $\mathfrak{M}$. Indeed, otherwise, by Replacement, it would be given by a function in the sense of $\mathfrak{M}$.

6.4. The von Neumann Hierarchy and the Axiom of Foundation

In this section, we will work in $\mathcal{U} \vDash \mathrm{ZF}^-$.

Definition. Let a be a set. By recursion on $n \in \omega$, one defines $a_0 := a$, $a_{n+1} := a_n \cup \bigcup a_n$. The set $\mathrm{tcl}(a) := \bigcup_{n\in\omega} a_n$ is then called the *transitive closure* of a.

Lemma 6.4.1 (ZF^-)**.** *The set* $\mathrm{tcl}(a)$ *is the smallest transitive set containing* a *as a subset. More precisely, the following properties hold:*

(1) $a \subseteq \mathrm{tcl}(a)$.

(2) $\mathrm{tcl}(a)$ *is a transitive set.*

(3) *If* $a \subseteq t$ *with* t *a transitive set, then* $\mathrm{tcl}(a) \subseteq t$. *In particular,* $a \subseteq b \Rightarrow \mathrm{tcl}(a) \subseteq \mathrm{tcl}(b)$.

(4) *If* a *is transitive, then* $\mathrm{tcl}(a) = a$.

(5) *If* $b \in a$, *then* $\mathrm{tcl}(b) \subseteq \mathrm{tcl}(a)$.

(6) $\mathrm{tcl}(a) = a \cup \bigcup_{b\in a} \mathrm{tcl}(b)$.

Proof. (1) and (2) are clear. To prove (3), one shows by induction that $a_n \subseteq t$ for all $n \in \omega$. (4) follows from (1-3).

(5) One has $b \in a \Rightarrow b \in \mathrm{tcl}(a) \Rightarrow b \subseteq \mathrm{tcl}(a) \Rightarrow \mathrm{tcl}(b) \subseteq \mathrm{tcl}(a)$, where the first implication follows from (1), the second from (2), and the last one from (3).

(6) One has $\mathrm{tcl}(a) \supseteq a \cup \bigcup_{b\in a} \mathrm{tcl}(b)$ by (1) and (5). To prove the other inclusion, it suffices by (3) to prove that $a \cup \bigcup_{b\in a} \mathrm{tcl}(b)$ is transitive, which is clear. □

Recall the definition of the von Neumann hierarchy: $V_0 := \emptyset$, $V_{\alpha+1} := \mathcal{P}(V_\alpha)$, $V_\lambda := \bigcup_{\alpha<\lambda} V_\alpha$ (for λ a limit ordinal).

We define the class V by the formula $\exists \alpha\, x \in V_\alpha$, which we will denote by $V(x)$. Informally, one thus has '$V = \bigcup_{\alpha\in \mathrm{Ord}} V_\alpha$'.

Definition. If a is a set, the *rank* of a is defined as

$$\mathrm{rk}(a) := \begin{cases} \text{the least } \gamma \text{ such that } a \in V_{\gamma+1}, \text{ if such a } \gamma \text{ exists;} \\ \infty, \text{ otherwise.} \end{cases}$$

Lemma 6.4.2.

(1) V_α *is a transitive set for any ordinal* α.

(2) $\beta \leq \alpha \Rightarrow V_\beta \subseteq V_\alpha$.

(3) $V_\alpha = \{x \in V \mid \mathrm{rk}(x) < \alpha\}$.

(4) *If* $x \in V$ *and* $y \in x$, *then* $y \in V$ *and* $\mathrm{rk}(y) < \mathrm{rk}(x)$.

(5) *If* $x \in V$, *then* $\mathrm{rk}(x) = \sup\{\mathrm{rk}(y) + 1 \mid y \in x\}$.

(6) *If* $x \in V$ *is transitive, then* $\{\mathrm{rk}(y) \mid y \in x\}$ *is an ordinal* α.

(7) *One has* $\mathrm{rk}(\alpha) = \alpha$ *for every* α. *In particular,* $\alpha \in V$ *and* $\{\beta \in V_\alpha \mid \beta \in \mathrm{Ord}\} = \alpha$.

(8) *Let* x *be a set. Then* $x \in V$ *if and only if* $x \subseteq V$.

(9) *Assume* (AC). *If* $x \in V$ *is transitive, then* $x \in V_{\mathrm{card}(x)^+}$.

Proof. (1) & (2) By transfinite induction on α, one shows that V_α is transitive and that $V_\beta \subseteq V_\alpha$ for all $\beta \leq \alpha$. The cases $\alpha = 0$ and α a limit ordinal are clear. Now suppose $\alpha = \gamma+1$. Since V_γ is a transitive set by the induction hypothesis, $\mathcal{P}(V_\gamma) = V_\alpha$ is transitive, too. If $\beta < \alpha$, then $\beta \leq \gamma$ and so inductively $V_\beta \subseteq V_\gamma$, whence $V_\beta \in V_\alpha$ and finally $V_\beta \subseteq V_\alpha$ by transitivity.

(3) If $x \in V$, then $\mathrm{rk}(x) < \alpha \Leftrightarrow (\exists \beta < \alpha) x \in V_{\beta+1} \Leftrightarrow x \in V_\alpha$.

(4) Let $\alpha = \mathrm{rk}(x)$. Then $x \in V_{\alpha+1} = \mathcal{P}(V_\alpha)$. For $y \in x$, one obtains $y \in V_\alpha$ and hence $y \in V$ and $\mathrm{rk}(y) < \alpha$ by (3).

(5) For $x \in V$, set $\alpha = \sup\{\mathrm{rk}(y) + 1 \mid y \in x\}$. By (4), one has $\alpha \leq \mathrm{rk}(x)$. Since $\mathrm{rk}(y) < \alpha$ for any $y \in x$, it follows from (3) that $x \subseteq V_\alpha$, whence $x \in V_{\alpha+1}$ and finally $\alpha \geq \mathrm{rk}(x)$ by definition.

(6) Suppose $x \in V$ is transitive and $\beta < \mathrm{rk}(x)$ is given. By (5) there exists $y \in x$ such that $\beta \leq \mathrm{rk}(y)$. Choose such an element y with minimal rank. If $z \in y$, then $z \in x$ (by transitivity of x) and $\mathrm{rk}(z) < \mathrm{rk}(y)$ by (4), so $\mathrm{rk}(z) < \beta$ by minimality of $\mathrm{rk}(y)$. This proves that $y \subseteq V_\beta$, and thus $y \in V_{\beta+1}$, and hence $\mathrm{rk}(y) \leq \beta$. It follows that $\mathrm{rk}(y) = \beta$.

(7) We prove by transfinite induction that $\alpha \in V$ and $\mathrm{rk}(\alpha) = \alpha$, the case $\alpha = 0$ being clear. Suppose that the result holds for all $\beta < \alpha$. Then $\beta \in V_{\beta+1} \subseteq V_\alpha$ for all $\beta < \alpha$, so $\alpha \subseteq V_\alpha$ and thus $\alpha \in V_{\alpha+1}$. We get $\mathrm{rk}(\alpha) = \sup\{\beta + 1 \mid \beta < \alpha\} = \alpha$ by (5).

(8) $x \in V \Rightarrow x \subseteq V$ follows from (4). Conversely, if x is a set such that $x \subseteq V$, then $\{\mathrm{rk}(y)+1 \mid y \in x\}$ is given by a set by Replacement. For $\alpha = \sup\{\mathrm{rk}(y) + 1 \mid y \in x\}$ we thus infer that $x \subseteq V_\alpha$, and so $x \in V_{\alpha+1}$.

(9) By (6), the set $\{\mathrm{rk}(y) \mid y \in x\}$ is equal to an ordinal α. Since $\alpha = \sup\{\beta + 1 \mid \beta < \alpha\}$, by (5) we get $\mathrm{rk}(x) = \alpha$. Thus $x \in V_{\mathrm{card}(x)^+}$ by (3), as $\mathrm{card}(\alpha) \leq \mathrm{card}(x)$ and hence $\alpha < \mathrm{card}(x)^+$. □

Theorem 6.4.3. *Let $\mathcal{U} \models \mathrm{ZF}^-$. The following are equivalent:*

(1) $\mathcal{U} \models$ (AF).

(2) $\mathcal{U} \models \forall x V(x)$.

Proof. (2)⇒(1): Let x be a non-empty set. We have to find an element y of x such that $y \cap x = \emptyset$. By hypothesis, every set is in V. We choose $y \in x$ such that $\mathrm{rk}(y)$ is minimal. Then $y \cap x = \emptyset$ by Lemma 6.4.2(4).

(1)⇒(2): Let x be a set. Put $y := \mathrm{tcl}(x)$, and consider the set $z := \{t \in y \mid t \notin V\}$. We have $x \subseteq y$. By Lemma 6.4.2(8), in order to prove $x \in V$, it suffices to prove that every element of y is in V, in other words that $z = \emptyset$. If z were not empty, by (AF) there would exist $t \in z$ with $t \cap z = \emptyset$. Let us consider such a t. Then, for $u \in t$, we would get $u \in y$ (by transitivity of y) and thus $u \in V$ (since $t \cap z = \emptyset$). But then $t \in V$ by Lemma 6.4.2(8), which is a contradiction. □

Remark. As the elements of V are constructed starting from the empty set (by a transfinite procedure), Theorem 6.4.3 expresses that (AF) is equivalent to the fact that every set is constructed from the empty set.

Remark 6.4.4. In the theory ZFC^-, the following are equivalent:

(1) (AF).

(2) There is no sequence $(a_i)_{i\in\omega}$ with $a_{i+1} \in a_i$ for all $i \in \omega$.

Proof. (1)⇒(2): (This implication does not use (AC).) If $(a_i)_{i\in\omega}$ is a sequence of sets, consider $a = \{a_i \mid i \in \omega\}$. By (AF), there exists $b \in a$ such that $b \cap a = \emptyset$. Hence for some $n \in \omega$ one has $a_n \cap a = \emptyset$, so in particular $a_{n+1} \notin a_n$.

(2)⇒(1): Let $a \neq \emptyset$ be a set which contradicts (AF). This means that for every $b \in a$ one has $b \cap a \neq \emptyset$. By (AC) there exists a function $f : a \to a$ such that $f(b) \in b$ for every $b \in a$. Choose $a_0 \in a$, and define recursively a sequence $(a_i)_{i\in\omega}$, putting $a_{n+1} = f(a_n)$. □

Lemma 6.4.5.

(1) *If $x \in V$, then $\bigcup x, \mathcal{P}(x)$ and $\{x\}$ are in V. The rank of these sets is strictly smaller than* $\mathrm{rk}(x) + \omega$.

(2) *If $x, y \in V$, then $x \times y, x \cup y, x \cap y, \{x, y\}, (x, y)$ and x^y are in V, too. Moreover, the rank of these sets is strictly smaller than* $\max\{\mathrm{rk}(x), \mathrm{rk}(y)\} + \omega$.

Proof. Exercise. □

Remark. As the Extensionality Axiom (which expresses in some sense that there are only sets), the Axiom of Foundation restricts the universe of sets to the place where the usual mathematics take place:

- The usual objects of mathematics (for instance $\mathbb{N}$ and $\mathbb{R}$) are in V (cf. Exercise 6.7.1).
- If we work in ZFC^-, then any (first-order) structure has an isomorphic copy in V. (We suppose that the signature $\sigma^{\mathcal{L}_0}$ of the language we consider is finite, to simplify the presentation.) Indeed, suppose that $\mathfrak{M} = \langle M; R_i, c_j, f_k\rangle$ is an $\mathcal{L}_0$-structure, and let $g : M \cong \mathrm{card}(M) = \kappa$ be a bijection. There exists a unique $\mathcal{L}_0$-structure $\mathfrak{N}$ with base set κ such that g is an $\mathcal{L}_0$-isomorphism between $\mathfrak{M}$ and $\mathfrak{N}$. Then $\kappa \in V_{\kappa+1}$, and so $\mathfrak{N} \in V_{\kappa+\omega}$ by Lemma 6.4.5.
- This remains true for structures outside the first-order context. Consider for example the case of a topological space $(X, \mathcal{T})$, with X a set and $\mathcal{T} \subseteq \mathcal{P}(X)$ the set of open subsets of X. Then if $g : X \cong \kappa$ is a bijection, one may argue as before to prove that $(X, \mathcal{T})$ admits an isomorphic copy in $V_{\kappa+\omega}$.

6.5. Some Results on Incompleteness, Independence and Relative Consistency

In this section, we will suppose that the $\mathcal{L}_\in$-formulas and the proofs are coded in ZF^-. To this aim, we may for example appeal to the coding we have given in arithmetic and use that if $\mathcal{U} \vDash \mathrm{ZF}^-$ and $\omega \in U$, then $\langle \omega; 0, +, \cdot, \mathrm{succ}, \in\restriction_\omega\rangle \vDash \mathrm{PA}$ (see Proposition 6.2.10). We continue to write $\#\varphi$ for the code of φ.

Gödel's incompleteness results have their analogues in set theory. We will state them and leave the proofs to the reader – the arguments are analogous to those in the case of Peano arithmetic. However, coding formulas and formal proofs is slightly simpler in set theory. Let us note that ZF^-, ZF, ZFC^- and ZFC are recursive theories.

Theorem 6.5.1 (Gödel's First Incompleteness Theorem)**.** *Let T be a recursive and consistent $\mathcal{L}_\in$-theory such that $T \supseteq \mathrm{ZF}^-$. Then T is incomplete.* □

Remark. If ZF^- is consistent, then (AF) is *independent* of ZF^-, that is, $\mathrm{ZF}^- \nvdash$ (AF) and $\mathrm{ZF}^- \nvdash \neg$(AF). (This is shown in Exercise 6.7.7.) Similarly, (AC) is then independent of ZF and (CH) is independent of ZFC.

All of (AF), (AC) and (CH) are mathematically meaningful statements. In contrast to this, in the case of arithmetic, assuming that PA is consistent, the sentences which we proved to be independent of PA were rather far fetched and involved the diagonal method.

Theorem 6.5.2 (Gödel's Second Incompleteness Theorem)**.** *Let T be a recursive and consistent $\mathcal{L}_\in$-theory such that $T \supseteq \mathrm{ZF}^-$. Then $T \nvdash \mathrm{Con}(T)$.* □

We work in a model $\mathcal{U}$ of ZF^-. One may then code the satisfaction in $\mathcal{U}$ as follows. Let $\mathcal{L}$ be a (finite) language and $\mathfrak{A} = \langle A; (Z^{\mathfrak{A}})_{Z\in\sigma^{\mathcal{L}}}\rangle$ an $\mathcal{L}$-structure with $\mathfrak{A} \in U$. One identifies the set of assignments (with values in $\mathfrak{A}$) with A^ω, which is an element of U. The following lemma may be proved by induction on the height of a formula, which corresponds to an induction on ω. We leave the details as an exercise.

Lemma 6.5.3. *There exists a functional class which to any triple $(\mathfrak{A}, \#\varphi, \alpha)$ in $\mathcal{U}$, with $\mathfrak{A}$ an $\mathcal{L}$-structure, φ an $\mathcal{L}$-formula and α an assignment with values in $\mathfrak{A}$, associates 1 if $\mathfrak{A} \vDash \varphi[\alpha]$, and 0 otherwise.*

In particular, if $\mathfrak{A}$ is an $\mathcal{L}$-structure in $\mathcal{U}$, then the collection $\#\,\mathrm{Th}(\mathfrak{A}) = \{\#\varphi \mid \varphi$ is an $\mathcal{L}$-sentence such that $\mathfrak{A} \vDash \varphi\}$ is given by a set in $\mathcal{U}$. □

A *relative consistency* result has the following form: given two theories T_1 and T_2, the consistency of T_1 is proved to imply the consistency of T_2. The proof method will be to construct a model of T_2 from a model of T_1.

Let us start with a result which establishes a relation between set theory and arithmetic. One verifies without difficulty that the proof of Proposition 6.2.10 may be done in ZF^-. As the structure $\langle\omega; +, \times, S, 0, <\rangle$ is a set in $\mathcal{U}$, Lemma 6.5.3 entails the following result.

Proposition 6.5.4. *One has $\mathrm{ZF}^- \vdash \mathrm{Con}(\mathrm{PA})$. In particular, if ZF^- is consistent, then Peano arithmetic* PA *is consistent, too.* □

Let $\mathcal{U} \vDash \mathrm{ZF}^-$. If X is a non-empty class in U, one may consider the (naive) $\mathcal{L}_\in$-structure $\langle X; \in\restriction_X\rangle$. In the proofs of the relative consistency results we will present, we will construct classes X such that if $\mathcal{U} \vDash T_1$, then $\langle X; \in\restriction_X\rangle \vDash T_2$, whence the desired relative consistency result.

Notation. We will sometimes write $X \vDash \varphi$ instead of $\langle X; \in\restriction_X\rangle \vDash \varphi$.

Definition (Relativization)**.** Let $\mathcal{L}$ be a language, and let $F(v_0)$ be an $\mathcal{L}$-formula. For every $\mathcal{L}$-formula φ one defines, by induction on $\mathrm{ht}(\varphi)$, an $\mathcal{L}$-formula φ^F, the *relativization of φ to F*:

- $\varphi^F := \varphi$ if φ is an atomic formula.
- $(\varphi \wedge \psi)^F := (\varphi^F \wedge \psi^F)$ and $[\neg\varphi]^F := \neg[\varphi^F]$.
- $[\exists x\varphi]^F := \exists x(F(x) \wedge \varphi^F)$.

Proposition 6.5.5. *Let $\mathcal{U} \vDash \mathrm{ZF}^-$, and let $X \subseteq U$ be a class.*

(1) *Suppose that $X = F[\mathcal{U}] = G[\mathcal{U}]$. For every $\mathcal{L}_\in$-formula φ, the formulas φ^F and φ^G are then equivalent in $\mathcal{U}$. One may thus write φ^X instead of φ^F, if one is only interested in the formula up to equivalence.*

(2) *For every $a_1, \dots, a_n \in X$ and formula $\varphi(x_1, \dots, x_n)$, one has $\mathcal{U} \vDash \varphi^X[\overline{a}]$ if and only if $X \vDash \varphi[\overline{a}]$.*

Proof. (1) The proof is an easy induction on $\mathrm{ht}(\varphi)$ and left as an exercise.

(2) The proof is by induction on $\mathrm{ht}(\varphi)$, the only non-trivial case being the case when φ is of the form $\exists x_0\psi$. In this case, one has

$$\mathcal{U} \vDash \varphi^X[a_1, \dots, a_n] \iff \mathcal{U} \vDash \exists x_0(F(x_0) \wedge \psi^X)[a_1, \dots, a_n]$$

$\iff$ there exists $b \in U$ such that $\mathcal{U} \vDash F[b]$ and $\mathcal{U} \vDash \psi^X[b, \overline{a}]$

$\iff$ there exists $b \in X$ such that $\mathcal{U} \vDash \psi^X[b, \overline{a}]$

$\iff$ there exists $b \in X$ such that $X \vDash \psi[b, \overline{a}] \iff X \vDash \varphi[\overline{a}]$. $\square$

Definition. Let X be a class defined by an $\mathcal{L}_\in$-formula $F(v_0)$. One says that an $\mathcal{L}_\in$-formula $\varphi(x_1, \dots, x_n)$ is *absolute for X* if one has $\mathcal{U} \vDash \forall x_1, \dots, x_n \left(\bigwedge_{i=1}^n F(x_i) \to (\varphi \leftrightarrow \varphi^X)\right)$.

Definition. The set of Δ_0-formulas is the smallest set of $\mathcal{L}_\in$-formulas which contains the atomic formulas and which is stable under boolean combinations and *bounded quantification* (if φ is a Δ_0-formula and x, y are two distinct variables, then $\exists x(x \in y \wedge \varphi)$ and $\forall x(x \in y \to \varphi)$ are Δ_0-formulas, too).

Lemma 6.5.6.

(1) *Assume that X is a non-empty class which is transitive (that is, $z \in y \in X \Rightarrow z \in X$). Then all Δ_0-formulas are absolute for X.*

Moreover, the set of formulas which are absolute for X is stable under boolean combinations and bounded quantification.

(2) *The following properties may be expressed by Δ_0-formulas: $x \subseteq y$, $x = \emptyset$, $x = y \cup \{y\}$, 'x is transitive', $z = \{x, y\}$, $y = \bigcup x$, $z = x \times y$.*

Proof. (1) Atomic formulas are absolute for every non-empty class. Moreover, for any class X, the set of formulas which are absolute for X is stable under boolean combinations. We now prove that if X is a transitive (non-empty) class and if $\varphi(x, y, v_1, \dots, v_n)$ is absolute for X, then the formula $\exists x(x \in y \wedge \varphi)$ is absolute for X, too. For elements $b, c_1, \dots, c_n \in X$, one has the following equivalences:

$$\begin{aligned}
&\mathcal{U} \vDash (\exists x(x \in y \wedge \varphi))^X [b, \overline{c}] \\
\iff &\mathcal{U} \vDash \left(\exists x(F(x) \wedge x \in y \wedge \varphi^X)\right)[b, \overline{c}] \\
\iff &\text{there exists } a \in b \cap X \text{ such that } \mathcal{U} \vDash \varphi^X[a, b, \overline{c}] \\
\iff &\text{there exists } a \in b \cap X \text{ such that } \mathcal{U} \vDash \varphi[a, b, \overline{c}] \\
\iff &\text{there exists } a \in b \text{ such that } \mathcal{U} \vDash \varphi[a, b, \overline{c}] \\
\iff &\mathcal{U} \vDash (\exists x(x \in y \wedge \varphi))[b, \overline{c}].
\end{aligned}$$

The first equivalence holds by definition, the third one follows from the induction hypothesis and the fourth one from the transitiviy of X. Stability under bounded universal quantification follows as well, since $\forall x(x \in y \to \varphi)$ is equivalent to $\neg\exists x(x \in y \wedge \neg\varphi)$.

The proof of (2) is straightforward. For example, the transitivity of x is expressed by the Δ_0-formula: $\forall y\,(y \in x \to \forall z(z \in y \to z \in x))$. □

Let X be a class. We say that a functional class $G(x, y)$ with $\mathrm{Dom}(G) \supseteq X$ is an *absolute functional class* for X (in $\mathcal{U}$) if $G(x, y)$ is absolute for X and if for any $a \in X$, the unique $b \in U$ such that $\mathcal{U} \vDash G(a, b)$ is in X. The following remark follows easily from the definitions:

Remark 6.5.7. A composition of absolute functional classes is an absolute functional class (for X). □

Lemma 6.5.8. *We work in $\mathcal{U} \vDash \mathrm{ZF}^-$.*

(1) *Any non-empty transitive class satisfies the Extensionality Axiom.*

(2) *Let X be a class defined in $\mathcal{U}$, and let G be an absolute functional class for X. Then $X \vDash \forall x \exists! y G(x, y)$.*

Moreover, if φ is absolute for X, then $\exists x(x \in G(z) \wedge \varphi)$ and $\forall x(x \in G(z) \to \varphi)$ are absolute for X, where x, z are distinct variables.

(3) *The Union Axiom holds in V and in any V_α with $\alpha > 0$.*

(4) *The Pairing Axiom holds in V and in any V_λ with λ a limit ordinal.*

(5) *Suppose that $\mathcal{U} \vDash (\forall x \in X)(\exists y \in X)\mathcal{P}(x) \cap X = y$ for some non-empty transitive class X. Then the Power Set Axiom holds in X. In particular, the Power Set Axiom holds in V and in V_λ for any limit ordinal λ.*

Moreover, $y = \mathcal{P}(x)$ is a functional class which is absolute for V and V_λ with λ a limit ordinal.

Proof. (1) The Extensionality Axiom relativized to X is given by the sentence $(\forall y \in X)(\forall z \in X)\,((\forall x \in X)(x \in y \leftrightarrow x \in z) \to y = z)$. Since X is transitive, if $y, z \in X$, then $y, z \subseteq X$. The result follows.

(2) The first part is clear. Now assume that G is an absolute functional class for X and that $\varphi(\overline{v}, x, z)$ is absolute for X. Given $\overline{a}, b$ from X, let $c = G(b)$ (computed in $\mathcal{U}$ or in X, which amounts to the same by the first part of (2)). Then $\mathcal{U} \vDash \exists x(x \in G(z) \wedge \varphi)[\overline{a}, b]$ if and only if $\mathcal{U} \vDash \exists x(x \in y \wedge \varphi)[\overline{a}, c]$, and similarly for X in place of $\mathcal{U}$. The absoluteness of $\exists x(x \in G(z) \wedge \varphi)$ then follows from Lemma 6.5.6(1).

(3) The formula $y = \bigcup x$ is Δ_0 by Lemma 6.5.6, so absolute for transitive classes. As $\mathrm{rk}(\bigcup x) \leq \mathrm{rk}(x)$, one has $x \in V_\alpha \Rightarrow \bigcup x \in V_\alpha$ for all α and in particular $x \in V \Rightarrow \bigcup x \in V$. One concludes by (2).

(4) One has $x, y \in V_\alpha \Rightarrow \{x, y\} \in V_{\alpha+1}$. It follows in particular that $x, y \in V_\lambda \Rightarrow \{x, y\} \in V_\lambda$ for λ a limit ordinal. One deduces that $(x, y) \mapsto \{x, y\}$ is given by a functional class which is absolute for V and V_λ (for λ a limit ordinal), and one may conclude by (2).

(5) One has $\mathcal{U} \vDash \forall x \in X \exists y \in X(\mathcal{P}(x) \cap X = y)$ if and only if $\mathcal{U} \vDash \forall x \in X \exists y \in X \forall z \in X(z \subseteq x \leftrightarrow z \in y)$. The latter sentence is just

the Power Set Axiom relativized to X, since $z \subseteq x$ is absolute for X by the transitivity of X. The proof of the remaining part of (5) is left as an exercise. □

Lemma 6.5.9. *The formulas* $\mathrm{Ord}(x)$ *and* $\mathrm{Card}(x)$ *are absolute for* V *as well as for* V_λ *if* λ *is a limit ordinal.*

Proof. We first consider $\mathrm{Ord}(x)$. The transitivity of x and the fact that $\in|_x$ defines a total order are expressed by Δ_0-formulas and are thus absolute in both cases. The items (2) and (5) of Lemma 6.5.8 entail that the following formula is absolute:

$$\forall z\,(z \in \mathcal{P}(x) \wedge z \neq \emptyset \rightarrow \exists u(u \in z \wedge \forall w(w \in z \rightarrow w \notin u)))\,.$$

This establishes the absoluteness of well-foundedness.

The formula $\mathrm{Ord}(x) \wedge \forall y(y \in x \rightarrow \neg\exists f \in \mathcal{P}(x \times y)\, f : x \cong y)$ is equivalent to $\mathrm{Card}(x)$. One proves easily that the formula $f : x \cong y$ (in the three variables f, x, y) is absolute for V and for V_λ if λ is a limit ordinal, and that the functional class $z = x \times y$ is an absolute functional class in both cases (exercise). This proves the absoluteness of $\mathrm{Card}(x)$ in both cases, using Lemma 6.5.8(2) and Remark 6.5.7. □

Definition. We work in ZF^-. Let κ be a cardinal.

- We say κ is a *strong limit* cardinal if for all $\mu < \kappa$ one has $2^\mu < \kappa$.
- We say κ is *inaccessible* (strongly) if it is strong limit, regular and $> \aleph_0$.

Example. By transfinite recursion, one defines a cardinal hierarchy as follows: $\beth_0 := \aleph_0$, $\beth_{\alpha+1} := 2^{\beth_\alpha}$, and $\beth_\lambda := \sup_{\alpha<\lambda} \beth_\alpha$ for λ a limit ordinal.

For any limit ordinal λ, $\beth_\lambda$ is then a strong limit cardinal. But as $\mathrm{cof}(\beth_\lambda) = \mathrm{cof}(\lambda)$ in this case, $\beth_\lambda$ is singular in general.

Lemma 6.5.10. *Let* $\mathcal{U} \models \mathrm{ZF}^-$*, and let* $X = V$ *or* $X = V_\omega$*, or* $X = V_\kappa$ *for* κ *an inaccessible cardinal. In the last case, we assume in addition that* $\mathcal{U} \models (\mathrm{AC})$*. Then* X *satisfies the Replacement Axiom Scheme and the Axiom of Foundation.*

Proof. Choose a formula $F(x)$ which defines X. Let $G(v_0, v_1)$ be a formula (with parameters from X) which defines a functional class in the

structure $\langle X, \in\restriction_X \rangle$. Then the formula $H(v_0, v_1) = F(v_0) \wedge F(v_1) \wedge G^F$ defines a functional class in $\mathcal{U}$. Set $b := H[a] = \{H(c) \mid c \in a\}$, where a is a set in X.

- If $X = V$, then $b \in V$ by Lemma 6.4.2(8), since $b \subseteq V$ and b is a set.
- If $X = V_\omega$, then, as a is finite, b is a finite subset of V_ω, so $b \subseteq V_n$ for some $n \in \omega$ and hence $b \in V_\omega$.
- If $X = V_\kappa$ for an inaccessible cardinal κ, essentially the same argument works. One proves by transfinite induction that $\mathrm{card}(V_\alpha) < \kappa$ for all $\alpha < \kappa$. (Since we assume $\mathcal{U} \vDash$ (AC), we may use cardinalities.) For α a successor ordinal, one uses that κ is strongly limit; for α a limit ordinal, one uses the regularity of κ.

  Now, if $a \in V_\kappa$, then $a \in V_\alpha$ for some $\alpha < \kappa$ and thus $a \subseteq V_{\alpha+1}$. It follows that $\mathrm{card}(b) \leq \mathrm{card}(a) < \kappa$. Moreover, one has $b \subseteq V_\kappa$. Since κ is regular, $\sup\{\mathrm{rk}(c) + 1 \mid c \in b\} < \kappa$ and hence $b \in V_\kappa$.

This proves the Replacement scheme in all three cases.

In order to prove that (AF) holds, we consider $\emptyset \neq a \in X$. It follows that $a \subseteq X$ in all three cases, as X is transitive. For any $b \in a$ of minimal rank, one has $a \cap b = \emptyset$, and any such b is in X. One concludes, since the formula $a \cap b = \emptyset$ is absolute for X. □

Lemma 6.5.11. *One has $V \vDash$ (AI), $V_\lambda \vDash$ (AI) for any limit ordinal $\lambda > \omega$, and $V_\omega \vDash \neg$(AI).*

Proof. One has $\omega \in V$, $\omega \in V_\lambda$ and $\omega \notin V_\omega$. The details are left to the reader. □

Lemma 6.5.12. *If $\mathcal{U} \vDash \mathrm{ZFC}^-$, then $V \vDash$ (AC) and $V_\kappa \vDash$ (AC), for κ an inaccessible cardinal.*

Proof. Let $(X_i)_{i \in I}$ be an element of V_κ. Then $I \in V_\kappa$ and every element $g \in \prod_{i \in I} X_i$ is in V_κ. For V, one concludes by the same argument. □

Theorem 6.5.13 (Relative consistency of (AF))**.**

(1) *If* $\mathcal{U} \models \mathrm{ZF}^-$*, then* $V \models \mathrm{ZF}$*. In particular, the consistency of* ZF^- *entails the consistency of* ZF*.*

(2) *If* $\mathcal{U} \models \mathrm{ZFC}^-$*, then* $V \models \mathrm{ZFC}$*. In particular, the consistency of* ZFC^- *entails the consistency of* ZFC*.*

Proof. It suffices to combine the preceding lemmas, taking into account the fact that the Replacement scheme implies the Comprehension scheme (cf. Lemma 6.2.5). □

Theorem 6.5.14. *If* $\mathcal{U} \models \mathrm{ZF}^-$*, then* $V_\omega \models \mathrm{ZFC}-(\mathrm{AI})+\neg(\mathrm{AI})$*. In particular,* $\mathrm{ZF}^- \models \mathrm{Con}(\mathrm{ZFC} - (\mathrm{AI}) + \neg(\mathrm{AI}))$*.*

Proof. We have proved everything in the lemmas but $V_\omega \models (\mathrm{AC})$. Observe that every element a of V_ω is a finite set and in bijection with an element of ω. Such a bijection f as well as the well-order on a induced by f is in V_ω. □

Let (IC) be the statement 'There exists an inaccessible cardinal'.

Theorem 6.5.15. *Let* $\mathcal{U} \models \mathrm{ZFC}^-$ *and* $\kappa \in U$ *be an inaccessible cardinal. Then* $V_\kappa \models \mathrm{ZFC}$*. In particular,* $\mathrm{ZFC}^- + (\mathrm{IC}) \models \mathrm{Con}(\mathrm{ZFC})$*.*

Proof. All axioms of ZFC^- hold in V_κ by the preceding lemmas. □

By the Second Incompleteness Theorem, it follows from Theorem 6.5.15 that $\mathrm{ZFC} \nvdash (\mathrm{IC})$. The following theorem states the corresponding relative consistency result. We will give a direct proof which does not rely on the Second Incompleteness Theorem.

Theorem 6.5.16. *If* ZFC *is consistent, then* $\mathrm{ZFC} + \neg(\mathrm{IC})$ *is consistent, too.*

Proof. Let $\mathcal{U} \models \mathrm{ZFC}$. We may suppose that $\mathcal{U} \models (\mathrm{IC})$. Let κ be the smallest inaccessible cardinal in $\mathcal{U}$. Then $V_\kappa \models \mathrm{ZFC}$ by Theorem 6.5.15. To conclude, it suffices to prove that $V_\kappa \models \neg(\mathrm{IC})$, a fact which follows from the following observations:

- $y = \mathcal{P}(x)$, $\mathrm{Ord}(x)$ and $\mathrm{Card}(x)$ are absolute formulas for V_κ (cf. Lemma 6.5.8 and Lemma 6.5.9).

- 'λ is a regular cardinal' is absolute for V_κ. [Indeed, it is easy to see that this property may be expressed by the formula $\neg(\exists\alpha < \lambda)(\exists f : \alpha \to \lambda \text{ cofinal})$.]
- 'λ is a strong limit cardinal' is absolute for V_κ. [Indeed, this property may be expressed by the following formula (in λ): $(\forall\alpha < \lambda)\neg(\exists f : \mathcal{P}(\alpha) \to \lambda \text{ surjective})$.] □

Remark 6.5.17. If ZFC is consistent, then

$$\text{ZFC} \nvdash \text{Con(ZFC)} \to \text{Con(ZFC} + \text{(IC))}.$$

Proof. Assume $\text{ZFC} \vdash \text{Con(ZFC)} \to \text{Con(ZFC}+\text{(IC))}$. Then we have in particular $\text{ZFC}+\text{(IC)} \vdash \text{Con(ZFC)} \to \text{Con(ZFC}^- + \text{(IC))}$, so $\text{ZFC}+\text{(IC)} \vdash \text{Con(ZFC}+\text{(IC))}$ by Theorem 6.5.15. By the Second Incompleteness Theorem, this means that ZFC + (IC) is inconsistent, which implies the inconsistency of ZFC by assumption. □

6.6. A Glimpse of Further Independence and Relative Consistency Results

At the end of this chapter, we will mention some important further results on independence and relative consistency in axiomatic set theory. We will not give any proofs, but we will sketch some key ideas of the methods behind these results. This part is meant as a motivation for further reading. The books by Krivine [**6**] and Kunen [**7**] are excellent references.

The results in the following theorem may be obtained, in a rather elementary way, by the *method of Fraenkel-Mostowski*. They will be treated entirely in the exercise section (cf. Exercise 6.7.7 and Exercise 6.7.8).

Theorem 6.6.1.

(1) *If* ZF *is consistent, then so is* $\text{ZFC}^- + \neg(\text{AF})$.

(2) *If* ZF *is consistent, then so is* $\text{ZF}^- + \neg(\text{AC})$.

It is possible to replace $\text{ZF}^- + \neg(\text{AC})$ by $\text{ZF} + \neg(\text{AC})$ in the second part of the preceding theorem, but then the proof gets more involved (see below).

Recall that the Generalized Continuum Hypothesis (GCH) is given by the sentence $\forall\alpha(2^{\aleph_\alpha} = \aleph_{\alpha+1})$.

Theorem 6.6.2 (Gödel)**.** *If* ZF *is consistent, then so is the theory* ZFC + (GCH)*.*

Gödel obtains this result using the *universe of constructible sets L*. The construction of L is similar to that of V inside a model $\mathcal{U}$ of ZF^-. Here is an outline of the construction.

- One uses the formalization in $\mathcal{U} \vDash$ ZF of the syntax and the satisfaction for structures $\langle a; \in\restriction_a\rangle$, for a in $\mathcal{U}$.
- One proves that there is a functional class $\mathcal{D}$ which to any set associates the set of its parameter definable subsets, that is, if a is a set, the set $\mathcal{D}(a)$ equals

$$\{b \in \mathcal{P}(a) \mid \text{there are } n \in \omega, \text{ an } \mathcal{L}_\in\text{-formula } \varphi(v_0, \dots, v_n) \text{ and } c_1, \dots, c_n \in a \text{ with } b = \{c_0 \in a \mid \langle a; \in\restriction_a\rangle \vDash \varphi[c_0, c_1, \dots, c_n]\}\}.$$

  By convention, one sets $\mathcal{D}(\emptyset) := \mathcal{P}(\emptyset) = \{\emptyset\}$.
- Using induction, one defines $L_0 := \emptyset$, $\mathcal{L}_{\alpha+1} := \mathcal{D}(L_\alpha)$, and $L_\lambda := \bigcup_{\alpha<\lambda} L_\alpha$ for λ a limit ordinal. Finally, one sets '$L = \bigcup_\alpha L_\alpha$', that is, L is defined by the formula $L(x) = \exists\alpha(\mathrm{Ord}(\alpha) \wedge x \in L_\alpha)$.
- As for the von Neumann hierarchy, one may establish certain basic properties, for instance, $\alpha \leq \beta \Rightarrow L_\alpha \subseteq L_\beta$ and the transitivity of the L_α. In this way, one gets a continuous hierarchy of transitive sets $(L_\alpha)_{\alpha\in\mathrm{Ord}}$.
- One defines a rank rk_L as in the case of V, and one may prove that $\mathrm{rk}_L(\alpha) = \alpha$, that is, $L_\alpha \cap \mathrm{Ord} = \alpha$. In particular, L is a proper class.
- The proof that $L \vDash$ ZF is very similar to the one for V. It also follows that L has the same ordinals as $\mathcal{U}$.
- One proves that in $\mathcal{U}$, $L^L = L$ holds. In other words, L satisfies the *Axiom of Constructibility* $\forall x\, L(x)$. To prove this, one establishes that the functional class $\mathcal{D}$ is absolute for any transitive class X which is a model of ZF with the Power Set Axiom taken

away, and then that the same absoluteness statement holds for the functional class $\alpha \mapsto L_\alpha$.

- In order to prove that $L \vDash (\mathrm{AC})$, one uses transfinite recursion to construct a well-ordering on L_α such that if $\alpha \leq \beta$, then L_α is an initial segment of L_β. In the successor step, one uses the well-ordering L_α to construct a well-ordering on $L_\alpha^{<\omega}$ (the set of finite sequences in L_α), then on $L_{\alpha+1}$, also enumerating the (codes) of $\mathcal{L}_\in$-formulas.
- Finally, $L \vDash (\mathrm{GCH})$ is established as follows. One proves first that, in any model of ZF^-, one has $\mathrm{card}(L_\alpha) = \mathrm{card}(\alpha)$ for every infinite ordinal α. Then, one proves that, in L, one has $L_\kappa = \{x \mid \mathrm{card}(\mathrm{tcl}(x)) < \kappa\}$ for every infinite cardinal κ. Thus, $L \vDash \mathcal{P}(\kappa) \subseteq L_{\kappa^+}$, and so $L \vDash (\mathrm{GCH})$.

Remark. A weaker statement, namely that the consistency of ZF entails the consistency of ZFC, is the content of Exercise 6.7.6.

Theorem 6.6.3 (Cohen)**.**

(1) *If* ZF *is consistent, then so is* $\mathrm{ZFC} + \neg(\mathrm{CH})$.

(2) *If* ZF *is consistent, then so is* $\mathrm{ZF} + \neg(\mathrm{AC})$.

In particular, combining the results by Gödel and Cohen, one gets the following result concerning the cardinality of the continuum.

Corollary 6.6.4. *If* ZF *is consistent, the Continuum Hypothesis* (*CH*) *is independent of* ZFC.

Cantor had formulated (CH) and thus raised the problem of the cardinality of the continuum in 1878. It was then put forward by Hilbert as the first problem of his list of 23 important problems in mathematics which he presented at the International Congress of Mathematicians in Paris in 1900.

Contrary to the constructions of models of set theory we have seen so far (and to the ones which will be treated in the exercises), Cohen's construction *is not done inside the ground model* $\mathcal{U}$. The method Cohen introduced in 1964 to prove his results, termed *forcing*, allows for constructions of models which *extend* a given model.

Weakenings of the Axiom of Choice. The following two variants of the Axiom of Choice are often considered.

Axiom of Dependent Choice (DC).

$$\forall r \forall a \forall x_0 \big[(x_0 \in a \wedge r \subseteq a^2 \wedge \forall x \in a \, \exists y \in a \, (x, y) \in r) \\ \rightarrow \exists f (f : \omega \rightarrow a \wedge f(0) = x_0 \wedge \forall n \in \omega \, ((f(n), f(n+1)) \in r)) \big].$$

Axiom of Countable Choice (CC).

$$\forall f [(\mathrm{Fn}(f) \wedge \mathrm{dom}(f) = \omega \wedge \emptyset \notin \mathrm{im}(f)) \\ \rightarrow \exists g \, (\mathrm{Fn}(g) \wedge \mathrm{dom}(g) = \omega \wedge \forall x (x \in \mathrm{dom}(g) \rightarrow g(x) \in f(x)))].$$

It expresses that the product of a countable family of non-empty sets is non-empty.

Proposition 6.6.5. *One has* (AC) $\Rightarrow$ (DC) $\Rightarrow$ (CC).

Proof. (AC)$\Rightarrow$(DC) Let $h : \mathcal{P}'(a) \rightarrow a$ be a choice function on a. By induction on ω, define a function $f : \omega \rightarrow a$, setting $f(0) := x_0$, $f(n+1) := h(\{y \in a \mid (f(n), y) \in r\})$. Clearly, f is as required.

(DC)$\Rightarrow$(CC) Let $(X_n)_{n \in \omega}$ be a countable family of non-empty sets. Set $Y_n := \{n\} \times X_n$ and $a := \bigcup_{n \in \omega} Y_n$, and let

$$r := \{(x, y) \in a^2 \mid \text{ there exists } n \in \omega \text{ such that } (x, y) \in Y_n \times Y_{n+1}\}.$$

By (DC) there exists a function $f : \omega \rightarrow a$ such that $f(n) \in Y_n$ for all $n \in \omega$. Then $g \in \prod_{n \in \omega} X_n$, where $g(n) := \pi((f(n))$, with π the projection onto the second coordinate. □

The usual construction of a set of real numbers which is not Lebesgue measurable may be done in ZFC. It proves the following:

Proposition 6.6.6.

ZFC $\vdash$ *'there exists a subset of* $\mathbb{R}$ *which is not Lebesgue measurable'*

Let us mention a theorem which is more difficult (its proof uses forcing).

Theorem 6.6.7 (Solovay, 1970)**.** *If* ZFC+(IC) *is consistent, then the theory* ZF + (DC) + *'every subset of* $\mathbb{R}$ *is Lebesgue measurable' is consistent, too.*

6.7. Exercises

Exercise 6.7.1. We work in $\mathcal{U} \vDash \mathrm{ZF}^-$, and we suppose that the sets $\mathbb{N}, \mathbb{Z}, \ldots$ are defined in the usual manner.

(1) Prove that the sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, C^0([0,1], \mathbb{C})$ are in $V_{\omega \cdot 2}$.

(2) Compute the ranks of the sets in (1).

Exercise 6.7.2 (Mostowski Collapse)**.** We work in $\mathcal{U} \vDash \mathrm{ZF}^-$. Let X be a class and $R \subseteq X \times X$ a definable relation on X.

We say R is *set-like* if for any a in X, the class $\mathrm{pred}_R(a)$ of R-predecessors of a, defined by $R(x, a)$, is given by a set; R is *well-founded* if any non-empty subset a of X contains an R-minimal element; finally, R is *extensional* if $\mathrm{pred}_R(a) = \mathrm{pred}_R(b)$ implies $a = b$.

(1) Assume that $R \subseteq X \times X$ is set-like. By induction on α, for $x \in X$, define the relation $\mathrm{rk}_R(x) \geq \alpha$ as follows:
   - $\mathrm{rk}_R(x) \geq 0$ for all $x \in X$;
   - $\mathrm{rk}_R(x) \geq \alpha + 1$ if and only if there is $y \in \mathrm{pred}_R(x)$ such that $\mathrm{rk}_R(y) \geq \alpha$;
   - if λ is a limit, then $\mathrm{rk}_R(x) \geq \lambda$ if and only if $\mathrm{rk}_R(x) \geq \alpha$ for all $\alpha < \lambda$.

   Set $\mathrm{rk}_R(x) := \infty$ if $\mathrm{rk}_R(x) \geq \alpha$ for all α; otherwise, $\mathrm{rk}_R(x)$ is defined as the least α such that $\mathrm{rk}_R(x) \ngeq \alpha + 1$. ($\mathrm{rk}_R$ is called the *foundation rank*.)

   Prove that R is well-founded if and only if rk_R takes ordinal values on X.

(2) Assume now that R is well-founded and set-like.
   (a) Prove that if F is a functional class with Domain X and Image contained in Ord such that $R(a, b)$ implies $F(a) < F(b)$, then $\mathrm{rk}_R(x) \leq F(x)$ for all $x \in X$.
   (b) Prove that the Image of rk_R is either an ordinal or the whole of Ord.
   (c) Prove that there is a unique functional class π with $\mathrm{Dom}(\pi) = X$ such that for every a in X one has $\pi(a) = \pi[\mathrm{pred}_R(a)]$. This π is called the *Mostowski Collapse* of (X, R). Moreover, prove that $\mathrm{Im}(\pi)$ is a transitive subclass of V.

(3) Suppose that R is well-founded, set-like and extensional, and let π be the Mostowski Collapse. Prove that π induces a naive isomorphism between (X, R) and $(\mathrm{Im}(\pi), \in\restriction_{\mathrm{Im}(\pi)})$.

(4) Suppose that X is a proper class and that R defines a set-like *well-ordering* (that is, a total order which is well-founded) on X. Observe that R is extensional. Prove that $\mathrm{Im}(\pi) = \mathrm{Ord}$, that is, π induces a naive order isomorphism between (X, R) and $(\mathrm{Ord}, <)$.
Example: Let $X = \mathrm{Ord}^{<\omega}$ be the class of finite sequences of ordinals. For $s = (s_0, \dots, s_{n-1})$ and $t = (t_0, \dots, t_{m-1})$ from $\mathrm{Ord}^{<\omega}$ set $R(s, t)$ if and only if
- $\max(s) < \max(t)$, or
- $\max(s) = \max(t)$ and $n < m$, or
- $\max(s) = \max(t)$, $n = m$, $s \neq t$ and $s_k < t_k$, where k is the smallest index where s and t differ.

Prove that R is a set-like well-ordering on X.

Exercise 6.7.3 (Reflection Principle)**.** We work in some $\mathcal{U} \vDash \mathrm{ZF}^-$.

(1) A class of ordinals $X \subseteq \mathrm{Ord}$ is called *CLUB* if it is closed (that is, for every subset $x \subseteq X$, one has $\sup x \in X$) and unbounded in Ord.
Observe that the intersection of two CLUB classes is CLUB.

(2) Let $(W_\alpha)_{\alpha \in \mathrm{Ord}}$ be a *continuous hierarchy of sets*, that is, a functional class $\mathcal{W} : \mathrm{Ord} \to U$, $\mathcal{W}(\alpha) = W_\alpha$, such that
- $W_\alpha \subseteq W_\beta$ for all $\alpha \leq \beta$ and
- $W_\lambda = \bigcup_{\alpha<\lambda} W_\alpha$ for any limit ordinal λ.

Let W be the 'union' of the W_α, that is, the class defined by the formula $\exists \alpha\, x \in W_\alpha$. Given an $\mathcal{L}_\in$-formula $\varphi(x_1, \dots, x_n)$, we say that W_α *reflects* φ if

$$\mathcal{U} \vDash \forall x_1, \dots, x_n \left(\bigwedge_{i=1}^{n} x_i \in W_\alpha \to \left(\varphi^W(\overline{x}) \leftrightarrow \varphi^{W_\alpha}(\overline{x}) \right) \right).$$

(a) Observe that the ordinals α such that W_α reflects φ form a class.

(b) Prove the following General Reflection Principle: For every formula $\varphi(\overline{x})$, the class of ordinals such that W_α reflects φ contains a CLUB.

[Hint: Proceed by induction on the height of φ.]

(c) Deduce the usual Reflection Principle: *For any formula $\varphi(\overline{x})$, one has*

$$\mathrm{ZF} \vDash \forall y \exists \alpha \big(y \in V_\alpha \wedge \forall \overline{x} \big(\varphi(\overline{x}) \leftrightarrow \varphi^{V_\alpha}(\overline{x}) \big) \big).$$

Exercise 6.7.4 (Independence of the Replacement Axiom Scheme)**.** The *Zermelo axioms* Z are given by the axioms of ZF without the Replacement scheme. We work in $\mathcal{U} \vDash \mathrm{ZF}^-$.

(1) Prove that if $\lambda > \omega$ is a limit ordinal, then $V_\lambda \vDash \mathrm{Z}$.

(2) Prove that $V_{\omega 2}$ does not satisfy the Replacement scheme.

[Hint: Consider the functional class sending α to $\omega + \alpha$.]

(3) Deduce that if Z is consistent, then it does not imply the Replacement scheme. Similarly, prove that if Z+(AC) is consistent, then it does not imply the Replacement scheme.

Exercise 6.7.5 (Non-finite axiomatizability of ZF)**.** The aim of this exercise is to prove that if $T \supseteq \mathrm{ZF}$ is consistent, then T is not finitely axiomatizable.

(1) Let $\mathcal{U} \vDash \mathrm{ZF}$, and let $X \subseteq U$ be a transitive class which is also a model of ZF. Prove that for any ordinal $\beta \in X$ one has $V_\beta^X = V_\beta \cap X$, where V_β^X denotes 'V_β computed in X'.

(2) Let $\mathcal{U} \vDash \varphi$, where φ is a sentence such that $\varphi \vdash \mathrm{ZF}$. Using the Reflection Principle (cf. Exercise 6.7.3) prove that there is α in U such that $V_\alpha \vDash \varphi$.

(3) Conclude.

(4) Prove that if ZF^- is consistent, then it is not finitely aximatizable.

(5) Prove the following sharpening: If $T \supseteq \mathrm{ZF}$ is consistent, then there is no sentence φ such that φ together with the Comprehension scheme axiomatizes T.

Exercise 6.7.6 (Relative consistency of (AC))**.** We work in $\mathcal{U} \vDash \mathrm{ZF}$. In this exercise, we assume that the set of $\mathcal{L}_\in$-formulas is coded in ω.

(1) The class of *ordinal definable* sets is given by the $\mathcal{L}_\in$-formula $\mathrm{OD}(x)$ which expresses the following: 'There exists α, a formula $\varphi(z, y_0, \dots, y_{n-1})$ and a sequence $(\alpha_0, \dots, \alpha_{n-1})$ of ordinals $< \alpha$ such that x is the only element of V_α with $V_\alpha \vDash \varphi[x, \alpha_0, \dots, \alpha_{n-1}]$.'

(a) Prove that if there are a (naive) $\mathcal{L}_\in$-formula $\Phi(x)$ with parameters from Ord such that a is *defined by* $\Phi(x)$, that is, $\Phi[\mathcal{U}] = \{a\}$, then a is in OD.

[Hint: Use the Reflection Principle (Exercise 6.7.3).]

(b) Prove that there is a (naive) $\mathcal{L}_\in$-formula $\Phi_{\mathrm{OD}}(x, y)$ without parameters such that a set a is in OD if and only if there is an ordinal α such that a is defined by $\Phi_{\mathrm{OD}}(x, \alpha)$.

[Hint: Use that any $\#\varphi$ is an ordinal and that any finite sequence of ordinals may be coded by an ordinal (Exercise 6.7.2).]

(c) Prove that the class of formulas in one free variable with parameters from Ord may be well-ordered (cf. Exercise 6.7.2) by an $\emptyset$-definable set-like relation. Deduce the same for the class OD.

(2) The class of *hereditarily ordinal definable* sets is given by the formula $\mathrm{HOD}(x)$ which expresses that every element of $\mathrm{tcl}(\{x\})$ is in OD.

(a) Prove that all ordinals as well as V_ω are in HOD.

(b) Prove that HOD is an $\emptyset$-definable transitive class, and that a set a is in HOD if and only if it is in OD and all its elements are in HOD.

(c) Prove that $\mathrm{HOD} \vDash \mathrm{ZF}$.

(d) Prove that $\mathrm{HOD} \vDash (\mathrm{AC})$.

(e) Conclude that if ZF is consistent, then ZFC is consistent.

(3) (a) Prove that $V_\omega^{\mathrm{HOD}} = V_\omega$.

(b) An $\mathcal{L}_\in$-sentence is said to be *arithmetical* if all its quantifiers are relativized to V_ω. Prove that if an arithmetical sentence is provable in ZFC, then it is provable in ZF.

Exercise 6.7.7 (Fraenkel-Mostowski models I – independence of (AF))**.** We work in $\langle U; \in \rangle = \mathcal{U} \vDash \mathrm{ZF}^-$. Let F be a functional class which defines a bijection between U and itself. Set $x \in' y :\Leftrightarrow x \in F(y)$ and $\mathcal{U}' = \langle U; \in' \rangle$.

(1) Prove that $\mathcal{U}'$ is a model of ZF^- which satisfies (AC) if $\mathcal{U}$ does.

(2) An *atom* is a set a such that $a = \{a\}$. Prove that one may choose F such that $\mathcal{U}'$ contains an atom. If $\mathcal{U} \vDash$(AF), prove that there is F such that the set $\mathcal{A}$ of atoms in $\mathcal{U}'$ is in bijection with ω.

(3) Prove that if ZF^- (resp. ZFC^-) is consistent, then so is ZF^- + ¬(AF) (resp. ZFC^- + ¬(AF)).

Exercise 6.7.8 (Fraenkel-Mostowski models II – relative consistency of ¬(AC))**.** We work in $\mathcal{U} \vDash \mathrm{ZF}^-$ and assume that $\mathcal{U}$ contains a non-empty set of atoms $\mathcal{A}$.

(1) By transfinite induction, define $W_0 = \mathcal{A}$, $W_{\alpha+1} = \mathcal{P}(W_\alpha)$, and $W_\lambda = \bigcup_{\alpha<\lambda} W_\alpha$ for λ a limit ordinal. Let W be the class defined by the formula $\exists \alpha\, x \in W_\alpha$.
   (a) Prove that all W_α are transitive sets and that one has $\alpha \leq \beta \Rightarrow W_\alpha \subseteq W_\beta$.
   (b) Prove that $W \vDash \mathrm{ZF}^-$.
   (c) Prove that an element $a \in W$ is an atom if and only if $a \in W_0$.
   [Hint: One may use an appropriate notion of rank in W.]
   (d) Prove that W satisfies

$$\forall a (a \neq \emptyset \to \exists b \in a\, (b = \{b\} \vee \forall x \in a\, (x \notin b))).$$

   (e) Prove that $\mathcal{U} \vDash \forall x (W^W(x) \leftrightarrow W(x))$.

Now assume that the class of atoms of $\mathcal{U}$ is given by the set $\mathcal{A}$ which is in bijection with ω, and that $\mathcal{U} \vDash \forall x W(x)$. (Note that if ZF^- is consistent, such a model of ZF^- exists by the first part, combined with Exercise 6.7.7.)

(2) Let σ_0 be a permutation of $W_0 = \mathcal{A}$.
   (a) Prove that for any α, σ_0 extends uniquely to an automorphism σ_α of $(W_\alpha, \in \restriction_{W_\alpha})$. Moreover, prove that if $\beta \leq \alpha$, then $\sigma_\alpha \restriction_{W_\beta} = \sigma_\beta$.

(b) Deduce that there is a (unique) functional class σ which extends σ_0 and induces a (naive) automorphism of $\mathcal{U}$.

(c) Let $\Phi(x_1, \dots, x_n)$ be an $\mathcal{L}_\in$-formula without parameters. Prove that

$$\mathcal{U} \vDash \forall x_1 \dots \forall x_n [\Phi(x_1, \dots, x_n) \leftrightarrow \Phi(\sigma(x_1), \dots, \sigma(x_n))].$$

(d) Prove that $\sigma(\alpha) = \alpha$ for every ordinal α.

(3) The class of *ordinal and atom definable* sets is given by the $\mathcal{L}_\in$-formula $\mathrm{OAD}(x)$ which expresses the following: 'There exists a formula $\varphi(z, y_0, \dots, y_{n-1}, z_0, \dots, z_{m-1})$, an ordinal α, a sequence $(\alpha_0, \dots, \alpha_{n-1})$ of ordinals $< \alpha$ and a sequence $(a_0, \dots, a_{m-1})$ of atoms such that x is the only element of W_α with $W_\alpha \vDash \varphi[x, \alpha_0, \dots, \alpha_{n-1}, a_0, \dots, a_{m-1}]$.'

(a) Prove that if there is a (naive) $\mathcal{L}_\in$-formula $\Phi(x)$ with parameters from Ord and $\mathcal{A}$ which defines the set c, then c is in OAD.

[Hint: For this and what follows, proceed as in Exercise 6.7.6.]

(b) Prove that there is a (naive) $\mathcal{L}_\in$-formula $\Phi_{\mathrm{OAD}}(x, y, z)$ such that a set c is in OAD if and only if there is an ordinal α and a finite sequence of atoms s such that c is defined by $\Phi_{\mathrm{OAD}}(x, \alpha, s)$.

(c) Let $c \subseteq \mathcal{A}^2$ be a total order on $\mathcal{A}$. Prove that c is not in OAD.

(4) The class of *hereditarily ordinal and atom definable* sets is given by the formula $\mathrm{HOAD}(x)$ which expresses that every element of $\mathrm{tcl}(\{x\})$ is in OAD.

(a) Prove that $\mathcal{A}$ and every ordinal is in HOAD.

(b) Prove that $\mathrm{HOAD} \vDash \mathrm{ZF}^- + \neg(\mathrm{AC}) + \neg(\mathrm{AF})$.

(c) Conclude that if ZF^- is consistent, so is the theory $\mathrm{ZF}^- + \neg(\mathrm{AC}) + \neg(\mathrm{AF})$.

Bibliography

[1] S. Barry Cooper, *Computability theory*, Chapman & Hall/CRC, Boca Raton, FL, 2004. MR2017461

[2] René Cori and Daniel Lascar, *Mathematical logic*, Part 1, Oxford University Press, 2010.

[3] René Cori and Daniel Lascar, *Mathematical logic*, Oxford University Press, Oxford, 2001. A course with exercises. Part II; Recursion theory, Gödel's theorems, set theory, model theory; Translated from the 1993 French original by Donald H. Pelletier; With a foreword to the original French edition by Jean-Louis Krivine and a foreword to the English edition by Wilfrid Hodges. MR1830848

[4] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical logic*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1994. Translated from the German by Margit Meßmer. MR1278260

[5] Thomas Jech, *Set theory*: *The third millennium edition, revised and expanded*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. MR1940513

[6] Jean-Louis Krivine, *Théorie des ensembles*, Nouvelle bibliothèque mathématique, Cassini, 1998.

[7] Kenneth Kunen, *Set theory*: *An introduction to independence proofs*, Studies in Logic and the Foundations of Mathematics, vol. 102, North-Holland Publishing Co., Amsterdam-New York, 1980. MR597342

[8] David Marker, *Model theory*: *An introduction*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002. MR1924282

[9] Bruno Poizat, *A course in model theory*: *An introduction to contemporary mathematical logic*, Universitext, Springer-Verlag, New York, 2000. Translated from the French by Moses Klein and revised by the author. MR1757487

[10] Hartley Rogers Jr., *Theory of recursive functions and effective computability*, 2nd ed., MIT Press, Cambridge, MA, 1987. MR886890

[11] Robert I. Soare, *Recursively enumerable sets and degrees*: *A study of computable functions and computably generated sets*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1987. MR882921

[12] Katrin Tent and Martin Ziegler, *A course in model theory*, Lecture Notes in Logic, vol. 40, Association for Symbolic Logic, La Jolla, CA; Cambridge University Press, Cambridge, 2012. MR2908005

[13] Martin Ziegler, *Mathematische Logik* (German), Mathematik Kompakt. [Compact Mathematics], Birkhäuser Verlag, Basel, 2010. MR2683672

Index

Selected Published Titles in This Series

89 **Martin Hils and François Loeser,** A First Journey through Logic, 2019

88 **M. Ram Murty and Brandon Fodden,** Hilbert's Tenth Problem, 2019

87 **Matthew Katz and Jan Reimann,** An Introduction to Ramsey Theory, 2018

86 **Peter Frankl and Norihide Tokushige,** Extremal Problems for Finite Sets, 2018

85 **Joel H. Shapiro,** Volterra Adventures, 2018

84 **Paul Pollack,** A Conversational Introduction to Algebraic Number Theory, 2017

83 **Thomas R. Shemanske,** Modern Cryptography and Elliptic Curves, 2017

82 **A. R. Wadsworth,** Problems in Abstract Algebra, 2017

81 **Vaughn Climenhaga and Anatole Katok,** From Groups to Geometry and Back, 2017

80 **Matt DeVos and Deborah A. Kent,** Game Theory, 2016

79 **Kristopher Tapp,** Matrix Groups for Undergraduates, Second Edition, 2016

78 **Gail S. Nelson,** A User-Friendly Introduction to Lebesgue Measure and Integration, 2015

77 **Wolfgang Kühnel,** Differential Geometry: Curves — Surfaces — Manifolds, Third Edition, 2015

76 **John Roe,** Winding Around, 2015

75 **Ida Kantor, Jiří Matoušek, and Robert Šámal,** Mathematics++, 2015

74 **Mohamed Elhamdadi and Sam Nelson,** Quandles, 2015

73 **Bruce M. Landman and Aaron Robertson,** Ramsey Theory on the Integers, Second Edition, 2014

72 **Mark Kot,** A First Course in the Calculus of Variations, 2014

71 **Joel Spencer,** Asymptopia, 2014

70 **Lasse Rempe-Gillen and Rebecca Waldecker,** Primality Testing for Beginners, 2014

69 **Mark Levi,** Classical Mechanics with Calculus of Variations and Optimal Control, 2014

68 **Samuel S. Wagstaff, Jr.,** The Joy of Factoring, 2013

67 **Emily H. Moore and Harriet S. Pollatsek,** Difference Sets, 2013

For a complete list of titles in this series, visit the AMS Bookstore at **www.ams.org/bookstore/stmlseries/**.

The aim of this book is to present mathematical logic to students who are interested in what this field is but have no intention of specializing in it. The point of view is to treat logic on an equal footing to any other topic in the mathematical curriculum. The book starts with a presentation of naive set theory, the theory of sets that mathematicians use on a daily basis. Each subsequent chapter presents one of the main areas of mathematical logic: first order logic and formal proofs, model theory, recursion theory, Gödel's incompleteness theorem, and, finally, the axiomatic set theory. Each chapter includes several interesting highlights—outside of logic when possible—either in the main text, or as exercises or appendices. Exercises are an essential component of the book, and a good number of them are designed to provide an opening to additional topics of interest.

ISBN 978-1-4704-5272-8

9 781470 452728

STML/89

For additional information and updates on this book, visit

www.ams.org/bookpages/stml-89

AMS

www.ams.org