Universitext

Shashi Mohan Srivastava

A Course on Mathematical Logic

Second Edition

Springer

Universitext

Universitext

Series Editors:

Sheldon Axler
San Francisco State University

Vincenzo Capasso
Università degli Studi di Milano

Carles Casacuberta
Universitat de Barcelona

Angus J. MacIntyre
Queen Mary College, University of London

Kenneth Ribet
University of California, Berkeley

Claude Sabbah
CNRS, École Polytechnique

Endre Süli
University of Oxford

Wojbor A. Woyczynski
Case Western Reserve University

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, to very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext*.

For further volumes:
http://www.springer.com/series/223

Shashi Mohan Srivastava

A Course on Mathematical Logic

Second Edition

Springer

Shashi Mohan Srivastava
Indian Statistical Institute
Kolkata, India

ISSN 0172-5939 ISSN 2191-6675 (electronic)
ISBN 978-1-4614-5745-9 ISBN 978-1-4614-5746-6 (eBook)
DOI 10.1007/978-1-4614-5746-6
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2012955369

Mathematics Subject Classification: 03B10, 03C10, 03C20

© Springer Science+Business Media New York 2008, 2013
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To Haimanti

Preface

This book is written on the occasion of the centenary of the birth of Kurt Gödel (1906–1978), the most exciting logician of all time, whose discoveries shook the foundations of mathematics. His beautiful technique of examining the whole edifice of mathematics within mathematics itself has been likened, not only figuratively but also in precise technical terms, to the music of Bach and drawings of Escher [6]. It has had a deep impact on philosophers and linguists. In a way, it ushered in the era of computers. His idea of arithmetization of formal systems led to the discovery of a universal computer program that simulates all programs. Based on his incompleteness theorems, physicists have propounded theories concerning artificial intelligence and the mind–body problem [13].

The main goal of this book is to state and prove Gödel's completeness and incompleteness theorems in precise mathematical terms. This has enabled us to present a short, distinctive, modern, and motivated introduction to mathematical logic for graduate and advanced undergraduate students of logic, set theory, recursion theory, and computer science. Any mathematician interested in knowing what mathematical logic is concerned with and who would like to learn the famous completeness and incompleteness theorems of Gödel should also find this book particularly convenient. The treatment is thoroughly mathematical, and the entire subject has been approached like any other branch of mathematics. Serious pains have been taken to make the book suitable for both classroom and self-instructional purposes. The book does not strive to be a comprehensive encyclopedia of logic, nor does it broaden its audience to linguists and philosophers. Still, it gives essentially all the basic concepts and results in mathematical logic.

The main prerequisite for this book is the willingness to work at a reasonable level of mathematical rigor and generality. However, a working knowledge of elementary mathematics, particularly naive set theory and algebra, is required. We suggest [17, pp. 1–15] for the necessary prerequisites in set theory. A good source for the algebra needed to understand some examples and applications would be [10].

Students who wish to specialize in foundational subjects should read the entire book, preferably in the order in which it is presented, and work out all the problems. Sometimes we have only sketched the proof and left out the routine arguments

for readers to complete. Students of computer science may leave out sections on model theory and arithmetical sets. Mathematicians working in other areas who wish to know about the completeness and incompleteness theorems alone may also omit these sections. However, sections on model theory give applications of logic to mathematics. Chapters 1–4, except for Sect. 2.4 and Sects. 5.1 and 5.4, should constitute a satisfactory course in mathematical logic for undergraduate students.

The book prepares students to branch out in several areas of mathematics related to foundations and computability such as logic, model theory, axiomatic set theory, definability, recursion theory, and computability. Hinman's recent book [5] is the most comprehensive one, with representation in all these areas. Shoenfield's [16] is still a very satisfactory book on logic. For axiomatic set theory, we particularly recommend Kunen [9] and Jech [8]. For model theory, readers should also consult Chang and Keisler [3] and Marker [11]. For recursion theory we suggest [12].

Acknowledgments. I thank M. G. Nadkarni, Franco Parlamento, Ravi A. Rao, B. V. Rao, and H. Sarbadhikari for very carefully reading the entire manuscript and for their numerous suggestions and corrections. Thanks are also due to my colleagues and research fellows at the Stat-Math Unit, Indian Statistical Institute, for their encouragement and help. I fondly acknowledge my daughter Rosy, my son Ravi, and my grandsons Pikku and Chikku for keeping my spirits up while I was writing this book. Last but not least, I shall ever be grateful to my wife, H. Sarbadhikari, for cheerfully putting up with me at home as well as at the office for the duration of my work on the book.

Preface to the Second Edition. In the second edition, we have given a fairly respectable introduction to model theory. It shows that logic is a lively subject with surprising connections elsewhere in mathematics. The work of Tarski, Julia Robinson, Vaught, Morley, Shelah, and others is a testimony to the fact that model theory in its own right is a beautiful and deep subject. Hrushovski's proof of the function-field Mordell–Lang conjecture [7], the proof of the Manin–Mumford conjecture by Pila and Zannier [15], and Pila's proof of the André–Oort conjecture [14] are some of the spectacular applications of model theory to geometry and number theory.

Our second edition aims at giving a first introduction to the easier parts of model theory. However, this is in no way a complete book on model theory. Still, we hope it will motivate and prepare readers to embark on a more serious study of the subject. In Chap. 2 we have added a section on homogeneous structures and a section on definability. The first three sections (including the proof of the completeness theorem for first-order logic) and the last section of Chap. 5 of the first edition have been transplanted to Chap. 4. Chapter 5 of the second edition is largely new and is devoted exclusively to model theory.

Significant new additions are ultraproduct of models, elimination of quantifiers, types, and atomic, saturated, and stable models. We study a large number of examples from algebra to illustrate our methods. A substantial study of real closed fields is an important new example from algebra. Several applications in

algebraically closed fields and real closed fields such as Chevalley's theorem, Hilbert's Nullstellensatz, A. Robinson's proof of Hilbert's 17th problem, and others are given. Apart from cosmetic changes and the additional examples, the rest of the material from the first edition has remained unchanged.

I have been greatly helped by my wife and colleague H. Sarbadhikari for her review of the first edition. I remain grateful to her. I fondly acknowledge the contribution of my daughter-in-law Deepali to keep me and my wife free of any domestic worry and my new grandson Rhishant (Totu) for providing sufficient entertainment as a diversion from this work. Help on LaTeX-related problems provided by my colleagues Pradipta Bandyopadhyay and Asish Mondal is gratefully acknowledged.

Contents

Chapter 1
Syntax of First-Order Logic

The main objects of study in mathematical logic are mathematical theories such as set theory, number theory, and the theory of algebraic structures such as groups, rings, fields, algebraically closed fields, etc., with the aim of developing tools to examine their consistency, completeness, and other similar questions concerning the foundation of these theories. In this chapter we take the first step toward logic and precisely define the notion of a first-order theory.

1.1 First-Order Languages

The objects of study in the natural sciences have a physical existence. By contrast, mathematical objects are concepts, e.g., "sets," "belongs to ($\in$)," "natural numbers," "real numbers," "complex numbers," "lines," "curves," "addition," "multiplication," etc.

There must be initial concepts in a theory. To elaborate on this a bit more, note that a concept can be defined in terms of other concepts. For instance, $x - y$ is the unique number z such that $y + z = x$; or if x and y are sets, $x \subset y$ if for every element z, $z \in x$ implies $z \in y$. Thus, "subtraction" can be "defined" in terms of "addition" and "subset ($\subset$)" in terms of "belongs to ($\in$)." At the onset, one begins with a minimal number of undefined concepts. For instance, in set theory, the undefined concepts are "sets" and "belongs to"; in number theory, the undefined concepts are "natural numbers," "zero," and the "successor function"; in the theory of real numbers (seen as an archimedean ordered field), the undefined concepts are "real numbers," "zero," "one," "addition," "multiplication," and "less than." In these examples, we see that there are two groups of concepts: sets or natural numbers or real numbers on the one hand and belongs to, zero, one, successor, addition, multiplication, less than, etc. on the other. Concepts of the first type are the main objects of study; concepts of the second type are used to reflect basic structural properties of the objects of the first type. Then one lists a set of axioms that give the basic structural properties of the

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_1,
© Springer Science+Business Media New York 2013

objects of study. It is expected that based on these undefined concepts and on the axioms, other concepts can be defined. Then the theory is developed by introducing more and more concepts and proving more and more theorems.

Clearly, we ought to have a language to develop a theory. Like any of the natural languages, for example, Latin, Sanskrit, or Tamil, a language suitable for a mathematical theory also has an alphabet. But unlike natural languages, a statement in a mathematical theory is expressed symbolically and has an unambiguous syntactical construction. Before giving precise definitions, we give some examples of statements in some theories that we are familiar with.

Example 1.1.1. Consider the following statement in group theory. For every x there exists y such that $x \cdot y = e$. Here $\cdot$ (dot) is a symbol for the binary group operation and e for the identity element. If we use the symbol $\forall$ to denote "for every" and $\exists$ for "there exists," then we can represent the foregoing statement as follows:

$$\forall x \exists y (x \cdot y = e).$$

Example 1.1.2. The following two statements appear in set theory:

$$\forall x \forall y \exists z (x \in z \wedge y \in z)$$

and

$$\neg \exists x \forall y (y \in x).$$

The first statement is a symbolic representation of the statement "Given any two sets x and y, there is a set z that contains both x and y"; the second statement means "There is no set x that contains all sets y."

We see that the language for a theory should have "variables" to represent the objects of study, e.g., sets in set theory, or elements of a group in group theory, etc., and some logical symbols like $\exists$ (there exists), $\wedge$ (and), $\neg$ (negation), $=$ (equality). These symbols are common to the languages for all theories. We call them logical symbols. On the other hand, there are certain alphabets that represent undefined concepts of a specific theory. For instance, in group theory we use two symbols: the dot $\cdot$ for the group operation and a symbol, say e, for the identity element; in set theory we have a binary relation symbol $\in$ for the undefined concept "belongs to."

We make one more observation before giving the first definition in the subject. Mathematicians use many logical connectives and quantifiers such as $\vee$ (or), $\wedge$ (and), $\exists$ (there exists), $\forall$ (for all), $\rightarrow$ (if $\cdots$, then $\cdots$), and $\leftrightarrow$ (if and only if). However, in their reasoning "two statements A and B are both true" if and only if "it is not true that any of A or B is false"; "A implies B" if and only if "either A is false or B is true," etc. This indicates that some of the logical connectives and quantifiers can be defined in terms of others. Thus, we can start with a few logical connectives and quantifiers. This economy will help in making many proofs quite short.

A first-order language L consists of two types of symbols: *logical symbols* and *nonlogical symbols*. Logical symbols consist of a sequence of *variables* $x_0, x_1, x_2, \ldots$; *logical connectives* $\neg$ (negation) and $\vee$ (disjunction); a *logical quantifier* $\exists$ (existential quantifier); and the *equality symbol* $=$. We call the order in which variables $x_0, x_1, x_2, \ldots$ are listed the *alphabetical order*. These are common to all first-order languages. Depending on the theory, nonlogical symbols of L consist of an (empty or nonempty) set of *constant symbols* $\{c_i : i \in I\}$; for each positive integer n, a set of n-ary *function symbols* $\{f_j : j \in J_n\}$; and a set of n-ary *relation symbols* $\{p_k : k \in K_n\}$.

When it is clear from the context, a first-order language will simply be called a language. Since logical symbols are the same for all languages, to specify a language one must specify its nonlogical symbols only. The collection of all nonlogical symbols is sometimes called the *signature* of the language. To avoid suffixes and for ease in reading, we shall use symbols x, y, z, u, v, w, with or without subscripts, to denote variables. Any finite sequence of symbols of a language L will be called an *expression* in L.

A language L is called *countable* if it has only countably many nonlogical symbols; it is called *finite* if it has finitely many nonlogical symbols.

Example 1.1.3. The language for set theory has only one nonlogical symbol: a binary relation symbol $\in$ for "belongs to."

Example 1.1.4. The language for group theory has a constant symbol e (for the identity element) and a binary function symbol $\cdot$ (for the group operation).

Example 1.1.5. The language of the theory of rings with identity has two constant symbols, 0 and 1, and two binary function symbols, $+$ and $\cdot$.

Example 1.1.6. The language for the theory of ordered fields has two constant symbols, 0 and 1, two binary function symbols, $+$ and $\cdot$, and a binary relation symbol, $<$.

A first-order language L' is called an *extension* of another language L if every constant symbol of L is a constant symbol of L' and every n-ary function (relation) symbol of L is an n-ary function (relation) symbol of L'.

Example 1.1.7. The language for the theory of ordered fields is an extension of the language of the theory of rings with identity.

Exercise 1.1.8. Show that the set of all expressions of a countable language is countable.

1.2 Terms of a Language

We now define the *terms* of a language L. Broadly speaking, they correspond to algebraic expressions.

The set of all terms of a language L is the smallest set $\mathscr{T}$ of expressions of L that contains all variables and constant symbols and is closed under the following operation: whenever $t_1,\dots,t_n \in \mathscr{T}$, $f_j t_1 \cdots t_n \in \mathscr{T}$, where f_j is any n-ary function symbol of L. Equivalently, all the terms of a language can be inductively defined as follows: variables and constant symbols are terms of rank 0; if $t_1,\dots,t_n$ are terms of rank $\leq k$, and if f_j is an n-ary function symbol, then $f_j t_1 \cdots t_n$ is a term of rank at most $k+1$. Thus, the *rank* of a term t is the smallest natural number k such that t is of rank $\leq k$.

Note that the set of variable-free terms is the smallest set $\mathscr{T}'$ of expressions of L that contains all constant symbols and is closed under the following operation: whenever $t_1,\dots,t_n \in \mathscr{T}'$, then $f_j t_1 \cdots t_n \in \mathscr{T}'$, where f_j is any n-ary function symbol of L.

We shall freely use parentheses and commas in a canonical way for easy readability. For instance, we shall often write $f_j(t_1,\dots,t_n)$ instead of $f_j t_1 \cdots t_n$, and $t+s$ instead of $+ts$. We shall also drop parentheses when there is no possibility of confusion. Further, we shall adopt the convention of association to the right for omitting parentheses. For instance, instead of writing $t_1 \cdot (t_2 \cdot (t_3 \cdot t_4))$, we shall write $t_1 \cdot t_2 \cdot t_3 \cdot t_4$. It is important to note that the term $((t_1 \cdot t_2) \cdot t_3) \cdot t_4$ is not the same as $t_1 \cdot t_2 \cdot t_3 \cdot t_4$. This term can only be written using parentheses, unless, of course, one writes it as

$$\cdots t_1 t_2 t_3 t_4 !$$

Similarly, $(t_1 \cdot t_2) \cdot (t_3 \cdot t_4)$ shall stand for

$$\cdot\cdot t_1 t_2 \cdot t_3 t_4 !$$

Example 1.2.1. Let L be the language for the theory of rings with identity: L has two constant symbols, 0 and 1, and two binary function symbols, $+$ and $\cdot$. Let $\underline{m}$ denote the term obtained by "adding" 1 to itself m times, i.e., $\underline{m}$ is the term

$$\underbrace{1+\cdots+1}_{m \text{ times}};$$

for any term t, let t^n denote the term obtained by "multiplying" t by itself n times, i.e., t^n is the term

$$\underbrace{t \cdot t \ \cdots \ t \cdot t}_{n \text{ times}}.$$

Then $\underline{m}$ and t^n are terms of L. Also, any "formal polynomial"

$$\underline{m_0} + \underline{m_1} x + \cdots + \underline{m_n} x^n,$$

with x a variable, is a term of L.

Example 1.2.2. Variables are the only terms in the language of set theory because it has no constant and no function symbols.

We define the set of all *subterms* of a term t by induction as follows: t is a subterm of t. If $ft_1\cdots t_n$, $t_1,\ldots,t_n \in \mathscr{T}$, is a subterm of t, then so is each t_i, $1 \le i \le n$. An expression is a subterm of t if it is obtained as above. Thus, the *set of all subterms of a term t is the smallest set* $\mathscr{S}$ of expressions that contains t and such that whenever $ft_1\cdots t_n \in \mathscr{S}$, then $t_1,\ldots,t_n \in \mathscr{S}$.

Example 1.2.3. Let t be the term $x\cdot y\cdot z$ of the language of group theory. Then $x\cdot y\cdot z$, x, $y\cdot z$, y, and z are all the subterms of t. Note that $x\cdot y$ is not a subterm of t.

Exercise 1.2.4. List all the subterms of the term

$$x\cdot u + y\cdot v + z\cdot w$$

of the language of ring theory.

Let s be a term. We shall write $s[v_1,\ldots,v_n]$ to indicate that variables occurring in s are among $v_1,\ldots,v_n$. If s is a term, then $s_{v_1,\ldots,v_n}[t_1,\ldots,t_n]$, or simply $s[t_1,\ldots,t_n]$ when there is no possibility of confusion, denotes the expression obtained from s by simultaneously replacing all occurrences of $v_1,\ldots,v_n$ in s by $t_1,\ldots,t_n$, respectively.

Example 1.2.5. Let s be the term $x\cdot(y+z)$ of the language for the theory of rings with identity. Then

$$s_{x,y,z}[x+z,1,y\cdot y] = (x+z)\cdot(1+y\cdot y).$$

Proposition 1.2.6. *Let $s[v_1,\ldots,v_n]$ and $t_1,\ldots,t_n$ be terms. The expression $s[t_1,\ldots,t_n]$ defined above is a term.*

Proof. We prove the result by induction on the rank of s. If s is a constant symbol c, then $s[t_1,\ldots,t_n] = c$; if s is a variable other than the v_i, then $s[t_1,\ldots,t_n] = s$; if s is v_i for some $1 \le i \le n$, then $s[t_1,\ldots,t_n] = t_i$. Thus, the assertion is true for terms of rank 0.

Let k be a natural number, and assume that the assertion is true for all terms s of rank $\le k$ (and all variables v_i and all terms t_i). Let $s_j[v_1,\ldots,v_n]$, $1 \le j \le m$, be terms of rank $\le k$, $t_1,\ldots,t_n$ terms, and let f be an m-ary function symbol. Suppose

$$s[v_1,\ldots,v_n] = f(s_1[v_1,\ldots,v_n],\ldots,s_m[v_1,\ldots,v_n]).$$

Then

$$s[t_1,\ldots,t_n] = f(s_1[t_1,\ldots,t_n],\ldots,s_m[t_1,\ldots,t_n]).$$

By the induction hypothesis, each $s_j[t_1,\ldots,t_n]$ is a term. Hence $s[t_1,\ldots,t_n]$ is a term. The proof is complete by induction on the rank of terms. □

Remark 1.2.7. The foregoing method of proving statements on terms by induction on the rank of terms is a fairly standard one in the subject. Sometimes, in the rest of this book, we may not give the complete argument and just say that the result can be proved by induction on the rank of terms.

1.3 Formulas of a Language

Our next concept is that of an atomic formula of the language L.

An *atomic formula* of a language is defined as follows: if t and s are terms of L, then $t = s$ is an atomic formula of L; if p is an n-ary relation symbol of L and $t_1, \ldots, t_n$ are terms, then $pt_1 \cdots t_n$ is an atomic formula; these are all the atomic formulas of L.

Example 1.3.1. $x \cdot y = 1$, $\underline{i} \cdot (\underline{j} + \underline{k}) = \underline{i} \cdot \underline{j} + \underline{i} \cdot \underline{k}$, $\underline{i} \cdot \underline{i} < \underline{m}$ are atomic formulas of the language of the theory of ordered fields.

Example 1.3.2. $v \in w$, $v = w$, where v and w are variables, are all the atomic formulas of the language of set theory.

A *formula* of a language is inductively defined as follows: every atomic formula is a formula – these are all the formulas of *rank* 0; if A and B are formulas of rank $\leq k$ and v is a variable, then $\neg A$ (the negation of A); $\exists vA$ and $\vee AB$ (the disjunction of A and B) are formulas of rank $\leq k+1$. The set of strings so obtained are all the formulas of L. Thus, the *set of all formulas of L is the smallest set of all expressions of L that contains all the atomic formulas and that is closed under negation, disjunction, and existential quantification.* Let A be a formula of L. The *rank* of A is the smallest natural number k such that the rank of A is $\leq k$. Atomic formulas or their negations are called *literals*.

Henceforth, unless otherwise stated, L will denote a first-order language, and by term (or formula) we shall mean a term (or a formula) of L.

We shall generally write $A \vee B$ instead of $\vee AB$. In the case of formulas also, we shall use parentheses and commas in a canonical way for easy readability. We adopt the convention of association to the right for omitting parentheses. This means that $A \vee B \vee C$ is to be read as $A \vee (B \vee C)$; $A \vee B \vee C \vee D$ is to be read as $A \vee (B \vee (C \vee D))$; and so on. Note that the formula $(A \vee B) \vee C$ is different from the formula $A \vee (B \vee C)$ and that the parentheses have to be used to write the former formula, unless, of course, one writes it as $\vee \vee ABC$! If $A_1, \cdots, A_n$ are formulas, then we shall write $\vee_{i=1}^{n} A_i$ for $A_1 \vee \cdots \vee A_n$. Also, we shall often write $t \neq s$ instead of $\neg(t = s)$, where t and s are terms of the language.

Remark 1.3.3. Any term or formula is of the form $Au_1 \cdots u_n$ where A is a symbol and $u_1, \cdots, u_n$ are terms or formulas. It should be noted that such a representation of a term or formula is unique. This allows us to define functions or give proofs by induction on the length of terms or formulas.

We now define some other commonly used logical connectives and quantifiers.

$\forall vA$ is an abbreviation of $\neg\exists v\neg A$; $A \wedge B$ abbreviates $\neg(\neg A \vee \neg B)$; $A \to B$ is an abbreviation of $(\neg A) \vee B$; and $A \leftrightarrow B$ abbreviates $(A \to B) \wedge (B \to A)$. Note that according to our convention of omitting parentheses, $A \to B \to C$ is to be read as $A \to (B \to C)$; $A \to B \to C \to D$ is to be read as $A \to (B \to (C \to D))$; and so on. The connective $\wedge$ is called a *conjunction* and the quantifier $\forall$ the *universal quantifier*. Note that we could have added all these symbols to our alphabet. There are several reasons for not doing so. For instance, the proof of some results concerning formulas

would become long if we did not exercise economy in the number of logical symbols. As in the case of disjunction, we shall write $\wedge_{i=1}^{n} A_i$ for $A_1 \wedge \cdots \wedge A_n$.

A formula of the form $\exists v A$ is called an *instantiation* of A, and a formula of the form $\forall v A$ is called a *generalization* of A. A formula is called *elementary* if it is either an atomic formula or an instantiation of a formula.

Exercise 1.3.4. Show that the set of all formulas is the smallest collection $\mathscr{F}$ of formulas such that each elementary formula is in $\mathscr{F}$ and that it is closed under $\neg$ and $\vee$, i.e., whenever $A, B \in \mathscr{F}$, then $\neg A$ and $A \vee B$ are in $\mathscr{F}$ as well.

A *subformula* of a formula A is inductively defined as follows: A is a subformula of itself; if $\neg B$ or $\exists v B$ is a subformula of A, then so is B; if $B \vee C$ is a subformula of A, then B and C are subformulas of A; nothing else is a subformula of A. Thus, the *set of subformulas of A is the smallest set $\mathscr{S}(A)$ of formulas of L that contains A and satisfies the following conditions: whenever $\neg B$ or $\exists v B$ is in $\mathscr{S}(A)$, then so is B, and whenever $B \vee C$ is in $\mathscr{S}(A)$, then so are B and C*.

Exercise 1.3.5. List all the subformulas of the following formulas:

1. $\forall x \exists y (x \cdot y = e)$.
2. $\forall x \forall y \exists z (x \in z \wedge y \in z)$.
3. $\neg \exists x \forall y (y \in x)$.

(The preceding formulas should be considered in their unabbreviated forms.)

An occurrence of a variable v in a formula A is *bound* if it occurs in a subformula of the form $\exists v B$; otherwise, the occurrence is called *free*. A variable is said to be free in A if it has a free occurrence in A. We shall write $\varphi[v_0, \ldots, v_n]$ if φ is a formula all of whose free variables belong to the set $\{v_0, \ldots, v_n\}$.

Example 1.3.6. In the formula

$$x \in y \vee \exists x (x \in y),$$

all the occurrences of y are free, the first occurrence of x is free, and other occurrences of x are bound.

A formula with no free variable is called a *closed formula* or a *sentence*. A formula that contains no quantifiers is called an *open formula*.

Exercise 1.3.7. Show that the set of all open formulas is the smallest collection $\mathscr{O}$ of formulas such that each atomic formula is in $\mathscr{O}$ and is closed under $\neg$ and $\vee$, i.e., whenever $A, B \in \mathscr{O}$, then $\neg A$ and $A \vee B$ are in $\mathscr{O}$ as well.

Let $A[x_0, \ldots, x_{n-1}]$ be a formula whose free variables are among $x_0, \ldots, x_{n-1}$ and x_{n-1} is free in A, where $x_0, \ldots, x_{n-1}$ are the first n variables in alphabetical order. We call

$$\forall x_{n-1} \cdots \forall x_0 A$$

the *closure* of A. Note that if A is closed, then it is its own closure.

Let t be a term, v a variable, and A a formula of a language L. We say that the *term t is substitutable for v in A* if for each variable w occurring in t no subformula of A of the form $\exists wB$ contains an occurrence of v that is free in A.

Example 1.3.8. In the formula

$$x \in y \vee \exists x(x \in y),$$

we cannot substitute any term containing x for y.

If t is substitutable for v in A, then $A_v[t]$ designates the expression obtained from A by simultaneously replacing each free occurrence of v in A by t. Similarly, if the terms $t_1,\ldots,t_n$ are substitutable in A for $v_1,\ldots,v_n$, respectively, then $A_{v_1,\ldots,v_n}[t_1,\ldots,t_n]$, or $A[t_1,\ldots,t_n]$ when there is no possibility of confusion, called an *instance* of A, will denote the expression obtained from A by simultaneously replacing all free occurrences of $v_1,\ldots,v_n$ in A by $t_1,\ldots,t_n$, respectively. Note that whenever we talk of $A[t_1,\ldots,t_n]$, it will be assumed that $t_1,\ldots,t_n$ are substitutable in A for $v_1,\ldots,v_n$, respectively.

Example 1.3.9. Let A be the formula

$$x \in y \vee \exists x(x \in y).$$

Then $A_x[z]$ is the formula $z \in y \vee \exists x(x \in y)$.

Proposition 1.3.10. *The sequence $A[t_1,\ldots,t_n]$ defined previously is a formula.*

Proof. As in the case of the corresponding result on terms, this result is also proved by induction on the rank of formulas. Let $A[v_1,\ldots,v_n]$ be an atomic formula. Then A is a formula of the form $p(s_1[v_1,\ldots,v_n],\ldots,s_m[v_1,\ldots,v_n])$, where p is an m-ary predicate symbol and $s_1,\ldots,s_m$ are terms of L (p may be the equality symbol; in this case $m=2$). Then,

$$A[t_1,\ldots,t_n] = p(s_1[t_1,\ldots,t_n],\ldots,s_m[t_1,\ldots,t_n]).$$

By Proposition 1.2.6, $s_j[t_1,\ldots,t_n]$, $1 \le j \le m$, are terms. Hence, $A[t_1,\ldots,t_n]$ is a formula. Thus, the assertion is true for formulas of rank 0.

Let k be a natural number, and assume that the assertion is true for all formulas of rank $\le k$ (and all variables v_i and all terms t_i).

Let $B[v_1,\ldots,v_n]$ and $C[v_1,\ldots,v_n]$ be formulas of rank $\le k$, and let $t_1,\ldots,t_n$ be substitutable for $v_1,\ldots,v_n$ respectively in B and C. If A is the formula $\neg B$, then $A[t_1,\ldots,t_n]$ is the expression $\neg B[t_1,\ldots,t_n]$, which is a formula by the induction hypothesis. If A is $B \vee C$, then $A[t_1,\ldots,t_n]$ is the expression $B[t_1,\ldots,t_n] \vee C[t_1,\ldots,t_n]$, which is a formula by the induction hypothesis.

Let $B[v,v_1,\ldots,v_n]$ be a formula of rank k, and let v be distinct from v_i. Suppose A is the formula $\exists vB$. Then $A[t_1,\ldots,t_n]$ is the expression $\exists vB[v,t_1,\ldots,t_n]$. This is clearly a formula by the induction hypothesis. Thus the assertion is true for all formulas of rank $k+1$. Our proof is complete by induction on the rank of formulas. □

Remark 1.3.11. The foregoing method of proving results by induction on the rank of formulas is a fairly standard method in the field. Sometimes, in the remainder of this book, we may not give the complete argument and simply say that the result can be proved by induction on the rank of formulas.

So far, we have been describing the "syntax," i.e., rules for arranging symbols into terms and sentences, of a theory. Here a sentence is just a string of symbols from the language of the theory (without having a meaning). One may consider this to be a useless representation of a sentence. But it is far from useless. Logical connectives and quantifiers have an intended logical meaning, so that whatever A may be, $\neg A \vee A$ is "true"; for any term t, $t = t$ is "true"; $A \vee B$ is "true" if and only if at least one of A or B is "true"; and so on. Thus, quite often the structure of a formula itself helps us to make inferences about the formula. We are now in a very good situation: we have a precise definition of a sentence; it exists concretely as the string of symbols we see; and we can make some inferences about it from its syntactical structure. Of course, we should know what an inference is and how it is done. This will be specified later in the book.

1.4 First-Order Theories

A *first-order theory*, or simply a *theory*, T consists of a first-order language L and a set of formulas of L. These formulas are called *nonlogical axioms* of T. By terms or formulas of T, we shall mean terms or formulas respectively of the language of T. The language of T will also be denoted by $L(T)$. A theory is called *countable* if its language is countable. It is *finite* if the set of all nonlogical symbols is finite. In general, a theory T whose set of all nonlogical symbols is of cardinality at most κ, with κ an infinite cardinal, is called a κ-*theory*.

Example 1.4.1. The theory of infinite sets has no nonlogical symbols and its axioms are the sentences A_n, $n \geq 2$, where A_n is the formula

$$\exists x_1 \cdots \exists x_n \wedge_{1 \leq i < j \leq n} x_i \neq x_j.$$

Example 1.4.2. Group theory is a theory whose nonlogical symbols are a constant symbol e and a binary function symbol $\cdot$ and whose nonlogical axioms are the following formulas (below, x, y, and z denote the first three variables):

1. $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,
2. $\forall x (x \cdot e = x \wedge e \cdot x = x)$,
3. $\forall x \exists y (x \cdot y = e \wedge y \cdot x = e)$.

Example 1.4.3. The theory of abelian groups is a theory whose nonlogical symbols are a constant symbol 0 and a binary function symbol $+$ and whose nonlogical axioms are the following formulas:

1. $\forall x \forall y \forall z(x+(y+z)=(x+y)+z)$,
2. $\forall x(x+0=x \wedge 0+x=x)$,
3. $\forall x \exists y(x+y=0 \wedge y+x=0)$,
4. $\forall x \forall y(x+y=y+x)$.

Example 1.4.4. The language of the *theory of rings with identity* has two constant symbols, 0 and 1, and two binary function symbols, $+$ and $\cdot$. The nonlogical axioms of this theory are axioms 1–4 of abelian groups together with the following axioms:

5. $\forall x \forall y \forall z(x \cdot (y \cdot z)=(x \cdot y) \cdot z)$,
6. $\forall x(x \cdot 1=x \wedge 1 \cdot x=x)$,
7. $\forall x \forall y \forall z(x \cdot (y+z)=x \cdot y+x \cdot z)$,
8. $\forall x \forall y \forall z((y+z) \cdot x=y \cdot x+z \cdot x)$.

We define the *theory of commutative rings with identity* by adding

9. $\forall x \forall y(x \cdot y=y \cdot x)$

as a nonlogical axiom.

Example 1.4.5. Field theory has the same language as the theory of rings with identity its nonlogical axioms are axioms 1–9 of the theory of commutative rings with identity together with the following axiom:

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

Example 1.4.6. Let L be a language with only one nonlogical symbol – a binary relation symbol $<$. The theory LO (the *theory of linearly ordered sets*) is a theory whose language is L and whose nonlogical axioms are as follows:

1. $\forall x \neg(x<x)$,
2. $\forall x \forall y \forall z((x<y \wedge y<z) \rightarrow x<z)$,
3. $\forall x \forall y(x<y \vee x=y \vee y<x)$.

Example 1.4.7. The *theory of ordered abelian groups*, denoted by OG, has a constant symbol 0, a binary function symbol $+$, and a binary relation symbol $<$, and its axioms are the axioms of abelian groups, axioms of linear order, and the following axiom:

$$\forall x \forall y \forall z(x<y \rightarrow x+z<y+z).$$

Example 1.4.8. The *theory of dense linearly ordered sets*, denoted by DLO, is obtained from LO by adding the following axioms:

4. $\forall x \forall y((x<y) \rightarrow \exists z(x<z \wedge z<y))$,
5. $\forall x \exists y(y<x)$,
6. $\forall x \exists y(x<y)$.

Exercise 1.4.9. Express the axioms of an equivalence relation as formulas of a suitable first-order language.

Example 1.4.10. Let F be the theory of fields.

Let $p > 1$ be a prime number. The theory obtained by adding

$$\wedge_{m=1}^{p-1}(\underline{m} \neq 0) \wedge (\underline{p} = 0)$$

to the axiom of F is called the *theory of fields of characteristic p*.

For each $m \geq 1$, let A_m be the formula $\underline{m} \neq 0$. The theory obtained by adding each A_m to the set of axioms of F as an axiom is called the *theory of fields of characteristic* 0.

Example 1.4.11. Let F be the theory of fields. Let L be an extension of the language for the theory of rings with identity obtained by adding a new binary predicate symbol $<$. Consider the theory OF whose language is L and whose nonlogical axioms are all the nonlogical axioms of F and the following axioms:

11. $\forall x \neg(x < x)$,
12. $\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z)$,
13. $\forall x \forall y(x < y \vee x = y \vee y < x)$,
14. $\forall x \forall y(x < y \rightarrow \forall z(x + z < y + z))$,
15. $\forall x \forall y((0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y)$.

The theory OF is known as the *theory of ordered fields*.

Example 1.4.12. We now give some axioms of number theory, which plays an important role in logic. We denote this theory by N. The nonlogical symbols of N are a constant symbol 0, a unary function symbol S (which designates the successor function), two binary function symbols $+$ and $\cdot$, and a binary relation symbol $<$. The nonlogical axioms of N are as follows:

1. $\forall x(\neg(Sx = 0))$,
2. $\forall x \forall y(Sx = Sy \rightarrow x = y)$,
3. $\forall x(x + 0 = x)$,
4. $\forall x \forall y(x + Sy = S(x + y))$,
5. $\forall x(x \cdot 0 = 0)$,
6. $\forall x \forall y(x \cdot Sy = (x \cdot y) + x)$,
7. $\forall x(\neg(x < 0))$,
8. $\forall x \forall y(x < Sy \leftrightarrow (x < y \vee x = y))$,
9. $\forall x(\forall y(x < y \vee x = y \vee y < x)$.

For any nonnegative integer n, the term

$$\underbrace{S \cdots S}_{m \text{ times}} 0$$

will be denoted by k_n. Such terms are called *numerals*. Note that k_0 is the constant symbol 0.

Example 1.4.13. Peano arithmetic is the theory obtained from N by deleting the last axiom and adding the following axiom schema, called an *induction axiom schema*: for every formula $A[v]$, the formula

$$A_v[0] \to \forall v(A \to A_v[Sv]) \to A$$

is called an induction axiom. This theory will be denoted by PA.

Example 1.4.14. We give below the axioms of set theory. This theory is called *Zermelo–Fraenkel set theory* and is designated by ZF. To convey the content of the axioms better, we shall state the axioms informally in words as well:

1. *Set existence. There exists a set.* This is expressed by the formula

$$\exists x(x = x).$$

2. *Extensionality. Two sets are the same if they contain the same sets:*

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

   This axiom has a serious consequence: *elements of a set are themselves sets*. For instance, the collections of all Indians and that of all Americans are not sets. For, if they were, they would be the same sets because they contain no sets.
3. *Comprehension (subset) schema.* For each formula $\varphi[x, w_1, \ldots, w_n]$, the following formula is an axiom:

$$\forall z \forall w_1 \cdots \forall w_n(\exists y \forall x(x \in y \leftrightarrow x \in z \wedge \varphi)).$$

   This axiom says that *given any "property of sets" expressed by a formula $\varphi[x, w_1, \ldots, w_n]$, for any fixed parameters $w_1, \ldots, w_n$ and for any set z, there is a set y that consists precisely of those $x \in z$ that satisfy $\varphi[x, w_1, \ldots, w_n]$.*

   By extensionality, it can be proved that such a set y is unique, usually denoted by

$$y = \{x \in z : \varphi[x, w_1, \ldots, w_n]\}.$$

   It is assumed that the variables x, y, and z and the w_i are distinct.
4. *Replacement schema.* For every formula $\varphi[x, y, z, u_1, \ldots, u_n]$, the following formula is an axiom:

$$\forall z \forall u_1 \cdots \forall u_n(\forall x \in z \exists! y \varphi \to \exists v \forall x(x \in z \to \exists y(y \in v \wedge \varphi))),$$

   where $\exists! y \varphi$ abbreviates the formula

$$\varphi \wedge \forall u(\varphi_y[u] \to u = y).$$

This axiom, together with comprehension, says that the range of a "function" on a set z that is defined by a formula φ is a set.

5. *Pairing. Given sets x and y, there is a set z that contains both x and y:*

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

This axiom, together with comprehension, helps us to speak of sets of the form $\{x\}, \{x, y\}, \{x, y, z\}$, etc.

6. *Union. Given any set x, there is a set y that contains all z that belong to a member of x:*

$$\forall x \exists y \forall z \forall u (u \in x \wedge z \in u \rightarrow z \in y).$$

This axiom, together with comprehension, will imply that the union of a family (i.e., a set) of sets is a set.

7. *Power set. Given any set x, there is a set y that contains all subsets z of x:*

$$\forall x \exists y \forall z (\forall u (u \in z \rightarrow u \in x) \rightarrow z \in y).$$

This axiom, together with comprehension, will enable us to define the power set of a set.

8. *Infinity.* Based on the axioms introduced so far, it can be "proved" that an empty set exists, which we shall denote by 0. The following formula is an axiom:

$$\exists x (0 \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x)).$$

Without the infinity axiom, we cannot prove the existence of an "infinite" set; without this axiom, we cannot prove that there is a set containing all natural numbers.

9. *Foundation.* This is the most unintuitive axiom. It is the following formula:

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

It says that the *binary relation $\in$ is well founded on every nonempty set.* It rules out the existence of a set that contains itself. Even by restricting the domain of discourse of set theory to well-founded sets, we can define all the mathematical objects, i.e., natural numbers, real numbers, complex numbers, Euclidean spaces, curves, surfaces, etc., as sets.

Chapter 2
Semantics of First-Order Languages

In the last chapter, we presented syntactical notions pertaining to first-order theories. However, in general, mathematical theories are not developed syntactically. In this chapter, we give the semantics of first-order languages to connect the syntactical description of a theory with the setting in which a mathematical theory is generally developed. This chapter should also be seen as the beginning of a branch of logic called model theory, which can be thought of as the general study of mathematical structures. Some important notions from model theory, for example, the downward Löwenheim–Skolem theorem, types, homogeneous structures, and definability, are introduced here.

Recall that instead of beginning with the syntactical object group theory, in practice, one begins by defining a group as a nonempty set G with a specified element e and a binary operation $\cdot : G \times G \to G$ satisfying the following three conditions:

1. For every a, b, c in G,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
2. For every $a \in G$,
$$a \cdot e = e \cdot a = a.$$
3. For every $a \in G$, there is a $b \in G$ such that
$$a \cdot b = b \cdot a = e.$$

Thus a group consists of a nonempty set G with "interpretations" or "meanings" of the nonlogical symbols $\cdot$ (a binary function symbol) and e (a constant symbol) such that all the axioms of group theory are "satisfied." Further, a statement in the language of group theory is called a theorem if it is satisfied in all groups. Thus, to give the connection we are looking for, first we should define the interpretation or the structure of a language L as a nonempty set A together with the interpretations

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_2,
© Springer Science+Business Media New York 2013

or meanings of all the nonlogical symbols of L. This is known as the semantics of L. Then the models of a theory T are those structures of the language for T in which all axioms are true.

2.1 Structures of First-Order Languages

A *structure* or an *interpretation* of a first-order language L consists of (a) a nonempty set M (called the *universe* of the structure), (b) for each constant symbol c of L, a fixed element $c_M \in M$, (c) for each n-ary function symbol f of L, an n-ary map $f_M : M^n \to M$, and (d) for each n-ary relation symbol p of L, an n-ary relation $p_M \subset M^n$ on M. The interpretation of "=" is always taken to be the equality relation in M.

Any group is a structure of the language of group theory; the usual set of real numbers with the usual 0, 1, $+$, $\cdot$, and $<$ is a structure for the language of the theory of ordered fields. Note that which statement is true in a structure and which is not is irrelevant in the definition of a structure. For instance, the set of all natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ as the universe, 0 as the interpretation of e, and $+$ the interpretation of $\cdot$ is a structure of the language of group theory even though it is not a group.

Example 2.1.1. Let $\mathbb{N}$ be the set of all natural numbers, and let 0, 1, $+$, $\cdot$, and $<$ have the usual meanings. Further, let $S(n) = n + 1$, $n \in \mathbb{N}$. This is a structure of the language of the theory N defined in Chap. 1. This structure will be called the *standard structure of N*.

Let L be an extension of L' and M a structure of L. By ignoring the interpretations of those nonlogical symbols of L that are not symbols of L', we get a structure M' of L'. We call M' the *restriction* of M to L' and denote it by $M|L'$. In this case we shall also call M an *expansion* of M' to L.

Recall that all variable-free terms can be obtained starting from constant symbols and iterating function symbols on them. Thus, we shall define the interpretation or meaning t_M of each variable-free term t of L in M by induction on the rank of t. The interpretation of a constant symbol c is already given by the structure, namely c_M. If $t_1, \ldots, t_n$ are variable-free terms whose interpretations have been defined and if f is an n-ary function symbol of L, then we define

$$(ft_1 \cdots t_n)_M = f_M((t_1)_M, \ldots, (t_n)_M).$$

By induction on the rank of terms, it is easy to see that we have defined t_M for each variable-free term t of L.

Example 2.1.2. Let L be the language of the theory of rings with identity. For each positive integer m, let $\underline{m}$ denote the term obtained by "adding" 1 to itself m times. Let $P(x)$ be a polynomial expression whose coefficients are of the form $\underline{m}$, i.e., $P(x)$ is a term of the form

$$\underline{m_0} + \underline{m_1}x + \cdots + \underline{m_n}x^n,$$

where x is a variable. Let R be a ring with identity. Then the interpretation of $\underline{m}$ in R is the element $m \in R$ obtained by adding the multiplicative identity of R to itself m times, and for any variable-free term t, the interpretation of $P_x[t]$ in R is the element

$$P(t_R) = m_0 + m_1 t_R + m_2 t_R^2 + \cdots + m_n t_R^n$$

of R.

2.2 Truth in a Structure

In this section, we shall define when a formula of L is true and when it is false in a structure of L. Note that if we have a structure of L with universe M and we would like to know whether there is an element $a \in M$ satisfying a formula $\varphi[x]$, then we have a bit of a problem because φ is a syntactical object and elements of M are not. To circumvent this problem, given a structure of L with universe M, we first describe an extension L_M of the language L.

Given L and a structure of L with universe M, let L_M be the first-order language obtained from L by adding a new constant symbol i_a for each $a \in M$. The symbol i_a is called the *name* of a. We regard M itself as the expansion of M to L_M by setting the interpretation of i_a to be a for each $a \in M$.

We are now in a position to define when a formula of L is true or valid or satisfiable in the structure M. To achieve this, we define the notion of the truth of a closed formula or a sentence of L_M in the structure M. The definition is based on the well-known intended meaning of the logical connectives $\vee$ and $\neg$ and that of the existential quantifier $\exists$. The notion of truth will be defined by defining a function from the set of all closed formulas of L_M to the set $\{T, F\}$ (T for true and F for false) satisfying some conditions. This will be done by induction on the rank of sentences of L_M. If a sentence takes the value T, we shall say that the sentence is true or valid in M; otherwise, it is said to be false in M.

Recall that formulas have been defined inductively starting from atomic formulas and iterating $\neg$, $\vee$, and $\exists$ on them. A variable-free atomic formula is of the form $pt_1 \cdots t_n$, where p is an n-ary relation symbol (including $=$) and $t_1, \ldots, t_n$ are variable-free terms. We say that $pt_1 \cdots t_n$ is true in the structure if

$$p_M((t_1)_M, \ldots, (t_n)_M)$$

holds, i.e.,

$$((t_1)_M, \ldots, (t_n)_M) \in p_M \subset M^n.$$

Otherwise, we say that $pt_1 \cdots t_n$ is false in the structure. A sentence $\neg A$ is true if and only if A is false. A sentence $A \vee B$ is true if either A is true or B is true. Finally, a sentence $\exists v A$ is true if $A_v[i_a]$ is true for some $a \in M$. We say that a formula A of L_M is true in the structure if its closure is true in the structure. If a formula A of L is true

in a structure M of L, we also say that A is *valid in the structure* and write $M \models A$. If A is not valid in M, then we write $M \not\models A$.

Note that if A and B are closed formulas, then

$$M \models \neg A \Leftrightarrow M \not\models A$$

and

$$M \models A \vee B \Leftrightarrow M \models A \text{ or } M \models B.$$

Exercise 2.2.1. Give an example of a formula (necessarily not closed) of the language of the theory N that is not true and whose negation is not true in the standard structure $\mathbb{N}$ of N. Similarly, give examples of formulas A and B of the language of the theory N such that $A \vee B$ is valid in the standard structure $\mathbb{N}$ but neither A nor B is valid in $\mathbb{N}$.

Exercise 2.2.2. Show the following:

1. A sentence $A \wedge B$ is valid in a structure if and only if both A and B are valid in the structure.
2. A sentence of the form $\forall v \varphi[v]$ is valid in a structure with universe M if and only if for each $a \in M$ the sentence $\varphi_v[i_a]$ of L_M is valid in the structure.
3. A sentence of the form $A \to B$ is valid in a structure if and only if either A is false or B is true in the structure.
4. A sentence of the form $A \leftrightarrow B$ is valid in a structure if and only if either both A and B are valid or both are not valid in the structure.

Exercise 2.2.3. Let $A[v_1, \ldots, v_n]$ be a formula and $t_1, \ldots, t_n$ be variable-free terms of L. Show that the formulas

$$\forall v_1 \cdots \forall v_n A \to A[t_1, \ldots, t_n]$$

and

$$A[t_1, \ldots, t_n] \to \exists v_1 \cdots \exists v_n A$$

are valid in all structures of L.

2.3 Models and Elementary Classes

A *model* of a first-order theory T is a structure of $L(T)$ with universe M in which all nonlogical axioms of T are valid. For instance, any group is a model of group theory. On the other hand, the set $\mathbb{N}$ of natural numbers, together with the usual 0 and $+$ as the interpretations of e and $\cdot$ respectively, is definitely a structure for the language of group theory but not a model of group theory.

Example 2.3.1. Show that the set of all natural numbers

$$\mathbb{N} = \{0, 1, \ldots\}$$

with the usual meanings of S (the successor function), $+$, $\cdot$, and $<$ is a model of the theory N and also of Peano arithmetic. This model will be called the *standard model* of N or of Peano arithmetic.

A formula A of T that is true in all models of T is called *valid* in T. One writes $T \models A$ if A is valid in T. If A is not valid in some model of T, we shall write $T \not\models A$.

Exercise 2.3.2. Let L be an extension of L', M a structure of L, and M' the restriction of M to L'. Note that M and M' have the same individuals. Use the same constant as a name for an individual in M and M'. Show that a statement of $L'_{M'}$ is valid in M' if and only if it is valid in M.

Let M be a structure of L and $Th(M)$ the set of all sentences of L that are true in M. Then $Th(M)$ is called the *Theory of M*.

A class $\mathcal{M}$ of structures of a language L is called *elementary* if there is a theory T with language L such that elements of $\mathcal{M}$ are precisely the models of T. Thus, the classes of infinite sets, dense linearly ordered sets with no first element and no last element, groups, rings, fields, ordered fields, etc., are elementary classes in the corresponding languages.

A field $\mathbb{K}$ is called *algebraically closed* if every nonconstant polynomial $P(X) \in \mathbb{K}[X]$ has a root in $\mathbb{K}$. Let L be the language of rings. For each $n \geq 1$, let A_n denote the formula

$$\forall v_0 \cdots \forall v_n \exists v_{n+1} (v_0 + v_1 \cdot v_{n+1} + \cdots + v_n \cdot v_{n+1}^n = 0).$$

Then the class of all algebraically closed fields is elementary, axiomatized by axioms of fields and $\{A_n : n \geq 1\}$. ACF will denote the theory of algebraically closed fields, $ACF(0)$ that of algebraically closed fields of characteristic 0, and $ACF(p)$ that of algebraically closed fields of characteristic p, p being a prime.

Exercise 2.3.3.
(i) Show that a ring with an identity has more than one element if and only if $0 \neq 1$.
(ii) Show that every algebraically closed field is infinite.
(iii) Show that if $\mathbb{K}$ is a nontrivial ordered field, then $0 < 1$.
(iv) Show that every nontrivial ordered field is of characteristic 0.
(v) Show that every nontrivial ordered field is order-dense.
(vi) Show that if $\mathbb{K}$ is an ordered field, then -1 cannot be written as a sum of squares of finitely many elements in $\mathbb{K}$.
(vii) Show that an algebraically closed field is not *orderable*, i.e., there is no linear order $<$ on the field making it into an ordered field.

Henceforth, we assume that if R is a ring with identity, then $0 \neq 1$.

Example 2.3.4. Let $(R,0,1,+,\cdot)$ be a commutative ring with identity. The *theory of left R-modules* has as its language an extension of abelian groups (with a constant symbol $0'$, a binary function symbol $+'$), and, for each $r \in R$, a unary function symbol $r\cdot$. Its axioms are those of abelian groups and the following sentences:

(1)
$$\forall x(1 \cdot x = x).$$

(2)
$$\forall x \forall y(r \cdot (x +' y) = r \cdot x +' r \cdot y).$$

(3)
$$\forall x((r + s) \cdot x = r \cdot x +' s \cdot x).$$

(4)
$$\forall x(r \cdot (s \cdot x) = (r \cdot s) \cdot x).$$

Models of the theory of left R-modules are called *left R-modules*. If, moreover, R is a field, then they are called *vector spaces over R*.

Let G be an abelian group. For any element $x \in G$, let nx denote the term

$$\underbrace{x + \cdots + x}_{n \text{ times}}.$$

We call a group G *divisible* if for every $n \geq 1$ and every $x \in G$ there exists a $y \in G$ such that $ny = x$. Call G *torsion-free* if for every $x \in G$, $x \neq 0$, and for every $n \geq 1$, $nx \neq 0$. Let $0 \neq x \in G$, and let there exist a positive integer n such $nx = 0$. We call the least such n the *order of x in G*.

Exercise 2.3.5. 1. Show that the class of divisible groups and that of torsion-free groups are elementary.
2. Show that every nontrivial ordered abelian group is torsion-free.
3. Let $n > 1$ be an integer. Show that the class of all nontrivial groups G such that every nonzero element in G is of order n is elementary. Also show that such an n must be prime.
4. Let G be a torsion-free, divisible abelian group. For any $x \in G$ and $n > 1$, show that there is a unique $y \in G$ such that $ny = x$. (Subsequently, we shall denote this y by x/n.)

The theories of divisible abelian groups and ordered divisible abelian groups will be denoted by *DAG* and *ODAG*, respectively.

Remark 2.3.6. For any rational number p/q, $q > 0$ relatively prime to p, define $(p/q)x = p(x/q)$. This makes G a vector space over the field $\mathbb{Q}$ of rationals. Further, if G is uncountable and B is a basis of G as a vector space over $\mathbb{Q}$, then B and G are of the same cardinality.

At this stage it is not possible to give examples of nonelementary classes. For instance, it will be proved later that the class of all finite sets is not elementary. Several more examples will be given later.

2.4 Embeddings and Isomorphisms

In this section we introduce notions analogous to subgroups of a group, isomorphisms of rings, isomorphic fields, etc. in the general context of first-order logic.

In the rest of this section, unless otherwise stated, M and N will denote structures of a fixed first-order language L.

For the sake of brevity, a sequence $(a_1,\dots,a_n) \in N^n$ will sometimes be denoted by $\overline{a}$ and $(i_{a_1},\dots,i_{a_n})$ by $i_{\overline{a}}$. Further, for any map $\alpha : N \to M$, $\alpha(\overline{a})$ will stand for the sequence $(\alpha(a_1),\dots,\alpha(a_n))$.

An *embedding* of N into M is a one-to-one map $\alpha : N \to M$ satisfying the following conditions:

(1) For every constant symbol c of L,

$$\alpha(c_N) = c_M.$$

(2) For every n-ary function symbol f of L and every $\overline{a} \in N^n$,

$$\alpha(f_N(\overline{a})) = f_M(\alpha(\overline{a})).$$

(2) For every n-ary relation symbol p of L and every $\overline{a} \in N^n$,

$$p_N(\overline{a}) \Leftrightarrow p_M(\alpha(\overline{a})),$$

i.e.,

$$\overline{a} \in p_N \Leftrightarrow \alpha(\overline{a}) \in p_M.$$

If, moreover, $\alpha : N \to M$ is a surjection, we call $\alpha : N \to M$ an *isomorphism*. In this case, M and N are called *isomorphic structures*. An *automorphism* of M is an isomorphism from M onto itself.

If $N \subset M$ and the inclusion map $N \hookrightarrow M$ is an embedding, then N is called a *substructure* of M.

Remark 2.4.1. Let N be a subset of a structure M such that for each constant symbol c, $c_M \in N$, and for every function symbol f, N is closed under f_M. We then make N a substructure of M by setting

(i) For every constant symbol c of L,

$$c_N = c_M;$$

(ii) For every n-ary relation symbol p,

$$p_N = p_M \cap N^n,$$

the restriction of p_M to N; and

(iii) For every n-ary function symbol f,

$$f_N = f_M | N^n,$$

the restriction of f_M to N^n.

Example 2.4.2. Let L be the language of group theory. If H is a subgroup of a group G, then H is a substructure of G. If G and H are groups, then a group isomorphism $\alpha : G \to H$ is an isomorphism from the structure G to the structure H.

Note that if G is a group and $H \subset G$ a substructure, then H need not be a subgroup. It is just a subset of G that contains the identity of the group G and is closed under the group operation. For instance, $\mathbb{N} \subset \mathbb{Z}$, the group of all integers, is a substructure but not a subgroup of $\mathbb{Z}$. Similarly, a substructure R' of a ring R with identity is a subset of R containing 0 and 1 and closed under $+$ and $\cdot$, but it may not be a subring.

It will be convenient to have the substructures of a group be a subgroup and those of a ring be its subrings. *Thus, henceforth we shall take the following as the definition of the theory of rings.* Its language is the extension of the language of rings as defined earlier and one more binary function symbol $-$. Its axioms are the axioms of the rings and the following statement:

$$\forall x \forall y \forall z (x - y = z \leftrightarrow x = y + z).$$

Similarly, henceforth the language of groups is augmented with a binary function symbol $-$ and the preceding axiom.

Substructures of a field $\mathbb{F}$ are subrings $\mathbb{D}$ of $\mathbb{F}$ satisfying

$$\forall x \forall y (x \cdot y = 0 \to (x = 0 \vee y = 0)).$$

Such commutative rings with identity are called *integral domains*.

Exercise 2.4.3. Show that if $\mathbb{K}$ is a field, then the ring of polynomials $\mathbb{K}[X_1, \cdots, X_n]$ is an integral domain.

(*Hint*: Let $P(X_1, \cdots, X_n) \cdot Q(X_1, \cdots, X_n) = 0$ and $P \neq 0$. This means that not all coefficients of P are zero and all coefficients of $P \cdot Q$ are zero. By a suitable inductive argument, show that all the coefficients of Q are 0. Also note that this result is true for all integral domains $\mathbb{K}$.)

We now proceed to study the notion of embeddings, isomorphisms, etc. in complete generality. This general study, which is more in the spirit of logic, will turn out to be very useful.

Proposition 2.4.4. *Let $\alpha : N \to M$ be an embedding and $t[v_1, \ldots, v_n]$ a term of L, and let $\overline{a} \in N^n$. Then*

$$\alpha(t[i_{\overline{a}}]_N) = t[i_{\alpha(\overline{a})}]_M.$$

Proof. We prove the result by induction on the rank of t. If t is a variable v_i, then both terms equal $\alpha(a_i)$. If t is a constant c, then the term on the left is $\alpha(c_N)$ and that on the right is c_M. They are equal because α is an embedding.

Now assume that the result is true for $t_1, \ldots, t_k$ and t is the term $f(t_1, \ldots, t_k)$. Then

$$\begin{aligned}
\alpha(t[i_{\overline{a}}]_N) &= \alpha(f_N(t_1[i_{\overline{a}}]_N, \ldots, t_k[i_{\overline{a}}]_N)) \\
&= f_M(\alpha(t_1[i_{\overline{a}}]_N), \ldots, \alpha(t_k[i_{\overline{a}}]_N)) \\
&= f_M(t_1[i_{\alpha(\overline{a})}]_M, \ldots, t_k[i_{\alpha(\overline{a})}]_M) \\
&= t[i_{\alpha(\overline{a})}]_M.
\end{aligned}$$

The first equality holds by the definition of $t[i_{\overline{a}}]_N$, the second equality holds because α is an embedding, the third equality holds by the induction hypothesis, and the fourth equality holds by the definition of $t[i_{\alpha(\overline{a})}]_M$.

The proof is complete. □

Proposition 2.4.5. *Let $\alpha : N \to M$ be an embedding and $\varphi[v_1, \ldots, v_n]$ an open formula of L, and let $\overline{a} \in N^n$. Then*

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \qquad (*)$$

Proof. Recall that the set of all open formulas is the smallest class of formulas that contains all atomic formulas and is closed under $\neg$ and $\vee$. Thus, the result will be proved if we show that the set of formulas φ satisfying $(*)$ contains all atomic formulas and is closed under $\neg$ and $\vee$.

By the definition of the truth in a structure, the definition of embedding, and Proposition 2.4.4, $(*)$ holds for formulas of the form $t = s$ as well as for atomic formulas of the form $p(t_1, \ldots, t_n)$.

Now assume that φ is the formula $\neg\psi$ and the result is true for ψ. Then

$$\begin{aligned}
N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \not\models \psi[i_{\overline{a}}] \\
&\Leftrightarrow M \not\models \psi[i_{\alpha(\overline{a})}] \\
&\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].
\end{aligned}$$

The first and last equivalences hold because the formulas $\psi[i_{\overline{a}}]$ and $\psi[i_{\alpha(\overline{a})}]$ are closed; the second equivalence holds by the induction hypothesis.

The case φ of the form $\psi \vee \eta$ is dealt with similarly:

$$\begin{aligned}
N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \models \psi[i_{\overline{a}}] \text{ or } N \models \eta[i_{\overline{a}}] \\
&\Leftrightarrow M \models \psi[i_{\alpha(\overline{a})}] \text{ or } M \models \eta[i_{\alpha(\overline{a})}] \\
&\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].
\end{aligned}$$

The proof is complete. □

Exercise 2.4.6. Let $\alpha : N \to M$ be a map such that for every atomic $\varphi[v_1, \ldots, v_n]$ and every $\overline{a} \in N^n$,

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].$$

Show that α is an embedding.

(*Hint*: To show that for any constant symbol c, $\alpha(c_N) = c_M$, let the formula $\varphi[x]$ be $c = x$ and consider $\varphi[i_{c_N}]$; to show that for $a, b \in N$, $\alpha(a) = \alpha(b)$ implies $a = b$, let $\varphi[x, y]$ be the formula $x = y$ and consider $\varphi[i_a, i_b]$, etc.)

Our next result gives a method to build an extension of a structure. Let M be a structure of a first-order language L. We define the *atomic diagram* , or simply the *diagram* of M, denoted by $Diag(M)$, by

$$Diag(M) = \{\varphi[i_{\overline{a}}] : \overline{a} \in M, M \models \varphi[i_{\overline{a}}], \varphi \text{ an atomic formula of } L\}.$$

Proposition 2.4.7. *If $N \models Diag(M)$, then M has an embedding into N.*

Proof. For $a \in M$, take $\alpha(a) = (i_a)_N$. By Exercise 2.4.6, $\alpha : M \to N$ is an embedding. □

Theorem 2.4.8. *Let $\alpha : N \to M$ be an isomorphism and $\varphi[v_1, \ldots, v_n]$ a formula of L_N. Then for every $\overline{a} \in N^n$,*

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \qquad (**)$$

In particular, for every sentence φ of L, $N \models \varphi$ if and only if $M \models \varphi$.

Proof. Since an isomorphism is an embedding, by the arguments contained in the proof of Proposition 2.4.5, the set of all formulas φ satisfying $(**)$ contains all atomic formulas and is closed under $\neg$ and $\vee$.

Let $\varphi[v_1, \ldots, v_n]$ be a formula of the form $\exists v \psi$, with v different from each of the v_i. Suppose $(**)$ holds for ψ and all $(a, a_1, \ldots, a_n) \in N^{n+1}$. To complete the proof, we now have only to show that $(**)$ holds for φ and every $\overline{a} \in N^n$. Thus, we take any $\overline{a} \in N^n$. Then

$$\begin{aligned} N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \models \psi[i_a, i_{\overline{a}}] \text{ for some } a \in N \\ &\Leftrightarrow M \models \psi[i_{\alpha(a)}, i_{\alpha(\overline{a})}] \text{ for some } a \in N \\ &\Leftrightarrow M \models \psi[i_b, i_{\alpha(\overline{a})}] \text{ for some } b \in M \\ &\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \end{aligned}$$

The first equivalence holds by the definition of validity in N, the second equivalence holds by the induction hypothesis, the third equivalence holds because α is surjective, and the last equivalence holds by the definition of validity in M.

The proof is complete. □

An embedding $\alpha : N \to M$ is called an *elementary embedding* if for every formula $\varphi[v_1, \ldots, v_n]$ and every $\overline{a} \in N^n$,

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].$$

If $N \subset M$ and the inclusion $N \hookrightarrow M$ is an elementary embedding, then we say that N is an *elementary substructure* of M or that M is an *elementary extension* of N. The structures N and M are called *elementarily equivalent* if for every closed formula φ,

$$N \models \varphi \Leftrightarrow M \models \varphi.$$

We write $N \equiv M$ if N and M are elementarily equivalent. Clearly, $\equiv$ is an equivalence relation on the class of all structures of L.

Below we present a method to build an elementary extension of a structure. Let M be a structure of a first-order language L. We define the *elementary diagram* of M, denoted by $Diag_{el}(M)$, by

$$Diag_{el}(M) = \{\varphi[i_{\overline{a}}] : \overline{a} \in M, M \models \varphi[i_{\overline{a}}],\ \varphi \text{ a formula of } L\}.$$

As before, we have the following result.

Proposition 2.4.9. *If $N \models Diag_{el}(M)$, then M has an elementary embedding into N.*

Remark 2.4.10. By Theorem 2.4.8, two structures N and M are elementarily equivalent if they are isomorphic. Later on in the book we shall show that any two algebraically closed fields of characteristic 0 are elementarily equivalent. But the field $\overline{\mathbb{Q}}^{\text{alg}}$ of algebraic numbers and the field $\mathbb{C}$ of complex numbers are two algebraically closed fields of characteristic 0 that are not even of the same cardinality. Hence, elementarily equivalent structures need not be isomorphic. Later in these pages we shall show that an elementary embedding $\alpha : N \to M$ need not be surjective.

Theorem 2.4.11. *Let N be a substructure of M. Then N is an elementary substructure of M if and only if for every formula $\varphi[v, v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$, if there is a $b \in M$ satisfying*

$$M \models \varphi[i_b, i_{\overline{a}}],$$

then there is a $b \in N$ satisfying

$$M \models \varphi[i_b, i_{\overline{a}}].$$

Proof. Let N be an elementary substructure of M. Take a formula $\varphi[v, v_1, \ldots, v_n]$. Let $\overline{a} \in N^n$, and suppose there is a $b \in M$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$. This means that $M \models \exists v \varphi[v, i_{\overline{a}}]$. Since N is an elementary substructure of M, we have $N \models \exists v \varphi[v, i_{\overline{a}}]$. Thus, there is a $b \in N$ satisfying $N \models \varphi[i_b, i_{\overline{a}}]$. Since N is an elementary substructure of M, $M \models \varphi[i_b, i_{\overline{a}}]$.

We prove the *if* part of the result by showing that for every formula $\psi[v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$,

$$N \models \psi[i_{\overline{a}}] \Leftrightarrow M \models \psi[i_{\overline{a}}]. \qquad (*)$$

We shall prove $(*)$ by induction on the rank of ψ. By Proposition 2.4.5, $(*)$ is true for all atomic formulas. Arguing as in the proof of that proposition, we can show that if $(*)$ is true for φ, then it is true for $\neg\varphi$, and if φ and ψ satisfy $(*)$, then so does $\varphi \vee \psi$.

Now assume that $\varphi[v_1,\ldots,v_n]$ is a formula of the form $\exists v\psi[v,v_1,\ldots,v_n]$ and $(*)$ holds for ψ and every $(a,a_1,\ldots,a_n) \in N^{n+1}$. Take $\overline{a} \in N^n$.

Suppose $N \models \varphi[i_{\overline{a}}]$. Then there is a $b \in N$ such that $N \models \psi[i_b, i_{\overline{a}}]$. By the induction hypothesis, $M \models \psi[i_b, i_{\overline{a}}]$. Thus, $M \models \varphi[i_{\overline{a}}]$.

Now assume that $M \models \varphi[i_{\overline{a}}]$. So there is a $b \in M$ such that $M \models \psi[i_b, i_{\overline{a}}]$. By our assumptions, there is a $b \in N$ such that $M \models \psi[i_b, i_{\overline{a}}]$. By the induction hypothesis, $N \models \psi[i_b, i_{\overline{a}}]$. Thus, $N \models \varphi[i_{\overline{a}}]$. □

2.5 Some Examples

Let $L(<)$ be a language with only one binary relation symbol $<$.

Proposition 2.5.1. *If $(M,<)$ is a countable linearly ordered set, then there is an embedding $\alpha : M \to \mathbb{Q}$, where $\mathbb{Q}$ is the set of all rational numbers with usual ordering.*

Proof. Let $r_0, r_1, \ldots$ be an enumeration of M such that the r_i are distinct. We define $\alpha(r_n)$ by induction on n. Set $\alpha(r_0) = 0$. Suppose $n > 0$, and $\alpha : \{r_i \in M : i < n\} \to \mathbb{Q}$ has been defined so that it is order-preserving. Since $\mathbb{Q}$ is a dense linearly ordered set with no first element and no last element, there is a $\alpha(r_n) \in \mathbb{Q}$ such that $\alpha : \{r_i \in M : i \leq n\} \to \mathbb{Q}$ is order-preserving. Thus we have defined an embedding $\alpha : M \to \mathbb{Q}$. □

Theorem 2.5.2. *Any two countable models $\mathbb{Q}_1$ and $\mathbb{Q}_2$ of DLO are isomorphic.*

Proof. Let $\{r_n\}$ and $\{s_m\}$ be enumerations of $\mathbb{Q}_1$ and $\mathbb{Q}_2$, respectively. Set $n_0 = 0$ and $m_0 = 0$. Suppose for some i, $n_0,\ldots,n_{2i}$ and $m_0,\ldots,m_{2i}$ have been defined so that the map f defined by

$$f(r_{n_j}) = s_{m_j},\ 0 \leq j \leq 2i,$$

is injective and order-preserving. Now let m_{2i+1} be the first natural number k such that s_k is different from each s_{m_j}, $j \leq 2i$. Show that there is a natural number l such that r_l is different from each r_{n_j}, $j \leq 2i$, and the extension of f sending r_l to $s_{m_{2i+1}}$ is order-preserving. Set n_{2i+1} to be the first such l. Thus, the map $f(r_{n_j}) = s_{m_j}$, $j \leq 2i+1$, is injective and order-preserving. Now define n_{2i+2} to be the first natural number l such that r_l is different from each r_{n_j}, $j \leq 2i+1$. Again, observe that there is a natural number k such that s_k is different from each s_{m_j}, $j \leq 2i+1$, and the extension of the preceding map by defining $f(r_{n_{2i+2}}) = s_k$ is order-preserving. Set s_{2i+2} to be the least such k. It is easily checked that $f : \mathbb{Q}_1 \to \mathbb{Q}_2$ is an isomorphism. □

Remark 2.5.3. The method of the foregoing proof is fairly common and will be repeated several times. It is known as the back-and-forth argument.

Exercise 2.5.4. Let $A \subset \mathbb{Q}$ be finite and $f : A \to \mathbb{Q}$ be an order-preserving, one-to-one map. Show that there is an order-preserving bijection $g : \mathbb{Q} \to \mathbb{Q}$ extending f.

Proposition 2.5.5. *Two divisible torsion-free abelian uncountable groups G_1 and G_2 are isomorphic if and only if they are of the same cardinality.*

Proof. We need to prove the *if* part only. Since the G_i are uncountable and of the same cardinality, they are of the same dimension as vector spaces over $\mathbb{Q}$. Hence, G_1 and G_2 are isomorphic as vector spaces over $\mathbb{Q}$. In particular, they are isomorphic as groups. □

Corollary 2.5.6. *The additive groups of real and complex numbers are isomorphic.*

Exercise 2.5.7. Show that the theory of divisible, torsion-free abelian groups has exactly $\aleph_0$-many nonisomorphic countable models such that any other countable model is isomorphic to one of these models.

Proposition 2.5.8. *Let $\mathbb{D}$ be an integral domain. Then there is a field $\mathbb{F}$ and an embedding $q : \mathbb{D} \to \mathbb{F}$ such that for every field $\mathbb{K}$ and every embedding $r : \mathbb{D} \to \mathbb{K}$, there is a unique embedding $s : \mathbb{F} \to \mathbb{K}$ such that $s \circ q = r$.*

We give only a sketch of the proof. The routine verifications are left to the reader as an exercise.

Proof. Set

$$E = \{(a,b) \in \mathbb{D} \times \mathbb{D} : b \neq 0\}.$$

We define an equivalence relation $\sim$ on E by

$$(a,b) \sim (c,d) \Leftrightarrow a \cdot d = b \cdot c$$

and set

$$\mathbb{F} = E/\sim \ = \left\{ \frac{a}{b} : (a,b) \in E \right\},$$

the set of all $\sim$-equivalence classes, i.e., $\frac{a}{b}$ denotes the equivalence class containing (a,b). We define

$$0 = \frac{0}{1}, 1 = \frac{1}{1},$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

It is easily checked that these are well defined and make $\mathbb{F}$ a field.

Now define $q : \mathbb{D} \to \mathbb{F}$ by

$$q(a) = \frac{a}{1}, a \in \mathbb{D}.$$

Then $q : \mathbb{D} \to \mathbb{F}$ is an embedding.

Given any embedding r of $\mathbb{D}$ into a field $\mathbb{K}$, define $s : \mathbb{F} \to \mathbb{K}$ by

$$s(\frac{a}{b}) = r(a) \cdot r(b)^{-1}, \ \ \frac{a}{b} \in \mathbb{F}. \qquad \square$$

It is easy to verify that if $q' : \mathbb{D} \to \mathbb{F}'$ is another such pair, then there is an isomorphism $h : \mathbb{F}' \to \mathbb{F}$ such that $h \circ q' = q$. In particular, $\mathbb{F}$ is unique up to isomorphism. Such an $\mathbb{F}$ is called the *quotient field* of $\mathbb{D}$.

Example 2.5.9. The field of rational numbers $\mathbb{Q}$ is the quotient field of the ring of integers $\mathbb{Z}$.

Example 2.5.10. If $\mathbb{K}[X_1, \cdots, X_n]$ is the ring of polynomials over a field $\mathbb{K}$, then its quotient field is denoted by $\mathbb{K}(X_1, \cdots, X_n)$. Its elements are called *rational functions over* $\mathbb{K}$. As described previously, its elements can be thought of as the formal quotients of two polynomials.

Similar results are true for torsion-free abelian groups and ordered abelian groups.

Proposition 2.5.11. *Let H be a torsion-free abelian group. Then there is a torsion-free, divisible abelian group G and an embedding $\alpha : H \to G$ such that for every torsion-free, divisible abelian group G' and every embedding $\beta : H \to G'$, there is a unique embedding $\gamma : G \to G'$ such that $\beta = \gamma \circ \alpha$.*

Proof. Set

$$E = \{(h, n) : h \in H, n > 0\}.$$

Define an equivalence relation $\sim$ on E by

$$(h, n) \sim (h', n') \Leftrightarrow n'h = nh'.$$

Let $\frac{h}{n}$ denote the equivalence class containing $(h, n) \in E$, and set

$$G = E/\sim \ = \left\{ \frac{h}{n} : (h, n) \in E \right\},$$

$$0 = \frac{0}{1},$$

$$\frac{h}{n} + \frac{h'}{n'} = \frac{n'h + nh'}{nn'},$$

and

$$\alpha(h) = \frac{h}{1}, h \in H.$$

Then these are well defined and make G a group with $\alpha : H \to G$ an embedding. Now given a torsion-free, divisible abelian group G' and an embedding $\beta : H \to G'$, define $\gamma : G \to G'$ by

$$\gamma\left(\frac{h}{n}\right) = \frac{\beta(h)}{n}, \quad \frac{h}{n} \in G,$$

where $\frac{\beta(h)}{n}$ is the unique element g of G' such that $ng' = \beta(h)$. □

The group G obtained above is unique up to isomorphism and is called the *divisible hull* of H.

Proposition 2.5.12. *Let H be an ordered abelian group. Then there is a divisible, ordered abelian group G and an embedding $\alpha : H \to G$ such that for every divisible, ordered abelian group G' and every embedding $\beta : H \to G'$ there is a unique embedding $\gamma : G \to G'$ such that $\beta = \gamma \circ \alpha$.*

Proof. Let $<$ denote the ordering on H. Recall that every ordered abelian group is torsion-free. We proceed as in the proof of Proposition 2.5.11 and define

$$\frac{h}{n} < \frac{h'}{n'} \Leftrightarrow n'h < nh'.$$ □

The ordered abelian group G is unique up to isomorphism and is called an *ordered divisible hull* of H.

A ring R is called orderable if there is a linear order $<$ on R such that for every $x, y, z \in R$ the following conditions are satisfied.

1. $0 < x$ and $0 < y$ imply $0 < x \cdot y$.
2. $x < y$ implies $x + z < y + z$.

Let D be an ordered integral domain and $\mathbb{K}$ its quotient field. Note that every element of $\mathbb{K}$ can be expressed in the form $\frac{c}{d} \in \mathbb{K}$ with $d > 0$.

Proposition 2.5.13. *Let D be an ordered integral domain and $\mathbb{K}$ its quotient field. For $\frac{a}{b}, \frac{c}{d} \in \mathbb{K}$ with $b, d > 0$, define*

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow a \cdot d < b \cdot c$$

and

$$\alpha(a) = \frac{a}{1}, \ a \in D.$$

This makes the quotient field $\mathbb{K}$ an ordered field with $\alpha : D \to \mathbb{K}$ an order-preserving embedding. Further, for every ordered field $\mathbb{F}$ and every order-preserving embedding $\beta : D \to \mathbb{F}$, there is a unique order-preserving embedding $\gamma : \mathbb{K} \to \mathbb{F}$ such that $\gamma \circ \alpha = \beta$.

Its entirely trivial proof is left to the reader as an exercise.

2.6 Homogeneous Structures

Let M and N be structures for a language L and $A \subset M$. A map $f : A \to N$ is called *partial elementary* if for every formula $\varphi[\overline{x}]$ and every $\overline{a} \in A$,

$$M \models \varphi[i_{\overline{a}}] \Leftrightarrow N \models \varphi[i_{f(\overline{a})}].$$

Note that a partial elementary map must be injective. Also, if f is partial elementary, then so is f^{-1}.

Remark 2.6.1. If $A = \emptyset \subset M$, then $f : A \to N$ (the empty function) is partial elementary if and only if M and N are elementarily equivalent. In particular, if for some $A \subset M$ there is a partial elementary map $f : A \to N$, then M and N are necessarily elementarily equivalent.

Let κ be an infinite cardinal. We call M *κ-homogeneous* if for all $A \subset M$ of cardinality less than κ, for all partial elementary maps $f : A \to M$, and for all $a \in M$, there is a partial elementary map $g : A \cup \{a\} \to M$ extending f. We call M *homogeneous* if it is $|M|$-homogeneous, where $|M|$ denotes the cardinality of M. We call a theory T *homogeneous* if all its models are homogeneous.

Example 2.6.2. The linearly ordered set of rationals $\mathbb{Q}$ is homogeneous. Let $A \subset \mathbb{Q}$ be finite and $f : A \to \mathbb{Q}$ a partial elementary. Then f is an order-preserving injection. In a slight modification of the argument contained in the proof of Theorem 2.5.2, we see that there is an order-preserving bijection $g : \mathbb{Q} \to \mathbb{Q}$ extending f. Thus, for every formula $\varphi[\overline{x}]$ and every $\overline{a} \in Q$,

$$\mathbb{Q} \models \varphi[i_{\overline{a}}] \Leftrightarrow \mathbb{Q} \models \varphi[i_{g(\overline{a})}].$$

Our contention now follows.

Following the back-and-forth argument, we have the following theorem.

Theorem 2.6.3. *Let M be a countable homogeneous structure of a language L, and let $A \subset M$ be finite. Then every partial elementary map $f : A \to M$ can be extended to an automorphism of M.*

Proof. Fix an enumeration $\{x_n\}$ of the elements of M. Set $f_{-1} = f$. We shall define a sequence $\{f_n\}$ of finite partial elementary maps such that for every n, f_{n+1} extends f_n and x_n belongs to the domain as well as to the range of f_n.

Assume f_n is defined. If $x_{n+1} \in \mathit{domain}(f_n)$, then set $g = f_n$. If $x_{n+1} \notin \mathit{domain}(f_n)$, then, by homogeneity, there is a partial elementary $g : \mathit{domain}(f_n) \cup \{x_{n+1}\} \to M$. Now, if $x_{n+1} \in \mathit{range}(g)$, then we set $f_{n+1} = g$. Otherwise, we take f_{n+1} to be the inverse of a partial elementary map $h : \mathit{range}(g) \cup \{x_{n+1}\} \to M$ extending g^{-1}, which exists by the homogeneity of M.

The map $f_\infty = \cup_n f_n$ is an automorphism of M extending f. □

Using the method of transfinite induction we can easily see that this result can be extended to all homogeneous structures as follows.

Theorem 2.6.4. *Let M be a homogeneous structure of a language L and $A \subset M$ of cardinality less than that of M. Then every partial elementary map $f : A \to M$ can be extended to an automorphism of M.*

Proof. We assume that $|M| > \aleph_0$. Enumerate $M \setminus A = \{a_\alpha : \alpha < |M|\}$, and set $f_0 = f$. By transfinite induction, for each $\alpha < |M|$, we define a partial elementary map $f_\alpha : A \cup \{a_\beta : \beta < \alpha\}$ such that for $\beta < \alpha < |M|$, f_α extends f_β.

Suppose $f_\alpha : A \cup \{a_\beta : \beta < \alpha\} \to M$ has been defined and is partial elementary. Since $|A \cup \{a_\beta : \beta < \alpha\}| < |M|$, by homogeneity, there is a partial elementary extension $f_{\alpha+1} : A \cup \{a_\beta : \beta \leq \alpha\} \to M$ of f_α.

If α is a limit ordinal and f_β, $\beta < \alpha$, have been defined, then we take $f_\alpha = \cup_{\beta<\alpha} f_\beta$. Finally, $g = \cup_{\alpha<|M|} f_\alpha : M \to M$ is a partial elementary map that extends f. □

Let M be a structure for a language L and $\overline{a} \in M^n$. We define

$$tp^M(\overline{a}) = \{\varphi[\overline{x}] : M \models \varphi[i_{\overline{a}}]\}$$

and call it a *complete n-type realized by* $\overline{a}$. Types play a very important role in model theory. $tp^M(\overline{a})$ may be thought of as the set of all properties $\varphi[\overline{x}]$ satisfied by $\overline{a}$.

Theorem 2.6.5. *Let M be a homogeneous structure for a language L and $\overline{a}, \overline{b} \in M^n$. Then $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if there is an automorphism $\alpha : M \to M$ with $\alpha(\overline{a}) = \overline{b}$.*

Proof. Observe that $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if the map $\overline{a} \to \overline{b}$ is partial elementary and use Theorem 2.6.4. □

Using the back-and-forth argument, we get the following proposition.

Proposition 2.6.6. *Let M and N be countable homogeneous structures for a language L such that for every $k \geq 1$,*

$$\{tp^M(\overline{a}) : \overline{a} \in M^k\} = \{tp^N(\overline{b}) : \overline{b} \in N^k\}.$$

Then M and N are isomorphic.

Proof. Fix enumerations $\{a_k\}$ and $\{b_k\}$ of M and N, respectively.

Set $a'_0 = a_0$, and consider $tp^M(a'_0)$. By our hypothesis, there is a $b \in N$ such that $tp^M(a'_o) = tp^N(b)$. Let b'_0 be the first such b in the preceding enumeration of N.

Now let b'_1 be the first element in the enumeration of N different from b'_0. By our hypothesis, there exist $a, a' \in M$ such that $tp^M(a, a') = tp^N(b'_0, b'_1)$. In particular, $tp^M(a) = tp^N(b'_0) = tp^M(a'_0)$. Thus, $a \to a'_0$ is partial elementary. Since M is homogeneous, there is an $a'' \in M$ such that $(a, a') \to (a'_0, a'')$ is partial elementary. Therefore, $tp^N(b'_0, b'_1) = tp^M(a, a') = tp^M(a'_0, a'')$. Since $b'_0 \neq b'_1$, $x \neq y$ is in $tp^N(b'_0, b'_1)$. This implies that $a'_0 \neq a''$. We let a'_1 denote the first such a'' in the enumeration of M.

Now let a'_2 be the first element in the enumeration of M not belonging to $\{a'_0, a'_1\}$. By our hypothesis, there exist $b, b', b'' \in N$ such that $tp^N(b,b',b'') = tp^M(a'_0,a'_1,a'_2)$. In particular, $tp^N(b,b') = tp^M(a'_0,a'_1) = tp^N(b'_0,b'_1)$. Thus, $(b,b') \to (b'_0,b'_1)$ is partial elementary. Since N is homogeneous, there exists a $b''' \in N$ such that $(b,b',b'') \to (b'_0,b'_1,b''')$ is partial elementary. Hence, $tp^N(b'_0,b'_1,b''') = tp^N(b,b',b'') = tp^M(a'_0,a'_1,a'_2)$. Since $a'_2 \notin \{a'_0,a'_1\}$, $b''' \notin \{b'_0,b'_1\}$. Let b'_2 be the first such b''' in the enumeration of N.

Continuing this back-and-forth method, we shall get enumerations $\{a'_k\}$ and $\{b'_k\}$ of M and N, respectively, such that for every k, $(a'_o, \cdots, a'_k) \to (b'_o, \cdots, b'_k)$ is partial elementary. Plainly, $a'_i \to b'_i$ defines an isomorphism from M to N. □

2.7 Downward Löwenheim–Skolem Theorem

In this section we present a method of constructing elementary substructures of small cardinality. From this it will follow that if a countable theory has a model, then it has a countable model. In particular, if there is a model of set theory, then there is a countable model of set theory. This is an important result in set theory. In Chap. 5, we will present a method to construct elementary extensions of arbitrarily large cardinalities.

Theorem 2.7.1 (Downward Löwenheim–Skolem theorem). *Let M be a structure of L and $X \subset M$. Suppose L has at most κ nonlogical symbols and κ an infinite cardinal number. Then there is an elementary substructure N of M such that $X \subset N$ and the cardinality of N is at most* $\max(\kappa, |X|)$*, where $|X|$ denotes the cardinality of X.*

Proof. Essentially, our N will be the smallest subset of M containing X satisfying the following conditions:

(i) Each $c_M \in N$, where c is a constant symbol of L.
(ii) The set N is closed under f_M for every function symbol f of L.
(iii) Whenever a sentence of the form $\exists v \varphi$ is valid in M, there is an element $a \in N$ such that $M \models \varphi_v[i_a]$.

By induction on k, we shall define

$$N_0 \subset N'_1 \subset N_1 \subset \ldots \subset N_k \subset N'_k \subset N_{k+1} \subset \ldots \subset M$$

such that each N'_k is a substructure of N and for every formula of the form $\exists v \varphi[v, v_1, \ldots, v_n]$ and every $\overline{a} \in N'^n_k$, if $M \models \exists v \varphi[v, i_{\overline{a}}]$, then there is a $b \in N_{k+1}$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. Further, each N_k is of cardinality $\leq \max(\kappa, |X|)$.

Let N_0 be the smallest subset of M containing X that contains all c_M and that is closed under all f_M. Note that $|N_0| \leq \max(\kappa, |X|)$ and that N_0 is a substructure of M.

Suppose N_k has been defined such that $|N_k| \leq \max(\kappa, |X|)$. Now we define N_k' and N_{k+1}. Let N_k' be the smallest subset of M containing N_k that is closed under all f_M. Then $|N_k'| \leq \max(\kappa, |X|)$.

Fix a formula of the form $\varphi[v, v_1, \ldots, v_n]$. Let ψ be the formula $\exists v \varphi$. For every $\overline{a} = (a_1, \ldots, a_n) \in (N_k')^n$, whenever $M \models \psi[i_{\overline{a}}]$, there is a $b \in M$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. Choose and fix one such b. Let N_{k+1} be obtained from N_k' by adding all the b thus chosen. Again note that $|N_{k+1}| \leq \max(\kappa, |X|)$.

Set

$$N = \cup_k N_k.$$

Then:

(i) For every constant symbol c, $c_M \in N$;
(ii) For every function symbol f, N is closed under f_M;
(iii) $|N| \leq \max(\kappa, |X|)$ and $X \subset N$.

Thus, N is a substructure of M as in Remark 2.4.1.

Let $\varphi[v_1, \ldots, v_n]$ be any formula and $\overline{a} \in N^n$. Since N is a substructure of M, by Theorem 2.4.11, the proof will be complete if we show that for every formula $\varphi[v, v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$, if there is a $b \in M$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$, then there is a $b \in N$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$. Let $\varphi[v, v_1, \ldots, v_n]$ be a formula, and let $\overline{a} \in N^n$ and $b \in M$ be such that $M \models \varphi[i_b, i_{\overline{a}}]$. Since $N_k \subset N_{k+1}$ for all k, there is a natural number p such that each $a_i \in N_p$. By the definition of N_{p+1}, there is a $b \in N_{p+1} \subset N$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. □

Remark 2.7.2. In the foregoing proof we used an important axiom of set theory called the axiom of choice.

Axiom of choice: If $\{X_i : i \in I\}$ is a family of nonempty sets, then there is a map $f : I \to \cup_{i \in I} X_i$ such that $f(i) \in X_i$ for all $i \in I$.

A function f satisfying the conclusion of the axiom of choice is called a *choice function* for the family $\{X_i : i \in I\}$. The axiom of choice asserts only the existence of a choice function – it gives no method to produce a choice function.

The theory obtained by adding the axiom of choice to the axioms of *ZF* is denoted by *ZFC*.

Corollary 2.7.3. *If a countable theory has a model, then it has a countable model.*

Corollary 2.7.4. *If ZF (or ZFC) has a model, then it has a countable model M.*

Remark 2.7.5. This seemingly paradoxical result calls for an explanation. First, we call a set x *transitive* if $y \in x \Rightarrow y \subset x$. In *ZF*, it can be shown that if M is a countable model of *ZF*, then it has a countable transitive model. Thus, we assume that M is countable and transitive.

Now, *ZF* proves that *there is an uncountable set*. Since M is a model of *ZF*, this statement is true in the model M. In particular, there is a set x in M such that

$$M \models |x| > \aleph_0.$$

Since M is transitive, $x \subset M$. But M itself is countable!

In the real world V (a model of *ZFC* in the present case, assuming that it exists), M is countable. Thus, in the real world there is a function f from $\mathbb{N}$ onto x. We have not asserted that such an $f \in M$. And in our situation, no such f belongs to M. This is not a contradiction at all.

Let $(R,<)$ be a linearly ordered set and $A \subset R$. An element u of R is called an *upper bound of* A if for every $a \in A$, $a \leq u$, where $x \leq y$ means that either $x < y$ or $x = y$. If u is an upper bound of A and no $v < u$ is an upper bound of A, then u is called the *least upper bound* of A. A linearly ordered set R is called *complete* if every nonempty subset A of R that has an upper bound has a least upper bound.

Proposition 2.7.6 (Cantor). *Every complete, order-dense, linearly ordered set $(R,<)$ with more than one element is uncountable.*

Proof. If possible, assume that R is countable. We shall arrive at a contradiction. Fix an enumeration $R = \{r_n\}$ of R. Let $x_0 < y_0$ be two distinct points of R. Since R is order-dense, there is a $x \in R$ such that $x_0 < x < y_0$. Let n be the first integer such that $x_0 < r_n < y_0$. Set $x_1 = r_n$. Since R is order-dense, there is a $y \in R$ such that $x_1 < y < y_0$. Set $y_1 = r_m$, where m is the first natural number with $x_1 < r_m < y_0$. Assuming, $x_0 < \cdots < x_n < y_n < \cdots < y_0$ have been defined, set x_{n+1} to be the first r_l such that $x_n < r_l < y_n$. Then take y_{n+1} to be the first r_k such that $x_{n+1} < r_k < y_n$.

Since $\{x_n\}$ is bounded above, it has a least upper bound, say r_p. Clearly, $r_p \leq y_n$ for all n. But, by our construction, no r_p can be the least upper bound of $\{x_n\}$. This contradiction proves our result. □

Here is an interesting corollary.

Corollary 2.7.7. *Let $L = L(<)$ be a language with only one nonlogical symbol, a binary relation symbol. Then the class $\mathcal{M}$ of all complete, order-dense, linearly ordered $L(<)$-structures with more than one point is not elementary.*

Proof. Suppose T is a theory with language $L(<)$ whose models are precisely the structures in $\mathcal{M}$. Clearly, T has a model. Since T is countable, T has a countable model. But, by Cantor's theorem, no structure in $\mathcal{M}$ is countable. □

Exercise 2.7.8. Show that the class of all complete ordered fields is not elementary.

2.8 Definability

In this section, we introduce the interesting and important notion of definability. This gives rise to interesting questions and applications in mathematics, which is very important from a logic point of view, too. For instance, this formed the basis for Gödel's model of constructible sets in which the axiom of choice and the continuum hypothesis hold. This also plays an important role in decidability questions pertaining to models.

Throughout this section, unless otherwise stated, M will stand for a structure of a language L.

For $n \geq 1$, $X \subset M^n$ is called *definable* (in the language L) if there is a formula $\varphi[v_1, \cdots, v_n, w_1, \cdots, w_m]$ of L and a $\overline{b} \in M^m$ such that

$$\overline{a} \in X \Leftrightarrow M \models \varphi[i_{\overline{a}}, i_{\overline{b}}].$$

$\overline{b}$ is called the *parameters*. If the parameters come from a subset A of M, we call X A-definable. Note that if X is definable, it is A-definable for some finite $A \subset M$. A function $f : M^k \to M^l$ is called definable if its graph is definable. An element $a \in M$ is called A-definable if the singleton set $\{a\}$ is A-definable.

Example 2.8.1. Let M be a structure for a language L. Then every finite $D \subset M^n$ is definable. To see this when $n = 1$, let $D = \{a_1, \cdots, a_k\} \subset M$. Then the formula $\vee_{i=1}^{k}(x = i_{a_i})$ defines D. The proof for $n > 1$ is left to the reader as an exercise.

Example 2.8.2. If c, f, and p are respectively constant, function, and relation symbols of L, then their interpretations c_M, f_M, and p_M are $\emptyset$-definable. The formula $x = c$ defines c_M, the formula $y = fx_1 \cdots x_n$ defines f_M, with f an n-ary function symbol, whereas the formula $py_1 \cdots y_m$ defines p_M, with p an m-ary relation symbol.

Since formulas are described inductively, it is natural to expect an inductive definition of definable sets, which we present in the next lemma. Its entirely routine proof is left as an exercise for the reader. For a set M, a family of subsets of M^n, $n \geq 1$, will be called a *pointclass*.

Lemma 2.8.3. *Let M be a structure of a language L. The pointclass of all definable subsets of M^n, $n \geq 1$, is the smallest pointclass $\mathcal{D}$ satisfying the following conditions:*

1. *$\{c_M\}$, p_M and the graph of f_M, c, p, and f respectively constant, relation, and function symbols of L, belong to $\mathcal{D}$.*
2. *The set $\{\overline{a} \in M^n : a_i = a_j\} \in \mathcal{D}$, $1 \leq i < j \leq n$.*
3. *If $A \subset M^{n+m}$ is in $\mathcal{D}$ and $\overline{b} \in M^m$, then the section*

$$A_{\overline{b}} = \{\overline{a} \in M^n : (\overline{a}, \overline{b}) \in A\} \in \mathcal{D}.$$

4. *If $A, B \subset M^n$ are in $\mathcal{D}$, then so are $A \cup B$ and $M^n \setminus A$.*
5. *If $A \subset M^{n+1}$ is in $\mathcal{D}$, then so is its projection*

$$\pi(A) = \{\overline{a} \in M^n : \exists a \in M((\overline{a}, a) \in A)\}.$$

Exercise 2.8.4. 1. Show that the pointclass $\mathcal{D}$ of definable sets is closed under finite intersections and under substitutions by definable functions, i.e., if $A \subset M^n$ is in $\mathcal{D}$ and $f_1, \cdots, f_n : M^m \to M$ are definable, then so is the set $B \subset M^m$ defined by

$$\overline{a} \in B \Leftrightarrow \overline{f}(\overline{a}) \in A.$$

In particular, if A is definable, then so is $M \times A$.

2. Show that if $A \subset M^{n+1}$ is definable, then so is its *coprojection* $B \subset M^n$ defined by

$$\overline{a} \in B \Leftrightarrow \forall a \in M((\overline{a}, a) \in A).$$

3. Show that $f = (f_1, \cdots, f_l) : M^k \to M^l$ is definable if and only if each $f_1, \cdots, f_l$ is definable.
4. Show that if $f : M^k \to M^l$ and $g : M^l \to M^m$ are definable, then so is their composition $g \circ f : M^k \to M^m$.
5. For $A \subset M$, define the *definable closure of* A, denoted by $dcl(A)$, by

$$dcl(A) = \{x \in M : x \ \ A - \text{definable}\}.$$

Show that $A \subset dcl(A)$, $A \subset B \Rightarrow dcl(A) \subset dcl(B)$, and $dcl(dcl(A)) = dcl(A)$.

Example 2.8.5. $<$ is $\emptyset$-definable in the ring of reals $\mathbb{R}$. This follows from

$$x < y \Leftrightarrow \exists z(z \neq 0 \wedge y = x + z^2).$$

Example 2.8.6. If L is the language of a ring without subtraction and R is a ring, then the subtraction $z = x - y$ is $\emptyset$-definable in the language L:

$$z = x - y \leftrightarrow x = y + z.$$

Example 2.8.7. Let $\mathbb{F}$ be a field and $R = \mathbb{F}[X_1, \cdots, X_n]$ the ring of polynomials over $\mathbb{F}$. We regard $\mathbb{F}$ as the set of all polynomials of degree 0. Then $\mathbb{F}$ is an $\emptyset$-definable subset of the ring R. It is defined by

$$x \in \mathbb{F} \Leftrightarrow x = 0 \vee \exists y(x \cdot y = 1).$$

Example 2.8.8. It was proved by Lagrange that every positive integer is a sum of squares of four integers. From this it follows that $<$ is $\emptyset$-definable in the ring $\mathbb{Z}$:

$$x < y \Leftrightarrow \exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge y = x + z_1^2 + \cdots + z_4^2).$$

In particular, the set of all natural numbers is an $\emptyset$-definable subset of $\mathbb{Z}$.

It is known that if $\mathbb{K}$ is an algebraically closed field of characteristic 0, then the ring $R = \mathbb{K}[X_1, \cdots, X_n]$ of polynomials over $\mathbb{K}$ satisfies Fermat's last theorem, i.e., if $n > 2$, then the equation $x^n + y^n = z^n$ has no nontrivial solution in R, i.e., if (x, y, z) is a solution, then $x, y, z \in \mathbb{K}$. (See [10], p. 194.) This implies the following:

Example 2.8.9. If $\mathbb{K}$ is an algebraically closed field of characteristic zero, then $\mathbb{K}$ is an $\emptyset$-definable subset of the field of rational functions $\mathbb{K}(X_1, \cdots, X_n)$. For instance, it is defined by the formula

$$f \in \mathbb{K} \Leftrightarrow \exists g \exists h(f = h^3 = 1 + g^3).$$

Example 2.8.10. Let $\mathbb{K}$ be a field. A subset X of $\mathbb{K}^n$ is defined by an atomic formula if and only if it is the set of all zeros (roots) of a polynomial over $\mathbb{K}$.

We need a well-known result of Hilbert now. (See [10].) Let $\mathbb{K}$ be a field, and let $P \subset \mathbb{K}[X_1, \cdots, X_n]$. Define

$$\mathcal{V}(P) = \{\overline{a} \in \mathbb{K}^n : f(\overline{a}) = 0 \text{ for all } f \in P\}.$$

Sets of the form $\mathcal{V}(P)$ are called *Zariski closed sets* or *affine algebraic varieties* in $\mathbb{K}^n$. Note that if $P \subset Q \subset \mathbb{K}[X_1, \cdots, X_n]$, then $\mathcal{V}(Q) \subset \mathcal{V}(P)$.

Theorem 2.8.11 (Weak Hilbert Basis Theorem). *If $\mathbb{K}$ is a field and $V \subset \mathbb{K}^n$ is Zariski closed, then there is a finite $P \subset \mathbb{K}[X_1, \cdots, X_n]$ such that $V = V(P)$.*

It follows that Zariski closed sets $V \subset \mathbb{K}^n$ are precisely the sets defined by finite conjunctions of atomic formulas, i.e., by finitely many polynomial equations.

Exercise 2.8.12. Readers familiar with topology should show that Zariski closed subsets of $\mathbb{K}^n$ are the family of all closed subsets of a topology on $\mathbb{K}^n$. This topology is called the *Zariski topology*.

Example 2.8.13. Let $\mathbb{K}$ be a field, and let $M_{m\times n}(\mathbb{K})$ denote the set of all $m \times n$ matrices over $\mathbb{K}$. We identify $M_{m\times n}(\mathbb{K})$ with $\mathbb{K}^{mn}$ in a canonical way. We shall follow the usual convention and write $M_n(\mathbb{K})$ in place of $M_{n\times n}(\mathbb{K})$. Show the following:

1. The determinant function $A \to |A|$, $A \in M_n(\mathbb{K})$ (i.e., its graph) is $\emptyset$-definable.
2. The set of all $n \times n$ nonsingular matrices $GL_n(\mathbb{K})$ is $\emptyset$-definable. In fact, it is defined by the negation of a polynomial equation.
3. Show that the matrix multiplication $M_{m\times n}(\mathbb{K}) \times M_{n\times k}(\mathbb{K}) \to M_{m\times k}(\mathbb{K})$ is $\emptyset$-definable.

A family $\mathcal{A}$ of subsets of a set X is called an *algebra of sets on X* if it contains X and is closed under complementations and finite unions. Sets belonging to the algebra of subsets of $\mathbb{K}^n$ generated by affine algebraic varieties $V \subset \mathbb{K}^n$ are called *constructible sets*.

Exercise 2.8.14. A subset $C \subset \mathbb{K}^n$ is constructible if and only if it is defined by an open formula.

Example 2.8.15. Let $D \subset \mathbb{R}^n$ be definable. Then its *closure*

$$\overline{D} = \{\overline{a} \in \mathbb{R}^n : \forall \varepsilon(\varepsilon > 0 \to \exists \overline{b} \in D(\sum_{i=1}^{n}(a_i - b_i)^2 < \varepsilon))\}$$

is definable.

If $\varphi[\overline{y}, i_{\overline{c}}]$, $\overline{c} \in \mathbb{R}$, defines D, then the formula

$$\forall x(x > 0 \to \exists \overline{y}(\varphi[\overline{y}, i_{\overline{c}}] \wedge \sum(x_i^2 - y_i^2) < x))$$

defines the closure of D.

Proposition 2.8.16. *Let $D \subset M^n$ be A-definable and $f : M \to M$ an automorphism of M such that $f(a) = a$ for all $a \in A$. Then $D = f(D)$. In particular, f fixes all A-definable points.*

Proof. Let $\varphi[\overline{x}, i_{\overline{a}}]$, with a_i in A, define D. For every any $\overline{b} \in M^n$, we have

$$\begin{aligned} \overline{b} \in D &\Leftrightarrow M \models \varphi[i_{\overline{b}}, i_{\overline{a}}] \\ &\Leftrightarrow M \models \varphi[i_{f(\overline{b})}, i_{f(\overline{a})}] \\ &\Leftrightarrow M \models \varphi[i_{f(\overline{b})}, i_{\overline{a}}] \\ &\Leftrightarrow f(\overline{b}) \in D. \end{aligned}$$

The second equivalence holds because f is an automorphism of M. The first and last equivalences hold because $\varphi[\overline{x}, i_{\overline{a}}]$ defines D. Our proof is complete. □

It is well known that for every finite sequence $\overline{a}$ of complex numbers there is a real number r and a complex number s (not in $\mathbb{R}$) such that there is a field isomorphism $f : \mathbb{C} \to \mathbb{C}$ fixing each $\overline{a}$ and mapping r to s. Thus we get the following interesting result.

Proposition 2.8.17. *The set of all real numbers $\mathbb{R}$ is not a definable subset of the field of complex numbers $\mathbb{C}$.*

Later we shall prove that the set of all rational numbers $\mathbb{Q}$ is not a definable subset of the field of real numbers. In a remarkable result (see [4] for an excellent account of this) using deep results on diophantine equations, Julia Robinson proved the following theorem.

Theorem 2.8.18 (J. Robinson). *The set of all integers is an $\emptyset$-definable subset of the ring of rational numbers $\mathbb{Q}$.*

The importance of these results for decision problems will be explained now.

Let M be a structure of L and $N \subset M$ a substructure. Suppose $\varphi[x, i_{\overline{a}}]$ defines N. For any formula ψ we define its *relativization to N*, denoted by ψ^N, by induction on the rank of ψ as follows: if ψ is atomic, then ψ^N is ψ. Further,

$$(\neg\psi)^N = \neg\psi^N, (\psi \vee \eta)^N = \psi^N \vee \eta^N$$

and

$$(\exists y \psi)^N = \exists y(\varphi[y, i_{\overline{a}}] \wedge \psi^N).$$

We may think of ψ^N as the relativization of ψ to N.

Proposition 2.8.19. *Let N be a definable substructure of M. Then for every formula $\psi[x_0, \cdots, x_{n-1}]$ and every $\overline{b} \in N^n$,*

$$N \models \psi[i_{\overline{b}}] \Leftrightarrow M \models \psi^N[i_{\overline{b}}].$$

Proof. We prove the result by induction on ψ. The result is clearly true for atomic ψ and is true for $\neg\psi$ ($\psi \vee \eta$) if it is true for ψ (resp. for ψ and η).

Now suppose the result is true for $\psi[x, x_0, \cdots, x_{n-1}]$ and every $\overline{c} \in N^{n+1}$ and $\eta[x_0, \cdots, x_{n-1}] = \exists x\psi$. Take any $\overline{b} \in N^n$.

Suppose $M \models \eta^N[i_{\overline{b}}]$. Then there is a $b \in M$ such that $M \models \varphi[i_b, i_{\overline{a}}]$ as well as $M \models \psi^N[i_b, i_{\overline{b}}]$. Since φ defines N, $b \in N$. By the induction hypothesis, $N \models \psi[i_b, i_{\overline{b}}]$. Thus, $N \models \eta[i_{\overline{b}}]$.

Now assume that $\overline{b} \in N^n$ and $N \models \eta[i_{\overline{b}}]$. Thus, there is a $b \in N$ such that $N \models \psi[i_b, i_{\overline{b}}]$. By the induction hypothesis, $M \models \psi^N[i_b, i_{\overline{b}}]$. Since φ defines N, $M \models \varphi[i_b, i_{\overline{a}}]$. This proves that $M \models \psi^N[i_{\overline{b}}]$. □

Remark 2.8.20. Suppose M is such that there is an algorithm to decide if a statement of L_M is true in M or not. Such a structure is called decidable. Otherwise it is called undecidable. (The concept of an algorithm will be defined later in the book.) The last result tells us that if $N \subset M$ is definable and M decidable, then N is decidable. Equivalently, if N is undecidable, so is M. It was proved by Tarski that $\mathbb{R}$ as an ordered field and $\mathbb{C}$ are decidable. It was proved by Gödel that $\mathbb{N}$ is undecidable in the language of the ordered ring. Julia Robinson's result implies that the ordered field of rationals is undecidable. These things will be dealt with in more detail later.

Suppose M is a structure of L and $f_M : M^n \to M$ definable, defined by, say, $\varphi[y, \overline{x}, i_{\overline{a}}]$. Let L' be the expansion of L obtained by introducing an n-ary function symbol f. We regard M as a structure of L' by interpreting f by f_M. For any formula ψ of L', let ψ^f be the formula of L obtained from ψ by replacing each subformula of ψ of the form $\eta[\cdots f\overline{t}\cdots]$ by the formula $\exists u(u = f\overline{t} \wedge \eta[\cdots u\cdots])$, where u is a variable not occurring in ψ, and then by replacing each subformula of the form $t = f(\overline{s})$ by $\varphi[t, \overline{s}, i_{\overline{a}}]$. If necessary, new variables should be used so that the essential nature of the formula φ is not changed. Then

Proposition 2.8.21.

$$M \models \psi \Leftrightarrow M \models \psi^f.$$

Its entirely trivial proof is left as an exercise. This result implies that if a set is definable by a formula of L', it is definable by a formula of L. A similar result is true for definable relations on M.

Let L and L' be first-order languages, M an L-structure, and N an L'-structure. We say that N is *interpretable in* M if there are a structure $N' \subset M^k$ (for some k) of L' with N' and interpretations of all nonlogical symbols of L in N' definable by formulas of L so that N and N' are isomorphic.

Example 2.8.22. If $\mathbb{K}$ is a field, then the group $GL_n(\mathbb{K})$ is interpretable in the field $\mathbb{K}$.

Let $GL_n^+(\mathbb{R})$ denote the set of all $n \times n$-real matrices with determinant positive, $O(n)$ the set of all orthonormal $n \times n$-real matrices, and $SO(n)$ the subgroup of $O(n)$ of matrices of determinant 1. Similarly, let $U(n)$ denote the set of all unitary matrices over $\mathbb{C}$ and $SU(n)$ the subgroup of $U(n)$ of determinant 1.

Let $\mathbb{K}$ be a field. A *linear algebraic group over* $\mathbb{K}$ is a subgroup G of $GL_n(\mathbb{K})$ such that G and the graph of the matrix multiplication on G are affine algebraic varieties. In general, an *algebraic group over* $\mathbb{K}$ is a group G that is an affine algebraic variety over $\mathbb{K}$, and the group operation $\cdot : G \times G \to G$ (more precisely, its graph) is an affine algebraic variety, i.e., definable by polynomial equations.

Example 2.8.23. The groups $GL_n^+(\mathbb{R})$, $O(n)$, and $SO(n)$ are interpretable in the field of reals. Moreover, $O(n)$ and $SO(n)$ are linear algebraic groups over $\mathbb{R}$. The groups $U(n)$ and $SU(n)$ are algebraic over $\mathbb{C}$ and interpretable in the field of complex numbers $\mathbb{C}$.

Chapter 3
Propositional Logic

We now turn our attention to the fundamental notion of a logical deduction or a proof. Note that in computing the truth value of a statement in a structure one uses some rules of inference depending only on the syntactical construction of the statement. For instance, if A or B is true in a structure, then we infer that $A \vee B$ is true in the structure. We have also noted that statements with some specific syntactical structures are valid in all structures. For instance, a statement of the form $\neg A \vee A$ is true in all structures. Statements true in all structures of a language are called *tautologies*. So all tautologies should be theorems. Are there a convenient list of tautologies (to be called *logical axioms*) and a list of *rules of inference* such that a statement is valid if and only if it can be inferred from logical and nonlogical axioms using the rules of inference from our list? Indeed there is.

In this chapter we first develop a simpler, but an important, form of logic called *propositional logic*. The main objective of propositional logic is to formalize reasoning involving logical connectives $\vee$ and $\neg$ only.

3.1 Syntax of Propositional Logic

Thus, the *language of a propositional logic L* consists of

(i) *Variables*: a nonempty set of symbols, and
(ii) *Logical connectives*: $\neg$ and $\vee$.

Throughout this chapter, unless otherwise stated, L will denote the language of a propositional logic.

Let $\mathcal{F}$ be the smallest set of expressions in L that contains all variables, the expression $\neg A$ whenever $A \in \mathcal{F}$, and $\vee AB$ whenever A and B are in $\mathcal{F}$. The expressions belonging to $\mathcal{F}$ are called *formulas* of L.

Example 3.1.1. Let R be a binary relation on a nonempty set X. Let A stand for the proposition "R is reflexive," B for "R is symmetric," C for "R is transitive," and E

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_3,
© Springer Science+Business Media New York 2013

for the proposition "R is an equivalence relation." Let the set of all variables of L be $\{A,B,C,E\}$. Then $E \leftrightarrow (A \wedge B \wedge C)$ is a formula of L standing for the statement "R is an equivalence relation if and only if R is reflexive, symmetric, and transitive."

Example 3.1.2. Let A stand for the statement "the humidity is high," B for "it will rain this afternoon," and C for "it will rain this evening." Let A,B,C be all the variables of L. Then the formula $A \rightarrow (B \vee C)$ stands for the statement "if the humidity is high, then it will rain this afternoon or this evening."

Exercise 3.1.3. Express the following statements as formulas of a propositional logic:

1. If the prime interest rate goes up, then people are not happy.
2. If stock prices go up, then people are happy.

The rank of a formula is defined as in Chap. 1. As in the case of a first-order language, we shall often write $A \vee B$ for $\vee AB$. We shall maintain the same convention in using parentheses. Also, logical connectives $\wedge$, $\rightarrow$, and $\leftrightarrow$ are defined similarly. We shall use letters A, B, C, P, Q, R, and S, with or without subscripts, for formulas of L.

Let A be a formula of L. The set of all *subformulas* of A is the smallest set $\mathcal{S}$ of expressions in L satisfying the following conditions:

(i) $A \in \mathcal{S}$.
(ii) $B \in \mathcal{S}$ whenever $\neg B \in \mathcal{S}$.
(iii) $B,C \in \mathcal{S}$ whenever $B \vee C \in \mathcal{S}$.

The following example is an important one for us.

Example 3.1.4. Let L be a first-order language and L' a propositional logic whose variables are elementary formulas of L. Then the set of all formulas of L' is the same as the set of all formulas of L.

3.2 Semantics of Propositional Logic

In this section, we use the intended meaning of the logical connectives and define the truth or falsity of a formula in terms of its subformulas.

A *truth valuation* or an *interpretation* or a *structure* of L is a map v from the set of all variables of L to $\{T,F\}$.

Let v be an interpretation of L. We extend v (and denote the extension by v itself) to the set of all formulas by induction as follows:

$$v(\neg A) = T \text{ if and only if } v(A) = F$$

and

$$v(A \vee B) = T \text{ if and only if } v(A) = T \text{ or } v(B) = T.$$

If $v(A) = T$, then we say that A is *true* in the structure v or that v satisfies A. Otherwise, A is said to be *false* in the structure.

Remark 3.2.1. The truth value $v(A)$ of a formula A depends only on the finitely many variables occurring in A.

Exercise 3.2.2. Let $\mathcal{F}$ denote the set of all formulas of a language L and $v : \mathcal{F} \to \{T,F\}$. Then there is a truth valuation that generates v as above if and only if for every $A,B \in \mathcal{F}$ the following holds:

$$v(\neg A) = T \text{ if and only if } v(A) = F$$

and

$$v(A \vee B) = T \text{ if and only if } v(A) = T \text{ or } v(B) = T.$$

Henceforth, a function $v : \mathcal{F} \to \{T,F\}$ satisfying these two conditions will also be referred to as a truth valuation.

Exercise 3.2.3. Let A,B,C be all the variables of L. For each truth valuation v of L, compute the truth values of the following formulas:

1. $A \to B \to C$.
2. $B \to A \to C$.
3. $A \to C \to B$.
4. $(\neg A \vee B) \to \neg(A \wedge \neg B)$.

Let $\mathcal{A}$ be a set of formulas of L. An interpretation v is called a *model* of $\mathcal{A}$ if every $A \in \mathcal{A}$ is true in v. In this case we write $v \models \mathcal{A}$. If $\mathcal{A}$ has a model, then we say that $\mathcal{A}$ is *satisfiable*.

Exercise 3.2.4. Show that $\{A, \neg(A \vee B)\}$, $\{\neg A, \neg B, A \vee B\}$ are not satisfiable.

Exercise 3.2.5. Let A and B be formulas and v a truth valuation of L. Prove the following statements:

(a) $v(A \wedge B) = T$ if and only if $v(A) = v(B) = T$.
(b) $v(A \to B) = T$ if and only if $v(A) = F$ or $v(B) = T$.
(c) $v(A \leftrightarrow B) = T$ if and only if $v(A) = v(B)$.

Let A and B be formulas and $\mathcal{A}$ a set of formulas.

(i) We say that A is a *tautological consequence* of $\mathcal{A}$, and we write $\mathcal{A} \models A$ if A is true in every model v of $\mathcal{A}$.
(ii) If A is a tautological consequence of the empty set of formulas, then we say that A is a *tautology* and write $\models A$. Thus, A is a tautology if and only if $v(A) = T$ for every truth valuation v of L.
1. If $A \leftrightarrow B$ is a tautology [i.e., $v(A) = v(B)$ for all truth valuations v], then we say that A and B are *tautologically equivalent* and write $A \equiv B$.

Exercise 3.2.6. (a) Show that $A \to B \to C$ and $B \to A \to C$ are tautologically equivalent.

(b) Show that $A \to B \to C$ and $A \to C \to B$ are not tautologically equivalent.
(c) Show that $A \to B \to C$ and $(A \to B) \to C$ are not tautologically equivalent.
(d) Show that $\neg(A \vee B) \vee C$ is a tautology if and only if both $\neg A \vee C$ and $\neg B \vee C$ are tautologies.

(*Hint*: Consider a language with variables A, B, and C.)

Exercise 3.2.7. Let $\mathcal{F}$ be the set of all formulas of L. Set

$$\mathbb{B} = \mathcal{F}/\equiv,$$

the set of $\equiv$-equivalence classes of formulas. For any formula A, let $[A]$ denote the $\equiv$-equivalence class containing A. Thus, $[A]$ is the set of all formulas tautologically equivalent to A. For formulas A and B, define

$$\begin{aligned} 0 &= [A \wedge \neg A], \\ 1 &= [A \vee \neg A], \\ [A]' &= [\neg A], \\ [A] \vee [B] &= [A \vee B], \end{aligned}$$

and

$$[A] \wedge [B] = [A \wedge B].$$

Show that these are well defined and that these make $\mathbb{B}$ a Boolean algebra [8, p. 78].

The following result is quite easy to prove. Therefore, its proof is left as an exercise.

Proposition 3.2.8. *Let A, A_1, A_2, …, A_n be formulas. Then the following statements are equivalent:*

(a) A is a tautological consequence of $A_1, A_2, \ldots, A_n$.
(b) $A_1 \to A_2 \to \cdots \to A_n \to A$ is a tautology.

Exercise 3.2.9. Prove the following statements:

(a) $A \equiv \neg\neg A$.
(b) $\neg(A \vee B) \equiv \neg A \wedge \neg B$.
(c) $\neg(A \wedge B) \equiv \neg A \vee \neg B$.
(d) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.
(e) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.

By a *literal* of L we shall mean either a variable or the negation of a variable of L. A formula is said to be in *conjunctive normal form* (CNF) if it is a conjunction of disjunctions of literals, i.e., it is of the form

$$\wedge_{i=1}^{k} \vee_{j=1}^{n_k} A_{ij},$$

where each A_{ij} is a literal. Similarly, a formula is said to be in *disjunctive normal form* (DNF) if it is a disjunction of conjunctions of literals, i.e., it is of the form

$$\vee_{i=1}^{k} \wedge_{j=1}^{n_k} A_{ij},$$

where each A_{ij} is a literal.

Exercise 3.2.10. Show that for every formula A there is a formula B in CNF and a formula C in DNF that are tautologically equivalent to A.

(*Hint*: Use induction on the length of A.)

Proposition 3.2.11. *Let $A \to A^*$ be a map from the set of formulas of L to itself such that for all formulas A and B,*

$$(\neg A)^* = \neg A^* \text{ and } (A \vee B)^* = A^* \vee B^*.$$

Assume that B is a tautological consequence of $A_1, \ldots, A_n$. Then B^* is a tautological consequence of $A_1^*, \ldots, A_n^*$.

Proof. Let v be a truth valuation. For every variable A, define

$$v'(A) = v(A^*).$$

By our hypothesis, it follows that for every formula A,

$$v'(A) = v(A^*).$$

By Exercise 3.2.2, v' is a truth valuation. Since B is a tautological consequence of $A_1, \ldots, A_n$, it follows that $v(B^*) = T$ if $v(A_1^*) = \ldots = v(A_n^*) = T$. □

3.3 Compactness Theorem for Propositional Logic

A binary relation $\leq$ on a set $\mathbb{P}$ is called a *partial order* if it is reflexive, antisymmetric, and transitive. An element p of $\mathbb{P}$ is called an *upper bound* of a subset A of $\mathbb{P}$ if $q \leq p$ for every $q \in A$. An element p of $\mathbb{P}$ is called a *maximal element* of $\mathbb{P}$ if for any $q \in \mathbb{P}$, $p \leq q$ implies that $p = q$. A partial order $\leq$ on $\mathbb{P}$ is called a *linear order* if for every $p, q \in \mathbb{P}$, $p \leq q$ or $q \leq p$. A *chain* in a partially ordered set $\mathbb{P}$ is a subset C of $\mathbb{P}$ such that for every $p, q \in C$, $p \leq q$ or $q \leq p$, i.e., the restriction of $\leq$ to C is a linear order.

Lemma 3.3.1 (Zorn's lemma). *Let $(\mathbb{P}, \leq)$ be a nonempty partially ordered set such that every chain in $\mathbb{P}$ has an upper bound in $\mathbb{P}$. Then $\mathbb{P}$ has a maximal element.*

Remark 3.3.2. It can be proved that the axiom of choice and Zorn's lemma are equivalent in *ZF*. In particular, Zorn's lemma is a theorem of *ZFC*.

We call $\mathcal{A}$ *finitely satisfiable* if every finite subset of $\mathcal{A}$ is satisfiable.

Clearly if $\mathcal{A}$ is satisfiable, then it is finitely satisfiable. The compactness theorem tells us that the converse is also true. We proceed now to prove this important result.

Lemma 3.3.3. *Let $\mathcal{A}$ be a finitely satisfiable set of formulas and A a formula of L. Then either $\mathcal{A} \cup \{A\}$ or $\mathcal{A} \cup \{\neg A\}$ is finitely satisfiable.*

Proof. Suppose $\mathcal{A} \cup \{A\}$ is not finitely satisfiable. We need to show that for every finite subset $\mathcal{B}$ of $\mathcal{A}$, $\mathcal{B} \cup \{\neg A\}$ is satisfiable. Suppose this is not the case for a finite $\mathcal{B} \subset \mathcal{A}$. Then A is a tautological consequence of $\mathcal{B}$. Fix a finite $\mathcal{C} \subset \mathcal{A}$. Since $\mathcal{B} \cup \mathcal{C}$ is finite, it is satisfiable. Let v be a truth valuation that satisfies it. Since A is a tautological consequence of $\mathcal{B}$, $v(A) = T$. In particular, $\mathcal{C} \cup \{A\}$ is satisfiable. Thus, $\mathcal{A} \cup \{A\}$ is finitely satisfiable, and we have arrived at a contradiction. □

Theorem 3.3.4 (Compactness theorem for propositional logic). *A set $\mathcal{A}$ of formulas of L is satisfiable if and only if it is finitely satisfiable.*

Proof. We need to prove the *if* part of the result only. Assume that $\mathcal{A}$ is finitely satisfiable. We must show that $\mathcal{A}$ is satisfiable. Let $\mathbb{P}$ denote the set of all finitely satisfiable collections of formulas containing $\mathcal{A}$. Since $\mathcal{A} \in \mathbb{P}$, $\mathbb{P} \neq \emptyset$. Equip $\mathbb{P}$ with the partial order $\subset$ (contained in). Let C be a chain in $\mathbb{P}$. Clearly, $\cup C$ is finitely satisfiable. Thus, it is an upper bound of C in $\mathbb{P}$. Thus, by Zorn's lemma, there is a maximal finitely satisfiable family $\mathcal{M}$ of formulas containing $\mathcal{A}$. Since $\mathcal{M}$ is maximal, by Lemma 3.3.3, for every formula A, either $A \in \mathcal{M}$ or $\neg A \in \mathcal{M}$.

Define $v : \mathcal{F} \to \{T, F\}$ by

$$v(A) = T \Leftrightarrow A \in \mathcal{M}. \qquad (*)$$

We claim that for formulas A and B of our language,

$$v(\neg A) = T \Leftrightarrow v(A) = F$$

and

$$v(A \vee B) = T \Leftrightarrow v(A) \text{ or } v(B) = T.$$

Suppose $v(\neg A) = T$. Then $\neg A \in \mathcal{M}$. Since $\mathcal{M}$ is finitely satisfiable, $A \notin \mathcal{M}$. Hence, $v(A) = F$. Now assume that $v(A) = F$. Then $A \notin \mathcal{M}$ by the definition of v. Hence, $\neg A \in \mathcal{M}$, implying $v(\neg A) = T$.

Now assume that $v(A \vee B) = T$ and $v(A) = v(B) = F$. Then $A \vee B$, $\neg A$, and $\neg B$ all belong to $\mathcal{M}$, contradicting the finite satisfiability of $\mathcal{M}$. For the converse, assume that $v(A) = T$ and $v(A \vee B) = F$. Then $A, \neg(A \vee B) \in \mathcal{M}$, contradicting the finitely satisfiability of $\mathcal{M}$.

Thus, v is a truth valuation such that $v(A) = T$ for every $A \in \mathcal{A}$. □

Exercise 3.3.5. Assume that L is countable. Give a proof of the compactness theorem using induction on the natural numbers and not using Zorn's lemma.

(*Hint*: Since L is countable, the set of all its formulas is countable. Let $\{A_0, A_1, A_2, \ldots\}$ be an enumeration of all its formulas. We define a sequence of natural numbers $n_0, n_1, n_2, \ldots$ as follows: let n_0 be the first natural number i such that $A_i \notin \mathcal{A}$ and $\mathcal{A} \cup \{A_i\}$ is finitely satisfiable. Suppose n_i, $0 \leq i \leq k$, have been defined in such a way that $\mathcal{A} \cup \{A_{n_0}, \ldots, A_{n_k}\}$ is finitely satisfiable. Set $\mathcal{B} = \mathcal{A} \cup \{A_{n_i} : 0 \leq i \leq k\}$. Let n_{k+1} be the least natural number i such that $A_i \notin \mathcal{B}$ and $\mathcal{B} \cup \{A_i\}$ is finitely satisfiable, if such an i exists. Otherwise, set $n_{k+1} = n_k$. Now consider the set $\mathcal{M} = \mathcal{A} \cup \{A_{n_i} : i \in \mathbb{N}\}$.)

Remark 3.3.6. One can prove the compactness theorem quite elegantly using Tychonoff's theorem for compact Hausdorff spaces. We give below the difficult part of the proof. Readers not familiar with these topics may skip the following proof.

Equip $X = \{T, F\}^{\mathcal{F}}$ with the product of discrete topologies on $\{T, F\}$, where $\mathcal{F}$ denotes the set of all variables of L. Thus, X is the set of all structures of L. By Tychonoff's theorem, X is compact and Hausdorff.

For each finite $\mathcal{B} \subset \mathcal{A}$, set

$$F_{\mathcal{B}} = \{v \in X : v(A) = T \text{ for all } A \in \mathcal{B}\}.$$

Let S denote the finite set of variables that occur in $\mathcal{B}$. Note that whenever $v(A) = T$ for all $A \in \mathcal{B}$ and $v'|S = v|S$, $v'(A) = T$ for all $A \in \mathcal{B}$. Hence, $F_{\mathcal{B}}$ is closed in X. They are nonempty by hypothesis. By hypothesis again, the family

$$\{F_{\mathcal{B}} : \mathcal{B} \subset \mathcal{A} \text{ finite}\}$$

has the finite intersection property. Since X is compact, this implies that

$$\cap\{F_{\mathcal{B}} : \mathcal{B} \subset \mathcal{A} \text{ finite}\} \neq \emptyset.$$

Any v in this set models $\mathcal{A}$. □

As a corollary to the compactness theorem, we get the following useful result.

Proposition 3.3.7. *Let $\mathcal{A}$ be a set of formulas and A a formula. Then A is a tautological consequence of $\mathcal{A}$ if and only if A is a tautological consequence of a finite $\mathcal{B} \subset \mathcal{A}$.*

Proof. The *if* part of the result is clear. So, assume that for no finite $\mathcal{B} \subset \mathcal{A}$, $\mathcal{B} \models A$. It follows that $\mathcal{A} \cup \{\neg A\}$ is finitely satisfiable. Hence, it is satisfiable by the compactness theorem. This implies that A is not a tautological consequence of $\mathcal{A}$. □

A *graph* is an ordered pair $G = (V, E)$, where V is a nonempty set and E a set of unordered pairs $\{x, y\}$, $x \neq y$, of elements of V. Elements of V are called the *vertices* and those of E the *edges* of G. A *subgraph* of G is a graph $G' = (V', E')$, where $V' \subset V$ and $E' \subset E$. A subgraph $G' = (V', E')$ is called an *induced subgraph* if

$$E' = \{\{x, y\} \in E : x, y \in V'\}.$$

For any natural number $k \geq 1$, we say that G is *k-colorable* if there is a map $c : V \to \{1,2,\ldots,k\}$ such that

$$\{x,y\} \in E \Rightarrow c(x) \neq c(y).$$

Exercise 3.3.8. Let G be a graph. Show that the following statements are equivalent:

1. The graph G is k-colorable.
2. Each finite subgraph of G is k-colorable.
3. Each finite induced subgraph of G is k-colorable.

[*Hint*: Let $G = (V,E)$ be a graph. Consider the language L for a propositional logic with the set of variables

$$\{A_{xi} : x \in V, 1 \leq i \leq k\}.$$

Informally, we think of A_{xi} as the statement "the vertex x is assigned the color i." Now consider the set Φ of formulas consisting of the following formulas:

$$A_{x1} \vee \ldots \vee A_{xk},\ x \in V,$$

$$\neg(A_{xi} \wedge A_{xj}),\ x \in V, 1 \leq i < j \leq k,$$

and

$$\neg(A_{xi} \wedge A_{yi}),\ \{x,y\} \in E, 1 \leq i \leq k.$$

Note that "Φ is satisfiable" means that G is k-colorable. Also, note that "Φ is finitely satisfiable" is equivalent to each of the statements 2 and 3.]

3.4 Proof in Propositional Logic

In this section we define a proof in propositional logic. To define a proof syntactically, we fix some tautologies and call them *logical axioms*. Further, we fix some *rules of inference*.

There is only one scheme of logical axioms, called *propositional axioms*. These are formulas of the form $\neg A \vee A$.

Rules of inference of propositional logic are as follows:

(a) *Expansion rule*: Infer $B \vee A$ from A.
(b) *Contraction rule*: Infer A from $A \vee A$.
(c) *Associative rule*: Infer $(A \vee B) \vee C$ from $A \vee (B \vee C)$.
(d) *Cut rule*: Infer $B \vee C$ from $A \vee B$ and $\neg A \vee C$.

Exercise 3.4.1. Show that the conclusion of any rule of inference is a tautological consequence of its hypotheses.

Let $\mathcal{A}$ be a set of formulas not containing any logical axiom. Elements of $\mathcal{A}$ will be called *nonlogical axioms*. A *proof* in $\mathcal{A}$ is a finite sequence of formulas $A_1, A_2, \ldots, A_n$ such that each A_i is either a logical axiom or a nonlogical axiom or can be inferred from formulas A_j, $j < i$, using one of the rules of inference. In this case we call the preceding sequence a proof of A_n in $\mathcal{A}$. If A has a proof in $\mathcal{A}$, then we say that A is a *theorem* of $\mathcal{A}$ and write $\mathcal{A} \vdash A$. We call $\mathcal{A}$ *inconsistent* if there is a formula A such that $\mathcal{A} \vdash A$ and $\mathcal{A} \vdash \neg A$; $\mathcal{A}$ is called *consistent* if it is not inconsistent.

We shall write $\vdash A$ instead of $\emptyset \vdash A$. Note that each logical and nonlogical axiom is a theorem.

Lemma 3.4.2. *If there is a sequence $A_1, A_2, \ldots, A_n$ such that each A_i is either a theorem of $\mathcal{A}$ or can be inferred from formulas A_j, $j < i$, using one of the rules of inference, then A_n is a theorem of $\mathcal{A}$.*

Proof. In the sequence $A_1, A_2, \ldots, A_n$, replace each A_i that is a theorem by a proof of it. The sequence thus obtained is a proof of A_n. □

Lemma 3.4.3. *Let $\mathcal{A}$ be a set of formulas of L and A a formula of L. Suppose $\mathcal{A} \vdash A$. Then there is a finite $\mathcal{B} \subset \mathcal{A}$ such that $\mathcal{B} \vdash A$.*

Proof. This follows from the fact that each proof is a finite sequence of formulas and so contains only finitely many nonlogical axioms. □

Theorem 3.4.4 (Soundness theorem for propositional logic). *If $\mathcal{A}$ is a set of formulas of L and A a formula, then*

$$\mathcal{A} \vdash A \Rightarrow \mathcal{A} \models A.$$

Proof. Let $A_1, A_2, \ldots, A_n$ be a proof of A. Thus, let v be a model of $\mathcal{A}$. By induction on i, $1 \leq i \leq n$, we show that $v(A_i) = T$, which will complete the proof. Note that A_1 must be a tautology or belong to $\mathcal{A}$. Thus, $v(A_1) = T$. Let $1 < i \leq n$ and $v(A_j) = T$ for all $j < i$. If A_i is a tautology or belongs to $\mathcal{A}$, then $v(A_i) = T$. Otherwise, by Exercise 3.4.1, A_i is a tautological consequence of $\{A_j : j < i\}$. Hence $v(A_i) = T$. □

3.5 Metatheorems in Propositional Logic

In this section we prove some metatheorems in propositional logic. Metatheorems in their own right are not very interesting. Their proofs are often mechanical and sometimes quite tedious. But they are unavoidable. They are needed to show that $\mathcal{A} \vdash A \Leftrightarrow \mathcal{A} \models A$. This is a very important result because this shows that we have indeed formalized the notion of logical deduction in propositional logic.

Lemma 3.5.1. *Let A and B be formulas of L such that $\vdash A \vee B$. Then $\vdash B \vee A$.*

Proof. Consider the sequence

$$A \vee B, \quad \neg A \vee A, \quad B \vee A.$$

The first element of this sequence is a theorem by the hypothesis, the second one is a propositional axiom, and the third one follows from the first two by the cut rule. By Lemma 3.4.2, $\vdash B \vee A$. □

Lemma 3.5.2. *A set of formulas $\mathcal{A}$ is inconsistent if and only if for every formula A, $\mathcal{A} \vdash A$.*

Proof. Let $\mathcal{A}$ be inconsistent. Thus, there is a formula A such that both A and $\neg A$ are theorems of $\mathcal{A}$. Now take any formula B. By the expansion rule, $\vdash B \vee A$ and $\vdash B \vee \neg A$. By Lemma 3.5.1, $\vdash A \vee B$ and $\vdash \neg A \vee B$. By the cut rule, $\vdash B \vee B$. By the contraction rule, $\vdash B$. This proves the only *if* part of the result. The *if* part of the result is trivial. □

Lemma 3.5.3 (Modus ponens). *Let A and B be formulas of L such that $\vdash A$ and $\vdash A \to B$. Then $\vdash B$.*

Proof. Since A is a theorem, by the expansion rule, $B \vee A$ is a theorem. Hence, by Lemma 3.5.1, $A \vee B$ is a theorem. Now consider the sequence

$$A \vee B, \quad A \to B, \quad B \vee B, \quad B.$$

The first formula is shown above to be a theorem; the second formula is a theorem by hypothesis; since $A \to B$ is the formula $\neg A \vee B$ by definition, the third formula is inferred from the first two by the cut rule; the last formula is inferred from the third formula by the contraction rule. The result follows by Lemma 3.4.2. □

Now, by induction on n, we easily obtain the following corollary.

Corollary 3.5.4 (Detachment rule). *Let B, $A_1, A_2, \ldots, A_n$ be formulas of L. Assume that each of $A_1, \ldots, A_n$ and $A_1 \to \cdots \to A_n \to B$ is a theorem. Then $\vdash B$.*

Lemma 3.5.5. *If $\vdash A \vee B$, then $\vdash \neg\neg A \vee B$.*

Proof. Since $\neg\neg A \vee \neg A$ is a logical axiom, $\vdash \neg\neg A \vee \neg A$. Then $\vdash \neg A \vee \neg\neg A$ by Lemma 3.5.1. By hypothesis, $\vdash A \vee B$. Hence, $\vdash B \vee \neg\neg A$ by the cut rule. Thus, $\vdash \neg\neg A \vee B$ by Lemma 3.5.1. □

Lemma 3.5.6. *Let $A_1, \ldots, A_n$ be formulas of L ($n \geq 2$) and $1 \leq i < j \leq n$. Suppose $\vdash A_i \vee A_j$. Then*

$$\vdash A_1 \vee \cdots \vee A_n.$$

Proof. We shall prove the result by induction on n. Clearly we can assume that $n \geq 3$.

If $i \geq 2$, then

$$\vdash A_2 \vee \cdots \vee A_n$$

by the induction hypothesis. Hence,

$$\vdash A_1 \vee A_2 \vee \cdots \vee A_n$$

by the expansion rule.

Now let $i = 1$ and $j \geq 3$. Then

$$\vdash A_1 \vee A_3 \vee \cdots \vee A_n$$

by the induction hypothesis. Thus,

$$\vdash (A_3 \vee \cdots \vee A_n) \vee A_1$$

by Lemma 3.5.1. Hence,

$$\vdash A_2 \vee ((A_3 \vee \cdots \vee A_n) \vee A_1)$$

by the expansion rule. Then

$$\vdash (A_2 \vee (A_3 \vee \cdots \vee A_n)) \vee A_1$$

by the associative rule. Hence,

$$\vdash A_1 \vee \cdots \vee A_n$$

by Lemma 3.5.1.

Finally, assume that $i = 1$ and $j = 2$. Then

$$\vdash (A_3 \vee \cdots \vee A_n) \vee (A_1 \vee A_2)$$

by the expansion rule. By the associative rule,

$$\vdash ((A_3 \vee \cdots \vee A_n) \vee A_1) \vee A_2.$$

By Lemma 3.5.1,

$$\vdash A_2 \vee ((A_3 \vee \cdots \vee A_n) \vee A_1).$$

By the associative rule,

$$\vdash (A_2 \vee \cdots \vee A_n) \vee A_1.$$

By Lemma 3.5.1 again,

$$\vdash A_1 \vee \cdots \vee A_n.$$

□

Lemma 3.5.7. *Let $m \geq 1$, $n \geq 1$, and $1 \leq i_1, i_2, \ldots, i_m \leq n$. Suppose*

$$\vdash A_{i_1} \vee A_{i_2} \vee \cdots \vee A_{i_m}.$$

Then

$$\vdash A_1 \vee A_2 \vee \cdots \vee A_n.$$

Proof. We shall prove the result by induction on m. In the rest of the proof, A will designate the formula $A_1 \vee \cdots \vee A_n$.

Case 1: $m = 1$. Set $i = i_1$. By the hypothesis, $\vdash A_i$. By the expansion rule,

$$\vdash (A_{i+1} \vee \cdots \vee A_n) \vee A_i.$$

By Lemma 3.5.1,

$$\vdash A_i \vee A_{i+1} \vee \cdots \vee A_n.$$

Applying the expansion rule repeatedly, we obtain

$$\vdash A_1 \vee \cdots \vee A_n.$$

Case 2: $m = 2$. Suppose $i_1 = i_2$. Then $\vdash A_{i_1}$ by the hypothesis and the contraction rule. The result now follows from Case 1.
Suppose $i_2 < i_1$. Then, by the hypothesis and Lemma 3.5.1, $\vdash A_{i_2} \vee A_{i_1}$. Hence, without loss of generality, we assume that $i_1 < i_2$. The result now follows from Lemma 3.5.6.

Case 3: $m > 2$. By the hypothesis and the associative law,

$$\vdash (A_{i_1} \vee A_{i_2}) \vee A_{i_3} \vee \cdots \vee A_{i_m}.$$

Applying the induction hypothesis to $A_{i_1} \vee A_{i_2}, A_{i_3}, \cdots, A_{i_m}$ (thereby reducing m by 1) and $A_{i_1} \vee A_{i_2}, A_1, \cdots, A_n$, by the induction hypothesis,

$$\vdash (A_{i_1} \vee A_{i_2}) \vee A.$$

By Lemma 3.5.1,

$$\vdash A \vee (A_{i_1} \vee A_{i_2}).$$

By the associative law,

$$\vdash (A \vee A_{i_1}) \vee A_{i_2}.$$

By the induction hypothesis,

$$\vdash (A \vee A_{i_1}) \vee A.$$

By Lemma 3.5.1,

$$\vdash A \vee (A \vee A_{i_1}).$$

By the associative law,

$$\vdash (A \vee A) \vee A_{i_1}.$$

By the induction hypothesis,

$$\vdash (A \vee A) \vee A.$$

By the induction hypothesis,

$$\vdash (A \vee A) \vee A \vee A.$$

Applying the contraction rule twice, we see that

$$\vdash A.$$

□

Lemma 3.5.8. *If* $\vdash \neg A \vee C$ *and if* $\vdash \neg B \vee C$, *then* $\vdash \neg(A \vee B) \vee C$.

Proof. Since $\neg(A \vee B) \vee (A \vee B)$ is a propositional axiom, by Lemma 3.5.7,

$$\vdash A \vee B \vee \neg(A \vee B).$$

Since $\vdash \neg A \vee C$, by the cut rule,

$$\vdash (B \vee \neg(A \vee B)) \vee C.$$

By Lemma 3.5.1,

$$\vdash C \vee B \vee \neg(A \vee B).$$

Hence, by Lemma 3.5.7,

$$\vdash B \vee C \vee \neg(A \vee B).$$

Since $\vdash \neg B \vee C$, by the cut rule,

$$\vdash (C \vee \neg(A \vee B)) \vee C.$$

By Lemma 3.5.1,

$$\vdash C \vee C \vee \neg(A \vee B).$$

Hence

$$\vdash \neg(A \vee B) \vee C$$

by Lemma 3.5.7. □

3.6 Post Tautology Theorem

In this section we prove the following theorem due to Emil Post.

Theorem 3.6.1 (Post tautology theorem). *If A is a formula of L, then*

$$\vdash A \Leftrightarrow \models A.$$

By Theorem 3.4.4, we only need to prove that every tautology is a theorem. Note that if A is a tautology, then so is $A \vee A$. By the contraction rule, our result will be proved if we show that every tautology of the form $A \vee A$ is a theorem. We shall prove a bit more.

Proposition 3.6.2. *Let $n \geq 2$, and let $A_1 \vee \cdots \vee A_n$ be a tautology. Then $\vdash A_1 \vee \cdots \vee A_n$.*

Proof. Suppose each A_i is a literal, i.e., each A_i is either a variable or the negation of a variable. Since $A_1 \vee \cdots \vee A_n$ is a tautology, there is a variable B such that both B and $\neg B$ occur in the sequence $A_1, \ldots, A_n$. But $\vdash \neg B \vee B$. Hence the result follows by Lemma 3.5.7.

Thus, we assume that for some $1 \leq i \leq n$, A_i is not a literal. By Lemma 3.5.7, without loss of generality, we assume that A_1 is not a literal. Thus A_1 is a formula in one of the three forms: $B \vee C$ or $\neg\neg B$ or $\neg(B \vee C)$.

We shall complete the proof by induction on the sum of lengths of the A_i.

Case 1. A_1 is of the form $B \vee C$; then $B \vee C \vee A_2 \vee \cdots \vee A_n$ is a tautology. Hence, it is a theorem by the induction hypothesis. The result in this case follows by the associative rule.

Case 2. A_1 is of the form $\neg\neg B$; from the hypothesis it follows that $B \vee A_2 \vee \cdots \vee A_n$ is a tautology. Hence it is a theorem by the induction hypothesis. The result in this case now follows from Lemma 3.5.5.

Case 3. A_1 is of the form $\neg(B \vee C)$; assuming the hypothesis, it is easy to check that $\neg B \vee A_2 \vee \cdots \vee A_n$ and $\neg C \vee A_2 \vee \cdots \vee A_n$ are tautologies. Thus, by the induction hypothesis, they are theorems. The result in this case follows from Lemma 3.5.8.

□

There is another very useful formulation of the Post tautology theorem.

Theorem 3.6.3. *If $\vdash A_1$, …, $\vdash A_n$ and if B is a tautological consequence of $A_1, \ldots, A_n$, then $\vdash B$.*

Proof. By Lemma 3.2.8, $A_1 \to \cdots \to A_n \to B$ is a tautology. Hence, by the Post tautology theorem,

$$\vdash A_1 \to \cdots \to A_n \to B.$$

The result now follows from Corollary 3.5.4 (the detachment rule). □

Theorem 3.6.4 (Completeness theorem for propositional logic). *Let $\mathcal{A}$ be a set of formulas of L. Then*

$$\mathcal{A} \vdash A \Leftrightarrow \mathcal{A} \models A.$$

Proof. Assume that $\mathcal{A} \vdash A$. Then there is a finite set of formulas $\{B_1, \ldots, B_n\}$ such that

$$\{B_1, \ldots, B_n\} \vdash A.$$

By the soundness theorem,

$$\{B_1, \ldots, B_n\} \models A.$$

Hence,

$$\mathcal{A} \models A.$$

Conversely, assume that $\mathcal{A} \models A$. Then, by the compactness theorem (Proposition 3.3.7), there is a finite set $\mathcal{B} \subset \mathcal{A}$ such that $\mathcal{B} \models A$. Hence, by Theorem 3.6.3, $\mathcal{B} \vdash A$. In particular, $\mathcal{A} \vdash A$.

Corollary 3.6.5. *(a) A set of formulas $\mathcal{A}$ is consistent if and only if it is satisfiable.*
(b) Suppose A and B are tautologically equivalent. Then $\vdash A$ if and only if $\vdash B$.
(c) Suppose $\vdash A \leftrightarrow B$. Then $\vdash A$ if and only if $\vdash B$.
(d) $\vdash A \to B$ if and only if $\vdash \neg B \to \neg A$.
(e) $\vdash A \wedge B$ if and only if $\vdash A$ and $\vdash B$.
(f) If $\vdash A \to B$ and $\vdash B \to C$, then $\vdash A \to C$.

The simple proof of this result is left as an exercise.

Remark 3.6.6. We have already seen that the compactness theorem is used to prove the completeness theorem. Further, the completeness theorem gives a trivial proof of the compactness theorem. To see this, let $\mathcal{A}$ be a set of formulas of L, and let A be a formula of L. Then

$$\begin{aligned} \mathcal{A} \models A &\Rightarrow \mathcal{A} \vdash A \\ &\Rightarrow \mathcal{B} \vdash A \text{ for some finite } \mathcal{B} \subset \mathcal{A} \\ &\Rightarrow \mathcal{B} \models A \text{ for some finite } \mathcal{B} \subset \mathcal{A}. \end{aligned}$$

The first implication holds by Theorem 3.6.4, the second implication holds because every proof contains only finitely many nonlogical axioms, and the last one holds by the soundness theorem for propositional logic.

Thus the compactness and the completeness theorems are equivalent.

Chapter 4
Completeness Theorem for First-Order Logic

In Chap. 1, we described what a first-order language is and what its terms and formulas are. We fixed a first-order language L. In Chap. 2, we described the semantics of first-order languages. In Chap. 3, we considered a simpler form of logic – propositional logic, defined what a proof is in that logic, and proved its completeness theorem. In this chapter we shall define proof in a first-order theory and prove the corresponding completeness theorem. The result for countable theories was first proved by Gödel in 1930. The result in its complete generality was first observed by Malcev in 1936. The proof given below is due to Leo Henkin.

4.1 Proof in First-Order Logic

Let L be a first-order language. The *logical axioms* of L are as follows:

(a) *Propositional axioms*: formulas of the form $\neg A \vee A$.
(b) *Identity axioms*: formulas of the form $x = x$, where x is a fixed variable.
(c) *Equality axioms*: formulas of the form

$$y_1 = z_1 \to \cdots \to y_n = z_n \to fy_1 \cdots y_n = fz_1 \cdots z_n$$

or formulas of the form

$$y_1 = z_1 \to \cdots \to y_n = z_n \to py_1 \cdots y_n \to pz_1 \cdots z_n,$$

with the x_i and y_i being distinct and fixed variables.
(d) *Substitution axioms*: formulas of the form $A_x[t] \to \exists x A$, where A is a formula and t a term substitutable for x in A.

The *rules of inference* in the language L are as follows:

(a) *Expansion rule:* Infer $B \vee A$ from A.
(b) *Contraction rule:* Infer A from $A \vee A$.

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_4,
© Springer Science+Business Media New York 2013

(c) *Associative rule:* Infer $(A \vee B) \vee C$ from $A \vee (B \vee C)$.
(d) *Cut rule:* Infer $B \vee C$ from $A \vee B$ and $\neg A \vee C$.
(e) $\exists$-*Introduction rule*: If x is not free in B, then infer $\exists xA \to B$ from $A \to B$.

The routine proof of the following result is left as an exercise.

Proposition 4.1.1. *Each logical axiom is valid in every structure of L. Also, the conclusion of each rule of inference is valid in any structure of L in which its hypotheses are valid.*

Let T be a first-order theory. A *proof* in T, a theorem in T, etc., are defined as before. Thus, a *proof in* T is a finite sequence $A_1, \ldots, A_n$ of formulas of $L(T)$ such that for each $i \leq n$, A_i is either an axiom (logical or nonlogical) of T or can be inferred from $\{A_j : j < i\}$ by a rule of inference. We shall write $T \vdash A$ or simply $\vdash A$ (when T is understood) to say that A is a theorem of T.

We prove the soundness theorem (also known as the validity theorem) for first-order theories in exactly the same way we proved the soundness theorem for propositional logic (Theorem 3.4.4). Recall that a formula in a theory is valid if it is true in all models of the theory.

Theorem 4.1.2 (Validity theorem). *Every theorem of T is valid in T.*

The famous completeness theorem of Gödel is the converse of this theorem.

A theory T' is called an *extension* of T if $L(T')$ is an extension of $L(T)$ and if every nonlogical axiom of T is a theorem of T'. If $L(T')$ is an extension of $L(T)$ and if every nonlogical axiom of T is a nonlogical axiom of T', then T is called a *part* of T'; moreover, if the number of nonlogical axioms of T is finite, then it is called a *finitely axiomatized* part of T'. If T and T' are extensions of each other, then they are called *equivalent*. Note that if T and T' are equivalent, then they have the same language, i.e., $L(T) = L(T')$. Let Γ be a set of formulas of T. An extension T' of T is called a *conservative extension* of T if every formula of T that is a theorem of T' is also a theorem of T; T' is a *simple extension* of T if $L(T) = L(T')$ and every axiom of T is a theorem of T'. The simple extension of the theory T obtained by adding Γ as new nonlogical axioms is designated by $T[\Gamma]$.

Exercise 4.1.3. Let T' be an extension of T. Show that every theorem of T is a theorem of T'. Moreover, if T' is a conservative extension of T, then every formula of T that is a theorem of T' is a theorem of T.

4.2 Metatheorems in First-Order Logic

As in the case of propositional logic, we need to prove some metatheorem in first-order theory to prove the completeness theorem.

Throughout this section, we fix a first-order theory T; by *theorem* we shall mean a theorem of T, and $\vdash A$ will mean that A is a theorem of T.

The next few definitions are needed to adapt results from propositional logic to first-order logic. Recall that a formula is called elementary if it is either an atomic formula or a formula of the form $\exists xB$. We have already seen that the formulas of L are precisely the formulas of the language of the propositional logic whose variables are precisely the elementary formulas of L. A *truth valuation* for L is a map v from the set of all elementary formulas into $\{T,F\}$. We extend v to the set of all formulas of L as before. Further, we define the notions of *tautological consequences*, *tautology*, and *tautologically equivalent formulas* in exactly the same way as before. For instance, A is a tautological consequence of a set $\mathscr{A}$ of formulas of L if $v(A) = T$ for every truth valuation v of L in which all formulas of $\mathscr{A}$ are true.

It is also clear that the detachment rule (Theorem 3.6.3), the Post tautology theorem (Theorem 3.6.1), etc., proved in the last chapter, hold for first-order theories also.

Proposition 4.2.1 (Detachment rule). *Suppose*

$$\vdash A_1, \ldots, \vdash A_n$$

and

$$\vdash A_1 \to \cdots \to A_{n-1} \to A_n \to A.$$

Then

$$\vdash A.$$

Theorem 4.2.2 (Post tautology theorem). *Suppose*

$$T \vdash A_1, \ldots, T \vdash A_n$$

and

$$A_1, \ldots, A_n \models A.$$

Then

$$T \vdash A.$$

Theorem 4.2.3. *Every tautology in a first-order theory is a theorem of the theory.*

The corollary to the tautology theorem given in the last chapter also holds for first-order theories.

Formulas A and B are called *equivalent* in T if

$$T \vdash A \leftrightarrow B.$$

We write $A \equiv_T B$ if A and B are equivalent in T. Note that if A and B are tautologically equivalent, then $A \equiv_T B$.

Exercise 4.2.4. Let T be a first-order theory. Let $\mathscr{O}$ be the smallest set of formulas that contains all literals and is closed under disjunctions and conjunctions. Show that every open formula is equivalent in T to a formula in $\mathscr{O}$ in *CNF* as well as to a formula in *DNF*.

Exercise 4.2.5. Show that $\equiv_T$ is an equivalence relation on the set of all formulas of T.

In the rest of this section, we shall prove some metatheorems involving terms, quantifiers, etc.

Lemma 4.2.6.

$$\vdash A \to \exists v_1 \cdots \exists v_n A.$$

Proof. Applying the substitution axiom repeatedly, we get

$$\vdash A \to \exists v_n A,$$

$$\vdash \exists v_n A \to \exists v_{n-1} \exists v_n A,$$

$$\vdots$$

$$\vdash \exists v_2 \ldots \exists v_n A \to \exists v_1 \cdots \exists v_n A.$$

Since $A \to \exists v_1 \ldots \exists v_n A$ is a tautological consequence of the preceding formulas, the result follows from the tautology theorem. □

Lemma 4.2.7.

$$\vdash (\forall v_1 \cdots \forall v_n A) \to A.$$

Proof. By 4.2.6,

$$\vdash \neg A \to \exists v_1 \cdots \exists v_n \neg A.$$

The result now follows from the tautology lemma.

Proposition 4.2.8 (∀-introduction rule). *If $\vdash A \to B$ and x is not free in A, then $\vdash A \to \forall x B$.*

Proof. By the hypothesis and the tautology theorem, we have

$$\vdash \neg B \to \neg A.$$

Then

$$\vdash \exists x \neg B \to \neg A$$

by the ∃-introduction rule. Thus,

$$\vdash A \to \neg \exists x \neg B.$$

Hence,

$$\vdash A \to \forall x B$$

by the definition of ∀. □

Proposition 4.2.9. *If* $\vdash A$, *then* $\vdash \forall xA$.

Proof. Since $\vdash A$, by the expansion rule,

$$\vdash \neg\forall xA \to A.$$

Then, by the $\forall$-introduction rule (Proposition 4.2.8),

$$\vdash \neg\forall xA \to \forall xA.$$

The result follows by the tautology theorem. □

By repeatedly using this lemma and the tautology theorem, we obtain the following proposition.

Proposition 4.2.10 (Generalization rule). *If* $\vdash A$, *then* $\vdash \forall x_1 \cdots \forall x_n A$.

Proposition 4.2.11 (Closure theorem). *Let B be the closure of A. Then* $\vdash A$ *if and only if* $\vdash B$.

Proof. If A is a theorem, then B is a theorem by the generalization rule. By Lemma 4.2.7, $\vdash B \to A$. Thus, if $\vdash B$, then $\vdash A$ by the detachment rule. □

Exercise 4.2.12. Let $L(T')$ be an extension of $L(T)$. Show that the following statements are equivalent.

(i) The theory T' is a conservative extension of T.
(ii) A sentence of T is a theorem of T' if and only if it is a theorem of T.

Proposition 4.2.13 (Substitution rule). *If B is an instance of A and if* $\vdash A$, *then* $\vdash B$.

Proof. We first prove the result in a simple case. Suppose t is substitutable for v in A and B is $A_v[t]$. By the substitution axiom,

$$\vdash \neg A_v[t] \to \exists v \neg A.$$

Thus, by the tautology theorem,

$$\vdash \forall vA \to B.$$

By hypothesis and the generalization rule,

$$\vdash \forall vA.$$

Hence

$$\vdash B$$

by the detachment rule.

Now let B be the formula $A_{v_1,\ldots,v_n}[t_1,\ldots,t_n]$. Let $w_1,\ldots,w_n$ be variables, each different from $v_1,\ldots,v_n$, not occurring in A or B. By repeated application of the first part,

$$\vdash A_{v_1}[w_1],$$
$$\vdash A_{v_1,v_2}[w_1,w_2],$$
$$\vdots$$
$$\vdash A_{v_1,\ldots,v_n}[w_1,\ldots,w_n].$$

Let C designate the formula $A_{v_1,\ldots,v_n}[w_1,\ldots,w_n]$. Then B is the formula $C_{w_1,\ldots,w_n}[t_1,\ldots,t_n]$. By repeated application of the first part, we see that

$$\vdash C_{w_1}[t_1],$$
$$\vdash C_{w_1,w_2}[t_1,t_2],$$
$$\vdots$$
$$\vdash C_{w_1,\ldots,w_n}[t_1,\ldots,t_n].$$

□

Using Lemmas 4.2.6 and 4.2.7 and the substitution rule (Proposition 4.2.13), we get the following result.

Proposition 4.2.14 (Substitution theorem).

(a) $\vdash A_{v_1,\ldots,v_n}[t_1,\ldots,t_n] \to \exists v_1 \cdots \exists v_n A$.
(b) $\vdash \forall v_1 \cdots \forall v_n A \to A_{v_1,\ldots,v_n}[t_1,\ldots,t_n]$.

Proposition 4.2.15.

$$\vdash (A \vee \exists x B) \to \exists x(A \vee B).$$

Proof. By the tautology theorem,

$$\vdash B \to A \vee B.$$

By the substitution axiom,

$$\vdash (A \vee B) \to \exists x(A \vee B).$$

By the $\exists$-introduction rule,

$$\vdash \exists x B \to \exists x(A \to B). \tag{1}$$

By the tautology theorem,

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

By the substitution axiom and tautology theorem, we have

$$\vdash A \to \exists x(A \vee B).$$

Thus, by the tautology theorem,

$$\vdash A \to \exists x(A \vee B). \tag{2}$$

Applying the tautology theorem to (1) and (2) we obtain the result. □

Sometimes a term t is not substitutable for a variable v in a formula A. Our next result shows how to circumvent this.

Proposition 4.2.16 (Variant theorem).

$$\vdash \exists vC \leftrightarrow \exists wC_v[w], \tag{1}$$

where w is not free in C and is substitutable for v in C.

Proof. By the substitution axiom,

$$\vdash C_v[w] \to \exists vC.$$

Thus, by the $\exists$-introduction rule,

$$\vdash \exists wC_v[w] \to \exists vC. \tag{2}$$

On the other hand, since w is not free in C, the formula $(C_v[w])_w[v]$ is C. In other words, if we replace free occurrences of v in C by w and then replace free occurrences of w by v, we get back C because w is not free in C. Hence, by the substitution axiom,

$$\vdash C \to \exists wC_v[w]. \tag{3}$$

By the $\exists$-introduction rule,

$$\vdash \exists vC \to \exists wC_v[w]. \tag{4}$$

Since the formula in Eq. (1) is a tautological consequence of those in Eqs. (2) and (4), Eq. (1) follows from the tautology theorem. □

Proposition 4.2.17.

$$\vdash \exists w(\exists vC \to C_v[w]),$$

where w is not free in C and is substitutable for v in C.

Proof. By Proposition 4.2.15,

$$\vdash (\exists vC \to \exists wC_v[w]) \to \exists w(\exists vC \to C_v[w]).$$

The result now follows from the variant theorem and the cut rule. □

Proposition 4.2.18 (Symmetry theorem). *For any two terms t and s,*

$$\vdash t = s \leftrightarrow s = t.$$

Proof. Let v and w be distinct variables. By the equality axiom and substitution rule,

$$\vdash v = w \rightarrow v = v \rightarrow v = v \rightarrow w = v.$$

By the identity axiom and the tautology theorem,

$$\vdash v = w \rightarrow w = v.$$

Substituting t for v and s for w, by the substitution rule,

$$\vdash t = s \rightarrow s = t.$$

Similarly,

$$\vdash s = t \rightarrow t = s.$$

The result now follows from the tautology theorem. □

Proposition 4.2.19 (Equality theorem).

(a) Let a term s be obtained from t by replacing subterms $t_1, \ldots, t_n$ by $s_1, \ldots, s_n$, respectively. If

$$\vdash t_i = s_i,$$

$1 \leq i \leq n$, then

$$\vdash t = s.$$

(b) Let a formula B be obtained from A by replacing some occurrences of terms $t_1, \ldots, t_n$ in A not immediately following $\exists$ or $\forall$ by $s_1, \ldots, s_n$, respectively. If

$$\vdash t_i = s_i,$$

$1 \leq i \leq n$, then

$$\vdash A \leftrightarrow B.$$

Proof. (a) We shall prove the result by induction on the rank of t.

If t is t_i for some i, then s is the term s_i and there is nothing to be proved. This, in particular, shows that the result is true for t of rank 0.

Let t be a term of the form $fa_1 \cdots a_k$. Then, the t_i are subterms of the a_j. Let a'_j be the term obtained from a_j by replacing appropriate occurrences of terms $t_1, \ldots, t_n$ by $s_1, \ldots, s_n$, respectively. Then, by the induction hypothesis,

$$\vdash a_j = a'_j,$$

$1 \leq j \leq k$. We have the equality axiom

$$x_1 = y_1 \to \cdots \to x_k = y_k \to fx_1 \cdots x_k = fy_1 \cdots y_k.$$

Thus, the result follows from the substitution rule and the tautology theorem.

(b) We prove the result by induction on the rank of A.

Assume A is an atomic formula of the form $pa_1 \cdots a_k$. Then the t_i are subterms of the a_j. Let a'_j be the term obtained from a_j by replacing appropriate occurrences of terms $t_1, \ldots, t_n$ by $s_1, \ldots, s_n$, respectively. Then B is the formula $pa'_1 \cdots a'_k$. By (a),

$$\vdash a_j = a'_j,$$

$1 \leq j \leq k$. We have the equality axiom

$$\vdash x_1 = y_1 \to \cdots \to x_k = y_k \to px_1 \cdots x_k \to py_1 \cdots y_k.$$

By the substitution rule and the tautology theorem,

$$\vdash pa_1 \cdots a_k \to pa'_1 \cdots a'_k.$$

Since, by the symmetry theorem,

$$\vdash a'_j = a_j,$$

by the tautology theorem,

$$\vdash pa'_1 \cdots a'_k \to pa_1 \cdots a_k.$$

Hence,

$$\vdash pa_1 \cdots a_k \leftrightarrow pa'_1 \cdots a'_k$$

by the tautology theorem.

Let A be a formula of the form $\exists vC$. Then, by the hypothesis in (b), B is the formula $\exists vD$, where D is obtained from C by replacing appropriate occurrences of terms $t_1, \ldots, t_n$ by $s_1, \ldots, s_n$, respectively. By the induction hypothesis,

$$\vdash C \leftrightarrow D.$$

The result follows from the distribution rule and the tautology theorem. The cases where A is of the form $\neg C$ or $C \vee D$ are dealt with similarly. □

In mathematics, while proving a sentence of the form $A \to B$, quite often one assumes A and then proves B. This means that one adds A as a new axiom and proves B in this extension of T. We now show that this is a correct method of proving $A \to B$ in T.

Recall that we designated the simple extension of a theory T obtained by adding a set Γ of formulas as new axioms by $T[\Gamma]$. If $\Gamma = \{A_1, \ldots, A_n\}$, then we shall write $T[A_1, \ldots, A_n]$ instead of $T(\Gamma)$.

Proposition 4.2.20. *Let A be a closed formula. Then*

$$T \vdash A \to B$$

if and only if

$$T[A] \vdash B.$$

Proof. Suppose

$$T \vdash A \to B.$$

Then

$$T[A] \vdash A \to B.$$

Also,

$$T[A] \vdash A.$$

Thus,

$$T[A] \vdash B$$

by the detachment rule.

Now assume that

$$T[A] \vdash B.$$

Fix a proof of $A_1, \ldots, A_n$ of B in $T[A]$. By induction on i, we shall prove that

$$T \vdash A \to A_i$$

for $1 \leq i \leq n$, which completes the proof.

The formula A_1 is an axiom of $T[A]$. If A_1 is an axiom of T, then

$$T \vdash A_1.$$

Hence,

$$T \vdash A \to A_1$$

by the expansion rule. If A_1 is A, then

$$T \vdash A \to A$$

by the propositional axiom.

Assume the hypothesis for all $j < i$. If A_i is an axiom of $T[A]$, then we have already proved that

$$T \vdash A \to A_i.$$

If A_i is inferred from $\{A_j : j < i\}$ using a rule of inference other than the $\exists$-introduction rule, then A_i is a tautological consequence of $\{A_j : j < i\}$. But then $A \to A_i$ is a tautological consequence of $\{A \to A_j : j < i\}$. By the induction hypothesis,

$$T \vdash A \to A_j$$

for every $j < i$. Hence,

$$T \vdash A \to A_i$$

by the tautology theorem.

Now assume that A_i is inferred from some A_j, $j < i$, by the $\exists$-introduction rule. Thus, A_j is a formula of the form $B \to C$ and A_i is of the form $\exists v B \to C$, where v is not free in C. By the induction hypothesis,

$$T \vdash A \to B \to C;$$

by the tautology theorem,

$$T \vdash B \to A \to C.$$

Since A is closed, v is not free in $A \to C$. Hence by the $\exists$-introduction rule,

$$T \vdash \exists v B \to A \to C;$$

by the tautology theorem,

$$T \vdash A \to \exists v B \to C,$$

i.e.,

$$T \vdash A \to A_i.$$

□

Corollary 4.2.21 (Deduction theorem). *If $A_1, \ldots, A_n$ are closed, then*

$$T[A_1, \ldots, A_n] \vdash B \Leftrightarrow T \vdash A_1 \to \cdots \to A_n \to B.$$

Exercise 4.2.22. For any consistent theory T that has a model with more than one point, show that

$$T[x = y] \vdash \forall x \forall y (x = y)$$

but

$$T \nvdash x = y \to \forall x \forall y (x = y).$$

Thus, the deduction theorem is not true if the A are not closed.

Proposition 4.2.23 (Theorem on constants). *Let T' be obtained from T by adding new constants but no new nonlogical axioms and with $A[\overline{x}]$ a formula of T. Then for all new constants $\overline{c} = (c_0, \cdots, c_{n-1})$,*

$$T' \vdash A[\overline{c}] \Leftrightarrow T \vdash A[\overline{x}].$$

In particular, T' is a conservative extension of T.

Proof. Suppose $T \vdash A[\overline{x}]$. Then $T' \vdash A[\overline{x}]$. Thus, by the substitution rule, $T' \vdash A[\overline{c}]$.

For the converse, assume that $T' \vdash A[\overline{c}]$. Fix a proof of $A[\overline{c}]$ in T', and let $y_0, \cdots, y_{n-1}$ be variables not occurring in this fixed proof. We replace each occurrences of $c_0, \cdots, c_{n-1}$ in the proof by $y_0, \cdots, y_{n-1}$, respectively. It is easy to check that the new sequence of formulas is a proof in T and whose last formula is $B = A_{\overline{x}}[\overline{y}]$. By the substitution rule, $A[\overline{x}] = B_{\overline{y}}[\overline{x}]$ is a theorem of T. □

Proposition 4.2.24. *Let t, $t_1, \ldots, t_n$ and $s_1, \ldots, s_n$ be terms. Then*

$$\vdash t_1 = s_1 \to \cdots \to t_n = s_n \to t[t_1, \ldots, t_n] = t[s_1, \ldots, s_n].$$

Proof. Replace each variable occurring in a t_i or in an s_i by a new constant. Designate the extension of T thus obtained by T'. Let t_i become t_i', s_i become s_i', and t become t'. By the theorem on constants, it suffices to prove that

$$T' \vdash t_1' = s_1' \to \cdots \to t_n' = s_n' \to t'[t_1', \ldots, t_n'] = t'[s_1', \ldots, s_n'].$$

By the deduction theorem, this will follow from

$$T'[t_1' = s_1', \ldots, t_n' = s_n'] \vdash t'[t_1', \ldots, t_n'] = t'[s_1', \ldots, s_n'].$$

This follows from the equality theorem. □

In the same way we prove the following result.

Proposition 4.2.25. *Let $t_1, \ldots, t_n$ and $s_1, \ldots, s_n$ be terms and A a formula of L. Then*

$$\vdash t_1 = s_1 \to \cdots \to t_n = s_n \to (A[t_1, \ldots, t_n] \leftrightarrow A[s_1, \ldots, s_n]).$$

Exercise 4.2.26. Let a variable v not occur in the term t and let A be a formula of L such that t is substitutable for v in A. Then

$$\vdash A_v[t] \leftrightarrow \exists v(v = t \wedge A).$$

4.3 Consistency and Completeness

A theory T is called *inconsistent* if every formula of T is a theorem of T. Otherwise, the theory is called *consistent*. While developing a theory axiomatically, one is naturally confronted with the question of the consistency of the theory. Proving the consistency of theories is often a challenging task in mathematics. This is one of the most important topics in axiomatic set theory. Interested readers may see the excellent book of Kenneth Kunen [9].

Lemma 4.3.1. *A theory T is inconsistent if and only if there is a formula A such that both A and $\neg A$ are theorems of T.*

Proof. The necessary part of the result is clear. Thus, assume that A is such that $\vdash A$ as well as $\vdash \neg A$. Take any formula B. By the expansion axiom and Lemma 3.5.1, $\vdash A \vee B$ and $\vdash \neg A \vee B$. Thus, by the cut rule, $\vdash B \vee B$. Hence, $\vdash B$ by the contraction rule. □

Since a proof is finite, it uses only a finite number of axioms. This immediately gives us the following important result.

Theorem 4.3.2. *A theory is consistent if and only if each of its finitely axiomatized parts is consistent.*

Lemma 4.3.3. *If T has a model, then T is consistent.*

Proof. Suppose T has a model M and it is inconsistent. Take a closed formula A. Then, both A and $\neg A$ are theorems of T. Hence, by the validity theorem, both are valid in M. This is a contradiction. □

Exercise 4.3.4. Let T' be an extension of T. If T' is consistent, show that T is also consistent. Assume, moreover, that T' is a conservative extension of T. Show that the converse is also true, i.e., if T is consistent, so is T'.

The following result is also useful.

Proposition 4.3.5. *Let B be the closure of A. Then $T \vdash A$ if and only if $T[\neg B]$ is inconsistent.*

Proof. Suppose $T \vdash A$. Then by the closure theorem, $T \vdash B$, and hence $T[\neg B] \vdash B$. Hence, $T[\neg B]$ is inconsistent.

Now assume that $T[\neg B]$ is inconsistent. Then $T[\neg B] \vdash B$. Thus, by the deduction theorem, $T \vdash \neg B \to B$. Hence, by the tautology theorem, $T \vdash B$. Thus, $T \vdash A$ by the closure theorem. □

Exercise 4.3.6 (Reduction theorem). Let Γ be a set of formulas of T. Then

$$T[\Gamma] \vdash A$$

if and only if there exist $B_1, \ldots, B_n$, with each being the closure of a formula in Γ, such that

$$T \vdash B_1 \to \cdots \to B_n \to A.$$

A formula A is said to be *undecidable* in a theory T if neither A nor $\neg A$ is a theorem of T; otherwise, the formula is called *decidable* in T.

It is not reasonable to expect that in a theory all formulas will be decidable.

Exercise 4.3.7. Show that the formula $v = 0$ of N is undecidable in N.

A theory T is called *complete* if it is consistent and if every closed formula is decidable in T.

Remark 4.3.8. The importance of giving a complete set of axioms in the foregoing sense cannot be overemphasized. Let T be a theory with a model M. Let T' be the simple extension of T whose nonlogical axioms are precisely those sentences that are valid in M. We designate this theory by $Th(M)$. Clearly $Th(M)$ is complete. However, we may not be able to mechanically decide whether a sentence is valid in M. This is obviously not a satisfactory situation. A theory for which there is an algorithm to decide whether a formula is an axiom is called an *axiomatized theory*. In an epoch-making discovery, Gödel showed that for most theories this is impossible. After introducing the notion of an algorithm, we shall briefly study axiomatized theories in Chap. 6.

Exercise 4.3.9. Let T be a complete theory and A and B closed formulas of T. Show that

(a) $T \vdash A \vee B \Leftrightarrow (T \vdash A \text{ or } T \vdash B)$,
(b) $T \vdash A \wedge B \Leftrightarrow (T \vdash A \text{ and } T \vdash B)$.

The following theorem is due to Adolf Lindenbaum.

Theorem 4.3.10 (Lindenbaum's theorem). *Every consistent theory T admits a simple complete extension.*

Proof. Let $\mathbb{P}$ be the family of subsets Γ of the set of formulas of T such that $T[\Gamma]$ is consistent. Since T is consistent, $\mathbb{P} \neq \emptyset$. ($\emptyset \in \mathbb{P}$.) Partially order $\mathbb{P}$ by inclusion $\subset$. Let C be a chain in $\mathbb{P}$ and $\Gamma = \cup C$. Since every proof is finite, $\Gamma \in \mathbb{P}$. Thus, by Zorn's lemma, $\mathbb{P}$ has a maximal element, say Δ.

Set $T' = T[\Delta]$. Clearly, T' is a simple consistent extension of T.

We claim that T' is complete. Let A be a closed formula of T that is not a theorem of T'. In particular, $A \notin \Delta$. We must show that $T' \vdash \neg A$. If not, then by Proposition 4.3.5, $T'[A]$ is consistent, contradicting the maximality of Δ. □

What follows are two equivalent formulations of the completeness theorem.

Theorem 4.3.11 (Completeness theorem, first form). *If formula A of T is valid in T, then it is a theorem of T.*

Theorem 4.3.12 (Completeness theorem, second form). *Every consistent theory has a model.*

We now show that the two forms are equivalent.

Proof. Assume the first form. Let T be consistent, and let B be a closed formula that is not a theorem of T. Thus, by the first form, it is not valid in T. This in particular gives us a model of T.

Now assume the second form. Assume that $T \models A$. If possible, suppose $T \nvdash A$. By the closure theorem, without loss of generality we assume that A is closed. By Proposition 4.3.5, $T[\neg A]$ is consistent. By the second form, it has a model. Any such model is a model of T in which A is false, i.e., $T \not\models A$. □

4.4 Proof of the Completeness Theorem

In this section we prove the completeness theorem in its second form.

Since we have only syntactical objects at hand, a model of T must be built out of these. Since syntactical objects that designate individuals of a model are variable-free terms of the language of T, it seems quite natural to start with these. However, T may have no constants. If the language of T has constant symbols, then there is indeed a canonical structure of the language.

Assume that $L = L(T)$ has at least one constant symbol. Let N denote the set of all variable-free terms L. For variable-free terms a and b, define

$$a \sim b \text{ if } T \vdash a = b.$$

Lemma 4.4.1. *The binary relation $\sim$ is an equivalence relation on N.*

Proof. (i) The relation $\sim$ is reflexive, i.e., for every variable-free term t,

$$T \vdash t = t.$$

This is so by the identity axiom and the substitution rule.

(ii) It is symmetric by the symmetry theorem and the tautology theorem.

(iii) By the equality axiom and the substitution rule,

$$\vdash s = t \to t = u \to s = u.$$

Hence, the relation is transitive by the detachment rule. □

We set M to be the set of $\sim$-equivalence classes. For any $a \in N$, let $[a]$ denote the equivalence class containing a. Since T has constant symbols, M is nonempty. The set M will be the universe of our intended structure.

We now define the interpretations of the nonlogical symbols of T in M in a natural way:

$$c_M = [c]$$
$$f_M([a_1], \ldots, [a_n]) = [f a_1 \cdots a_n]$$

and

$$p_M([a_1], \ldots, [a_n]) \text{ if and only if } T \vdash p a_1 \cdots a_n.$$

In the preceding definitions, c is a constant symbol (so a variable-free term), $a_1, \ldots, a_n$ are variable-free terms, f is an n-ary function symbol, and p is an n-ary relation symbol. The preceding functions and relations on M are well defined by the equality theorem.

The structure M of L is called its *canonical structure*. By induction on the length of expressions, the following result is quite routine to prove.

Lemma 4.4.2. *For every variable-free term a, $a_M = [a]$.*

Proof. If a is a constant symbol, then the assertion follows by the definition. Suppose the assertion is true for $a_1, \cdots, a_n$, f is a n-ary function symbol, and $a = fa_1 \cdots a_n$. Then

$$a_M = f_M([a_1]_M, \cdots, [a_n]_M) = f_M([a_1], \cdots, [a_n]) = [a].$$

□

This implies the following lemma.

Lemma 4.4.3. *For every atomic sentence A,*

$$T \vdash A \Leftrightarrow M \models A.$$

Proof. Let A be $pa_1 \cdots a_k$ and p a k-ary relation symbol (including =). Then

$$T \vdash A \Leftrightarrow p_M([a]_1, \cdots, [a_k]) \Leftrightarrow p_M((a_1)_M, \cdots, [a_k]_M) \Leftrightarrow M \models pa_1 \cdots a_k.$$

□

When is the canonical structure of L a model of T? We give a sufficient condition first. A theory T is called a *Henkin theory* if for every closed formula of the form $\exists xA$ there is a constant symbol, say c, of L such that

$$T \vdash \exists xA \to A_x[c].$$

Theorem 4.4.4. *If T is a complete Henkin theory, then the canonical structure of T is a model of T.*

Proof. By the closure theorem, the result will be proved if we show that for every closed formula A of L_M,

$$T \vdash A \Leftrightarrow M \models A. \qquad (*)$$

The proof of $(*)$ proceeds by induction on the rank of A.

By Lemma 4.4.3, $(*)$ holds for all atomic A.

Suppose B is the closed formula $\neg A$ and that $(*)$ holds for A. Let $T \vdash B$. Since T is consistent, $T \nvdash A$. By the induction hypothesis, $M \not\models A$. But then $M \models B$. Conversely, suppose $T \nvdash B$. Since T is complete, $T \vdash A$. By the induction hypothesis, $M \models A$. So $M \not\models B$.

Now suppose $A = B \vee C$ and $(*)$ holds for B and C. If $M \models A$, then $M \models B$ or $M \models C$. By the induction hypothesis, $T \vdash B$ or $T \vdash C$. Then $T \vdash A$ by the tautology theorem. On the other hand, assume that $T \vdash A$. Then either $T \vdash B$ or $T \vdash C$. If not, by completeness of T, $T \vdash \neg B$ and $T \vdash \neg C$. By the last case, $M \not\models B$ and $M \not\models C$. This contradicts $M \models A$.

Suppose B is the closed formula $\exists xA$ and $(*)$ holds for all formulas of rank less than the rank of B. Let $T \vdash \exists xA$. Since T is a Henkin theory, there is a constant symbol c such that

$$T \vdash \exists xA \to A_x[c].$$

By the detachment rule,

$$T \vdash A_x[c].$$

By the induction hypothesis, $M \models A_x[c]$. Hence, $M \models B$.

Conversely, suppose $M \models B$. Then there is an $m \in M$ such that $M \models A_x[i_m]$, with i_m the name for m in the language L_M. Let $m = [a]$ for some variable-free term a. By Lemma 4.4.2, $a_M = (i_m)_M = m$, i.e., $M \models a = i_m$. Hence, $M \models A_x[a]$. By the induction hypothesis,

$$T \vdash A_x[a].$$

Since $A_x[a] \to \exists x A$ is a substitution axiom, by the detachment rule,

$$T \vdash B.$$

□

An extension of T that is Henkin is called a *Henkin extension* of T. Clearly, the completeness theorem will be proved if we show that every consistent theory admits a complete Henkin extension, say T'. Then the restriction of the canonical structure of $L(T')$ to $L(T)$ will be a model of T. We proceed to prove this result now.

Lemma 4.4.5. *Let T be a theory and $\exists x B$ a closed formula of T. Let T' be obtained from T by adding a new constant c and a new axiom $\exists x B \to B_x[c]$. Then T' is a conservative extension of T.*

Proof. Let A be a formula of $L(T)$ and $T' \vdash A$. By the deduction theorem,

$$T'' \vdash (\exists x B \to B_x[c]) \to A,$$

where T'' is the theory obtained by introducing the constant symbol c and no new axiom. Let y be a variable distinct from x and not occurring in A and B. By the theorem on constants,

$$T \vdash (\exists x B \to B_x[y]) \to A.$$

But y does not occur in A. Thus, by the $\exists$-introduction rule,

$$T \vdash \exists y(\exists x B \to B_x[c]) \to A.$$

The result now follows from Proposition 4.2.17 and the cut rule. □

Theorem 4.4.6. *Every theory T has a conservative Henkin extension T_∞. In particular, if T is consistent, then so is T_∞.*

Proof. Set $T_0 = T$. Suppose T_n is defined. For each closed formula of the form $D = \exists x B$, introduce a new constant symbol c_D to T_n and a new axiom $D' = \exists x B \to B_x[c_D]$. Let T_{n+1} designate the theory thus obtained.

We claim that T_{n+1} is a conservative extension of T_n. To show this, let A be a formula of T_n and $T_{n+1} \to A$. If T' denotes the theory obtained from T_n by adding these new constants and no new axiom, then by the deduction theorem, there exist new axioms $D'_1, \cdots D'_k$ such that

$$T' \vdash D'_1 \to \cdots \to D'_k \to A.$$

Using Lemma 4.4.5 repeatedly, we see that

$$T_n \vdash A.$$

Now take T_∞ to be the union of all these theories T_n. The rest of the proof is easy. □

Theorem 4.4.7. *Every consistent theory T admits a complete Henkin extension T'.*

Proof. By the last theorem T has a conservative Henkin extension T_∞. Since T is consistent, so is T_∞. By Lindenbaum's theorem, T_∞ has a complete, simple extension T'. Since T' is a simple extension of a Henkin theory, it is Henkin. Thus, we have proved our result. □

The completeness theorem is now proved.

The completeness theorem is a very important result in mathematical logic. It shows that our definition of proof is a correct one. In addition, it is quite useful. Instead of giving the tedious syntactical proofs, now one can establish results using the notion of truth. This is often an easier job. Further, arguments no longer depend on logical axioms and rules of inference.

Let κ be an infinite cardinal. Recall that a theory T is called a κ-theory if its language has at most κ nonlogical symbols.

Theorem 4.4.8. *Let κ be an infinite cardinal and T a consistent κ-theory. Then there is a model M of T such that $|M| \leq \kappa$. In particular, every countable consistent theory has a countable model.*

Proof. The model M obtained in the proof is of cardinality at most κ. (We invite the reader to prove it.) □

Exercise 4.4.9. Let $L(T')$ be an extension of $L(T)$. Show that T' is an extension of T if and only if the restriction of every model of T' to $L(T)$ is a model of T.

Exercise 4.4.10. Show that two theories are equivalent if and only if they have the same models.

Since validity and provability have been shown to be equivalent, the next few results can be proved routinely.

Exercise 4.4.11 (Equivalence Theorem). Let A be a formula of T, and let A' be obtained from A by simultaneously replacing some subformulas $B_1, \cdots, B_k$ of A by $B'_1, \cdots, B'_k$, respectively, and $T \vdash B_i \leftrightarrow B'_i$, $1 \leq i \leq k$. Show that $T \vdash A \leftrightarrow A'$.

Exercise 4.4.12. Show that a formula of T of the form $\neg(fx_1 \cdots x_n = y)$ is equivalent in T to a formula of the form

$$\exists z(\neg(y = z) \wedge fx_1 \cdots x_n = z),$$

with $y, z, x_1, \ldots, x_n$ distinct.

Exercise 4.4.13. (a) Show that

$$\vdash \neg\exists vA \leftrightarrow \forall v\neg A.$$

(b) Show that

$$\vdash \neg\forall vA \leftrightarrow \exists v\neg A.$$

(c) If v is not free in B, show that

$$\vdash \exists vA \vee B \leftrightarrow \exists v(A \vee B),$$

$$\vdash \forall vA \vee B \leftrightarrow \forall v(A \vee B),$$

$$\vdash B \vee \exists vA \leftrightarrow \exists v(B \vee A),$$

and

$$\vdash B \vee \forall vA \leftrightarrow \forall v(B \vee A).$$

Exercise 4.4.14. Show the following:

(a) $\vdash \exists v(A \vee B) \leftrightarrow \exists vA \vee \exists vB$.
(b) $\vdash \forall v(A \wedge B) \leftrightarrow \forall vA \wedge \forall vB$.
(c) $\vdash \exists v(A \wedge B) \rightarrow \exists vA \wedge \exists vB$.
(d) $\vdash \forall vA \vee \forall vB \rightarrow \forall v(A \vee B)$.

Exercise 4.4.15. Give examples A and B of formulas of N such that the formulas

$$\forall v(A \vee B) \rightarrow \forall vA \vee \forall vB$$

and

$$\exists vA \wedge \exists vB \rightarrow \exists v(A \wedge B)$$

are not theorems of N.

Exercise 4.4.16. Let v and w be distinct variables. Show the following:

(a) $\vdash \exists v\exists wA \leftrightarrow \exists w\exists vA$.
(b) $\vdash \forall v\forall wA \leftrightarrow \forall w\forall vA$.
(c) $\vdash \exists v\forall wA \rightarrow \forall w\exists vA$.

Exercise 4.4.17. Give a formula of N of the form

$$\forall v\exists wA \rightarrow \exists w\forall vA$$

that is not a theorem.

A formula A is said to be in *prenex form* if it is in the form

$$Q_1 v_1 \cdots Q_n v_n B,$$

where each Q_i is either $\exists$ or $\forall$, and B is open. Then $Q_1 v_1 \cdots Q_n v_n$ is called the *prefix* and B the *matrix* of A. A formula in prenex form is called *existential* if all the quantifiers in its prefix are $\exists$; a formula in prenex form is called *universal* if all the quantifiers in its prefix are $\forall$.

Exercise 4.4.18. Show that every formula is equivalent in T to a formula in prenex form whose matrix is of the form

$$\wedge_{i=1}^{k} \vee_{j=1}^{n_i} B_{ij},$$

where each B_{ij} is a literal.

Exercise 4.4.19. Let T be a consistent theory. Call formulas A and B *equivalent in* T if $T \vdash A \leftrightarrow B$ and write $A \equiv_T B$. Show that $\equiv_T$ is an equivalence relation on the set $\mathscr{F}$ of formulas of T. Set

$$\mathscr{L}(T) = \mathscr{F} / \equiv_T = \{[A] : A \in \mathscr{F}\},$$

which is the set of all $\equiv_T$-equivalence classes $[A]$ of formulas A of T. Now define

$$\begin{aligned} 0 = [A \wedge \neg A], 1 &= [A \vee \neg A], \\ [A]' &= [\neg A], \\ [A] + [B] &= [A \vee B], \end{aligned}$$

and

$$[A] \cdot [B] = [A \wedge B].$$

Show that these are well defined and that they make $\mathscr{L}(A)$ a Boolean algebra called the *Lindenbaum algebra of* T.

4.5 Interpretations in a Theory

In this section we define an interpretation of a theory T in another theory T'. Semantically, this would mean that given any model of T' one can define a model of T. For instance, starting from the Peano axioms, we construct rational numbers and show that they form a field. Thus we can say that field theory has a model in Peano arithmetic.

Let L and L' be first-order languages. An *interpretation* I of L in L' consists of the following items:

(a) A unary predicate symbol U_I of L' called the *universe* of L;
(b) For each constant symbol c of L, a constant symbol c_I of L';
(c) For each n-ary function symbol f of L, an n-ary function symbol f_I of L';
(d) For each n-ary relation symbol p of L other than $=$, an n-ary relation symbol p_I of L'.

Let I be an interpretation of L in L' as above and t a term of L. The term, designated by t_I, of L' obtained from t by replacing each nonlogical symbol u of L by u_I is called the *interpretation of t by I*.

An *interpretation* of L in a theory T' is an interpretation I of L in $L(T')$ such that

$$T' \vdash U_I(c_I) \tag{1}$$

for each constant symbol c of L,

$$T' \vdash \exists x U_I x, \tag{2}$$

and

$$T' \vdash U_I x_1 \to \cdots \to U_I x_n \to U_I f_I x_1 \ldots x_n \tag{3}$$

for each n-ary function symbol f of L.

The first condition requires that T' prove that the universe U_I contains each c_I; the second requires that T' prove that U_I is nonempty; the third requires that in the theory T', f_I must be an n-ary function whose restriction to U_I takes values in U_I. An interpretation I of L in T' may be thought of as a structure of L in T' where the underlying universe is U_I.

Let A be a formula of L. We now proceed to define a formula A^I of L' such that $T' \vdash A^I$ will mean that A is true in the structure U_I. Let A_I be the formula of $L(T')$ obtained from A by replacing each nonlogical symbol u occurring in A by u_I and also replacing each subformula of A of the type $\exists x B$ by $\exists x(U_I x \wedge B_I)$. More precisely, we define A_I by induction on the rank of A. For atomic formulas, we obtain A_I from A by replacing each nonlogical symbol u occurring in A by u_I. If A is $\neg B$ or $B \vee C$, then A_I is $\neg B_I$ or $B_I \vee C_I$, respectively. If A is $\exists x B$, then A_I is $\exists x(U_I x \wedge B_I)$.

Finally, if $x_0, \ldots, x_{n-1}$ are all the variables that are free in A (and hence in A_I) in alphabetical order, then A^I is the formula

$$U_I x_0 \to \cdots \to U_I x_{n-1} \to A_I.$$

Note that if A is closed, then A^I is the formula A_I.

An *interpretation* of a theory T in a theory T' is an interpretation I of $L(T)$ in $L(T')$ such that for every nonlogical axiom A of T, $T' \vdash A^I$.

Theorem 4.5.1. *If T has an interpretation in T' and if T' is consistent, then so is T.*

Proof. Let I be an interpretation of T in T' with universe U_I. Since T' is consistent, by the completeness theorem, it has a model M.

Set

$$N = (U_I)_M.$$

By (1) and the validity theorem, N is a nonempty set. For any relation symbol p of T, let p_N be the restriction of $(p_I)_M$ to N. Now take an n-ary function symbol f of T. By (2) and the validity theorem, N is closed under $(f_I)_M$. We define f_N as the restriction of $(f_I)_M$ to N. Thus, N is a structure for $L(T)$.

Now let A be a nonlogical axiom of T. Then $T' \vdash A^I$. Hence, by the validity theorem, $M \models A^I$. Now it is quite easy to check that $N \models A$. So N is a model of T. □

An interpretation I of T in T' is called *faithful* if for every formula φ of T, $T' \vdash \varphi^I \Rightarrow T \vdash \varphi$.

Exercise 4.5.2. Suppose T has a faithful interpretation in an extension by definitions of T' and T' is consistent. Show that T is consistent.

4.6 Extension by Definitions

In a theory we begin with a minimal possible number of undefined concepts (constant, function, and predicate symbols of the theory). Axioms of the theory state their basic properties. But as the theory develops, more and more concepts are introduced, and they are treated as an integral part of the theory. For instance, in number theory, subtraction is not a nonlogical symbol of N. It is defined later. Similarly, in set theory, $\subset$ (inclusion) is a defined concept and not a nonlogical symbol of the language of set theory. Results proved using these concepts are taken as theorems of the original theory. In this section, we show that this is a logically correct process.

Let $\varphi[v_1, \ldots, v_n]$, with v_i being distinct, be a formula of T. We form an extension T' of T by adding a new n-ary relation symbol p and adding a new nonlogical axiom

$$pv_1 \cdots v_n \leftrightarrow \varphi. \tag{1}$$

Formula (1) is called the *defining axiom* of p.

Example 4.6.1. In *ZF*, if we add a binary relation symbol $\subset$ and a new axiom

$$x \subset y \leftrightarrow \forall z(z \in x \rightarrow z \in y),$$

then we get an extension by definition of *ZF* in which $\subset$ (*subset*) is a defined concept.

Proposition 4.6.2. *Let $\varphi[v_1,\dots,v_n]$ be a formula of T, and let T' be obtained from T by adding a new n-ary relation symbol p, with*

$$pv_1\cdots v_n \leftrightarrow \varphi$$

as its defining axiom. Then T' is a conservative extension of T.

Proof. Let A be a formula of T that is a theorem of T'. By the completeness theorem, the proof will be complete if we show that A is valid in T. Let M be a model of T. Interpret p in M as follows: for $a_1,\dots,a_n \in M$,

$$p(a_1,\dots,a_n) \Leftrightarrow M \models \varphi_{v_1,\dots,v_n}[i_{a_1},\dots,i_{a_n}].$$

Thus, we get a model M' of T'. By the validity theorem,

$$M' \models A.$$

But this implies that

$$M \models A.$$

□

Now we consider a similar method of adding a function symbol to a theory. Let $v_0,\dots,v_{n-1}$ and w,w' be distinct variables, and let $\varphi[v_0,\dots,v_{n-1},w]$ be a formula of T. Further, assume that

$$T \vdash \exists w\varphi \tag{i}$$

and

$$T \vdash (\varphi \wedge \varphi_w[w']) \rightarrow w = w'. \tag{ii}$$

Informally speaking, conditions (i) and (ii) say that for all $v_0,\dots,v_{n-1}$, there is a unique w "satisfying" φ. We form T' from T by adding a new n-ary function symbol f and a new nonlogical axiom

$$w = fv_0\cdots v_{n-1} \leftrightarrow \varphi. \tag{iii}$$

Formula (iii) is called the *defining axiom* of f.

Example 4.6.3. In ZF (after adding $\subset$), consider the following formula $\varphi[x,y]$:

$$\forall z(z \in y \leftrightarrow z \subset x).$$

Using the power set, comprehension, and extensionality axioms, one shows that the formula φ satisfies (i) and (ii) for $T = ZF$ (in fact the extension of ZF obtained by adding $\subset$). Thus, one may add a new unary function symbol $\mathscr{P}$ (traditionally called a *power set*) and a new nonlogical axiom

$$y = \mathscr{P}(x) \leftrightarrow \varphi.$$

Remark 4.6.4. Note that if $n = 0$, then this method adds a new constant symbol to T. As an example, we can add a constant symbol 0 (called an *empty set*) in an extension by definition of *ZF*. This can be seen as follows. Let $A[y]$ be the formula

$$\forall x \neg (x \in y).$$

Using the set existence, extensionality, and comprehension axioms of *ZF*, one shows that A satisfies conditions (i) and (ii) for $T = ZF$. One then defines an extension by definition of *ZF* by adding a new constant symbol 0 and a new axiom

$$y = 0 \leftrightarrow A.$$

Proposition 4.6.5. *Let T' be obtained from T by adding a new n-ary function symbol f with*

$$w = f v_0 \cdots v_{n-1} \leftrightarrow \varphi$$

as its defining axiom. Then T' is a conservative extension of T.

Proof. Let A be a formula of T that is a theorem of T'. By the completeness theorem, the proof will be complete if we show that A is valid in T. Let M be a model of T. Interpret f in M as follows: for $b, a_0, \ldots, a_{n-1} \in M$,

$$b = f_M(a_0, \ldots, a_{n-1}) \Leftrightarrow M \models \varphi_{w,v_0,\ldots,v_{n-1}}[i_b, i_{a_0}, \ldots, i_{a_{n-1}}].$$

Thus, we get a structure M' of $L(T')$ that is an expansion of M. It is easy to check that M' is a model of T'.

By the validity theorem,

$$M' \models A.$$

But this implies that

$$M \models A.$$

□

We say that T' is an *extension by definitions* of T if T' is obtained from T by a finite number of extensions of the two types that we have described.

Theorem 4.6.6. *If T' has an interpretation in an extension by definitions of T, then T' is a conservative extension of T. In particular, T is consistent if and only if T' is consistent.*

Remark 4.6.7. This is a very important result. It gives a method to prove relative consistency results.

We state some interesting results without proof.

Theorem 4.6.8. *Peano arithmetic PA has an interpretation in an extension by definitions of* ZF *[9].*

Theorem 4.6.9. *Each Peano arithmetic PA and ZF − Infinity has a faithful interpretation in an extension by the definitions of the other. In particular, PA is consistent if and only if ZF − Infinity is consistent. [9, Exercise 30, p.149].*

4.7 Some Metatheorems in Arithmetic

In this section we prove a few metatheorems pertaining to the theories N and PA. They are needed to prove the first incompleteness theorem.

Proposition 4.7.1. *For any formula A of N and any $n \in \mathbb{N}$,*

$$N \vdash A_v[k_0] \to \cdots \to A_v[k_{n-1}] \to v < k_n \to A.$$

Proof. We prove the result by induction on n. For $n = 0$, the result follows since $\neg(v < 0)$ is an axiom of N.

Let the result be true for some n. By axiom (8) of N,

$$N \vdash v < k_{n+1} \leftrightarrow v < k_n \vee v = k_n.$$

By the equality theorem,

$$N \vdash v = k_n \to (A \leftrightarrow A_v[k_n]).$$

Hence, by the induction hypothesis and the tautology theorem,

$$N \vdash A_v[k_0] \to \cdots \to A_v[k_{n-1}] \to A_v[k_n] \to v < k_{n+1} \to A.$$

□

Proposition 4.7.2. *Let $N \vdash \neg A_v[k_i]$ for all $i < n$ and $N \vdash A_v[k_n]$. Then*

$$N \vdash A \wedge \forall w(w < v \to \neg A_v[w]) \leftrightarrow v = k_n.$$

Proof. Let B denote the formula

$$A \wedge \forall w(w < v \to \neg A_v[w]).$$

By the equality theorem,

$$N \vdash v = k_n \to (B \leftrightarrow B_v[k_n]). \tag{1}$$

By Proposition 4.7.1, we have

$$N \vdash \neg(A_v[w])_w[k_0] \to \cdots \to \neg(A_v[w])_w[k_{n-1}] \to w < k_n \to \neg A_v[w]. \tag{2}$$

Hence, by the hypothesis of our proposition, the detachment rule, and the generalization rule,

$$N \vdash \forall w(w < k_n \to \neg A_v[w]). \tag{3}$$

Since $N \vdash A_v[k_n]$, by (1) and (3) and the tautology theorem,

$$N \vdash v = k_n \to B. \tag{4}$$

By the substitution theorem, we have

$$N \vdash \forall w(w < v \to \neg A_v[w]) \to (k_n < v \to \neg A_v[k_n]).$$

But $N \vdash A_v[k_n]$. Hence, by the tautology theorem,

$$N \vdash B \to \neg(k_n < v). \tag{5}$$

Since $N \vdash \neg A_v[k_i]$, $i < n$, by Proposition 4.7.1 and the detachment rule,

$$N \vdash v < k_n \to \neg A.$$

Hence,

$$N \vdash B \to \neg(v < k_n). \tag{6}$$

By axiom (9) of N,

$$N \vdash v < k_n \vee v = k_n \vee k_n < v. \tag{7}$$

Hence, by (4)–(7) and the tautology theorem, we get

$$N \vdash B \leftrightarrow v = k_n.$$

□

Example 4.7.3. Peano arithmetic *PA* is an extension of N.

This will follow if we show that axiom (9)

$$x < y \vee x = y \vee y < x$$

of theory N is a theorem of *PA*. We show this in three steps.

Step 1: $PA \vdash 0 = y \vee 0 < y$.

Let A be the formula $0 = y \vee 0 < y$. Then $PA \vdash A_y[0]$. By axiom (8) of N (which is also an axiom of *PA*),

$$PA \vdash A \leftrightarrow 0 < Sy.$$

Also,

$$PA \vdash 0 < Sy \to A_y[Sy].$$

Hence,

$$PA \vdash A \to A_y[Sy].$$

Thus, by the induction axiom of PA,

$$PA \vdash A.$$

Step 2: $PA \vdash x < y \to Sx < Sy$.

Let B be the formula $x < y \to Sx < Sy$. By axiom (7) of N,

$$PA \vdash B_y[0].$$

By axiom (8) of N,

$$PA \vdash B_y[Sy] \leftrightarrow ((x < y \vee x = y) \to (Sx < Sy \vee Sx = Sy)).$$

Thus, by the equality axiom,

$$PA \vdash (x < y \vee x = y) \to (Sx < Sy \vee Sx = Sy).$$

Hence,

$$PA \vdash B \to B_y[Sy].$$

By the induction axiom of PA, $PA \vdash B$.

Step 3: Let C denote the formula $x < y \vee x = y \vee y < x$. Since $PA \vdash A$ (Step 1),

$$PA \vdash C_x[0].$$

Since $PA \vdash B$ (Step 2), by axiom (8) of N,

$$PA \vdash x < y \to (Sx < y \vee Sx = y)$$

and

$$PA \vdash (y < x \vee y = x) \to y < Sx.$$

Hence,

$$PA \vdash C \to C_x[Sx].$$

Thus, by the induction axiom of P,

$$PA \vdash C.$$

Thus PA is a finite extension of N.

Exercise 4.7.4. Let φ be a formula of *PA*, with x, y distinct, such that y variables does not occur in φ. Show the following:

(a) $PA \vdash \forall x(\forall y(y < x \to \varphi_x[y]) \to \varphi) \to \forall x\varphi$.
(b) $PA \vdash \exists x\varphi \to \exists x(\varphi \wedge \forall y(y < x \to \neg\varphi_x[y]))$.

Exercise 4.7.5. Let φ be a formula of *PA* in which no variable besides $v_1, \ldots, v_n$ and w is free, with $v_1, \ldots, v_n, w$ distinct. Suppose $PA \vdash \exists w\varphi$. Let w' be a new variable and ψ the formula

$$\varphi \wedge \forall w'(w' < w \to \neg\varphi_w[w']).$$

Show the following:

(a) $PA \vdash \exists w\psi$.
(b) $PA \vdash \psi \wedge \psi_w[w''] \to w = w''$.

Chapter 5
Model Theory

This chapter is devoted to model theory. Model theory is a general study of mathematical structures such as groups, rings, fields, and several other mathematical structures. Model theory is used to prove substantial results in conventional mathematics such as number theory, algebra, and algebraic geometry. Also, questions from logic pertaining to conventional mathematical structures throw up a good challenge to logic. This interplay between mathematics and logic has grown into very fascinating mathematics and is a very active area of research today. Chapter 2 should be considered as a part of model theory where, for example, embeddings, isomorphisms, homogeneous structures, and definability have been introduced and some important results are proved.

5.1 Applications of the Completeness Theorem

In this section, we give some applications of the completeness theorem for first-order theories.

Proposition 5.1.1. *Let T be a consistent theory. Then the following statements are equivalent:*

(1) *The theory T is complete.*
(2) *Any two models M and N of T are elementarily equivalent.*
(3) *For any model M of T, T is equivalent to $Th(M)$, i.e., they have the same models.*

Proof. We first show that (1) implies (2). Let φ be a sentence in T. If $T \vdash \varphi$, then $M \models \varphi$ as well as $N \models \varphi$. If $T \nvdash \varphi$, then by (1), $T \vdash \neg\varphi$. But then $N \not\models \varphi$ and $M \not\models \varphi$. Thus (1) implies (2).

Now assume (2). Any model of $Th(M)$ is clearly a model of T. On the other hand, let N be a model of T. By (2), every theorem of $Th(M)$ is valid in N, i.e., N is a model of $Th(M)$. Thus, T and $Th(M)$ are equivalent.

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_5,
© Springer Science+Business Media New York 2013

We now prove that (3) implies (1). Let φ be a closed formula. Exactly one of φ, $\neg\varphi$ is in $Th(M)$. Hence, by (3), exactly one of them is a theorem of T. □

Let L be a language and $\mathscr{M}$ a class of structures for L. We say that $\mathscr{M}$ is *finitely axiomatizable* if there is a finite set T of sentences of L such that $M \models T \Leftrightarrow M \in \mathscr{M}$.

Proposition 5.1.2. *Any finite set of first-order sentences that is valid in the theory T of torsion-free abelian groups is true in some abelian group with torsion. Hence, the theory of torsion-free abelian groups is not finitely axiomatizable.*

Proof. Let $A_1, \ldots, A_n$ be sentences of L that are valid in T. Thus, by the completeness theorem, these are theorems of T. Since a proof of A_i, $1 \leq i \leq n$, contains only finitely many axioms P_m of the form

$$\forall x(x \neq 0 \rightarrow mx \neq 0),$$

there is a natural number k such that each A_i has a proof in T without using axioms P_i for $i > k$. Now take a prime $p > k$ and consider the abelian group $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p. Since $P_2, \cdots, P_k$ as well as $A_1, \cdots, A_n$ are true in it and it is not torsion-free, the result follows. □

The same is true of the theories of divisible abelian groups *DAG*, of ordered divisible abelian groups *ODAG*, and of algebraically closed fields *ACF*.

Proposition 5.1.3. (*i*) *The class of all divisible abelian groups is not finitely axiomatizable.*
(*ii*) *The class of all ordered divisible abelian groups is not finitely axiomatizable.*
(*iii*) *The class of all algebraically closed fields is not finitely axiomatizable.*
(*iv*) *Any finite set of first-order sentences of the theory of fields that are valid in the theory of fields of characteristic zero are valid in fields of characteristic p for all large p.*
(*v*) *The class of all algebraically closed fields of characteristic p, with p a prime or $p = 0$, is not finitely axiomatizable.*

Proof. For $n > 0$, let P_n denote the formula

$$\forall v_0 \cdots \forall v_n \exists v_{n+1}(v_n v_{n+1}^n + v_{n-1} v_{n+1}^{n-1} + \cdots + v_1 v_{n+1} + v_0 = 0).$$

Let $A_1, \cdots, A_k$ be finitely many theorems of the theory of algebraically closed fields. By arguing as above, we see that there is a field that is not algebraically closed but in which all A_i are true. This proves (*iii*). We leave the rest of the proof as an exercise for the reader. □

5.2 Compactness Theorem

In this section we prove a very important theorem in model theory – the compactness theorem – and give some of its applications.

Using the fact that a proof is finite, the completeness theorem immediately gives us the following theorem.

Theorem 5.2.1 (Compactness theorem). *A theory T has a model if and only if each finite $T' \subset T$ has a model.*

Proof.

$$\begin{aligned} T \text{ has a model} &\Leftrightarrow T \text{ is consistent} \\ &\Leftrightarrow \text{each finite } T' \subset T \text{ is consistent} \\ &\Leftrightarrow \text{each finite } T' \subset T \text{ has a model.} \end{aligned}$$

□

Remark 5.2.2. The compactness theorem for first-order theories was first proved for countable theories by Gödel in 1930. In its full generality, it was proved by Malcev. Malcev was also the first to see the power of this theorem.

Let L be a first-order language and Φ a set of formulas of L. Let $x_0, x_1, \ldots$ be all the variables (finitely or countably many), with x_i distinct, that has a free occurrence in a $\varphi \in \Phi$. We say that Φ is *satisfiable* if there is a structure M for L and $a_0, a_1, \ldots \in M$ such that for all $\varphi[x_0, \cdots, x_{n-1}] \in \Phi$, $M \models \varphi[i_{\overline{a}}]$. We say that Φ is finitely satisfiable if every finite $\Phi' \subset \Phi$ is satisfiable.

Proposition 5.2.3. *Every finitely satisfiable Φ is satisfiable.*

Proof. Introduce in L a new constant c_i corresponding to each x_i that has a free occurrence in Φ and call the resulting language L'. Now consider

$$\Phi' = \{\varphi[\overline{c}] : \varphi[\overline{x}] \in \Phi\}.$$

Note that Φ is satisfiable if and only if Φ' has a model. By the compactness theorem, it is sufficient to prove that each finite part of Φ' has a model. This follows because Φ is finitely satisfiable. □

Proposition 5.2.4. *If a theory T has arbitrarily large finite models, it has an infinite model.*

Proof. Let $\{c_n : n \in \mathbb{N}\}$ be a sequence of distinct symbols not appearing in L. Let T' be the extension of T obtained by adding each c_n as a new constant symbol, and for each $m < n$ let the formula $c_n \neq c_m$ be an axiom.

Since T has arbitrarily large finite models, each finite $T'' \subset T'$ has a model. Hence, by the compactness theorem, T' has a model. Clearly, any model of T' is infinite and a model of T. □

Remark 5.2.5. This also shows that there is no theory T whose models are precisely finite sets.

The compactness theorem gives nonstandard models of number theory, real numbers, etc.

Proposition 5.2.6. *Let L be a language with constants 0, 1, binary function symbols $+$ and $\cdot$, and a binary relation symbol $<$. Let $\mathbb{N}$ denote the standard model of natural numbers. There is a structure M for L elementarily equivalent to the standard model $\mathbb{N}$ and having an element b such that for every natural number n, $n < b$.*

Proof. Introduce a new constant symbol c to $L_{\mathbb{N}}$. For each natural number m, let A_m be the formula $\underline{m} < c$. Now consider the theory

$$N' = Diag_{el}(\mathbb{N}) \cup \{A_m : m \in \mathbb{N}\}.$$

Since every finite set of natural numbers has an upper bound in $\mathbb{N}$, it is a model of each finite part of N'. Hence, by the compactness theorem, N' has a model M. This model has the required properties with $b = c_M$. □

Proposition 5.2.7. *There is a non-Archimedean ordered field ${}^*\mathbb{R}$ elementarily equivalent to the ordered field $\mathbb{R}$.*

Proof. Let T denote the theory of ordered fields with a language, say L. Add a new constant symbol c to $L_{\mathbb{R}}$. For natural numbers n, let A_n be the formula $n1 < c$, and consider

$$T' = T \cup Diag_{el}(\mathbb{R}) \cup \{A_n : n \in \mathbb{N}\}.$$

Since the real line $\mathbb{R}$ is a model of each finite $T'' \subset T'$, by the compactness theorem, T' has a model. Any model ${}^*\mathbb{R}$ of T' does the job. □

Exercise 5.2.8. Show that the class of all Archimedean ordered fields is not elementary.

A linearly ordered set $(M, <)$ is called *well ordered* if $\emptyset \neq A \subset M$ implies that there exists an $x \in A$ such that $x \leq y$ for all $y \in A$, i.e., A has a least element x. For instance the set $\mathbb{N}$ with the usual order is a well-ordered set.

Exercise 5.2.9. Show that a linearly ordered set $(M, <)$ is well ordered if and only if there is no infinite sequence $\{a_n\}$ in M such that $a_{n+1} < a_n$ for all n.

Proposition 5.2.10. *The class of all well-ordered sets is not elementary.*

Proof. Let L be a language with a binary predicate symbol $<$ alone. If possible, let T be a theory with language L whose models are precisely well-ordered sets. For each $n \in \mathbb{N}$, introduce a new constant symbol c_n to L and an axiom $c_{n+1} < c_n$. Let T' denote the new theory. The well-ordered set $\mathbb{N}$ is a model of each finite $T'' \subset T'$. So T' has a model M that is a model of T but is not well ordered. □

5.3 Upward Löwenheim–Skolem Theorem

Theorem 5.3.1 (Tarski). *Let κ be an infinite cardinal. Assume that T has an infinite model M. Then T has a model of cardinality at least κ.*

Proof. Fix a set $\{c_\alpha : \alpha < \kappa\}$ of cardinality κ of distinct symbols not appearing in L. Let L' be the extension of L obtained by adding each c_α as a constant symbol. Set $\Gamma = \{c_\alpha \neq c_\beta : \alpha < \beta < \kappa\}$, and consider the theory $T' = T[\Gamma]$ with language L'.

We claim that T' is finitely satisfiable. To see this, fix a finite subset Γ' of Γ. Let $c_{\alpha_1}, \ldots, c_{\alpha_k}$ be all the new constants that appear in a formula in Γ'. Since M is infinite, there exist distinct elements $b_1, \ldots, b_k$ of M. Interpret c_{α_i} by b_i, $1 \leq i \leq k$. Thus we get a model of $T[\Gamma']$. Hence, by the compactness theorem, T' has a model. Now note that any model of T' is of cardinality at least κ and a model of T. □

Under the hypothesis of Tarski's theorem, we can say more.

Theorem 5.3.2 (Tarski). *Let κ be an infinite cardinal and T a consistent κ-theory. Assume that T has an infinite model M. Then T has a model of cardinality κ.*

Proof. Let T' be the theory obtained from T as in the proof of Theorem 5.3.1. Note that T' is a consistent κ-theory. By Theorem 4.4.8, T' has a model N of cardinality at most κ. Since any model of T' is of cardinality at least κ, $|N| = \kappa$. Thus, we get a model of T of cardinality κ. □

Theorem 5.3.3 (Upward Löwenheim–Skolem theorem). *Let κ be an infinite cardinal and L a κ-language. Then every infinite structure N of L of cardinality at most κ has an elementary extension M of cardinality κ.*

Proof. Note that the elementary diagram $Diag_{el}(N)$ of N is a consistent κ-theory. Further, N is an infinite model of $Diag_{el}(N)$. Hence, by Theorem 5.3.2, $Diag_{el}(N)$ has a model M of cardinality κ. By Proposition 2.4.9, M is an elementary extension of N. □

Exercise 5.3.4. Show that there are models of N of arbitrarily large infinite cardinality elementarily equivalent to $\mathbb{N}$.

Let κ be an infinite cardinal. A consistent κ-theory T is called κ-*categorical* if any two models of T of cardinality κ are isomorphic.

Our interest in this concept stems from the following result of Robert Vaught.

Theorem 5.3.5 (Vaught). *Let κ be an infinite cardinal and T a consistent κ-theory all of whose models are infinite. If T is κ-categorical, then T is complete.*

Proof. Suppose a sentence φ is not decidable in T. By Proposition 4.3.5, the theories $T_1 = T[\varphi]$ and $T_2 = T[\neg\varphi]$ are consistent. Since T has no finite models, both T_1 and T_2 have infinite models. Thus, by Theorem 5.3.2, T_1 and T_2 have models M_1 and M_2, respectively, of cardinality κ. Hence, by the hypothesis of the theorem, they are isomorphic. But φ is valid in M_1 and not in M_2, contradicting that T is κ-categorical. Hence, T is complete. □

5.4 Ultraproduct of Models

It is natural to ask whether the compactness theorem can be proved directly without using the completeness theorem, i.e., can we build a model of T from the models of its finite parts? Indeed we can. In this section, we present such a proof. This also gives us an important technique for building models.

Let I be a nonempty set. A *filter on* I is a family $\mathscr{F}$ of subsets of I satisfying the following conditions:

1. $\emptyset \notin \mathscr{F}$ and $I \in \mathscr{F}$.
2. $A, B \in \mathscr{F} \Rightarrow A \cap B \in \mathscr{F}$.
3. If $A \in \mathscr{F}$ and $B \supset A$, $B \in \mathscr{F}$.

It is clear that if $\mathscr{F}$ is a filter, then it satisfies the *finite intersection property*, i.e., for every finite $\mathscr{F}' \in \mathscr{F}$, $\cap \mathscr{F}' \neq \emptyset$.

Exercise 5.4.1. Let $\mathscr{B}$ be a family of subsets of I with the finite intersection property. Then

$$\mathscr{F} = \{A \subset I : \exists B_1, \cdots B_n \in \mathscr{B}(\cap_j B_j \subset A)\}$$

is a filter on I.

Indeed, the filter $\mathscr{F}$ described above is the smallest filter containing $\mathscr{B}$, which we shall refer to as the filter generated by $\mathscr{B}$.

Let L be a first-order language and $\mathscr{F}$ a filter on a nonempty set I. Suppose for each $i \in I$ we are given a structure M_i of L. Set

$$M = \times_{i \in I} M_i.$$

For $\alpha, \beta \in M$, define

$$\alpha \sim \beta \Leftrightarrow \{i \in I : \alpha(i) = \beta(i)\} \in \mathscr{F}.$$

Since $I \in \mathscr{F}$, $\sim$ is reflexive. Clearly, it is symmetric. Since $\mathscr{F}$ is closed under finite intersections, $\sim$ is transitive. Thus, $\sim$ is an equivalence relation on $\times_i M_i$.

We set

$$M(\mathscr{F}) = M/\sim = \{[\alpha] : \alpha \in M\}.$$

Thus, $M(\mathscr{F})$ is the set of all $\sim$-equivalence classes $[\alpha]$, $\alpha \in M$.

We now interpret the nonlogical symbols of L as follows:

1. If c is a constant symbol, $c_{M(\mathscr{F})} = [\alpha]$, where $\alpha(i) = c_{M_i}$, $i \in I$.
2. If p is an n-ary relation symbol, then

$$p_{M(\mathscr{F})}([\alpha_1], \cdots, [\alpha_n]) \Leftrightarrow \{i \in I : p_{M_i}(\alpha_1(i), \cdots, \alpha_n(i))\} \in \mathscr{F}.$$

3. If f is an n-ary function symbol, then we define

$$[\beta] = f_{M(\mathscr{F})}([\alpha_1], \cdots, [\alpha_n]) \Leftrightarrow \{i \in I : \beta(i) = f_{M_i}(\alpha_1(i), \cdots, \alpha_n(i))\} \in \mathscr{F}.$$

We need to show that $p_{M(\mathscr{F})}$ and $f_{M(\mathscr{F})}$ are well defined. Suppose $\alpha_j \sim \beta_j$, $1 \leq j \leq n$. Since $\mathscr{F}$ is closed under finite intersections, there is an $X \in \mathscr{F}$ such that $\alpha_j(i) = \beta_j(i)$ for all $1 \leq j \leq n$ and all $i \in X$. This implies the well-definedness of $p_{M(\mathscr{F})}$ and $f_{M(\mathscr{F})}$.

From the definition it follows that for every atomic formula $\varphi[\overline{x}]$ and every $\overline{\alpha} \in M$,

$$M(\mathscr{F}) \models \varphi[i_{[\alpha_0]}, \cdots i_{[\alpha_{n-1}]}] \Leftrightarrow \{i \in I : M_i \models \varphi[i_{\alpha_0(i)}, \cdots, i_{\alpha_{n-1}(i)}]\} \in \mathscr{F}.$$

We would like this equivalence to hold for every formula. We now proceed to present an important sufficient condition.

Given a filter $\mathscr{F}$ on I, consider

$$\mathbb{P} = \{\mathscr{F}' : \mathscr{F}' \supset \mathscr{F} \text{ and } \mathscr{F}' \text{ a filter on } I\}.$$

Since $\mathscr{F} \in \mathbb{P}$, $\mathbb{P} \neq \emptyset$. $\mathbb{P}$ is a partially ordered set, partially ordered by the inclusion $\subset$.

If $\{\mathscr{F}_a : a \in A\}$ is a chain in $\mathbb{P}$, then $\cup_a \mathscr{F}_a$ is a filter on I containing each $\mathscr{F}_a$. Thus, by Exercise 5.4.1 and Zorn's lemma, we now have the following proposition.

Proposition 5.4.2. *Every family $\mathscr{B}$ of subsets of I with the finite intersection property is contained in a maximal filter on I.*

Maximal filters are also called *ultrafilters*. If $\mathscr{U}$ is an ultrafilter on I, then the structure $M(\mathscr{U})$ is called the *ultraproduct of M_i*. If each $M_i = M$, then it is denoted by $M^{\mathscr{U}}$ and is called an *ultrapower* of M.

Proposition 5.4.3. *Let $\mathscr{F}$ be a filter on I. The following conditions are equivalent.*

(a) $\mathscr{F}$ is an ultrafilter.
(b) If $B \subset I$ is such that $B \cap A \neq \emptyset$ for every $A \in \mathscr{F}$, then $B \in \mathscr{F}$.
(c) For every $B \subset I$, $B \in \mathscr{F}$ or $I \setminus B \in \mathscr{F}$.

Proof. Assume (a). If B satisfies the hypothesis of (b), then $\mathscr{F} \cup \{B\}$ satisfies the finite intersection property. Hence, by Exercise 5.4.1, there is a filter $\mathscr{F}' \supset \mathscr{F} \cup \{B\}$. Now the maximality of $\mathscr{F}$ implies that $B \in \mathscr{F}$.

Now assume (b). Let $B \subset I$ be a subset of I such that neither B nor $I \setminus B$ belongs to $\mathscr{F}$. By (b), there exist $A_1, A_2 \in \mathscr{F}$ such that $B \cap A_1 = \emptyset$ and $(I \setminus B) \cap A_2 = \emptyset$. This implies that $\emptyset = A_1 \cap A_2 \in \mathscr{F}$, which is not the case. Thus, (b) implies (c).

Now assume (c). Suppose there is a filter $\mathscr{F}'$ on I containing $\mathscr{F}$ properly. Take $B \in \mathscr{F}'$, which does not belong to $\mathscr{F}$. By (c), $I \setminus B \in \mathscr{F}$. Thus, both $B, I \setminus B \in \mathscr{F}'$, which is not possible because $\mathscr{F}'$ is a filter. This contradiction shows that (c) implies (a). □

Proposition 5.4.4. *Let $\mathscr{U}$ be an ultrafilter on a nonempty set I and $A, B \subset I$ are such that $A \cup B \in \mathscr{U}$. Then either $A \in \mathscr{U}$ or $B \in \mathscr{U}$.*

Proof. Suppose $A \cup B \in \mathscr{U}$, $A \notin \mathscr{U}$, and $B \notin \mathscr{U}$. By Proposition 5.4.3, $I \setminus A, I \setminus B \in \mathscr{U}$. Since $\mathscr{U}$ is closed under finite intersections, it follows that $\emptyset \in \mathscr{U}$. This contradiction proves the result. □

Exercise 5.4.5. If $\mathscr{U}$ is an ultrafilter on I, show that $\cap\,\mathscr{U}$ contains at most one point.

A filter $\mathscr{F}$ is called *free* if $\cap\mathscr{F} = \emptyset$.

Exercise 5.4.6. Show that a free filter does not contain a finite set.

Theorem 5.4.7. *Let $\mathscr{U}$ be an ultrafilter on I, $\varphi[\bar{x}]$ a formula of L, and $[\alpha_0], \cdots, [\alpha_{n-1}] \in M(\mathscr{U})$. Then*

$$M(\mathscr{U}) \models \varphi[i_{[\alpha_0]}, \cdots, i_{[\alpha_{n-1}]}] \Leftrightarrow \{i \in I : M_i \models \varphi[i_{\alpha_0(i)}, \cdots, i_{\alpha_{n-1}(i)}]\} \in \mathscr{U}. \qquad (*)$$

Proof. For atomic φ, $(*)$ follows from the definition. Suppose φ satisfies $(*)$ and ψ is the formula $\neg\varphi$. Take $[\alpha_0], \cdots, [\alpha_{n-1}] \in M$. Then

$$\begin{aligned} M(\mathscr{U}) \models \psi[i_{[\alpha_0]}, \cdots, i_{[\alpha_{n-1}]}] &\Leftrightarrow M(\mathscr{U}) \not\models \varphi[i_{[\alpha_0]}, \cdots, i_{[\alpha_{n-1}]}] \\ &\Leftrightarrow \{i \in I : M_i \models \varphi[i_{\alpha_0(i)}, \cdots, i_{\alpha_{n-1}(i)}]\} \notin \mathscr{U} \\ &\Leftrightarrow \{i \in I : M_i \models \psi[i_{\alpha_0(i)}, \cdots, i_{\alpha_{n-1}(i)}]\} \in \mathscr{U}. \end{aligned}$$

The second equivalence holds because φ satisfies $(*)$, whereas, by Proposition 5.4.3, the third equivalence holds because $\mathscr{U}$ is an ultrafilter. Using Proposition 5.4.4, similarly we show that if φ and ψ satisfy $(*)$, then so does $\varphi \vee \psi$.

Now assume that $(*)$ holds for $\psi[x_0, x_1, \cdots, x_n]$, $n \geq 0$, and all $(\alpha_0, \cdots, \alpha_n) \in M^{n+1}$. Consider $\varphi = \exists x_0 \psi$. Take any $\alpha_1, \cdots, \alpha_n \in M$ such that

$$M(\mathscr{U}) \models \varphi[i_{[\alpha_1]}, \cdots, i_{[\alpha_n]}].$$

Then there exists $[\alpha_0] \in M(\mathscr{U})$ such that

$$M(\mathscr{U}) \models \psi[i_{[\alpha_0]}, \cdots, i_{[\alpha_n]}].$$

By our hypothesis,

$$\{i \in I : M_i \models \psi[i_{\alpha_0(i)}, \cdots, i_{\alpha_n(i)}]\} \in \mathscr{U}.$$

This clearly implies that

$$\{i \in I : M_i \models \varphi[i_{\alpha_1(i)}, \cdots, i_{\alpha_n(i)}]\} \in \mathscr{U}.$$

To prove the converse, assume that the set

$$U = \{i \in I : M_i \models \varphi[i_{\alpha_1(i)}, \cdots, i_{\alpha_n(i)}]\} \in \mathscr{U}.$$

Thus, for each $i \in U$ there exists an $\alpha_0(i) \in M_i$ such that

$$M_i \models \psi[i_{\alpha_0(i)}, \cdots, i_{\alpha_n(i)}]\}.$$

Take any extension α_0 of $i \to \alpha_0(i)$, $i \in U$, to I. Then by our assumption,

$$M(\mathscr{U}) \models \psi[i_{[\alpha_0]}, \cdots, i_{[\alpha_n]}].$$

Thus,

$$M(\mathscr{U}) \models \varphi[i_{[\alpha_1]}, \cdots, i_{[\alpha_n]}].$$

The result is thus seen by induction on the rank of φ. □

Exercise 5.4.8. Let $\mathscr{U}$ be an ultrafilter on I with $\cap\mathscr{U} = \{j\}$. Suppose $\{M_i : i \in I\}$ is a family of structures of a language L. Show that $M(\mathscr{U})$ is isomorphic to M_j.

Exercise 5.4.9. Let M be a structure for a language L and $\mathscr{U}$ an ultrafilter on I. Define the inclusion map $j : M \to M^{\mathscr{U}}$ by

$$j(x) = [c_x], x \in M,$$

where $c_x : I \to M$ is the constant map $c_x(i) = x$, $i \in I$. Show that j is an elementary embedding.

Using the ultraproduct of models we now present another proof of the compactness theorem. Thus, assume that T is a finitely satisfiable set of sentences of a language L. For each finite $i \subset T$, let M_i be a model of i. Set $I = \{i : i \subset T \text{ finite}\}$. For each sentence φ, set

$$B_\varphi = \{i \in I : \varphi \in i\}.$$

Let $\varphi_1, \cdots, \varphi_n \in T$. $\{\varphi_1, \cdots, \varphi_n\} \in \cap_{i=1}^n B_{\varphi_i}$. Thus, the family $\{B_\varphi : \varphi \in T\}$ has the finite intersection property. Hence, by Proposition 5.4.2, it is contained in an ultrafilter $\mathscr{U}$.

We claim that $M(\mathscr{U}) \models T$. Let $\varphi \in T$. Then for every $i \in B_\varphi$, $M_i \models \varphi$. Hence, by Theorem 5.4.7, $M(\mathscr{U}) \models \varphi$. This completes the proof of the compactness theorem.

5.5 Some Applications in Algebra

We have already observed the following (Exercise 2.5.2 and Proposition 2.5.5).

Example 5.5.1. 1. The theory *DLO* of order-dense linearly ordered sets with no first and no last element is $\aleph_0$-categorical. Also, all its models are infinite.
2. The theory of divisible torsion-free abelian groups *DAG* is κ-categorical for all uncountable κ. Further, all its models are infinite.

Let $\mathbb{K}$ be a field of characteristic 0. Then the smallest subfield of $\mathbb{K}$ is isomorphic to the field $\mathbb{Q}$ of rational numbers. Similarly, if $\mathbb{K}$ is a field of characteristic p, with p a prime, then the field $F_p = \mathbb{Z}/p\mathbb{Z}$ is isomorphic to the smallest subfield of $\mathbb{K}$. Given a field $\mathbb{K}$, a field κ such that there is an embedding $\alpha : \kappa \to \mathbb{K}$ with the property that for every field κ' and every embedding $\beta : \kappa' \to \mathbb{K}$, there is a unique embedding $\gamma : \kappa \to \kappa'$ such that $\beta \circ \gamma = \alpha$ is called a *prime field* of $\mathbb{K}$. Any two prime fields of a field are easily seen to be isomorphic. Thus, prime fields of a field are unique up to isomorphism.

Let $\mathbb{K}$ be a field and κ its prime field. A subset $B \subset \mathbb{K}$ is called *polynomially independent* if whenever

$$\sum a_{\bar{i}} x_0^{i_0} \cdots x_n^{i_n} = 0,$$

$n \in \mathbb{N}$, $\bar{i} = (i_0, \cdots, i_n)$, with $i_0, \cdots, i_n$ nonnegative integers, $a_{\bar{i}} \in \kappa$, $x_0, \cdots x_n \in B$, each $a_i = 0$. It should be noted that an algebraically closed field may not have a nonempty polynomially independent subset. For instance, the algebraic closure F_p^{alg} of F_p, with p a prime, has no polynomially independent subset.

We recall a standard result from algebra.

Proposition 5.5.2. *Let p be a prime and F_p denote the field of integers modulo p. Then*

$$F_p^{alg} = \cup_{n \geq 1} F_{p^n},$$

where F_{p^n} denotes the field with p^n many elements. (See [10].) In particular, every subfield of F_p^{alg} generated by finitely many elements is finite.

A maximal polynomially independent subset of $\mathbb{K}$ is called a *transcendence basis* of $\mathbb{K}$. By Zorn's lemma it is easily seen that every field $\mathbb{K}$ has a transcendence basis. Further, any two transcendence bases are of the same cardinality, which we call the *transcendence degree* of $\mathbb{K}$. If B is a nonempty transcendence basis of $\mathbb{K}$ and κ its prime field, then every $x \in \mathbb{K}$ has a unique representation

$$a = \sum a_{\bar{i}} x_0^{i_0} \cdots x_n^{i_n},$$

where $n \in \mathbb{N}$, $\bar{i} = (i_0, \cdots, i_n)$, $i_0, \cdots, i_n$ are nonnegative integers, $a_{\bar{i}} \in \kappa$, and $x_0, \cdots x_n \in B$.

If $\mathbb{K}$ has no nonempty polynomially independent subset, then its transcendence degree is 0. We have the following result. Its easy proof is omitted.

Proposition 5.5.3. *If $\mathbb{K}$ is countable, algebraically closed, of characteristic $p \neq 0$, and of transcendence degree 0, then it is isomorphic to F_p^{alg}, where F_p denotes the field of integers modulo p.*

Now assume that $\mathbb{K}_1$ and $\mathbb{K}_2$ are two algebraically closed fields of the same characteristic with B_1 and B_2 respectively their transcendence bases of the same positive cardinality with $B_1 \neq \emptyset \neq B_2$. Then every bijection $\alpha : B_1 \to B_2$ can be extended uniquely to an isomorphism $\beta : \mathbb{K}_1 \to \mathbb{K}_2$. (See [10], p. 355.) Thus, we have the following proposition.

Proposition 5.5.4. *Two algebraically closed fields of the same characteristic and same transcendence degree are isomorphic.*

A simple cardinality argument now easily gives us the following result.

Proposition 5.5.5. *The theory $ACF(p)$, with $p = 0$ or a prime, is κ-categorical for every uncountable κ. Further, every model of $ACF(p)$ is infinite.*

The following result follows from Vaught's theorem 5.3.5.

Proposition 5.5.6. *The theories DLO, DAG, and $ACF(p)$, with $p = 0$ or a prime, are complete.*

By Proposition 5.1.1 we now have the following result.

Corollary 5.5.7. *1. The model $\mathbb{Q} \models DLO$ is elementarily equivalent to every model $M \models DLO$.*
2. The model $\mathbb{Q} \models DAG$ is elementarily equivalent to every model $M \models DAG$.
3. The model $\mathbb{C} \models ACF(0)$ is elementarily equivalent to every model $M \models ACF(0)$.
4. The model $F_p^{alg} \models ACF(p)$, p a prime, is elementarily equivalent to every model $M \models ACF(p)$.

Theorem 5.5.8. *Let φ be a sentence of the language of the theory of fields. The following statements are equivalent:*

(i) *φ is true in the field $\mathbb{C}$ of complex numbers.*
(ii) *φ is true in all algebraically closed fields of characteristic 0.*
(iii) *φ is true in some algebraically closed field of characteristic 0.*
(iv) *There is an m such that for all prime $p > m$, φ is true in some algebraically closed field of characteristic p.*
(v) *There is an m such that for all prime $p > m$, φ is true in all algebraically closed fields of characteristic p.*

Proof. By Proposition 5.1.1, (i) implies (ii) and also (iii) implies (ii). Now assume (ii). Then by the completeness theorem, φ is a theorem of $ACF(0)$. Since a proof of φ contains only finitely many nonlogical axioms, there is an m such that for all primes $p > m$, φ is a theorem of $ACF(p)$. Hence, (iv) is true by the validity theorem.

Statement (iv) implies (v) because each $ACF(p)$ is complete. We now show that (v) implies (ii). Let $ACF(0) \not\models \varphi$, i.e., φ is not a theorem of $ACF(0)$. Since $ACF(0)$ is complete, it follows that $\neg\varphi$ is a theorem and so valid in $ACF(0)$. Since (ii) implies (v) (Proposition 5.1.3), it follows that there is an m' such that for all primes $p > m'$, $\neg\varphi$ is valid in all algebraic closed fields of characteristic p. Thus, (v) is false. □

We close this section by giving an application in algebra.

Proposition 5.5.9. *Let $p > 1$ be prime and*

$$f_1(X_1,\ldots,X_n),\ldots,f_n(X_1,\ldots,X_n) \in (F_p^{alg})^n[X_1,\ldots,X_n].$$

If the map

$$f = (f_1, \ldots, f_n) : (F_p^{alg})^n \to (F_p^{alg})^n$$

is injective, then it is surjective.

Proof. Suppose f is not surjective. Let $\{a_1, \ldots, a_k\}$ be the set of all coefficients of $f_1, \ldots, f_n$. Let $b_1, \ldots, b_n \in F_p^{alg}$ be such that $(b_1, \ldots, b_n)$ is not in the range of f. Let $\mathbb{K}$ be the subfield of F_p^{alg} generated by $\{a_1, \ldots, a_k, b_1, \ldots, b_n\}$. By Proposition 5.5.2, $\mathbb{K}$ is finite. But now we have an injective map $f : \mathbb{K}^n \to \mathbb{K}^n$ that is not surjective. This is impossible since $\mathbb{K}^n$ is a finite set. □

Theorem 5.5.10 (Ax). *Let $\mathbb{K}$ be an algebraically closed field and*

$$f_1(X_1, \ldots, X_n), \ldots, f_n(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n].$$

If the map

$$f = (f_1, \ldots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$$

is injective, it is surjective.

Proof. Let each f_i be of degree at most d. It is not hard to see that there is a sentence φ of the language of fields saying that if $f_1, \ldots, f_n$ are polynomials of degree at most d and if the map $f = (f_1, \ldots, f_n)$ is injective, then it is surjective.

Let $\mathbb{K}$ be of characteristic p for some prime $p > 1$. Then φ is valid in F_p^{alg} by Proposition 5.5.9. Thus, φ is valid in $\mathbb{K}$ by Corollary 5.5.7.

Now let $\mathbb{K}$ be of characteristic 0. In this case the result follows from Proposition 5.5.9 and Theorem 5.5.8. □

5.6 Extensions of Partial Elementary Maps

In this section we make some general observations on types. The importance of these will become clear as we go along.

Let M be a structure of a language L. An *n-type* $p[x_0, \cdots x_{n-1}] = p[\bar{x}] = p$ is a set of formulas $\varphi[\bar{x}]$ of L such that $p \cup Th_M$ is satisfiable, i.e., there is a model $N \models Th_M$ and an $\bar{a} \in N$ such that $N \models \varphi[i_{\bar{a}}]$ for every $\varphi \in p$. As we saw earlier, the compactness theorem implies the following proposition.

Proposition 5.6.1. *A set of formulas p with free variables among $\bar{x}$ is an n-type if and only if $p \cup Th_M$ is finitely satisfiable.*

Example 5.6.2. Consider $(\mathbb{N}, 0, 1, <)$ as a structure of the language with 0, 1, and $<$ as nonlogical symbols and

$$p[x] = \{x > \underline{n} : n \in \mathbb{N}\},$$

where $\underline{n}$ is the term $\underbrace{1+\cdots+1}_{n-\text{times}}$. Clearly, $\mathbb{N}$ models every finite subset of $p \cup Th_{\mathbb{N}}$. Hence p is a 1-type.

Example 5.6.3. Let $\overline{a} \in M^n$. Then $tp^M(\overline{a}) = \{\varphi[\overline{x}] : M \models \varphi[i_{\overline{a}}]\}$ is an n-type.

Let p be an n-type. We say that an $\overline{a} \in M^n$ *realizes* p in M if $M \models \varphi[i_{\overline{a}}]$ for every $\varphi \in p$. If no such $\overline{a}$ exists in M^n, then we say that M *omits* p. In the preceding example, $\mathbb{N}$ omits p.

Proposition 5.6.4. *Let M be a structure of L and p an n-type. Then there is an elementary extension N of M that realizes p.*

Proof. Consider $\Gamma = p \cup Diag_{el}(M)$ and $\Delta \subset \Gamma$ finite. Let

$$\varphi[\overline{x}] \wedge \psi[i_{\overline{a}}]$$

denote the conjunction of a finite set of formulas in Δ, where $\overline{a} \in M$ and $M \models \psi[i_{\overline{a}}]$. In particular, $\exists \overline{x} \psi[\overline{x}] \in Th_M$. Since p is an n-type, there is a structure N_0 and $\overline{c} \in N_0$ such that

$$N_0 \models \varphi[i_{\overline{c}}] \wedge \exists \overline{x} \psi[\overline{x}].$$

Thus, Γ is finitely satisfiable. Hence, by the compactness theorem, it is satisfiable. Thus, we get $N \models Diag_{el}(M)$ (implying that N is an elementary extension of M) and a $\overline{c} \in N$ such that $N \models \varphi[i_{\overline{c}}]$ for all $\varphi \in p$. □

Remark 5.6.5. If L and M are countable, then N can be chosen to be countable.

We call an n-type p a *complete n-type* if for every formula $\varphi[\overline{x}]$ either φ or $\neg\varphi$ belongs to p. The set of all complete n-types will be denoted by $S_n^M(\emptyset)$. Note that for every $\overline{a} \in M$, $tp^M(\overline{a})$ is a complete n-type. Not only this, if N is an elementary extension of M, $\overline{a} \in N$, then $tp^M(\overline{a})$ consisting of all formulas $\varphi[\overline{x}]$ of L with $N \models \varphi[i_{\overline{a}}]$ is a complete n-type.

Exercise 5.6.6. Let $p[\overline{x}]$ and $q[\overline{x}]$ be complete n-types and $\varphi[\overline{x}]$ and $\psi[\overline{x}]$ formulas of L. Show the following:

1. Exactly one of φ and $\neg\varphi$ belongs to p.
2. If $p \subset q$, then $p = q$.
3. $\varphi \wedge \psi \in p$ if and only if both φ and ψ belong to p.
4. $\varphi \vee \psi \in p$ if and only if at least one of φ and ψ belong to p.

We will now characterize when for two $\overline{a}, \overline{b} \in M^k$, $tp^M(\overline{a}) = tp^M(\overline{b})$, i.e., when $\overline{a}$ and $\overline{b}$ satisfy the same properties. We need a few auxiliary results.

Proposition 5.6.7. *Let M, N be structures for L, $A \subset M$, $f : A \to N$ a partial elementary map, and $a \in M$. Then there is an elementary extension N' of N and a partial elementary map $g : A \cup \{a\} \to N'$ that extends f.*

Proof. Suppose $\overline{a} \in A$ and $\varphi[x,\overline{x}]$ is such that $M \models \varphi[i_a, i_{\overline{a}}]\}$. Then $M \models \exists x \varphi[x, i_{\overline{a}}]$. Since f is partial elementary, $N \models \exists x \varphi[x, i_{f(\overline{a})}]$. From this it is entirely routine to show that every finite subset of

$$Diag_{el}(N) \cup \{\varphi[x, i_{f(\overline{a})}] : \overline{a} \in A \wedge M \models \varphi[i_a, i_{\overline{a}}]\}$$

is satisfiable in N. Hence, by the compactness theorem, it is satisfiable. Therefore, there is an elementary extension N' of N and a $b \in N'$ such that $N' \models \varphi[i_b, i_{f(\overline{a})}]$ whenever $M \models \varphi[i_a, i_{\overline{a}}]$. We extend f to $A \cup \{a\}$ by setting $f(a) = b$. This works. □

Remark 5.6.8. If L, A, and N are countable, then N' can be chosen to be countable.

Using transfinite induction, we also have the following result.

Proposition 5.6.9. *Let M and N_0 be structures of L and $A \subset M$, and let $f_0 : A \to N_0$ be partial elementary. Then there exists an elementary extension N_∞ of N_0 such that f_0 can be extended to an elementary embedding $f_\infty : M \to N_\infty$.*

Proof. Fix an enumeration $\{a_\alpha : \alpha < |M|\}$ of M. We shall proceed by induction and for each $\alpha < |M|$ will get a structure N_α of L and a map $f_\alpha : A \cup \{a_\beta : \beta < \alpha\} \to N_\alpha$ satisfying the following conditions.

1. Each f_α is partial elementary.
2. $N_{\alpha+1}$ is an elementary extension of N_α, $N_\alpha = \cup_{\beta<\alpha} N_\beta$ if α limit ordinal.
3. $f_{\alpha+1}$ extends f_α and $f_\alpha = \cup_{\beta<\alpha} f_\beta$ if α limit.

Our hypothesis is just the initial case. Suppose f_α, N_α satisfying the desired properties have been defined. If $a_\alpha \in domain(f_\alpha)$, then we set $N_{\alpha+1} = N_\alpha$ and $f_{\alpha+1} = f_\alpha$. Otherwise, by Proposition 5.6.7, there is an elementary extension $N_{\alpha+1}$ of N_α and a partial elementary map

$$f_{\alpha+1} : A \cup \{a_\beta : \beta \leq \alpha\} \to N_{\alpha+1}$$

extending f_α. Now take $N_\infty = \cup_{\alpha<|M|} N_\alpha$ and $f_\infty = \cup_\alpha f_\alpha$. □

Remark 5.6.10. Since every consistent countable, theory has a countable model, if L, M, and N are countable, then we can choose N_∞ countable.

Theorem 5.6.11. *Let M be a countable structure of a countable language L and $\overline{a}, \overline{b} \in M^n$. Then $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if there is a countable elementary extension N of M and an automorphism $\alpha : N \to N$ such that $\alpha(\overline{a}) = \overline{b}$.*

Proof. The *if* part of the result follows because α is an automorphism such that $\alpha(\overline{a}) = \overline{b}$. Thus, we need to prove the *only if* part only.

Assume that $\overline{a}, \overline{b} \in M^n$ are such that $tp^M(\overline{a}) = tp^M(\overline{b})$. Using Remark 5.6.10, for each k we shall define countable structures M_k, N_k and elementary embeddings $\alpha_k : M_k \to N_k$ satisfying the following conditions:

1. M_0 is an elementary extension of M.
2. $\alpha_0(\overline{a}) = \overline{b}$.

3. For each k, N_k is an elementary extension of M_k and M_{k+1} is an elementary extension of N_k.
4. For each k, α_{k+1} extends α_k.

Since $tp^M(\overline{a}) = tp^M(\overline{b})$, the map $\overline{b} \to \overline{a}$ is partial elementary. By Remark 5.6.10, there is a countable elementary extension M_0 of M and an elementary embedding $\beta_0 : M \to M_0$ such that $\beta_0(\overline{b}) = \overline{a}$. Since β_0 is elementary, it is one-to-one. Now consider $A_0 = range(\beta_0) \subset M_0$ and $\beta_0^{-1} : A_0 \to M$. Clearly, it is partial elementary. Regard M as an elementary substructure of M_0 and $\beta_0^{-1} : A_0 \to M_0$. By the same argument, there is a countable elementary extension N_0 of M_0 and an elementary extension $\alpha_0 : M_0 \to N_0$ of β_0^{-1}.

Now set $A_1 = \alpha_0(M_0) \subset N_0$ and $\beta_1 = (\alpha_0)^{-1}$. Then $\beta_1 : A_1 \to N_0$ is partial elementary. As before, there is a countable elementary extension M_1 of N_0 and an elementary embedding $\beta_1' : N_0 \to M_1$ of β_1. Now consider $B_1 = range(\beta_0') \subset M_1$ and $\beta_0'^{-1} : B_1 \to N_0$. As before, there is an elementary extension N_1 of M_1 and an elementary embedding $\alpha_1 : M_1 \to N_1$ extending $\beta_0'^{-1}$.

Proceeding by induction, we similarly define the M_k, N_k, and α_k satisfying the foregoing conditions. Now take $N = \cup M_k = \cup N_k$ and $\alpha = \cup_k \alpha_k$. This works. □

The same argument also gives us the following result.

Theorem 5.6.12. *Let M be a structure of a language L and $\overline{a}, \overline{b} \in M^n$. Then $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if there is an elementary extension N of M and an automorphism $\alpha : N \to N$ such that $\alpha(\overline{a}) = \overline{b}$.*

5.7 Elimination of Quantifiers

In Chap. 2, we introduced the notion of definability. But it is very useful to know when definable sets are defined by open formulas. This question has led to many interesting and deep applications in mathematics. This section is devoted to this topic.

Let M be a structure of a language L. We say that M admits *elimination of quantifiers* if for every formula $\varphi[\overline{x}]$ of L there is an open formula $\psi[\overline{x}]$ such that

$$M \models \forall \overline{x}(\varphi[\overline{x}] \leftrightarrow \psi[\overline{x}]).$$

Let T be a theory with language L with a constant symbol c. If L has no constant symbol, then by the theorem on constants, without any loss of generality, we can introduce a constant symbol c. We say that T admits elimination of quantifiers if for every formula $\varphi[\overline{x}]$ of L there is an open formula $\psi[\overline{x}]$ such that

$$T \vdash \forall \overline{x}(\varphi[\overline{x}] \leftrightarrow \psi[\overline{x}]).$$

Example 5.7.1. Let φ be a sentence decidable in T; then $T \vdash \varphi \leftrightarrow c = c$ if $T \vdash \varphi$, else $T \vdash \varphi \leftrightarrow c \neq c$.

Proposition 5.7.2. *Assume that for every open formula $\varphi[x,\overline{y}]$, there is an open formula $\psi[\overline{y}]$ such that*

$$T \vdash \forall \overline{y}((\exists x \varphi[x,\overline{y}]) \leftrightarrow \psi[\overline{y}]).$$

Then T admits elimination of quantifiers.

Proof. By induction on the rank of formulas, we prove that for every formula $\varphi[\overline{x}]$ of L there is an open formula $\psi[\overline{x}]$ such that

$$T \vdash \forall \overline{x}(\varphi[\overline{x}] \leftrightarrow \psi[\overline{x}]). \qquad (*)$$

$(*)$ is clearly true for open φ. It is easy to prove that if $(*)$ is true for φ and ψ, then it is true for $\neg\varphi$ and $\varphi \vee \psi$. (Use either closure and tautology theorems or the completeness theorem.)

To complete the proof, assume that $(*)$ holds for $\varphi[x,\overline{y}]$ and $\psi[\overline{y}]$ is the formula $\exists x \varphi[x,\overline{y}]$. Get an open formula $\eta[x,\overline{y}]$ such that

$$T \vdash \forall x \forall \overline{y}(\varphi[x,\overline{y}] \leftrightarrow \eta[x,\overline{y}]).$$

This implies that

$$T \vdash \forall \overline{y}((\exists x \varphi[x,\overline{y}]) \leftrightarrow \exists x \eta[x,\overline{y}]).$$

By our hypothesis, there is an open formula $\psi[\overline{y}]$ such that

$$T \vdash \forall \overline{y}((\exists x \eta[x,\overline{y}]) \leftrightarrow \psi[\overline{y}]).$$

Now it is clear that

$$T \vdash \forall \overline{y}((\exists x \varphi[x,\overline{y}]) \leftrightarrow \psi[\overline{y}]).$$

Our proof is complete. □

Theorem 5.7.3. *Let T be a theory with a constant symbol c and $\varphi[\overline{x}]$ a formula of T. The following are equivalent:*

(1) *There is an open formula $\psi[\overline{x}]$ such that*

$$T \vdash \forall \overline{x}(\varphi[\overline{x}] \leftrightarrow \psi[\overline{x}]). \qquad (*)$$

(2) *For any two models $M,N \models T$, for any common substructure A of M, N, and for any $\overline{a} \in A$,*

$$M \models \varphi[i_{\overline{a}}] \Leftrightarrow N \models \varphi[i_{\overline{a}}].$$

Proof. We prove that (1) implies (2). Take M, N, A, and $\overline{a}$ as in (2). By (1), there is an open formula $\psi[\overline{x}]$ such that $T \vdash \forall \overline{x}(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x}))$. Thus,

$$M \Leftrightarrow \varphi(i_{\overline{a}}) \Leftrightarrow M \models \psi[i_{\overline{a}}]$$

and

$$N \Leftrightarrow \varphi(i_{\overline{a}}) \Leftrightarrow N \models \psi[i_{\overline{a}}].$$

But because A is a common substructure of M and N, since $\overline{a} \in A$ and ψ is open,

$$M \models \psi(i_{\overline{a}}) \Leftrightarrow A \models \psi(i_{\overline{a}}) \Leftrightarrow N \models \psi(i_{\overline{a}}).$$

Hence,

$$M \models \varphi(i_{\overline{a}}) \Leftrightarrow N \models \varphi(i_{\overline{a}}).$$

We now proceed to prove that (2) implies (1). Thus, assume that $\varphi[\overline{x}]$ satisfies (2). When a closed formula φ satisfies (2), φ is either true in all models or in none. Now note that $T \vdash \varphi \leftrightarrow c = c$ if $T \vdash \varphi$. Otherwise, $T \vdash \neg\varphi$ when $T \vdash \varphi \leftrightarrow c \neq c$. The same argument works when $\varphi[\overline{x}]$ is not closed but decidable in T.

It remains to prove the result if both $T[\varphi[\overline{x}]]$ and $T[\neg\varphi[\overline{x}]]$ are satisfiable. Introduce new constants $\overline{c}$ to the language and consider

$$\Gamma = \{\psi[\overline{c}] : T \vdash \varphi[\overline{x}] \rightarrow \psi[\overline{x}], \psi \text{ open}\}.$$

We first see that it is sufficient to prove that

$$T[\Gamma] \vdash \varphi[\overline{c}]. \qquad (*)$$

Then by the deduction theorem (Corollary 4.2.21), there exist $\psi_1[\overline{c}], \cdots, \psi_n[\overline{c}] \in \Gamma$ such that

$$T \vdash \wedge_{i=1}^{n} \psi_i[\overline{c}] \rightarrow \varphi[\overline{c}].$$

By the theorem on constants, it follows that

$$T \vdash \forall\overline{x}(\varphi[\overline{x}] \leftrightarrow \wedge_{i=1}^{n} \psi_i[\overline{x}])$$

and $\wedge_{i=1}^{n} \psi_i[\overline{x}]$ is open.

We prove $(*)$ by contradiction. Thus, assume that

$$T[\Gamma] \nvdash \varphi[\overline{c}].$$

Let

$$M \models T[\Gamma] \cup \{\neg\varphi[\overline{c}]\}.$$

Let A be the substructure of M generated by $\overline{c_M}$. Now consider

$$\Delta = T \cup Diag(A) \cup \{\varphi[\overline{c}]\}.$$

We claim that Δ has a model. If not, there exists $\psi_1[\overline{c}], \cdots, \psi_n[\overline{c}] \in Diag(A)$ such that

$$T \vdash \wedge_{i=1}^{n} \psi_i[\overline{c}] \rightarrow \neg\varphi[\overline{c}].$$

By the theorem on constants,

$$T \vdash \wedge_{i=1}^{n} \psi_i[\overline{x}] \to \neg\varphi[\overline{x}].$$

Set $\psi[\overline{x}] = \neg \wedge_{i=1}^{n} \psi_i[\overline{x}]$. Note that ψ is open. By the tautology theorem,

$$T \vdash \varphi[\overline{x}] \to \psi[\overline{x}].$$

Thus, $\psi[\overline{c}] \in \Gamma$ and $A \models \psi[\overline{c}]$, contradicting that $\psi_1[\overline{c}], \cdots, \psi_n[\overline{c}] \in Diag(A)$.

Now take a model $N \models \Delta$. By Proposition 2.4.7, A is a substructure of N. But $M \models \neg\varphi[\overline{c}]$ and $N \models \varphi[\overline{c}]$. This contradicts (2) and proves $(*)$. □

Since every open formula is equivalent to an open formula in disjunctive normal form (*DNF*) (Exercise 4.2.4), using Proposition 5.7.2 and Theorem 5.7.3, one easily sees the following very useful result.

Corollary 5.7.4. *Let T be a theory with a constant. The following are equivalent:*

(1) *T admits elimination of quantifiers.*
(2) *For every conjunction of literals $\varphi[x,\overline{y}]$, for any two models $M,N \models T$, for every common substructure A of M, N, and for every $\overline{a} \in A$, if there is a $b \in M$ such that $M \models \varphi[i_b, i_{\overline{a}}]$, then there is a $c \in N$ such that $N \models \varphi[i_c, i_{\overline{a}}]$.*

Example 5.7.5. The theory *DLO* admits elimination of quantifiers.

Proof. Let $\varphi[x,\overline{y}]$ be a conjunction of literals. For instance, suppose

$$\varphi[x,\overline{y}] = y_1 < \cdots < y_{i-1} < x < y_i < \cdots < y_n.$$

Suppose $M,N \models DLO$, A is a common substructure of M,N, $\overline{a} \in A$ and there is a $b \in M$ satisfying

$$a_1 < \cdots < a_{i-1} < b < a_i < \cdots < a_n.$$

This, in particular, implies that

$$a_1 < \cdots < a_{i-1} < a_i < \cdots < a_n.$$

Since $N \models DLO$, there is a $c \in N$ such that

$$a_1 < \cdots < a_{i-1} < c < a_i < \cdots < a_n.$$

Cases where $\varphi[x,\overline{x}]$ is "$x < y_1 < \cdots < y_n$" or "$y_1 < \cdots < y_n < x$" are dealt with similarly because N has no first and no last elements. □

Example 5.7.6. The theory *DAG* of torsion-free divisible abelian groups admits elimination of quantifiers.

Proof. We take $G_1, G_2 \models DAG$, a common subgroup $H \subset G_1, G_2$. Let $\varphi[x,\overline{y}]$ be a conjunction of literals. Suppose $\overline{a} \in H$. Replacing H by its divisible hull considered

as a common subgroup of both G_1 and G_2, we further assume that H too is divisible. Now $\varphi[x,\overline{y}]$, being a conjunction of literals, can be assumed to be of the form

$$\wedge_{i=0}^{k-1}\sum_{j=1}^{m_i}(n_{ij}y_j+n_ix=0)\wedge\wedge_{p=0}^{l-1}\sum_{q=1}^{r_p}(n'_{pq}y_j+n'_px\neq 0)). \qquad (*)$$

Assume that there is a $b\in G_1$ such that

$$G_1\models\varphi[i_b,i_{\overline{a}}].$$

We need to show that there is a $c\in G_2$ such that

$$G_2\models\varphi[i_c,i_{\overline{a}}].$$

Since H is a substructure of G_2, it is sufficient to show that there is such a c in H.

If any $n_i\neq 0$, as H is divisible,

$$b=-\frac{\sum_{j=1}^{m_i}n_{ij}a_j}{n_i}\in H,$$

and we are done. Thus, assume that all $n_i=0$. Then b disappears from the equalities appearing in $(*)$. Since H is infinite, we can certainly find a $c\in H$ satisfying all inequalities in $(*)$. □

Example 5.7.7. The theory *ODAG* of ordered divisible abelian groups admits elimination of quantifiers.

Proof. As in the previous case, we take ordered divisible abelian groups, a common subgroup H, a conjunction of literals $\varphi[x,\overline{y}]$, and an $\overline{a}\in H$. Assume that there is a $b\in G_1$ such that $G_1\models\varphi[i_b,i_{\overline{a}}]$. Again, as in the last example, it is sufficient to show that if H' is the ordered divisible hull of H, then there is a $c\in H'$ such that $H'\models\varphi[i_c,i_{\overline{a}}]$. To show this, note that we can assume that $\varphi[x,\overline{y}]$ is of the form

$$\wedge_{i=0}^{k-1}\sum_{j=1}^{m_i}(n_{ij}y_j+n_ix=0)\wedge\wedge_{p=0}^{l-1}\Big(\sum_{j=1}^{r_p}n'_{pj}y_j<n'_px\Big).$$

Observe that H' is order-dense. Arguing as in the last example, we get a required $c\in H'$. □

Example 5.7.8. The theory *ACF* of algebraically closed fields admits elimination of quantifiers.

Proof. Note that a substructure of a field is an integral domain. Also, recall that if D is an integral domain, then its quotient field embeds into every field in which D is embedded. Therefore, as in the last two cases, we only need to show that whenever $\mathbb{F}\subset\mathbb{K}$ are algebraically closed fields, $\varphi[x,\overline{y}]$ a conjunction of literals, and $\overline{a}\in\mathbb{F}$, if

there is a $b \in \mathbb{K}$ such that $\mathbb{K} \models \varphi[i_b, i_{\overline{a}}]$, then there is a $c \in \mathbb{F}$ such that $\mathbb{F} \models \varphi[i_c, i_{\overline{a}}]$. Now note that we can take $\varphi[x, \overline{a}]$ in the form

$$\wedge_{i=0}^{k-1}(P_i(x) = 0) \wedge \wedge_{j=0}^{l-1}(Q_j(x) \neq 0),$$

and $P_i[X]$ and $Q_j[X]$ are polynomials over the smallest subfield of $\mathbb{F}$ generated by $\overline{a}$. If $k \geq 1$, then $b \in \mathbb{F}$ because it is algebraically closed. Otherwise, since $\mathbb{F}$ is infinite, it certainly has a c that is not a root of any $Q_j[X]$, which works for us. □

The similarity to the last three proofs suggests that there is a more general result showing the elimination of quantifiers. This is indeed the case. For a theory T, let $T_\forall$ denote the set of all universal formulas $\forall \overline{x} \varphi[\overline{x}]$, with φ open, that are theorems of T. Having introduced subtraction in the language of groups and fields, note the following:

Example 5.7.9. 1. If T is the theory *DAG*, then models of $T_\forall$ are precisely torsion-free abelian groups.
2. If T is the theory *ODAG*, then models of $T_\forall$ are precisely ordered abelian groups.
3. If T is the theory of fields, models of $T_\forall$ are precisely integral domains.

Exercise 5.7.10. Show that every algebraically closed field is homogeneous.

Let T be a theory. We say that T has *algebraically prime models* if for every model $M \models T_\forall$ there is a model $N \models T$ and an embedding $\alpha : M \to N$ such that for every model $N' \models T$ and for every embedding $\beta : M \to N'$, there is an embedding $\gamma : N \to N'$ such that $\gamma \circ \alpha = \beta$.

The following result is easily seen by the arguments contained in the last three proofs.

Theorem 5.7.11. *Let T be a theory such that*

(a) The theory T has algebraically prime models,
(b) For any two models $M, N \models T$ with M a substructure of N, for every conjunction of literals $\varphi[x, \overline{y}]$ and for every $\overline{a} \in M$,

$$N \models \exists x \varphi[x, \overline{a}] \Rightarrow M \models \exists x \varphi[x, \overline{a}].$$

Then T admits elimination of quantifiers.

5.8 Applications of Elimination of Quantifiers

A theory T is called *model-complete* if $M, N \models T$ and M is a substructure of N imply that M is an elementary substructure of N.

Theorem 5.8.1. *If T admits elimination of quantifiers, then it is model-complete.*

Proof. Let $M, N \models T$ and M be a substructure of N. We need to show that the inclusion map $i : M \hookrightarrow N$ is an elementary embedding. Take a formula $\varphi[\overline{x}]$ and an $\overline{a} \in M$. By elimination of quantifiers, there is an open formula $\psi[\overline{x}]$ such that

$$T \vdash \forall \overline{x}(\varphi[\overline{x}] \leftrightarrow \psi[\overline{x}]).$$

Thus,

$$M \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \psi[i_{\overline{a}}],$$
$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow N \models \psi[i_{\overline{a}}],$$

and since M is a substructure of N,

$$M \models \psi[i_{\overline{a}}] \Leftrightarrow N \models \psi[i_{\overline{a}}].$$

The result follows now. □

Corollary 5.8.2. *The theories DLO, DAG, ODAG, and ACF are model-complete.*

Remark 5.8.3. We now see that there does exist a proper elementary extension of a structure in some cases. This, in particular, shows that an elementary embedding need not be surjective.

Exercise 5.8.4. Let T be model-complete and admit algebraically prime models. Show that T admits elimination of quantifiers.

Model completeness also gives another method of proving the completeness of theories.

Theorem 5.8.5. *Let T be model-complete and have a model that embeds into all other models. Then T is complete.*

Proof. Let $M \models T$ embed into every model of T. Since T is model-complete, M has an elementary embedding into all models of T, implying that every model of T is elementarily equivalent to M. By Proposition 5.1.1, it follows that T is complete. □

Exercise 5.8.6. Let T be the theory of nontrivial, dense linearly ordered sets. Show that there are nonisomorphic models of T that embed into all models of T.

Exercise 5.8.7. If T is a countable, consistent theory and $M \models T$ embeds into all models of T, then show that M is countable.

We have seen that the theories *DLO*, *DAG*, *ODAG*, and $ACF(p)$, with $p = 0$ or a prime, all satisfy the hypothesis of the last theorem. Thus, Theorem 5.8.5, apart from proving that *DLO*, *DAG*, and $ACF(p)$, with $p = 0$ or a prime, are complete, also proves the following theorem.

Theorem 5.8.8. *The theory ODAG of ordered divisible abelian groups is complete.*

Since $(\mathbb{Q}, +, <)$ is a model of *ODAG*, we get the following corollary.

Corollary 5.8.9. *The model $(\mathbb{Q},+,<)$ of ODAG of rational numbers is elementarily equivalent to all models of ODAG.*

Elimination of quantifiers also gives us interesting facts about definable subsets of models.

Theorem 5.8.10. *Let T admit elimination of quantifiers and $M \models T$. Then $D \subset M^n$ is definable if and only if D is defined by an open formula.*

Exercise 2.8.14 now gives us the following theorem.

Theorem 5.8.11. *Let $\mathbb{K}$ be an algebraically closed field. Then every definable $D \subset \mathbb{K}^n$ is constructible.*

Theorem 5.8.12. *Let G be a divisible abelian group. Then $D \subset G^n$ is definable if and only if it belongs to the smallest algebra of subsets of G^n containing hyperplanes of the form*

$$\{\overline{g} \in G^n : \sum p_i g_i + \sum q_j h_j = 0\},$$

$\overline{p},\overline{q} \in \mathbb{Z}$ and $\overline{h} \in G$. In particular, $D \subset G$ is definable if and only if either D or its complement is finite, i.e., cofinite.

Here is an important definition. A structure M for a language L is called *strongly minimal* if every definable subset of M is either finite or cofinite.

Example 5.8.13. The field of real numbers $\mathbb{R}$ is not strongly minimal. The set

$$\{x \in \mathbb{R} : \exists y \in \mathbb{R}(x = y^2)\}$$

is definable and is neither finite nor coinfinite.

A theory T is called *strongly minimal* if every definable subset D of every model M of T is either finite or cofinite. Thus, the theory of divisible torsion-free abelian groups is strongly minimal.

Theorem 5.8.14. *The theory ACF of algebraically closed fields is strongly minimal.*

Proof. Let $\mathbb{K}$ be an algebraically closed field. Since *ACF* admits elimination of quantifiers, every definable subset of $\mathbb{K}$ is constructible and belongs to the algebra generated by sets

$$\{x \in \mathbb{K} : f(x) = 0\},$$

$f[X] \in \mathbb{K}[X]$. The result now follows because polynomials have only finitely many roots. □

Corollary 5.8.15. *Any field that is not strongly minimal is not algebraically closed.*

Let L be a language having a binary relation symbol $<$. Since *ODAG* admits elimination of quantifiers, if G is an ordered divisible abelian group, then a subset $D \subset G^n$ is definable if and only if it is defined by an open formula. Thus, $D \subset G^n$ is definable if and only if it belongs to the algebra generated by sets of the form

$$\{\overline{g} \in G^n : \sum_i n_i g_i + \sum_j m_j h_j = 0\}$$

and

$$\{\overline{g} \in G^n : \sum_i n_i g_i + \sum_j m_j h_j < 0\},$$

where $\overline{h} \in G$ and $\overline{n}, \overline{m} \in \mathbb{Z}$. In particular, this gives us the following interesting result.

Theorem 5.8.16. *If G is an ordered divisible abelian group, then $D \subset G$ is definable if and only if D is a union of a finite set and finitely many intervals.*

Corollary 5.8.17. *The sets of all natural numbers $\mathbb{N}$ and of all rational numbers $\mathbb{Q}$ are not definable subsets of the ordered field of real numbers $\mathbb{R}$.*

Here is another important definition in model theory. A linearly ordered structure $(D, <, \ldots)$ is called *o-minimal* if its definable subsets are precisely sets that are a union of a finite set and finitely many intervals.

5.9 Real Closed Fields

We now turn our attention to the important field of reals $\mathbb{R}$. We shall be a bit sketchy and refer the reader to [2] for more details.

Since the field $\mathbb{R}$ of reals is not strongly minimal, it does not admit elimination of quantifiers. Note that -1 cannot be expressed as a sum of finitely many squares of real numbers, and for every real r, either r or $-r$ is a square. Also, every odd-degree polynomial in one variable over $\mathbb{R}$ has a real root. We can take these as axioms, but since the field $\mathbb{R}$ is not strongly minimal, it will still not admit elimination of quantifiers. In fact, to achieve this useful property, we must introduce some new symbols.

Now note that $\mathbb{R}$ has a natural ordering that makes it an ordered field. It turns out that this is of fundamental importance. We call an ordered field $\mathbb{K}$ *real closed* if

1. $\forall x \exists y (x = y^2 \vee x + y^2 = 0)$, i.e., for every $x \in \mathbb{K}$, either x or $-x$ has a square root and
2. every polynomial in one variable over $\mathbb{K}$ of odd degree has a root in $\mathbb{K}$.

Example 5.9.1. Besides $\mathbb{R}$, the field of real algebraic numbers, denoted by $\mathbb{R}_{alg}$, is a real closed field.

Note that if $x \in \mathbb{K}$ is a square, then it must be ≥ 0, and if $x \geq 0$, then there is a unique $y \geq 0$ such that $x = y^2$. We then write $\sqrt{x}$ for y.

Remark 5.9.2. If $\mathbb{K}$ is a real closed field, then it has a unique ordering because its nonnegative elements are given by

$$\mathbb{K}^+ = \{x \in \mathbb{K} : \exists y \in \mathbb{K} (y \neq 0 \wedge x = y^2)\}.$$

This also shows that the ordering of $\mathbb{K}$ is definable in the language of rings. However, it may not be definable by an open formula. If $\mathbb{K} = \mathbb{R}$ and $<$ is defined by an open formula, then $\mathbb{R}^+$ should be either finite or cofinite, which it is not. Also note that every definable subset of $\mathbb{K}$ is definable in the language of rings.

Fix a real closed field $\mathbb{K}$, and for $\overline{x}, \overline{y} \in \mathbb{K}^n$ define

$$\rho(\overline{x}, \overline{y}) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}.$$

Note that $\rho(\overline{x}, \overline{y}) \geq 0$ and $\rho(\overline{x}, \overline{y}) = \rho(\overline{y}, \overline{x})$.

Exercise 5.9.3. For $\overline{x}$, $\overline{y}$, $\overline{z}$, show the following:

1. $\rho(\overline{x}, \overline{y}) = 0 \Leftrightarrow \overline{x} = \overline{y}$;
2. $\rho(\overline{x}, \overline{z}) \leq \rho(\overline{x}, \overline{y}) + \rho(\overline{y}, \overline{z})$.

(*Hint:* Observe that the Cauchy–Schwarz inequality holds.)

This enables us to treat $\mathbb{K}^n$ as a metric space inducing a topology on $\mathbb{K}^n$, which we shall call the usual topology. (See [17].)

We call a field *real* if -1 is not a sum of squares. Note that every ordered field is real.

Remark 5.9.4. A field $\mathbb{F}$ is real if and only if for all $\overline{a} \in \mathbb{F}$, $\sum_i a_i^2 = 0$ implies each $a_i = 0$.

Proposition 5.9.5. *Let $\mathbb{F}$ be a real field. Then the field of rational functions $\mathbb{F}(X_1, \cdots, X_n)$ is real.*

Proof. Our result will be proved if we show that for polynomials $f_1(\overline{X}), \cdots, f_k(\overline{X})$ over $\mathbb{F}$, $\sum_i f_i^2 = 0$ implies that each $f_i = 0$. We prove this by induction on n. In the case $n = 1$, let $f_i(X) = \sum_j a_{ij} X^j$ with $\sum_i f_i^2 = 0$. Since $\mathbb{F}$ is real, note that the leading coefficients of those f_i whose degree is the highest among those of $f_1, \cdots, f_k$ are zero. Thus, each f_i must be 0. For an inductive step, note that

$$\mathbb{F}[X_1, \cdots, X_n] = \mathbb{F}[X_1, \cdots, X_{n-1}][X_n].$$

□

Lemma 5.9.6. *Let $\mathbb{F}$ be a real field and $a \neq 0$ in $\mathbb{F}$. Then $\mathbb{F}[\sqrt{a}]$ is real if and only if $-a$ is not a sum of squares in $\mathbb{F}$.*

Proof. If $\mathbb{F}[\sqrt{a}]$ is real and $-a$ is a sum of squares, then $a + \sum_i b_i^2 = 0$. This implies that $a = 0$. This proves the *only if* part. Now assume that $\mathbb{F}[\sqrt{a}]$ is not real. Then we get $\overline{x}, \overline{y} \in \mathbb{F}$ such that $\overline{y} \neq 0$ and $\sum_i (x_i + y_i\sqrt{a})^2 = 0$. This, in particular, implies that $\sum_i x_i^2 + a \sum_i y_i^2 = 0$. Hence

$$-a = \frac{(\sum_i x_i^2)(\sum_i y_i^2)}{(\sum_i y_i^2)^2},$$

contradicting that $-a$ is not a sum of squares. □

Now, by Zorn's lemma, we get the following result.

Theorem 5.9.7. *Every real field $\mathbb{K}$ has a real algebraic extension $\mathbb{F}$ such that in $\mathbb{F}$ for every $a \in \mathbb{F}$, either a is a square or $-a$ is a sum of squares.*

Proof. Set

$$\mathbb{P} = \{\mathbb{F} : \mathbb{F} \text{ real algebraic extension of } \mathbb{K}\}.$$

Then $\mathbb{K} \in \mathbb{P}$, showing that $\mathbb{P}$ is nonempty. We partially order $\mathbb{P}$ by inclusion $\subset$. Note that if $\{\mathbb{F}_\alpha\}$ is a chain in $\mathbb{P}$, then $\cup_\alpha \mathbb{F}_\alpha$ is an upper bound of the chain in $\mathbb{P}$. Thus, by Zorn's lemma, $\mathbb{P}$ has a maximal element, say $\mathbb{F}$. By Lemma 5.9.6, this works. □

Now assume that $\mathbb{F}$ is a real field such that for every $a \in \mathbb{F}$ either a is a square or $-a$ is a sum of squares. Since $\mathbb{F}$ is real, this immediately implies that for every $a \neq 0$, exactly one of a and $-a$ is a sum of squares. We define

$$x < y \Leftrightarrow \exists \overline{z} \in \mathbb{F}(\overline{z} \neq 0 \wedge y = x + \sum_i z_i^2), x, y \in \mathbb{F}.$$

Exercise 5.9.8. Show that $<$ is a linear order on $\mathbb{F}$, making it an ordered field.

Thus, if $\mathbb{K}$ is a real field with no proper real algebraic extension, then the preceding ordering will be called the *canonical order of* $\mathbb{K}$. The foregoing result, in particular, gives us the following result of Artin and Schreier.

Theorem 5.9.9. *Let $\mathbb{F}$ be a real field and $a \in \mathbb{F}$ not a sum of squares. Then there is an order $<$ on $\mathbb{F}$ making $\mathbb{F}$ an ordered field and $a < 0$.*

Corollary 5.9.10. *A field is orderable if and only if it is real.*

The following result is also due to Artin and Schreier.

Proposition 5.9.11 (Weierstrass Nullstellensatz). *Let $\mathbb{K}$ be a real field with no proper real algebraic extension, with $<$ its canonical order, and let $f[X] \in \mathbb{K}[X]$ and $a < b \in \mathbb{K}$ be such that $f(a) \cdot f(b) < 0$. Then there is a $c \in \mathbb{K}$ with $a < c < b$ and $f(c) = 0$.*

Proof. First we observe that it is sufficient to show that f has a root in $\mathbb{K}$. Thus, let $c_0, \cdots, c_{n-1}$ be all the roots of f less than a. Then

$$f(x) = (x - c_0) \cdots (x - c_{n-1}) \cdot g(x),$$

where g is a polynomial having no root less than a. Note that $g(a) \cdot g(b) < 0$. We now work similarly with the roots $d_0, \cdots, d_{m-1}$ of f greater than b. They are precisely the roots of g greater than b. Thus, we write

$$g(x) = (x - d_0) \cdots (x - d_{m-1}) \cdot h(x),$$

with h having no roots either less than a or greater than b. Still we have $h(a) \cdot h(b) < 0$. Any root of h is a root of f between a and b.

Suppose our result is not true. Thus, there is a polynomial $f \in \mathbb{K}[X]$ and $a < b$ such that $f(a) \cdot f(b) < 0$, but f has no root in $\mathbb{K}$. We choose one such f of least degree. It is easily seen that f is irreducible. Then $\mathbb{F} = \mathbb{K}[X]/(f(X))$ is a proper algebraic extension of $\mathbb{K}$, and so not real. Set $\alpha = [X] \in \mathbb{F}$. We then get nonzero polynomials $g_i(X) \in \mathbb{K}[X]$, $1 \leq i \leq k$, such that $\sum_i g_i^2(\alpha) = 0$. Hence, $\sum_i g_i^2(X) = f(X) \cdot h(X)$ for some h. We choose such an h of the least degree. Note that we can arrange things so that the degree of each g_i is less than the degree of f. This implies that the degree of h is less than the degree of f. Since $f(a) \cdot h(a), f(b) \cdot h(b) \geq 0$, and $f(a) \cdot f(b) < 0$, either $h(a) = 0$ or $h(b) = 0$ or h changes signs between a and b. Since f was one such polynomial of least degree with no root, h has a root r in $\mathbb{K}$. Since $\mathbb{K}$ is real, r is a root of each g_i. Hence, there exist polynomials $h_i(X) \in \mathbb{K}[X]$ such that $g_i(X) = (X - r) \cdot h_i(X)$, $1 \leq i \leq k$. Since f has no root in $\mathbb{K}$, this implies that $(X - r)^2$ divides $h(X)$. Let $h(X) = (X - r)^2 \cdot f_1(X)$. Now we get $\sum_i h_i^2(X) = f(X) \cdot f_1(X)$, contradicting that h has the least possible degree satisfying such an identity. □

Artin and Schreier proved the following crucial result.

Theorem 5.9.12. *Let $\mathbb{K}$ be a real field. Then the following statements are equivalent.*

(*a*) *$\mathbb{K}$ has no proper real algebraic extension.*
(*b*) *$\mathbb{K}$ is real closed.*
(*c*) *The ring $\mathbb{K}[i] = \mathbb{K}[X]/(X^2 + 1)$ is algebraically closed.*

Proof. Suppose $\mathbb{K}$ has no proper real algebraic extension. Let $<$ denote the canonical order of $\mathbb{K}$ and $a > 0$ be in $\mathbb{K}$. Consider the polynomial

$$f(X) = X^2 - a$$

in $\mathbb{K}[X]$. Then $f(0) < 0$ and $f(1 + a) > 0$. Thus, by the Weierstrass Nullstellensatz, there is a $c \in \mathbb{K}$ such that $f(c) = 0$. Thus every positive element of $\mathbb{K}$ has a square root in $\mathbb{K}$.

Now take a monic polynomial $f(X) \in \mathbb{K}[X]$ of odd degree. Then, arguing as in the case of $\mathbb{R}$, we can find $a < b$ such that $f(a) < 0 < f(b)$. Hence, f has a root in $\mathbb{K}$ by the Weierstrass Nullstellensatz. Thus, (a) implies (b).

We now show that (b) implies (c). We first note that it is sufficient to prove that every $f \in \mathbb{K}[X]$ has a root in $\mathbb{K}[i]$. To see this, take any $g \in \mathbb{K}[i][X]$. Let $\overline{g}$ denote the polynomial obtained from g by replacing all its coefficients by their conjugates. Then $g \cdot \overline{g} \in \mathbb{K}[X]$. Hence, by our assumption, it has a root, say α, in $\mathbb{K}[i]$. Thus, α is a root of either g or $\overline{g}$. If α is not a root of g, then the conjugate $\overline{\alpha}$ of α is a root of g.

Thus, fix $f \in \mathbb{K}[X]$. Let $d = 2^m(2n + 1)$ be the degree of f. By induction on m, we show that f has a root in $\mathbb{K}[i]$. If $m = 0$, then the degree of f is odd. Thus, by (b), it has a root in $\mathbb{K} \hookrightarrow \mathbb{K}[i]$. Now assume that the assertion is true for $m - 1$.

Let $r_1, \cdots, r_d$ be all the roots of f in an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. For any $k \in \mathbb{Z}$, consider the polynomial

$$g_k(X) = \Pi_{1 \le p < q \le d}(X - r_p - r_q - k r_p \cdot r_q) \in \overline{\mathbb{K}}[X].$$

This is invariant under all transpositions of $r_1, \cdots, r_d$ and so is symmetric in $r_1, \cdots, r_d$. Since all the elementary symmetric polynomials in $r_1, \cdots, r_d$ are coefficients of f, they belong to $\mathbb{K}$. It is well known that all symmetric polynomial in $r_1, \cdots, r_d$ are functions of elementary symmetric polynomials. Hence, each g_k is a polynomial over $\mathbb{K}$. The degree of each g_k equals $\frac{d(d-1)}{2} = 2^{m-1}n'$, with n' odd. By the induction hypothesis, each g_k has a root in $\mathbb{K}[i]$. Therefore, there exist $1 \le p < q \le d$ and $k \ne k'$ such that

$$r_p + r_q + k r_p \cdot r_q, r_p + r_q k' r_p \cdot r_q \in \mathbb{K}[i].$$

This implies that there exist $1 \le p < q \le d$ such that $r_p + r_q, r_p \cdot r_q \in \mathbb{K}[i]$. Now it is elementary to check that $r_p, r_q \in \mathbb{K}[i]$. We have shown that (b) implies (c).

To show that (c) implies (a), first note that by (c), $\mathbb{K}[i]$ is the only nontrivial algebraic extension of $\mathbb{K}$. Further, $\mathbb{K}[i]$ is clearly not real. Hence, $\mathbb{K}$ has no proper real algebraic extension. □

Exercise 5.9.13. Let $\mathbb{K}$ be a field such that $\mathbb{K}[i]$ is algebraically closed. Show that $\mathbb{K}$ is real. Conclude that in Theorem 5.9.12 we need not assume that $\mathbb{K}$ is real.

Corollary 5.9.14. *Let $\mathbb{F}$ and $\mathbb{K}$ be real closed fields with $\mathbb{F}$ a subfield of $\mathbb{K}$. Then every root in $\mathbb{K}$ of a polynomial $f(X)$ over $\mathbb{F}$ lies in $\mathbb{F}$.*

Proof. Let $x \in \mathbb{K}$ be a root of a polynomial $f(X) \in \mathbb{F}[X]$. Note that the subfield generated by $\mathbb{F}$ and x is a real algebraic extension of $\mathbb{F}$. But $\mathbb{F}$ has no proper real algebraic extension. Hence, $x \in \mathbb{F}$. □

Remark 5.9.15. Let $\mathbb{F}$ be a real closed field and $a \ne 0$ be in $\mathbb{F}$. Then a is a square if and only if $-a$ is not a sum of squares.

A real algebraic extension of $\mathbb{K}$ with no proper real algebraic extension will be called a *real closure* of $\mathbb{K}$.

Remark 5.9.16. Consider the real field $\mathbb{F} = \mathbb{Q}(X)$ of rational functions over $\mathbb{Q}$. Clearly, $\mathbb{F}[\sqrt{X}]$ and $\mathbb{F}[\sqrt{-X}]$ are real fields. Their real closures are not isomorphic.

However, there is a uniqueness result for ordered fields.

Proposition 5.9.17. *Let $(\mathbb{K}, 0, 1, +, \cdot, <)$ be an ordered field, $0 < x \in \mathbb{K}$, which is not a square in $\mathbb{K}$; then there is an order on the extension field $\mathbb{K}[\sqrt{x}]$ extending the order $<$ on $\mathbb{K}$.*

Proof. For $a + b\sqrt{x}$, $c + d\sqrt{x}$ in $\mathbb{K}[\sqrt{x}]$, define

$$a + b\sqrt{x} < c + d\sqrt{x}$$

if any one of the following conditions is satisfied:

(i) $c = d = 0$ and $a < b$.
(ii) $b = d$ and $a < c$.
(iii) $b < d$ and either $a < c$ or $\frac{(a-c)^2}{(b-d)^2} < x$.
(iv) $b > d$ and $c < a$ and $x < \frac{(a-c)^2}{(b-d)^2}$.

It is entirely routine to check that this works. □

Theorem 5.9.18. *Let $(\mathbb{K}, <)$ be an ordered field. Then there is a real closure of $\mathbb{K}$ whose canonical order is compatible with $<$. If $\mathbb{K}_1$ and $\mathbb{K}_2$ are real closed algebraic extensions of $\mathbb{K}$, then there is a unique order-preserving isomorphism $\alpha : \mathbb{K}_1 \to \mathbb{K}_2$ fixing $\mathbb{K}$.*

Proof. Consider

$$\mathbb{P} = \{(\mathbb{F}, <') : \mathbb{F} \text{ an ordered algebraic extension of } \mathbb{K} \wedge <' | \mathbb{K} = <\},$$

partially ordered by the inclusion $\subset$. By Zorn's lemma, it has a maximal element, say $(\mathbb{K}', <')$. By Proposition 5.9.17, every positive element of $\mathbb{K}'$ has a square root in $\mathbb{K}'$. Note that $\mathbb{K}'$ does not have a proper real algebraic extension because then its canonical ordering would extend $<$ since every positive element of $\mathbb{K}$ has a square root in $\mathbb{K}'$. Clearly, $\mathbb{K}'$ satisfies the desired properties. We omit the proof of the uniqueness. □

If $\mathbb{K}$ is an ordered field, then a real closed algebraic extension of $\mathbb{K}$ preserving $<$ is called the *real closure* of $\mathbb{K}$. Note that $\mathbb{R}_{alg}$ is the real closure of $\mathbb{Q}$.

Example 5.9.19. The $\mathbb{R}_{alg}$ order isomorphically embeds into all real closed fields.

Example 5.9.20. The models of $RCF_\forall$ are precisely ordered integral domains.

Proof. It is clear that every model of $RCF_\forall$ is an ordered integral domain. On the other hand, given an ordered integral domain D, let $\mathbb{F}$ be its ordered hull as defined in Proposition 2.5.13. By Theorem 5.9.18, it is order-isomorphically embedded in its real closure, say $\mathbb{K}$. Since $\mathbb{K} \models RCF$, $D \models RCF_\forall$. □

The arguments contained in Example 5.9.20 give us the following proposition.

Proposition 5.9.21. *The theory RCF of real closed fields has algebraically prime models.*

Proposition 5.9.22. *The theory RCF of real closed fields admit elimination of quantifiers.*

Proof. As in the cases of, say, *ODAG* and *ACF* etc., we only need to show that if $\varphi[x, \bar{y}]$ is a conjunction of literals, $\mathbb{F} \subset \mathbb{K} \models RCF$, and $\bar{a} \in \mathbb{F}$, then

$$\mathbb{K} \models \exists x \varphi[x, i_{\bar{a}}] \Rightarrow \mathbb{F} \models \exists x \varphi[x, i_{\bar{a}}].$$

We can assume that $\varphi[x,\bar{y}]$ is of the form

$$\wedge_{i=1}^{n}(p_i(x,\bar{y})=0)\wedge\wedge_{j=1}^{m}(q_j(x,\bar{y})>0),$$

with p_i and q_j being terms.

Choose a $b\in\mathbb{K}$ such that

$$\mathbb{K}\models\varphi[i_b,i_{\bar{a}}].$$

Now if any of the equality terms is present, by Corollary 5.9.14, $b\in\mathbb{F}$.

Thus, assume no p_i is present. We will now use Corollary 5.9.14. Note that the roots of q_j, if any, belong to $\mathbb{F}$. If a q_j has no root in the field and since $q_j(b)>0$, by Proposition 5.9.11, $q_j(c)>0$ for all $c\in\mathbb{F}$. By considering finitely many roots of all q_j (all of which belong to $\mathbb{F}$), by Proposition 5.9.22, we find a nonempty open interval I in $\mathbb{K}$ with end points in $\mathbb{F}$ such that $b\in I$ and $q_j(x)>0$ for all $x\in I$. Using the order denseness of $\mathbb{F}$, we have a $b\in\mathbb{F}$ that lies in I. This b witnesses $\mathbb{F}\models\varphi[i_b,i_{\bar{a}}]$. □

Corollary 5.9.23. *The theory RCF of real closed fields is model-complete and is o-minimal.*

Theorem 5.9.24. *The theory RCF of real closed fields is complete.*

Proposition 5.9.25. *Every model of RCF is elementarily equivalent to* $\mathbb{R}$ *as well as to* $\mathbb{R}_{alg}$.

Let M be a model of a theory T and $A\subset M$. We say that M is *prime over* A or that M is a *prime model extension* of A if for every model N of T and every partial elementary map $h:A\to N$ there is an elementary embedding $g:M\to N$ such that $h=g|A$.

Example 5.9.26. Consider the theory *ACF* of algebraically closed fields. Let D be an integral domain and $\mathbb{F}$ the algebraic closure of the fraction field of D. We know that given any $\mathbb{K}\models ACF$ and a partial elementary map $h:D\to\mathbb{K}$ (an embedding, in particular), there is an embedding $g:\mathbb{F}\to\mathbb{K}$ such that $h=g|D$. Since *ACF* has elimination of quantifiers, g is elementary.

Example 5.9.27. Consider the theory *RCF* of real closed fields. Let D be an ordered integral domain and $\mathbb{F}$ the real closure of the ordered fraction field of D. We know that given any $\mathbb{K}\models RCF$ and an elementary map $h:D\to\mathbb{K}$, there is an embedding $g:\mathbb{F}\to\mathbb{K}$ such that $h=g|D$. Since *RCF* has elimination of quantifiers, g is elementary.

Example 5.9.28. Consider the theory *DLO* of dense linearly ordered sets with no end points. Let $(A,<)$ be a linearly ordered set. We define a dense linearly ordered set A^* as follows: if A has a least element, say x, then add a copy of $\mathbb{Q}$ with the usual order to the left of x, if A has a greatest element, say y, then add a copy of $\mathbb{Q}$ with the usual order to the right of y, and if $x<y$ are two elements of A with no element in between, then add a copy of $\mathbb{Q}$ with the usual order between x and y. There is a canonical inclusion map $f:A\hookrightarrow A^*$. Now given any $B\models DLO$ and a

partial elementary map $h : A \to B$, it is easy to define an embedding $g : A^* \to B$ such that $h = g \circ f$. Since *DLO* admits elimination of quantifiers, g is elementary.

Later in this chapter we shall address the following interesting question: When does a structure A of a theory T admit a prime model extension?

5.10 Some Applications in Algebra and Geometry

In this section, we give some applications in algebra and geometry, showing some of the ways in which logic can be used to prove deep results in mathematics.

Theorem 5.10.1 (Chevalley). *Let $\mathbb{K}$ be an algebraically closed field and $D \subset \mathbb{K}^n$ be constructible. If $f_1, \cdots, f_m \in \mathbb{K}[X_1, \cdots, X_n]$ are polynomials over $\mathbb{K}$, then $X = f(D) \subset \mathbb{K}^m$ is constructible, where $f = (f_1, \cdots, f_m)$.*

Proof. Note that

$$\bar{y} \in X \Leftrightarrow \exists \bar{x}(\bar{x} \in D \wedge \bar{y} = f(\bar{x})).$$

Since D is definable, we now easily see that X is defined by a formula whose parameters are the coefficients of f and those used to define D. Thus, X is constructible by Theorem 5.8.11. □

Our next result is a basic result in algebraic geometry proved by David Hilbert. We shall assume some results from commutative algebra and refer the reader to [10].

We fix a commutative ring R with identity 1. An *ideal* I in R is a subring $I \subset R$ such that if $x \in I$, then so does $x \cdot y$ for every $y \in R$. The ideal I is called proper if $1 \notin I$. This is the same as saying that I is a proper subset of the ring.

Given an ideal I in R, for $x, y \in R$, define

$$x \sim_I y \Leftrightarrow x - y \in I.$$

Then $\sim_I$ is an equivalence relation on R satisfying the following statements:

1. If $x \sim_I y$ and $x' \sim_I y'$, then $x + x' \sim_I y + y'$.
2. If $x \sim_I y$ and $x' \sim_I y'$, then $x \cdot x' \sim_I y \cdot y'$.

Set

$$R/I = R/\sim_I = \{[x] : x \in R\},$$

where $[x]$ is the $\sim_I$-equivalence class containing $x \in R$. Let $q : R \to R/I$ denote the quotient map. For $x, y \in R$, define

$$\overline{0} = [0] \text{ and } \overline{1} = [1],$$

$$[x] + [y] = [x + y],$$

and

$$[x] \cdot [y] = [x \cdot y].$$

These are well defined and make R/I a commutative ring with identity and $q : R \to R/I$ a homomorphism with kernel I.

An ideal I in R is called a *prime ideal* if $x \cdot y \in I$ implies $x \in I$ or $y \in I$.

Example 5.10.2. $I \subset \mathbb{Z}$ is an ideal in the ring of integers $\mathbb{Z}$ if and only if there is a positive integer m such that $I = m\mathbb{Z}$, and it is a prime ideal if and only if m is prime.

The following result is quite easy to prove.

Proposition 5.10.3. *An ideal I in R is a prime ideal if and only if R/I is an integral domain.*

An ideal I in R is called a *radical ideal* if for every $x \in R$, whenever $x^n \in I$ for some $n \in \mathbb{N}$, $x \in I$. Note that every prime ideal is a radical ideal and so is an intersection of prime ideals.

Now fix a field $\mathbb{K}$ and consider the ring $\mathbb{K}[\overline{X}] = \mathbb{K}[X_1, \cdots, X_n]$ of polynomials over $\mathbb{K}$ in n variables.

We refer the reader to [10] for a proof of the following result.

Theorem 5.10.4 (Prime Decomposition Theorem). *If I is a radical ideal in $\mathbb{K}[\overline{X}]$, then there exist prime ideals $P_1, \cdots, P_k$ such that $I = \cap_{i=1}^{k} P_i$.*

Corollary 5.10.5. *If $I \neq J$ are radical ideals in $\mathbb{K}[\overline{X}]$ and $f \in I \setminus J$, then there is a prime ideal $P \supset J$ such that $f \notin P$.*

For $X \subset \mathbb{K}^n$, set

$$\mathscr{I}(X) = \{f \in \mathbb{K}[\overline{X}] : f(\overline{x}) = 0 \ \forall \overline{x} \in X\}.$$

Then $\mathscr{I}(X)$ is a radical ideal in $\mathbb{K}[\overline{X}]$, and if $X \subset Y \subset \mathbb{K}^n$, then $\mathscr{I}(Y) \subset \mathscr{I}(X)$.

For $S \subset \mathbb{K}[\overline{X}]$, recall

$$\mathscr{V}(S) = \{\overline{x} \in \mathbb{K}^n : f(\overline{x}) = 0 \ \forall f \in S\}.$$

The following statements are quite easy to prove.

1. $X \subset \mathscr{V}(\mathscr{I}(X))$ for all $X \subset \mathbb{K}^n$.
2. $S \subset \mathscr{I}(\mathscr{V}(S))$ for all $S \subset \mathbb{K}[\overline{X}]$.
3. For $S \subset T \subset \mathbb{K}[\overline{X}]$, $\mathscr{V}(T) \subset \mathscr{V}(S)$.
4. $\mathscr{V}(S) = \mathscr{V}(\mathscr{I}(\mathscr{V}(S)))$ for all $S \subset \mathbb{K}[\overline{X}]$.

To see the last identity, if possible, suppose there exists an $\overline{x} \in \mathscr{V}(S) \setminus \mathscr{V}(\mathscr{I}(\mathscr{V}(S)))$. Then there exists an $f \in S \subset \mathscr{I}(\mathscr{V}(S))$ such that $f(\overline{x}) \neq 0$. This is a contradiction.

We need one more result of Hilbert from commutative algebra to give a model-theoretic proof of the aforementioned theorem of Hilbert.

Theorem 5.10.6 (Hilbert's Basis Theorem). *Every ideal in the polynomial ring* $\mathbb{K}[\overline{X}]$*, with* $\mathbb{K}$ *a field, is finitely generated.*

Theorem 5.10.7 (Hilbert's Nullstellensatz). *Let* $\mathbb{K}$ *be an algebraically closed field and* I *a radical ideal in* $\mathbb{K}[\overline{X}]$*. Then*

$$I = \mathscr{I}(\mathscr{V}(I)).$$

Proof. We clearly have $I \subset \mathscr{I}(\mathscr{V}(I))$. If possible, suppose there is an $f \in \mathscr{I}(\mathscr{V}(I)) \setminus I$. By Corollary 5.10.5, there is a prime ideal $P \supset I$ not containing f. Since P is a prime ideal in $\mathbb{K}[\overline{X}]$, $\mathbb{K}[\overline{X}]/P$ is an integral domain.

Let $\mathbb{F}$ be the algebraic closure of the quotient field of $\mathbb{K}[\overline{X}]/P$. By Hilbert's basis theorem, we fix a basis $g_1, \cdots, g_k \in I$ generating I. Note that each X_i can be regarded as an element of $\mathbb{K}[\overline{X}]$. Because $f \notin P$ and $g_1, \cdots, g_k \in I$, we have

$$\mathbb{F} \models \wedge_{i=1}^{k} g_i([X_1], \cdots [X_n]) = 0 \wedge f([X_1], \cdots [X_n]) \neq 0.$$

In particular,

$$\mathbb{F} \models \exists \overline{y}(\wedge_{i=1}^{k} g_i(\overline{y}) = 0 \wedge f(\overline{y}) \neq 0).$$

By model completeness,

$$\mathbb{K} \models \exists \overline{y}(\wedge_{i=1}^{k} g_i(\overline{y}) = 0 \wedge f(\overline{y}) \neq 0).$$

This gives an $\overline{a} \in \mathbb{K}$ such that for all $1 \leq i \leq k$, $g_i(\overline{a}) = 0$ and $f(\overline{a}) \neq 0$. But if $g_i(\overline{a}) = 0$ for all $1 \leq i \leq k$, as $g_1, \cdots, g_k$ generate I, $\overline{a} \in \mathscr{V}(I)$. Since $f \in \mathscr{I}(\mathscr{V}(I))$, $f(\overline{a}) = 0$. This contradiction proves the result. □

We now give some applications to real closed fields. The first result is a counterpart of Chevalley's theorem for real closed fields.

Fix a real closed field $\mathbb{F}$. Call a set $X \subset \mathbb{F}^n$ *semialgebraic* if it belongs to the smallest algebra on $\mathbb{F}^n$ generated by sets of the form

$$\{\overline{x} \in \mathbb{F}^n : 0 < f(\overline{x})\},$$

$f(\overline{X}) \in \mathbb{F}[\overline{X}]$. A map $f : \mathbb{F}^n \to \mathbb{F}^m$ is called *semialgebraic* if its graph is semialgebraic.

Exercise 5.10.8. A set $X \subset \mathbb{F}^n$ is semialgebraic if and only if it is defined by an open formula.

Since *RCF* admits elimination of quantifiers, we have the following theorem.

Theorem 5.10.9. *If* $\mathbb{F}$ *is a real closed field, then* $X \subset \mathbb{F}^n$ *is semialgebraic if and only if it is definable.*

Theorem 5.10.10 (Tarski–Seidenberg). *If* $\mathbb{F}$ *is a real closed field, with* $X \subset \mathbb{F}^n$ *and* $f : \mathbb{F}^n \to \mathbb{F}^m$ *semialgebraic, then* $f(X) \subset \mathbb{F}^m$ *is semialgebraic.*

We have already seen that if $\mathbb{F}$ is a real closed field, then there is a "metric" ρ on $\mathbb{F}^n$ inducing a topology on $\mathbb{F}^n$ called the usual topology.

Proposition 5.10.11. *If $\mathbb{F}$ is a real closed field and $X \subset \mathbb{F}^n$ semialgebraic, then so is its closure $\overline{X}$ in the usual topology.*

Proof. Note that

$$\bar{y} \in \overline{X} \Leftrightarrow \forall z(z > 0 \to \exists \bar{x}(\bar{x} \in X \wedge \rho(\bar{y}, \bar{x}) < z).$$

This shows that $\overline{X}$ is definable. By elimination of quantifiers, it follows that $\overline{X}$ is semialgebraic. □

Exercise 5.10.12. Let $\mathbb{F}$ be a real closed field. Define

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{otherwise.} \end{cases}$$

Show that $x \to |x|$ is semialgebraic.

Exercise 5.10.13. Show that the Cauchy–Schwarz inequality holds in all real closed fields.

Exercise 5.10.14. Let $\mathbb{F}$ be a real closed field and $f : \mathbb{F}^n \to \mathbb{F}^m$ a semialgebraic map. Show that there is a sentence φ such that

$$\mathbb{F} \models \varphi \Leftrightarrow f \text{ is continuous.}$$

Exercise 5.10.15. Let $\mathbb{F}$ be a real closed field, and let both $C \subset \mathbb{F}^n$ and $f : \mathbb{F}^n \to \mathbb{F}^m$ be semialgebraic. Show that there is a sentence ψ such that $\mathbb{F} \models \psi$ if and only if "C is closed and bounded and f continuous implies that $f(C)$ is closed and bounded."

It is well known that ψ is true in the field $\mathbb{R}$. Since any two models of *RCF* are elementarily equivalent, we now get the following proposition.

Proposition 5.10.16. *If $\mathbb{F}$ is a real closed field, $C \subset \mathbb{F}^n$ is closed, bounded, and semialgebraic, and $f : \mathbb{F}^n \to \mathbb{F}^m$ is continuous and semialgebraic, then $f(C) \subset \mathbb{F}^m$ is semialgebraic and closed and bounded.*

We now present a model-theoretic solution, due to Abraham Robinson, of *Hilbert's 17th problem*. The problem was first solved by Emil Artin.

Theorem 5.10.17. *Let $\mathbb{F}$ be a real closed field and $f \in \mathbb{F}(\overline{X}) = \mathbb{F}(X_1, \cdots, X_n)$ a rational function over $\mathbb{F}$ in n variables such that for no $\bar{x} \in \mathbb{F}^n$, $f(\bar{x}) < 0$. Then f is a sum of squares of rational functions over $\mathbb{F}$.*

Proof. Suppose f is not a sum of squares. By Proposition 5.9.5, the field of rational functions $\mathbb{F}(\overline{X})$ is real. By Theorem 5.9.9, there is a linear order $<$ on the field $\mathbb{F}(\overline{X})$ of rational functions over $\mathbb{F}$, making it an ordered field, where $f < 0$.

Let $\mathbb{K}$ be the real closure of $\mathbb{F}(\overline{X})$ with order compatible with $<$. Then

$$\mathbb{K} \models \exists \overline{x}(f(\overline{x}) < 0).$$

(Take $x_i = X_i \in \mathbb{K}$.) By model completeness,

$$\mathbb{F} \models \exists \overline{x}(f(\overline{x}) < 0).$$

But there is no $\overline{a} \in \mathbb{F}$ such that $f(\overline{a}) < 0$. Thus, f must be a sum of squares of rational functions over $\mathbb{F}$. □

Exercise 5.10.18. Let $\mathbb{K}$ be a real closed field and $f(X) \in \mathbb{K}[X]$ a polynomial such that for no $x \in \mathbb{K}$, $f(x) < 0$. Show that f is a sum of squares of polynomials over $\mathbb{K}$.

(*Hint:* Prove it for $\mathbb{R}$.)

Remark 5.10.19. If $\mathbb{K}$ is a real closed field, $n > 1$, and $f \in \mathbb{K}[X_1, \cdots, X_n]$ is such that for no $\overline{x} \in \mathbb{K}^n$ $f(\overline{x}) < 0$, then f need not be a sum of squares of polynomials over $\mathbb{K}$. The Motzkin polynomial

$$X^2Y^4 + X^4Y^2 + 1 - 3X^2Y^2 \in \mathbb{R}[X, Y]$$

never takes a value less than 0 but is not a sum of squares of polynomials. We invite the reader to verify this.

The next three results are well known for the field of real numbers $\mathbb{R}$. Thus, by the elementary equivalence of real closed fields, they hold for all real closed fields.

Theorem 5.10.20 (Rolle's Theorem). *Let $\mathbb{F} \models RCF$, $f(X) \in \mathbb{F}[X]$, and $a < b$ in $\mathbb{F}$ be such that $f(a) = 0 = f(b)$. Let $f'(X)$ denote the formal derivative of f. Then there is a $c \in \mathbb{F}$ such that $a < c < b$ and $f'(c) = 0$.*

Theorem 5.10.21 (Mean value Theorem). *Let $\mathbb{F} \models RCF$, $f(X) \in \mathbb{F}[X]$, and $a < b$ in $\mathbb{F}$. Then there is a $c \in \mathbb{F}$ such that $a < c < b$ and*

$$f(b) = f(a) + (b - a) \cdot f'(c).$$

Theorem 5.10.22. *Let $\mathbb{F} \models RCF$, $f(X) \in \mathbb{F}[X]$, and $a < b$ in $\mathbb{F}$ be such that for all $a < c < b$, $f'(c) > 0$. Then $f(a) < f(b)$.*

The reader should see a very fine expository note of Swan [18] on these applications to algebraically and real closed fields. We have relied heavily on Swan's article in our presentation. For real algebraic geometry, we strongly recommend [2].

5.11 Isolated and Omitting Types

Let $p[\overline{x}]$, or simply p when $\overline{x}$ is understood, be a set of formulas in variables $x_0, \ldots, x_{n-1}$ such that $T \cup p$ is satisfiable. We call such a p an *n-type in T* and a *complete n-type* if for every formula $\varphi[\overline{x}]$ either φ or $\neg\varphi$ is in p. The set of all

complete n-types in T will be denoted by $S_n(T)$. Note the difference between the definitions of types given now and earlier.

Remark 5.11.1. If T is complete and $M \models T$, then $S_n(T) = S_n^M(\emptyset)$, because in this case Th_M is precisely the set of all theorems of T.

By Lindenbaum's theorem, we have the following result.

Proposition 5.11.2. *Every n-type p in T is contained in a complete n-type in T.*

Exercise 5.11.3. Let $p \in S_n(T)$. Show that $\varphi \wedge \psi \in p$ if and only if both φ and ψ belong to p and $\varphi \vee \psi \in p$ if and only if at least one of φ and ψ belongs to p.

Let $[\varphi]$ denote the set of all complete n-types containing φ. The following identities are easy to check:

$$[\varphi \wedge \neg\varphi] = \emptyset, [\varphi \vee \neg\varphi] = S_n(T),$$

$$[\varphi \wedge \psi] = [\varphi] \cap [\psi], [\varphi \vee \psi] = [\varphi] \cup [\psi],$$

and

$$[\neg\varphi] = S_n(T) \setminus [\varphi].$$

Note that the sets $[\varphi]$ form the base of a topology on $S_n(T)$ with respect to which it is zero-dimensional.

Lemma 5.11.4. *Let $\Gamma = \{\varphi[\bar{x}] : \varphi[\bar{x}]$ a formula$\}$ be a set of formulas such that $\{[\varphi] : \varphi \in \Gamma\}$ has the finite intersection property. Then there is an n-type $p \supset \Gamma$, i.e., $\cap_{\varphi\in\Gamma}[\varphi] \neq \emptyset$.*

Proof. By Lindenbaum's theorem, it is sufficient to show that $T[\Gamma]$ is satisfiable. By the compactness theorem, it is sufficient to show that $T[\Gamma]$ is finitely satisfiable. This is implied by our assumption that $\{[\varphi] : \varphi \in \Gamma\}$ has the finite intersection property. □

Remark 5.11.5. Thus $S_n(T)$ is a compact, zero-dimensional, Hausdorff space. It is Hausdorff because if $p \neq q \in S_n(T)$, then there is a formula $\varphi[\bar{x}] \in p$ such that $\neg\varphi[\bar{x}] \in q$. Hence, $p \in [\varphi], q \in [\neg\varphi]$, and, of course, $[\varphi] \cap [\neg\varphi] = \emptyset$. If T is countable, then $S_n(T)$ is compact, Hausdorff, and second countable. Thus, $S_n(T)$ is compact and metrizable if T is countable.

We say that a formula $\varphi[\bar{x}]$ *isolates* p if $T \cup \{\varphi\}$ is satisfiable, i.e., $T \cup \{\exists\bar{x}\varphi\}$ has a model, and

$$\psi[\bar{x}] \in p \Leftrightarrow T \vdash \forall\bar{x}(\varphi[\bar{x}] \rightarrow \psi[\bar{x}]).$$

In particular, $\varphi \in p$. Note that p is an isolated type if and only if p is an isolated point of $S_n(T)$. Indeed, if φ isolates p, then $\{p\} = [\varphi]$. Further following the terminology from topology, we say that *isolated types are dense* in $S_n(T)$ if every nonempty $[\varphi]$ contains an isolated type.

Remark 5.11.6. Since isolated points are open, if every $p \in S_n(T)$ is isolated, then by the compactness of $S_n(T)$, $S_n(T)$ is finite.

Similarly, if M is a structure of a first-order language L and $p \in S_n^M(\emptyset)$, we say that a formula $\varphi[\overline{x}]$ of L *isolates* p if

$$\psi[\overline{x}] \in p \Leftrightarrow M \models \forall \overline{x}(\varphi[\overline{x}] \to \psi[\overline{x}]).$$

In particular, $\varphi \in p$.

Example 5.11.7. Since DLO is complete, $S_n(DLO) = S_n^{\mathbb{Q}}(\emptyset)$. Let $p(\overline{x}) \in S_n(DLO)$. Then there exists a countable elementary extension $\mathbb{Q}'$ of $\mathbb{Q}$ in which p is realized. Since $\mathbb{Q}$ and $\mathbb{Q}'$ are isomorphic, it follows that p is realized in $\mathbb{Q}$, say by $\overline{r}$. Let π be a permutation of $n = \{0, 1, \cdots, n-1\}$ such that $r_{\pi(0)} < \cdots < r_{\pi(n-1)}$. It is easy to check that the formula $x_0 < \cdots < x_{n-1}$ isolates p. Thus, every type in $S_n(DLO)$ is isolated. Hence, $S_n(DLO)$ is finite for each n.

Proposition 5.11.8. *Let M be a model of T and $(\overline{a}, \overline{b}) \in M$ be such that $tp^M(\overline{a}, \overline{b})$ is isolated. Then $tp^M(\overline{a})$ is isolated.*

Proof. Let $\varphi[\overline{x}, \overline{y}]$ isolate $tp^M(\overline{a}, \overline{b})$. Since

$$M \models \forall \overline{x} \forall \overline{y}(\varphi[\overline{x}, \overline{y}] \to \varphi[\overline{x}, \overline{y}]),$$

$\varphi \in tp^M[\overline{a}, \overline{b}]$. Therefore, $M \models \varphi[i_{\overline{a}}, i_{\overline{b}}]$.

Now consider $\psi[\overline{x}] = \exists \overline{y} \varphi$. Thus, $M \models \psi[i_{\overline{a}}]$. Suppose $M \models \forall \overline{x}(\psi[\overline{x}] \to \eta[\overline{x}])$. In particular, $M \models \eta[i_{\overline{a}}]$, i.e., $\eta[\overline{x}] \in tp^M(\overline{a})$. Trivially, $tp^M(\overline{a}) \subset tp^M(\overline{a}, \overline{b})$. Therefore, $\eta[\overline{x}] \in tp^M(\overline{a}, \overline{b})$.

Conversely, suppose $M \models \eta[i_{\overline{a}}]$. We are required to show that

$$M \models \forall \overline{x}(\psi[\overline{x}] \to \eta[\overline{x}]).$$

Suppose not. Then there exists a $\overline{c} \in M$ such that $M \models \psi[i_{\overline{c}}] \wedge \neg \eta[i_{\overline{c}}]$. Since $M \models \psi[i_{\overline{c}}]$, there is a $\overline{d} \in M$ such that $M \models \varphi[i_{\overline{c}}, i_{\overline{d}}]$. Since φ isolates $tp^M(\overline{a}, \overline{b})$,

$$M \models \forall \overline{x} \forall \overline{y}(\varphi[\overline{x}, \overline{y}] \to \eta[\overline{x}]).$$

In particular, $M \models \eta[i_{\overline{c}}]$. This contradiction proves our result. □

Proposition 5.11.9. *Let T be a complete theory. Then every isolated type is realized in every model of T.*

Proof. Let p be an n-type isolated by, say, $\varphi[\overline{x}]$ and $M \models T$. We claim that $M \models \exists \overline{x} \varphi$. If not, $M \models \neg \exists \overline{x} \varphi$. Since T is complete, it follows that $T \vdash \neg \exists \overline{x} \varphi$. But this implies that $T \cup \{\varphi\}$ is not satisfiable.

Thus, take $\overline{a} \in M$ such that $M \models \varphi[i_{\overline{a}}]$. Since φ isolates p, it follows that $M \models \psi[i_{\overline{a}}]$ for all $\psi \in p$. □

Interestingly, the converse is true for countable theories T. The argument contained in the proof below is quite important and can be adopted in many model construction.

Theorem 5.11.10 (Omitting Types Theorem). *Let T be a countable, consistent theory and p a nonisolated n-type in T. Then there is a countable model M of T that omits p.*

Proof. We add countably many distinct new constant symbols $\{c_k\}$ to the language of T and call the new language L (and the new theory T itself). Let $\{\psi_n\}$ be an enumeration of all closed formulas of L and $\{a_k\}$ an enumeration of all n-tuples of new constants c_m.

We shall get a complete Henkin simple extension T^* of T and a countable model M of T^* such that

(a) Every element of M is the interpretation of some c_k;
(b) For every k, there is a formula $\psi[\overline{x}] \in p$ such that $M \not\models \psi[i_{a_k}]$.

It will then follow that M is a countable model of T that omits p.

To construct such a T^* we shall first define a sequence of closed formulas $\{\varphi_n\}$ of L such that

(c) For every k, $T[\varphi_k]$ is consistent;
(d) For $k < l$, $T \vdash \varphi_l \to \varphi_k$;
(e) For every k, if ψ_k is an existential sentence $\exists v \eta[v]$ such that $T[\varphi_{2k}] \vdash \psi_k$, then $T[\varphi_{2k+1}] \vdash \eta_v[c_m]$ for some m;
(f) For every k, there is a $\psi \in p$ such that $T[\varphi_{2k+2}] \vdash \neg\psi[a_k]$.

Take φ_0 to be any sentence consistent with T. Suppose φ_{2k} has been defined such that $T[\varphi_{2k}]$ is consistent.

If ψ_k is not an existential sentence, or if $T[\varphi_{2k}] \not\vdash \psi_k$, then we take $\varphi_{2k+1} = \varphi_{2k}$. Otherwise, ψ_k is a closed existential formula, say $\exists v \eta[v]$, and $T[\varphi_{2k}] \vdash \psi_k$. Since only a finite number of the new constants c_l appear in φ_{2k} and ψ_k, take a constant symbol c_m that does not occur in φ_{2k} and ψ_k. Set $\varphi_{2k+1} = \varphi_{2k} \wedge \eta_v[c_m]$.

We need to show that $T[\varphi_{2k+1}]$ is consistent, i.e., that $T[\{\varphi_{2k}, \eta_v[c_m]\}]$ has a model. To see this take a model N of $T[\varphi_{2k}]$. Then $N \models \psi_k$. Thus, there is a $b \in N$ such that $N \models \eta_v[i_b]$. Now interpret c_m by b in N. We definitely have $T[\varphi_{2k+1}] \vdash \eta_v[c_m]$.

Let $a_k = (c_{i_1}, \cdots, c_{i_n})$. Replace each occurrence of c_{i_j} in φ_{2k+1} by a new variable x_j and each $c_m \notin \{c_{i_j} : 1 \le j \le n\}$ occurring in φ_{2k+1} by a new variable y_m to get φ' and set $\varphi''[\overline{x}] = \exists \overline{y} \varphi'$. Because p is not isolated, there is a $\psi[\overline{x}] \in p$ such that

$$T \not\vdash \forall \overline{x}(\varphi'' \to \psi). \qquad (*)$$

Set $\varphi_{2k+2} = \varphi_{2k+1} \wedge \neg\psi[\underline{a}_k]$. We must show that $T[\varphi_{2k+2}]$ is consistent. By $(*)$, there is a model N of T and a $\overline{b} \in N$ such that

$$N \models \varphi''[i_{\overline{b}}] \wedge \neg\psi[i_{\overline{b}}].$$

Interpreting c_{i_j} by b_j, $1 \leq j \leq n$, we see that $N \models \varphi_{2k+2}$. This completes our construction.

Let T' be the theory $T[\{\varphi_k : k \geq 0\}]$. Then T' is a countable consistent Henkin theory such that for every k there exists a $\psi \in p$ such that $T' \vdash \neg\psi[a_k]$. By Lindenbaum's theorem, T' has a complete simple extension T^*. Clearly, T^* is countable.

Let M be the canonical model of T^*. We claim that every element in M is an interpretation of some c_k. To see this, take a variable-free term $t = ft_1 \cdots t_l$ and consider $\psi = \exists x(x = t)$. By substitution, axiom $T' \vdash t = t \to \psi$. Hence, $T' \vdash \psi$. Thus, ψ must have occurred at some stage (e) in our construction, giving us a c_l such that $T^* \vdash c_l = t$. □

Remark 5.11.11. Let T be theory whose language has uncountably many constant symbols and no other non-logical symbols. Let $C \cup D$ be the set of all constant symbols, where C is uncountable, D is countably infinite and $C \cap D = \emptyset$. The axioms of T are formulas $c \neq c'$, where c and c' are distinct constant symbols belonging to C.

Let $p(x) = \{x \neq d : d \in D\}$. Clearly, $p(x)$ is a 1-type in T. Let $\varphi[x]$ be a formula consistent with T. Since only finitely many constants occur in φ, there is a $d \in D$ such that $\varphi[x] \wedge (x = d)$ is consistent with T. Thus, p is not isolated. As every model of T is uncountable, $p(x)$ is realized in every model of T.

Theorem 5.11.12. *Let T be a countable, consistent theory and $\{p_m\}$ a sequence of nonisolated n-types in T. Then there is a countable model of T that omits each p.*

This is proved by imitating the last proof with the following change. For each k of the form $2^q(2r+1)-1$ we ensure that there is a $\psi \in p_q$ such that $T[\varphi_{2k+2}] \vdash \neg\psi[a_r]$. This clearly can be done. The model M thus built will still be countable such that for each q and each r, there is a $\psi \in p_q$ such that $M \not\models \psi[a_r]$.

Proposition 5.11.13. *Let T be a countable, consistent, $\aleph_0$-categorical theory. Then every type in $S_n(T)$, $n \geq 1$, is isolated and, thus, finite.*

Proof. If possible, suppose there exists a $p \in S_n(T)$ that is not isolated. By Theorem 5.11.10, T has a countable model M that omits p. On the other hand, there is a countable model N of T that realizes p. But then M and N are not isomorphic. □

5.12 Relative Types

Let T be a complete theory with a countable language L, M a model of T, and $A \subset M$. Let L_A denote the language obtained from L by introducing a constant symbol i_a for each $a \in A$. We canonically treat M as a structure for L_A by interpreting each i_a by a, $a \in A$. A set of formulas $p = p[\overline{x}]$ of L_A with free variables among $\overline{x} = (x_0, \cdots, x_{n-1})$

is called an *n-type over A* if $p \cup Th_A(M)$ is satisfiable, where $Th_A(M)$ denotes the set of all closed L_A-formulas true in M. By the compactness theorem, p is an n-type over A if and only if each finite subset of $p \cup Th_A(M)$ is satisfiable.

An n-type p over A is called *complete* if for every formula $\varphi[\overline{x}]$ of L_A either φ or $\neg\varphi$ is in p. By Lindenbaum's theorem, each n-type over A is contained in a complete n-type over A.

Example 5.12.1. For $\overline{a} \in M^n$, we set

$$tp^M(\overline{a}/A) = \{\varphi[\overline{x}] : \varphi \text{ a formula of } L_A \ \wedge\ M \models \varphi[i_{\overline{a}}]\}.$$

Then $tp^M(\overline{a}/A)$ is a complete n-type over A.

We shall denote the set of all complete n-types over A by $S_n^M(A)$. For any formula $\varphi[\overline{x}]$, we set

$$[\varphi] = \{p \in S_n^M(A) : \varphi \in p\}.$$

We have the following identities:

$$[\neg\varphi] = S_n^M(A) \setminus [\varphi],$$

$$[\varphi \wedge \psi] = [\varphi] \cap [\psi],$$

and

$$[\varphi \vee \psi] = [\varphi] \cup [\psi].$$

As before, it is easy to see that $[\varphi]$ form a base of a topology on $S_n^M(A)$, which makes it a compact, Hausdorff, totally disconnected space. Further, if L and A are countable, then it is second countable and, thus, a compact, totally disconnected, metrizable space.

Example 5.12.2. Consider the linearly ordered set $\mathbb{Q}$ of rationals and $\overline{a}, \overline{b} \in \mathbb{Q}^n$. Then $tp^{\mathbb{Q}}(\overline{a}/\mathbb{N}) = tp^{\mathbb{Q}}(\overline{b}/\mathbb{N})$ if and only if there is an automorphism α of $\mathbb{Q}$ fixing $\mathbb{N}$ [i.e., $f(i) = i$ for all $i \in \mathbb{N}$] such that $\alpha(\overline{a}) = \overline{b}$.

To see this, suppose $tp^{\mathbb{Q}}(\overline{a}/\mathbb{N}) = tp^{\mathbb{Q}}(\overline{b}/\mathbb{N})$. Consider the map on $\mathbb{N} \cup \{a_i : i < n\}$ fixing $\mathbb{N}$ and mapping a_i to b_i, $i < n$. By our hypothesis, this map is an order-preserving injection. It is easy to prove that it can be extended to an order-preserving bijection $\mathbb{Q} \to \mathbb{Q}$. The converse is quite routine to prove.

Lemma 5.12.3. *Let $p \subset q \in S_n^M(A)$. Then $p = q$.*

Proof. If possible, suppose there exists a $\varphi \in q \setminus p$. But then $\neg\varphi \in p \subset q$. This contradicts that q is a type. □

For $p \in S_n^M(A)$ and $f : A \to N$ partial elementary, N a structure of L, we define

$$f(p) = \{\varphi[\overline{x}, i_{f(\overline{a})}] : \varphi[\overline{x}, i_{\overline{a}}] \in p\}.$$

Lemma 5.12.4. *Let $p \in S_n^M(A)$ and $f : A \to N$ be partial elementary. Then $f(p) \in S_n^N(f(A))$.*

Proof. We know that there exists an elementary extension M' of M in which p is realized. Thus, if $\varphi[\overline{x}, i_{\overline{a}}] \in p$, then $M' \models \exists \overline{x} \varphi[\overline{x}, i_{\overline{a}}]$. As M is an elementary substructure of M', $M \models \exists \overline{x} \varphi[\overline{x}, i_{\overline{a}}]$. Since $f : A \to N$ is partial elementary, $N \models \exists \overline{x} \varphi[\overline{x}, i_{f(\overline{a})}]$. Thus, there is a $\overline{b} \in N$ such that $N \models \varphi[i_{\overline{b}}, i_{\overline{a}}]$. Now it is easy to see that $f(p) \cup Th_N(f(A))$ is finitely satisfiable and, thus, satisfiable. Since p is complete, it is clear that $f(p)$ is complete. □

It should be noted that many of the results that we proved for types over $\emptyset$ hold, with essentially the same proof, for relative types also. In particular, we have the following proposition.

Proposition 5.12.5. *Let $A \subset M$, and let p be an n-type over A. Then there is an elementary extension N of M in which p is realized.*

Exercise 5.12.6. Prove the last result. Also show that if L and A are of cardinality $\leq \kappa$, then we can choose N so that $|N| \leq \kappa$.

Let $B \subset A \subset M$, and let $p[\overline{x}]$ be an n-type over A. We define the restriction $p|B$ of p to B as the set of all L_B-formulas that belong to p.

Proposition 5.12.7. *Let $B \subset A \subset M$. Then the map $p \to p|B$ from $S_n^M(A)$ to $S_n^M(B)$ is surjective.*

Proof. Given a $q \in S_n^M(B)$, we need to show that there is a $p \in S_n^M(A)$ such that $q = p|B$. By Proposition 5.12.5, there is an elementary extension N of M and an $\overline{a} \in N^n$ realizing q. Then $q = p|B$, where $p = tp^N(\overline{a}/A)$. □

As before, we call a $p[\overline{x}] \in S_n^M(A)$ *isolated by a formula* $\varphi[\overline{x}]$ of L_A if for every formula $\psi[\overline{x}]$ of L_A,

$$\psi[\overline{x}] \in p \Leftrightarrow M \models \forall \overline{x}(\varphi[\overline{x}] \to \psi[\overline{x}]).$$

Lemma 5.12.8. *Let $\varphi[\overline{x}]$ isolate p, and let $q[\overline{x}]$ be a complete n-type containing φ. Then $p = q$.*

Proof. Using our hypothesis, it is easy to check that $p \subset q$. □

Exercise 5.12.9. Let M and N be structures for a language L, $A \subset M$, $f : A \to N$ be partial elementary, and $p[\overline{x}]$ be a complete n-type over A isolated by, say, $\varphi[\overline{x}, i_{\overline{a}}]$, $\overline{a} \in A$. Show that $f(p) \in S_n^N(f(A))$ is isolated by $\varphi[\overline{x}, i_{f(\overline{a})}]$.

Exercise 5.12.10. Let $A \subset B \subset M$, M be a structure of L, $\overline{a}, \overline{b} \in M$. Show the following.

1. Suppose $\varphi[\overline{x}]$ is a formula of L_A that isolates $tp^M(\overline{a}/B)$. Then φ isolates $tp^M(\overline{a}/A)$.
2. If $tp^M(\overline{a}, \overline{b}/A)$ is isolated, then so is $tp^M(\overline{a}/\overline{b}, A)$.
3. $tp^M(\overline{a}, \overline{b}/A)$ is isolated if and only if $tp^M(\overline{b}/A)$ and $tp^M(\overline{a}/\overline{b}, A)$ are isolated.

Lemma 5.12.11. *Let κ be an infinite cardinal, L a κ-language, M a structure for L, $A \subset M$ of cardinality at most κ, and $|[\varphi[\overline{x}]]| > \kappa$. Then there is a formula $\psi[\overline{x}]$ of L_A such that $|[\varphi \wedge \psi]| > \kappa$ as well as $|[\varphi \wedge \neg\psi]| > \kappa$.*

Proof. Suppose not. Set

$$p = \{\psi : |[\varphi \wedge \psi]| > \kappa\}.$$

Note that $\varphi \in p$. Since $[\varphi] = [\varphi \wedge \psi] \cup [\varphi \cup \neg\psi]$, for each ψ, either ψ or $\neg\psi$ belongs to p. Thus, by our assumption, for every ψ exactly one of ψ, $\neg\psi$ belongs to p.

We claim that $p \cup Th_A(M)$ is finitely satisfiable. If not, then there exists $\psi_1, \cdots, \psi_k$ in p such that $\{\wedge_{i=1}^k \psi_i\} \cup Th_A(M)$ is not satisfiable. In particular, $\wedge_{i=1}^k \psi_i \notin p$. Hence, $\vee_{i=1}^k \neg\psi_i \in p$. But this implies that $|[\varphi \wedge \neg\psi_i]| > \kappa$ for some $1 \leq i \leq k$, a contradiction.

Thus, p is a complete n-type, and for every $\psi \notin p$, $|[\varphi \wedge \psi]| \leq \kappa$. Now note that

$$[\varphi] = \{p\} \cup \cup_{\psi \notin p} [\varphi \wedge \psi].$$

Since L and A are of cardinality at most κ, $|[\varphi]| \leq \kappa$. This contradiction proves our result. □

We now proceed to present an important dichotomy theorem involving types. The construction given below is also quite useful. We need to fix some notation. $2^{<\mathbb{N}}$ will denote the set of all finite sequences of 0s and 1s including the empty sequence e. For $s, t \in 2^{<\mathbb{N}}$ and $\varepsilon = 0, 1$, $|s|$ will denote the length of s, $s \prec t$ will mean that t extends s, and $s\,\varepsilon$ will denote the concatenation of s and ε.

Theorem 5.12.12. *Let T be a countable complete theory, $M \models T$, and $\kappa \geq \aleph_0$. Suppose there exists $A \subset M$ of cardinality κ such that $|S_n^M(A)| > \kappa$. Then there exists a countable $A_0 \subset A$ such that $|S_n^M(A_0)| = 2^{\aleph_0}$.*

Proof. Since $|A| = \kappa$ and T is countable, there are only κ-many formulas of L_A. Thus, there is a formula φ_e of L_A such that $|[\varphi_e]| > \kappa$.

We will now use Lemma 5.12.11 and for each $s \in 2^{<\mathbb{N}}$ we will define a formula φ_s of L_A satisfying the following conditions:

1. If $s \prec t$, then $T \vdash \varphi_t \to \varphi_s$.
2. $|[\varphi_s]| > \kappa$.
3. If $s \neq t$ and $|s| = |t|$, then $T[\varphi_s] \models \neg\varphi_t$.

Suppose φ_s is defined so that $|[\varphi_s]| > \kappa$. By Lemma 5.12.11, there is a formula ψ such that $|[\varphi_s \wedge \psi]|$ and $|[\varphi_s \wedge \neg\psi]|$ are greater than κ. Set $\varphi_{s\,0} = \varphi_s \wedge \psi$ and $\varphi_{s\,1} = \varphi_s \wedge \neg\psi$. Our construction is complete. We invite the reader to prove that φ_s have the foregoing properties.

For each $\alpha \in 2^{\mathbb{N}}$, by Lemma 5.11.4, $\cap_n [\varphi_{\alpha|n}] \neq \emptyset$. Choose and fix a $p_\alpha \in \cap_n [\varphi_{\alpha|n}]$. Suppose $\alpha \neq \beta \in 2^{\mathbb{N}}$. Obtain an n such that $\alpha|n \neq \beta|n$. Then $\varphi_{\alpha|n} \in p_\alpha \setminus p_\beta$.

Let A_0 be the set of all parameters from A that appear in φ_s. Clearly, A_0 is countable and all the p_α are complete n-types over A_0. In particular, $|S_n^M(A_0)| = 2^{\aleph_0}$. □

The set $S_n^M(A_0)$ obtained previously is homeomorphic to the Cantor set. We now obtain several results.

Theorem 5.12.13. *Let T be a countable, complete theory, with $M \models T$ and $A \subset M$ countable. Then exactly one of the following holds:*

1. $|S_n^M(A)| \leq \aleph_0$.
2. $|S_n^M(A)| = 2^{\aleph_0}$.

Remark 5.12.14. Our construction shows that if $S_n^M(A)$ is uncountable, then it contains a homeomorph of the Cantor set.

We say that *isolated types are dense* in $S_n^M(A)$ if for every formula φ of L_A such that $\{\varphi\} \cup Th_M(A)$ is satisfiable, there is an isolated type p containing φ. This is the same as saying that isolated points of $S_n^M(A)$ are dense in the topology of $S_n^M(A)$ generated by $\{[\varphi] : \varphi \text{ a formula of } L_A\}$.

Lemma 5.12.15. *Let $\varphi[\overline{x}]$ be consistent with $Th_A(M)$ and there is no isolated type p in $[\varphi]$. Then there exists a formula $\psi[\overline{x}]$ such that*

$$[\varphi \wedge \psi] \neq \emptyset \neq [\varphi \wedge \neg\psi].$$

Proof. Suppose for every ψ, $[\varphi \wedge \psi] \neq \emptyset$ implies $[\varphi \wedge \neg\psi] = \emptyset$. Set

$$p = \{\psi : M \models \forall\overline{x}(\varphi \rightarrow \psi)\}.$$

Then p is an n-type over A. Also, p is complete. Suppose not. Then there is a formula $\psi[\overline{x}]$ of L_A such that

$$M \not\models \forall\overline{x}(\varphi \rightarrow \psi) \;\&\; M \not\models \forall\overline{x}(\varphi \rightarrow \neg\psi).$$

This implies that both $\{\varphi \wedge \psi\} \cup Th_A(M)$ and $\{\varphi \wedge \neg\psi\} \cup Th_A(M)$ are satisfiable. Hence,

$$[\varphi \wedge \psi] \neq \emptyset \neq [\varphi \wedge \neg\psi],$$

a contradiction.

Clearly, p is isolated by φ and $\varphi \in p$. This contradiction proves the result. □

In the preceding theorem, since $[\varphi]$ contains no isolated type, none of $[\varphi \wedge \psi]$ or $[\varphi \wedge \neg\psi]$ contains an isolated type.

Theorem 5.12.16. *Let T be a countable, complete theory, $M \models T$ and $A \subset M$. Suppose isolated types are not dense in $S_n^M(A)$. Then there exists a countable $A_0 \subset A$ such that $|S_n^M(A_0)| = 2^{\aleph_0}$. Further, if isolated types are dense in $S_n^M(A)$, the $S_n^M(A)$ must be countable.*

Proof. Let φ_e be an L_A formula such that $[\varphi_e] \neq \emptyset$ and contains no isolated type. We now use Lemma 5.12.15 and follow the same method to get our result. □

Remark 5.12.17. Suppose $A \subset M$ is countable and $|S_n^M(A)| < 2^{\aleph_0}$. Then isolated types are dense in $S_n^M(A)$.

In the remaining part of this chapter we show the importance of types in model theory.

5.13 Prime and Atomic Models

A model M of a theory T is called a *prime model of* T if for every model N of T there is an elementary embedding $\alpha : M \to N$. By model completeness, we get the following examples.

Example 5.13.1.
1. The field of algebraic numbers is a prime model of $ACF(0)$. To see this, note that the field of algebraic numbers is a submodel of every algebraically closed field of characteristic zero. Since $ACF(0)$ admits elimination of quantifiers, it follows that the field of algebraic numbers is an elementary substructure of every algebraically closed field of characteristic zero.
2. The algebraic closure of the field F_p of integers modulo p is a prime model of $ACF(p)$, with p a prime.
3. The field of real algebraic numbers is a prime model of RCF.

Exercise 5.13.2. Give examples of prime models of the theories DLO, DAG, and $ODAG$.

Also note that any two prime models of the preceding theories are isomorphic.

Exercise 5.13.3. Show that every prime model of a countable, consistent theory is countable.

Proposition 5.13.4. *A theory T with prime models must be complete.*

Proof. Let M be a prime model of a theory T, $N \models T$, and φ a sentence. Suppose $M \models \varphi$. Since M is elementarily embedded in N, $N \models \varphi$. By the completeness theorem, $T \vdash \varphi$. Similarly, if $M \models \neg\varphi$, then $T \vdash \neg\varphi$. Thus, T is complete. □

A model M of T is called a *minimal model* if it has no proper elementary submodel. Prime models of ACF, RCF, DAG, and $ODAG$ are minimal. On the other hand, consider $M \models DLO$. Then M has $\mathbb{Q}$ as an elementary submodel. Further, $\mathbb{Q} \setminus \{0\}$ is also an elementary submodel. This shows that DLO has no minimal model and that a prime model need not be minimal.

Proposition 5.13.5. *The standard model $\mathbb{N}$ of the theory N is a prime model of $Th(\mathbb{N})$ and an initial segment of every model $M \models Th(\mathbb{N})$.*

Proof. Let $M \models Th(\mathbb{N})$. Using that M is a model of the theory N, it is easy to check that $\mathbb{N}$ is an initial segment of M: let $a \in M \setminus \mathbb{N}$. By induction on $n \in \mathbb{N}$, we show that $M \models \underline{n} < i_a$. This is the same as showing that $M \models i_n < i_a$ for all $n \in \mathbb{N}$.

Let $i : \mathbb{N} \hookrightarrow M$ be the inclusion map. We claim that i is an elementary embedding. To see this, take a formula $\varphi[i_{\overline{n}}]$ of $L_{\mathbb{N}}$, $\overline{n} = (n_0, \cdots, n_{k-1}) \in \mathbb{N}^k$. Now consider the sentence $\varphi[\underline{n_0}, \cdots, \underline{n_{k-1}}]$ of $L_{\mathbb{N}}$. Since $Th(\mathbb{N})$ is complete, M and $\mathbb{N}$, being models of $Th(\mathbb{N})$, are elementarily equivalent. In particular,

$$\mathbb{N} \models \varphi[\underline{n}] \Leftrightarrow M \models \varphi[\underline{n}].$$

This is the same as

$$\mathbb{N} \models \varphi[i_{\overline{n}}] \Leftrightarrow M \models \varphi[i_{\overline{n}}].$$

Our result is proved. □

Are prime models of a complete theory isomorphic? For a countable theory, yes. We proceed to show this now.

We call a model M of a theory T *atomic* if for every $\overline{a} \in M$, $tp^M(\overline{a})$ is isolated.

Example 5.13.6. Let M be a structure for a language L. When considered as a structure for L_M, M is atomic. Indeed, if $\overline{a} \in M^n$, then the formula $\wedge_{i=1}^n (x_i = i_a)$ isolates $tp^M(\overline{a}/M)$.

Example 5.13.7. The standard model $\mathbb{N}$ of arithmetic is atomic. Indeed, if $\overline{k} \in \mathbb{N}^n$, then the formula $\wedge_{j=1}^n (x_j = S^{k_j}0)$ isolates $tp^{\mathbb{N}}(\overline{k})$.

Exercise 5.13.8. Show that the ordered field of real algebraic numbers is atomic.

Exercise 5.13.9. Show that the field of all algebraic numbers is atomic.

Example 5.13.10. Consider the ordered field of all real numbers $\mathbb{R}$. For $a < b \in \mathbb{R}$, there exists an $m \in \mathbb{Z}$ and a positive integer n such that $n \cdot a < m < n \cdot b$. But then $\underline{n} \cdot x < \underline{m} \in tp^{\mathbb{R}}(a)$, but not in $tp^{\mathbb{R}}(b)$. Since there are only countably many formulas, there are only countably many isolated types. It follows that the ordered field of real numbers is not atomic.

Exercise 5.13.11. Let $M \models DLO$ and $\overline{a}, \overline{b} \in M^n, n \geq 1$. Show the following:

1. $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if there is a permutation π of n such that $a_{\pi(0)} < \cdots < a_{\pi(n-1)}$ as well as $b_{\pi(0)} < \cdots < b_{\pi(n-1)}$.
2. Show that M is atomic.

Proposition 5.13.12. *Every countable atomic model M of T is homogeneous.*

Proof. Let $\overline{a}, \overline{b} \in M^n$ such that the map $\overline{a} \to \overline{b}$ is partial elementary. Take an $a \neq a_i$, $i < n$. Since M is atomic, there is a formula $\varphi[x_0, \cdots, x_n]$ that isolates $tp^M(\overline{a}, a)$. In particular, $M \models \varphi[i_{\overline{a}}, i_a]$, implying $M \models \exists x \varphi[i_{\overline{a}}, x]$. Since $\overline{a} \to \overline{b}$ is partial elementary, $M \models \exists x \varphi[i_{\overline{b}}, x]$. Hence, there is a $b \in M$ such that

$$M \models \varphi[i_{\overline{b}}, i_b]. \qquad (*).$$

We extend $\overline{a} \to \overline{b}$ to $\{a_0, \cdots, a_{n-1}, a\}$ by sending a to b. Since φ isolates $tp^M(\overline{a}, a)$, it follows that

$$tp^M(\overline{a}, a) = tp^M(\overline{b}, b).$$

[This will imply that $(\overline{a}, a) \to (\overline{b}, b)$ is partial elementary.] To see this, let $\psi[\overline{x}, x] \in tp^M(\overline{a}, a)$. Then

$$T \vdash \forall \overline{x} \forall x(\varphi[\overline{x}, x] \to \psi[\overline{x}, x]).$$

By $(*)$, $M \models \psi[i_{\overline{b}}, i_b]$, i.e, $\psi \in tp^M(\overline{b}, b)$. The reverse inclusion is proved similarly. Our proof is complete. □

Theorem 5.13.13. *Let T be a countable complete theory. Then a model M of T is prime if and only if M is countable and atomic.*

Proof. Let M be a prime model of T. By Exercise 5.13.3, M is countable.

Take any $\overline{a} \in M$. If possible, suppose $tp^M(\overline{a})$ is nonisolated. By Theorem 5.11.10, there is a model N of T omitting $tp^M(\overline{a})$. Since M is prime, there is an elementary embedding $\alpha : M \to N$. However, as $\alpha : M \to N$ is elementary, $\alpha(\overline{a})$ realizes $tp^M(\overline{a})$. This contradiction proves the *only if* part of the result.

To prove the converse, let M be a countable atomic model of T and $N \models T$. Fix an enumeration $\{a_k\}$ of M. Since M is atomic, for each $(a_0, \cdots, a_k)$, there is a formula $\varphi_k[x_0, \cdots, x_k]$ that isolates $tp^M(a_0, \cdots, a_k)$. By induction, for each k, we shall define a partial elementary map $\alpha_k : \{a_i : i < k\} \to N$ such that α_{k+1} extends α_k for each k. It will follow that $\alpha = \cup_k \alpha_k : M \to N$ is elementary.

Since T is complete, M and N are elementarily equivalent. Thus, the empty function from M to N is indeed elementary. Suppose $\alpha_k : \{a_i : i < k\} \to N$ has been defined and is partial elementary.

Since $M \models \varphi_k[i_{a_o}, \cdots, i_{a_k}]$, $M \models \exists x \varphi_k[i_{a_0}, \cdots, i_{a_{k-1}}, x]$. Since α_k is partial elementary, we get $N \models \exists x \varphi_k[i_{\alpha_k(a_0)}, \cdots, i_{\alpha_k(a_{k-1})}, x]$. This gives us a $b \in N$ such that $N \models \varphi_k[i_{\alpha_k(a_0)}, \cdots, i_{\alpha_k(a_{k-1})}, i_b]$. We let $\alpha_{k+1} : \{a_i : i \leq k\} \to N$ to be the extension of α_k with $\alpha_{k+1}(a_k) = b$. We need to show that α_{k+1} is partial elementary. Because φ_k isolates $tp^M(a_0, \cdots, a_k)$, as we argued earlier,

$$tp^M(a_0, \cdots, a_k) = tp^N(\alpha_{k+1}(a_0), \cdots, \alpha_{k+1}(a_k)),$$

showing that α_{k+1} is partial elementary. □

Theorem 5.13.14. *Let T be a countable complete theory and M and N prime models of T. Then M and N are isomorphic.*

Proof. By Theorem 5.13.13, M and N are countable and atomic. Therefore, each realized type in M and N is isolated, implying that they realize the same complete types. By Proposition 5.13.12, M and N are homogeneous. Hence, by Proposition 2.6.6, M and N are isomorphic. □

Proposition 5.13.15. *Let T be a complete theory. If T has an atomic model, isolated types are dense in $S_n(T)$.*

Proof. Fix an atomic $M \models T$. Suppose $[\varphi[\overline{x}]] \neq \emptyset$. Then there is a model $N \models T$ such that $N \models \exists \overline{x} \varphi$. Since T is complete, $M \models \exists \overline{x} \varphi$. Thus, there exists $\overline{a} \in M$ such that $M \models \varphi[i_{\overline{a}}]$. Thus, $tp^M(\overline{a}) \in [\varphi]$. Since M is atomic, $tp^M(\overline{a})$ is isolated, and our result is proved. □

Interestingly, the converse of this result is true if, moreover, T is countable.

Theorem 5.13.16. *Let T be a countable complete theory such that for every $n \geq 1$, isolated types are dense in $S_n(T)$. Then T has an atomic model.*

Proof. We add an infinite sequence of distinct symbols to T and still call the theory T. Enumerate all the constant symbols, say $\{c_n\}$. Let $\{\varphi_n\}$ be an enumeration of all the sentences.

By induction on n, we shall now define a sequence of sentences $\{\psi_n\}$ such that $T[\{\psi_n\}]$ is a complete Henkin theory whose canonical structure is a countable atomic model of T.

We take $\psi_0 = \exists x(x = x)$. Suppose $n = 3m$ and $\psi_0, \cdots \psi_n$ have been defined.

If $T[\psi_n \wedge \varphi_m]$ is satisfiable, then we take $\psi_{n+1} = \psi_n \wedge \varphi_m$, else set $\psi_{n+1} = \psi_n \wedge \neg\varphi_m$. Note that $T[\psi_{n+1}]$ is consistent.

Let φ_m be a closed existential formula, say $\exists x \varphi[x]$. If $T[\psi_{n+1}] \nvdash \varphi_m$, then take $\psi_{n+2} = \psi_{n+1}$. Otherwise, we take the first new constant symbol c_k not occurring in $T[\psi_{n+1}]$ and set $\psi_{n+2} = \psi_{n+1} \wedge \varphi_n[i_{c_k}]$. Arguing as in the proof of the omitting-types theorem, we see that $T[\psi_{n+2}]$ is consistent.

Finally, let k be the first integer such that the constants occurring in ψ_{n+2} are among $c_0, \cdots, c_k$. By choosing a variant of ψ_{n+2}, if necessary, let $\psi[x_0, \cdots, x_k]$ be such that $\psi_{n+2} = \psi[\overline{c}]$. Thus, $[\psi] \neq \emptyset$. Let $p \in [\psi]$ be an isolated $(k+1)$-type, isolated by, say, $\eta[\overline{x}]$. We set $\psi_{n+3} = \psi_{n+2} \wedge \eta$. Clearly, $T[\psi_{n+3}]$ is satisfiable.

It is fairly routine to check that $T[\{\psi_n\}]$ is a complete Henkin theory. Let M be its canonical model. We claim that M is an atomic model of T. Take $\overline{a} \in M$. Let k be the least integer such that all a_i occur among $(c_0)_M, \cdots, (c_k)_M$ and there exists an $m = 3j + 2$ such that all the constants occurring in ψ_m occur among $c_0, \cdots, c_k$. By our construction, $tp^M[\overline{c_M}]$ is isolated. Hence, $tp^M(\overline{a})$ is isolated by Proposition 5.11.8. □

Corollary 5.13.17. *Let T be a countable, complete theory such that for some $n \geq 1$, $|S_n(T)| < 2^{\aleph_0}$. Then T has a prime model.*

Proof. Let $M \models T$. Since T is complete, $S_n(T) = S_n^M(\emptyset)$. By our hypothesis and Theorem 5.12.16, isolated points are dense in $S_n(T)$. By Theorem 5.13.16, T has an atomic model. The result now follows from Theorem 5.13.13. □

5.14 Saturated Models

Let κ be an infinite cardinal and $M \models T$. We say that M is κ-*saturated* if for every $A \subset M$ of cardinality less than κ, every type over A is realized in M. Since every type

is contained in a complete type, $|M|$ is κ-saturated if and only if all complete types over A, $|A| < \kappa$, are realized in M. We call $M \models T$ *saturated* if it is $|M|$-saturated.

Theorem 5.14.1. *Let M and N be models of T with $N\kappa$-saturated, $A \subset M$ of cardinality less than κ, $f : A \to N$ partial elementary, and $a \in M \setminus A$. Then there is a partial elementary map $g : A \cup \{a\} \to N$ that extends f.*

Proof. Take any $\overline{a} \in A^n$ and a formula $\varphi[x,\overline{x}]$ of L such that $M \models \varphi[i_a, i_{\overline{a}}]$. Then $M \models \exists x \varphi[x, i_{\overline{a}}]$. Since f is partial elementary, $N \models \exists x \varphi[x, i_{f(\overline{a})}]$. From this it easily follows that

$$p = \{\varphi[x, i_{f(\overline{a})}] : \overline{a} \in M^n \wedge M \models \varphi[i_a, i_{\overline{a}}]\}$$

is finitely satisfiable in N, i.e., p is a 1-type over $f(A)$, which is, of course, of cardinality less than κ. Since N is κ-saturated, there is a $b \in N$ that realizes it. This implies that $tp^M(a,\overline{a}) = tp^N(b, f(\overline{a}))$. Thus, $g = f \cup \{(a,b)\}$ is partial elementary. This proves our result. □

Corollary 5.14.2. *Every κ-saturated model of T is κ-homogeneous.*

Example 5.14.3. Let $\mathbb{Q}$ and $\mathbb{R}$ have the usual order and $M = \mathbb{Q} \times \mathbb{R}$ in lexicographic order. Thus,

$$(r,a) < (s,b) \Leftrightarrow r < s \ \vee \ (r = s \ \wedge \ a < b).$$

Then $M \models DLO$. Now take $A = \{0\} \times \mathbb{Q} \subset M$ and $f : A \to M$ defined by

$$f(0,r) = (r,0), \ \ r \in \mathbb{Q}.$$

Then $f : A \to M$ is an embedding. Since DLO admits elimination of quantifiers, f is elementary. Take $b = (1,0) \in M$. Then $a < b$ for every $a \in A$. But $f(A)$ is unbounded above. Hence, f cannot be extended as an order-preserving injection from $A \cup \{b\} \to M$. This shows that M is not homogeneous. Hence, M is not saturated.

It is worth noting that we only used that 1-types are realized. Here is a result explaining this.

Proposition 5.14.4. *Let $M \models T$ be such that for every $A \subset M$ of cardinality less than κ, $\kappa \geq \aleph_0$, every 1-type over A is realized in M. Then M is κ-saturated.*

Proof. By induction on n, we show that every complete n-type over $A \subset M$, $|A| < \kappa$, is realized in M. For $n = 1$ this is our hypothesis. Now let $n > 1$ and take a complete n-type $p(\overline{x})$ over $A \subset M$ of cardinality less than κ, and consider

$$q = \{\varphi[x_0, \cdots, x_{n-2}] : \varphi \in p\}.$$

Clearly, q is an $(n-1)$-type over A. Suppose there exists an $\overline{a} \in M^{n-1}$ that realizes q. Now consider the 1-type

$$r = \{\psi[i_{\overline{a}}, x_{n-1}] : \psi[\overline{x}] \in p\}$$

over $A \cup \{a_i : i < n-1\}$. Since κ is infinite, $|A \cup \{a_i : i < n-1\}| < \kappa$. Hence, by our hypothesis, there exists an a_{n-1} that realizes r. Plainly, $(a_0, \cdots, a_{n-1})$ realizes p. □

Proposition 5.14.5. *Let T be a complete theory, $M \models T$ κ-saturated, $\kappa \geq \aleph_0$, and $N \models T$ with $|N| \leq \kappa$. Then N can be elementarily embedded in M.*

Proof. Fix an enumeration $\{x_\alpha : \alpha < \kappa\}$ of the elements of N. For $\alpha < \kappa$, set $A_\alpha = \{x_\beta : \beta < \alpha\}$.

Set f_0 to be the empty function. Proceeding by induction and using Theorem 5.14.1, for each $\alpha < \kappa$, we get a partial elementary map $f_\alpha : A_\alpha \to M$ such that f_α extends f_β whenever $\beta < \alpha$ and $f_\alpha = \cup_{\beta<\alpha} f_\beta$ if α is a limit ordinal.

Plainly, $f = \cup_{\alpha<\kappa} f_\alpha : N \to M$ is an elementary embedding. □

The converse of this result is true for countable theories.

Proposition 5.14.6. *Let T be a countable complete theory and κ an infinite cardinal. Suppose M is a κ-homogeneous model of T such that every model N of T of cardinality $\leq \kappa$ is elementarily embedded in M. Then M is κ-saturated.*

Proof. Take any $A \subset M$ of cardinality less than κ and a $p \in S_1^M(A)$. By Proposition 5.14.4, it is sufficient to prove that p is realized in M. By Proposition 5.12.5, get an elementary extension N of M that realizes p, say, by a. We can choose N so that $|N| \leq \kappa$. By our hypothesis, there is an elementary map $f : N \to M$. Plainly, $f(a) \in M$ realizes p. □

Remark 5.14.7. In the final result, if κ is uncountable, then it is sufficient to assume that every model of cardinality less than κ is elementarily embedded in M. This is because by the downward Löwenheim–Skolem theorem, we can have $|N| < \kappa$.

Exercise 5.14.8. Show that $\mathbb{Q} \models DLO$ is saturated.

Exercise 5.14.9. Show that every uncountable, algebraically closed field is saturated.

Exercise 5.14.10. Let $\mathbb{F}$ be a countable, algebraically closed field of characteristic 0 and transcendence degree $\aleph_0$. Show that $\mathbb{F}$ is saturated.

Proposition 5.14.11. *Let T be a countable complete theory and $M \models T$. The following conditions are equivalent.*

(1) *M is $\aleph_0$-saturated.*
(2) *The model M is $\aleph_0$-homogeneous and realize every complete type in T.*

Proof. That (1) implies (2) follows from Proposition 5.14.2 and the definition of saturated models.

We now prove that (2) implies (1). Let $M \models T$ satisfy condition (2). Take any $\overline{a} \in M^n$ and a complete m-type $p[\overline{x}]$ over $\overline{a}$. Consider

$$q = \{\varphi[\overline{x}, \overline{y}] : \varphi[\overline{x}, i_{\overline{a}}] \in p\}.$$

It is easily seen that $q \in S_{m+n}(T)$. By our hypothesis, there exists a $(\overline{b},\overline{c}) \in M^m \times M^n$ that realizes it. In particular, $tp^M(\overline{a}) = tp^M(\overline{c})$, i.e., $\overline{a} \to \overline{c}$ is partial elementary. Since M is assumed to be $\aleph_0$-homogeneous, we get a $\overline{d} \in M^m$ such that $(\overline{b},\overline{c}) \to (\overline{d},\overline{a})$ is partial elementary, i.e., $tp^M((\overline{d},\overline{a})) = tp^M((\overline{b},\overline{c}))$. This implies that $\overline{d}$ realizes p, proving our result. □

Here is an important consequence of this result on saturated models.

Proposition 5.14.12. *Any two countable saturated models of T are isomorphic.*

Proof. Let M and N be countable saturated models of T. By Proposition 5.14.11, M and N are homogeneous and realize the same complete types in T. The result now follows from Proposition 2.6.6. □

Using Theorem 5.14.1, we can generalize this result for all $\kappa \geq \aleph_0$.

Theorem 5.14.13. *Let M and N be saturated models of T. Then M and N are isomorphic if and only if $|M| = |N|$.*

Proof. We need to prove the *if* part only. Fix enumerations $M = \{a_\alpha : \alpha < \kappa\}$ and $N = \{b_\alpha : \alpha < \kappa\}$. Consider $p[x] = tp^M(a_0)$. Since N is saturated, there is a $b \in N$ that realizes it. We let $a'_0 = a_0$ and $b'_0 \in N$ to be the first element in the preceding enumeration of B such that $tp^M(a'_0) = tp^N(b'_0)$. Then $a'_0 \to b'_0$ is partial elementary.

Suppose for $0 < \alpha < \kappa$, $\{a'_\beta \in M : \beta < \alpha\}$, and $\{b'_\beta \in N : \beta < \alpha\}$ have been defined such that for every $\beta < \alpha$, $(a'_\gamma : \gamma < \beta) \to (b'_\gamma : \gamma < \beta)$ is partial elementary. If α is a limit ordinal, then $(a'_\beta : \beta < \alpha) \to (b'_\beta : \beta < \alpha)$ is partial elementary.

Suppose α is an odd successor ordinal, say $\beta + 1$. Let b'_α be the first element in the enumeration of N different from b'_γ, $\gamma < \alpha$. By our assumption, $(b'_\gamma : \gamma < \beta) \to (a'_\gamma : \gamma < \beta)$ is partial elementary. Since M is κ-saturated, by Theorem 5.14.1, there is an $a \in M$ such that $(b'_\gamma : \gamma \leq \alpha) \to ((a'_\gamma : \gamma < \alpha), a)$ is partial elementary. We let a'_α denote first such a in the enumeration of M.

If α is an even successor ordinal order, we take a'_α as the first element in the enumeration of M different from a'_γ, $\gamma < \alpha$. Since N is κ-saturated, by Theorem 5.14.1, there is a $b \in B$ such that $(a'_\gamma : \gamma' \leq \alpha) \to ((b'_\gamma, \gamma < \alpha), b)$ is partial elementary. We let $b_{\alpha'}$ be the first such element in the foregoing enumeration of B.

Thus, we have defined enumerations $M = \{a'_\alpha : \alpha < \kappa\}$ and $N = \{b'_\alpha : \alpha < \kappa\}$ such that for every $\alpha < \kappa$, $(a'_\beta : \beta < \alpha) \to (b'_\beta : \beta < \alpha)$ is partial elementary. It follows that $(a'_\beta : \beta < \kappa) \to (b'_\beta : \beta < \kappa)$ is an isomorphism from M to N. □

Here is a useful variant of Proposition 5.14.11.

Proposition 5.14.14. *Let M and N be elementarily equivalent models of a theory T with N κ-homogeneous, κ an infinite cardinal. Suppose for every $\overline{a} \in M^n$ there exists $\overline{b} \in N^n$ such that $tp^M(\overline{a}) = tp^N(\overline{b})$. Then for every $A \subset M$ with $|A| \leq \kappa$, there is a partial elementary map $f_\infty : A \to N$.*

Proof. First assume that A is finite, say $A = \{a_0, \cdots, a_n\}$. By our hypothesis, there exist $b_0, \cdots, b_n \in B$ such that $tp^M(\overline{a}) = tp^N(\overline{b})$. Plainly, $a_i \to b_i$, $i \leq n$, is an elementary map from A into N.

We complete the proof by induction on $|A|$. Let $\lambda \leq \kappa$ and the result be true for $A \subset M$ of cardinality less than λ. Take any $A = \{a_\alpha : \alpha < \lambda\} \subset M$ of cardinality λ. By induction on $\alpha < \lambda$, we define elementary maps $f_\alpha : \{a_\beta : \beta < \alpha\} \to N$ such that f_α extends f_β whenever $\beta < \alpha$. This will then complete the proof by taking $f = \cup_{\alpha<\lambda} f_\alpha$.

Suppose $\alpha < \lambda$ and f_β, $\beta < \alpha$, have been defined. If α is a limit ordinal, we define $f_\alpha = \cup_{\beta<\alpha} f_\beta$. Now suppose $\alpha = \beta + 1$ to be a successor ordinal. By our assumption, there is a partial elementary map $f : \{a_\gamma : \gamma \leq \beta\} \to N$. Let $B = f(\{a_\gamma : \gamma < \beta\})$, and let C be the range of f_β. Note that every partial elementary map is injective. Thus, we have a partial elementary map $g = f_\beta \circ f^{-1} : B \to C$. Since N is κ-homogeneous, there is a partial elementary map $h : B \cup \{f(a_\beta)\} \to N$. Suppose $b = h(f(a_\beta))$. Then $f_\alpha = f_\beta \cup \{(a_\beta, b)\}$ is partial elementary. □

Corollary 5.14.15. *If a model M of T is κ-homogeneous and realizes all types in $S_n(T)$, $n \geq 1$, then M is κ-saturated.*

Proof. Let $N \models T$ be of cardinality $\leq \kappa$. By Proposition 5.14.6, it is sufficient to show that there is an elementary embedding $\alpha : N \to M$. But this follows from Proposition 5.14.14. □

Using the back-and-forth method, we now prove the following theorem.

Theorem 5.14.16. *Let T be a countable complete theory and $M, N \models T$ homogeneous. Then M and N are isomorphic if and only if $|M| = |N|$ and they realize the same types.*

Proof. We need to prove the *if* part only. Let $|M| = |N| = \kappa$, and let them realize the same types. Fix enumerations $M = \{a_\alpha : \alpha < \kappa\}$ and $N = \{b_\alpha : \alpha < \kappa\}$. Set f_0 to be the empty function.

By induction, we define partial elementary maps $f_\alpha, \alpha < \kappa$, as follows: assume f_α have been defined. Let a be the first element in the preceding enumeration of M that does not belong to the domain of f_α. By Proposition 5.14.14, there is a partial elementary map, say $g = f_\alpha \cup \{(a, b)\}$, into N. Now let b be the first element of N not in the range of g. By Proposition 5.14.14 again, there is a partial elementary map, say $h = g^{-1} \cup \{(b, a)\}$, into M. We take $f_{\alpha+1} = h^{-1}$. In the limit case, we take $f_\alpha = \cup_\beta f_\beta$.

Plainly, $f = \cup_{\alpha<\kappa} f_\alpha$ is an isomorphism from M onto N. □

Theorem 5.14.17. *A countable complete theory T has a countable saturated model if and only if $S_n(T)$ is countable for each $n \geq 1$.*

Proof. If T has countable saturated M, each $p \in S_n(T)$ is $tp^M(\overline{a})$ for some $\overline{a} \in M^n$. Thus, $S_n(T)$ is countable for each $n \geq 1$.

For the converse, fix an enumeration $\{p_k\}$ of $\cup_n S_n(T)$. Let M_0 be a countable model of T. By induction, we define a sequence of countable models M_n of T satisfying the following conditions:

1. M_{i+1} is an elementary extension of M_i.
2. p_i is realized in M_{i+1}.

This can be done by repeatedly applying Remark 5.6.5. It is easy to see that $M = \cup_n M_n$ is a countable saturated model of T. □

Proposition 5.14.18. *If a countable complete theory T has a countable saturated model, it has a prime model.*

Proof. Since T has a countable saturated model M, it has only countably many complete types. The result now follows from Corollary 5.13.17. □

Proposition 5.14.19. *If a countable complete theory T has fewer than $2^{\aleph_0}$-many nonisomorphic countable models, then T has a countable saturated model.*

Proof. Suppose for some $n \geq 1$, T has uncountably many complete n-types. Then by Theorem 5.12.13, $|S_n(T)| = 2^{\aleph_0}$. Now a countable model can realize only countably many complete types and isomorphic models realize the same types. It follows that T has at least $2^{\aleph_0}$-many nonisomorphic, countable models. The proof is complete. □

We now proceed to prove a result on the existence of saturated models. Assume that T is a countable, consistent theory.

Lemma 5.14.20. *Given any model $M \models T$ and $\kappa \geq \aleph_0$, there is an elementary extension N of M of cardinality $\leq |M|^\kappa$ that realizes every complete 1-type $p \in S_1^M(A)$ over subsets A of M of cardinality $\leq \kappa$.*

Proof. An easy cardinality argument implies that there are at most $|M|^\kappa$-many complete 1-types over subsets A of cardinality $\leq \kappa$. Thus, let $\{p_\alpha : \alpha < |M|^\kappa\}$ be an enumeration of all complete 1-types over subsets of M of cardinality $\leq \kappa$.

By induction on $\alpha < |M|^\kappa$, we define models $N_\alpha \models T$ satisfying the following conditions:

1. $N_0 = M$.
2. $|N_\alpha| \leq |M|^\kappa$.
3. $N_\alpha = \cup_{\beta<\alpha} N_\beta$ if α limit.
4. $N_{\alpha+1}$ is an elementary extension of N_α realizing p_α.

Now take $N = \cup_{\alpha<|M|^\kappa} N_\alpha$. □

By iterating this lemma, we now have the following theorem.

Theorem 5.14.21. *Under the hypothesis of the last lemma, there is a κ^+-saturated, elementary extension N of M of cardinality $\leq |M|^\kappa$.*

Proof. By iterating the last lemma, we have $N_\alpha \models T$, $\alpha < \kappa^+$, satisfying

1. $N_0 = M$;
2. $N_\alpha = \cup_{\beta<\alpha} N_\beta$ if α limit ordinal;
3. $N_{\alpha+1}$ is an elementary extension of N_α such that for every $A \subset N_\alpha$ of cardinality at most κ, every $p \in S_1^{N_\alpha}(A)$ is realized in $N_{\alpha+1}$;
4. $|N_\alpha| \leq |M|^\kappa$.

Now take $N = \cup_{\alpha<\kappa^+} N_\alpha$. Then N is an elementary extension of M with $|N| \leq |M|^\kappa$. That N is κ^+-saturated can be seen from the fact that every $A \subset N$ of cardinality $\leq \kappa$ must be contained in some N_α. □

Corollary 5.14.22. *Assume the generalized continuum hypothesis: $\forall \kappa \geq \aleph_0 (2^\kappa = \kappa^+)$. Suppose T is a countable, consistent theory. Then for every $\kappa \geq \aleph_0$, T has a saturated model of size κ^+.*

(Start with a countable $M \models T$.)

Here is an application to elimination of quantifiers.

Theorem 5.14.23. *Let T be a theory with a constant symbol. Then T admits elimination of quantifiers if and only if, when $M \models T$, with A a substructure of M, $N \models T$ $|M|^+$-saturated, and $f : A \to N$ an embedding, f admits an elementary extension $g : M \to N$ of f.*

Proof. We prove the *if* part first. Suppose $M, N \models T$, with A a common substructure of M, N, $\varphi[x, \bar{y}]$ open, $\bar{a} \in A$, and $M \models \exists x \varphi[x, i_{\bar{a}}]$. By Theorem 5.7.3, it is sufficient to prove that $N \models \exists x \varphi[x, i_{\bar{a}}]$.

By Theorem 5.14.21, there is an $|M|^+$-saturated elementary extension N' of N. Thus, by our hypothesis, there is an elementary embedding $g : M \to N'$ that extends the inclusion map $A \hookrightarrow N \subset N'$. Hence, $N' \models \exists x \varphi[x, i_{\bar{a}}]$. Since N is an elementary substructure of N', $N \models \exists x \varphi[x, i_{\bar{a}}]$.

Conversely, suppose T admits elimination of quantifiers, $M \models T$ and where A is a substructure of M, $N \models T$ $|M|^+$-saturated and $f : A \to N$ is an embedding. By elimination of quantifiers, f is partial elementary. Since N is $|M|^+$-saturated, as before, there is an elementary extension $g : M \to N$ of f. □

5.15 Stable Theories

We now introduce a very important class of theories – stable theories.

Let T be a countable complete theory and κ an infinite cardinal. We call T *κ-stable* if, when $M \models T$, $A \subset M$ of cardinality κ, $|S_n^M(A)| = \kappa$. If $\kappa = \aleph_0$, then κ-stable theories are traditionally called ω-stable. A structure M of a countable language L is called κ-stable if Th_M is κ-stable.

By Theorem 5.12.12, we have the following theorem.

Theorem 5.15.1. *Every ω-stable theory is κ-stable for every $\kappa \geq \aleph_0$.*

Theorem 5.15.2. *Let T be a countable, complete, ω-stable theory, with $M \models T$ and $A \subset M$. Then the isolated types are dense in $S_n^M(A)$.*

Proof. If isolated types are not dense in $S_n^M(A)$, then, by Theorem 5.12.16, there is a countable $A_0 \subset A$ such that $|S_n^M(A_0)| = 2^{\aleph_0}$. This contradicts that T is ω-stable. □

Example 5.15.3. Consider $\mathbb{R} \models RCF$. We saw earlier that for $a \neq b \in \mathbb{R}$, $tp^{\mathbb{R}}(a/\emptyset) \neq tp^{\mathbb{R}}(b/\emptyset)$. Thus, $|S_1^{\mathbb{R}}(\emptyset)| = 2^{\aleph_0}$. This implies that RCF is not ω-stable.

Example 5.15.4. Consider the theory DLO. Thus, let $(M, <) \models DLO$ and $\emptyset \neq A \subset M$.

Let $p \in S_1^M(A)$. Since p is a complete 1-type, for each $a \in A$, exactly one of the formulas $x < a$, $x = a$, $a < x$ belongs to p.

If for some $a \in A$, $x = a$ is in p, then, by completeness, $p = \{\varphi[x] : M \models \varphi[i_a]\}$. Thus, in this case, p is isolated by $x = a$ and also realized by a. Note that these are all the $p \in S_1^M(A)$ realized in A.

Thus, assume that $p \in S_1^M(A)$ is not realized by any $a \in A$. Set

$$L_p = \{a \in A : a < x \in p\} \ \& \ U_p = \{b \in A : x < b \in p\}.$$

Then $L_p \cap U_p = \emptyset$, $L_p \cup U_p = A$, $a < b$ whenever $a \in L_p$ and $b \in U_p$, if $a \in L_p$ and $a' < a$ in A, $a' \in L_p$, whereas if $b \in U_p$ and $b < b'$, then $b' \in U_p$. Thus, each $p \in S_1^M(A)$ determines a cut (L_p, U_p) in A.

Conversely, suppose (L, U) is a cut in A. Then $\{a < x : a \in L\} \cup \{x < b : b \in U\}$ is finitely satisfiable in M. Thus, there is a complete 1-type containing all these formulas. Now let p, q be complete 1-types over A such that

$$p, q \in \cap_{a \in L}[a < x] \cap \cap_{b \in U}[x < b].$$

This implies that p and q contain the same atomic formulas $\varphi[x] \in L_A$. By induction on the rank of atomic formulas and the completeness of p and q, it follows that p and q contain the same open formulas $\varphi[x] \in L_A$. Since DLO admits elimination of quantifiers, it follows that $p = q$. Thus, there is a natural one-to-one correspondence between $S_1(M(A)$ and cuts in A.

This immediately implies that $|S_1^{\mathbb{Q}}(\mathbb{Q})| = 2^{\aleph_0}$. In particular, DLO is not ω-stable.

Example 5.15.5. In fact, DLO is not κ-stable for any infinite κ. To see this, start with an $M \models DLO$ of cardinality κ. For instance, if D is a linearly ordered set of cardinality κ, then $M = D \times \mathbb{Q}$ with lexicographic ordering is one such model. Now consider the set $\mathbb{M}$ of all proper, nonempty subsets L of M such that L has no greatest element and whenever $x \in L$ and $y < x$, $y \in L$. We order $\mathbb{M}$ by inclusion. Then $\mathbb{M} \models DLO$ and $x \to \{y \in M : y < x\}$ embeds M into $\mathbb{M}$ as a dense subset. It is also easy to see that every nonempty, upper bounded subset of $\mathbb{M}$ has a least upper bound. Imitating the proof of Proposition 2.7.6, we see that $|\mathbb{M}| > |M|$. It is now easily seen that $|S_1^M(M)| > |M|$, and our claim is proved.

Example 5.15.6. Now fix an algebraically closed field $\mathbb{K}$ and $A \subset \mathbb{K}$. Let κ denote the prime field of $\mathbb{K}$, with $\mathbb{A}$ the subfield generated by A and $n \geq 1$.

We claim that $p \to p|A$ is a bijection from $S_n^{\mathbb{K}}(\mathbb{A}) \to S_n^{\mathbb{K}}(A)$. By Proposition 5.12.7, this map is a surjection. Take $p \neq q \in S_n^{\mathbb{K}}(\mathbb{A})$. Then there is a formula $\varphi[\overline{x}, i_{\overline{a}}]$ of $L_{\mathbb{A}}$ such that $\varphi \in p$ and $\neg\varphi \in q$. Since *ACF* admits elimination of quantifiers, without any loss of generality, we assume that φ is open. Now note that there exist $b_1, \cdots, b_m \in A$, and for each a_i, an $f_i \in \kappa(X_1, \cdots X_m)$ such that $a_i = f_i(b_1, \cdots b_m)$. Replacing $\overline{a}$ by $\overline{b}$, we now get a formula $\psi'[\overline{x}]$ of L_A such that $\psi' \in p$ and $\neg\psi' \in q$.

For a complete n-type p in $S_n^{\mathbb{K}}(\mathbb{A})$, define

$$I_p = \{f[\overline{X}] \in \mathbb{A}[\overline{X}] : f(\overline{x}) = 0 \in p\}.$$

It is quite routine to check that I_p is an ideal on $\mathbb{A}[\overline{X}]$. Now suppose $f, g \in \mathbb{A}[\overline{X}]$ and $f \cdot g \in I_p$, i.e., $(f \cdot g)(\overline{x}) = 0 \in p$. This is the same as

$$f(\overline{x}) = 0 \vee g(\overline{x}) = 0 \in p.$$

Since p is complete, either $f(\overline{x}) = 0 \in p$ or $g(\overline{x}) = 0 \in p$. It follows that $f \in I_p$ or $g \in I_p$, i.e., I_p is a prime ideal.

Let R be a commutative ring with identity. The set of all prime ideals of R is called the *Spec* of R and is denoted by $Spec(R)$.

Example 5.15.7. Interestingly, every prime ideal J of $\mathbb{A}[\overline{X}]$ induces a complete n-type p over $\mathbb{A}$ such that $J = I_p$, and this correspondence between $S_n^{\mathbb{K}}(\mathbb{A})$ and the $Spec(\mathbb{A}[\overline{X}])$ is a bijection.

It is known that given J, there is a prime ideal I on $\mathbb{K}[\overline{X}]$ such that

$$J = I \cap \mathbb{A}[\overline{X}].$$

(See [10].) Thus $\mathbb{K}[\overline{X}]/I$ is an integral domain. Let $\mathbb{F}$ denote the algebraic closure of its quotient field. By model completeness, $\mathbb{F}$ is an elementary extension of $\mathbb{K}$. Set $a_i = [X_i] \in \mathbb{F}$. Note that, for $f \in \mathbb{K}[\overline{X}]$,

$$f(\overline{a}) = 0 \Leftrightarrow f \in I.$$

Thus, if $p = tp^{\mathbb{F}}(\overline{a}/\mathbb{A})$, $I_p = J$.

The elimination of quantifiers for *ACF* helps us to prove that this correspondence is one-to-one. Let $p, q \in S_n^{\mathbb{K}}(\mathbb{A})$ and $I_p = I_q$. Any open formula of $L_{\mathbb{A}}$ is equivalent to a disjunction of formulas of the form

$$\wedge_{i=i}^{m}(f_i(\overline{x}) = 0) \wedge \wedge_{j=1}^{n}(g_j(\overline{x}) \neq 0),$$

$f_i, g_j \in \mathbb{A}[\overline{X}]$. Since $I_p = I_q$, it follows that both p and q contain the same open formulas of $L_{\mathbb{A}}$. Since ACF has elimination of quantifiers, it follows that p and q contain the same formulas and so are equal.

This, together with the weak Hilbert basis theorem, immediately tells us the following.

Theorem 5.15.8. *The theory ACF is κ-stable for every $\kappa \geq \aleph_0$.*

Proof. Let $\mathbb{K} \models ACF$, with $A \subset \mathbb{K}$ of cardinality κ and $\mathbb{A}$ the subfield of $\mathbb{K}$ generated by A. Then $|\mathbb{A}| = \kappa$. By the weak Hilbert basis theorem, each prime ideal of $\mathbb{A}[\overline{X}]$ is finitely generated. Thus, $|Spec(\mathbb{A}[\overline{X}])| = \kappa$. Therefore, $|S_n^{\mathbb{K}}(A)| = |S_n^{\mathbb{K}}(\mathbb{A})| = |Spec(\mathbb{A}[\overline{X}])| = \kappa$. □

For stable theories, one can prove a sharper result than Corollary 5.14.22 on the existence of saturated models.

Theorem 5.15.9. *Let T be a countable, complete, κ-stable theory, with $\kappa \geq \aleph_0$ regular and $M \models T$ of cardinality κ. Then there is a saturated elementary extension N of M of cardinality κ. In particular, if T is ω-stable, then T has a saturated model of cardinality κ for every regular cardinal κ.*

Proof. The proof is exactly the same as the proof of Theorem 5.14.21. Under our hypothesis, since $|S_n^M(A)| = \kappa$ for $|A| = \kappa$, we can get each N_α of cardinality κ. Since κ is regular, any $A \subset N$ of cardinality less than κ must be contained in some N_α, implying that N is κ-saturated. □

We close this section by giving an application on the existence of prime model extensions.

Theorem 5.15.10. *Let T be a countable, complete, ω-stable theory, with $M \models T$ and $A \subset M$. Then there exists an elementary substructure N of M containing A and prime over A.*

Proof. For ordinals α we define $A_\alpha \subset M$ satisfying

(*a*) $A_0 = A$;
(*b*) For $\alpha < \beta$, $A_\alpha \subset A_\beta$;
(*c*) If α is a limit ordinal and A_α is defined, $A_\alpha = \cup_{\beta<\alpha} A_\beta$;
(*d*) If A_α is such that there is an isolated complete 1-type of A_α realized in $M \setminus A_\alpha$, then $A_{\alpha+1} = A_\alpha \cup \{a_\alpha\}$ where $a_\alpha \in M \setminus A_\alpha$, realizing an isolated complete 1-type over A_α.

We stop building A_α when we cannot further enlarge it by (d) and set $N = A_\delta$ at the first such stage.

We first show that N is closed under f^M, f an n-ary function symbol of L. Let $\overline{a} \in N = A_\delta$ and $a = f^M(\overline{a})$. Then

$$M \models i_a = f(i_{\overline{a}}).$$

Thus, there is a complete 1-type containing $x = f(i_{\overline{a}})$, say ψ. Since T is ω-stable, by Theorem 5.15.2, there is an isolated type containing ψ and realized by, say, b. This b is unique, equals a, and so $a \in N$. Thus, we think of N as a substructure of M canonically.

We now show that N is an elementary substructure of M. To prove this, we take an open formula $\varphi[x]$ of L_N and assume that there is an $a \in M$ such that $M \models \varphi[i_a]$. We need to show that there is an $a \in N$ such that $M \models \varphi[i_a]$. We see that there is a complete 1-type over N containing $\varphi[x]$. Thus, it contains an isolated type realized by a. Then we must have picked up one such $a \in N$.

It remains to see that N is prime over A. To show this, fix a model $N' \models T$ and a partial elementary map $f : A \to N'$. We need to define an embedding $f_\infty : N \to N'$ such that $f_\infty | A = f$. For each ordinal $\alpha \leq \delta$, we shall define a partial elementary map $f_\alpha : A_\alpha \to N'$ such that $f_0 = f$, and whenever $\alpha < \beta \leq \delta$, $f_\alpha \subset f_\beta$. Suppose $f_\beta : A_\beta \to N'$ have been defined for all $\beta < \alpha$. If α is limit ordinal, then we take $f_\alpha = \cup_{\beta<\alpha} f_\beta$. Clearly, $f_\alpha : A_\alpha \to N'$ is partial elementary.

Now consider the case where α is a successor ordinal, say $\alpha = \beta + 1$. Note that $tp^N(a_\beta / A_\beta)$ is isolated by, say, $\varphi[x, i_{\overline{a}}]$, $\overline{a} \in A_\beta$. Then $f_\beta(tp^N(a_\beta / A_\beta)) \in S_1^{N'}(f_\beta(A_\beta))$ is isolated by $\varphi[x, i_{f(\overline{a})}]$. Since $N \models \exists x \varphi[x, i_{\overline{a}}]$ and f_β partial elementary, $N' \models \exists x \varphi[x, i_{f_\beta(\overline{a})}]$. This gives us a $b \in N'$ such that $N' \models \varphi[b, i_{f_\beta(\overline{a})}]$. Now it is easy to see that $f_\beta \cup (a_\beta, b)$ is partial elementary.

Set $f_\infty = f_\delta : N \to N'$. Clearly, f_∞ is partial elementary. □

Chapter 6
Recursive Functions and Arithmetization of Theories

Let us ask the following question: is there an algorithm to decide whether an arbitrary sentence of the language of N is true in $\mathbb{N}$? Many important mathematical problems are of this type. For instance, the famous *Hilbert's tenth problem* sought an algorithm to decide whether an arbitrary polynomial equation

$$F(X_1, \ldots, X_n) = 0$$

with integer coefficients (also known as a Diophantine equation) had a solution in rational numbers. Problems of this form are called *decision problems*. A related question is: is there a set of sentences of the language of N that are true in $\mathbb{N}$ and is a complete theory? There is, of course, a trivial answer to the last question: the set of all sentences true in $\mathbb{N}$ is one such. Thus, in Hilbert's question is an underlying assumption, namely, there should be an algorithm to decide if a sentence is a chosen axiom or not. These questions of Hilbert had a tremendous impact on mathematical thought and culture. Gödel answered the first and last questions in the negative, and his answer is rated among the most surprising discoveries of twentieth-century mathematics. The second question was also answered in the negative by Matiyasevich.

The possibility of the nonexistence of an algorithm for a decision problem calls for defining the notion of algorithm precisely. This was considered by several logicians including Herbrand, Church, Kleene, Gödel, and Turing. Several possible definitions were advanced, and, quite remarkably, all of them were shown to be equivalent. The notion of algorithm is quite important for the incompleteness theorems. We shall adopt the definition given by Gödel. He introduced a class of functions $f : \mathbb{N}^k \to \mathbb{N}^l$, now called *recursive functions*. These are all the functions that can be computed mechanically. The definition given by Gödel is quite mathematical and helps to prove quite a strong form of incompleteness theorem.

In this chapter we shall study recursive functions. We shall also introduce techniques to show how a general decision problem can be converted to show whether a particular function is recursive.

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_6,
© Springer Science+Business Media New York 2013

6.1 Recursive Functions and Recursive Predicates

Throughout this and the next section, unless otherwise stated, by a number we shall mean a natural number, by a relation or a predicate we shall mean an n-ary relation on $\mathbb{N}$*,* $n \geq 1$*, and by a function we shall mean a function of the form* $f : \mathbb{N}^m \to \mathbb{N}^n$*,* $m, n \geq 1$*. A sequence of numbers* $(n_0, \ldots, n_{k-1})$ *will usually be denoted by* $\overline{n}$*. Further, we shall not distinguish between a k-ary relation and a subset of* $\mathbb{N}^k$. In fact, in our context, it is more convenient and natural to treat a subset of $\mathbb{N}^k$ as a k-ary relation. Thus, for $P, Q \subset \mathbb{N}^k$,

$$\neg P = P^c = \mathbb{N}^k \setminus P,\ \ P \vee Q = P \cup Q,\ \ P \wedge Q = P \cap Q$$

and

$$P \to Q = P^c \cup Q,\ \ P \leftrightarrow Q = (P \to Q) \cap (Q \to P).$$

If $Q \subset \mathbb{N}^{k+1}$, then we have the following equivalence:

$$\exists m Q(m, \overline{n}) \leftrightarrow (\pi_1 Q)(\overline{n}),$$

where $\pi_1 Q$ denotes the projection of Q to the last $\mathbb{N}^k$ coordinate space.

The *characteristic function* χ_A of $A \subset X$ is defined by

$$\chi_A(x) = \begin{cases} 0 \text{ if } x \in A, \\ 1 \text{ otherwise.} \end{cases}$$

We caution the reader that some authors define $\chi_A(x)$ as 1 if $x \in A$ and 0 otherwise.

Let P be a k-ary relation. We define a $(k-1)$-ary function by

$$\mu m P(m, \overline{n}) = \begin{cases} 0 & \text{if } \forall m \neg P(m, \overline{n}), \\ \text{first } m \text{ such that } P(m, \overline{n}) \text{ holds} & \text{otherwise,} \end{cases}$$

where $\overline{n} = (n_0, \ldots, n_{k-2})$. In particular, if k is 1, then this defines the following natural number:

$$\mu m P(m) = \begin{cases} 0 & \text{if } \forall m \neg P(m), \\ \text{first } m \text{ such that } P(m) \text{ holds} & \text{otherwise.} \end{cases}$$

The operation μ is called *minimalization*. In the sequel, we shall also need *bounded minimalization* $\mu^<$ and *bounded quantifiers* $\exists^<$, $\forall^<$, $\exists^\leq$, and $\forall^\leq$. We define

$$\mu^{<m} P(m, \overline{n}) \leftrightarrow \mu k[P(k, \overline{n}) \vee k = m],$$

$$\exists^{<m} P(m, \overline{n}) \leftrightarrow \exists k[k < m \wedge P(k, \overline{n})],$$

and

$$\forall^{<m} P(m,\overline{n}) \leftrightarrow \forall k[k < m \rightarrow P(k,\overline{n})].$$

The bounded quantifiers $\exists^{\leq}$ and $\forall^{\leq}$ are similarly defined.

In what follows, we give examples of some simple functions.

Successor function: $S(n) = n+1$;

Constant functions: For any $k \geq 1$ and any $p \geq 0$,

$$C_p^k(n_1,\ldots,n_k) \equiv p;$$

Projection functions: For any $k \geq 1$ and $1 \leq i \leq k$,

$$\pi_i^k(n_1,\ldots,n_k) = n_i.$$

The functions $+$ (addition), $\cdot$ (multiplication), $\chi_<$, and π_i^k, $k \geq 1, 1 \leq i \leq k$, will be called *initial functions*.

Now we fix some constructive schemes for defining a function f from given functions.

Composition: Given $h(n_1,\ldots,n_m)$ and $g_i(l_1,\ldots,l_k)$, $1 \leq i \leq m$, define

$$f(l_1,\ldots,l_k) = h(g_1(l_1,\ldots,l_k),\ldots,g_m(l_1,\ldots,l_k)).$$

Minimalization: Given a function g of $(m+1)$ variables such that for every $(n_1,\ldots,n_m)$ there is a k such that $g(k,n_1,\ldots,n_m) = 0$, we define f by

$$f(n_1,\ldots,n_m) = \mu k[g(k,n_1,\ldots,n_m) = 0].$$

A function f is called *recursive* if it can be defined by successive applications of composition and minimalization starting with initial functions. More precisely, the set of recursive functions is the smallest collection of functions that contains all initial functions and that is closed under composition and minimalization. A relation R is called *recursive* if its characteristic function χ_R is recursive.

Note that by definition, $<$ is a binary recursive predicate.

It has been accepted that *a function is "computable mechanically" if and only if it is recursive.* The statement in italics is known as *Church's thesis*. Once again we mention that several natural definitions of mechanically computable functions were given. All definitions are shown to be equivalent.

We shall see that many decision problems can be converted in such a way that they show whether a function $f : \mathbb{N}^m \rightarrow \mathbb{N}^n$ is computable.

Remark 6.1.1. It is quite easy to see that the sets of recursive functions and recursive predicates are countable. Thus, there are functions and predicates that are not recursive. However, it is not easy to give examples of such functions and predicates.

This is because nonrecursive functions and nonrecursive predicates are, in some sense, nonconstructive.

Now we proceed systematically to give examples and closure properties of recursive functions and predicates.

If $\pi : \mathbb{N}^k \to \mathbb{N}^n$ is the projection to the first n coordinate spaces, and if f is a an n-ary recursive function, then so is the k-ary map g defined by

$$g(\overline{u}) = f(\pi(\overline{u})).$$

Lemma 6.1.2. *If $P(\overline{n})$ is a k-ary recursive predicate, and if $f_i(\overline{u})$, $1 \leq j \leq k$, are recursive, then the predicate*

$$Q(\overline{u}) \Leftrightarrow P(f_1(\overline{u}), \ldots, f_k(\overline{u}))$$

is recursive. In particular, if π is a permutation of $\{0,1,\ldots,n-1\}$ and P an n-ary recursive predicate, then so is the predicate Q defined by

$$Q(l_0, \ldots, l_{n-1}) \leftrightarrow P(l_{\pi(0)}, \ldots, l_{\pi(n-1)}).$$

Proof. Since the set of all recursive functions is closed under composition, the result follows from the following identity:

$$\chi_Q(\overline{u}) = \chi_P(f_1(\overline{u}), \ldots, f_k(\overline{u})).$$

□

The foregoing closure property of the set of all recursive predicates is called closure under *recursive substitutions*.

Proposition 6.1.3. *If P and Q are n-ary recursive predicates, then so are $\neg P$ and $P \vee Q$. It follows that the predicates $P \wedge Q$, $P \to Q$, and $P \leftrightarrow Q$ are also recursive if P and Q are. In particular, each finite subset of $\mathbb{N}^k$, $k \geq 1$, is recursive.*

Proof. The result follows from the following identity:

$$\chi_{\neg P}(\overline{p}) = \chi_<(0, \chi_P(\overline{p})) \text{ and } \chi_{P \vee Q}(\overline{p}) = \chi_P(\overline{p}) \cdot \chi_Q(\overline{p}),$$

where $\overline{p} = (p_1, \ldots, p_n)$. □

Lemma 6.1.4. *If $P(m,\overline{n})$ is a recursive predicate such that for every $\overline{n}$, $P(m,\overline{n})$ holds for some m, then*

$$f(\overline{n}) = \mu m P(m,\overline{n})$$

is recursive.

Proof. The result follows from the identity

$$f(\overline{n}) = \mu m[\chi_P(m,\overline{n}) = 0]$$

and the minimalization rule. □

Lemma 6.1.5. *Every constant function C_p^k, $k \geq 1$, $p \geq 0$, is recursive. In particular, $\emptyset$ and each $\mathbb{N}^k$ are recursive.*

Proof. For each k, we prove the result by induction on p. Since

$$C_0^k(\overline{n}) = \mu m[\pi_1^{k+1}(m,\overline{n}) = 0],$$

C_0^k is recursive. Assume that C_p^k is recursive. Now,

$$C_{p+1}^k = \mu m[C_p^k < m].$$

The result follows by the induction hypothesis. □

In what follows, instead of giving complete proofs, we shall define functions and predicates in such a way that it would not be hard to show that they are recursive.

Example 6.1.6. The successor function $S(n) = n+1$ is recursive. This follows from the identity

$$S(n) = \pi_1^1(n) + C_1^1(n).$$

Example 6.1.7. The binary predicates $\leq$, $>$, and $\geq$ are recursive. This follows from the following equivalences and the closure properties of recursive predicates already proved:

$$m \leq n \Leftrightarrow m < n+1,$$
$$m > n \Leftrightarrow n < m,$$
$$m \geq n \Leftrightarrow m+1 > n,$$

and

$$m = n.$$

Example 6.1.8. We define $m \dot{-} n$ as follows:

$$m \dot{-} n = \begin{cases} m-n \text{ if } m \geq n, \\ 0 \qquad \text{otherwise.} \end{cases}$$

The function $m \dot{-} n$ is recursive. To see this, note the following identity:

$$m \dot{-} n = \mu k[n+k = m \vee m < n].$$

Exercise 6.1.9. Show that the following functions are recursive:

(i) $|m-n|$.
(ii) $\min(m,n)$.
(iii) $\max(m,n)$.

(iv)
$$\alpha(n) = \begin{cases} 1 \text{ if } n = 0, \\ 0 \text{ if } n > 0. \end{cases}$$

(v)
$$sg(n) = \begin{cases} 0 \text{ if } n = 0, \\ 1 \text{ if } n > 0. \end{cases}$$

Example 6.1.10. Let $P(m,\overline{n})$ be a $(k+1)$-ary recursive predicate. Then

$$\exists^{<m}(\overline{n}) = \mu m(k = m \dot{-} 1 \vee P(m,\overline{n})),\ \overline{n} \in \mathbb{N}^k,$$

is recursive. In particular, the predicates

$$Q(m,\overline{n}) \Leftrightarrow \exists^{<m} P(m,\overline{n}),$$

$$Q'(m,\overline{n}) \Leftrightarrow \exists^{\leq m} P(m,\overline{n}),$$

$$R(m,\overline{n}) \Leftrightarrow \forall^{<m} P(m,\overline{n}),$$

and

$$R'(m,\overline{n}) \Leftrightarrow \exists^{\leq m} P(m,\overline{n})$$

are recursive.

[*Hint:* Note that $Q(m,\overline{n}) \Leftrightarrow f(\overline{n}) < m$.]

Remark 6.1.11. In the next chapter, we shall show that the set of all recursive predicates is not closed under existential and universal quantifiers.

Exercise 6.1.12. Let $A_1,\ldots,A_m$ be pairwise disjoint recursive subsets of $\mathbb{N}^k$ whose union is $\mathbb{N}^k$. Suppose $f_1,\ldots,f_m$ are k-ary recursive functions. Define $g : \mathbb{N}^k \to \mathbb{N}$ by

$$g(\overline{a}) = \begin{cases} f_1(\overline{a}) & \text{if} \quad \overline{a} \in A_1, \\ \quad\vdots & \\ f_m(\overline{a}) & \text{if} \quad \overline{a} \in A_m. \end{cases}$$

Show that g is recursive.

We now proceed to show that we can effectively code a finite sequence of numbers, a finite sequence of finite sequences of numbers, etc. by numbers. This remarkable idea is due to Gödel, who turned it into a powerful tool for proving his incompleteness theorems.

Exercise 6.1.13. The following predicates are recursive:

(i) (*Divisibility*) $m|n \leftrightarrow \exists^{\leq n} k[m \cdot k = n]$.
(ii) (*Prime*) $\text{Prime}(p) \leftrightarrow p$ is a prime.

(iii) (*Relatively prime*) $RP(m,n) \leftrightarrow m \neq 0 \wedge n \neq 0 \wedge \forall p \leq m[(\text{Prime}(p) \wedge p|m) \rightarrow \neg p|n]$.

For an ordered pair (m,n) of natural numbers, we define

$$OP(m,n) = (m+n)\cdot(m+n+1)+n+1.$$

Clearly, $OP(m,n)$ is recursive.

Lemma 6.1.14. *The function OP is one-to-one.*

Proof. Let $OP(m,n) = OP(m',n')$. We first show that $m+n = m'+n'$. Suppose not. Without any loss of generality, we assume that $m+n < m'+n'$. Now

$$OP(m,n) \leq (m+n+1)^2 \leq (m'+n')^2 < OP(m',n').$$

This is a contradiction.

Since $m+n = m'+n'$ and $OP(m,n) = OP(m',n')$, from the definition of OP it follows that $n = n'$. This in turn implies that $m = m'$ too. □

We shall need the following two simple lemmas from number theory.

Lemma 6.1.15. *Let $m_1,\ldots,m_k$ and $n_1,\ldots,n_l$ be sequences of numbers such that $\forall i \forall j[RP(m_i,n_j)]$. Then there is a number x such that $\forall i[m_i|x]$ and $\forall j[RP(x,n_j)]$.*

Proof. Take x to be the product of all the m_i. If a prime p divides x, then it divides some m_i. Hence, $\neg p|n_j$ for all j. The result follows. □

Lemma 6.1.16. $\forall m,n \forall j[m|n \rightarrow RP(1+(j+m)n, 1+jn)]$.

Proof. Let p be a prime number such that $p|1+(j+m)n$ and $p|1+jn$. Then $p|mn$. Since p is a prime, either $p|m$ or $p|n$. If $p|m$, then $p|n$ also because $m|n$. Hence, $p|n$. But then $\neg(p|1+jn)$. This contradiction proves our result. □

The following result is due to Gödel.

Theorem 6.1.17. *There is a 2-ary function $\beta(n,i)$ satisfying the following properties:*

(a) β is recursive.
(b) $\beta(0,i) = 0$ for all i.
(c) $n \neq 0 \rightarrow \beta(n,i) < n$ for all i.
(d) For every finite sequence $\overline{n} = (n_0,\ldots,n_{k-1})$ of positive length, there is an n such that

$$\forall i < k[\beta(n,i) = n_i].$$

Proof. Define

$$\beta(n,i) = \mu^{<n}x\exists^{<n}y\exists^{<n}z[n = OP(y,z) \wedge (1+(OP(x,i)+1)\cdot z)|y],$$

i.e., $\beta(n,i)$ is the first natural number $x < n$ for which there exist $y,z < n$ satisfying $n = OP(y,z)$ and $1 + (OP(x,i)+1)\cdot z|y$. If such an x does not exist, then $\beta(n,i) = n \dot{-} 1$.

Properties (a)–(c) of β follow from the definition. To prove (d), take a finite sequence $\overline{n} = (n_0,\ldots,n_{k-1})$ of positive length. Let

$$u = \max\{OP(n_i,i)+1 : i < k\},$$

and let z be the product of all nonzero numbers less than u. Then, by Lemma 6.1.16,

$$j < l < u \Rightarrow RP(1+jz, 1+lz).$$

For $i < k$, set

$$m_i = 1 + (OP(n_i,i)+1)z.$$

Let $\{l_j\}$ be an enumeration of all numbers of the form $1+vz$, where $0 < v < u$ and $v \neq OP(n_i,i)+1$ for all $i < k$. Then, by Lemma 6.1.15, there is a number y such that

$$\forall j < u[1 + jz|y \Leftrightarrow \exists i(j = OP(n_i,i)+1)].$$

Set $n = OP(y,z)$.

It remains to show that $\beta(n,i) = n_i$ for all i. This will follow if we show that n_i is the smallest number x such that

$$1 + (OP(x,i)+1)z|y.$$

Note that this will follow if for all $x < n_i$, $OP(x,i) < u$ and $OP(x,i) \neq OP(n_j,j)$ for all j. This can easily be seen using the fact that OP is one-to-one (Lemma 6.1.14). □

The function β defined above is called *Gödel's β-function*.

For each $n \geq 0$ and each finite sequence $(k_0,\ldots,k_{n-1})$, we define

$$\langle k_0,\ldots,k_{n-1}\rangle = \mu m[\beta(m,0) = n \wedge \beta(m,1) = k_0 \wedge \cdots \wedge \beta(m,n) = k_{n-1}].$$

We shall call such a number a *sequence number*.

The empty sequence of natural numbers will be denoted by $\langle\ \rangle$, and its sequence number equals 0 by definition.

Remark 6.1.18. The map $(k_0,\cdots,k_{n-1}) \to \langle k_0,\cdots k_{n-1}\rangle$ is recursive.

We now introduce some relations and functions of sequence numbers:

seq will denote the set of all sequence numbers, $lh(n) = \beta(n,0)$ (the length of the sequence coded by n), $(n)_i = \beta(n,i+1)$ (the ith element of the sequence coded by n), and concatenation

$$\langle m_0,\ldots,m_{l\dot{-}1}\rangle * \langle n_1,\ldots,n_{k\dot{-}1}\rangle = \langle m_0,\ldots,m_{l\dot{-}1},n_0,\ldots,n_{k\dot{-}1}\rangle.$$

Proposition 6.1.19. *The following functions and predicates are recursive:* $n \Rightarrow lh(n)$, $(n,i) \Rightarrow (n)_i$, *seq, and the concatenation* $(m,n) \to m*n$.

Proof. Since $lh(n) = \beta(n,0)$ and $(n)_i = \beta(n,i+1)$, and since β is recursive, the functions $lh(n)$ and $(n)_i$ are recursive. That seq is recursive follows from the following equivalence:

$$\text{seq}(n) \Leftrightarrow \exists^{<n} u_0, \ldots, u_{lh(n)\dot{-}1} \forall 0 \leq i < lh(n)[\beta(n,i+1) = u_i].$$

Let $m = \langle m_0, \ldots, m_{lh(m)-1} \rangle$ and $n = \langle n_0, \ldots, n_{lh(n)-1} \rangle$. Then

$$\begin{aligned} m*n = \mu u[&seq(u) \wedge lh(u) = lh(m) + lh(n) \\ &\wedge \forall i < lh(m)((u)_i = m_j) \wedge \forall j < lh(n)((u)_{l+j} = n_j)]. \end{aligned}$$

Hence the concatenation function $*$ is recursive. □

We introduce yet another operation on recursive functions.

Primitive recursion: Given an m-ary function g and an $(m+2)$-ary function h, we define an $(m+1)$-ary function f by

$$\begin{aligned} f(0,\overline{n}) &= g(\overline{n}), \\ f(k+1,\overline{n}) &= h(f(k,\overline{n}),k,\overline{n}). \end{aligned}$$

The scheme of primitive recursion is a general form of definition of functions by induction. It should be noted that m may be 0 and that a 0-ary function is nothing but a constant. Thus, given a natural number p and a 2-ary function h, this procedure defines a sequence $\{x_k\}$ by induction: set $x_0 = p$ and $x_{k+1} = h(x_k,k)$. Intuitively, it should be obvious that if g and h are "computable," then so is f.

Proposition 6.1.20. *If* g *is an* m*-ary and* h *an* $(m+2)$*-ary recursive function, and if* f *is defined by primitive recursion as above, then* f *is recursive.*

Proof. The function $f : \mathbb{N}^{m+1} \to \mathbb{N}$ is defined by

$$\begin{aligned} f(0,\overline{n}) &= g(\overline{n}), \\ f(k+1,\overline{n}) &= h(f(k,\overline{n}),k,\overline{n}). \end{aligned}$$

We first define a function $F : \mathbb{N}^{m+1} \to \mathbb{N}$ as follows:

$$\begin{aligned} F(p,\overline{n}) = \mu k[&lh(k) = p+1 \wedge (k)_0 = g(\overline{n}) \\ &\wedge \forall i < p((k)_{i+1} = h((k)_i,i,\overline{n})]. \end{aligned}$$

By the closure properties of recursive functions and recursive predicates, F is recursive. Now note that for all $p \geq 0$,

$$f(p,\overline{n}) = (F(p,\overline{n}))_p.$$

The result can now easily be seen. □

Exercise 6.1.21. Let $\mathscr{R}$ be the smallest set of functions that contains the successor function S, constant functions C_k^n, and the projection maps π_i^n and that is closed under composition, minimalization, and primitive recursion. Show that a function is recursive if and only if it belongs to $\mathscr{R}$.

The previous exercise gives a more traditional definition of recursive functions. Further, coding a sequence, sequence of sequences, etc. is achieved more easily with this definition. However, our definition of recursive function is chosen to give the best-known form of Gödel's incompleteness theorem.

Example 6.1.22. The exponentiation function m^n inductively defined by

$$\begin{aligned} m^0 &= 1, \\ m^{n+1} &= m^n \cdot m \end{aligned}$$

is recursive.

Exercise 6.1.23. The function $n!$ is recursive.

Exercise 6.1.24. Show that the *predecessor function* $p(n)$ defined below is recursive:

$$\begin{aligned} p(0) &= 0, \\ p(n+1) &= n. \end{aligned}$$

Exercise 6.1.25. Show that the functions $\max\{m,n\}$ and $\min\{m,n\}$ and, for any $k > 1$, $\max\{n_1,\ldots,n_k\}$ and $\min\{n_1,\ldots,n_k\}$ are recursive.

Exercise 6.1.26. Let $2 = p_0, p_1, p_2, \ldots$ be the increasing enumeration of all prime numbers. Show that $n \to p_n$ is recursive.

Proposition 6.1.27. *A function $f : \mathbb{N}^k \to \mathbb{N}$ is recursive if and only if its graph $gr(f)$ is recursive, where for any $\overline{n} \in \mathbb{N}^k$,*

$$(\overline{n}, m) \in gr(f) \Leftrightarrow f(\overline{n}) = m.$$

Proof. If f is recursive, then $gr(f)$ is recursive because $=$ is recursive and the set of all recursive predicates is closed under recursive substitutions. Conversely, if $gr(f)$ is recursive, then f is recursive because of the following identity:

$$f(\overline{n}) = \mu m[(\overline{n}, m) \in gr(f)].$$

□

Theorem 6.1.28 (Closure under complete recursion). *Let $f(m,\overline{n})$ be recursive and $g(m,\overline{n})$ be defined by the equation*

$$g(m,\overline{n}) = f(\langle g(0,\overline{n}),\ldots,g(m-1,\overline{n})\rangle,\overline{n}).$$

Then g is recursive.

Proof. We first show that the function

$$(m,\overline{n}) \to h(m,\overline{n}) = \langle g(0,\overline{n}),\cdots,g(m-1,\overline{n})\rangle$$

is recursive. Since $g(m,\overline{n}) = (h(m+1,\overline{n}))_{m+1}$, this will complete the proof. We show h is recursive by showing that its graph is recursive. For this note that

$$\begin{aligned} h(m,\overline{n}) = k \Leftrightarrow\ & \mathrm{seq}(k) \wedge lh(k) = m \\ & \wedge \forall i < m((k)_i = f(\langle (k)_0,\cdots,(k)_{i-1}\rangle,\overline{n})). \end{aligned}$$

□

We prove the following result using the well-known diagonal argument of Cantor. Gödel uses it beautifully to prove the first incompleteness theorem.

Proposition 6.1.29. *There is no recursive set $U \subset \mathbb{N}\times\mathbb{N}$ such that for every recursive set $A \subset \mathbb{N}$ there is an $n \in \mathbb{N}$ satisfying*

$$\forall m[m \in A \Leftrightarrow (n,m) \in U],$$

i.e., there is no recursive set $U \subset \mathbb{N}\times\mathbb{N}$ whose vertical sections exactly list all recursive subsets of $\mathbb{N}$.

Proof. Suppose such a recursive set U exists. Define

$$A^* = \{m \in \mathbb{N} : (m,m) \notin U\}.$$

Since the predicate U^c is recursive and since the set of all recursive predicates is closed under recursive substitutions, A^* is recursive. Thus, by the hypothesis, there is an $n^* \in \mathbb{N}$ such that

$$\forall m[m \in A^* \Leftrightarrow (n^*,m) \in U]. \qquad (*)$$

If $n^* \in A^*$, then $(n^*,n^*) \in U$ by $(*)$. But then $n^* \notin A^*$ by the definition of A^*. On the other hand, if $n^* \notin A^*$, then $(n^*,n^*) \in U^c$ by $(*)$. But then $n^* \in A^*$ by the definition of A^*. We have arrived at a contradiction. □

For the next exercise, recall the definition of standard model and true formulas of N.

Exercise 6.1.30. Recall that for any $n \in \mathbb{N}$, k_n denotes the term

$$\underbrace{S\cdots S}_{n \text{ times}}0$$

of N. Let $\varphi[x_1,\ldots,x_p]$ be an open formula of N. Show that the predicate

$$\{\overline{n} \in \mathbb{N}^p : \varphi_{x_1,\ldots,x_p}[k_{n_1},\ldots,k_{n_p}] \text{ is true}\}$$

is recursive.

6.2 Semirecursive Predicates

A nonempty subset of $\mathbb{N}^k$ is called *semirecursive* or *recursively enumerable* (*r.e.*) if it is the projection to the last k coordinate space of a $(k+1)$-ary recursive predicate, i.e., there is a recursive $Q \subset \mathbb{N}^{k+1}$ such that for every $\overline{n} \in \mathbb{N}^k$,

$$P(\overline{n}) \Leftrightarrow \exists m[Q(m,\overline{n})].$$

Proposition 6.2.1. *Every recursive predicate is semirecursive.*

Proof. Let P be a k-ary recursive predicate. Define $Q \subset \mathbb{N}^{k+1}$ by

$$Q(m,\overline{n}) \Leftrightarrow P(\overline{n}).$$

Then Q is recursive and $P(\overline{n}) \Leftrightarrow \exists m Q(m,\overline{n})$. Hence P is semirecursive. □

Proposition 6.2.2. *The set of all semirecursive predicates is closed under $\vee$, $\wedge$, projections, bounded universal quantifiers, and recursive substitutions.*

Proof. Let P and Q be k-ary semirecursive predicates. Fix $(k+1)$-ary recursive predicates P' and Q' such that for all $\overline{n} \in \mathbb{N}^k$,

$$P(\overline{n}) \Leftrightarrow \exists m P'(m,\overline{n}) \text{ and } Q(\overline{n}) \Leftrightarrow \exists m Q'(m,\overline{n}).$$

Let f_i, $1 \le i \le k$, be l-ary recursive functions. For any $\overline{n} \in \mathbb{N}^k$, $\overline{m} \in \mathbb{N}^l$ note the following:

$$(P \vee Q)(\overline{n}) \Leftrightarrow \exists m[(P' \vee Q')(m,\overline{n})],$$
$$P(f_1(\overline{m}),\ldots,f_k(\overline{m})) \Leftrightarrow \exists r P'(r,f_1(\overline{m}),\ldots,f_k(\overline{m})),$$

and

$$(P \wedge Q)(\overline{n}) \Leftrightarrow \exists m[P'((m)_0,\overline{n}) \wedge Q'((m)_1,\overline{n})].$$

These show that the set of all semirecursive predicates is closed under $\vee$, $\wedge$, and recursive substitutions.

We use Gödel's coding functions to show other closure properties also. Let P be a $(k+2)$-ary recursive predicate, and let Q be defined by

$$Q(\overline{n}) \Leftrightarrow \exists l \exists m P(l,m,\overline{n}).$$

Then

$$Q(\overline{n}) \Leftrightarrow \exists m P((m)_0,(m)_1,\overline{n}).$$

This shows that the set of all semirecursive predicates is closed under the existential quantifier.

Let P be a $(k+1)$-ary semirecursive predicate, and let Q be defined by

$$Q(m,\overline{n}) \Leftrightarrow \forall^{<m} p P(p,\overline{n}).$$

Let $R \subset \mathbb{N} \times \mathbb{N}^{k+1}$ be a recursive predicate such that

$$\forall p \forall \overline{n} \in \mathbb{N}^k [P(p, \overline{n}) \Leftrightarrow \exists q R(q, p, \overline{n})].$$

Then

$$Q(m, \overline{n}) \Leftrightarrow \exists q[\text{seq}(q) \wedge lh(q) = m \wedge \forall^{<m} p R((q)_p, p, \overline{n})].$$

This shows that the set of all semirecursive predicates is closed under the bounded universal quantifier $\forall^{<}$. The result is now easily seen. □

Exercise 6.2.3. A nonempty subset P of $\mathbb{N}$ is semirecursive if and only if it is the range of a unary recursive function.

The following is an important result in recursive function theory.

Theorem 6.2.4 (Kleene). *A predicate P is recursive if and only if both P and $\neg P$ are semirecursive.*

Proof. If P is recursive, then so is $\neg P$. By Proposition 6.2.1, both P and $\neg P$ are semirecursive.

Now let P be k-ary and both P and $\neg P$ be semirecursive. Choose $(k+1)$-ary recursive predicates Q and R such that for all $\overline{n} \in \mathbb{N}^k$,

$$P(\overline{n}) \Leftrightarrow \exists m Q(m, \overline{n}) \text{ and } \neg P(\overline{n}) \Leftrightarrow \exists m R(m, \overline{n}).$$

Then $S = Q \vee R$ is recursive. Note that

$$\forall \overline{n} \in \mathbb{N}^k \exists m S(m, \overline{n}).$$

We define

$$s(\overline{n}) = \mu m S(m, \overline{n}).$$

The function s is recursive. Further,

$$P(\overline{n}) \Leftrightarrow Q(s(\overline{n}), \overline{n}).$$

This shows that P is recursive. □

Remark 6.2.5. Let $P \subset \mathbb{N}^k$ be semirecursive, and let there exist a $(k+1)$-ary recursive predicate Q such that for all $\overline{n}$,

$$P(\overline{n}) \Leftrightarrow \forall m Q(\overline{n}, m).$$

Then P is recursive. By Theorem 6.2.4, our assertion will be proved if we show that $\neg P$ is semirecursive. This follows from the following equivalence:

$$\neg P(\overline{n}) \Leftrightarrow \exists m \neg Q(\overline{n}, m).$$

Proposition 6.2.6. *Let $f : \mathbb{N}^k \to \mathbb{N}$ be any function. Then the following statements are equivalent:*

(i) The function f is recursive.
(ii) The graph of f, $gr(f)$ is recursive.
(iii) The graph of f is semirecursive.

Proof. By Proposition 6.1.27 and Theorem 6.2.4, we only need to show that if $gr(f)$ is semirecursive, then $\neg gr(f)$ is semirecursive. This follows from the following equivalence:

$$f(\overline{n}) \neq m \Leftrightarrow \exists l[m \neq l \wedge f(\overline{n}) = l].$$

□

A function $f = (f_1, \ldots, f_p) : \mathbb{N}^k \to \mathbb{N}^p$ is called *recursive* if each f_i, $1 \leq i \leq p$, is recursive.

Exercise 6.2.7. Let $f : \mathbb{N}^k \to \mathbb{N}^p$ be any function. Then the following statements are equivalent:

(i) The function f is recursive.
(ii) The graph of f, is recursive.
(iii) The graph of f is semirecursive.

6.3 Arithmetization of Theories

The next idea, arithmetization of theories, is a beautiful idea due to Gödel. It represents syntactical objects, e.g., symbols, terms, formulas, proofs, of a theory by natural numbers. Consequently, statements about syntactical objects are expressed in terms of numbers. Its importance and beauty cannot be overemphasized. It has the potential to convert a metamathematical statement into a number-theoretic statement. Thus, the problem of whether a metamathematical statement is true is translated into a number-theoretic problem. This idea also plays a significant role in the theory of computation. The same idea is now used to convert many questions concerning algorithms into proving whether a number-theoretic function or relation is recursive. To elaborate a bit more, one can code each algorithm by an integer, or one can translate questions about algorithms into number-theoretic problems.

Throughout this section, unless otherwise stated, T will denote a fixed first-order theory. To simplify the matter, we assume that T is finite and its nonlogical symbols are enumerated in some order.

In the first step we assign a *symbol number* to each symbol of $L(T)$.

Set $SN(x_i) = 2i$, $i \geq 0$; $SN(\neg) = 1$; $SN(\vee) = 3$; $SN(\exists) = 5$; $SN(=) = 7$; if α is the ith nonlogical symbol, then we set $SN(\alpha) = 7 + 2i$.

Note that a number n is the symbol number of a variable if and only if it is even, i.e., $2|n$. Hence, the predicate

$$\text{vble}(n) \Leftrightarrow n \text{ is the symbol number of a variable}$$

is recursive. Since every finite set is recursive, the predicate

$$\mathrm{sn}(n) \Leftrightarrow n \text{ is a symbol number}$$

is easily seen to be recursive. In other words, there is an algorithm to decide whether an integer is a symbol number. Further, intuitively it is easy to see that there is an algorithm such that given a symbol number n, the algorithm recovers the symbol whose symbol number is n. More precisely, if n is a symbol number, it is either even or equals one of the finitely many odd numbers assigned to the symbols other than the variables. Also, if $n = 2i$, then n is the symbol number of the variable x_i.

Let func_0 denote the set of symbol numbers of all constant symbols. We also define

$$\mathrm{pred}(n) \Leftrightarrow n \text{ is the symbol number of a predicate symbol}$$

and

$$\mathrm{func}(n) \Leftrightarrow n \text{ is the symbol number of a function symbol.}$$

Since T is finite, these predicates are finite and, hence, recursive.

Let t be a term and A a formula of T. We now define the *Gödel numbers* $\ulcorner t \urcorner$ and $\ulcorner A \urcorner$ of t and A, respectively, by induction on the rank of t and A.

If t is a variable or a constant, then set

$$\ulcorner t \urcorner = \langle SN(t) \rangle.$$

If f is an n-ary function and $t_1, \ldots, t_n$ are terms whose Gödel numbers have been defined, then we set

$$\ulcorner f t_1 \ldots t_n \urcorner = \langle SN(f), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_n \urcorner \rangle.$$

We define

$$\mathrm{term}(n) \Leftrightarrow n \text{ is the Gödel number of a term.}$$

Proposition 6.3.1. *The predicate* term *is recursive.*

Proof. Note that for any n,

$$\begin{aligned} \mathrm{term}(n) \Leftrightarrow \mathrm{seq}(n) \wedge [(lh(n) = 1 \wedge \mathrm{func}_0((n)_0)) \vee [lh(n) > 1 \wedge \\ \mathrm{func}((n)_0) \wedge \forall 0 < i < lh(n)(\mathrm{term}((n)_i))]]. \end{aligned}$$

Using closure under complete recursion (Exercise 6.1.28), it can now be seen that *term* is recursive. We leave the details as an exercise for the reader. □

We recall that the terms

$$\underbrace{S \cdots S}_{n \text{ times}} 0$$

of N is denoted by k_n and that these terms are called numerals.

Lemma 6.3.2. *The map*

$$\mathrm{num}(n) = \ulcorner k_n \urcorner, \quad n \in \mathbb{N},$$

is recursive.

Proof. This follows from the following identities:

$$\begin{aligned} \mathrm{num}(0) &= \langle SN(0) \rangle, \\ \mathrm{num}(n+1) &= \langle SN(S), \mathrm{num}(n) \rangle. \end{aligned}$$

□

If A is an atomic formula $pt_1 \cdots t_n$, then define

$$\ulcorner A \urcorner = \langle SN(p), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_n \urcorner \rangle.$$

Proposition 6.3.3. *The predicate*

$$\mathrm{aform}(n) \Leftrightarrow n \textit{ is the Gödel number of an atomic formula}$$

is recursive.

Proof. We have

$$\mathrm{aform}(n) \Leftrightarrow \mathrm{seq}(n) \wedge lh(n) > 1 \wedge \mathrm{pred}((n)_0) \wedge \forall 0 < i < lh(n)[\mathrm{term}((n)_i)].$$

□

If A is $\neg B$, and if $\ulcorner B \urcorner$ has been defined, then

$$\ulcorner A \urcorner = \langle SN(\neg), \ulcorner B \urcorner \rangle.$$

If A is $\vee BC$, then

$$\ulcorner A \urcorner = \langle SN(\vee), \ulcorner B \urcorner, \ulcorner C \urcorner \rangle.$$

If A is $\exists xB$, then

$$\ulcorner A \urcorner = \langle SN(\exists), \ulcorner x \urcorner, \ulcorner B \urcorner \rangle.$$

Proposition 6.3.4. *The predicate*

$$\mathrm{form}(n) \Leftrightarrow n \textit{ is the Gödel number of a formula}$$

is recursive.

Proof. We define the following predicates:

$$A_1(n) \Leftrightarrow [\mathrm{seq}(n) \wedge lh(n) = 2 \wedge (n)_0 = SN(\neg) \wedge \mathrm{form}((n)_1)],$$

$$A_2(n) \Leftrightarrow [\mathrm{seq}(n) \wedge lh(n) = 3 \wedge (n)_0 = SN(\vee) \wedge \mathrm{form}((n)_1) \wedge \mathrm{form}((n)_2)],$$

and

$$A_3(n) \Leftrightarrow [\text{seq}(n) \wedge lh(n) = 3 \wedge (n)_0 = SN(\exists) \wedge \text{vble}((n)_1) \wedge \text{form}((n)_2)].$$

By closure under complete recursion (Exercise 6.1.28), it is not hard to show that these predicates are recursive. Now note that

$$\text{form}(n) \Leftrightarrow \text{aform}(n) \vee A_1(n) \vee A_2(n) \vee A_3(n).$$

It follows that the predicate $\text{form}(n)$ is recursive. □

Now we systematically proceed and show that many metamathematical statements (statements about the theory itself or statements about syntactical objects such as formulas and proofs) can be turned into number-theoretic statements. Many of the functions and predicates thus defined are recursive or semirecursive. However, we shall not verify this in full detail. Interested readers should complete the proofs as an exercise.

Proposition 6.3.5. *There is a recursive function* $\text{sub}(l,m,n)$ *such that if* l *is the Gödel number of a term* t *or a formula* A*, if* m *is the Gödel number of a variable* v*, and if* n *is the Gödel number of a term* s*, then* $\text{sub}(l,m,n)$ *is the Gödel number of* $t_v[s]$ *or* $A_v[s]$*, respectively.*

Proof. Define

$$\text{sub}_1(l,m,n) = \begin{cases} n \text{ if } \text{vble}(l), & \wedge l = m, \\ l \text{ otherwise}, \end{cases}$$

$$\text{sub}_2(l,m,n) = \langle (l)_0, \text{sub}_2((l)_1,m,n), \ldots, \text{sub}_2((l)_{lh(l) \dot{-} 1},m,n)\rangle,$$

$$\text{sub}_3(l,m,n) = \begin{cases} \langle (l)_0, \text{sub}_3((l)_1,m,n)\rangle & \text{if } \text{seq}(l) \wedge lh(l) = 2, \\ \langle (l)_0, \text{sub}_3((l)_1,m,n), \text{sub}_3((l)_2,m,n)\rangle & \\ & \text{if } \text{seq}(l) \wedge lh(l) = 3 \\ & \wedge (l)_0 \neq SN(\exists), \\ \langle (l)_0, (l)_1, \text{sub}_3((l)_2,m,n)\rangle & \text{if } \text{seq}(l) \wedge lh(l) = 3 \\ & \wedge (l)_0 = SN(\exists) \\ & \wedge (l)_1 \neq m, \\ l & \text{otherwise.} \end{cases}$$

Now define

$$\text{sub}(l,m,n) = \begin{cases} \text{sub}_1(l,m,n) & \text{if } \text{vble}(l) \vee \text{func}_0(l), \\ \text{sub}_2(l,m,n) & \text{if } \text{pred}((l)_0) \vee \text{func}((l)_0), \\ \text{sub}_3(l,m,n) & \text{if } \text{form}(l) \wedge \neg\text{aform}(l), \\ l & \text{otherwise.} \end{cases}$$

Then $\mathrm{sub}(l,m,n)$ is a recursive function with the desired properties. □

Exercise 6.3.6. For each $n \geq 1$, show that there is a recursive function $\mathrm{sb} : \mathbb{N} \times \mathbb{N}^n \to \mathbb{N}$ such that when $m = \lceil E \rceil$, with E a term or a formula of the theory N,

$$\mathrm{sb}(m, b_0, \ldots, b_{n-1}) = \left\lceil E_{x_0,\ldots,x_{n-1}}[k_{b_0}, \ldots, k_{b_{n-1}}] \right\rceil,$$

where $x_0, x_1, \ldots, x_{n-1}$ are the first n variables in alphabetical order.

Exercise 6.3.7. For each $m, n \geq 1$, show that there is a recursive function $s_n^m : \mathbb{N} \times \mathbb{N}^m \to \mathbb{N}$ such that when $p = \lceil A \rceil$, with A a formula of the theory N,

$$s_n^m(p, b_{m+1}, \ldots, b_{m+n}) = \left\lceil A_{x_{m+1},\ldots,x_{m+n}}[k_{b_{m+1}}, \ldots, k_{b_{m+n}}] \right\rceil,$$

where $x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ are the first $(m+n)$ variables in alphabetical order.

Proposition 6.3.8. *There is a recursive predicate* $\mathrm{fr}(m,n)$ *such that if m is the Gödel number of a term or a formula E and if n is the Gödel number of a variable v, then*

$$\mathrm{fr}(m,n) \Leftrightarrow v \textit{ is free in } E.$$

Proof. Set

$$\chi_{\mathrm{fr}}^1(m,n) = \chi_{\mathrm{fr}}((m)_1, n) \ldots \chi_{\mathrm{fr}}((m)_{lh(m)-1}, n).$$

Now take

$$\chi_{\mathrm{fr}}(m,n) = \begin{cases} 0 & \text{if } \mathrm{vble}(m) \wedge m = n, \\ \chi_{\mathrm{fr}}^1(m,n) & \text{if } \mathrm{pred}((m)_0) \vee \mathrm{func}((m)_0), \\ \chi_{\mathrm{fr}}((m)_1, n) & \text{if } (m)_0 = SN(\neg), \\ \chi_{\mathrm{fr}}((m)_1, n) \cdot \chi_{\mathrm{fr}}((m)_2, n), & \text{if } lh(m) = 3 \\ & \wedge (m)_0 = SN(\vee), \\ \chi_{\mathrm{fr}}((m)_2, n)), & \text{if } lh(m) = 3 \\ & \wedge (m)_0 = SN(\exists) \wedge (m)_1 \neq n, \\ 1 & \text{otherwise.} \end{cases}$$

Then χ_{fr} is a recursive function with the desired properties. □

Proposition 6.3.9. *There is a recursive function* $\mathrm{substl}(l,m,n)$ *such that if l is the Gödel number of a formula A, if m is the Gödel number of a variable v, and if n is the Gödel number of a term t, then*

$$\mathrm{substl}(l,m,n) \Leftrightarrow t \textit{ is substitutable for } v \textit{ in } A.$$

The proof is left as an exercise.

Exercise 6.3.10. Let I be an interpretation of a theory T' in T. Show that there is a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that if n is the Gödel number of a formula A of T', then $f(n)$ is the Gödel number of its meaning A^I in I.

We shall now show that the set LAx_T of Gödel numbers of all logical axioms of T is recursive. We define four recursive predicates first:

$$\mathrm{pax}(m) \Leftrightarrow \exists^{<m} n[\mathrm{form}(n) \wedge m = \langle SN(\vee), \langle SN(\neg), n\rangle, n\rangle].$$

Note that for all m,

$$\mathrm{pax}(m) \Leftrightarrow m \text{ is the Gödel number of a propositional axiom,}$$

$$\mathrm{idax}(m) \Leftrightarrow \exists^{<m} n[\mathrm{vble}(n) \wedge m = \langle SN(=), n, n\rangle].$$

Note that

$$\mathrm{idax}(m) \Leftrightarrow m \text{ is the Gödel number of an identity axiom.}$$

Exercise 6.3.11. Show that the unary predicates sax and eax of Gödel numbers of all substitution axioms and of all equality axioms, respectively, are recursive.

We now have the following theorem.

Theorem 6.3.12. *The unary predicate* $\mathrm{LAx}_T \subset \mathbb{N}$ *consisting of Gödel numbers of all logical axioms of* T *is recursive.*

We call a theory T *axiomatized* if it is finite and if the set $\mathrm{NAx}_T \subset \mathbb{N}$ of Gödel numbers of all nonlogical axioms of T is recursive.

That T is axiomatized means that there is an algorithm to decide whether a formula of T is an axiom. This is a natural condition on the set of axioms for any axiomatic system.

We define

$$\mathrm{Ax}_T(n) \Leftrightarrow n \text{ is the Gödel number of an axiom of } T.$$

The following result is obvious from Theorem 6.3.12 and the definition of axiomatized theories.

Proposition 6.3.13. *If* T *is axiomatized, then* Ax_T *is recursive.*

Example 6.3.14. The theory N has only finitely many nonlogical axioms. Thus, N is axiomatized.

Exercise 6.3.15. (i) Show that the set of Gödel numbers of formulas of N of the form

$$A_v[0] \to \forall v(A \to A_v[Sv]) \to A,$$

where A is a formula and v a variable, is recursive.

(ii) Show that Peano arithmetic is axiomatized.
(iii) Show that ZF and ZFC are axiomatized. (Note that the language of set theory has only one binary relation symbol. You need only show that the sets of all Gödel numbers of comprehension axioms and those of replacement axioms are recursive. Show this for replacement axioms also.)

Henceforth, in this section, T will be a fixed finite theory.

We now introduce some recursive predicates related to rules of inference:

$$\mathrm{cont}(n,m) \Leftrightarrow m = \langle SN(\vee), n, n\rangle.$$

If $n = \lceil B\rceil$ and $m = \lceil B \vee B\rceil$, then $\mathrm{cont}(m,n)$ holds. Further, if n is the Gödel number of a formula B, and if m is the Gödel number of a formula A, and if $\mathrm{cont}(m,n)$ holds, then A can be inferred from B by the contraction rule.

We define recursive predicates corresponding to other rules as follows:

$$\mathrm{exp}(m,n) \Leftrightarrow \mathrm{form}(n) \wedge m = \langle SN(\vee), (m)_1, n\rangle,$$

$$\begin{aligned}\mathrm{assoc}(m,n) \Leftrightarrow n &= \langle SN(\vee), (n)_1, \langle SN(\vee), ((n)_2)_1, ((n)_2)_2\rangle\rangle,\\ \wedge (m)_0 &= SN(\vee) \wedge ((m)_1)_0 = SN(\vee),\\ \wedge ((m)_1)_1 &= (n)_1,\\ \wedge ((m)_1)_2 &= ((n)_2)_1 \wedge (m)_2 = ((n)_2)_2,\end{aligned}$$

$$\begin{aligned}\mathrm{cut}(l,m,n) \Leftrightarrow m &= \langle SN(\vee), (m)_1, (m)_2\rangle,\\ \wedge n &= \langle SN(\vee), \langle SN(\neg), (m)_1\rangle, (n)_2\rangle,\\ \wedge l &= \langle SN(\vee), (m)_2, (n)_2\rangle,\end{aligned}$$

and

$$\begin{aligned}\mathrm{intr}(m,n) \Leftrightarrow n &= \langle SN(\vee), \langle SN(\neg), ((n)_1)_1\rangle, (n)_2\rangle\\ \wedge m &= \langle SN(\vee), \langle SN(\neg), \langle SN(\exists), (((m)_1)_1)_1, ((n)_1)_1\rangle, (n)_2\rangle\rangle\\ \wedge \mathrm{vble}(((m)_1)_1) &\wedge \neg \mathrm{fr}(((m)_1)_1, (n)_2).\end{aligned}$$

Exercise 6.3.16. Show that the predicates cont, assoc, cut, and intr are recursive.

We continue the idea further. Recall that any proof in a theory is a finite sequence of formulas of the theory. Hence, the following definition is quite important. It will be used to code proofs by numbers in such a way that there is a mechanical procedure to decide whether a natural number codes a proof. Further, the procedure decodes the proof.

If $A_1, \ldots, A_n$ is a sequence of formulas of T, then the number

$$\langle \lceil A_1\rceil, \ldots, \lceil A_n\rceil\rangle$$

will be called the Gödel number of the sequence.

Proposition 6.3.17. *If T is axiomatized, then the set* Pr_T *of Gödel numbers of all proofs in T is recursive.*

Proof. This follows from the following equivalence:

$$\begin{aligned}\mathrm{Pr}_T(n) \Leftrightarrow\ & \mathrm{seq}(n) \wedge \forall i < lh(n)[\mathrm{Ax}_T((n)_i) \\ & \vee \exists j < i((\mathrm{cont} \vee \mathrm{assoc} \vee \mathrm{intr})((n)_i,(n)_j)) \\ & \vee \exists j,k < i[\mathrm{cut}((n)_i,(n)_j,(n)_k)].\end{aligned}$$

□

Proposition 6.3.18. *If T is axiomatized, then the set* $\mathrm{Prf}_T \subset \mathbb{N} \times \mathbb{N}$ *of all pairs of numbers (m,n), such that m is the Gödel number of a proof of a formula whose Gödel number is n, is recursive.*

Proof. Note that for any m, n,

$$\mathrm{Prf}_T(m,n) \Leftrightarrow lh(m) > 0 \wedge \mathrm{Pr}_T(m) \wedge (m)_{lh(m) \dot{-} 1} = n.$$

□

Theorem 6.3.19. *If T is axiomatized, then the set* Thm_T *of Gödel numbers of all theorems of T is semirecursive.*

Proof. This follows from the following equivalence:

$$\mathrm{Thm}_T(n) \Leftrightarrow \exists m[\mathrm{Prf}_T(m,n)].$$

□

But is the predicate Thm_T recursive? Not always. However, in the next section we shall prove that if, moreover, T is complete, then Thm_T is recursive. Quite interestingly, in the next chapter we shall show that Thm_N, Thm_{PA}, and Thm_{ZF} are not recursive. This is the essence of Gödel's first incompleteness theorem.

Remark 6.3.20. Let $F(X_1,\ldots,X_n) \in \mathbb{Z}[X_1,\ldots,X_n]$. We can give a similar coding scheme and assign a natural number, say $g(F)$, to F in such a way that Hilbert's tenth problem has a positive answer if and only if the set H of all those $g(F)$ for which the Diophantine equation $F = 0$ has an integral solution is recursive. We invite readers to carry out such a coding. It has been shown that Hilbert's tenth problem has a negative answer.

6.4 Decidable Theories

We call a finite theory T *decidable* if Thm_T is recursive. Otherwise, the theory is called *undecidable*.

Thus, if a theory is decidable, there is an algorithm to decide whether a formula of T is a theorem or not. Hilbert believed that there should be a decidable set of axioms of number theory (and of most of the interesting mathematical theories) such that every true formula of N is provable. Gödel shocked the mathematical world by showing the impossibility of Hilbert's dream.

Our next result is the following.

Theorem 6.4.1. *Every axiomatized complete theory is decidable.*

We need the following lemma.

Lemma 6.4.2. *There is a recursive map $g : \mathbb{N} \to \mathbb{N}$ such that if n is the Gödel number of a formula A, then $g(n)$ is the Gödel number of a closed formula B such that*

$$T \vdash A \Leftrightarrow T \vdash B.$$

Proof. Consider the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$f(0,n) = n,$$

and for all $m \geq 0$,

$$f(m+1,n) = \langle SN(\neg), \langle SN(\exists), \langle 2m \rangle, \langle SN(\neg), f(m,n) \rangle \rangle \rangle.$$

It is routine to check that f is recursive. Further, if n is the Gödel number of a formula A, then $f(m+1,n)$ is the Gödel number of $\forall x_m \ldots \forall x_0 A$, where $x_0, \ldots, x_m$ are the first $(m+1)$ variables in alphabetical order. Now set

$$g(n) = f(n,n), \quad n \in \mathbb{N}.$$

Using the closure theorem, generalization rule, and the closure properties of the class of recursive functions and recursive predicates, it is easy to check that the map g has the desired properties. □

Proof of 6.4.1. By Theorems 6.2.4 and 6.3.19, it is sufficient to show that $\neg \mathrm{Thm}_T$ is semirecursive. Fix any $n \in \mathbb{N}$. Now note the following:

$$\begin{aligned} \neg \mathrm{Thm}_T(n) &\Leftrightarrow \neg \mathrm{form}(n) \vee \mathrm{Thm}_T(\langle SN(\neg), g(n) \rangle) \\ &\Leftrightarrow \exists m[\neg \mathrm{form}(n) \vee \mathrm{Prf}_T(m, \langle SN(\neg), g(n) \rangle)]. \end{aligned}$$

Since Prf_T is recursive and g is recursive, it follows that $\neg \mathrm{Thm}_T$ is semirecursive. □

This is a very important theorem. It says that if T is axiomatized and Thm_T is not recursive, then T is not complete. Gödel uses it beautifully to establish the first incompleteness theorem.

Exercise 6.4.3. Let $p = 0$ or a prime > 1. Show that the theory $ACF(p)$ is axiomatized and decidable.

Exercise 6.4.4. Show that the theories *DLO*, *DAG*, *ODAG*, and *RCF* are axiomatized and decidable.

We call a structure M of a finite language L *decidable* if Th_M is recursive. We now have the following theorem.

Theorem 6.4.5. *The rings $\mathbb{R}$ and $\mathbb{C}$ are decidable. Also, the ordered field $\mathbb{R}$ is decidable.*

Similarly, we see that the linearly ordered set $\mathbb{Q}$, the group $\mathbb{Q}$, and the ordered group $\mathbb{Q}$ are decidable.

Theorem 6.4.6. *If T is a decidable theory with elimination of quantifiers, then there is an algorithm that, given any formula $\varphi[\overline{x}]$, outputs an open formula $\psi[\overline{x}]$ such that*

$$T \vdash \varphi \leftrightarrow \psi.$$

Proof. Let $\{\psi_n\}$ be a recursive enumeration of all open formulas of T. Now given any $\varphi[\overline{x}]$, one scans through this recursive enumeration one by one and stops when one gets an open formula $\psi_n[\overline{x}]$ such that $T \vdash \forall \overline{x}(\varphi \leftrightarrow \psi_n)$. □

Theorem 6.4.7. *Let M be a structure for a finite language L and $N \subset M$ a definable substructure. If M is decidable, then so is N.*

Proof. Let $\varphi[x, i_{\overline{a}}], \overline{a} \in M$, define N. Recall that in Proposition 2.8.19, we associated to each formula ψ a formula ψ^N such that for every $\overline{b} \in N^n$,

$$N \models \psi[i_{\overline{b}}] \Leftrightarrow M \models \psi^N[i_{\overline{b}}].$$

Now note that $\psi \to \psi^N$ is recursive. Fix an algorithm $\mathscr{A}$ that decides whether a sentence of L_M is true in M or not. Given any sentence ψ of L_N, first compute ψ^N and then run the algorithm $\mathscr{A}$ on ψ^N. This works. □

This result in turn says that if N is undecidable, then so is M.

A simple extension T' of T is called a *finite extension* if at most finitely many nonlogical axioms of T' are not theorems of T.

Theorem 6.4.8. *Let T be an undecidable theory. Suppose T' satisfies one of the following conditions:*

(a) T' is a conservative extension of T.
(b) T is an extension by definitions of T'.
(c) T is a finite consistent extension of T'.
(d) T has a faithful interpretation in T'.

Then T' is undecidable.

Proof. In each case, we show that there is a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that if n is the Gödel number of a formula φ of T, then $f(n)$ is the Gödel number of a formula φ^* of T' such that

$$T \vdash \varphi \Leftrightarrow T' \vdash \varphi^*.$$

Assuming this is done, we complete the proof first. Suppose in some case (a)–(d), $\mathrm{Thm}_{T'}$ is recursive. Then

$$\mathrm{Thm}_T(n) \Leftrightarrow \mathrm{form}_T(n) \wedge \mathrm{Thm}_{T'}(f(n)).$$

Hence, Thm_T is recursive by the closure properties of the set of recursive predicates. This contradicts that T is undecidable.

In case (a), we take $f(n) = n$. Since an extension by definitions of T is a conservative extension of T (Theorem 4.6.6), the result in case (b) follows from case (a).

We now prove the result in case (c). Let $B_1, \ldots, B_m$ be an enumeration of the closures of all the nonlogical axioms of T' that are not theorems of T. Let p be the Gödel number of $\neg B_1 \vee \cdots \vee \neg B_m$. If n is the Gödel number of a formula A of T, then we define

$$f(n) = \langle SN(\vee), p, n \rangle.$$

Otherwise, we define $f(n) = 0$. Since the set of Gödel numbers of formulas is a recursive set, it follows that f is recursive. By the reduction theorem (Exercise 4.3.6),

$$\mathrm{Thm}_T(n) \Leftrightarrow \mathrm{Thm}_{T'}(f(n)).$$

To prove the result in case (d), fix a faithful interpretation I of T in T'. It is fairly routine to see that there is a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that if n is the Gödel number of a formula A of T, then $f(n)$ is the Gödel number of A^I (Exercise 6.3.10). Since I is a faithful interpretation,

$$\mathrm{Thm}_T(n) \Leftrightarrow \mathrm{form}_T(n) \wedge \mathrm{Thm}_{T'}(f(n)).$$

□

Chapter 7
Representability and Incompleteness Theorems

This chapter gives the most important landmarks of mathematical logic – the incompleteness theorems of Gödel. We still have to do some work, which we do in the first section. As a side output, in Sect. 7.3, we initiate the study of recursion theory.

7.1 Representability

In this section, we present yet another beautiful concept, called *representability*, introduced by Gödel, which shows that recursive functions and predicates can be represented by formulas of the theory N.

Let $P \subset \mathbb{N}^p$. We say that a formula A of N with distinct variables $v_1, \ldots, v_p$ *represents* P if for every sequence of numbers $n_1, \ldots, n_p$,

$$(n_1, \ldots, n_p) \in P \Rightarrow N \vdash A_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}]$$

and

$$(n_1, \ldots, n_p) \notin P \Rightarrow N \vdash \neg A_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}].$$

We say that P is *representable* if some formula A with distinct variables $v_1, \ldots, v_p$ represents it.

Let $f : \mathbb{N}^p \to \mathbb{N}$ be a map. We say that a formula A of N with distinct variables $v_1, \ldots, v_p, w$ *represents* f if for every sequence of numbers $n_1, \ldots, n_p$,

$$N \vdash A_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}] \leftrightarrow w = k_m,$$

where $m = f(n_1, \ldots, n_p)$. We say that f is *representable* if some formula A with distinct variables $v_1, \ldots, v_p, w$ represents it.

Theorem 7.1.1. *Every representable predicate $P \subset \mathbb{N}^n$ is recursive.*

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_7,
© Springer Science+Business Media New York 2013

Proof. Let a formula φ of N with variables $x_1, \ldots, x_n$ represent P. Then for every $(a_1, \ldots, a_n) \in \mathbb{N}^n$, we have

$$P(a_1, \ldots, a_n) \Rightarrow N \vdash \varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}]$$

and

$$\neg P(a_1, \ldots, a_n) \Rightarrow N \vdash \neg\varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}].$$

Since N is consistent, we now have

$$P(a_1, \ldots, a_n) \Leftrightarrow \mathrm{Thm}_N(\ulcorner \varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}] \urcorner)$$

and

$$\neg P(a_1, \ldots, a_n) \Leftrightarrow \mathrm{Thm}_N(\ulcorner \neg\varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}] \urcorner).$$

Since N is axiomatized, by Theorem 6.3.19, Thm_N is semirecursive. Further, the maps

$$(a_1, \ldots, a_n) \to \ulcorner \varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}] \urcorner$$

and

$$(a_1, \ldots, a_n) \to \ulcorner \neg\varphi_{x_1,\ldots,x_n}[k_{a_1}, \ldots, k_{a_n}] \urcorner$$

are recursive. (See Exercise 6.3.6.) Hence, both P and $\neg P$ are semirecursive. The result now follows from Theorem 6.2.4. □

The main theorem of this section is as follows.

Theorem 7.1.2 (Representability theorem). *Every recursive function and every recursive predicate is representable.*

This result is proved essentially by showing that the initial functions are representable and that the set of all representable functions is closed under composition and minimalization. We will see later in this section that every representable function is recursive.

Lemma 7.1.3. *Let P be a p-ary representable predicate on $\mathbb{N}$ and $x_1, \ldots, x_p$ distinct variables. Then there is a formula B of N such that B with $x_1, \ldots, x_p$ represents P.*

Proof. Let A with $v_1, \ldots, v_p$ represent P. Taking a variant of A, if necessary, by the variant theorem, we can assume that $x_1, \ldots, x_p$ do not occur in A. Now take B to be

$$A_{v_1,\ldots,v_p}[x_1, \ldots, x_p].$$ □

The following result is also proved similarly.

Lemma 7.1.4. *Let f be a p-ary representable function on $\mathbb{N}$ and $x_1, \ldots, x_p, y$ distinct variables. Then there is a formula B of N such that B with $x_1, \ldots, x_p, y$ represents f.*

Let f be a p-ary function. We say that a term t of N with distinct variables $v_1,\ldots,v_p$ represents f if for every $n_1,\ldots,n_p$,

$$N \vdash t_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}] = k_m,$$

where $m = f(n_1,\ldots,n_p)$.

Lemma 7.1.5. *Let a term t with distinct variables $v_1,\ldots,v_p$ represent $f : \mathbb{N}^p \to \mathbb{N}$, and let w be a variable distinct from each v_i. Then the formula $w = t$ with $v_1,\ldots,v_p,w$ represents f.*

Proof. Let $m = f(n_1,\ldots,n_p)$. We have

$$N \vdash t_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}] = k_m.$$

We are required to show that

$$N \vdash w = t_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}] \leftrightarrow w = k_m.$$

This essentially follows from the equality axiom, the substitution rule, and the detachment rule. □

Proposition 7.1.6. *A p-ary predicate P is representable if and only if χ_P is representable.*

Proof. Let A with distinct variables $v_1,\ldots,v_p$ represent P. Let the variable w be distinct from each of v_i, and let B be the formula

$$(A \wedge w = k_0) \vee (\neg A \wedge w = k_1).$$

Fix any $(n_1,\ldots,n_p)$. Suppose $(n_1,\ldots,n_p) \in P$. Then

$$N \vdash A_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}]. \tag{1}$$

By (1) and the tautology theorem,

$$N \vdash B_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}] \leftrightarrow w = k_0.$$

If $(n_1,\ldots,n_p) \notin P$,

$$N \vdash \neg A_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}]. \tag{2}$$

By (2) and the tautology theorem,

$$N \vdash B_{v_1,\ldots,v_p}[k_{n_1},\ldots,k_{n_p}] \leftrightarrow w = k_1.$$

Conversely, assume that A with distinct variables $v_1,\ldots,v_p,w$ represents χ_P. Let B be the formula $A_w[k_o]$. We claim that B with $v_1,\ldots,v_p$ represents P.

Since $\neg(Sx = 0)$ is an axiom of N,

$$N \vdash \neg(k_1 = k_0).$$

Fix any $(n_1, \ldots, n_p)$. Suppose $(n_1, \ldots, n_p) \in P$. Then

$$N \vdash w = k_0 \leftrightarrow A_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}].$$

By the substitution rule,

$$N \vdash k_0 = k_0 \leftrightarrow B_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}].$$

Since $N \vdash k_0 = k_0$, we have

$$N \vdash B_{v_1,\ldots,v_p}[k_{n_1}, \ldots, k_{n_p}].$$

Since $N \vdash \neg(k_1 = k_0)$, the other case is similarly proved. □

Note that by the previous proposition, to prove the representability theorem, we only need to show that every recursive function is representable. We shall show that all initial functions are representable and that the set of all representable functions is closed under composition and minimalization.

Proposition 7.1.7. *The formula $x = y$ with distinct variables x and y represents $=$ in N.*

Proof. We need to show the following:

$$m = n \Rightarrow N \vdash k_m = k_n$$

and

$$m \neq n \Rightarrow N \vdash \neg(k_m = k_n).$$

The first assertion follows from the identity axiom and the substitution rule. By the symmetry theorem (Lemma 3.5.1), in the proof of the second assertion, we can assume that $m > n$. We proceed by induction on n. If $n = 0$, for all m, then this follows from the axiom (1) of N and the substitution rule. Let $m \geq n > 0$, and let the second assertion hold for $n - 1$ and all m. Now note the following:

$$N \vdash k_m = k_n \Rightarrow k_{m-1} = k_{n-1}$$

by axiom (2) of N, the closure theorem, and the substitution rule. By the induction hypothesis, we have

$$N \vdash \neg(k_{m-1} = k_{n-1}).$$

Hence,

$$N \vdash \neg(k_m = k_n)$$

by the tautology theorem. □

Proposition 7.1.8. *All initial functions are representable.*

Proof. (i) Let $v_1, \ldots, v_n$ be distinct variables, and let t be the term v_i. Fix natural numbers $p_1, \ldots, p_n$. Clearly

$$N \vdash t_{v_1,\ldots,v_n}[k_{p_1}, \ldots, k_{p_n}] = k_{p_i}.$$

This shows that the projection maps Π_i^n, $n \geq 1$, $1 \leq i \leq n$, are representable.

(ii) Let x and y be distinct variables, and let t be the term $x+y$. We show that t with x, y represents $+$. We need to show that for all natural numbers m, n,

$$N \vdash k_m + k_n = k_{m+n}. \tag{1}$$

We fix m and show (1) by induction on n. By axiom (3) of N, we have

$$N \vdash k_m + 0 = k_m.$$

Now assume that

$$N \vdash k_m + k_n = k_{m+n}. \tag{2}$$

By axiom (4) of N and the substitution rule, we have

$$N \vdash k_m + k_{n+1} = S(k_m + k_n).$$

By the equality axiom and (2), we have

$$N \vdash S(k_m + k_n) = k_{m+n+1}.$$

Thus,

$$N \vdash k_m + k_{n+1} = k_{m+n+1}.$$

(iii) Similarly, using axioms (5) and (6) of N, we show that the term $x \cdot y$ with distinct variables x and y represents $\cdot$, the multiplication.

(iv) Finally, we show that the formula $x < y$ with distinct variables x and y represents $<$. This in turn will show that $\chi_<$ is representable, and the result will be proved. We are required to show that for every natural number m and n,

$$m < n \Longrightarrow N \vdash k_m < k_n \tag{3}$$

and

$$\neg(m < n) \Longrightarrow N \vdash \neg(k_m < k_n). \tag{4}$$

For every n, we show that (3) and (4) hold for all m. We proceed by induction on n. For $n = 0$, we only need to prove (4) for all m; (4) follows from axiom (7) of N.

Now assume that for some n, (3) and (4) hold for all m. Suppose $m < n+1$. If $m < n$, then

$$N \vdash k_m < k_n,$$

and hence

$$N \vdash k_m < k_{n+1}$$

by axiom (8), the substitution rule, and the induction hypothesis. If $m = n$, then

$$N \vdash k_m = k_n$$

by Proposition 7.1.7. Then

$$N \vdash k_m < k_{n+1}$$

by the same arguments.

Now suppose $m \geq n+1$. Then,

$$N \vdash \neg(k_m < k_n)$$

by the induction hypothesis and

$$N \vdash \neg(k_m = k_n)$$

by Proposition 7.1.7. Thus,

$$N \vdash \neg(k_m < k_{n+1})$$

using axiom (8) of N and the tautology theorem. □

Proposition 7.1.9. *The set of all representable functions is closed under composition.*

Proof. Let

$$h(n_1, \ldots, n_k) = g(f_1(n_1, \ldots, n_k), \ldots, f_m(n_1, \ldots, n_k)),$$

where g, $f_1, \ldots, f_m$ are representable. We choose distinct variables, $u, v_1, \ldots, v_m$, $w_1, \ldots, w_k$ and formulas $B, A_1, \ldots, A_m$ such that B with $v_1, \ldots, v_m$, and u represents g, and A_i with $w_1, \ldots, w_k$, and v_i represents f_i, $1 \leq i \leq m$.

Now consider the formula C defined by

$$\exists v_1 \cdots \exists v_m (A_1 \wedge \cdots \wedge A_m \wedge B).$$

We claim that C with $w_1, \ldots, w_k$ and u represents h. Fix $(n_1, \ldots, n_k)$. Let $p_i = f_i(n_1, \ldots, n_k)$ and $q = g(p_1, \ldots, p_m)$. Then $q = h(n_1, \ldots, n_k)$. For $1 \leq i \leq m$, set

$$A_i' = (A_i)_{w_1, \ldots, w_k}[k_{n_1}, \ldots, k_{n_k}]$$

and

$$C' = C_{w_1, \ldots, w_k}[k_{n_1}, \ldots, k_{n_k}].$$

By our assumptions, we have

$$N \vdash A_i' \leftrightarrow v_i = k_{p_i},$$

$1 \leq i \leq m$. By the equivalence theorem, we have

$$N \vdash C' \leftrightarrow \exists v_1 \cdots \exists v_m (v_1 = k_{p_1} \wedge \cdots \wedge v_m = k_{p_m} \wedge B).$$

Let D denote the formula

$$\exists v_1 \cdots \exists v_m (v_1 = k_{p_1} \wedge \cdots \wedge v_m = k_{p_m} \wedge B).$$

By the repeated application of Proposition 4.2.26, we have

$$N \vdash \exists v_2 \cdots \exists v_m (v_2 = k_{p_2} \wedge \cdots \wedge v_m = k_{p_m} \wedge B_{v_1}[k_{p_1}]) \leftrightarrow D,$$

$$\vdots$$

$$N \vdash B_{v_1,\ldots,v_m}[k_{p_1},\ldots,k_{p_m}] \leftrightarrow \exists v_m (v_m = k_{p_m} \wedge B_{v_1,\ldots,v_{m-1}}[k_{p_1},\ldots,k_{p_{m-1}}]).$$

By the equivalence theorem and the tautology theorem, we get

$$N \vdash C' \leftrightarrow B_{v_1,\ldots,v_m}[k_{p_1},\ldots,k_{p_m}].$$

Since B with $v_1,\ldots,v_m$ and u represents g and $q = g(p_1,\ldots,p_m)$, we have

$$N \vdash B_{v_1,\ldots,v_m}[k_{p_1},\ldots,k_{p_m}] \leftrightarrow u = k_q.$$

Thus by the equivalence theorem,

$$N \vdash C' \leftrightarrow u = k_q.$$

□

It remains to show that the set of all representable functions is closed under minimalization.

Proposition 7.1.10. *The set of all representable functions is closed under minimalization.*

Proof. Let $f(m,\overline{n})$ be representable, where $\overline{n} = (n_0,\ldots,n_{p-1})$. Let A with $v, v_0,\ldots, v_{p-1}$ and w represent f. Assume that

$$\forall \overline{n} \exists m (f(m,\overline{n}) = 0).$$

Let

$$g(\overline{n}) = \mu m (f(m,\overline{n}) = 0).$$

We now show that g is representable.

Let u be a new variable, and let B be the formula

$$A_w[0] \wedge \forall u (u < v \rightarrow \neg A_{v,w}[u,0]).$$

We claim that B with $v_0,\ldots,v_{p-1}$ and v represents g.

Fix $\overline{n} = (n_0, \ldots, n_{p-1}) \in \mathbb{N}^p$. Let $m = g(\overline{n})$. Then $f(i, \overline{n}) = l_i \neq 0$, $i < m$, and $f(m, \overline{n}) = 0$. Set

$$A' = A_{v_0,\ldots,v_{p-1}}[k_{n_0}, \ldots, k_{n_{p-1}}]$$

and

$$B' = B_{v_0,\ldots,v_{p-1}}[k_{n_0}, \ldots, k_{n_{p-1}}].$$

We have

$$N \vdash A'_v[k_i] \leftrightarrow w = k_{l_i},$$

$i < m$, and

$$N \vdash A'_v[k_m] \leftrightarrow w = 0.$$

Since $l_i \neq 0$, we have

$$N \vdash \neg(0 = k_{l_i}),$$

$i < m$. Thus, for all $i < m$, we have

$$N \vdash \neg A'_{v,w}[k_i, 0]$$

and

$$N \vdash A'_{v,w}[k_m, 0].$$

Hence, by Proposition 4.7.2,

$$N \vdash (A'_w[0] \wedge \forall u(u < v \rightarrow \neg A'_{v,w}[u, 0])) \rightarrow v = k_m,$$

i.e.,

$$N \vdash B' \leftrightarrow v = k_m.$$

Our claim is proved. □

We have completed the proof of the representability theorem.

Exercise 7.1.11. Show that every representable function $f : \mathbb{N}^n \rightarrow \mathbb{N}$ is recursive.

Remark 7.1.12. We have presented an amazing loop constructed by Gödel that has been likened to the music of Bach and the drawings of Escher [6]. To make statements about numbers, first one develops a formal language (for instance, the language of N) and expresses statements about numbers syntactically in N (or in a suitable extension of N). In this language, a statement about numbers is now a sentence of N. Then, using the idea of Gödel numbers, one expresses statements about syntactical objects by numbers themselves. Finally, by the representability theorem, one represents a certain class S of statements about numbers by formulas of N. For instance, if

$$\{n \in \mathbb{N} : n \text{ is the Gödel number of a sentence in } S\}$$

is recursive, we represent it by a formula of N. This technique enables one to hop into the theory N from the metaworld and vice versa. Thus many questions in the metaworld are expressed by formulas of N. Sometimes even a proof in the

metaworld is converted into a proof inside the theory. Thus, Gödel built a very powerful tool and destroyed the beliefs of many great mathematicians of his time, including Hilbert. In the remaining part of this chapter, we present some remarkable discoveries of Gödel.

7.2 First Incompleteness Theorem

Theorem 7.2.1 (First incompleteness theorem). *Every axiomatized, consistent extension of N is undecidable and so incomplete.*

Proof. To arrive at a contradiction, assume that Thm_T is recursive. Fix a variable v. There is a recursive function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that if m is the Gödel number of a formula B of T, then $f(m,n)$ is the Gödel number of $B_v[k_n]$. Then the binary predicate $U \subset \mathbb{N} \times \mathbb{N}$ defined by

$$U(m,n) \Leftrightarrow \mathrm{Thm}_T(f(m,n))$$

is recursive. Thus, the predicate

$$P(m) \Leftrightarrow \neg U(m,m)$$

is recursive.

By the representability theorem, there is a formula A of N such that A with v represents P. This means that for every $n \in \mathbb{N}$,

$$n \in P \Rightarrow N \vdash A_v[k_n]$$

and

$$n \notin P \Rightarrow N \vdash \neg A_v[k_n].$$

Since T is an extension of N, A is a formula of T, and for every $n \in \mathbb{N}$,

$$n \in P \Rightarrow T \vdash A_v[k_n] \qquad (a)$$

and

$$n \notin P \Rightarrow T \vdash \neg A_v[k_n]. \qquad (b)$$

Now let m be the Gödel number of A.

Suppose $m \in P$. Then, by (a), $T \vdash A_v[k_m]$, i.e., $U(m,m)$ holds by the definition of U. Hence, $m \notin P$ by the definition of P. This is a contradiction.

On the other hand, suppose $m \notin P$. Then, by (b), $T \vdash \neg A_v[k_m]$. Since T is consistent, this implies that $T \nvdash A_v[k_m]$. Therefore, by the definition of U, $\neg U(m,m)$ holds. But then $m \in P$ by the definition of P. We have arrived at a contradiction again. □

Remark 7.2.2. Since $\mathbb{N}$ with the usual interpretations of S, $+$, $\cdot$, and $<$ is a model of *PA*, *PA* is consistent. Further, by Exercise 6.3.15, *PA* is axiomatized. Hence, by Theorem 6.4.8, *PA* is undecidable, and so incomplete by the first incompleteness theorem.

Remark 7.2.3. There is an extension by definitions of *ZF* (or of *ZFC*) in which there is a suitable interpretation of the theory *N* so that we can carry out the same arguments and prove the incompleteness of *ZF* and *ZFC*.

Corollary 7.2.4. *The set of natural numbers is undecidable in the language of N, as an ordered ring as well as a ring.*

Proof. The first part is a direct consequence of the first incompleteness theorem. Since $S(n) = n+1$ is clearly definable in the language of a ring and using Lagrange's theorem, we saw that $<$ on $\mathbb{N}$ is definable in the language of a ring, and the remaining part of the result also follows. □

We have mentioned that Julia Robinson showed that the ring of integers $\mathbb{N}$ is a definable subset of the ring $\mathbb{Q}$ of rational numbers (Theorem 2.8.18). Thus, by Theorems 7.2.4 and 6.4.7, we get the following theorem.

Theorem 7.2.5. *The ring $\mathbb{Q}$ is undecidable.*

However, since *DLO* and *ODAG* are complete, $\mathbb{Q}$ is decidable as an ordered space as well as an ordered ring.

Remark 7.2.6 (Comparison with the liar's paradox). In the foregoing proof we produced a formula $A[v]$ that says that a formula whose Gödel number is m is not provable for "$v = m$." This is similar to the statement "I am lying" of the liar's paradox. This argument also shows a way to make a self-referential statement inside a theory.

Remark 7.2.7. Now we can state Hilbert's problem precisely. *Is there?* an axiomatized extension P' of *PA* such that a sentence of P' is true (in the standard model) if and only if it is a theorem of P'. Since such a theory P' is complete, the first incompleteness theorem answers Hilbert's question in the negative.

7.3 Arithmetical Sets

In this section, we present some basic results in recursion theory. We have already initiated the study of recursive and semirecursive sets. The representability theorem and the ideas contained in the proof of the first incompleteness theorem help us to continue this study further.

A set of predicates (of not necessarily fixed parity) on $\mathbb{N}$ will be called a *pointclass*. For brevity, we shall write $\overline{n}$ for $(n_1, \ldots, n_k)$. For $P \subset \mathbb{N} \times \mathbb{N}^k$, we define k-ary predicates $\exists^\omega P$ and $\forall^\omega P$ by

$$\exists^{\omega} P(\overline{n}) \Leftrightarrow \exists m P(m, \overline{n})$$

and

$$\forall^{\omega} P(\overline{n}) \Leftrightarrow \forall m P(m, \overline{n}).$$

If Γ is a pointclass, then we define

$$\neg\Gamma = \{\neg P : P \in \Gamma\},$$

$$\exists^{\omega}\Gamma = \{\exists^{\omega} P : P \in \Gamma\},$$

and

$$\forall^{\omega}\Gamma = \{\forall^{\omega} P : P \in \Gamma\}.$$

Note that for any pointclass,

$$\forall^{\omega}\Gamma = \neg\exists^{\omega}\neg\Gamma$$

and

$$\exists^{\omega}\Gamma = \neg\forall^{\omega}\neg\Gamma.$$

In the sequel, these two identities and other such simple set-theoretic identities will be used without mention.

We define *arithmetical pointclasses* Σ^0_n, Π^0_n, and Δ^0_n, $n \geq 1$, by induction as follows:

$$\Sigma^0_1 = \text{ the poinclass of all semirecursive sets,}$$

$$\Pi^0_n = \neg\Sigma^0_n,$$

$$\Sigma^0_{n+1} = \exists^{\omega}\Pi^0_n,$$

and

$$\Delta^0_n = \Sigma^0_n \cap \Pi^0_n.$$

Theorem 7.3.1. *The pointclass Δ^0_1 consists precisely of all recursive sets and*

$$\Sigma^0_1 = \exists^{\omega}\Delta^0_1 \text{ and } \Pi^0_1 = \forall^{\omega}\Delta^0_1.$$

Proof. The first assertion is just a restatement of Kleene's theorem (Theorem 6.2.4); the second one follows from the definition of semirecursive sets and Kleene's theorem (Theorem 6.2.4), and the third one follows from the second one. □

Call a pointclass Γ closed under *recursive substitutions* if when $P(n_1, \ldots, n_k) \in \Gamma$, for all recursive functions $f_i : \mathbb{N}^l \to \mathbb{N}$, $1 \leq i \leq k$, the l-ary predicate Q defined by

$$Q(m_1, \ldots, m_l) \Leftrightarrow P(f_1(m_1, \ldots, m_l), \ldots, f_k(m_1, \ldots, m_l))$$

is in Γ.

Proposition 7.3.2. *(1) Each arithmetical pointclass is closed under $\vee$, $\wedge$ (thus, under finite unions and finite intersections), and recursive substitutions.*

(2) *For each n, Σ^0_n is closed under $\exists^\omega$, Π^0_n under $\forall^\omega$, and Δ^0_n under $\neg$.*
(3) *For each n,*

$$\Sigma^0_n = \exists^\omega \Delta^0_n \text{ and } \Pi^0_n = \forall^\omega \Delta^0_n,$$
$$\Sigma^0_n \cup \Pi^0_n \subset \Delta^0_{n+1}.$$

Proof. We shall prove (1) by induction on n. The closure properties listed in (1) were already proved for Σ^0_1 in Proposition 6.2.2. Then the result for Π^0_1 follows from its definition. The result for Δ^0_1 is now easily seen.

Assume that Σ^0_n, Π^0_n, and Δ^0_n have the closure properties listed in (1). Note that a pointclass Γ is closed under $\exists^\omega$ if and only if $\neg\Gamma$ is closed under $\forall^\omega$; a pointclass Γ is closed under recursive substitutions if and only if $\neg\Gamma$ is, and if both Γ and $\neg\Gamma$ satisfy the closure properties listed in (1), then so does $\Delta = \Gamma \cap \neg\Gamma$.

Now let $f_i : \mathbb{N}^l \to \mathbb{N}$, $1 \le i \le k$, be recursive functions. Let $P(m_1, \ldots, m_k) \in \Pi^0_{n+1}$. We are required to show that the predicate Q defined by

$$Q(\bar{l}) \Leftrightarrow P(f_1(\bar{l}), \ldots, f_k(\bar{l}))$$

is in Π^0_{n+1}. Get $P' \in \Sigma^0_n$ such that $P = \forall^\omega P'$. Then

$$Q(\bar{l}) \Leftrightarrow \forall m P'(m, f_1(\bar{l}), \ldots, f_k(\bar{l})).$$

Since Σ^0_n is closed under recursive substitutions, $Q \in \Pi^0_{n+1}$.

Let $P, Q \in \Sigma^0_{n+1}$. Get $P', Q' \in \Pi^0_n$ such that $P = \exists^\omega P'$ and $Q = \exists^\omega Q'$. The following identities are easy to check:

$$P \vee Q \Leftrightarrow \exists^\omega (P' \vee Q')$$

and

$$(P \wedge Q)(\bar{l}) \Leftrightarrow \exists m (P'((m)_0, \bar{l}) \wedge Q'((m)_1, \bar{l}).$$

By the induction hypothesis, it follows that Σ^0_{n+1} is closed under $\vee$ and $\wedge$. This in turn implies that Π^0_{n+1} and Δ^0_{n+1} are closed under $\vee$ and $\wedge$.

We shall now prove (2). The pointclass Δ^0_n is clearly closed under $\neg$. By Proposition 6.2.2, Σ^0_1 is closed under $\exists^\omega$. Let $P(p, q, \bar{l}) \in \Pi^0_n$. Then

$$\exists p \exists q P(p, q, \bar{l}) \Leftrightarrow \exists m P((m)_0, (m)_1, \bar{l})).$$

Since Π^0_n is closed under recursive substitutions, it follows that Σ^0_{n+1} is closed under $\exists^\omega$. Hence, Π^0_{n+1} is closed under $\forall^\omega$.

We prove (3) also by induction on n. By Propositions 6.2.1 and 6.2.2, $\Sigma^0_1 = \exists^\omega \Delta^0_1$. Thus, $\Pi^0_1 = \forall^\omega \Delta^0_1$. Further, since $\Delta^0_1 \subset \Pi^0_1$, we conclude that $\exists^\omega \Delta^0_1 \subset \exists^\omega \Pi^0_1$. Hence, $\Sigma^0_1 \subset \Sigma^0_2$ by the definition of Σ^0_2.

If P is Σ^0_1 and $Q(m, \overline{n}) \Leftrightarrow P(\overline{n})$, by recursive substitutions, Q is Σ^0_1 and $P(\overline{n}) \Leftrightarrow \forall m Q(m, \overline{n})$, showing that P is Π^0_2. Thus, $\Sigma^0_1 \subset \Pi^0_2$. This shows that $\Sigma^0_1 \subset \Delta^0_2$. Since

Δ_2^0 is closed under $\neg$, it follows that $\Pi_1^0 \subset \Delta_2^0$ as well. This proves the result for $n = 1$. (3) can be proved similarly for all n by induction. □

Remark 7.3.3. The inclusion relations between these pointclasses are summed up by the following diagram:

$$\begin{array}{ccccccc} & \Sigma_1^0 & & \Pi_2^0 & & \Sigma_3^0 & \dots \\ \Delta_1^0 & & \Delta_2^0 & & \Delta_3^0 & & \dots \\ & \Pi_1^0 & & \Sigma_2^0 & & \Pi_3^0 & \dots \end{array}$$

where a pointclass in any column is contained in all pointclasses to its right.

Corollary 7.3.4. *(i) Let n be even. Then*

$$\Sigma_n^0 = \underbrace{\exists^\omega \forall^\omega \dots \exists^\omega \forall^\omega}_{n \text{ times}} \Delta_1^0$$

and

$$\Pi_n^0 = \underbrace{\forall^\omega \exists^\omega \dots \forall^\omega \exists^\omega}_{n \text{ times}} \Delta_1^0.$$

(ii) Let n be odd. Then

$$\Sigma_n^0 = \underbrace{\exists^\omega \forall^\omega \dots \exists^\omega}_{n \text{ times}} \Delta_1^0$$

and

$$\Pi_n^0 = \underbrace{\forall^\omega \exists^\omega \dots \forall^\omega}_{n \text{ times}} \Delta_1^0.$$

A predicate in

$$\cup_n \Sigma_n^0 = \cup_n \Delta_n^0 = \cup_n \Pi_n^0$$

is called an *arithmetical set*.

Exercise 7.3.5. Show that all the arithmetical pointclasses are closed under $\exists^<$, $\exists^\leq$, $\forall^<$, and $\forall^\leq$.

Using the representability theorem and ideas contained in the proof of the first incompleteness theorem, we now show that all the inclusions in the arithmetical hierarchy are strict.

Let Γ be an arithmetical pointclass. Let $k \geq 1$. Call a $(k+1)$-ary predicate U^k *universal* for Γ if $U^k \in \Gamma$ and if for every k-ary predicate P in Γ there is an m such that for all $\overline{n} \in \mathbb{N}^k$,

$$P(\overline{n}) \Leftrightarrow U^k(m, \overline{n}).$$

Strictly speaking, we should say that U^k is universal for k-ary predicates in Γ. We shall not do this; it should be understood from the exponent k.

We now make some simple observations.

(a) U^k is universal for Σ_n^0 if and only if $\neg U^k$ is universal for Π_n^0.

(b) Let U^{k+1} be universal for Π^0_n. Set

$$U^k = \exists^\omega U^{k+1}.$$

We claim that U^k is universal for Σ^0_{n+1}.

Clearly, $U^k \in \Sigma^0_{n+1}$. Now let P be a k-ary predicate in Σ^0_{n+1}. Then there is a $(k+1)$-ary predicate Q in Π^0_n such that

$$P = \exists^\omega Q.$$

Since U^{k+1} is universal for Π^0_n, there is a p such that for all q and for all $\overline{m}$,

$$Q(q,\overline{m}) \Leftrightarrow U^{k+1}(p,q,\overline{m}).$$

Our assertion follows.

(c) Let U^1 be universal for Σ^0_n. Define P by

$$P(m) \Leftrightarrow U^1(m,m).$$

Then P is Σ^0_n. We claim that it is not Δ^0_n.

Since Σ^0_n is closed under recursive substitutions, $P \in \Sigma^0_n$. We claim that $P \notin \Pi^0_n$. Suppose not. Then $\neg P \in \Sigma^0_n$. Let m be such that for all k,

$$\neg P(k) \Leftrightarrow U^1(m,k).$$

But then

$$P(m) \Leftrightarrow U^1(m,m) \Leftrightarrow \neg P(m),$$

and we have arrived at a contradiction.

(d) Arguing as in (c), we see that for any n, Δ^0_n does not contain any universal set for Σ^0_n or Π^0_n.

Theorem 7.3.6. *For each $k \geq 1$, there is a $(k+1)$-ary predicate U^k that is universal for Σ^0_1.*

Proof. Let $x_0, x_1, x_2, x_3, \ldots$ be all the variables of the theory N in alphabetical order. For each $\overline{a} \in \mathbb{N}^k$, set

$$\mathrm{num}(\overline{a}) = (\mathrm{num}(a_0), \ldots, \mathrm{num}(a_{k-1})).$$

Define U^k by

$$U^k(m,\overline{a}) \Leftrightarrow \exists p \mathrm{Thm}_N(\langle m, \mathrm{num}(p), \mathrm{num}(\overline{a})\rangle),$$

where sb is the recursive function defined in Exercise 6.3.6.

Since $\mathrm{Thm}_N \in \Sigma^0_1$, $U^k \in \Sigma^0_1$. Now let $P \subset \mathbb{N}^k$ be semirecursive. Then there is a recursive set $Q \subset \mathbb{N}^{k+1}$ such that

$$P \Leftrightarrow \exists^{\omega} Q.$$

By the representability theorem, there is formula A of N such that A with $x_0, \ldots, x_k$ represents Q. Let $m = \lceil A \rceil$. Since N is consistent, we see that for all $\overline{a}$,

$$P(\overline{a}) \Leftrightarrow U^k(m, \overline{a}).$$

□

The following theorem is also now easy to see.

Theorem 7.3.7. *Let Γ be any of the pointclasses Σ_n^0 or of Π_n^0, $n \geq 1$. Then, for every $k \geq 1$, there is a $(k+1)$-ary predicate $U^k \in \Gamma$ that is universal for Γ.*

Remark 7.3.8. We now see that the hierarchy of arithmetical sets is strict, i.e., for all n, Δ_n^0 is properly contained in both Σ_n^0 and Π_n^0.

Hint: Suppose every Δ_n^0 set is Σ_n^0. Let U^1 be a universal Σ_n^0 set. Then it is a universal Δ_n^0 set too. But such a set cannot exist. (See the proof of Proposition 6.1.29.)

Proposition 7.3.9. *Let Γ be any of Σ_n^0 or of Π_n^0, $n \geq 1$. Then, for every $k \geq 1$, there are $(k+1)$-ary predicates $U_0^k, U_1^k \in \Gamma$ such that for every pair of sets $A_0, A_1 \subset \mathbb{N}^k$ in Γ, there is an m such that*

$$(\forall \overline{a} \in \mathbb{N}^k)(A_0(\overline{a}) \Leftrightarrow U_0^k(m, \overline{a}) \ \wedge \ A_1(\overline{a}) \Leftrightarrow U_1^k(m, \overline{a})).$$

Proof. Define

$$U_i^k(m, \overline{a}) \Leftrightarrow U^k((m)_i, \overline{a}),$$

$i = 0, 1$. Since Γ is closed under recursive substitutions, each U_0^k and U_1^k is in Γ. Given $A_0, A_1 \subset \mathbb{N}^k$ in Γ, choose m_0, m_1 such that

$$\forall \overline{a}(A_i(\overline{a}) \Leftrightarrow U^p(m_i, \overline{a})),$$

$i = 0, 1$. Take $m = \langle m_0, m_1 \rangle$. □

The pair U_0^k, U_1^k obtained above will be called a *universal pair for Γ*.

Let Γ be any of Σ_n^0 or of Π_n^0, $n \geq 1$. We say that Γ has the *uniformization property* if for every $k \geq 1$ and every $P \in \Gamma$, $P \subset \mathbb{N}^k \times \mathbb{N}$, there is a $Q \subset P$ in Γ such that

$$(\forall \overline{a} \in \mathbb{N}^k)(\exists m P(\overline{a}, m) \Rightarrow \exists! m Q(\overline{a}, m)),$$

where $\exists! m \ldots$ abbreviates "there is a unique $m \ldots$." Such a set Q is called a *uniformization* of P.

Let Γ be any of Σ_n^0 or of Π_n^0, $n \geq 1$. We say that Γ has the *reduction property* if for every $P_1, P_2 \subset \mathbb{N}^k$ in Γ there exist $Q_1 \subset P_1, Q_2 \subset P_2$ in Γ such that $Q_1 \cap Q_2 = \emptyset$ and $Q_1 \cup Q_2 = P_1 \cup P_2$.

Proposition 7.3.10. *If Γ has the uniformization property, then it has the reduction property.*

Proof. To see the result, given $P_1, P_2 \subset \mathbb{N}^k$ in Γ, define

$$P = (P_1 \times \{1\}) \cup (P_2 \times \{2\}).$$

Then $P \in \Gamma$. Choose a uniformization $Q \subset P$ of P in Γ. Set

$$Q_i(\overline{a}) \Leftrightarrow Q(\overline{a}, i),$$

$i = 1, 2$. □

Let Γ be any of Σ^0_n or of Π^0_n, $n \geq 1$ and $\Delta = \Gamma \cap \neg\Gamma$. We say that Γ has the *separation property* if for every disjoint $P_1, P_2 \subset \mathbb{N}^k$ in Γ there exists a $Q \subset \mathbb{N}^k$ in Δ such that

$$P_1 \subset Q \ \wedge \ Q \cap P_2 = \emptyset.$$

Proposition 7.3.11. *If Γ has the reduction property, then $\neg\Gamma$ has the separation property.*

Proof. To see this, take $P_1, P_2 \subset \mathbb{N}^k$ in $\neg\Gamma$ such that $P_1 \cap P_2 = \emptyset$. Let

$$Q_i = \mathbb{N}^k \setminus P_i,$$

$i = 1, 2$. Then $Q_1, Q_2 \in \Gamma$ and $Q_1 \cup Q_2 = \mathbb{N}^k$. Since Γ has the reduction property, there exists $R_i \subset Q_i$ in Γ, $i = 1, 2$, such that $R_1 \cap R_2 = \emptyset$ and $R_1 \cup R_2 = \mathbb{N}^k$. Thus, $R_1 \in \Delta$. Set $Q = \mathbb{N}^k \setminus R_1$. □

Exercise 7.3.12. Let $\Gamma = \Sigma^0_n$ or Π^0_n, $n \geq 1$. Show that Γ cannot satisfy both the reduction property and the separation property.

Hint: Using Proposition 7.3.9, take a universal pair U^1_1, U^1_2 for Γ. Let $V_1, V_2 \in \Gamma$ reduce the pair U^1_1, U^1_2 in the preceding sense. Let $W \supset V_1$, $W \cap V_2 = \emptyset$, and $W \in \Delta$. Show that W is universal for Δ.

Theorem 7.3.13 (Uniformization theorem). *Every arithmetical pointclass Σ^0_n has the uniformization property.*

Proof. Let $P \subset \mathbb{N}^k \times \mathbb{N}$ be in Σ^0_n. Choose $R \subset \mathbb{N} \times \mathbb{N}^k \times \mathbb{N}$ in Δ^0_n such that $P = \exists^\omega R$. Define Q by

$$Q'(\overline{a}, n) \Leftrightarrow R((n)_0, \overline{a}, (n)_1) \wedge \forall^{<n} k \neg R((k)_0, \overline{a}, (k)_1)$$

and set

$$Q(\overline{a}, m) \Leftrightarrow \exists n[m = (n)_0 \wedge Q'(\overline{a}, n)].$$

□

Corollary 7.3.14. *Each arithmetical pointclass Π^0_n, $n \geq 1$, has the separation property, and each Σ^0_n, $n \geq 1$, has the reduction property.*

We close this section by proving two basic results in recursion theory. We shall establish some notation first. For $\overline{a} = (a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+n})$, we have

$$l_m(\overline{a}) = (a_1, \ldots, a_m)$$

and

$$r_n(\overline{a}) = (a_{m+1}, \ldots, a_{m+n}).$$

Theorem 7.3.15 (s^m_n-Theorem). *The sequence of universal sets $U^1, U^2, \ldots$ for Σ^0_1 defined in 7.3.6 satisfies*

$$U^{m+n}(p, \overline{a}) \Leftrightarrow U^m(s^m_n(p, r_n(\overline{a})), a_1, \ldots, a_m),$$

where $\overline{a} = (a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+n})$ and the function s^m_n is as defined in Exercise 6.3.7.

Proof. The result follows directly from the definitions of the U^k and the function s^m_n. □

If P is a k-ary semirecursive predicate and m is such that for all $\overline{a} \in \mathbb{N}^k$,

$$P(\overline{a}) \Leftrightarrow U^k(m, \overline{a}),$$

then we say that m is a *code* of P.

As an application of the s^m_n-theorem we show the following proposition.

Proposition 7.3.16. *There exist recursive functions $\vee^k(m,n)$ and $\wedge^k(m,n)$ such that if m is a code of $P \subset \mathbb{N}^k$ and n a code of $Q \subset \mathbb{N}^k$, then $\vee^k(m,n)$ and $\wedge^k(m,n)$ are codes of $P \vee Q$ and $P \wedge Q$, respectively.*

Proof. First we define $\vee^k(m,n)$. Let U^k be as defined in Theorem 7.3.6. Now define

$$R(\overline{a}, m, n) \Leftrightarrow U^k(m, \overline{a}) \vee U^k(n, \overline{a}).$$

Then there is a p such that

$$R(\overline{a}, m, n) \Leftrightarrow U^{k+2}(p, \overline{a}, m, n).$$

Set

$$\vee^k(m,n) = s^k_2(p, m, n).$$

We define $\wedge^k$ similarly. □

We refer to the foregoing closure properties of Σ^0_1 by saying that Σ^0_1 is *uniformly closed* under $\vee$ and $\wedge$ (with respect to the universal sets U^k).

Exercise 7.3.17. Show that Σ^0_1 and Π^0_1 are uniformly closed under $\exists^<$, $\forall^<$, $\exists^\leq$, and $\forall^\leq$. Further, Σ^0_1 is uniformly closed under $\exists^\omega$ and Π^0_1 under $\forall^\omega$. For instance, show that for each $k \geq 1$, there is a recursive function $\exists^<_k : \mathbb{N} \to \mathbb{N}$ such that if n codes $P(m,\overline{a})$, a $(k+1)$-ary predicate, $\exists^<_k(n)$ codes the predicate

$$Q(p,\overline{a}) \Leftrightarrow \exists^{<p} P(p,\overline{a}).$$

Theorem 7.3.18 (Kleene's recursion theorem). *Let P be a $(k+1)$-ary predicate in Σ^0_1. Then there is an n^* such that for all $\overline{m}$,*

$$P(n^*,\overline{m}) \Leftrightarrow U^k(n^*,\overline{m}).$$

Proof. Define a $(k+1)$-ary predicate Q by

$$Q(\overline{m},p) \Leftrightarrow P(s^k_1(p,p),\overline{m}).$$

Then $Q \in \Sigma^0_1$. Thus, there is a q such that

$$Q(\overline{m},p) \Leftrightarrow U^{k+1}(q,\overline{m},p).$$

Take $n^* = s^k_1(q,q)$. □

Kleene's recursion theorem is very useful in showing that certain functions and predicates are recursive.

Example 7.3.19. Let α be a unary recursive function and β and γ 3-ary recursive functions. Then the 2-ary function δ defined by

$$\begin{aligned} \delta(0,n) &= \alpha(n), \\ \delta(m+1,n) &= \beta(\delta(m,\gamma(\delta(m,n),m,n)),m,n)) \end{aligned}$$

is recursive.

To show this, by Proposition 6.1.27, it suffices to show that the graph of δ is semirecursive. To show this, we define a 4-ary semirecursive predicate G as follows:

$$\begin{aligned} G(l,m,n,k) \Leftrightarrow\ & (m = 0 \wedge k = \alpha(n)) \\ & \vee \exists p \exists q \exists r \exists s (m = p+1 \\ & \wedge U^3(l,p,n,q) \\ & \wedge r = \gamma(q,p,n) \\ & \wedge U^3(l,p,r,s) \\ & \wedge k = \beta(s,p,n)), \end{aligned}$$

where U^3 is the universal set for Σ^0_1-sets in $\mathbb{N}^3$ defined earlier. Clearly, G is a 4-ary semirecursive predicate. Hence, by Kleene's recursion theorem,

$$\exists l^* \forall m \forall n \forall k (G(l^*, m, n, k) \Leftrightarrow U^3(l^*, m, n, k)).$$

It is fairly routine to check that the 3-ary semirecursive predicate $U^3(l^*, \cdot, \cdot, \cdot)$ is a graph of δ.

Exercise 7.3.20. Let $n \geq 1$, and let Γ equal Σ_n^0 or Π_n^0, and let the U^k be the universal sets for Γ obtained in Theorem 7.3.7. Show that the s_n^m-theorem (with the same function s_n^m) and Kleene's recursion theorem hold for Γ.

Remark 7.3.21. It is fairly easy to see that the s_n^m-theorem for any of these arithmetical pointclasses can be used to show their uniform closure properties, and Kleene's recursion theorem can be used to show that predicates are in these classes.

7.4 Recursive Extensions of Peano Arithmetic

The arithmetization of theories due to Gödel enables one to examine questions about a theory, such as *PA* or *ZF*, within the theory itself. For instance, using the representability theorem, we can now express the metasentence "Peano arithmetic is consistent" by a formula of *PA* itself, and we can examine whether this formula is a theorem of *PA*. This involves formalizing proofs in metatheory inside the theory itself. A key step in this direction is to show that every true closed existential formula of *PA* is a theorem of *PA*. (Recall that a sentence φ of the language of N is called true if it is valid in the standard model $\mathbb{N}$ of the theory N.) In this section we prove this vital theorem.

Let P' be an extension by definitions of *PA*, and let φ be a formula of P' in which no variable other than $v_1, \ldots, v_n$ and w is free, with $v_1, \ldots, v_n$, w distinct. Suppose $P' \vdash \exists w \varphi$. Let w' be a new variable and ψ the formula

$$\varphi \wedge \forall w' (w' < w \rightarrow \neg \varphi_w[w']).$$

By Exercise 4.7.5, we have the following:

(a) $P' \vdash \exists w \psi$.
(b) $P' \vdash \psi \wedge \psi_w[w''] \rightarrow w = w''$.

Thus, we can introduce to P' a new n-ary function symbol f with the defining axiom ψ. We shall write

$$f v_1 \cdots v_n = \mu w \varphi$$

to express that f has been introduced as above with ψ as its defining axiom.

We say that P' is a *recursive extension of PA* if it is obtained by a finite number of extensions of *PA* where the defining axiom for a predicate is an open formula and the defining axiom for a function symbol is a formula of the form ψ described previously with φ open.

Example 7.4.1. Let $1 \leq i \leq n$, and let $\varphi[w, v_1, \ldots, v_n]$ be the formula $w = v_i$. Then

$$\pi_i^n v_1 \cdots v_n = \mu w \varphi$$

introduces the projection map π_i^n in a recursive extension of *PA*.

The following exercise is quite easy to prove.

Exercise 7.4.2. Show that functions and predicates that can be introduced in a recursive extension of *PA* are recursive.

Proposition 7.4.3. *Let R be an n-ary predicate on $\mathbb{N}$. Then R can be introduced in a recursive extension of PA if and only if χ_R can be introduced.*

Proof. Suppose R has been introduced in a recursive extension of *PA* with the defining axiom an open formula φ. Then we can introduce χ_R by

$$\chi_R(v_1, \ldots, v_n) = \mu w((\varphi(v_1, \ldots, v_n) \wedge w = 0) \vee (\neg\varphi(v_1, \ldots, v_n) \wedge w = 1)).$$

Now assume that χ_R has P' of *PA*. Then the formula

$$\chi_R(v_1, \ldots, v_n) = 0$$

introduces R. □

Example 7.4.4. The functions $+$ (addition) and $\cdot$ (multiplication) are nonlogical symbols of *PA*. By Example 7.4.1, each projection map π_i^n can be introduced. Since $<$ is a nonlogical symbol of *PA*, by Proposition 7.4.3, $\chi_<$ can be introduced. Thus, all initial recursive functions can be introduced in a recursive extension of *PA*.

Example 7.4.5. Let $n \geq 1$ and $p \in \mathbb{N}$. We can introduce the n-ary constant function C_p^n by taking the formula $\varphi[w, v_1, \cdots, v_n]$ to be $w = k_p$.

Example 7.4.6. We can introduce $\dot{-}$ to *PA* by

$$x \dot{-} y = \mu z(x + z = y \vee x < y)$$

using the foregoing method.

Proposition 7.4.7. *The set of functions that can be introduced in a recursive extension of PA is closed under composition.*

Proof. Let $f_1, \ldots, f_k$ be n-ary functions and g a k-ary function that have been introduced in a recursive extension P' of *PA*. Further, assume that

$$f_i v_1 \cdots v_n = \mu w_i \varphi_i[w_i, v_1, \ldots, v_n], \quad 1 \leq i \leq k,$$

and

$$g w_1 \cdots w_k = \mu w \varphi[w, w_1, \ldots, w_k].$$

Suppose

$$h(m_1,\ldots,m_n) = g(f_1(m_1,\ldots,m_n),\ldots,f_k(m_1,\ldots,m_n)).$$

It is not difficult to prove that

$$P' \vdash \exists w[w = g(f_1(v_1\ldots,v_n),\ldots,f_k(v_1,\ldots,v_n))].$$

Hence, we can introduce h as follows:

$$hv_1\cdots v_n = \mu w[w = g(f_1(v_1\ldots,v_n),\ldots,f_k(v_1,\ldots,v_n))].$$

□

Remark 7.4.8. Let g be an $(n+1)$-ary function that has been introduced in a recursive extension P' of PA, and let

$$\forall m_1\cdots\forall m_n\exists l[g(m_1,\ldots,m_n,l) = 0].$$

Define

$$h(m_1,\ldots,m_n) = \mu l[g(m_1,\ldots,m_n,l) = 0].$$

Suppose

$$gv_1\cdots v_{n+1} = \mu w\varphi[w,v_1,\ldots,v_{n+1}].$$

If

$$P \vdash \exists v_{n+1}[gv_1\cdots v_nv_{n+1} = 0],$$

then we can introduce h as follows:

$$hv_1\cdots v_n = \mu v_{n+1}gv_1\cdots v_nv_{n+1} = 0.$$

A great many recursive functions and recursive predicates can be introduced in a recursive extension of PA. Further, the set of all functions and predicates that can be introduced in a recursive extension satisfies some of the closure properties satisfied by the set of recursive functions and recursive predicates. One can easily see this by looking at the explicit definitions of many recursive functions that we defined earlier and the proofs of closure properties of the set of all recursive functions and recursive predicates.

Exercise 7.4.9. 1. Let $f_1,\ldots,f_k$ be n-ary functions and P a k-ary predicate. Assume that $f_1,\ldots,f_k$ and P can be introduced. Show that the n-ary predicate Q defined by

$$Q(m_1,\ldots,m_n) \Leftrightarrow P(f_1(m_1,\ldots,m_n),\ldots,f_k(m_1,\ldots,m_n))$$

can be introduced.

2. Let P and Q be n-ary predicates that can be introduced. Show that the predicates $\neg P$, $P\vee Q$, $P\wedge Q$, $P\to Q$, and $P\leftrightarrow Q$ can be introduced.

3. Show that the set of all functions and predicates that can be introduced is closed under bounded minimalizations and bounded quantifiers.

Exercise 7.4.10. Show that the divisibility $m|n$, the ordered pair function OP, and Gödel's β-function can be introduced in a recursive extension of PA.

Exercise 7.4.11. Let $A_1,\dots,A_m$ be pairwise disjoint subsets of $\mathbb{N}^k$ whose union is $\mathbb{N}^k$. Suppose $f_1,\dots,f_m$ are k-ary functions. Define $g:\mathbb{N}^k\to\mathbb{N}$ by

$$g(\overline{a})=\begin{cases} f_1(\overline{a}) & \text{if } \overline{a}\in A_1,\\ \quad\vdots & \\ f_m(\overline{a}) & \text{if } \overline{a}\in A_m.\end{cases}$$

Show that if $A_1,\dots,A_m$ and $f_1,\dots,f_m$ can be introduced in a recursive extension of PA, then g can be introduced.

Exercise 7.4.12. Show that the set of all functions that can be introduced in a recursive extension of PA is closed under primitive recursion.

Exercise 7.4.13. Show that all the finitely many functions and predicates for PA that were introduced in the section on arithmetization of theories can be introduced in a recursive extension of PA.

We now proceed to prove that every true closed existential formula of a recursive extension P' of PA is a theorem of P'.

In the sequel we shall use the same notation for the functions and predicates introduced. For instance, we shall use form *for both the predicate* $\mathrm{form}(n)$ *and the corresponding function symbol introduced,* num *for both the function* $\mathrm{num}(n)$ *and the corresponding function symbol introduced, and* Prf_{PA} *for both the predicate* $\mathrm{Prf}_{PA}(m,n)$ *and the corresponding symbol, and so on.*

Let P' be a recursive extension of PA. The set of *R-formulas* of P' is the smallest class of formulas $\mathscr{F}$ that contains all formulas of the form $fv_1\cdots v_n=v$, $pv_1\cdots v_n$, and $\neg pv_1\cdots v_n$ (f and p function and predicate symbols of P') and that satisfies

(a) $A,B\in\mathscr{F}\Rightarrow A\vee B, A\wedge B\in\mathscr{F}$;
(b) If $A\in\mathscr{F}$ and if x,y are distinct variables, then $\forall x(x<y\to A)\in\mathscr{F}$;
(c) If $A\in\mathscr{F}$, $\exists xA\in\mathscr{F}$.

A formula of PA of the form $\varphi_{v_1,\dots,v_m}[k_{n_1},\dots,k_{n_m}]$, $n_1,\dots,n_m\in\mathbb{N}$, will be called a *numerical instance* of φ.

Proposition 7.4.14. *Let A be an R-formula of PA. Then every true numerical instance of A is a theorem of PA.*

Proof. That R-formulas of the form $x=y$, $Sx=y$, $x+y=z$, $x\cdot y=z$, $x<y$ and negations of these formulas satisfy the conclusion of the proposition follows from the representability of $=$, S, $+$, $\cdot$, and $<$ and the fact that PA is an extension of N.

Now we show that the set $\mathscr{G}$ of formulas that satisfy the conclusion of the proposition satisfies the three closure properties (a)–(c). If A and B satisfy the conclusion, then it is quite easy to check that $A \vee B$ and $A \wedge B$ also satisfy the conclusion. Thus, (a) holds for $\mathscr{G}$.

We now show that (c) holds for $\mathscr{G}$. Let A satisfy the conclusion of the proposition, and let B be the formula $\exists x A$. A numerical instance B' of B is of the form $\exists x A'$, where A' is obtained by substituting numerals in A for all free variables other than x. Suppose B' is true. Then $A'_x[k_n]$ is true for some n. By our assumption, $PA \vdash A'_x[k_n]$. This implies that $PA \vdash B'$ by the substitution axiom and the detachment rule.

Finally, we show that (b) holds for $\mathscr{G}$. Let A satisfy the conclusion of the proposition, and let B be the formula $\forall x(x < y \to A)$. A numerical instance B' of B is of the form $\forall x(x < k_n \to A')$, where A' is obtained by substituting numerals in A for all free variables other than x and k_n for y. Suppose B' is true. Then for each $i < n$, $A'_x[k_i]$ is true. Hence, by our hypothesis, they are theorems of PA. By Lemma 4.7.1, the detachment rule, and the $\forall$-introduction rule,

$$PA \vdash B'. \qquad \square$$

Recall that a formula is called existential if it is in prenex form and all the quantifiers in its prefix are $\exists$.

Proposition 7.4.15. *Let P' be a recursive extension of PA. Then every existential formula A of P' is equivalent in P' to an R-formula.*

Proof. In view of the defining condition (c) of R-formulas, it is sufficient to prove that every open formula A of P' is equivalent in P' to an R-formula.

Step 1: Let $t[x_1, \ldots, x_n]$ be a term of P', and A the formula $x = t$. The result holds for A.

We proceed by induction on the length of t. If t is a variable, then A is an R-formula. If t is a constant, then $t = x$ is an R-formula. This is equivalent to $x = t$ by the symmetry theorem. Now let $t = ft_1 \cdots t_n$. Then, by Proposition 4.2.26,

$$P' \vdash x = t \leftrightarrow \exists y_1 \cdots \exists y_n (y_1 = t_1 \wedge \cdots \wedge y_n = t_n \wedge x = f y_1 \cdots y_n).$$

The result now follows from the induction hypothesis, the symmetry theorem, and the definition of R-formulas.

Step 2: Let A be a formula of the form $pt_1 \cdots t_n$, p a relation symbol, and $t_1, \cdots, t_n$ terms. We have

$$P' \vdash A \leftrightarrow \exists y_1 \cdots \exists y_n (y_1 = t_1 \wedge \cdots \wedge y_n = t_n \wedge p y_1 \cdots y_n).$$

Since each formula $y_i = t_i$ is equivalent to an R-formula, the result holds for A.

Similarly, we prove the result for formulas that are negations of atomic formulas.

The class of formulas for which the theorem holds is, by the defining condition (a) of R-formulas, closed under $\vee$ and $\wedge$. Hence, the result for open formulas follows from Exercise 4.2.4.

□

Proposition 7.4.16. *Let P' be a recursive extension of PA. Then every R-formula of P' is equivalent in P' to an R-formula in PA.*

Proof. Suppose P'' is a recursive extension of P' obtained by adding just one nonlogical symbol. Our result will be proved if we show that every R-formula A in P'' is equivalent in P'' to an R-formula in P'. By the equivalence theorem, it is sufficient to prove the result for A of the form $fx_1 \cdots x_n = y$ or $px_1 \cdots x_n$ or their negations.

Since the defining axiom of p is an open formula of P', the result is easy to prove for a formula of the form $px_1 \cdots x_n$ and their negations by Proposition 7.4.15. Since a formula of the form $\neg(fx_1 \cdots x_n = y)$ is equivalent in P'' to a formula $\exists z(\neg(y = z) \wedge fx_1 \cdots x_n = z)$, the result follows for such formulas by Proposition 7.4.15.

Let A be $fx_1 \cdots x_n = y$. Then A is equivalent to a formula of P' of the form

$$B \wedge \forall x(x < y \rightarrow C),$$

where B and C are open. The result can be easily seen now by Proposition 7.4.15.

□

From the last three results we have the following theorem.

Theorem 7.4.17. *If P' is a recursive extension of PA, then every true closed existential formula is a theorem of P'.*

7.5 Second Incompleteness Theorem

We are now in a position to prove that "*PA* is consistent" is not a theorem of *PA*.

Henceforth, we assume that P' is a recursive extension of PA in which all the recursive functions and recursive predicates for PA introduced in the section on arithmetization of theories have been introduced. We introduce some notation first.

Let $t, t_1, \ldots, t_n$ be terms and $x_1, \ldots, x_n$ be the first n variables in alphabetical order. We define the terms $S(t, t_1, \ldots, t_n)$ by induction:

$$S(t, t_1) = \text{sub}(t, k_{\lceil x_1 \rceil}, t_1),$$

$$S(t, t_1, t_2) = \text{sub}(S(t, t_1), k_{\lceil x_2 \rceil}, t_2)$$

$$\vdots$$

$$S(t, t_1, \ldots, t_n) = \text{sub}(S(t, t_1, \ldots, t_{n-1}), k_{\lceil x_n \rceil}, t_n).$$

Since each formula in P' has a translation in PA and since P' is a conservative extension of PA, we shall not distinguish between a formula of P' and its translation in P. With these conventions, we abbreviate the formula $\exists y \mathrm{Prf}_{PA}(x,y)$ by $\mathrm{Thm}_{PA}(x)$ and

$$\neg\forall x(\mathrm{form}_{PA}(x) \to \mathrm{Thm}_{PA}(x))$$

by Con_{PA}.

By formalizing the proof of Proposition 7.4.14 inside P', we shall prove the following lemma.

Lemma 7.5.1. *For any R-formula $A[x_1,\ldots,x_n]$ of PA,*

$$P' \vdash A \to \mathrm{Thm}_{PA}(S(k_{\ulcorner A \urcorner}, x_1, \ldots, x_n)).$$

Proof. We shall prove the result by induction on the length of A. We shall give only a few steps of the proof. Readers should not find it difficult to complete the proof themselves.

Let A be the formula $0 = x$. We have

$$S(k_{\ulcorner A \urcorner}, x) = \langle k_{SN(=)}, \mathrm{num}(0), \mathrm{num}(x)\rangle.$$

We must show that

$$P' \vdash 0 = x \to \mathrm{Thm}_{PA}(\langle k_{SN(=)}, \mathrm{num}(0), \mathrm{num}(0)\rangle).$$

By the equality theorem, this will be proved if we show that

$$P' \vdash \mathrm{Thm}_{PA}(\langle k_{SN(=)}, \mathrm{num}(0), \mathrm{num}(0)\rangle).$$

But the formula

$$\mathrm{Thm}_{PA}(\langle k_{SN(=)}, \mathrm{num}(0), \mathrm{num}(0)\rangle)$$

is a true closed existential formula. Hence it is a theorem of P' by Theorem 7.4.17.

Similarly, by formalizing the proofs of the representability of S, $+$, $\cdot$, and $<$ inside P', we can prove the assertion for formulas of the form $Sx = y$, $x + y = z$, $x \cdot y = z$, $x < y$, etc.

We shall show only one inductive step and leave the others for the reader to prove. Let $A[x_1,\ldots,x_n]$ be of the form $\exists x B$ and the result holds for the formula B. Set

$$t = S(k_{\ulcorner B \urcorner}, x_1, \ldots, x_n).$$

Since $S(k_{\ulcorner A \urcorner}, x_1, \ldots, x_n) = \langle k_{SN(\exists)}, k_{\ulcorner x \urcorner}, t\rangle$ is a true closed existential formula, by Theorem 7.4.17,

$$P' \vdash S(k_{\ulcorner A \urcorner}, x_1, \ldots, x_n) = \langle k_{SN(\exists)}, k_{\ulcorner x \urcorner}, t\rangle. \qquad (a)$$

By the induction hypothesis,

$$P' \vdash B \to \mathrm{Thm}_{PA}(\mathrm{sub}(t, k_{\ulcorner x \urcorner}, \mathrm{num}(x))).$$

By the distribution rule, we have

$$P' \vdash A \to \exists x \mathrm{Thm}_{PA}(\mathrm{sub}(t, k_{\lceil x \rceil}, \mathrm{num}(x))). \tag{b}$$

Using the fact that every true existential sentence is a theorem, we can formalize the proof of "if $P' \vdash B_x[k_n]$ for some n, then $P' \vdash \exists x B$" inside P'. Thus, we get

$$P' \vdash \exists x \mathrm{Thm}_{PA}(\mathrm{sub}(t, k_{\lceil x \rceil}, \mathrm{num}(x))) \to \mathrm{Thm}_P(\langle k_{SN(\exists)}, k_{\lceil x \rceil}, t \rangle). \tag{c}$$

Our assertion for A follows from (a), (b), and (c). □

Essentially, by formalizing the proof of the first incompleteness theorem inside P', we get the following very interesting result.

Theorem 7.5.2 (Second incompleteness theorem). *Con_{PA} is not a theorem of PA.*

Proof. Let $A[x]$ denote the translation of the formula

$$\neg \exists y \mathrm{Prf}_{PA}(sub(x, k_{\lceil x \rceil}, \mathrm{num}(x)), y)$$

in PA. Let $a = \lceil A \rceil$. We need to show that

$$PA \nvdash \mathrm{Con}_{PA}. \tag{1}$$

Since P' is an extension by definition of PA, it is sufficient to prove that

$$P' \nvdash \mathrm{Con}_{PA}. \tag{2}$$

For this, it is enough to prove that

$$P' \vdash \mathrm{Con}_{PA} \to A_x[k_a] \tag{3}$$

because by the argument contained in the proof of the first incompleteness theorem, $P' \nvdash A_x[k_a]$ and $A_x[k_a]$ is a tautological consequence of $\mathrm{Con}_{PA} \to A_x[k_a]$ and Con_{PA}.

Let B be an R-formula in PA that is equivalent in P' to

$$\exists y \mathrm{Prf}_{PA}(\mathrm{sub}(x, k_{\lceil x \rceil}, \mathrm{num}(x))), y)_x[k_a].$$

Hence, by the equivalence theorem,

$$P' \vdash \neg B \leftrightarrow A_x[k_a]. \tag{4}$$

Let $b = \lceil B \rceil$ and $c = \lceil A_x[k_a] \rceil$. By the definition of consistency and Theorem 7.4.17, we have

$$P' \vdash \mathrm{Con}_{PA} \to (\neg \mathrm{Thm}_{PA}(k_c) \vee \neg \mathrm{Thm}_{PA}(neg(k_c))), \tag{5}$$

where $neg(k_c) = \langle k_{SN(\neg)}, c\rangle$. Thus, by the tautology theorem, it is sufficient to show that

$$P' \vdash (\neg \mathrm{Thm}_{PA}(k_c) \vee \neg \mathrm{Thm}_{PA}(neg(k_c))) \to A_x[k_a]. \tag{6}$$

By the tautology theorem again, it is enough to show that

$$P' \vdash \neg \mathrm{Thm}_{PA}(k_c) \to A_x[k_a] \tag{7}$$

and

$$P' \vdash \neg \mathrm{Thm}_{PA}(neg(k_c)) \to A_x[k_a]. \tag{8}$$

We prove (7) as follows.

Note that $k_c = \mathrm{sub}(k_a, k_{\lceil x \rceil}, \mathrm{num}(k_a))$ is a true closed existential formula of P'. Hence, by Theorem 7.4.17, it is a theorem of P'. By the equality theorem and the definition of A, we now have $P' \vdash \neg A_x[k_a] \to \mathrm{Thm}_{PA}(k_c)$. This proves (7).

To prove (8), first note that by (4),

$$P' \vdash B \to \neg A_x[k_a].$$

Hence,

$$\mathrm{Thm}_{PA}(\langle k_{SN(\vee)}, neg(k_b), neg(k_c)\rangle)$$

is a true closed existential formula. Hence, by Theorem 7.4.17,

$$P' \vdash \mathrm{Thm}_{PA}(k_b) \to \mathrm{Thm}_{PA}(neg(k_c)). \tag{9}$$

Finally, by Lemma 7.5.1, we have

$$P' \vdash B \to \mathrm{Thm}_{PA}(k_b). \tag{10}$$

Now note that $\neg \mathrm{Thm}_{PA}(neg(k_c)) \to A_x[k_a]$ is a tautological consequence of

$$\mathrm{Thm}_{PA}(k_b) \to \mathrm{Thm}_{PA}(neg(k_c)),$$

$$B \to \mathrm{Thm}_{PA}(k_b),$$

and

$$\neg B \leftrightarrow A_x[k_a].$$

Hence, (8) follows from (9), (10), and (4) by the tautology theorem. □

Remark 7.5.3. There is an extension by definitions of ZF (or of ZFC) in which there is a suitable interpretation of Peano arithmetic PA so that the representability theorem can be proved with the theory N replaced by ZF. Hence, we can express Con_{ZF} and Con_{ZFC} as formulas of ZF. Again, using similar ideas, we can prove the following result:

$$ZF \nvdash Con_{ZF}.$$

References

1. Ax, J.: The elementary theory of finite fields. Ann. Math. **88**, 103–115 (1968)
2. Bochnak, J., Coste, M., Roy, M-F.: Real Algebraic Geometry, vol. 36, A Series of Modern Surveys in Mathematics. Springer, New York (1998)
3. Chang, C.C., Keisler, H.J.: Model Theory, 3rd edn. North-Holland, London (1990)
4. Flath, D., Wagon, S.: How to pick out integers in the rationals: An application of number theory to logic. Am. Math. Mon. **98**, 812–823 (1991)
5. Hinman, P.: Fundamentals of Mathematical Logic. A. K. Peters (2005)
6. Hofstadter, D.R.: Gödel, Escher, Bach: An Eternal Golden Braid. Vintage Books, New York (1989)
7. Hrushovski, E.: The Mordell–Lang conjecture for function fields. J. Am. Math. Soc. **9**(3), 667–690 (1996)
8. Jech, T.: Set Theory, Springer Monographs in Mathematics, 3rd edn. Springer, New York (2002)
9. Kunen, K.: Set Theory: An Introduction to Independence Proofs. North-Holland, Amsterdam (1980)
10. Lang, S.: Algebra, 3rd edn. Addison-Wesley (1999)
11. Marker, D.: Model Theory: An Introduction, GTM 217. Springer, New York (2002)
12. Rogers, H.J.: Theory of Recursive Functions and Effective Computability. McGraw-Hill, New York (1967)
13. Penrose, R.: The Emperor's New Mind. Oxford University Press, Oxford (1990)
14. Pila, J.: *O*-minimality and André-Oort conjecture for $\mathbb{C}^n$. Ann. Math. (2) **172**(3), 1779–1840 (2011)
15. Pila, J., Zannier, U.: Rational points in periodic analytic sets and the Manin-Mumford conjecture, Atti. Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei(9). Mat. Appl. **19**(2), 149–162 (2008)
16. Shoenfield, J.R.: Mathematical Logic. A. K. Peters (2001)
17. Srivastava, S.M.: A Course on Borel Sets, GTM 180. Springer, New York (1998)
18. Swan, R.G.: Tarski's principle and the elimination of quantifiers (preprint)

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6,

© Springer Science+Business Media New York 2013

Index

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6,

© Springer Science+Business Media New York 2013