Undergraduate Texts in Mathematics

H.D. Ebbinghaus
J. Flum
W. Thomas

Mathematical Logic

Springer-Verlag New York • Berlin • Heidelberg • Tokyo

H.-D. Ebbinghaus
J. Flum
W. Thomas

Mathematical Logic

Springer-Verlag
New York Berlin Heidelberg Tokyo

H.-D. Ebbinghaus
J. Flum
Mathematisches Institut
Universität Freiburg
Albertstrasse 23b
7800 Freiburg
Federal Republic of Germany

W. Thomas
Lehrstuhl für Informatik II
RWTH Aachen
Büchel 29–31
5100 Aachen
Federal Republic of Germany

Translated from *Einführung in die mathematische Logik*, published by Wissenschaftliche Buchgesellschaft, Darmstadt, by Ann S. Ferebee, Kohlweg 12, D-6240 Königstein 4, Federal Republic of Germany.

AMS Subject Classification (1980): 03–01

Library of Congress Cataloging in Publication Data
Ebbinghaus, Heinz-Dieter, 1939–
Mathematical logic.
(Undergraduate texts in mathematics)
Translation of: Einführung in die mathematische Logik.
Bibliography: p.
Includes index.
1. Logic, Symbolic and mathematical. I. Flum, Jörg.
II. Thomas, Wolfgang. III. Title. IV. Series.
QA9.E2213 1984 511.3 83-20060

With 1 Illustration

Typeset by Composition House Ltd., Salisbury, England.
Printed and bound by R. R. Donnelley & Sons, Harrisonburg, Virginia.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90895-1 Springer-Verlag New York Berlin Heidelberg Tokyo
ISBN 3-540-90895-1 Springer-Verlag Berlin Heidelberg New York Tokyo

Preface

Some of the central questions of mathematical logic are: What is a mathematical proof? How can proofs be justified? Are there limitations to provability? To what extent can machines carry out mathematical proofs?

Only in this century has there been success in obtaining substantial and satisfactory answers, the most pleasing of which is given by Gödel's completeness theorem: It is possible to exhibit (in the framework of first-order languages) a simple list of inference rules which suffices to carry out all mathematical proofs. "Negative" results, however, appear in Gödel's incompleteness theorems. They show, for example, that it is impossible to prove all true statements of arithmetic, and thus they reveal principal limitations of the axiomatic method.

This book begins with an introduction to first-order logic and a proof of Gödel's completeness theorem. There follows a short digression into model theory which shows that first-order languages have some deficiencies in expressive power. For example, they do not allow the formulation of an adequate axiom system for arithmetic or analysis. On the other hand, this difficulty can be overcome—even in the framework of first-order logic—by developing mathematics in set-theoretic terms. We explain the prerequisites from set theory that are necessary for this purpose and then treat the subtle relation between logic and set theory in a thorough manner.

Gödel's incompleteness theorems are presented in connection with several related results (such as Trahtenbrot's theorem) which all exemplify the limitations of machine oriented proof methods. The notions of computability theory that are relevant to this discussion are given in detail. The concept of computability is made precise by means of a simple programming language.

The development of mathematics in the framework of first-order logic (as indicated above) makes use of set-theoretic notions to an extent far beyond that of mathematical practice. As an alternative one can consider logical systems with more expressive power. We introduce some of these systems, such as second-order and infinitary logics. In each of these cases we point out deficiencies contrasting first-order logic. Finally, this empirical fact is confirmed by Lindström's theorems, which show that there is no logical system that extends first-order logic and at the same time shares all its advantages.

The book does not require special mathematical knowledge; however, it presupposes an acquaintance with mathematical reasoning as acquired, for example, in the first year of a mathematics or computer science curriculum. Exercises enable the reader to test and deepen his understanding of the text. The references in the bibliography point out essays of historical importance, further investigations, and related fields.

The original edition of the book appeared in 1978 under the title "Einführung in die mathematische Logik." Some sections have been revised for the present translation; furthermore, some exercises have been added. We thank Dr. J. Ward for his assistance in preparing the final English text. Further thanks go to Springer-Verlag for their friendly cooperation.

Freiburg and Aachen
November 1983

H.-D. EBBINGHAUS
J. FLUM
W. THOMAS

Contents

PART A

CHAPTER I
Introduction

Towards the end of the nineteenth century mathematical logic evolved into a subject of its own. It was the works of Boole, Frege, Russell, and Hilbert, among others,[1] that contributed to its rapid development. Various elements of the subject can already be found in traditional logic, for example, in the works of Aristotle or Leibniz. However, while traditional logic can be considered as part of philosophy, mathematical logic is more closely related to mathematics. Some aspects of this relation are:

(1) *Motivation and Goals.* Investigations in mathematical logic arose mainly from questions concerning the foundations of mathematics. For example, Frege intended to base mathematics on logical and set-theoretical principles. Russell tried to eliminate contradictions that arose in Frege's system. Hilbert's goal was to show that "the generally accepted methods of mathematics taken as a whole do not lead to a contradiction" (this is known as Hilbert's program).

(2) *Methods.* In mathematical logic the methods used are primarily *mathematical.* This is exemplified by the way in which new concepts are formed, definitions are given, and arguments are conducted.

(3) *Applications in Mathematics.* The methods and results obtained in mathematical logic are not only useful for treating foundational problems; they also increase the stock of tools available in mathematics itself. There are applications in many areas of mathematics, such as algebra and topology.

[1] Aristotle (384–322 B.C.), G. W. Leibniz (1646–1716), G. Boole (1815–1864), G. Frege (1848–1925), D. Hilbert (1862–1943), B. Russell (1872–1970).

However, these mathematical features do not result in mathematical logic being of interest solely to mathematicians. For example, the mathematical approach leads to a clarification of concepts and problems that also are of importance in traditional logic and in other fields, such as epistemology or the philosophy of science. In this sense the restriction to mathematical methods turns out to be very fruitful.

In mathematical logic, as in traditional logic, *deductions* and *proofs* are central objects of investigation. However, it is the methods of deduction and the types of argument as used in *mathematical* proofs which are considered in mathematical logic (cf. (1)). In the investigations themselves, mathematical methods are applied (cf. (2)). This close relationship between the subject and the method of investigation, particularly in the discussion of foundational problems, may create the impression that we are in danger of becoming trapped in a vicious circle. We shall not be able to discuss this problem in detail until Chapter VII, and we ask the reader who is concerned about it to bear with us until then.

§1. An Example from Group Theory

In this and the next section we present two simple mathematical proofs. They serve as illustrations of some of the methods of proof as used by mathematicians. Guided by these examples we raise some questions which lead us to the main topics of the book.

We begin with the proof of a theorem from group theory. We therefore require the *axioms of group theory*, which we now state. We use $\circ$ to denote the group multiplication and e to denote the identity element. The axioms may then be formulated as follows:

(G1) For all x, y, z: $(x \circ y) \circ z = x \circ (y \circ z)$.
(G2) For all x: $x \circ e = x$.
(G3) For every x there is a y such that $x \circ y = e$.

A *group* is a triple $(G, \circ^G, e^G)$ which satisfies (G1), (G2), and (G3). Here G is a set, e^G is an element of G, and $\circ^G$ is a binary function on G, i.e., a function defined on all pairs of elements from G, the values of which are also elements of G. The variables x, y, z range over elements of G, $\circ$ refers to $\circ^G$, and e refers to e^G.

As an example of a group we mention the additive group of reals $(\mathbb{R}, +, 0)$, where $\mathbb{R}$ is the set of real numbers, $+$ is the usual addition, and 0 is the real number zero. On the other hand, $(\mathbb{R}, \cdot, 1)$ is not a group (where $\cdot$ is the usual multiplication). For example, the real number 0 violates axiom (G3): there is no real number r such that $0 \cdot r = 1$.

We call triples such as $(\mathbb{R}, +, 0)$ or $(\mathbb{R}, \cdot, 1)$ *structures*. In Chapter III we shall give an exact definition of the notion of structure.

Now we prove the following simple theorem from group theory:

1.1 Theorem (Existence of a Left Inverse). *For every x there is a y such that $y \circ x = e$.*

PROOF. Let x be chosen arbitrarily. From (G3) we know that, for a suitable y,

$$x \circ y = e. \tag{1}$$

Again from (G3) we get, for this y, an element z such that

$$y \circ z = e. \tag{2}$$

We can now argue as follows:

$$\begin{aligned} y \circ x &= (y \circ x) \circ e && \text{(by (G2))} \\ &= (y \circ x) \circ (y \circ z) && \text{(from (2))} \\ &= y \circ (x \circ (y \circ z)) && \text{(by (G1))} \\ &= y \circ ((x \circ y) \circ z) && \text{(by (G1))} \\ &= y \circ (e \circ z) && \text{(from (1))} \\ &= (y \circ e) \circ z && \text{(by (G1))} \\ &= y \circ z && \text{(by (G2))} \\ &= e && \text{(from (2)).} \end{aligned}$$

Since x was arbitrary, we conclude that for every x there is a y such that $y \circ x = e$. □

The proof shows that in every structure where (G1), (G2), and (G3) are satisfied, i.e., in every group, the theorem on the existence of a left inverse holds. A mathematician would also describe this situation by saying that the theorem on the existence of a left inverse *follows from*, or *is a consequence of* the axioms of group theory.

§2. An Example from the Theory of Equivalence Relations

The theory of equivalence relations is based on the following three axioms (xRy is to be read "x is equivalent to y"):

(E1) For all x: xRx.
(E2) For all x and y: If xRy, then yRx.
(E3) For all x, y, z: If xRy and yRz, then xRz.

Let A be a nonempty set, and let R^A be a binary relation on A, i.e., $R^A \subset A \times A$. For $(a, b) \in R^A$ we also write aR^Ab. The pair (A, R^A) is another example of a structure. We call R^A an *equivalence relation on* A, and the structure (A, R^A) an *equivalence structure* if (E1), (E2), and (E3) are satisfied. For example, $(\mathbb{Z}, R_5)$ is an equivalence structure, where $\mathbb{Z}$ is the set of integers and

$$R_5 = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } b - a \text{ is divisible by } 5\}.$$

On the other hand, the binary relation R_{rp} on $\mathbb{Z}$, which holds between two integers if they are relatively prime, is not an equivalence relation over $\mathbb{Z}$. For example, 5 and 7 are relatively prime, and 7 and 15 are relatively prime, but 5 and 15 are not relatively prime; thus (E3) does not hold for R_{rp}.

We now prove a simple theorem about equivalence relations.

2.1 Theorem. *If x and y are both equivalent to a third element, they are equivalent to the same elements. More formally, for all x and y, if there is a u such that xRu and yRu, then for all z, xRz if and only if yRz.*

PROOF. Let x and y be given arbitrarily; suppose that for some u

(1) $$xRu \quad \text{and} \quad yRu.$$

From (E2) we then obtain

(2) $$uRx \quad \text{and} \quad uRy.$$

From xRu and uRy we deduce, using (E3),

(3) $$xRy,$$

and from yRu and uRx we likewise get (using (E3))

(4) $$yRx.$$

Now let z be chosen arbitrarily. If

(5) $$xRz$$

then, using (E3), we obtain from (4) and (5)

$$yRz.$$

On the other hand, if

(6) $$yRz$$

then, using (E3), we get from (3) and (6)

$$xRz.$$

Thus the claim is proved for all z. □

As in the previous example, this proof shows that every structure (of the form (A, R^A)) which satisfies the axioms (E1), (E2), and (E3), also satisfies Theorem 2.1, i.e., that 2.1 follows from (E1), (E2), and (E3).

§3. A Preliminary Analysis

We sketch some aspects which the two examples just given have in common. In each case one starts from a system Φ of propositions which is taken to be a *system of axioms* for the theory in question (group theory, theory of equivalence relations). The mathematician is interested in finding the propositions which *follow* from Φ, where a proposition ψ is said to follow from Φ if ψ holds in every structure which satisfies all propositions in Φ. A *proof* of ψ from a system Φ of axioms shows that ψ follows from Φ.

When we think about the scope of methods of mathematical proof, we are led to ask about the converse:

(*) Is every proposition ψ which follows from Φ also provable from Φ?

For example, is every proposition which holds in all groups also provable from the group axioms (G1), (G2), and (G3)?

The material developed in Chapters II through V and in Chapter VII yields an essentially positive answer to (*). Clearly it is necessary to make the concepts "proposition", "follows from", and "provable", which occur in (*), more precise. We sketch briefly how we shall do this.

(1) *The Concept "Proposition"*. Normally the mathematician uses his everyday language (e.g., English or German) to formulate his propositions. But since sentences in everyday language are not, in general, completely unambiguous in their meaning and structure, we cannot specify them by precise definitions. For this reason we shall introduce a *formal language L* which reflects features of mathematical statements. Like programming languages used today, L will be formed according to fixed rules: Starting with a set of symbols (an "alphabet"), we obtain so-called *formulas* as finite symbol strings built up in a standard way. These formulas correspond to propositions expressed in everyday language. For example, the symbols of L will include $\forall$ (to be read "for all"), $\wedge$ ("and"), $\rightarrow$ ("if ... then"), $\equiv$ ("equal"), and variables like x, y, and z. Formulas of L will be expressions like

$$\forall x\, x \equiv x, \qquad x \equiv y, \qquad x \equiv z,$$

and

$$\forall x\, \forall y\, \forall z((x \equiv y \wedge y \equiv z) \rightarrow x \equiv z).$$

Although the expressive power of L may at first appear to be limited, we shall later see that many mathematical propositions can be formulated in L. We shall even see that L is in principle sufficient for all of mathematics. The definition of L will be given in Chapter II.

(2) *The Concept "Follows From" (the Consequence Relation).* Axioms (G1)–(G3) of group theory obtain a meaning when interpreted in structures of the form $(G, \circ^G, e^G)$. In an analogous way we can define the general notion of an L-formula holding in a structure. This enables us (in Chapter III) to define the consequence relation: ψ *follows from* (is a consequence of) Φ if and only if ψ holds in every structure where all formulas of Φ hold.

(3) *The Concept "Proof".* A mathematical proof of a proposition ψ from a system Φ of axioms consists of a series of *inferences* which proceeds from axioms of Φ or propositions that have already been proved to new propositions, and which finally ends with ψ. At each step of a proof the mathematician writes something like "From ... and ____ one obtains directly that ~~~~", and he expects it to be clear to anyone that the validity of ... and of ____ entails the validity of ~~~~.

An analysis of examples shows that the grounds for accepting such inferences are often closely related to the meaning of *connectives*, such as "and", "or", or "if-then", and *quantifiers*, "for all" or "there exists", which occur there. For example, this is the case in the first step of the proof of 1.1, where we deduce from "*for all* x there is a y such that $x \circ y = e$" that for the given x there is a y such that $x \circ y = e$. Or consider the step from (1) and (2) to (3) in the proof of 2.1, where from the proposition "xRu *and* yRu" we infer the left member of the conjunction, "xRu", and from "uRx *and* uRy" we infer the right member, "uRy", and then using (E3) we conclude (3).

The formal character of the language L makes it possible to represent these inferences as formal operations on symbol strings (the L-formulas). Thus, the inference of "xRu" from "xRu and yRu" mentioned above corresponds to the passage from the L-formula $(xRu \wedge yRu)$ to xRu. We can view this as an application of the following *rule*:

(+) It is permissible to pass from an L-formula of the form $(\varphi \wedge \psi)$ to the L-formula φ.

In Chapter IV we shall give a finite system **S** of rules which, like (+), correspond to elementary inference steps the mathematician uses in his proofs. A *formal proof* of the L-formula ψ from the L-formulas in Φ (the "axioms") consists then (by definition) of a sequence of formulas in L which ends with ψ, and in which each L-formula is obtained by application of a rule from **S** to the axioms or to preceding formulas in the sequence.

Having introduced the precise notions, one can convince oneself by examples that mathematical proofs can be imitated by formal proofs in L. Moreover, in Chapter V we shall return to the question (∗) and answer it positively, showing that if a formula ψ follows from a set Φ of formulas, then there is a proof of ψ from Φ, even a formal proof. This is the content of the so-called *Gödel completeness theorem*.

§4. Preview

Gödel's completeness theorem forms a bridge between the notion of proof, which is formal in character, and the notion of consequence, which refers to the meaning in structures. In Chapter VI we shall show how this connection can be used in algebraic investigations.

Once a formal language and an exact notion of proof have been introduced, we have a precise framework for mathematical investigations concerning, for instance, the consistency of mathematics or a justification of rules of inference used in mathematics (Chapters VII and X).

Finally, the formalization of the notion of proof creates the possibility of using a computer to carry out or check proofs. In Chapter X we shall discuss the range and the limitations of such machine-oriented methods.

In the formulas of L the variables refer to the *elements* of a structure, for example, to the elements of a group or the elements of an equivalence structure. In a given structure we often call elements of the domain A *first-order objects*, while subsets of A are called *second-order objects*. Since L only has variables for first-order objects (and thus expressions such as "$\forall x$" and "$\exists x$" apply only to the elements of a structure), we call L a *first-order language*.

Unlike L, the so-called *second-order language* also has variables which range over subsets of the domain of a structure. Thus a proposition about a given group which begins "For all subgroups..." can be directly formulated in the second-order language. We shall investigate this language and others in Chapter IX. In Chapter XII we shall be able to show that no language with more expressive power than L enjoys both an adequate formal concept of proof and other useful properties of L. From this point of view L is a "best-possible" language, and so we succeed in justifying the dominant rôle which the first-order language plays in mathematical logic.