FUNDAMENTALS OF MATHEMATICS

VOLUME I

Foundations of Mathematics
The Real Number System and Algebra

Edited by
H. Behnke
F. Bachmann
K. Fladt
W. Süss

with the assistance of
H. Gerike
F. Hohenberg
G. Pickert
H. Rau

Translated by
S. H. Gould

The MIT Press Cambridge, Massachusetts, and London, England

Contents

Translator's Foreword

The pleasant task of translating this unique work has now extended over several years, in the course of which I have received invaluable assistance from many sources. Fortunately I had the opportunity, in personal conversation or in correspondence, of discussing the entire translation with the original authors, many of whom suggested improvements, supplied exercises, or made changes and additions in the German text, wherever they seemed desirable to bring the discussion up to date, for example, on the continuum hypothesis, Zorn's lemma, or groups of odd order. To all these authors I express my gratitude.

For technical and clerical help I am especially indebted to Linda Shepard, of the Law School at the University of Utah, for her expert typing and discriminating knowledge of English; to Diane Houle, supervisor of the Varitype Section of the American Mathematical Society, for her unrivaled skill and experience in the typing of mathematical translations; to Linda Rinaldi and Ingeborg Menz, secretaries, respectively, of the Translations Department of the Society and the firm Vandenhoeck and Ruprecht, for keeping straight a long and complicated correspondence; to the staff of The MIT Press for their customary technical expertness; and to my wife, Katherine Gould, for help too varied and too substantial to be readily described.

S. H. Gould
Institute of Mathematics
Academia Sinica
Taipei, Taiwan
Republic of China

September 1973

From the Preface

Volume One was begun as the first contribution, by the German section of the International Commission for Mathematical Instruction, to the topic of the scientific foundations of instruction in mathematics, which was one of the topics chosen by the Commission, at a meeting in Paris in October 1954, in preparation for the International Congress of Mathematicians in Edinburgh in 1958. Originally we kept chiefly in mind the needs and interests of the instructor in mathematics, but as our cooperative effort continued from year to year, it became clear that the material in our book was equally important for mathematicians in science, government, and industry. For the best realization of our general purposes, each chapter has been written by two authors, one of them a university professor, the other an instructor with long experience in teaching. In addition to these specifically named authors, of whom there will eventually be more than one hundred, from Germany, Yugoslavia, the Netherlands, Austria, and Switzerland, important contributions have been made to each chapter, in joint semiannual sessions, by the other members of our large group of coworkers.

H. Behnke
K. Fladt

PART A

FOUNDATIONS OF MATHEMATICS

1. Conceptions of the Nature of Mathematics

1.1. *Mathematics and Its Foundations*

In this section, which is an introduction to the work as a whole, we shall be discussing the foundations of mathematics. In other words, we are not *doing* mathematics here; we are talking about mathematics. We are engaged in a scientific activity that has received the appropriate name of *metamathematics*.

Metamathematics forms a bridge between mathematics and philosophy. Some of its investigations can be carried out by mathematical methods, and to this extent the subject shares the exactness of mathematics, the most precise of all sciences. But other parts of metamathematics, among them the most fundamental, are not of a mathematical nature, so that we cannot expect them to have the absolute clarity of mathematics. As in all other branches of philosophy, the answers to many questions are to some extent a matter of subjective attitude and even of faith, and in any given period the attitude predominantly adopted is determined in part by the general spirit of the age. Fundamental philosophical concepts, such as idealism, realism, and nominalism, which for centuries have contended with one another with varying success, are reflected in the different views about the nature of mathematics. Apparently there is no hope of progress in an attempt to refute any one of these views scientifically; rather we try to characterize them as precisely and clearly as possible and in this way keep them apart.

Studies about the foundations of mathematics have experienced a tremendous upsurge during the past hundred years, especially since the turn of the century. The chief impetus for these investigations was provided by the discovery of contradictions in the theory of sets, a mathematical

discipline created during the nineteenth century in connection with eventually successful attempts to clear up the nature of the real numbers. Since many of these paradoxes had already become apparent in antiquity, it is natural to ask why we are now able to deal with them successfully, whereas the ancients found them completely intractable. The answer is that the paradoxes necessarily remained intractable as long as they were expressed in one of the natural languages, such as English. On the shaky ground of such an imprecise language it is impossible to deal with questions of great subtlety, and our present-day successes are entirely due to a new instrument, the thoroughgoing formalization of mathematics. With this new tool it has at last become possible to construct metamathematical theories (for example, that of "classical" logic) which are just as exact as the theories of ordinary mathematics. These new metamathematical theories are regarded by many mathematicians as the essential hallmark of present-day mathematics.

In the following pages we shall describe some of the various conceptions of the nature of mathematics, but it must be remembered that they are only ex post facto idealizations of the nature of mathematics. All idealizations are extreme in one direction or another, so that scarcely any mathematician will agree with every detail of any of the positions that we shall describe. Mathematics as it exists today is in fact the creation of scientists whose inspiration has come from the most varied sources. It is to this variety that mathematics owes its immense vitality.

1.2. *The Genetic Conception of Mathematics*

We first describe a conception of mathematics in which the central role is played by the human being and his capabilities, so that mathematics may almost be said to be a branch of psychology. For example, let us consider the subject of geometry. It is certainly true that the earliest knowledge of geometry, say among the Babylonians, depended on the empirical results of practical surveyors; it is easy to imagine, for instance, how the Pythagorean theorem could arise from individual observations. Yet at this stage the theorem can hardly be called *mathematical*, since the characteristic difference between a natural science and the purely abstract science of mathematics is considered to be that the statements of a natural science can be tested (directly or indirectly) by observation, whereas for mathematical statements such a test is regarded (for widely varying reasons), as meaningless; mathematics is an a priori science in the sense of Kant. Consequently, geometry was in its origins a natural science, and was not "raised" to the position of an abstract, and therefore mathematical, science until the time of the Greeks. It was they who under the influence of Plato distinguished between axioms and the theorems derived from them. In their view the axioms were self-evident (cf. §1.3),

and the theorems were derived by the process of logical deduction. It is probable that the Greek mathematicians took the same attitude toward logic as is taken today by most "naive" mathematicians: in principle, the ability to reason logically is inborn but can be improved with practice.

Arithmetic and many other branches of mathematics may well have begun like geometry as a collection of empirical facts, which was gradually raised to the status of a mathematical science.

But mathematical sciences can arise in another way, which may be called *intramathematical*, to distinguish it from the natural sciences. One of the strongest impulses here is the inborn urge, experienced by most mathematicians and particularly well-developed among the Greeks, toward the sort of beauty that manifests itself in simplicity and symmetry. The mathematician feels compelled, while continuing to observe the demands of logic, *to do away with exceptions*. The desire to make the operations of subtraction and division universally applicable led to the rational numbers. Exceptions in the operation of passing to the limit no longer arose in the field of real numbers. The exceptional case of parallel lines was removed by the introduction of "infinitely distant" points, and in recent times the many exceptional cases arising from the existence of nondifferentiable functions have been avoided by the introduction of *distributions* (cf. Vol. III, chap. 3, §3), which had already turned up among the physicists, in the form of the Dirac δ-function.

Most of these new mathematical entities, created to avoid the necessity for exceptional cases, were in the first place introduced more or less uncritically to meet the demands of each given case. But subsequently there arose a desire to establish the actual existence of such entities. A powerful tool here is the process of *abstraction*, which may be described as follows. Let there be given a set of entities which agree in many of their properties but differ in others. By an act that is in essence arbitrary, we shall declare that some of these properties, depending on the context in which we make the decision, are *essential* while all others are not essential. The act of "abstraction" from the nonessential properties consists of *identifying* (i.e., regarding as identical) those entities that differ only in nonessential properties. A set of such entities thus becomes a single unit and in this way a new entity is created (cf. §8.5). This act of creation, familar to every present-day mathematician, may be regarded as a general human capability. Here we shall only remark that in modern mathematics the process of abstraction, in conjunction with the search for simplicity, has led to the general structures that are to be found, for example, in the theory of groups (cf. §4.3, and Vol. IB, chap. 2).

1.3. *The Extent to Which Mathematical Propositions Are Self-Evident*

As mentioned before, the Greeks divided valid mathematical propositions into axioms and theorems derived therefrom. The axioms were considered self-evident, immediately obvious to everyone, "neither in need of proof nor admitting proof." The theorems, on the other hand, were not immediately obvious in themselves but became evident by being derived from the axioms through a series of arguments, each of which was obviously valid. But today, as a result of the discovery of non-Euclidean geometries, hardly any mathematician holds to the obviousness of Euclidean geometry. The axioms of group theory, field theory, lattice theory, and so forth are no longer considered obvious. At most, the theorems of arithmetic, logic, and perhaps the theory of sets may appear evident (either directly or indirectly) to certain mathematicians. For example, the *intuitionists*, following L. E. J. Brouwer, require that every mathematical construction shall be so immediately apparent to the human mind, and the result so clear, that no further proof is necessary. In §4.7 we shall discuss the attempts that have been made to show that mathematics is free of inconsistencies. Clearly such a proof of consistency will be more widely accepted if it can be based on concepts intuitively apparent to everyone.

To clarify these remarks, let us give an example of a statement that will be considered self-evident by many readers. Let there be given two distinct symbols, neither of which can be divided into meaningful parts. Then it will be considered self-evident that the two "words" obtained by writing these symbols, first in the one order and then in the other, are distinct from each other.

1.4. *The Meaning of Mathematical Propositions*

In general, mathematicians are convinced that their propositions are meaningful, the extreme position in this respect being that of the so-called *formalists*, who consider mathematics to be a mere game with symbols, the rules of which, in the last analysis, are chosen arbitrarily (*conventionalism*). Formalism was introduced by Hilbert as a methodological principle whereby the concept of a proof of consistency could be clearly stated. The formalistic point of view can also be applied to physics if with H. Hertz[1] we define the task of theoretical physics as follows: "Within our own minds we create images or symbols of the external objects, and we construct them in such a way that the logically necessary consequences of the images are again the images of the physically necessary consequences of the objects." In other words, we construct a process parallel to the process of nature. But the essential feature here

[1] *Die Prinzipien der Mechanik*, Ambrosius Barth, Leipzig (1894), Introduction.

is not that this process involves "logical thought" but rather that it runs parallel to the process of nature. Thus we could equally well have chosen a purely formalistic process, which of course would have to be suitably constructed.

Although, as was stated before, the majority of mathematicians hold to the belief that mathematical propositions are not meaningless, they hold widely different opinions about their meaning. It is impossible to go into details here about these varied opinions, and we shall content ourselves with discussing a fundamental dividing line among them, having to do with the concept of infinity. If we adopt the *concept of actual (completed) infinity*, we may speak of the totality of all natural numbers just as readily, for example, as of the totality of natural numbers between 10 and 100. But those who hold to the *concept of potential infinity* emphasize that the infinite totality of all natural numbers as a set is not immediately available to us, and that we can only approach it step by step, by means of successive constructions, such as are indicated by

$$|, ||, |||, \ldots.$$

This is the so-called *constructive* point of view; compare the concept of an algorithm described in §5.

If we examine these concepts further, certain other differences come to light, one of which we will now illustrate by an example. For any given natural number, we can determine in a finite number of steps whether the number is perfect or not.[2] The proposition:

(1.1) *either there exists an odd perfect number between 10 and 100, or else there exists no odd perfect number between 10 and 100*

is acceptable from either the actual or the potential point of view. But matters are quite different for the proposition:

(1.2) *either there exists an odd perfect number, or else there exists no odd perfect number.*

From the *actual* point of view, there is no essential difference between these two propositions. In each case the argument runs as follows: either there exists an odd perfect number between 10 and 100 (or in the set of all natural numbers), in which case (1.1) and (1.2) are correct, or else there is no such number, and in this case also (1.1) and (1.2) are correct.

But in case (1.2) an adherent of the *constructivist* school will argue as follows: the assertion that an odd perfect number exists is meaningful only if such a number has been found (constructed). On the other hand, the assertion that no odd perfect number exists is meaningful only after

[2] A natural number is called *perfect* if it is equal to half the sum of its divisors; for example, 6 is perfect. It is not known whether an odd perfect number exists.

we have shown that the assumption of the existence of such a number leads to a contradiction (i.e., that we can construct a contradiction on the basis of this assumption). But in the present state of our knowledge we cannot make either of these assertions and thus we have no reason to conclude that case (1.2) is true.

Propositions like (1.1) and (1.2) are special cases of the so-called *law of the excluded middle* (tertium non datur). The actual point of view, in contrast to the potential, accepts this law in every case.

The constructive mathematician is an *inventor*; by means of his constructions he creates new entities. On the other hand, the classical mathematician, who regards the infinite as given, is a *discoverer*. The only entities he can *find* are those that already exist.

It is customary nowadays to give the name *classical* to the actual point of view, although the potential attitude can also be traced back to antiquity.

1.5. *Remarks on the Following Sections*

These and other differences in the various conceptions of mathematics have given rise to a great diversity of opinion about the foundations and nature of mathematics, particularly with regard to where the boundary should be drawn between mathematics and logic. Within the space at our disposal it is impossible to discuss all these questions from every point of view. In the following sections we give preference to the classical position, with an occasional reference to the constructivist point of view, when the difference between them is important. Our reasons for giving preference to the classical position are as follows: (1) the greater part of established present-day mathematics is based more or less on the classical conception, whereas many parts of constructive mathematics are still in the process of being built up; (2) the constructive mathematics appears to be far more complicated than the classical. For example, it is not possible to speak simply of the real numbers. These numbers fall into various "levels," and for each level there exist still more complicated numbers.

In the present chapter we have no intention of giving an encyclopedic survey. We have given priority to such questions as are naturally related to college instruction. In some cases the treatment is more detailed because the authors believe that the subject is suitable for discussion by undergraduates in a mathematics club.

The material has been arranged as follows: mathematical proof depends on the fact that propositions have a certain structure (§2); from the classical point of view the basic concept of logic and mathematics is that of a consequence (§3), which plays a fundamental role in the axiomatic method (§4); in practice, the mathematician obtains consequences by

carrying out proofs (§6), a process which has been analyzed in a profound way in the theory of calculi (§5). The next three sections deal with the theory of sets (§7), Boolean algebra (§8), and the theory of relations (§9). A system of axioms of great importance for the mathematician is the Peano system for the natural numbers (§10). Finally, we give an analysis of some of the best-known antinomies (§11).

Bibliography

The bibliography at the end of the present chapter contains several textbooks of mathematical logic dealing with the various problems discussed in the following sections. Let us mention here, once and for all: Beth [1], Curry [1], Kneebone [1], Novikov [1], Rosser [1], Wang [1], and the article on "Logic" by Church [2] in the Encyclopaedia Britannica. On intuitionism see Heyting [1] and Lorenzen [1], and on the history of logic see Kneale [1].

2. Logical Analysis of Propositions

2.1. *The Language of Mathematics*

The results of mathematics, like those of any other science, must be communicable. The communication may take place in either spoken or written form, but for mathematics the difference between them is of no great importance. In studying the foundations of mathematics it is customary to use written symbols.

Communication is ordinarily carried on in one of the natural languages, such as English. But a natural language decays and renews itself like an organism, so that we are engaged in a rather risky business if we wish to entrust "eternal, unchanging truths" of mathematics to such a changing language. Everyone knows how easily misunderstandings arise in the ordinary spoken language. So to attain clarity in his science, the mathematician must try to eliminate the ambiguities of such a language, although the attempt involves a laborious process of evolution and cannot be completely successful. One method of producing greater clarity lies in *formalization*. In the ordinary mathematical literature this process is only partly carried out, as can be seen by a glance at any mathematical text, but in studies of the foundations of mathematics, ordinary speech has been completely replaced by formalized languages. To some extent these artificial languages have been abstracted from ordinary language by a process of analyzing the statements of the latter and retaining only what is logically important. Let us now undertake this process of *logical analysis*. The reader will note a certain resemblance to grammatical analysis, but many of the distinctions made in grammar have no significance in logic. As a result, technical terms common to logic and grammar do not

necessarily have the same meaning. Finally, let us emphasize once and for all that the process of logical analysis is not uniquely determined and could just as well be undertaken in a manner different from the one adopted here.

2.2. *Propositions*

Many combinations of letters are called *propositions*. For example:

(2.1) *Every even number is the sum of two odd numbers.*

(2.2) *Every odd number is the sum of two even numbers.*

(2.3) *Every positive even number, with the exception of the number two, is the sum of two prime numbers.*

In classical logic, which goes back to Aristotle, propositions are divided into *true propositions* and *false propositions*. The *principle of two-valuedness* states that every proposition is either true or false, although it is not required that we should always be able to decide which is the case. For example, it remains unknown at the present time whether the *Goldbach conjecture* (2.3) is true or false, but in classical logic it is assumed that statement (2.3) is in fact either true or false.

Thus the classical logic recognizes two truth values, *true* and *false* (often represented by T and F). Today attention is also paid to *many-valued logics*, and attempts are being made to apply them in quantum mechanics.

The classical point of view has often been criticized (cf. §1.4). But even if we adopt a different attitude, we still *accept* certain propositions, for example (2.1) and *reject* others, for example (2.2); and in general there will be propositions which, at least up to now, have been neither accepted nor rejected, for example proposition (2.3).

It must be emphasized that in the terminology adopted here, which is customary in modern researches in the foundations of mathematics, a proposition is simply a set of written symbols, so that it becomes essential to distinguish between the proposition itself and the state of affairs which it describes. Since this distinction will be of importance in the following sections, let us point out that one of the most profound thinkers in modern logic, G. Frege (1848–1925), distinguishes between the *sense* (Sinn) and the *denotation* (Bedeutung) of a proposition. By the *denotation* of a proposition, Frege means its truth value. Thus the propositions "$1 + 1 = 2$" and "$2 + 2 = 4$" have the same denotation, namely *true*.[3] But these propositions have different *senses*. Similarly, the desig-

[3] One must distinguish between a proposition and a *name* for the proposition, and when we speak of an object, we must have a name for it. Thus we shall make frequent use of the following convention: we obtain a name for a proposition (or more generally for a set of written symbols) if we enclose the proposition (the set of written symbols) in quotation marks. In the present section we shall strictly observe this convention, but later it will be convenient, as frequently in mathematics, to let a set of written symbols stand as a name for itself (*autonomous notation*).

nations (not propositions) "$2 \cdot 2$" and "2^2" have the same denotation, namely the number four, but they too have different senses.

2.3. *Propositional Forms*

In mathematics, we frequently encounter, in addition to the propositions, sets of symbols of the following sort:

(2.4) $x + 3 = y$, (2.5) $f(2, 3) = 5$,

(2.6) $f(x, y) = z$, (2.7) $P2$.

We are not dealing here with propositions, since it is obviously meaningless to ask, for example, whether (2.4) is true or false. The characteristic feature of these new formations is that they contain *variables*, namely "x," "y," "f," "P." Variables are letters that do not refer to any definite entity but rather to a definite range of entities, whose names can be substituted for these variables; the range of the variables must be determined in each case. Thus in (2.4) and (2.6) the "x," "y," and "z" are number variables; for the "x," "y," "z" we may substitute the names of numbers, e.g., "3" or "π." In examples (2.5) and (2.6) the "f" is a function variable, for which we may, for example, substitute "$+$" and in this way[4] convert (2.5) into the proposition "$2 + 3 = 5$." In particular, the range to which the variable refers may consist of sets of linguistic expressions, when we may allow the entities themselves (and not their names) to be substituted for the variables. A case of this sort occurs in (2.7), where "P" is a *predicate variable*, referring to predicates. An example of a predicate is the set of written symbols "is a prime number." When this predicate is substituted for "P," the expression (2.7) becomes the proposition "2 is a prime number." Written symbols like "2" are called subjects (cf. 2.5), so that "x," "y," "z" are *subject variables*.

In order to indicate that a variable "x" has the real numbers for its range, mathematicians often say that x is an *indeterminate real number*, but phrases of this sort are misleading and should be avoided.

After replacement of the variables by objects in their specified ranges, expressions (2.4) through (2.6) become propositions. Consequently, such sets of symbols are called *propositional forms* (formulas).[5] If we agree, as is often done, to extend the meaning of a propositional form to include the propositions themselves, then the latter are propositional forms *without* free variables.

When a proposition is analyzed logically step by step, we usually encounter intermediate forms that are no longer propositions but are still propositional forms. For example, consider the *Fermat conjecture*:

[4] Strictly speaking, of course, this proposition should read "$+ (2, 3) = 5$," but we will permit ourselves to make such changes tacitly.

[5] See the footnote in §4.1.

(2.8) *There do not exist natural numbers* x, y, z, n, *for which* $x \cdot y \cdot z \neq 0$ *and* $2 < n$ *and* $x^n + y^n = z^n$,

where it is natural to regard the propositional form

(2.9) $\qquad x \cdot y \cdot z \neq 0 \quad \textit{and} \quad 2 < n \quad \textit{and} \quad x^n + y^n = z^n,$

as a logically important part of (2.8).

Let us therefore examine propositions and propositional forms simultaneously. In the analysis of propositional forms we find, in addition to the variables, two types of elements. *First* there are such frequently repeated words (or groups of words) as "not," "and," "or," "for all," which in a certain sense are the logical framework of a proposition. The most important of these are the propositional constants (§2.4) and the quantifiers (§2.6). *Secondly* there are the words (or groups of words) that are characteristic of the mathematical theory under examination at the moment and do not occur, in general, in other theories. Examples are "2," "π," "is a prime number," "lies on," "+." The most important types here are subjects, predicates, and function signs (§2.5).

In the following sections we shall examine these elements more closely. They should be compared with the operator of set formation in §7.7, the notation for functions in §8.4, and the description operator in §2.7.

2.4. *The Propositional Constants*

These serve the purpose of combining propositional forms in order to construct new propositional forms. A simple example is "and."

The two propositional forms

(2.10) 2 *divides* x $\qquad$ (2.11) 3 *divides* x

are combined by "and" into the *one* propositional form

(2.12) 2 *divides* x *and* 3 *divides* x.

The propositional form (2.12) is called the *conjunction* of (2.10) and (2.11). The conjunction of two *propositions* is again a *proposition*, which is true (accepted) if and only if both the components united by the "and" are true (accepted). This fact is expressed by the

Truth table (logical matrix) for conjunction

	T	F
T	T	F
F	F	F

For example, the conjunction of a false proposition (the "F" in the left column of the above table) with a true proposition (the "T" of the top

row) is a false proposition (the "*F*" at the intersection of the given row and column).

Another propositional constant is "not," as in

(2.13) 8 *is not a perfect square.*

In a logical systematization of the language it is customary to put the "not" at the beginning and to write:

(2.13′) *Not* 8 *is a perfect square.*

The proposition (2.13′) is called the *negation* of "8 is a perfect square." In the nonclassical schools of logic, negation is either completely banned or, if admitted, it is variously interpreted by the various schools. *One* possibility consists of accepting the negation of a proposition *a* if from *a* we can derive a contradiction (i.e., a proposition that is always rejected). If negation is admitted at all, it is always subject to the condition that no proposition is accepted together with its negative. In the classical two-valued logic it follows that "not" reverses the truth value. Thus we have:

Truth table (logical matrix) for negation

T	*F*
F	*T*

Another important propositional constant is "*or*." The word "or," which in everyday English has several different meanings, is almost always used in mathematics in the nonexclusive sense of the Latin "*vel*," for example:

(2.14) *Every natural number greater than two is a prime number or has a prime factor.*

The combination of two propositions by the nonexclusive "or" is called an *alternative* (or also a *disjunction*, although it would be more correct to reserve the word "disjunction" for the combination of propositions expressed by "either–or"). An alternative is true (accepted) if and only if at least one of its components is true (accepted):

Truth table (logical matrix) for the alternative (disjunction)

	T	*F*
T	*T*	*T*
F	*T*	*F*

The "either–or" is used like the Latin "*aut*," as indicated in the following table:

Truth table (logical matrix) for the strict disjunction

	T	*F*
T	*F*	*T*
F	*T*	*F*

Among the other constants of the propositional calculus we shall mention here only *implication* (and its consequence *equivalence*), which in the English language is represented by the words "*if—then*." For the "if—then" of ordinary spoken language, the logicians have distinguished, in the course of the centuries, several essentially different meanings. We shall restrict ourselves here to describing the one which appears most often in classical logic and mathematics and can be traced back to the Stoics (Philon, ca. 300 B.C.). If a reader feels that he cannot reconcile the "if—then" of the following truth table with his everyday spoken language, he is referred to §3.

Let us now take up the task of constructing a truth table for "if—then." [The four entries will be determined as soon as we have fixed on the truth value of the following four propositions:

(2.15) *If* $1 + 1 = 2$, *then* $1 + 1 = 2$.

(2.16) *If* $1 + 1 = 2$, *then* $1 + 1 = 3$.

(2.17) *If* $-2 = 2$, *then* $(-2)^2 = 2^2$.

(2.18) *If* $1 + 1 = 3$, *then* $1 + 1 = 3$.]

We regard (2.15) and (2.18) as true, and (2.16) as false. As for (2.17), we can argue as follows: The proposition

(2.17′) *For arbitrary real numbers* x, y *it is true that, if* $x = y$, *then* $x^2 = y^2$

is true. A statement that holds for arbitrary real numbers x, y, holds in particular for $x = -2$ and $y = 2$. Thus we recognize (2.17) as a true proposition. Consequently we have the

Truth table (logical matrix) for implication

	T	F
T	T	F
F	T	T

We establish the *convention* that in discussing the classical logic we shall use "if—then" in the above sense. It should be noted that there is no inherent connection between the two parts of an implication defined in this way. For example, the following proposition is true: "*if* $7 + 4 = 11$, *then a triangle with three equal angles has three equal sides.*"

An *equivalence* ("*if and only if*") may be defined as a conjunction of reciprocal implications (see below). Thus we have the

Truth table (logical matrix) for equivalence

	T	F
T	T	F
F	F	T

The propositional constants "not," "and," "or," "if—then," "if and only if" occur so frequently in mathematics that it is worthwhile to introduce *symbols* for them. Usage in present-day logic is not yet uniform. In the following table the symbol given first is the one used in this article.

List of Propositional Symbols

Connective	Everyday English	Symbol
Negation	not	$\neg$ (suggests "—"), over-lining
Conjunction	and	$\wedge$ (dual to "v"), &, ., immediate juxtaposition
Alternative	or	v (suggests "vel")
Implication	if—then	$\rightarrow$, $\supset$
Equivalence	if and only if	$\leftrightarrow$ (combination of "$\rightarrow$" and "$\leftarrow$"), $\equiv$

As already mentioned, we may consider an equivalence as the conjunction of two reciprocal implications. But then we may also say that the equivalence is *defined* by this conjunction. If we introduce the *propositional variables* "p," "q," it is easy to calculate from the tables that we may put "$p \leftrightarrow q$" in place of "$(p \rightarrow q) \wedge (q \rightarrow p)$," as may be seen by calculating the four cases $p, q = T, T;\ T, F;\ F, T;\ F, F$. To state a definition we use the sign "$\Leftrightarrow$," thus, in the present case:

$$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p). \tag{2.19}$$

Similarly, we can justify the following definitions

$$p \rightarrow q \Leftrightarrow \neg p \vee q, \tag{2.20}$$

$$p \vee q \Leftrightarrow \neg(\neg p \wedge \neg q), \tag{2.21}$$

$$p \wedge q \Leftrightarrow \neg(\neg p \vee \neg q). \tag{2.22}$$

2.5. *Subjects, Predicates, and Function Signs*

If we examine the following propositions and propositional forms:

(2.23) 4 *is a prime number*, (2.24) *x lies between* 2 *and* 9,

(2.25) $3 < x$, (2.26) $2 + 4 = 8$,

we see that in addition to the variable "x" they contain the following elements:

the *subjects* "2," "3," "4," "8," "9,"

the *predicates* "*is a prime number*," "*lies between—and*," "$<$," "$=$,"

the *function sign* "$+$."

In the proposition "6 exceeds 3," it is true that from the grammatical point of view "6" is the subject and "3" is the object, but in logic both the "6" and the "3" are subjects.

The above predicates are successively 1, 3, 2, 2-place predicates, and the function sign "$\frac{\ }{\ }$" is a two-place predicate.

Higher-place predicates also occur in mathematics: e.g., the four-place predicate in the propositional form "the point-pair A, B separates the point-pair C, D." A k-place predicate becomes a proposition through the adjunction of k subjects, and in agreement with this manner of speaking we shall sometimes say that the propositions are 0-*place predicates*.

In principle, function signs can be dispensed with entirely, being replaced by predicates. For example, the "$\frac{\ }{\ }$" is superfluous if we introduce the three-place predicate "is the sum of ... and." For then in (2.26) we may write: "8 is the sum of 2 and 4." Since function signs can be eliminated in this way, it is a common practice in purely logical investigations to confine oneself to predicates, and in §3 we will take advantage of this simplification. But mathematicians would be unwilling to give up the functional notation, which is a very suggestive one.

The importance of subjects and predicates will be discussed below in §3.3.

2.6. *Operators in the Calculus of Predicates; Bound Variables*

The proposition

(2.27) *All positive numbers are squares*

contains the operator (or *quantifier*) "all" of predicate logic, which we may analyze in the following way (although there are other possibilities): we are dealing here with the one-place predicates "is a positive number" and "is a square," which we may make more prominent by reformulating the proposition:

(2.27′) *For all entities: If an entity is a positive number, then this entity is a square.*

Here the repeated word "entity" obviously has the task of indicating the places to which the operator "all" shall refer. The same task may be performed in a clear and simple way if we insert one and the same sign in each of these places; for example, the letter "z." Thus we get the standard form:

(2.27″) *For all z: If z is a positive number, then z is a square.*

The letter "z" serves only to mark the place; instead we could use any other letter, e.g., "y." It must be noted that "z" is not a variable of the

kind considered in §2.5, since (2.27″) is a genuine proposition, as distinct from a propositional form. If "z" is replaced in (2.27″) by the name of a number, e.g., "2," we do not obtain a proposition, but rather the linguistic gibberish: "for all 2: If 2 is a ... ."

It is customary to call the letter "z," as used in (2.27″), a *bound variable*, whereas the variables considered earlier are *free variables*. In the propositional form

(2.28) *If z is a positive number, then z is a square*

the letter "z" is a free variable, and (2.27″) is obtained from (2.28) by binding the "z" with the quantifier "all." In this way, a free variable becomes bound.

Bound variables refer, in the same way as free variables, to a given range; in the present case, for example, to the set of real numbers.

The quantifier "all" is called the *universal quantifier*, and (2.27″) is the *universal quantification* of (2.28). A synonym for "all" is, e.g., "every," and a phrase like "for no z" means "for all z not."

A second operator in the calculus of predicates is the *existential quantifier* "there exists" or "there exist" or "for some," as in the following example.

(2.29) *There exist prime numbers.* (2.29′) *There exists a y, such that y is a prime number.*

(2.29″) *For some x: x is a prime number.* (2.30) *x is a prime number.*

The propositions (2.29′) and (2.29″) are variants of (2.29). The existential quantifier can also be used to bind variables. In this connection (2.29) is called an existential quantification of (2.30).

If the range of the variable is finite (for example, the natural numbers from 1 to 9), then the universal and existential quantifiers are, respectively, equivalent to a multiple conjunction and a multiple alternative. Thus if "P" stands for "is a prime number," then "*Every number is a prime number*" is equivalent to "$P1 \wedge P2 \wedge \cdots \wedge P9$" and "*There exists a prime number*" is equivalent to "$P1 \vee P2 \vee \cdots \vee P9$." Consequently we speak of a generalized conjunction or alternative and introduce the symbols "$\bigwedge$" for the universal quantifier and "$\bigvee$" for the existential. Then the familiar Cauchy definition of the continuity of a function f in an interval I takes the following easily understood form:[6]

$$(2.31)\quad \bigwedge_x \bigwedge_\epsilon (x \in I \rightarrow \bigvee_\delta \bigwedge_y (y \in I \wedge |x - y| < \delta \rightarrow |f(x) - f(y)| < \epsilon)).$$

[6] Here the variables x, y refer to real numbers, and the variables ϵ, δ to positive real numbers. Without the latter convention, the statement of (2.31) would be somewhat more complicated.

For every x and every ϵ there exists, if x is an element of the interval I, a δ such that for every element y of the interval I whose distance from x is less than δ the difference between the functional values $f(x)$ and $f(y)$ is less than ϵ.

It is essential to note that if, as in the present case, several quantifiers appear in the same proposition (or propositional form), then the bound variables used (here x, y, ϵ, δ) must be *distinct* from one another.

In classical logic (but only there!) either of the above quantifiers can be defined in terms of the other. For if H is an arbitrary propositional form, we can write:

(2.32) $$\bigwedge_x \mathsf{H} \Leftrightarrow \neg \bigvee_x \neg \mathsf{H},$$

(2.33) $$\bigvee_x \mathsf{H} \Leftrightarrow \neg \bigwedge_x \neg \mathsf{H}.$$

These definitions indicate a certain "duality" between $\wedge$ and $\vee$, which corresponds to a duality between $\wedge$ and $\vee$ (cf. also §9.2).

The following notations are to be found in the literature:

Universal quantifier: $\bigwedge_x \mathsf{H}$, $(x)\mathsf{H}$, $\forall x \mathsf{H}$, $\prod_x \mathsf{H}$,

Existential quantifier: $\bigvee_x \mathsf{H}$, $(\exists x)\mathsf{H}$, $(Ex)\mathsf{H}$, $\exists x \mathsf{H}$, $\sum_x \mathsf{H}$.

2.7. *Identity and Description*

The notation $x = y$ $(x \equiv y)$ means that x and y are the same entity. With this sign for identity we can formulate the statement that the property denoted by a given predicate is possessed by *exactly one* entity. If we let "$\mathfrak{P}$" stand for the predicate "is an even prime number," then the fact that there exists exactly one even prime number can be represented by the proposition:

$$\bigvee_x \mathfrak{P}x \wedge \bigwedge_x \bigwedge_y (\mathfrak{P}x \wedge \mathfrak{P}y \rightarrow x = y).$$

If the property indicated by a predicate holds for exactly one entity, we may speak of *the* entity which has this property. Here we need the *description operator*, represented in ordinary English by some such words as "that—which" and usually denoted in logic by the symbol (ιx). Thus $(\iota x)\,\mathfrak{P}x$ is a name for the number 2, in which x occurs as a bound variable (cf. §2.6). If we are given an arbitrary predicate $\mathfrak{Q}$, e.g., "is divisible by 2," then $\mathfrak{Q}(\iota x)\,\mathfrak{P}x$ means that the property indicated by $\mathfrak{Q}$ is possessed by that unique entity for which $\mathfrak{P}x$ holds. The expression $\mathfrak{Q}(\iota x)\,\mathfrak{P}x$ is often used by Russell as an abbreviation for the proposition: There exists exactly one entity which possesses the property indicated by $\mathfrak{P}$, and all

entities which have this property also have the property indicated by $\mathfrak{Q}$; or, expressed in symbols:

$$\bigvee_x \mathfrak{P}x \wedge \bigwedge_x \bigwedge_y (\mathfrak{P}x \wedge \mathfrak{P}y \rightarrow x = y) \wedge \bigwedge_x (\mathfrak{P}x \rightarrow \mathfrak{Q}x).$$

This proposition is still meaningful (though false), if the property indicated by $\mathfrak{P}$ does not hold for exactly one entity.

Exercises for §2

1. Set up the truth table for "neither-nor." Represent this connective in terms of
   (a) $\neg$ and $\wedge$,
   (b) $\neg$ and $\vee$.
2. Calculate the truth tables for the propositional forms:
   (a) $(p \wedge q) \rightarrow \neg p$
   (b) $(p \rightarrow q) \rightarrow (\neg p \rightarrow \neg q)$
   (c) $(p \vee \neg q) \wedge \neg (q \rightarrow p)$
   (d) $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
3. Express (2.14) in formal language, with the following definitions:
   $Nx \Leftrightarrow x$ is a natural number,
   $Px \Leftrightarrow x$ is a prime number,
   $Gxy \Leftrightarrow x$ is greater than y,
   $Rxy \Leftrightarrow x$ divides y.
4. Translate into English:
   $$\bigvee_x (Nx \wedge \bigwedge_y (Gxy \wedge Ny \rightarrow (Ryx \vee Py))).$$
5. What does
   $$\forall x\,(31 < x \wedge \neg R2x \wedge \neg R3x \wedge x < 37)$$
   mean?
6. Formulate the axioms of a system of axioms for geometry in the symbolism of the predicate logic.

Bibliography

On the technical use of symbols see Carnap [2]. Information on the use of symbols can also be found in many textbooks of mathematical logic (see the bibliographies for §1 and §6). Especially interesting to mathematicians are Tarski [1] and Frege [2].

3. The Concept of a Consequence

3.1. *Semantics*

In this section we discuss a concept which must be considered as basic in the classical treatment of mathematics and particularly of axiomatization. We wish to investigate the connection that exists between, for example, the Euclidean axioms and the theorem of Pythagoras, a connection which is usually expressed in the form: the theorem of Pythagoras is a consequence of the Euclidean axioms. In the present section we think of this connection as being *static*: if the Euclidean axioms are given, then the Pythagorean theorem is in some sense given at the same time. But we may also think of the situation as a *dynamic* one: given the Euclidean axioms, how can we proceed, step by step, to derive the theorem from them. We will return to this question in §6.

The connection between the theorem and the axioms established by saying that the theorem is a *consequence* of the axioms, can be described as follows: the language in which we formulate our mathematical theorems stands in a certain relation to the actual "world," which is to some extent described by the language. In other words, the actual world provides an *interpretation* of the language. The science that deals with such questions is today called *semantics*. Some of the concepts of semantics can be traced as far back as Aristotle and were important in the work of Bolzano, which remained to a great extent unrecognized in his time. The *modern* science of semantics is due to A. Tarski.

In contrast to semantics, investigations of a language that have nothing to do with any interpretation of it are called *syntax*.

3.2. *Definitions*[7]

In the construction of a mathematical theory we not only formulate and prove theorems but also make definitions. A *definition* is an abbreviation. For example, "x is a prime number" stands for "x is a natural number which is different from 1 and has no factor other than 1 and itself." Although the importance of definitions is largely a practical one, it must not be underestimated. If it were not for such abbreviations, the majority of mathematical theorems would be so cumbersome as to be completely unintelligible.

In our study of the concept of a consequence, we must take the definitions into account. It would be simplest, of course, to eliminate them entirely by replacing them with the expressions for which they stand. In the Pythagorean theorem, for example, the expression "is a right-angled triangle" would be replaced by some expression involving only the fundamental concepts of geometry. If, for convenience, we allow the

[7] For the so-called recursive definitions see §7.4.

definitions to stand as they are, it would be more precise to say: the theorem of Pythagoras is a consequence of the Euclidean axioms *and* the definitions that are used in the formulation of the theorem.

3.3. *The Ontological Assumptions of Semantics*

Let us examine more carefully the ideas underlying this attempt to define a consequence more precisely, since in the semantic construction of mathematics it is assumed that such ideas are "understood." If we ask for the meaning of the linguistic expressions we have called *subjects* and *predicates*, we see that a subject is a name for an *individual*, and a predicate is a name for an *attribute* (a *property*). Subjects in ordinary speech, such as "Lincoln" or "New York," name individuals that have a "real existence." Many mathematicians hold the view that individuals such as those named by the subjects "2" and "π" have an "ideal existence," being of different kinds according to the branch of mathematics under consideration. In real analysis, for example, they are the real numbers; and in the theory of functions of a complex variable they are the complex numbers. The individuals investigated in any given context are regarded as forming a *domain of individuals*: for example, the domain of natural numbers. The domain of individuals may have finitely or infinitely many elements but is assumed to have at least one element.

It is also assumed that together with any given domain of individuals the totality of all relevant properties is also given. In this connection a property is relevant if for each individual in the domain the answer to the question whether or not the individual possesses the property is in the nature of things well defined, even though we may not be able to decide whether it is "yes" or "no." This is the ontological basis of the Aristotelian principle of two-valuedness (cf. §2.2). In addition to the one-place properties, such as the one described by the predicate "is a prime number," we also consider many-place properties, e.g., the two-place property (or *relation*) denoted by "$<$." For an n-place property (or relation), it is assumed that for every ordered n-tuple of individuals from the domain under consideration it is determined in the nature of things whether the individuals in the given order stand in the given relation or not.

3.4. *Mathematical Axioms as Propositional Forms*

The concept of a mathematical consequence has been developed chiefly in connection with geometry, above all in researches on the independence of the parallel postulate. We shall therefore take geometry as the starting point for our discussion. The modern attitude toward the axioms of geometry was described in a drastic way by Hilbert when he said: "We must always be able to replace the words 'point,' 'line,' and 'plane' by 'table,' 'chair,' and 'beer-mug.'"

Of course, Hilbert does not mean that the theorems of geometry will remain *true* if we make the suggested change, but only that *for mathematics*, which has the problem of determining *consequences* of the axioms of geometry, it is of no importance whether we speak of points, etc., or of tables, etc. In other words: if a geometrical proposition is a consequence of the Euclidean axioms, then the proposition that arises from it through Hilbert's suggested change in terminology is a consequence of the corresponding axioms arising from the change. In the epigrammatic phrase of Bertrand Russell, "a mathematician does not need to know what he is talking about, or whether what he says is true."

Since in geometry (as in any purely mathematical science; cf. §1.2) we have no interest in the meaning of the predicate "is a point," we may replace it (and correspondingly the other geometric predicates) by a predicate *variable*, thereby concentrating our attention on what is mathematically essential and doing away with everything else. If we write "P" for "is a point," "G" for "is a line," and "L" for "lies on," the first Euclidean axiom (in Hilbert's formulation)

(3.1) *Given any two points A, B, there exists a line a which corresponds to each of the two points A, B.*

Given two points A, B, there is not more than one line which corresponds to each of the given points A, B,

becomes, in the logical symbols introduced in our earlier sections:

$$(3.2)\qquad \bigwedge_x \bigwedge_y ((Px \wedge Py \wedge x \neq y) \rightarrow \bigvee_g (Gg \wedge Lxg \wedge Lyg))$$

$$\bigwedge_x \bigwedge_y \bigwedge_g \bigwedge_h (Px \wedge Py \wedge x \neq y \wedge Gg \wedge Gh \wedge Lxg \wedge Lxh \wedge Lyg \wedge Lyh \rightarrow g = h).$$

Thus we see that for the pure mathematician it is more precise to regard the geometric axioms as *propositional forms* [like (3.2)] than as propositions [like (3.1)]. The so-called *fundamental concepts* of a given mathematical theory, i.e., the subjects and predicates appearing in its axioms, are in this sense simply linguistic paraphrases for subject variables and predicate variables. When the axioms are regarded as propositional forms, they cannot be said to be either true or false. They become true or false only after the variables occurring in them (i.e., the fundamental concepts of the given mathematical theory) have been given an *interpretation*; that is, only when to each (free) subject variable we have assigned an individual of the underlying domain of individuals and to each predicate variable a property (with the same number of places) of the elements of the domain. When propositional variables occur, they are

to be interpreted by means of propositions. Then it becomes meaningful to say that a given propositional form is *true* or *false* in this interpretation. The fact that a propositional form H is true in the interpretation $\mathfrak{D}$ is expressed by saying: $\mathfrak{D}$ satisfies H, $\mathfrak{D}$ is a model of H, $\mathfrak{D}$ verifies H, or H is true in $\mathfrak{D}$. As an example let us choose the domain of natural numbers and consider the propositional forms

(3.3) Px (3.4) $\neg Px$

(3.5) $Px \wedge Qx$ (3.6) $Px \vee Qx$

(3.7) $Px \wedge \neg Px$ (3.8) $Px \vee \neg Px$

(3.9) $\bigvee_x (Px \wedge Qxy)$ (3.10) $\bigwedge_x Px \leftrightarrow \bigwedge_y Py$.

The form (3.3) is true in the interpretation which to the variable x assigns the number 4, and to the variable P the property of being even; in other words, 4 has this property. The form (3.3) is not true if P is interpreted as before while x is interpreted as 5. The form (3.4) is the opposite of (3.3). The form (3.6) is true, and (3.5) is not true, if x is interpreted as 4, while P is interpreted as the property of being prime, and Q as that of being a perfect square. The form (3.8) is true for any interpretation, and (3.7) for none. Consequently, (3.8) is said to be *valid* or a *tautology*, and (3.7) is *contradictory* or a *contradiction*. In (3.9) only the P, Q, y require interpretation and in (3.10) only the P, since the other variables are *bound* (cf. §2.6). The form (3.9) is true if y is interpreted as 10, P as the property of being prime, and Q as the relation of "smaller than," since there exists at least one number which is both prime and smaller than 10. The form (3.10) is a tautology, expressing the fact that a bound variable may be renamed at will. See also the examples in §3.8.

3.5. *The Artificial Language of the Predicate Logic*

The propositional forms (3.2), (3.3), ... (3.10) contain, apart from brackets, only logical symbols and subject and predicate variables. These propositional forms are called *expressions in the predicate logic*. Here it is important that only the subject variables, and not the predicate variables, can be bound by quantifiers.[8] The language of this predicate logic is an artificial language capable of expressing a great part of mathematics. As soon as we have chosen a domain of individuals, we can interpret the subject variables and the predicate variables and can then give an exact definition of what it means to say that a proposition is true in this interpretation. It is most convenient to construct a definition inductively by

[8] If we also allow the predicate variables to be bound, we are in the so-called "logic of the second order," or "extended predicate logic," cf. §10.2.

proceeding from simpler to more complicated expressions. Through lack of space we must content ourselves with this remark and with the above examples.

3.6. *The Concept of a Consequence*

Now let $\mathfrak{A}$ be the set of axioms and H a theorem in a mathematical theory, e.g., in Euclidean geometry. We then say that H is a consequence of $\mathfrak{A}$. If we now take H and the elements of $\mathfrak{A}$ to be propositional forms and interpret the fundamental concepts in such a way that all the axioms are true, it is reasonable to expect that in the given interpretation H will also be true. Thus we have a necessary condition which the concept of a consequence must satisfy. In order to give the widest possible meaning to the concept, we agree to regard this necessary condition as being also sufficient. In this way we arrive at the following

Definition of a Consequence: *The propositional form* H *follows from the set* $\mathfrak{A}$ *of propositional forms* (H *is a consequence of* $\mathfrak{A}$) *if every model common to all the propositional forms of* $\mathfrak{A}$ *is also a model of* H.

Examples: Py, and also Qy follow from $Py \wedge Qy$; and $\vee_x Px$ follows from $\wedge_x Px$ (here it must be noted that by §3.3 a domain of individuals contains at least one element). Also, $\wedge_y Py$ follows from $\wedge_x Px$ and conversely. Every propositional form follows from a contradictory propositional form. A tautology follows from any propositional form.

3.7. *Consequence and Tautology*

If the number of axioms is finite, we can reduce the concept of a consequence to that of a tautology. For this purpose we first form the conjunction Θ of all the axioms in $\mathfrak{A}$. Then we have the important theorem:

H *follows from* $\mathfrak{A}$ *if and only if* $\Theta \rightarrow$ H *is a tautology.*

This theorem expresses the relation between "follows from" and "if—then." The theorem is proved as follows:

(*a*) We first assume that H follows from $\mathfrak{A}$. Then we must show that $\Theta \rightarrow$ H is a tautology, i.e., that $\Theta \rightarrow$ H is true for every interpretation over an arbitrary domain of individuals. To this end we make an arbitrary interpretation $\mathfrak{D}$ of the given domain. In case Θ is false in $\mathfrak{D}$, then $\Theta \rightarrow$ H is certainly true in $\mathfrak{D}$ (cf. the logical matrix in §2.4); and in case Θ is true in $\mathfrak{D}$, then H must also be true in $\mathfrak{D}$, in view of the hypothesis that H is a consequence of $\mathfrak{D}$; thus in this case also $\Theta \rightarrow$ H is true in $\mathfrak{D}$.

(*b*) We now assume that $\Theta \rightarrow$ H is a tautology and must show that H follows from $\mathfrak{A}$. But if this were not the case, then there would be an interpretation $\mathfrak{D}$ for which all the propositional forms in $\mathfrak{A}$ (and there-

fore Θ) would be true but H would be false. Then $\mathfrak{D}$ falsifies $\Theta \to \mathsf{H}$, in contradiction to the hypothesis that $\Theta \to \mathsf{H}$ is a tautology.

3.8. *Examples of Tautologies*

$$\neg \neg p \leftrightarrow p, \tag{3.11}$$

$$\neg (p \wedge p) \leftrightarrow (\neg p \vee \neg q), \tag{3.12}$$

$$\neg (p \vee q) \leftrightarrow (\neg p \wedge \neg q), \tag{3.13}$$

$$\neg (p \to q) \leftrightarrow (p \wedge \neg q), \tag{3.14}$$

$$\neg (p \leftrightarrow q) \leftrightarrow (p \leftrightarrow \neg q), \tag{3.15}$$

$$\neg \bigwedge_x \mathsf{H} \leftrightarrow \bigvee_x \neg \mathsf{H}, \tag{3.16}$$

$$\neg \bigvee_x \mathsf{H} \leftrightarrow \bigwedge_x \neg \mathsf{H}. \tag{3.17}$$

These tautologies form the basis for the *technique of negation*. We obtain a simple application of the theorem in 3.7 if we weaken (3.14) to

$$\neg (p \to q) \to (p \wedge \neg q). \tag{3.14'}$$

Then $p \wedge \neg q$ follows from $\neg (p \to q)$.

Exercises for §3

1. Which of the following propositional forms are tautologies and which are contradictions?

   (a) $\bigvee_x Px \vee \bigwedge_x \neg Px$,

   (b) $\bigwedge_x Px \vee \bigvee_x Px$,

   (c) $\neg \bigwedge_x Px \wedge \neg \bigvee_x \neg Px$,

   (d) $\bigvee_x \neg Px \to \bigvee_y (Py \to Qy)$,

   (e) $\bigwedge_x \bigwedge_y (Rxy \wedge Ryx \to x = y)$.

2. $H_1(=) \bigwedge_x \bigwedge_y (Rxy \wedge Ryz \to Rxz)$

   $H_2(=) \bigwedge_x \bigwedge_y (Rxy \vee Ryx)$

   Over the domain of individuals $\{1, 2, ..., 10\}$ give interpretations which will falsify, or verify,

   (a) H_1

   (b) H_2

   (c) $H_1 \wedge H_2$

3. $H_1 (=) \bigvee_y \bigwedge_x Rxy$

$H_2 (=) \bigwedge_x \bigwedge_y Rxy$

$H_3 (=) \bigwedge_x \bigwedge_y Rxy$

$H_4 (=) \bigvee_x \bigvee_y Rxy$

$H_5 (=) \bigwedge_y \bigwedge_x Rxy$

$H_6 (=) \bigvee_y \bigvee_x Rxy$

Which expressions follow from which? In the cases in which H_i does not follow from H_k give a counterexample, i.e., a model of H_i which is not a model of H_k.

Bibliography

On the foundations of geometry see Borsuk-Szmielew [1], and on modern semantics see Carnap [1], Linsky [1] and Tarski [2].

4. Axiomatization

4.1. *The Origin of Systems of Axioms*

It is today customary to construct a mathematical science axiomatically, that is, by first choosing a set of propositions[9] as the axioms and then drawing consequences from them. The subjects and predicates that occur in the axioms are called the *fundamental concepts* of the system of axioms. From the modern point of view these axioms are considered to be variables, as explained in §3.4. In general, the number of axioms is finite, although infinite systems of axioms are sometimes admitted if their structure is immediately clear. For example, we might take for axioms all the propositions of a certain form. In this case we sometimes speak of an *axiom schema* (for examples, see §10.3 and §11.2).

If the fundamental concepts occurring in the axioms are taken to be variables, so that the axioms themselves become propositional forms, we can no longer regard them as "self-evident." Moreover, if two systems of axioms are *equivalent* (that is, if each of them is a consequence of the other), then in principle they are on an equal footing, even though one of them may be preferred on more or less subjective grounds, e.g., because of its greater logical clarity.

Theoretically, we could use any propositions at all to form our set of axioms, but it turns out that in modern mathematics relatively few systems

[9] By the arguments in §3.4 we should really say "propositional forms" instead of "propositions," but here we wish to conform to the ordinary mathematical usage, in which axioms and theorems are called "propositions."

are in actual use. So it is natural to ask about the motives for choosing these particular systems. We shall confine ourselves to a discussion of this question from the following point of view: It is an established fact that in many cases the theory had a prior existence (at least to a great extent) and the axioms for it were chosen later. But in many cases the axioms are primary; and the theory is to a certain extent secondary, since it has been created and defined by the axioms themselves. We shall distinguish the two cases by speaking of an *heteronomous* and an *autonomous system of axioms*, but it must be emphasized that these concepts are idealizations; in fact, it is often very hard to decide how a given system of axioms actually arose.

4.2. *Heteronomous Systems of Axioms (Subsequent Choice of Axioms)*

In general, we are dealing here with the following problem: we are given a set $\mathfrak{B}$, usually large, of preassigned propositions and we must find a system of axioms (as simple and clear as possible) from which all these propositions follow.[10]

A characteristic example is provided by any theory in physics, or in any other science based on observation. Here the preassigned set $\mathfrak{B}$ consists of a large number of empirical facts, perhaps accompanied by certain hypotheses, and it is our task to find a system of axioms $\mathfrak{A}$ that will provide an economical description of the whole relevant body of knowledge $\mathfrak{B}$. Assuming that we have found such a system of axioms $\mathfrak{A}$, we obtain a *mathematical science* if we ask what are the consequences that follow from $\mathfrak{A}$; but if we then proceed to ask whether these consequences (so far as they can be tested) are in agreement with observation, we are in the domain of *theoretical physics*. Here again the distinction is clear between a *natural science* (cf. §1.2) and mathematics as a purely *abstract science*. When a mathematical system of axioms $\mathfrak{A}$ has arisen in this way, we shall say that the theory determined by $\mathfrak{A}$ has a physical (or, more generally, an empirical) origin. It seems reasonable to believe that Euclidean geometry is such a science. Basic geometrical concepts, like point and line, originated from the need to describe physical data, and consequently the first geometrical propositions were of a physical nature. An example is the theorem of Pythagoras, already well known to the Babylonians in 1700 B.C. This physical origin of geometry becomes particularly clear when we reflect that "experiments" are often made in school to convince the students that the sum of the angles in a triangle is 180°. The axiomatization of geometry was begun by the Greeks, who from the time of Thales (about 590 B.C.) showed that certain geometrical propositions could be made to depend upon others. In relinquishing all

[10] The system of axioms must, of course, be consistent. See §4.7.

recourse to experience, they became the creators of mathematics in the strict sense of the word. The name of Euclid (about 300 B.C.) marks the completion (for the time being) of the axiomatization of geometry.

It is also reasonable to suppose that arithmetic and, to take a modern example, the theory of sets have an empirical origin. The axiomatization of these sciences will be discussed in §10 and §7.

4.3. *Autonomous Systems of Axioms (Systems of Axioms as Sources of New Theories)*

The mathematical theories discussed above were already in existence, at least in a certain sense, long before the corresponding systems of axioms, as becomes quite clear when we recall that in the schoolroom these sciences are often presented without reference to any system of axioms at all; for example, Euclidean geometry in the secondary school and the infinitesimal calculus or naive set theory in the university are often taught in this way. But the situation is completely different in modern mathematical sciences like group theory, ring theory, or lattice theory. These theories cannot be separated from their axioms, since it is only through the axioms that they have come into existence at all. A typical example is the *theory of groups*. In the development of mathematics it has often happened that widely diverse subjects have been seen to depend on lines of argument that are surprisingly similar to one another; e.g., the period of the decimal expansion of a given rational number compared with the number of times a dodecahedron must be rotated in order to bring it back to its original position. It would clearly be more economical not to repeat such arguments at every new occasion but to present them once and for all in such a form that they are immediately applicable to every special case. But an even more important advantage is the fact that by proceeding in this way we concentrate on the essential features of the situation, thereby gaining a deeper insight into the connections among its various parts. In group theory such a program has been carried out. It is possible to formulate a small number of axioms with only *one* fundamental concept, namely *group multiplication*, such that the theory is defined, or so to speak created, by the axioms themselves. The consequences of these axioms are called the *theorems of group theory*. Then by interpreting the group multiplication in various ways, each of which must satisfy the axioms, we at once obtain the original theorems in the various branches of mathematics that led us originally to create the theory of groups. The whole of modern mathematics is characterized (cf. III14) by the attempt to give an increasingly central role to such systems of axioms as those of group theory.

Several of the more modern studies of geometry consist of examining the consequences of a part of the Euclidean axioms, e.g., the axioms of

connection or the axioms of order. Systems of axioms of this sort can also be called autonomous. Similarly, the autonomous systems for algebra are to be considered as arising from the heteronomous system for arithmetic.

4.4. *Independence of a System of Axioms*

A system of axioms is said to be *independent* if no axiom is a consequence of the others. In general, independence is desirable but not altogether necessary; often it is an advantage that can be obtained only at the cost of great complication.

The independence of a given system of axioms is most simply demonstrated by finding for each axiom H an interpretation in which H is false but all the other axioms are true. As a simple example let us consider the three axioms that define an *equivalence relation R*:

$$\bigwedge_x Rxx \qquad \text{(reflexivity)} \tag{4.1}$$

$$\bigwedge_x \bigwedge_y (Rxy \rightarrow Ryx) \qquad \text{(symmetry)} \tag{4.2}$$

$$\bigwedge_x \bigwedge_y \bigwedge_z ((Rxy \wedge Ryz) \rightarrow Rxz) \qquad \text{(transitivity)} \tag{4.3}$$

In each case let us choose as domain of individuals the set of three natural numbers $\{1, 2, 3\}$.

Independence of (1): we interpret R as the empty relation (i.e., the relation that holds for no pair).

Independence of (2): we interpret R as the $\leqslant$ relation.

Independence of (3): we interpret R as the relation that holds between two elements x, y of the domain of individuals if and only if $|x - y| \leqslant 1$.

The fact that the parallel axiom is independent of the other Euclidean axioms can also be proved by this method (see II2, §2).

4.5. *Completeness of a System of Axioms*

Let there be given an axiom system $\mathfrak{A}$. A proposition that contains only subjects and predicates already occurring in $\mathfrak{A}$ will be called a *relevant proposition* and $\mathfrak{A}$ is said to be *complete*[11] if for every relevant proposition H, either H follows from $\mathfrak{A}$ or $\neg$ H follows from $\mathfrak{A}$. This is of course, different from saying that H $\vee \neg$ H follows from $\mathfrak{A}$; the latter proposition is always true, since H $\vee \neg$ H is a tautology (tertium non datur).

[11] Other definitions of completeness can also be found in the literature; cf. §6.2.

Autonomous systems of axioms are in general incomplete as a result of their inherent nature (cf. §4.6). E.g., from the system of axioms for group theory it is impossible, as can be easily shown by examples, to deduce either

$$(4.3)\quad \bigwedge_x x = x^{-1} \qquad \text{or} \qquad (4.4)\quad \neg \bigwedge_x x = x^{-1}$$

On the other hand it is natural to expect, in general, that heteronomous systems of axioms will be complete in view of their physical origin. For suppose we have a relevant proposition H such that neither H nor $\neg$ H follows from the axioms. Then the physicist will at once attempt to obtain *experimental* evidence of the correctness or falsity of this proposition and, if successful, will add either H or $\neg$ H to the set of axioms. Thus, physicists are always striving to complete their systems of axioms, so that it is natural to expect completeness in a well developed theory.

Examples of a complete system of axioms are the system for Euclidean geometry or the Peano system for the natural numbers (cf. §10.2).

4.6. *Monomorphy of a System of Axioms*

The concept of isomorphy, familiar to every mathematician from group theory (see, e.g., IB2, §4.2), can be generalized (we omit the definition here; cf. IB10, §1.3) in such a way that one may speak of *isomorphic interpretations* of a system of axioms. To take an example from geometry: The "natural" interpretation of the Euclidean system of axioms, in which the points are "idealized actual points" and the lines are "idealized actual lines," etc. is isomorphic to the interpretation provided by analytical geometry, in which the points are triples of numbers, the lines are the coefficients of the Hesse normal form, etc.

If a given system of axioms is valid in one interpretation, it is also valid in any isomorphic interpretation. For example, if a given structure is a group, then every isomorphic structure is also a group.

Consequently, it is impossible to characterize a given model completely by means of a system of axioms. The most that can be attained in this direction is to characterize the model "up to isomorphism." A system of axioms is said to be monomorphic (categorical) if any two models are isomorphic.

Autonomous systems of axioms are intended to have a wide range of application and therefore, in general, they are not monomorphic; in fact, there exist nonisomorphic groups, nonisomorphic rings, etc. On the other hand, the heteronomous systems of Euclidean geometry and arithmetic (cf. §10) are monomorphic.

Every monomorphic system of axioms $\mathfrak{A}$ *is complete*: Let H be a relevant proposition. Then we must show that H or $\neg$ H follows from $\mathfrak{A}$. We proceed indirectly by assuming that neither H nor $\neg$ H follows from $\mathfrak{A}$. By the definition of a consequence given in §3, there exists an interpretation $\mathfrak{D}_1$ in which, since H does not follow from $\mathfrak{A}$, all the axioms of $\mathfrak{A}$ are true but H is false. In the same way, there exists an interpretation $\mathfrak{D}_2$ in which, since $\neg$ H does not follow from $\mathfrak{A}$, all the axioms of $\mathfrak{A}$ are true but $\neg$ H is false, and therefore (by the tertium non datur) H is true. On account of the assumed monomorphy of $\mathfrak{A}$, the two interpretations $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are isomorphic, and since H is true in $\mathfrak{D}_2$, it follows that H must also be true in $\mathfrak{D}_1$. But this contradiction refutes the assumption.

4.7. *Consistency of a System of Axioms*

Here we discuss the concept of *semantic consistency*, to be distinguished from *syntactic consistency* (see §5.7), which is another extremely important concept in modern studies in the foundations of mathematics. A system of axioms is said to be (*semantically*) *consistent* if it has at least one model.

In view of the physical origin of many heteronomous systems of axioms, it is natural to regard them as being consistent. But it must always be kept in mind that the consistency of a system of axioms is not, in general, an established fact but only a belief based on confidence in our intuitions. Particularly problematical is the consistency of a set of axioms that can only be interpreted in a domain with infinitely many individuals.

The question of the consistency of a given system of axioms can often be reduced to the same question for another system, in which case we speak of a *proof of relative consistency*. Thus, by means of analytical geometry we can show that the system of axioms for Euclidean geometry is consistent if the system for real analysis is consistent. The most interesting proof of relative consistency is due to Gödel, who proved that a system of axioms for set theory which includes the axiom of choice and the continuum hypothesis (see §7) is consistent relative to the same system without these axioms.

In fact it is well known that belief in the existence of a suitable interpretation can be quite mistaken, for example, in naive set theory (see §7 and §11).

A system of axioms $\mathfrak{A}$ *is inconsistent (self-contradictory) if and only if the proposition* H $\wedge \neg$ H *follows from* $\mathfrak{A}$ *for every relevant proposition* H. For if $\mathfrak{A}$ is inconsistent, then $\mathfrak{A}$ has no model. Thus, every model of $\mathfrak{A}$ is also a model of any arbitrary relevant proposition H, and in particular of H $\wedge \neg$ H; that is, H $\wedge \neg$ H follows from $\mathfrak{A}$. On the other hand, if H $\wedge \neg$ H follows from $\mathfrak{A}$, every model of $\mathfrak{A}$ must also be a model of H $\wedge \neg$ H; but H $\wedge \neg$ H is unrealizable, and therefore $\mathfrak{A}$ has no model.

Exercises for §4

1. The order and the successor relation for the natural numbers can be described by the following axioms (Peano-Hilbert-Bernays):

$$\begin{aligned}
&{}_{x}\,(\neg x < x)\\
&{}_{xyz}\,((x < y \wedge y < z) \rightarrow x < z)\\
&{}_{x}\,x < x'\\
&{}_{x}\,\neg x' = 0\\
&{}_{xy}\,(x' = y' \rightarrow x = y)
\end{aligned}$$

Show by means of suitable models that this system of axioms is independent.

Bibliography

See the textbooks listed in the other sections.

5. The Concept of an Algorithm

5.1. *Examples of Algorithms*

Mathematicians are interested not only in theoretical insight and profound theorems but also in general methods for solving problems, methods whereby certain classes of problems can be handled in such a systematic way that the actual process of solution becomes, so to speak, automatic. Every newly discovered method represents an advance in mathematics, although the problems that are solvable by this method thereby become trivial and cease to form an interesting part of creative mathematics.

A general method of this sort is often called a *calculus*, the name being derived from the small stones or calculi formerly used in computation. Another word with the same meaning is *algorithm*, derived from the name of the Arabic mathematician al-Khuwārizmi (about A.D. 800).

Let us give some examples of algorithms: (*a*) the usual methods of addition, subtraction, multiplication, and division of integers in the decimal notation; (*b*) the Euclidean algorithm for the highest common factor of two integers; (*c*) the well-known procedures for solving linear and quadratic equations with integral coefficients; (*d*) the method of extracting a square root by computing successive decimal places; (*e*) integration of rational functions by means of partial fractions.

The essential feature of an algorithm is that it requires no inspiration or inventiveness but only the ability to recognize sets of symbols and to combine them and break them up according to rules prescribed in advance;

in other words, to carry out elementary procedures that can in principle be entrusted to a machine.

An algorithm proceeds step by step. Some algorithms, when applied to a concrete problem, break off after a finite number of steps, as in the above examples (*a*), (*b*), (*c*), (*e*). Others do not come to an end but can be carried out as far as we like, as in the extraction of a square root, example (*d*). In the above examples every step is, in general, uniquely determined. But in other algorithms it may happen that each step depends upon a free choice among several (finitely many) possibilities. For example, consider the algorithm (*f*) which, when applied to two prescribed integers *a*, *b* (in decimal notation), leaves open at each step a free choice between two possibilities: when two numbers (including *a* and *b*) are already found, we may take (1) their sum or (2) their difference. This algorithm enables us to find all the numbers in the module (*a*, *b*) generated[12] by the two numbers *a* and *b*.

A set of numbers (i.e., a row of symbols) which, as in this example, can be determined by an algorithm, is said to be *recursively enumerable*. Of course as long as the word "algorithm" is being used in an intuitive way, the meaning of "recursively enumerable" also remains intuitive; precise definitions are given in §5.5.

Algorithm (*f*) has two initial "formulas," *a* and *b*, to be thought of as given in their decimal notation, since an algorithm is restricted by its very definition to operating with rows of symbols (or equivalent objects). The above possibilities (1) and (2) for proceeding from one step to the next are called the *rules of the algorithm.*

The initial formulas of an algorithm are sometimes called *axioms* and its rules are *rules of inference*. A finite sequence of formulas, in which each formula is an axiom or arises from the preceding formulas by application of one of the rules, is called a *derivation* or a *proof*. These terms are borrowed from logic but are used here in a much more general sense.

5.2. *Examples of "Arithmetical" Algorithms*

An algorithm for the enumeration of finite sets of strokes (or, as we may say, "of natural numbers") can be described by one axiom

(5.1) $\quad |,$

and one rule

(5.2) $\quad \dfrac{e}{e|}.$

[12] For the concept of a module, see IB1, §2.3.

(Here a/b is to be read: from a we may proceed to b.) This rule contains a *proper variable* e, to be interpreted as follows: any expression already derived may be substituted for e, and then a stroke may be added to the right of it. For example, in the algorithm defined by (5.1) and (5.2), the following expressions are derivable: | (as an axiom), ||, |||, ||||.

For the expressions derived in a given algorithm, we may use variables, say n, m, p, q, for the rows of symbols in the algorithm just described, and then these variables can be used to describe further algorithms. For example, we can define an algorithm for the addition of natural numbers (sequences of strokes). As an axiom we take

(5.3) $$n + | = n |,$$

which is more precisely an *axiom schema*. Then n can be replaced by any one of the rows of symbols, e.g., ||, that are derivable in the algorithm defined by (5.1) and (5.2). As a specialization of (5.3), we obtain the axiom:

(5.3′) $$|| + | = |||.$$

As the only rule in the new algorithm we take

(5.4) $$\frac{n + m = p}{n + m | = p |}.$$

By setting || for n, | for m, and ||| for p, we obtain from (5.3′) the formula

(5.4′) $$|| + || = ||||.$$

In order to construct an algorithm for multiplication, we adjoin the further axiom (axiom schema):

(5.5) $$n \times | = n,$$

and the rule (now with two "premisses"):

(5.6) $$\frac{\begin{array}{c} n \times m = p, \\ p + n = q \end{array}}{n \times m | = q}.$$

As a special case of (5.5) we obtain

(5.5′) $$|| \times | = ||.$$

If we apply the rule (5.6) to (5.4′) and (5.5′), we have

(5.6′) $$|| \times || = ||||.$$

5.3. *Recursively Enumerable and Decidable Sets*

Although it has been possible to set up algorithms for the solution of many mathematical problems, others have continued to resist every attack of this kind, a prominent example being the "word problem" in group theory (cf. IB2, §16.1). As a result, mathematicians finally began to suspect that certain problems cannot be solved by any algorithm whatever. It is obvious that a theorem of this sort will become meaningful, and we can proceed to demonstrate it, only when we have given an exact definition of the concept of an algorithm.

More precisely, we need only know what we mean by saying that a given set of rows of symbols is recursively enumerable, i.e., can be found by means of an algorithm. Here we must realize that more is expected from such a definition than, for example, from the definition of continuity of a function. In the latter case we are quite satisfied with the simple, well-known definition of Cauchy, since it is to a great extent in agreement with our intuition, although everyone knows, from certain striking examples, that this agreement is by no means complete. But for a recursively enumerable set, where we are dealing with the question of what can or cannot be accomplished in an actual computation, the definition must agree to the greatest possible extent with our basic intuitive notion of what is meant by effective calculation of the answer to a given problem. The assertion that a given set is not recursively enumerable, i.e., that it is impossible to construct an algorithm for finding the elements of the set, is of interest only to the extent to which our formal definition of an algorithm is in agreement with our intuitive notion of a process of computation.

Several different definitions have been suggested for enumerability (the first one of them by Church in 1936), but in spite of the fact that they originated in very different settings, they are all equivalent to one another. Consequently, many logicians and mathematicians are convinced that these definitions correspond completely to our intuitive notion of computability. They are to be considered from the classical point of view, since they make use of the nonconstructive phrase "there exists." If they have been criticized, it is usually by mathematicians who do not share the classical point of view and therefore assert that the definitions include more than our original intuitive notions. However, a proof of non-enumerability based on too broad a definition retains its validity when the definition is restricted.

After a preparatory section, we shall give in §5.5 a definition of algorithm (or alternatively of recursive enumerability) which is based on the concept of a recursive function. We could set up an alternative definition by generalizing the procedure in §5.2; and a third method stems from the fact that, in principle, every algorithm can be entrusted to a machine

(Turing). There are further possibilities but we omit them here for lack of space.

A property $\mathfrak{E}$ of formulas is said to be *decidable* if the set of formulas that have the property $\mathfrak{E}$ and also the set of formulas that do not have it are recursively enumerable. The decidability of several-place properties (relations) is defined correspondingly. In the case of a decidable property we can decide, by any of the three methods of recursive enumeration mentioned above, whether a given formula ζ has the property or not.

5.4. *Gödelization*

The formulas that can be written in a given finite or countably infinite alphabet can be characterized in various ways by natural numbers (or by the sequences of strokes that correspond to them). We now describe one such method, taking as an example the formulas (words) that can be written with the twenty-six letters of the Latin alphabet. We first enumerate the letters; e.g., 1. a, 2. b, ..., 26. z. Now consider a given n-letter word (i.e., a formula) in the alphabet, and let the numerals assigned to the successive letters of this word be $\nu_1, \ldots, \nu_n$. Also let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the sequence of prime numbers. Then the given word can be characterized by the number (Gödel index)

(5.7)
$$p_1^{\nu_1} \cdot p_2^{\nu_2} \cdots p_n^{\nu_n}.$$

For example, the word "cab" will receive the number $600 = 2^3 \cdot 3^1 \cdot 5^2$. Distinct words correspond to distinct numbers but not every number corresponds to a word. If the number of a word is known, the word itself can be recovered.

A transition of this sort from the words to the corresponding numbers is called *arithmetization* or *Gödelization*. In all questions concerning algorithms, it makes no difference whether we discuss the original formulas or their Gödel numbers.

A recursively enumerable set of words is transformed in this way into a recursively enumerable set of natural numbers and vice versa. It therefore makes no difference, in principle, whether the desired exact definition of recursive enumerability is expressed in terms of words or of natural numbers. Since the natural numbers have a somewhat simpler structure and are more familiar to mathematicians, we will now proceed to define the concept of recursive enumerability for a set of natural numbers.

5.5. *Computable Functions and Recursively Enumerable Sets*

Instead of giving a direct definition of a recursively enumerable set, we shall first define the concept of a computable function, to which the concept of recursive enumerability can be reduced.

We consider functions, with one or more arguments ranging over the entire set of natural numbers, whose values are also natural numbers. Such a function is said to be *computable* (in the intuitive sense) if, for arbitrarily preassigned arguments, there exists a procedure for calculating the value of the function in a finite number of steps. Examples of computable functions are the sum of two numbers, and their product. The following example defines a function f about which we do not know at the present time whether it is computable or not:

$$(5.8)\quad f(n) = \begin{cases} 0, \text{ in case there exist natural numbers } x, y, z \text{ such that} \\ x \cdot y \cdot z \neq 0 \quad \text{and} \quad x^n + y^n = z^n, \\ 1 \text{ otherwise.} \end{cases}$$

At present we know only a few of the values of this function, e.g.,

$$f(1) = f(2) = 0, \qquad f(3) = f(4) = \cdots = f(100) = 1.$$

If the Fermat conjecture is true, then $f(n) = 1$ for $n \geqslant 3$.

The following argument shows that the computable functions are exceptional. There cannot exist a greater number of computable functions than there are methods for computing them. Every method of computation must be capable of being described. A description consists of a finite number of symbols. It follows that there are only countably many possible descriptions, and therefore only countably many computable functions. On the other hand, the total of number of functions is uncountable, as may be proved by the same diagonal procedure as the uncountability of the continuum (see §7).

The concept of a recursively enumerable set can be reduced to that of a computable function. For we have the theorem:

A non-empty set of natural numbers is recursively enumerable if and only if it is the range of values of a computable function.[13]

To prove this theorem we argue as follows: A set which is the range of values of a computable function f can be recursively enumerated by calculating the successive values $f(0)$, $f(1)$, $f(2)$, ..., as may be done in each case in a finite number of steps. We thus obtain an algorithm that produces all the elements of the set (in general, of course, they will not be obtained in order of magnitude, but that is not necessary).

On the other hand, let there be given a non-empty, recursively enumerable set M, so that M contains at least one element n_0. Now the successive steps of an algorithm for the recursive enumeration of M can be arranged (if necessary by the adjunction of certain rules) in a unique

[13] It is customary to say that the empty set is also recursively enumerable.

sequence, with a zeroth, first, second step, etc. Every step produces an element of M, or at least an intermediate stage toward the production of such an element. We now define a function f as follows:

$$f(n) = \begin{cases} n_0, \text{ in case the } n\text{th step provides only an} \\ \text{intermediate stage,} \\ k, \text{ in case the } n\text{th step provides an element of } M \\ \text{and this element is } k. \end{cases}$$

From the definition of f it is clear that f is computable and that the range of values of f coincides with the set M.

Thus it is only necessary to give a precise definition of the concept of a computable function. This precise definition is provided by the *recursive functions* as defined in the next section.

5.6. *Recursive Functions*

In the domain of natural numbers the sum function is determined by two equations (cf. §5.2):

(5.9) $$x + 0 = x,$$

(5.10) $$x + y' = (x + y)',$$

where the successor of y is denoted by y'. These equations enable us to calculate the sum $u + v$ of any pair of natural numbers u, v in a purely formal way. For this purpose we require only two rules: (a) for the variables occurring in (5.9) and (5.10) we may substitute numerals $(0, 0'(=1), 0''(=2), \ldots)$, and (b) if for these numerals we have already derived the result $z_1 + z_2 = z_3$, then on the right-hand side of any subsequently derived equation we may replace $z_1 + z_2$ by z_3. Corresponding rules hold for the product function, except that in this case the set of two equations (5.9) and (5.10) must be augmented by two further equations

(5.11) $$x \cdot 0 = 0,$$

(5.12) $$x \cdot y' = x \cdot y + x.$$

Thus the sum plays the role of an auxiliary function for the product.

The concept of a recursive function, as defined by Herbrand and Gödel, is based on a generalization of the above procedure. An n-place function ϕ is said to be *recursive* if there exists a finite system of equations Σ containing a function symbol f corresponding to ϕ and also in general, containing function symbols g, h, ... for auxiliary functions, such that for

every choice of $n + 1$ numbers $k_1, \ldots, k_n, k$ we have the following result:[14] if $z_1, \ldots, z_n, z$ are the numerals corresponding to the numbers $k_1, \ldots k_n, k$, then the equation $f(z_1, \ldots, z_n) = z$ can be derived from $\sum$ if and only if $\phi(k_1, \ldots, k_n) = k$. In the process of derivation we may make use of two rules corresponding to the ones given above: (*a*) in every equation of $\sum$ we may substitute numerals for the variables; (*b*) if for any given numerals $Z_1, \ldots, Z_n, Z$ and function symbol F we have already derived an equation $F(Z_1, \ldots, Z_n) = Z$, then on the right-hand side of any subsequently derived equation we may replace $F(Z_1, \ldots, Z_n)$ by Z.

The precise concept of a recursive function is to be regarded as corresponding to the intuitive concept of a computable function. In particular, the functions x^y, $x!$, $| x - y |$ are recursive.

5.7. *Consistency of an Algorithm and Consistency of Mathematics*

The formulas that can be derived by an algorithm consist of rows of single symbols (not necessarily letters in the ordinary sense of the word) from a given *alphabet*. In general, it will not be possible to derive all the various formulas that could be constructed from this alphabet. There will be at least one formula A whose derivability is "undesirable." Such a formula might, for example, be $Px \wedge \neg Px$ (cf. §4.7), or $x \neq x$, or $| = ||$.[15] An algorithm K is called *consistent* with respect to a formula A of this sort if A is not derivable. We are speaking here of the *syntactical consistency* already mentioned in §4. A *consistency proof* for K consists in a demonstration that A is not derivable. A consistency proof in the constructive sense must employ only self-evident assertions and must avoid all ideas that are problematical from the semantic point of view, e.g., the idea of the actual-infinite, since such ideas are not accepted by all mathematicians. On the other hand, it is considered acceptable to make use of inductive proofs concerning the structure of an algorithm. Let us give a simple example: the alphabet of the algorithm K consists of the two letters $\circ$ and $|$. There is a single axiom

$$\circ. \tag{5.13}$$

As a rule of inference (with the proper variable e) we take

$$\frac{e}{e\,|}\,. \tag{5.14}$$

[14] Let us note the difference between numbers and numerals. It is customary to regard numbers as some sort of ideal entities that are represented in writing by symbols called numerals. In order to make the discussion more systematic, it is better here not to use the ordinary Arabic numerals for the numbers but, as was mentioned above, to represent the number 4, for example, by the numeral $0''''$. Numbers cannot be written down, but numerals can.

[15] $x \equiv y$ means that x and y are the same formulas.

In this algorithm the formula | is not derivable: that is, A is consistent with respect to |. The proof is inductive: we cannot derive | from (5.13), since | is different from ⊃. Also, we cannot derive | from (5.14) since every formula that can be derived from (5.14) must consist of more than a single letter.

For many of the important algorithms in mathematics, it has been possible to derive their consistency by "acceptable" methods of this sort, sometimes called "finitary." Moreover, the researches of Hilbert, Gentzen, Ackermann, Schütte, Lorenzen, and others have proved the consistency of the so-called *ramified analysis* closely connected with constructive mathematics (cf. §1, Nr. 4 and 5). On the other hand, no one has yet succeeded in proving the consistency of classical analysis.

Even though algorithms are of great importance for mathematics, it is still the opinion of many researchers that the whole of mathematics itself cannot be regarded as an algorithm (cf. "Incompleteness of Arithmetic," §10.5). In this case it makes no sense to speak of the syntactical consistency of mathematics as a whole.

For the *constructivist school* of mathematics, as represented, for example, by Curry and Lorenzen (§1.4, 5), all mathematical theorems are evident in the above sense. For the adherents of this school the whole of mathematics is a priori as reliable as a consistent algorithm.

Exercises for §5

1. From the functional equations

(5.9)

(5.10)

(5.11)

(5.12)

and the rules given in the text prove that

$$0''' \cdot 0'' = 0''''' \qquad (3 \cdot 2 = 6).$$

2. Give recursion equations for the function x^y. From them prove that

$$(0'')^{0''} = 0'' \qquad (2^2 = 4).$$

3. Introduce the functions

$x!$

$\mathfrak{P}(x)$ (predecessor of X; 0 if $x = 0$)

$a \dot{-} b$ (difference; 0 if $a < b$)

by recursion equations. Assume $a + b$, $a \cdot b$ and functions already defined.

4. Show that the calculus determined by the equations (5.9), (5.10), together with the rules (a) and (b) given for them in the text, is syntactically consistent.

5. If a set of natural numbers arranged in order of increasing magnitude is recursively enumerable, then it is also decidable.

Bibliography

For recursive functions and the concepts related to them see Davis [1], Hermes [1], and Kleene [1].

6. Proofs

6.1. *Rules of Inference and Proofs*

Let there be given a system of axioms, say the axioms of Euclidean geometry. The theorem of Pythagoras is a consequence of these axioms, but that fact is not immediately obvious; it becomes so only step by step. Each step consists of the application of a rule of inference. A *rule of inference* is an instruction concerning a possible transition from certain preceding formulas (the premisses) to a subsequent formula (the conclusion). A simple example with two premisses is the *modus ponens* (the *rule of separation*)

$$\frac{\mathsf{H} \to \Theta \qquad \mathsf{H}}{\Theta} \tag{6.1}$$

This rule enables us to make the transition from the two premisses $\mathsf{H} \to \Theta$ and H to the conclusion Θ. An *inference* is a transition in accordance with a rule of inference. A *proof* (*derivation*, *deduction*) is a finite sequence of expressions each of which (unless it is an axiom) can be derived from the preceding expressions by means of the rules of inference.

6.2. *A Complete System of Inference*

Although it is clear that there exist an infinite number of different rules of inference, in actual practice the mathematician makes use of only a very few of them, which recur again and again in many different arrangements. So we naturally ask whether it is possible to find a *finite* system of rules of inference by means of which we can deduce *all* the consequences of an arbitrary system of axioms. Such a system may be called a *complete system of rules of inference*, and it is one of the basic discoveries of modern logic that, within certain limitations, complete systems of rules of inference actually exist. The limitations in each case depend on how much the given system of logic is able to express. For example, a complete system can be

found if we confine ourselves to axioms and to consequences expressible in the language of predicate logic, which is sufficient for many parts of mathematics. But the situation is different if we admit quantification of predicate variables. See the "Incompleteness of the Extended Predicate Logic" (§10).

The fact that within the framework of predicate logic every consequence can be derived by a finite system of rules of inference is described by saying that the predicate calculus determined by these rules is *complete*. The existence of such a calculus was foreseen by Leibniz in his demand for an *ars inveniendi*; to a certain extent it was experimentally verified by Whitehead and Russell in their monumental work *Principia Mathematica* (1910–1913) (based on the preliminary work of various logicians; in particular, Boole's *Algebra of Logic*, 1847), and finally, in 1930, it was proved by Gödel in his famous Gödel *completeness theorem*.

In the terminology of the foregoing section the Gödel completeness theorem asserts the existence of an algorithm for recursively enumerating all consequences of an arbitrary system of axioms that can be stated in the language of predicate logic.

6.3. *The Complete System of Rules of Inference of Gentzen (1934) and Quine (1950)*

Several different complete systems of rules of inference are known today but here we must restrict ourselves to the one which, since it is closely related to the ordinary reasoning of mathematicians, is called the "*system of natural inference*." The advantage of close relationship with ordinary mathematical practice is gained at the expense of unnecessary loss of symmetry and formal elegance, so that in purely logical investigations it is customary to use other systems.

For a greater clarity let us make some preliminary remarks. A characteristic feature of mathematical reasoning is the use of *assumptions*. Among the assumptions introduced during the course of a proof in any given mathematical theory we must include the axioms of the theory, or at any rate those axioms that are referred to in the proof. But in addition to the axioms, a mathematician will often introduce further (unproved) assumptions, on the basis of which the proof then proceeds. Of course, all assumptions that are made in this way must later be eliminated.

A special case of the introduction of assumptions occurs in an *indirect proof*. Here we arbitrarily assume the negative of the theorem to be proved.[16] Then in the course of the proof we try to reduce this assumption

[16] In case we wish to prove $\neg H$, we arbitrarily assume the proposition H (cf. the last example in §6.6).

ad absurdum, that is, we try to deduce from it two mutually contradictory results. It should be emphasized that, at least from the point of view of the classical logic under discussion here, an indirect proof is just as good as any other (although the situation is different for other schools of logic; see §6.7).

Another characteristic feature of mathematical reasoning is the introduction of variables for entities whose existence is already known. Consider, for example, two nonparallel lines g and h in a plane. We know that g and h have at least one point in common (in particular if the two lines coincide), and then the mathematician will say something like, "let a be a point common to the two lines." But the variable a here has no independent significance; it is meaningful only with respect to the proposition asserting its existence, a fact that must be kept in mind during the course of the proof. Variables of this sort also occur in the system of Gentzen and Quine, where they are called *flagged variables*. In order to avoid the danger of misunderstanding and consequent mistakes, it is not permissible to introduce the same variable for different entities during the course of a proof; this restriction is called the *restriction against flagging the same variable twice*. In general, a flagged variable will "depend" on other variables that have already appeared in the proof (in our example, a depends on g and h), in which case we stipulate that no variable may depend (even indirectly) on a second variable which in turn depends on the first; this restriction is called the *restriction against circularity*.

6.4. *List of the Rules of Gentzen and Quine*

For an explanation of these rules see §6.5, and the example of §6.6. Most of the rules have to do with the *introduction* or the *elimination* of a logical constant.

Two further rules without premisses (cf. §6.5):

a. the rule for *introduction of assumptions*,

b. the rule of *tertium non datur*.

6.5. *Explanation of the Rules*

By a *proof* we shall mean, here and in the rest of this section, a finite sequence of expressions that follow one another according to these two rules. Here it must be emphasized that this precise definition of a proof is altogether necessary in studies of the foundations of mathematics, in contrast to the situation in ordinary unformalized mathematics, where it is not customary to state the rules of inference being used. The lines in a given proof can now be numbered. Each line consists of finitely many *assumptions* (perhaps none) and an *assertion*. As a typical example we take the rule for $\wedge$-induction. This rule allows us to proceed from a line

numbered i and a line numbered k ($i \neq k$) to a line numbered l (with $l > i, l > k$), whose assertion is the conjunction of the assertions of the ith and kth lines, and whose assumptions consist of the "juxtaposition" of the assumptions of the ith and kth lines; i.e., an expression is an

The Rules of Gentzen and Quine for the Predicate Calculus

Logical Constant	*Introduction*	*Elimination*
$\wedge$	$\dfrac{\mathsf{H} \quad \Theta}{\mathsf{H} \wedge \Theta}$	$\dfrac{\mathsf{H} \wedge \Theta}{\mathsf{H}} \quad \dfrac{\mathsf{H} \wedge \Theta}{\Theta}$
$\vee$	$\dfrac{\mathsf{H}}{\mathsf{H} \vee \Theta} \quad \dfrac{\Theta}{\mathsf{H} \vee \Theta}$	$\dfrac{\mathsf{H} \vee \Theta \quad \mathsf{H} \to \mathsf{Z} \quad \Theta \to \mathsf{Z}}{\mathsf{Z}}$
$\leftrightarrow$	$\dfrac{\mathsf{H} \to \Theta \quad \Theta \to \mathsf{H}}{\mathsf{H} \leftrightarrow \Theta}$	$\dfrac{\mathsf{H} \leftrightarrow \Theta}{\mathsf{H} \to \Theta} \quad \dfrac{\mathsf{H} \leftrightarrow \Theta}{\Theta \to \mathsf{H}}$
$\neg$	$\dfrac{\mathsf{H} \to \Theta \quad \mathsf{H} \to \neg\Theta}{\neg\mathsf{H}}$	$\dfrac{\mathsf{H} \quad \neg\mathsf{H}}{\Theta}$
$\to$	$\dfrac{\Theta}{\mathsf{H} \to \Theta}$	$\dfrac{\mathsf{H} \to \Theta \quad \mathsf{H}}{\Theta}$
$\vee$	$\dfrac{\Theta\ ^{17}}{\underset{x}{\vee}\,\mathsf{H}}$	$\dfrac{\underset{x}{\vee}\,\mathsf{H}\ ^{17}}{\Theta}$
$\wedge$	$\dfrac{\Theta\ ^{18}}{\underset{x}{\wedge}\,\mathsf{H}}$	$\dfrac{\underset{x}{\wedge}\,\mathsf{H}\ ^{18}}{\Theta}$

[17] Assumption: H becomes Θ by free renaming of x to a variable y, and conversely Θ becomes H by the reverse renaming of y to x. *The variable y must be flagged* with respect to the free variables occurring in $\wedge_x \mathsf{H}$ and $\vee_x \mathsf{H}$.

[18] Assumption: H becomes Θ by *free renaming* of the variable x to a variable y. (An exact definition of free renaming cannot be given here. We shall merely give a typical example: H $(\wedge_u Pxu \wedge Qxy)$ becomes Θ $(\wedge_u Pyu \wedge Qyy)$ by free renaming of x to y.) Here y may also coincide with x.

assumption of the lth line if it is an assumption of the ith or of the kth line (the order in which the assumptions are written is of no importance, and an assumption which occurs several times may be written only once); schematically:

Line Number	*Assumptions*	*Assertion*
...	...	...
i	$A_1, ..., A_r$	H
...	...	...
k	$B_1, ..., B_s$	Θ
...	...	...
l	$A_1, ..., A_r, B_1, ..., B_s$	$\mathsf{H} \wedge \Theta$

When use is made of the rules of $\vee$-elimination (elimination of the existential quantifier) or of $\vee$-introduction (introduction of the universal quantifier), it is mandatory to *flag a variable* with a statement of the variables on which it depends. For example, if $u_1, ..., u_n$ are the free variables in $\vee_x H$, then in making use of the rule of $\vee$-elimination we must write the new line l as follows:

Line	*Flagged Variables*	*Assumptions*	*Assertion*
l	$y(u_1, ..., u_n)$	$A_1, ..., A_r$	Θ.

The procedure for the rule of $\wedge$-introduction is analogous.[19]

The rule for $\rightarrow$-introduction may also be called *assumption-elimination*; for if H is an arbitrary assumption of the initial line (see the list of rules), then H will no longer occur as an assumption in the final line of the proof. In contrast to the rules described up to now, which allow us to pass from one, two, or three lines of the proof to a new line, the two rules of assumption-introduction and tertium non datur allow us to write down a line in the proof without making use of any preceding line. The rule of *assumption-introduction* consists simply of writing down an arbitrary proposition both as assumption and as assertion:

Line Number	*Assumptions*	*Assertion*
l	H	H

[19] In this rule the necessity for flagging is perhaps not immediately obvious; let us motivate it by the remark that the rule for $\wedge$-introduction is *dual* to the rule for $\vee$-elimination.

The rule of *tertium non datur* allows us to write down any particular case of tertium non datur without assumptions:

Line Number	*Assumptions*	*Assertion*
l	—	$\mathsf{H} \vee \neg \mathsf{H}$

The last line of a *finished proof* must not contain any flagged variable as a free variable, since such a variable has no independent significance. Also, after constructing such a proof, we must verify that we have observed the restrictions against flagging a variable twice and against circularity.[20]

It can be proved that the assertion of the last line of a finished proof is a consequence (in the sense of §3.6) *of the assumptions of the last line of the proof. Conversely, if* Θ *is a consequence of* $\mathsf{H}_1, \ldots, \mathsf{H}_n$, *then there always exists a finished proof with a last line whose assumptions are* $\mathsf{H}_1, \ldots, \mathsf{H}_n$ *and whose assertion is* Θ.

In the present sense of the word, a proof is analogous to a schematic procedure for making a computation. Thus the process of proof has all the advantages and disadvantages of other schematic procedures that have been developed in mathematics. The *advantage* lies in the fact that in a mechanical procedure of this sort it is no longer necessary to do any thinking, or at least not as much as before, although this advantage can only be gained at the cost of considerable training in the art of carrying out the procedure. The *disadvantage* of a schematic procedure is that the rules which are simplest from the formal point of view are not always the ones that are most immediately obvious to the human mind.

On the other hand, if we wish to explain why exactly these formal rules were chosen, and no others, our explanation must be based on arguments whose meaning is intuitively clear. For lack of space we cannot give a detailed explanation here and will merely make a few remarks: the rules for V-introduction express the fact that if we have proved an assertion H under certain assumptions, then under the same assumptions we may make the weaker assertion $\mathsf{H} \vee \Theta$ or $\Theta \vee \mathsf{H}$. This rule is used in arithmetic, for example, in making approximations where we proceed from an already proved assertion of the form $x < 1$ to the weaker assertion $x \leqslant 1$ (i.e., $x < 1 \vee x = 1$). The rule for $\neg$-elimination expresses the following fact: if the assertion H follows from certain assumptions, and the assertion $\neg \mathsf{H}$ from certain other assumptions, then the two sets of assumptions taken together form an inconsistent system from which an arbitrary proposition Θ follows trivially. The rule for $\rightarrow$-introduction means only that if a proposition Θ follows from certain assumptions, including in particular the assumption H, then the proposition *if* H *then* Θ follows from the same set of assumptions excluding H.

We now give two examples of proofs. The reader is advised to direct his attention less to the actual meaning of the steps in the proof than to the question

[20] The restriction against flagging a variable twice prevents us from proceeding from $\vee_x \mathsf{H}$ through H to $\wedge_x \mathsf{H}$, since x would have to be flagged twice; and even if we introduce a new variable y, we cannot pass from $\vee_x \mathsf{H}$ to $\wedge_x \mathsf{H}$ without double flagging.

whether the above formal rules have been correctly applied. Of course, this will cost him some effort, comparable to the effort required when one undertakes for the first time to solve a quadratic equation by some formal procedure.

6.6. *Two Examples of Proofs*[21]

We begin with a proof that H follows from $\neg\neg$ H. This fact, which is valid only in classical logic, makes use of the tertium non datur. In the right-hand column we indicate the rule and the preceding lines that justify the step taken in each line.

Line Number	*Assumptions*	*Assertion*	*Rule Used*
1	$\neg\neg$ H	$\neg\neg$ H	introduction of assumption
2	$\neg$ H	$\neg$ H	introduction of assumption
3	$\neg\neg$ H, $\neg$ H	H	$\neg$-elimination (2, 1)
4	$\neg\neg$ H	$\neg$ H $\rightarrow$ H	elimination of assumption (3)
5	H	H	introduction of assumption
6		H $\rightarrow$ H	elimination of assumption (5)
7		H $\vee \neg$ H	tertium non datur
8	$\neg\neg$ H	H	$\vee$-elimination (7, 6, 4)

Since we have used only rules from the propositional calculus, there has been no need to flag variables.

In the same way we can prove the four rules of contraposition, by which we mean the following steps: (1) from H $\rightarrow \Theta$ to $\neg \Theta \rightarrow \neg$ H, (2) from H $\rightarrow \neg \Theta$ to $\Theta \rightarrow \neg$ H, (3) from $\neg$ H $\rightarrow \Theta$ to $\neg \Theta \rightarrow$ H, (4) from $\neg$ H $\rightarrow \neg \Theta$ to $\Theta \rightarrow$ H.[22]

As a second example (see page 48) we wish to give part of an indirect proof and choose for this purpose the proof of the irrationality of $\sqrt{2}$. We use the variables $p, q, r, s, t, u, x, y, z$ for positive integers and take advantage of the fact that a rational number can be represented as the quotient of two natural numbers which have no factor in common and thus, in particular, are not both even. Then our problem is to prove the proposition

$$\neg \bigvee_p \bigvee_q (2q^2 = p^2 \wedge \neg (2 \mid p \wedge 2 \mid q)). \tag{6.2}$$

Since $2 \mid p$ is only an abbreviation for $\bigvee_s 2s = p$, we may rewrite (6.2) in the form

$$\neg \bigvee_p \bigvee_q (2q^2 = p^2 \wedge \neg (\bigvee_s 2s = p \wedge \bigvee_s 2s = q)), \tag{6.3}$$

[21] A further example is given in §11.2.

[22] The last two rules are not valid in the logic of intuitionism, which also rejects the step from $\neg\neg$ H to H.

Line Number	*Flagged Variables*	*Assumptions*	*Assertion*	*Rule Used*
1		H_0	$\bigvee_p \bigvee_q (2q^2 = p^2 \wedge \neg (\bigvee_s 2s = p \wedge \bigvee_s 2s = q))$	introduction of assumption
2	p	H_0	$\bigvee_q (2q^2 = p^2 \wedge \neg (\bigvee_s 2s = p \wedge \bigvee_s 2s = q))$	$\vee$-elimination (1)
3	$q(p)$	H_0	$2q^2 = p^2 \wedge \neg (\bigvee_s 2s = p \wedge \bigvee_s 2s = q)$	$\vee$-elimination (2)
4		H_0	$2q^2 = p^2$	$\wedge$-elimination (3)
5		H_0	$\bigvee_t 2t = p^{2(23)}$	$\vee$-introduction (4)
6		$A_1, \ldots, A_n$	$\bigwedge_u (\bigvee_t 2t = u^2 \rightarrow \bigvee_s 2s = u)$	(arithmetic)
7		$A_1, \ldots, A_n$	$\bigvee_t 2t = p^2 \rightarrow \bigvee_s 2s = p$	$\wedge$-elimination (6)
8		$H_0, A_1, \ldots, A_n$	$\bigvee_s 2s = p$	$\rightarrow$-elimination (7, 5)
9	$s(p)$	$H_0, A_1, \ldots, A_n$	$2s = p$	$\vee$-elimination (8)
10		$H_0, A_1, \ldots, A_n$	$2q^2 = p^2 \wedge 2s = p$	$\wedge$-introduction (4, 9)
11		$A_1, \ldots, A_n$	$\bigwedge_x \bigwedge_y \bigwedge_z (2x = y^2 \wedge 2z = y \rightarrow 2z = x)$	(arithmetic)
12		$A_1, \ldots, A_n$	$\bigwedge_y \bigwedge_z (2q^2 = y^2 \wedge 2z = y \rightarrow 2z^2 = q^2)^{2(24)}$	$\wedge$-elimination (11)
13		$A_1, \ldots, A_n$	$\bigwedge_z (2q^2 = p^2 \wedge 2z = p \rightarrow 2z^2 = q^2)$	$\wedge$-elimination (12)
14		$A_1, \ldots, A_n$	$2q^2 = p^2 \wedge 2s = p \rightarrow 2s^2 = q^2$	$\wedge$-elimination (13)
15		$H_0, A_1, \ldots, A_n$	$2s^2 = q^2$	$\rightarrow$-elimination (14, 10)
16		$H_0, A_1, \ldots, A_n$	$\bigvee_t 2t = q^2$	$\vee$-introduction (15)
17		$A_1, \ldots, A_n$	$\bigvee_t 2t = q^2 \rightarrow \bigvee_s 2s = q$	$\wedge$-elimination (6)
18		$H_0, A_1, \ldots, A_n$	$\bigvee_s 2s = q$	$\rightarrow$-elimination (17, 16)
19		$H_0, A_1, \ldots, A_n$	$\bigvee_s 2s = p \wedge \bigvee_s 2s = q$	$\wedge$-introduction (8, 18)
20		H_0	$\neg (\bigvee_s 2s = p \wedge \bigvee_s 2s = q)$	$\wedge$-elimination (3)
21		$H_0, A_1, \ldots, A_n$	$\neg H_0$	$\neg$-introduction (19, 20)
22		$A_1, \ldots, A_n$	$H_0 \rightarrow \neg H_0$	elimination of assumption (21)
23			$H_0 \rightarrow H_0$	elimination of assumption (1)
24		$A_1, \ldots, A_n$	H_0	$\rightarrow$-introduction (23, 22)

[23] Strictly interpreted, the rule of existence-introduction in §6.4 allows us to go from $\vee_t 2t = p^2$ to $2q^2 = p^2$ by introducing a suitable variable for the variable t. But that is not exactly what we are doing here, since we must replace t by q^2, and q^2 is not a variable. The difficulty lies in the fact that for simplicity in the above example, and for consistency with the nomenclature of ordinary mathematics, we have used the functional notation, which, in principle, we could have avoided, as we have seen in §2.5.

[24] Here we have replaced x by q^2. Cf. the preceding note.

which we shall now abbreviate to $\neg \mathsf{H}_0$. Here the axioms of arithmetic are indicated simply by $A_1, \ldots, A_n$. From $A_1, \ldots, A_n$ it follows that an arbitrary positive integer u is even if its square is even. We have made use of this fact in the second line and, strictly speaking, we should give a complete proof of it. The same remark applies to line 11, which expresses an elementary result from arithmetic.

It is easy to verify that we have now constructed a finished proof in which we have respected the restrictions against flagging the variable twice and against circularity.

From this example it is clear that proofs in the precise sense in which we are now using the word are generally much longer than the "proofs" of ordinary mathematics. This fact should cause no surprise, since we are employing only a few rules of inference of a very elementary character.

6.7. *Recursive Enumerability and Decidability in the Predicate Logic*

The calculus discussed above has provided us with a procedure (an *ars inveniendi*) for recursively enumerating the theorems of any theory that is axiomatized in the language of the predicate logic. The verification of the correctness of any proof can be carried out, at least in principle, by a machine, since we are dealing here only with simple formal relationships among rows of symbols. Thus, it is a *decidable* question whether or not a given sequence of expressions is a proof.

But it must be emphasized that such a calculus does not enable us, for an arbitrary finite system of axioms $\mathfrak{A}$ and an arbitrarily given expression H, to decide whether or not H follows from $\mathfrak{A}$. To decide such a question would require an *ars iudicandi* in the sense of Leibniz, and since 1936 it is known (Church) that for the predicate logic such a decision procedure cannot exist.

6.8. *Nonclassical Systems of Rules*

As was pointed out in §6.5, the rules given in §6.4 for the predicate logic can be established semantically. But the nonclassical conceptions of logic can lead to corresponding systems of rules that are not necessarily equivalent to the system described here. For example, the rule of *tertium non datur* is not valid for a potential interpretation of infinity (cf. §1.4).

Exercise for §6

Let the axioms for a group be given in the following form:

M (Multiplication) $\bigwedge_x \bigwedge_y \bigvee_z xy = z$

A (Associative law) $\bigwedge_x \bigwedge_y \bigwedge_z x(yz) = (xy)z$

U (Unity) $\bigwedge_x xe = z$

J (Inverse)	$\bigwedge_x \bigwedge_y xy = 0$
E_1 (Equality)	$T = T$
E_2 (Equality)	$H(T_1) \wedge T_1 = T_2 \rightarrow H(T_2)$

Here T, T_1, T_2 denote terms, e.g., ab, $(ab)c$ and so forth, and $H(T_1)$ is an arbitrary term-equation containing the term T_1. Also, E_1 and E_2 are axiom-schemes (4.1). The axiom E_2 can be represented more conveniently, and equivalently, by the additional rule of inference

$$E_2 \qquad \frac{H(T_1),\ T_1 = T_2}{H(T_2)}$$

From these axioms construct a proof for the propositional form

$$\bigwedge_a \bigvee_b ba = e$$

(existence of a left inverse).

Bibliography

The following textbooks of logic discuss the methods of proof for the predicate logic, but on the basis of rules of inference quite different from those described in the present section: Church [1], Hilbert-Ackermann [1], Kalish-Montague [1], Kleene [1], Quine [1], Quine [2], Rosenbloom [1].

7. Theory of Sets

7.1. *Introductory Remarks*

Many definitions and theorems contain such expressions as *set*, *totality*, *class*, *domain*, and so forth. For example, in the definition of a real number by means of a Dedekind cut (see IB1, §4.3) the *totality* of the rational numbers is divided into two non-empty *classes*, a first or lower and a second or upper class. An ordered *set* (cf. §7.2) is said to be well-ordered if every non-empty *subset* contains a smallest element. Again, we may visualize a real function as the *set* of points of a curve and may speak of its *domain* and *range* (§8.3). Finally, we have already spoken of a *domain* of individuals in our definition of the concept of a mathematical consequence (§3.6).

The concept of a *set*, which is thus seen to be of fundamental importance, was for a long time regarded as being so intuitively clear as to need no further discussion. Cantor (1845–1918) was the first to subject it to systematic study. His definition of a set (not a definition in the strict mathematical sense of the word but only a useful hint in the right direction) runs as follows: *A "set" is any assemblage, regarded as one entity M, of definite and separate objects m of our perception or thought.*

The Cantor theory of sets developed rapidly and soon exercised a great influence on many branches of mathematics, the theory of point sets, real functions, topology, and so forth.

But with the discovery of contradictions—the so-called *antinomies of the theory of sets* (cf. §7.2 and §11)—the foundations of the theory, and therewith of the whole of classical mathematics, were placed in jeopardy. The discussion of this problem, which is still continuing, has contributed in an essential way to the development of modern research on the foundations of mathematics. The various schools of thought have made several suggestions for the construction of a theory of sets; let us mention a few of the most important.

The *naive* or *intuitive theory of sets* simply attempts to avoid the introduction of contradictory concepts. Frege and Russell tried (logicism) to reduce the theory of sets to logic. Zermelo, von Neumann, and others have introduced systems of axioms for the theory of sets from which it is possible to deduce many of the theorems of the naive theory. The consistency of these systems of axioms remains an open question (cf. §4.7). Still other authors insist that a set must be explicitly definable by a linguistic expression (a propositional form with a free variable), which must then satisfy certain additional conditions, depending on the school of thought to which the author belongs.

In Sections 7, 8, and 9 we deal chiefly with the naive theory of sets; as for the axiomatic theory, we confine ourselves to a brief description of *one* of the various systems in use. The three sections are closely related to one another in subject matter and are separated here only for convenience.

7.2. *Naive Theory of Sets*

The Cantor definition of a set makes it natural for us to gather into one set all the entities that have a given property; for example: (1) the set of chairs in the room (these are objects of our perception), or (2) the set of even numbers (objects of our thought). To denote variables for sets and their elements we use the Latin letters a, b, c, ... M, N, ..., and so forth. To express the fact that *y is an element of x* we write $y \in x$, and for $\neg\, y \in x$ we also write $y \notin x$. It is possible for one set to be an element of another set. Sets that contain the same elements are regarded as being equal, i.e.,

$$\bigwedge_x (x \in a \leftrightarrow x \in b) \rightarrow a = b. \tag{7.1}$$

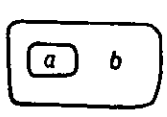
This requirement is called the *principle of extensionality*. Thus a set is determined by the elements "contained" in it, by its *content* or *extension*.

The property of being a prime number between eight and ten defines a set that contains no element. By the principle of extensionality there can

be only *one* such set, which is called the *empty set*, and is here denoted by 0, although some authors use the special symbol $\emptyset$.

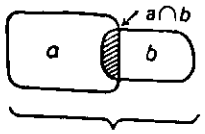
Let us now define the simplest set-theoretic concepts: A set a is called a *subset* of b (a *is contained in* b, $a \subseteq b$) if $\wedge_x (x \in a \rightarrow x \in b)$. If $a \neq b$, then a is a *proper subset* of b or is *properly contained* in $b (a \subset b)$. The set c is called the *union* of a and $b (c = a \cup b)$ if $\wedge_x (x \in c \leftrightarrow x \in a \vee x \in b)$. The set c is the *intersection* of a and $b (c = a \cap b)$ if $\wedge_x (x \in c \leftrightarrow x \in a \wedge x \in b)$. Two sets a, b are *disjoint* if they have no element in common, i.e., $a \cap b = 0$. The *complement* $\bar{x}$[25] of a set x is the set of all elements which are not elements of x. But here we must be careful, since the complement of the empty set is then the "universal set," which easily leads to contradictions (cf. §7.5). These contradictions can be avoided if we consider only subsets of a certain fixed set M. Then $\bar{x}$ is the set of y with $y \in M \wedge y \notin x$.

It is convenient to illustrate these concepts with sets of points in the plane:



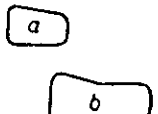
$a \subset b$

Fig. 1



$a \cup b$

Fig. 2



a and b disjoint

Fig. 3

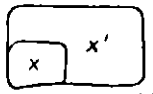


Fig. 4

By the *power set* $\mathfrak{P}a$ of a set a we mean the set of all subsets of a: $\wedge_x (x \in \mathfrak{P}a \leftrightarrow x \subseteq a)$. The set that contains x as its single element is written $\{x\}$,[26] and correspondingly $\{x, y\}$ is the set containing exactly the two elements x and y, and so forth. For example, $\{0\}$ contains exactly one element, namely the empty set, whereas 0 contains no element at all. In a set-theoretic treatment of functions (cf. §8) an important role is played by the *ordered pairs* $\langle x, y \rangle$,[27] defined by

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}. \tag{7.2}$$

From $\langle x, y \rangle = \langle u, v \rangle$ follows $x = u \wedge y = v$. Thus the order of the components in an ordered pair is significant.[28]

[25] The complement of x is often denoted by "x'."

[26] $\{x\}$ and x differ from each other, since in general x does not have x as its only element. Nevertheless, in cases where no confusion can arise, it is customary to write x for $\{x\}$.

[27] Ordered pairs are also denoted by (x, y).

[28] For sequences of symbols the construction of ordered pairs may be carried out simply by means of juxtaposition and a suitable symbol for separation.

It is easy to prove the following rules, which lead us to speak of an *algebra of sets* (cf. §9) or of a *field of sets*.

Laws for $\cap$ *and* $\cup$:

(1) *The commutative laws:*

$$a \cap b = b \cap a, \qquad a \cup b = b \cup a.$$

(2) *The associative laws:*

$$a \cap (b \cap c) = (a \cap b) \cap c, \qquad a \cup (b \cup c) = (a \cup b) \cup c.$$

(3) *The absorption laws:*

$$a \cap (a \cup b) = a, \qquad a \cup (a \cap b) = a.$$

(4) *The distributive laws:*

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c),$$
$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

Laws for $\subseteq$:

(1) *The reflexive law:*

$$a \subseteq a.$$

(2) *The identitive law:*

$$a \subseteq b \wedge b \subseteq a \rightarrow a = b.$$

(3) *The transitive law:*

$$a \subseteq b \wedge b \subseteq c \rightarrow a \subseteq c.$$

Thus, the relation $\subseteq$ is a partial ordering (in the sense of §8.3).

Laws for $\subseteq$, $\cap$, $\cup$:

(1) $a \subseteq b \leftrightarrow a \cap b = a, \qquad a \subseteq b \leftrightarrow b \cup a = b,$

(2) $a \subseteq b \cap c \leftrightarrow a \subseteq b \wedge a \subseteq c, \qquad a \cup b \subseteq c \leftrightarrow a \subseteq c \wedge b \subseteq c.$

Laws for complementation (a, b are subsets of m):

(1) $a = b \leftrightarrow \bar{a} = \bar{b}$, (2) $\overline{(\bar{a})} = a$,

(3) $a \subseteq \bar{b} \leftrightarrow \bar{b} \subseteq \bar{a}$, (4) $\bar{0} = m, \quad \bar{m} = 0$,

(5) $\overline{(a \cap b)} = \bar{a} \cup \bar{b}, \qquad \overline{(a \cup b)} = \bar{a} \cap \bar{b}$,

(6) $a \subseteq b \leftrightarrow a \cap \bar{b} = 0, \qquad a \subseteq b \leftrightarrow \bar{a} \cup b = m.$

Laws for 0 *and* m (a is a subset of m):

(1) $a \cup 0 = a, \qquad a \cap m = a,$

(2) $a \cap 0 = 0, \qquad a \cup m = m.$

Up to now we have introduced the concept of union for two sets only, but it is often necessary to consider the union of arbitrarily many sets. Let M be a set of sets. Then by $\bigcup_{x \in M} x$ we denote the set of elements y belonging to at least one x in M. Correspondingly, as a generalization of the intersection of two sets, we write $\bigcap_{x \in M} x$ for the set of those elements of y which belong to every x in M.

7.3. *Cardinal Numbers in the Naive Theory of Sets*

One of the most important concepts introduced by Cantor is that of the *power* or *cardinality* of a set. It represents an extension to infinite sets of the number of objects in a finite set. Two sets x, y are said to be *equivalent* ($x \sim y$) if a one-to-one correspondence can be set up between the elements of x and those of y. For example, the set $\{1, 2, 3\}$ and $\{0, \{0\}, \{\{0\}\}\}$ are equivalent; moreover, the set of natural numbers and the set of squares are equivalent, as is shown by the following correspondence between them:

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 4 & 9 & 16 & \ldots . \end{array}$$

This example shows that an "infinite" set a can be equivalent to a proper part of itself, a property which is usually taken as the definition of infinity *(Dedekind definition of infinity)*. The *cardinal number* $\tilde{x}$[29] of a set x is then regarded as representing "that which is common" to all sets that are equivalent to x. Thus, we might say that the cardinal number of x is simply the set of all sets that are equivalent to x, although such a definition is problematical on account of its relationship to the universal set. On the other hand, among all the sets that are equivalent to x we could choose one definite set as a representative of x and then say that this set is the cardinal number of x. But the problematical feature of such a definition is that we do not know how to decide which set should be chosen as the representative. In any case we have

$$x \sim y \Leftrightarrow \tilde{x} = \tilde{y}. \tag{7.3}$$

The cardinal number of a finite set can simply be identified with the number of elements in the set.

For all sets, finite or infinite, we have the *Bernstein equivalence theorem:*

$$\text{If} \quad x \subseteq y \quad \text{and} \quad y \subseteq z \quad \text{and} \quad x \sim z, \quad \text{then} \quad y \sim z.$$

An ordering $\leqslant$ for the cardinal numbers (cf. §8.3) can be defined by setting $\tilde{x} \leqslant \tilde{z} \Leftrightarrow \mathsf{V}_y (y \subseteq z \wedge x \sim y)$, $\tilde{x} < \tilde{z} \Leftrightarrow \tilde{x} \leqslant \tilde{z} \wedge \tilde{x} \neq \tilde{z}$ (cf. §7.4).

[29] Cardinal numbers are also often denoted by "$\bar{x}$."

The cardinal number of the set of natural numbers is denoted by $\aleph_0$ (pronounced aleph-zero). If $\bar{x} < \aleph_0$, the cardinal number $\bar{x}$ is said to be *finite*, but if $\bar{x} \geqslant \aleph_0$, then $\bar{x}$ is *transfinite*. If $\bar{x} = \aleph_0$, then $\bar{x}$ is *countable*, and if $\bar{x} \leqslant \aleph_0$, then $\bar{x}$ is *at most countable*.[30] A transfinite cardinal number that is not countable is said to be *uncountable*. A set is called *countable*, *at most countable*, or *uncountable* if its cardinal number has the corresponding property. Finite cardinal numbers correspond to finite sets, and transfinite cardinal numbers to infinite sets.

The set of rational numbers is countable. The truth of this assertion is evident from the following *schema* in which every "positive" rational number occurs at least once *(first Cantor diagonal procedure):*

$$
\begin{array}{l}
0 \to 1 \quad 2 \to 3 \quad 4 \to 5 \cdots \\
\quad\ \downarrow \\
\quad\ \tfrac{1}{2} \nearrow \tfrac{2}{2} \swarrow \tfrac{3}{2} \nearrow \tfrac{4}{2} \swarrow \tfrac{5}{2} \cdots \\
\\
\quad\ \tfrac{1}{3} \swarrow \tfrac{2}{3} \nearrow \tfrac{3}{3} \swarrow \tfrac{4}{3} \quad \tfrac{5}{3} \cdots \\
\quad\ \downarrow \\
\quad\ \tfrac{1}{4} \nearrow \tfrac{2}{4} \swarrow \tfrac{3}{4} \quad \tfrac{4}{4} \quad \tfrac{5}{4} \cdots \\
\quad\quad \swarrow \\
\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ \cdots .
\end{array}
$$

The existence of uncountable sets was first proved by Cantor by his *second diagonal procedure: the set of real numbers* α with $0 < \alpha < 1$ is uncountable. Proof: let us assume that we have set up a one-to-one correspondence between these numbers and the positive integers:

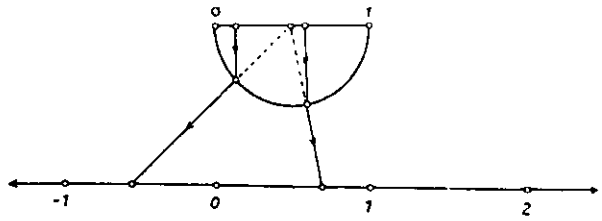
$$
\begin{aligned}
\alpha_1 &= 0.\, a_{11}a_{12}a_{13} \cdots \\
\alpha_2 &= 0.\, a_{21}a_{22}a_{23} \cdots \\
\alpha_3 &= 0.\, a_{31}a_{32}a_{33} \cdots \\
&\ . \ . \ . \ . \ . \ . \ . \ . \ . \ .
\end{aligned}
$$

Here the real numbers have been written as infinite decimals, so that $0 \leqslant a_{ik} \leqslant 9$. Now let us form the number $\alpha' = 0, a_1'a_2'a_3' \ldots$, where $a_i' = 1$ if $a_{ii} \neq 1$, and $a_i' = 2$ if $a_{ii} = 1$. Then α' differs from every number listed above in at least one decimal place, since it differs from α_n in the nth place, and thus α' is not included in the list. Since $0 < \alpha' < 1$, our assumption is wrong and the theorem is proved.

The correspondence set up in Figure 5 shows that the set of all real numbers, often called the *continuum*, has the same power as the set of real numbers in the interval just considered.

[30] The terms *countable* and *countably infinite* are often used in the sense of our "at most countable" and "countable," respectively.

Fig. 5



7.4. *Ordinal Numbers in the Naive Theory of Sets*

A set x for which an order (cf. §8) has been defined is called an *ordered set*. Two ordered sets that can be put into one-to-one correspondence with each other with preservation of the order (so that they are isomorphic in the sense of §8.4) are said to be *similar*. By the *order type* $|x|$ we mean "that which is common" to all sets similar to the given ordered set x (cf. the remarks on the concept of a cardinal number in §7.3). If the ordering of x is a well-ordering in the sense of §8.3, then $|x|$ is an *ordinal number*. For the ordinal numbers we can define an ordering $<$, which turns out to be a well-ordering, by setting $|x| < |y| \Leftrightarrow \mathsf{V}_z(z \subset y \wedge |x| = |z|) \wedge |x| \neq |y|$. For every ordinal number β the set of ordinal numbers with $\alpha < \beta$ in the ordering $<$ is itself a representative of β. The *well-ordering theorem*, which can be proved on the basis of the axiom of choice (cf. §7.6), states that *every set can be well-ordered*. Only by means of this theorem can we prove that the relation $\leqslant$ defined for the cardinal numbers in §7.3 is an ordering and in fact a well-ordering.

A non-empty set S of ordinal numbers is called a *number class* if (1) any two members of the set are equivalent (§7.3), and (2) every ordinal that is equivalent to S belongs to S. Thus, every cardinal number determines a number class. To every finite cardinal number corresponds exactly one ordinal number, so that the corresponding class has only one element. But the number classes corresponding to transfinite cardinal numbers have infinitely many elements.

The natural numbers can be identified with the finite ordinal numbers, or also with the finite cardinal numbers. Then the empty set 0 corresponds to the number 0, the class of sets with a single element to the number 1, and so forth. The cardinal number of the set $\{0, \ldots, n-1\}$ is n. In this way we can construct a theory of natural numbers on the basis of the theory of sets; and in particular, we obtain a model for the Peano axioms (cf. §10).

If to a representative a of a given ordinal number we adjoin another element x, which thus becomes the "last" element in the sense of the ordering, the set $b = a \cup \{x\}$ thus created represents an ordinal number $|b|$, which is called the *successor* of $|a|$ and is denoted by $|a|'$. Thus there is no ordinal number between $|a|$ and $|a|'$. Ordinal numbers (except 0) which, unlike $|b|$, have no immediate predecessor are called *limit numbers*.

Every non-empty set of ordinal numbers contains a smallest element (since the ordinal numbers are well-ordered). Thus we may state the principle of *transfinite induction* [a generalization of induction for the natural numbers (cf. §10.2)]: if w is a well-ordering for a set a, then a property H holds for all $x \in a$ if it satisfies the following conditions:

(1) H holds for the w-smallest element of a.

(2) If H holds for all x that are w-smaller than $y (y \in a)$, then H also holds for y.

The ordinal number of the set of natural numbers, well-ordered in the usual way, is denoted by ω, which is thus the smallest transfinite ordinal number. For a general discussion of the transfinite ordinal numbers, cf. IB1, Appendix.

Functions whose domain is a transfinite set of ordinal numbers are often defined inductively by means of three conditions; for example, as follows (α, β are arbitrary ordinal numbers, λ is an arbitrary limit number and $\lim_{\beta\in\lambda} f(\alpha, \beta)$ is the smallest ordinal number γ with $f(\alpha, \beta) \in \gamma$ for all $\beta \in \lambda$):

$$(1) \quad f(\alpha, 0) = \alpha,$$
$$(2) \quad f(\alpha, \beta') = f(\alpha, \beta)',$$
$$(3) \quad f(\alpha, \lambda) = \lim_{\beta\in\lambda} f(\alpha, \beta).$$

This is not an explicit definition, since in (2) and (3) the symbol "f" to be defined occurs on the right-hand side, but by transfinite induction we can show that there exists exactly one function f with the properties (1), (2), (3), and then we can write $\alpha + \beta$ for $f(\alpha, \beta)$. A schema of the form (1), (2), (3) is called a *transfinite inductive definition*. If condition (3) is omitted, the result is a recursive definition, for functions whose arguments are natural numbers. For the justification of such a recursive definition we need only the usual *complete induction* (cf. §10.2).

7.5. *Antinomies in the Naive Theory of Sets*

It is easy to show that the power set of any set x has a greater cardinal number than x itself: $\tilde{x} < \widetilde{\mathfrak{P}x}$. For finite sets x we have $\widetilde{\mathfrak{P}x} = 2^{\tilde{x}}$, which leads us to write $2^{\tilde{x}}$ for $\widetilde{\mathfrak{P}x}$ in the case of infinite sets as well. The power of the continuum is $2^{\aleph_0}$. If we form the set A of all sets (the so-called *universal set*), we first of all have $\tilde{A} < \widetilde{\mathfrak{P}A}$. On the other hand $\mathfrak{P}A$ is certainly equivalent to a subset of A, in view of the definition of A; thus $\widetilde{\mathfrak{P}A} \leqslant \tilde{A}$, in contradiction to the fact that $\leqslant$ is an ordering. This is the *antinomy of the universal set*.

Another example of a contradictory concept is the *set Ω of all ordinal numbers (antinomy of Burali-Forti)*. Like every set of ordinal numbers,

this set is well-ordered by $<$, and thus it has an ordinal number $|\Omega|$. By the definition of a successor we have $|\Omega| < |\Omega|'$, but by the definition of Ω we also have $|\Omega|' \leqslant |\Omega|$, in contradiction to the fact that $<$ is a well-ordering.

These examples show that caution must be exercised in the formation of sets. (Cf. also the Russell antinomy in §11.)

7.6. *Axiomatic Theory of Sets*

The antinomies of the naive-set theory mostly arise from the fact that *arbitrary* properties, described by propositional forms $\mathsf{H}(x)$, are admitted for the definition of sets. Thus the trouble arises from assuming that for every propositional form $\mathsf{H}(x)$ there exists a set a described by the axiom schema $\bigwedge_x (x \in a \leftrightarrow \mathsf{H}(x))$. In the axiomatization of von Neumann, Bernays, and others, to which we now turn, this axiom scheme (axiom of comprehension) is suitably restricted.

The system deals with objects $x, y, z, \ldots$, called *classes*, between which a two-place relation $\in$ can exist. Thus $x \in y$ is read: *class x is an element of class y*. There is no formal distinction between classes and elements. Certain classes are called *sets:* namely those which are elements of at least one class

$$Mx \Leftrightarrow \bigvee_u x \in u. \tag{7.4}$$

Our first task is to define *equality* of classes. It is clear that two classes may be regarded as identical if (1) they contain the same elements and if (2) whenever either one of them is an element of a class, the other is an element of the same class.

$$a = b \Leftrightarrow \bigwedge_x (x \in a \leftrightarrow x \in b) \wedge \bigwedge_x (a \in x \leftrightarrow b \in x). \tag{7.5}$$

For our first axiom we may take the principle of extensionality (7.1) from the naive theory of sets:

$$\bigwedge_x (x \in a \leftrightarrow x \in b) \rightarrow a = b. \tag{7.6}$$

Thus a class is completely determined by its elements.

Now let $\mathsf{H}(x)$ be a relevant propositional form (see §4.5); for example, $x = x$ or $x \in y \vee x \in z$. The restricted *axiom of comprehension* is

$$\bigwedge_x (\mathsf{H}(x) \rightarrow Mx) \rightarrow \bigvee_u \bigwedge_x (x \in u \leftrightarrow \mathsf{H}(x)), \tag{7.7}$$

where $\mathsf{H}(x)$ does not contain u as a free variable.

Thus a property $\mathsf{H}(x)$ can be used as the definition of a class only if it refers exclusively to sets, that is to classes which can be an element of

some class [cf. also (7.9)]. Then the class defined by $\mathsf{H}(x)$ is uniquely determined by (7.6) and can be given a name appropriate to its definition.

Let us now try to prove, for example, the Russell antinomy (see §11) by setting $x \notin x$ for $\mathsf{H}(x)$, so that from (7.7) we obtain

$$\bigwedge_x (x \notin x \to Mx) \to \bigvee_u \bigwedge_x (x \in u \leftrightarrow x \notin x).$$

In particular, for $x = u$

$$\bigwedge_x (x \notin x \to Mx) \to \bigvee_u (u \in u \leftrightarrow u \notin u). \tag{7.8}$$

The right-hand side is obviously false, and therefore, by *logical rules* the left-hand side is also false. Thus $\neg \bigwedge_x (x \notin x \to Mx)$, and consequently

$$\bigvee_x (x \notin x \wedge \neg Mx). \tag{7.9}$$

Instead of a contradiction we have obtained the (acceptable) proposition that there exists a class x (with $x \notin x$) which is not a set.

Let us now examine certain properties to see whether they are suitable for the definition of a class.

(1) Mx for $\mathsf{H}(x)$. The premiss for (7.7) then reads $\bigwedge_x (Mx \to Mx)$ and thus is satisfied. Consequently, there exists a class A which includes *all sets* and which we therefore call the *universal class:*

$$x \in A \Leftrightarrow Mx. \tag{7.10}$$

(2) $x = x$ for $\mathsf{H}(x)$. Because of $\bigwedge_x x = x$, the proposition $\bigwedge_x (x = x \to Mx)$ would then lead to $\bigwedge_x Mx$, which contradicts (7.9). Thus there is no class that includes all *classes* as its elements, and in this way we have avoided the antinomy of the universal set.

(3) $x \neq x$ for $\mathsf{H}(x)$. This expression is always false, so that we always have $\mathsf{H}(x) \to Mx$. Thus $x \neq x$ defines a class which obviously contains no element: it is the empty class 0.

(4) $x \in y \vee x \in z$ for $\mathsf{H}(x)$. Here Mx follows from $x \in y$ and also from $x \in z$, so that the premiss of (7.7) is satisfied. Thus $\mathsf{H}(x)$ defines a class that depends only on y and z, namely their *union* $y \cup z$.

Other classes can now be defined as in the naive theory of sets; for example, the *intersection* $a \cap b$ of two sets a and b, the class containing one element $\{a\}$, and the class of pairs $\{a, b\}$ and $\langle a, b\rangle$. The theorems in the algebra of classes can then be proved in the same way as in the naive theory of sets and, to a great extent, the theory of cardinal and ordinal numbers can be developed analogously. For this purpose we must introduce step by step the following axioms, which for the most part require that certain classes shall be sets.

The axiom for the empty set: $M0$.

The axiom for sets with one element: $Mx \to M\{x\}$.

The first axiom for unions: $Mx \wedge My \to M(x \cup y)$.

The axiom of infinity: MNz (*where* Nz is the class of natural numbers).

The second axiom for unions: $Mx \to M \bigcup x$ ($\bigcup x$ is the union of all the elements of x).

The replacement axiom: If the domain of a function (8.3) is a set, then its range is also a set. This axiom enables us to prove that for every set a there exists a *power class* $\mathfrak{P}a$.

The power set axiom: $Mx \to M\mathfrak{P}x$.

The axiom of choice: If a is a class of non-empty sets x, there exists a function (§8.3) f such that $f(x) \in x$ for all $x \in a$. (Thus from every set $x \in a$ the function f "chooses" an element $f(x)$.) Here also the axiom of choice is an essential instrument in the proof of the well-ordering theorem.

The continuum hypothesis: Between the cardinal number of an infinite set x and the cardinal number of its power set $\mathfrak{P}x$ there is no other cardinal number. The particular case $\tilde{x} = \aleph_0$ is the *special continuum hypothesis*. From the special hypothesis it follows that every uncountable subset of the set of real numbers has the power of the continuum.

7.7. *Independence of the Axiom of Choice and the Continuum Hypothesis*

In §4.7 we have mentioned the Gödel proof of relative consistency. Gödel's result can be formulated as follows: let $\mathfrak{A}$ be the system of axioms for set theory as stated just above (§7.6), but without the axiom of choice A and the continuum hypothesis K. Let it be assumed that $\mathfrak{A}$ is consistent (although it is still unknown today whether this assumption is true). Then $-A$ cannot be deduced from $\mathfrak{A}$ nor K from $\mathfrak{A} \cup \{A\}$.

In 1963 Cohen proved further that (if $\mathfrak{A}$ is consistent) it is also impossible to deduce A from $\mathfrak{A}$ or K from $\mathfrak{A} \cup \{A\}$. Thus we have shown (see also §4.4) that A is independent of $\mathfrak{A}$ and K is independent of $\mathfrak{A} \cup \{A\}$.

7.8. *Symbols for Sets*

If we are given a propositional form $\cdots x \cdots$, it is convenient to have a symbol for the set of those x which possess the property corresponding to this propositional form. Several notations are customary in the literature:

$$\hat{x}(\cdots x \cdots), \qquad \{x;\ \cdots x \cdots\}, \qquad \{x \mid \cdots x \cdots\},$$

all of which are read: the set of x with the property $\cdots x \cdots$ Let us note that the set in question could be denoted just as well by $\hat{y}(\cdots y \cdots)$; in other words, we are dealing here with a bound variable (cf. §2.6).

Exercises for §7

1. Let (n) be the set of rational integers divisible by n. Illustrate the sets (3), (6), (9), (15) by point sets in the plane (as in figures 1–4) in such a way that the proper inclusions are correctly represented. What is the number-theoretic significance of the various intersections and unions?

2. Show by dual representations that the set of real numbers x with $0 < x < 1$ has the same power as the set of points $\langle x, y\rangle$ of the square $(0 < x < 1;\ 0 < y < 1)$.

3. Let x' be defined by $xu\{x\}$ (cf. 7.4); also let

$$(*)\ n \in N \Leftrightarrow \bigwedge_x [(0 \in x \,.(r \in x \to r' \in x)) \to n \in x].$$

Assume the principle of extensionality, the restricted axiom of comprehension, the axiom of the empty set, the axiom for sets with one element, and the first axiom for unions.

Prove:

(a) The right-hand side of (*) defines a class N.

(b) $0 \in N$

(c) $0' \in N$

(d) $\bigwedge_x (x \in N \to x' \in N)$

(e) $\bigwedge_x (x' \in N \to x \in N)$

(*f*) $\bigwedge_x (x' \in N \to 0 \in x')$

Bibliography

Relatively elementary is Kleene [1]. Let us also mention Bernays [1], Fraenkel [1], Fraenkel and Bar-Hillel [1], Halmos [1], Sierpiński [1] and Suppes [1].

8. Theory of Relations

8.1. *The Concept of a Relation*

We may consider *relations* as properties of ordered pairs (§7.2). For example, $3 < 4$ (3 stands in the $<$-relation to 4) states that the property "smaller than" holds for the ordered pair $\langle 3, 4\rangle$. Or: *the point A lies on the line g* states that the pair $\langle A, g\rangle$ has the property described by the predicate *lies on*.

Analogously, we may regard an *n-place relation* as a property of ordered n-tuples. For example, the expression $x + y = z$ defines a three-place relation for the natural numbers. Except when otherwise noted, we shall always take the word *relation* to mean a two-place relation.

Relations have the same fundamental importance in mathematics as sets. Many of the basic concepts of mathematics are to be defined by relations (e.g., function, congruence, order) or at least can be understood in terms of relations (e.g., group, lattice, factor group, cf. §8.5).

For simplicity we here take the naive point of view (cf. §7.1), so that relations may simply be regarded as *sets of ordered pairs*. Thus instead of saying: x is in the relation r to y (abbreviated xry), we can equally well say: the ordered pair $\langle x, y\rangle$ is an element of the set r:

(8.1) $$xry \Leftrightarrow \langle x, y\rangle \in r.$$

The elements of the pairs are assumed to belong to a fixed *ground set* M in which the relations are defined, and $r, s, t, f, g, h, \ldots$ are variables for them. For example, if M is the set Nz of natural numbers, then $\langle m, n\rangle$ belongs to the relation $\leqslant$ if and only if $m \leqslant n$. Thus $\leqslant$ consists of the pairs $\langle 0, 0\rangle$, $\langle 0, 1\rangle$, ..., $\langle 1, 1\rangle$, $\langle 1, 2\rangle$, ... and so forth. By the *first domain* $\theta_1(r)$ of a relation r we mean the set defined by $\bigvee_y xry$, and by the *second domain* $\theta_2(r)$ we mean the set defined by $\bigvee_y yrx$. For example, $\theta_1(<) = \{0, 1, 2, \ldots\}$, $\theta_2(<) = \{1, 2, 3, \ldots\}$. The set $\theta_1(r) \cup \theta_2(r)$ is called the *domain* of the relation r.

An important relation is the *identity* I, defined by $xIy \Leftrightarrow x = y$. For the class of natural numbers it consists of the pairs $\langle 0, 0\rangle$, $\langle 1, 1\rangle$, and so forth. The *empty* or *void* relation, which contains no pair at all, will be denoted here by $\hat{0}$. It is identical with the empty set 0 (§7.2). The *universal relation*, which contains *every* pair with elements from M, will be denoted by $\hat{1}$. It is to be distinguished from the "universal set." Obviously we have $\bigwedge_x \bigwedge_y \neg\, x\hat{0}y$, $\bigwedge_x \bigwedge_y x\hat{1}y$.

8.2. *Combination of Relations (Algebra of Relations)*

Since the relations are defined as sets, it is clear what we mean by the *intersection* $r \cap s$, the *union* $r \cup s$, and the *complement* $\bar{r}$:

(8.2) $$x(r \cap s)\, y \Leftrightarrow xry \wedge xsy, \qquad x(r \cup s)\, y \Leftrightarrow xry \vee xsy,$$
$$x\bar{r}y \Leftrightarrow \neg\, xry.$$

Similarly, the *inclusion* $r \subseteq s$ is defined by $\bigwedge_x \bigwedge_y (xry \rightarrow xsy)$.

In addition to these purely set-theoretic constructions, there are two other important ways of combining relations: the *converse relation* $\breve{r}$ and the *relative product* rs. The *converse relation* is defined by:

(8.3) $$x\breve{r}y \Leftrightarrow yrx.$$

Thus the *converse* $\breve{r}$ of r arises from r through "reversal" of all the pairs.

The *relative product* is defined by:

$$x(rs)\,y \Leftrightarrow \bigvee_z (xrz \wedge zsy). \tag{8.4}$$

Thus the *relative product* rs of r and s arises, roughly speaking, from "juxtaposition" of r and s. As may be shown by simple examples, this operation is not commutative. For rr it is customary to write r^2. Thus, if M is the class of natural numbers, we have: $I \subset \leqslant$, $< \cap I = 0$, $rI = Ir = r$ for every r, $\breve{<} = >$, $I^2 = I$. A set of relations which is closed (cf. IB10, §2.2) with respect to all these operations is called a *field of relations*. For computation with relations we have the same rules as for the algebra of sets (§7.2), and also certain other rules, which are easily proved directly from the definitions; for example,

$$\begin{gathered}(r \cap s)\breve{} = \breve{r} \cap \breve{s}, \qquad (r \cup s)\breve{} = \breve{r} \cup \breve{s}, \qquad \breve{\breve{r}} = r, \qquad \overline{(\breve{r})} = (\bar{r})\breve{}, \\ r(s \cup t) = (rs) \cup (rt), \qquad r(s \cap t) \subseteq (rs) \cap (rt).\end{gathered} \tag{8.5}$$

8.3. *Special Properties of Relations*

A relation r is *symmetric* if $\wedge_x \wedge_y (xry \rightarrow yrx)$, a requirement which by (8.3) may also be written in the shorter form $r \subseteq \breve{r}$. Definitions like this last one, which make no reference to the elements of the ground set, are often more concise. In what follows we shall give the definitions, wherever possible, in both forms, leaving to the reader the task of proving that they are equivalent. In the examples, M is the class of natural numbers, unless otherwise noted.

If xrx for all x, the relation r is *reflexive* ($I \subseteq r$). Example: $x \geqslant y$.

A *transitive* relation is defined by $\wedge_x \wedge_y \wedge_z ((xry \wedge yrz) \rightarrow xrz)$. (Alternatively written $r^2 \subseteq r$.) Example: $x < y$.

A relation is *identitive* if $\wedge_x \wedge_y ((xry \wedge yrx) \rightarrow x = y)$. (In the shorter form, $r \cap \breve{r} \subseteq I$.) Example: x is a factor of y.

A relation is *connex* if $\wedge_x \wedge_y (xry \vee yrx)$. (In the shorter form, $r \cup \breve{r} = \mathrm{i}$.) Example: $x \leqslant y$.

Relations which are transitive, identitive, and connex are called *orderings in the sense of* $\leqslant$ (example: $x \leqslant y$). For *orderings in the sense of* $<$ the requirements of identitivity and connexity are replaced by $\wedge_x \neg xrx$ and $\wedge_x \wedge_y (x \neq y \rightarrow xry \vee yrx)$ (example: $x < y$).

If we discard connexity altogether, we obtain the so-called *partial orderings* (*in the sense of* $\leqslant$ *or in the sense of* $<$), which are sometimes called *semi-orderings*. Examples are: inclusion, and strict inclusion (cf. §7.2), for the set of all subsets of a given set. In more recent literature, partial orderings in the above sense are sometimes called orderings, and orderings are called total or complete orderings.

If an ordering $<$ contains no infinite "decreasing" sequence $\cdots < x_3 < x_2 < x_1$ $(x_{i+1} \neq x_i)$, it is called a *well-ordering* (of M), where a distinction is to be made between well-orderings in the sense of $<$ and well-orderings in the sense of $\leqslant$. Thus an ordering is a well-ordering if and only if every non-empty subset M_1 of its field has a *minimal element* in the sense of the ordering, i.e., an element for which there is no smaller element in M_1. By discarding the requirement of connexity, we obtain the *partial well-orderings*.

A set M is said to be *directed* with respect to a relation r if r is transitive and if for every $x, y \in M$ there exists a $z \in M$ such that xrz and yrz.

8.4. *Functions*

An important class of relations consists of the *functions*, defined by the requirement of uniqueness $\wedge_x \wedge_y \wedge_z ((xry \wedge xrz) \rightarrow y = z)$. (In the shorter form, $\breve{r}r \subseteq I$.) For functions it is customary to write $f(x) = y$ in place of xfy. The function f is a *mapping* of the first domain $\theta_1(f)$ *onto* the second domain $\theta_2(f)$; if $\theta_2(f)$ is contained in a set A, we say that f is a mapping *into* A. If $(f)x = y$, we say that y is the *image* of x (under f) and that x is the *pre-image* of y. If $\breve{f}$ is also a function (that is, $\breve{f}f \subseteq I$), then f is a one-to-one (*invertible*) mapping of $\theta_1(f)$ onto $\theta_2(f)$, and $\breve{f}$ is called the *inverse function* of f. Functions whose domain is the set of natural numbers are also called *sequences*. On the basis of the definition (7.1) for equality of sets, two functions are equal (or *identical*) if they have the same domain and if for every element in that domain the two functions have the same values.

As an example, let us formulate the Dedekind definition of an infinite set (§7.3) in the language of the theory of relations:

$$\text{Infinite} \quad a \Leftrightarrow \bigvee_f (\breve{f}f \subseteq I \wedge f\breve{f} \subseteq I \wedge \theta_1(f) = a \wedge \theta_2(f) \subset a).$$

In words: There exists a one-to-one mapping of a onto a proper subset of a.

Two relations r, s are said to be *isomorphic* if there exists a one-to-one mapping f of their fields onto each other such that $\wedge_x \wedge_y (xry \leftrightarrow f(x)\, sf(y))$.

In mathematical literature a function f is often written in the form $f(x)$, but this notation is essentially incorrect, since it appears to mean that the variable x is free. If we wish to use the variable x as part of the notation for a function, we must indicate that this variable is bound. Acceptable notations are $\lambda x f(x)$ or $x \rightarrow f(x)$[1].[31]

[31] The second of these is more common in recent literature, but it is to be noted that the arrow here has nothing to do with the symbol for implication in §2.4.

8.5. *Equivalence and Congruence Relations*

Relations which are symmetric, reflexive, and transitive are called *equivalence relations* (e.g., the identity I), cf. §4.4. They play an important role in mathematics, especially in algebra.

If we assume reflexivity, we may replace the requirement of transitivity and symmetry by that of *comparativity*: $x \sim z \wedge y \sim z \to x \sim y$.

Let $\sim$ be an equivalence relation in M, and let $\tilde{z}$ denote the set defined by $x \in \tilde{z} \Leftrightarrow x \sim z$. This set is called the *equivalence class* generated by z or corresponding to z. We have

$$z \in \tilde{z}, \tag{8.6}$$

$$(x \in \tilde{z} \wedge y \in \tilde{z}) \to x \sim y, \tag{8.7}$$

$$(u \in \tilde{x} \wedge u \in \tilde{y}) \to \tilde{x} = \tilde{y}. \tag{8.8}$$

All the elements of an equivalence class are thus equivalent to one another, i.e., they are related by $\sim$. Two equivalence classes are either identical or without common element, so that every equivalence relation generates a partition of its field M into disjoint classes. Conversely, every such partition of M into classes generates an equivalence relation in M; for if M is the union of disjoint subclasses, we define: $x \sim y \Leftrightarrow (x$ and y lie in the same subclass).

An equivalence relation defined in a ground set M gives rise to a *process of abstraction* (cf. §1.2), which means that elements of the same equivalence class are regarded as indistinguishable; in other words, we abstract from their distinguishing features. Conversely, every process of abstraction in M gives rise to an equivalence relation in the field M.

If for a ground set M there are given finitely many k-place functions $f_1, \ldots, f_n$ with values in M, then $\langle M, f_1, \ldots, f_n \rangle$ is called an *abstract algebra* (cf. IB10, §1.2). For example, let there be given a two-place function f, whose value for the arguments x, y we shall write in the form $x \cdot y$. Then it is clear that we shall usually be interested in those abstractions that preserve the operation $x \cdot y$; that is, if we denote the new equality by $\sim$, we must be able to define $\tilde{x} \cdot \tilde{y}$ as $\widetilde{x \cdot y}$. This will be possible if

$$\bigwedge_{x_1} \bigwedge_{x_2} \bigwedge_{y_1} \bigwedge_{y_2} ((x_1 \sim x_2 \wedge y_1 \sim y_2) \to x_1 \cdot y_1 \sim x_2 \cdot y_2). \tag{8.9}$$

In this case the equivalence relation $\sim$ is called a *congruence relation* (with respect to the operation $x \cdot y$). The situation can also be described in the following way: a congruence relation is an equivalence relation that is *consistent* with the operations of the abstract algebra. For example, in the ring of rational integers, $x \equiv y \pmod 6$ is a congruence with respect to addition and multiplication (cf. IB6, §4.1).

If the algebra has a unit element e such that $\Lambda_x (x \cdot e = x)$, then the set of x with $x \sim e$ forms a subalgebra N, since from $x \sim e$, $y \sim e$ it follows that $x \cdot y \sim e \cdot e = e$. Let $x \cdot N$ be the set of products of x with arbitrary elements of N. For every x we have $x \cdot N \subseteq \tilde{x}$. The congruence classes (complete classes of mutually congruent elements) form an algebra of the same "type." If $\Lambda_x\, x \cdot N = \tilde{x}$, then N is a "normal factor." In this way many algebraic concepts and theorems (e.g., the theorem of Jordan-Hölder; see IB2, §12.1) can be interpreted as concepts and theorems in the theory of relations.

Exercises for §8

1. Prove (cf. §§8.3 and 8.4) that

r is reflexive $\leftrightarrow I \subseteq r$,

r is transitive $\leftrightarrow r^2 \subseteq r$,

r is identitive $\leftrightarrow r \cap \breve{r} \subseteq I$,

r is connex $\leftrightarrow r \cup \breve{r} = I$,

r is a function $\leftrightarrow \breve{r}r \subseteq I$,

r is a one-to-one mapping $\leftrightarrow \breve{r}r \cup r\breve{r} \subseteq I$.

2. State the axiom of choice and the well-ordering theorem in the symbolic language developed in §§7 and 8.

Bibliography

For the concepts and applications of the theory of relations see Carnap [2].

9. Boolean Algebra

9.1. *Preliminary Remarks*

In the present section we are interested in certain phenomena that first came to light in the study of the propositional calculus (§2); the fact that they are essentially algebraic in nature was first recognized by G. Boole (1847).

Let us consider the one-place predicates P, Q, ... for a fixed domain of individuals M (cf. §3). These predicates can be put in one-to-one correspondence with the subsets p, q, ... of M by assigning x to p if and only if P holds for x; that is,

(9.1)
$$x \in p \leftrightarrow Px.$$

The conjunction of two predicates obviously corresponds to the intersection of two sets; similarly, the alternative corresponds to their union:

$$x \in p \cap q \leftrightarrow Px \wedge Qx, \qquad x \in p \cup q \leftrightarrow Px \vee Qx. \tag{9.2}$$

The distributive, associative, and other laws for $\cap$ and $\cup$ correspond to the same laws for $\wedge$ and $\vee$. Negation corresponds to complementation ($x \in \bar{p} \leftrightarrow \neg Px$), where (cf. §2.2):

$$\begin{aligned} p \cup \bar{p} &= M, \qquad Px \vee \neg Px \leftrightarrow W, \\ p \cap \bar{p} &= 0, \qquad Px \wedge \neg Px \leftrightarrow F. \end{aligned} \tag{9.3}$$

Logical implication corresponds to set-theoretic inclusion:

$$p \subseteq q \leftrightarrow \bigwedge_x (Px \rightarrow Qx). \tag{9.4}$$

We see that the domain of predicates for M has the same "structure" as the domain of subsets of M; the two domains are isomorphic. For the general study of such domains it is therefore natural to introduce an abstract algebra by means of axioms. The system of axioms will be *autonomous* in the sense of §4.

9.2. *Boolean Lattices*

A set M of elements $a, b, \ldots$ with operations $\cap, \cup, -$ is called a *Boolean lattice* if the following axioms are satisfied:

B0. $a \cap b$, $a \cup b$, $\bar{a}$ are defined for all elements of M and are themselves elements of M.

B11. $a \cap b = b \cap a$
B12. $a \cup b = b \cup a$ } (Commutative laws)

B21. $a \cap (b \cap c) = (a \cap b) \cap c$
B22. $a \cup (b \cup c) = (a \cup b) \cup c$ } (Associative laws)

B31. $a \cap (a \cup b) = a$
B32. $a \cup (a \cap b) = a$ } (Absorption laws)

B41. $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$
B42. $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$ } (Distributive laws)

There exist elements 0 and 1 in M such that for every a in M

B51. $a \cap \bar{a} = 0$
B52. $a \cup \bar{a} = 1$ } (Complementation laws)

In the set-theoretic interpretation, $a \cap b$ and $a \cup b$ are read as *intersection of a and b* and *union of a and b*, respectively, and in the logical interpretation, as *a and b* and *a or b*. This system of axioms is denoted by B.

Looking through the list of axioms in B, we see that for every axiom there exists a *dual* axiom, formed by interchanging $\cap$ with $\cup$ and 0 with 1. Thus for every theorem there is also a dual theorem, whose statement and proof arise from the given theorem by these interchanges (*principle of duality* for Boolean algebra). A corresponding principle of duality holds for the predicate logic, if we interchange T and F. For example, the theorem $\wedge_x Px \vee \vee_x \neg Px \leftrightarrow T$ is dual to $\vee_x Px \wedge \wedge_x \neg Px \leftrightarrow F$.

Let us state a few easily proved theorems for Boolean lattices:

$$
\begin{aligned}
&a \cap a = a, \quad a \cup a = a,\\
&a \cap 0 = 0, \quad a \cup 1 = 1, \quad a \cup 0 = a, \quad a \cap 1 = a,\\
&a \cup b = b \rightarrow a \cap b = a, \quad a \cap b = b \rightarrow a \cup b = a,\\
&\bar{0} = 1, \quad \bar{1} = 0.
\end{aligned} \tag{9.5}
$$

A domain with operations $\cap$ and $\cup$, for which only the axioms B0 (without complementation), B1, B2, and B3 are required, is called a *lattice*. Boolean lattices are distributive and complemented (cf. IB9, §1).

9.3. *Inclusion in Boolean Lattices*

Inclusion can be defined by

$$a \subseteq b \Leftrightarrow a = a \cap b, \tag{9.6}$$

which corresponds to the set-relation, or equivalently by (§7.2) $b \subseteq a \Leftrightarrow a = a \cup b$.

Let $a \subset b$ signify that $a \subseteq b$ and $a \neq b$. It is easy to show that the relation $\subseteq$ is reflexive, transitive, and identitive, and is thus a partial ordering in the sense of $\leqslant$ (cf. §8.3). Also,

$$a \cap b \subseteq a, \quad a \subseteq a \cup b, \quad a \subseteq 1, \quad 0 \subseteq a, \tag{9.7}$$

$$(a \subseteq b \wedge a \subseteq c) \rightarrow a \subseteq b \cap c, \quad (b \subseteq a \wedge c \subseteq a) \rightarrow b \cup c \subseteq a. \tag{9.8}$$

From (9.8) it follows that $b \cap c$ and $b \cup c$ may serve as *greatest lower bound* and *least upper bound* of b and c with respect to $\subseteq$. Every element that is contained in b and c is also contained in the greatest lower bound $b\,c$, and every element that contains b and c also contains the least upper bound $b \cup c$ of b and c. The greatest lower bound of all the elements is 0, and their least upper bound is 1. Thus every lattice is partially ordered, with a least upper bound and a greatest lower bound for arbitrary a and b. Conversely, the above properties of inclusion may be used to construct a lattice from a partial ordering with least upper bound and greatest lower bound. For example, we may define $x = a \cap b$ by

$$x = a \cap b \Leftrightarrow \wedge ((z \subseteq a \wedge z \subseteq b) \leftrightarrow z \subseteq x). \tag{9.9}$$

If we note that for $a \cap b = c \cup d$ we may also write $\bigvee_x (x = a \cap b \wedge x = c \cup d)$, we see that the axioms of $\mathfrak{B}$ may be at once translated into axioms for $\subseteq$. For $a = 0$ we write $\bigwedge_x (a \subseteq x)$; for $a = 1$ we write $\bigwedge_x (x \subseteq a)$; and for $a = \bar{b}$ we write $\bigwedge_x (x \subseteq a \cup b) \wedge \bigwedge_x (a \cap b \subseteq x)$.

9.4. *Boolean Rings*

A third possibility for the description of Boolean algebra lies in the theory of rings. We define

$$a \cdot b \Leftrightarrow a \cap b, \qquad a + b \Leftrightarrow (a \cap b') \cup (a' \cap b). \tag{9.10}$$

Then we can easily show

$$\begin{aligned} &a \cdot b = b \cdot a, \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c), \qquad a + b = b + a, \\ &a + (b + c) = (a + b) + c, \qquad a \cdot (b + c) = a \cdot b + a \cdot c, \\ &a \cdot 1 = a, \qquad a + 0 = a. \end{aligned} \tag{9.11}$$

$$a \cdot a = a, \qquad a + a = 0. \tag{9.12}$$

These are the axioms for a commutative idempotent ring with unity element.[32] Such a ring is called a *Boolean ring*. Conversely, from a Boolean ring we can form a Boolean lattice by setting

$$a \cap b \Leftrightarrow a \cdot b, \qquad a \cup b \Leftrightarrow a + b + a \cdot b, \qquad \bar{a} \Leftrightarrow 1 + a. \tag{9.13}$$

9.5. *Finite Boolean Lattices*

The subsets of a finite set M form a finite Boolean lattice with respect to the set-theoretic operations. Here the empty set represents the element 0 and the whole set M represents the element 1. If M has n elements, then the lattice has 2^n elements (cf. §7.2). Thus every finite Boolean lattice has 2^n elements ($n = 0, 1, 2, \ldots$), since we can show that every finite Boolean lattice is isomorphic to a lattice of subsets. The proof of this theorem rests on the fact that every element of a finite Boolean lattice is the union of atoms in the lattice, where an element a is called an *atom* if $a \neq 0$ and if from $x \subset a$ it follows that $x = 0$. The atoms of a lattice of subsets are the sets with one element $\{x\}$ (see §7.2). The finite Boolean lattices can be very clearly illustrated by diagrams in which the elements are represented by points in a plane in such a way that if $a \subset b$ and $\neg \bigvee_c (a \subset c \wedge c \subset b)$, then a lies below b and is joined to b by a line segment. Thus if the number of elements is 2^0, 2^1, 2^2, 2^3, we obtain the following figures:

[32] For the concept of rings see IB5, §1.5 ff.; a ring is *idempotent* if $a \cdot a = a$ for each of its element.

Fig. 6

Fig. 7

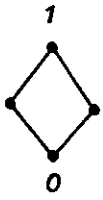


Fig. 8

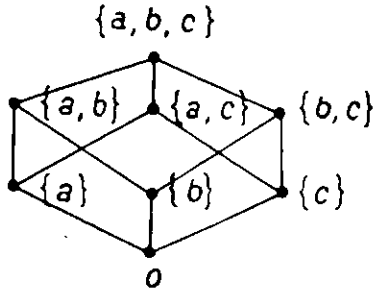


Fig. 9

The diagram for the lattice with 2^3 elements shows the subsets of the 3-element set $M = \{a, b, c\}$.

Exercises for §9

1. Prove

   (a) (9.5) from the system of axioms $\mathfrak{B}$,

   (b) (9.7) and (9.8) from $\mathfrak{B}$ and (9.6),

   (c) (9.11) and (9.12) from $\mathfrak{B}$ and (9.10).

2. Consider propositional forms constructed from countably many (cf. 7.3) propositional variables $p, q, \ldots$ (cf. 2.4) by the connectives $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ (cf. 2.4) of the propositional calculus. Define

   $$H \sim \Theta \Leftrightarrow H \leftrightarrow \Theta \text{ is a tautology (3.4).}$$

   Now prove

   (a) $\sim$ is an equivalence relation

   (b) $\sim$ is consistent with the functions K, A, N defined on the set of propositional forms as follows:

   $$K(H, \Theta) = H \wedge \Theta$$
   $$A(H, \Theta) = H \vee \Theta$$
   $$N(H) = \neg H.$$

   (c) The equivalence classes form a Boolean algebra under the following definitions:

   (1) $\tilde{H} \cap \tilde{\Theta} = \widetilde{H \wedge \Theta}$

   (2) $\tilde{H} \cup \tilde{\Theta} = \widetilde{H \vee \Theta}$

   (3) $\tilde{\tilde{H}} = \widetilde{\neg H}$

   (4) $0 = \widetilde{p \wedge \neg p}$

   (5) $1 = \widetilde{p \vee \neg p}$

By b) the definitions (1)–(3) are independent of the representatives of the equivalence classes. Show that in (4) and (5) the definitions are independent of the choice of the propositional variable p.

(d) If the number of propositional variables is finite, then the Boolean algebra is also finite. If n is the number of variables, then the number of elements in the Boolean algebra is 2^{2^n}.

Bibliography

For Boolean algebra, see Goodstein [1].

10. Axiomatization of the Natural Numbers

10.1. *Preliminary Remarks*

The theory of natural numbers occupies an especially important place in studies in the foundations of mathematics. In the first place, the arithmetic of natural numbers offers a simple and important example of a theory with an infinite domain of individuals, in which the problems connected with the concept of *infinity* can be studied. Secondly, it has turned out that many other interesting metamathematical questions can be reduced to arithmetic (cf. the arithmetization in §5.4). Finally, the results of Gödel on arithmetical algorithms have had a lasting influence on the whole program of metamathematics. Let us discuss these remarks in greater detail.

The "leap to infinity" involved in recognizing the domain of the natural numbers is already adequate for all the ontological needs of the predicate logic (cf. §3); this is the meaning of the fundamental theorem of Löwenheim and Skolem, which essentially states that in order to investigate the concept of a consequence there is no need to use any domain of individuals other than the natural numbers.

Since in a system of axioms $\mathfrak{S}$ the means of expression (variables, logical symbols, and so forth), are obviously *countable*, it is clear that the obtainable expressions are also countable. Thus the expressions can be "numbered" constructively (see §5.4). For every expression the resulting index is computable and, conversely, for every number we can decide whether or not it is the index of an expression; if it is, then the expression can be recovered. As a result, certain metamathematical properties like *...is an expression*, *...is the conjunction of... and...* *...is true* are transformed into number-theoretical properties. Thus all questions of decidability can be translated into the corresponding questions for arithmetic. Moreover, if the system $\mathfrak{S}$ includes an arithmetical system of axioms, many of the metamathematical propositions about $\mathfrak{S}$ can be

formulated in $\mathfrak{S}$ itself, and in this way it is possible to obtain extremely general theorems about mathematical systems of axioms (cf. §10.5).

For a long time the concept of the (infinite!) *totality of natural numbers* was held to be intuitively clear, and indeed quite self-evident [cf. the similar situation for the concept of a set (§7.1)]. It was Frege (1884) who first pointed out the necessity for an exact definition of a *natural number*. In his attempt to reduce arithmetic to logic he defined the number 1, for example, as the totality of all one-place predicates that hold for exactly one individual. This definition is closely related to the set-theoretical introduction of the natural numbers and leads to the same kind of difficulties as the naive theory of sets (§7.3). Thus we naturally seek, as in that theory, to characterize the natural numbers by a system of axioms. The best-known system of axioms for the natural numbers is due to Dedekind (1888) but is named after Peano (1889). In §10.3 we shall discuss a somewhat modified system, formulated in the language of predicate logic. The question of axiomatizing the whole of arithmetic (§10.4) then leads us to the well-known Incompleteness Theorem of Gödel (§10.5). The present section closes with some remarks on the operational construction of arithmetic recently proposed by Lorenzen.

10.2. *The Peano Axioms*

The Peano axioms (with unimportant changes):

(a) 0 *is a natural number.*[33]

(b) *If* n *is a natural number, then so is* n'.

(c) *If* $m' = n'$, *then* $m = n$.

(d) *There is no number* n *for which* $n' = 0$.

(e) *Axiom of complete induction:*

If a property P *of the natural numbers satisfies the following two conditions, then* P *holds for every natural number:*

(1) P *holds for* 0.

(2) *For every natural number* n, *if* P *holds for* n, *then* P *holds for* n'.

These axioms can be stated in a formal language consisting, as before, of formulas or rows of symbols, but now, in view of the fact that the axiom (e) speaks of an *arbitrary property*, we must make use of a generalized *predicate* variable; that is, a predicate variable bound by the universal quantifier. Expressions with quantified predicate variables are regarded as belonging to *logic of the second order*, or to the *extended predicate logic*. Expressions in which only subject variables are quantified are said to

[33] The sequence of natural numbers is often taken to begin with 1.

belong to *logic of the first order*, or to *elementary predicate logic*. For the extended predicate logic, as well as for the elementary (§3), it is possible to give a semantic definition of the concept of a consequence.

Except for axiom (e) we will continue to confine our arithmetical expressions to the elementary logic. *In particular, in questions of completeness and decidability we shall consider only relevant expressions of the first order.* The fundamental concepts of our system of axioms are: (1) an individual variable for zero; as such we take the traditional symbol 0; (2) a predicate variable for the relation of successor; we make use of the functional notation and denote the successor of x by x' (cf. §2.5); (3) a predicate variable for identity; as such we use the traditional symbol $=$. There is no need to mention the axioms (a) and (b), since we do not admit any individuals other than the natural numbers. In a supplementary axiom we express the conditions that must be satisfied by the identity.

The Peano system of axioms $\mathfrak{P}$ *in the extended predicate logic.*[34]

(P1) $$x' = y' \to x = y,$$

(P2) $$\neg\, x' = 0,$$

(Ind) $$\bigwedge_P (P0 \wedge \bigwedge_y (Py \to Py') \to \bigwedge_x Px),$$

(G) $$x = y \leftrightarrow \bigwedge_P (Px \to Py).$$

The semantic consistency (cf. §4.7) of $\mathfrak{P}$ is obvious for anyone who feels convinced of the "existence" of the natural numbers. But for the extended predicate logic we have not yet defined a concept of deducibility, so that for the time being the question of syntactical consistency (cf. §5.7) does not arise.

The system $\mathfrak{P}$ *is monomorphic* (§4.6) and thus, as desired, it characterizes the natural numbers. Let us outline the proof.

Let M and $\bar{M}$ be arbitrary models (cf. §3) of $\mathfrak{P}$. Then M contains a domain of individuals J, a function f (for x') defined on J and a fixed element n (representing 0) in J. We denote the corresponding objects for $\bar{M}$ by $\bar{J}$, $\bar{f}$, $\bar{n}$. We must now show that M and $\bar{M}$ are isomorphic (§8.4); that is, we must demonstrate the existence of a mapping Φ of J onto $\bar{J}$ with the properties of an isomorphism.

(10.1) $$\Phi(n) = \bar{n},$$

(10.2) $$\Phi(f(x)) = \bar{f}(\Phi(x)).$$

[34] For clarity, we have emphasized here that P is generalized, i.e., bound by the universal quantifier. Of course, x and y are also to be considered as generalized.

First we define inductively a *relation* Φ by

(10.3) $$n\Phi\bar{n},$$

(10.4) $$\bigwedge_x \bigwedge_y ((x \in J \wedge y \in \bar{J}) \to (x\Phi y \to f(x)\ \Phi f(y))),$$

(10.5) Let $x\Phi y$ hold only as required by (10.3) or (10.4).

We now prove step by step [with tacit use of the axiom of equality (*G*)].

(1) The first domain of Φ is J (proof by the axiom of induction for the model M).

(2) The second domain of Φ is $\bar{J}$ (proof by the induction axiom for the model $\bar{M}$).

(3) There is no x in J with $n = f(x)$ [proof by the axiom (P2) for M].

(4) There is no x in J with $f(x)\ \Phi\bar{n}$ [proof by (3) and (10.3, 4, 5)].

(5) If $x\Phi\bar{n}$ and $y\Phi\bar{n}$, then $x = y$ [proof by (4) and (1)].

(6) If $x\Phi z$ and $y\Phi z$, then $x = y$; that is, $\breve{\Phi}$ is a function (8.3) [proof by induction for $\bar{M}$, (5) and (P1)].

(7) Φ is a function [proof analogous to (6)].

Thus we have shown that Φ is a one-to-one mapping of J onto $\bar{J}$, from which the properties of an isomorphism follow immediately by (10.3) and (10.4).

We must note, however, that this proof can be attacked on the ground that it is based in an essential way on semantic ideas that are closely associated with the naive theory of sets. For in fact the "totality of all properties" referred to in (G) and (Ind) is uncountable. From the monomorphy of $\mathfrak{P}$ it follows that $\mathfrak{P}$ is complete (cf. §4.5).

10.3. *The Peano Axiom with Restricted Axiom of Induction*

We now turn to an axiom system $\mathfrak{P}_1$, which completely avoids the extended predicate logic. In order to exclude quantification of predicate variables, we must first make some change in the axiom of equality (G). Let us replace it by the two axioms

(G1) $$x = x,$$

(G2) $$x = y \to (\mathsf{H}(x) \to \mathsf{H}(y)).$$

Since for $\mathsf{H}(x)$ we may write any expression of the elementary predicate logic, it follows that, strictly speaking, (G2) is not an axiom but an *axiom schema* (§4) which in an obvious way represents countably many axioms.

The axioms (P1) and (P2) remain unchanged, but for (Ind) we must also introduce an axiom schema:

(Ind_1) $\quad \mathsf{H}(0) \wedge \bigwedge_y (\mathsf{H}(y) \to \mathsf{H}(y')) \to \mathsf{H}(x)$ *(induction schema).*

The system (G1, G2, P1, P2, Ind_1) will be denoted by $\mathfrak{P}_1$. Like $\mathfrak{P}$, the system $\mathfrak{P}_1$ is of course semantically consistent. On the other hand, monomorphy is lost in the transition from $\mathfrak{P}$ to $\mathfrak{P}_1$. For we see that the proof of monomorphy for P cannot simply be repeated for $\mathfrak{P}_1$, since the properties to which (Ind) was applied in that proof are not necessarily capable of formulation (and in fact cannot be formulated) in the elementary predicate logic (cf. §10.2). In §10.5 we shall see that P_1 actually admits nonisomorphic models. It can be shown that the set of deductions from $\mathfrak{P}_1$ or from $\mathfrak{P}$ is decidable.[35] These systems are therefore complete and their theorems can be obtained by algorithms.

10.4. *Systems* $\mathfrak{Z}$ *and* $\mathfrak{Z}_1$ *for Arithmetic*

For the construction of arithmetic it is clear that the successor function alone is not enough. We also need addition and multiplication. These functions, as we know, can be defined recursively (§5.6), and the equations defining them can be adjoined to the axioms. Let us first state the axioms for addition:

$$x + 0 = x, \tag{10.6}$$

$$x + n' = (x + n)'. \tag{10.7}$$

From $\mathfrak{P}$ and $\mathfrak{P}_1$ we thus obtain axiom systems $\mathfrak{D}$ and $\mathfrak{D}_1$, respectively, to which the properties of monomorphy and nonmonomorphy, of completeness and decidability, are transferred. But these advantages are offset by a certain poverty in our means of expression. To be sure, we can still express such number-theoretical concepts as $x < y$ or 3 *is a factor of* x:

$$x < y \Leftrightarrow \bigvee_z (z \neq 0 \wedge x + z = y), \tag{10.8}$$

$$3 \mid x \Leftrightarrow \bigvee_z (z + z + z = x). \tag{10.9}$$

But it can be shown that other important concepts like $x \mid y$ or x *is a prime number* cannot be defined, so that many interesting number-theoretical problems cannot be formulated and thus cannot be decided within the framework of these theories.

[35] It must be noted that in these formal systems multiplication does not occur and cannot be (explicitly) defined.

In order to enrich our means of expression we adjoin the recursive definition of multiplication to the axioms of $\mathfrak{D}$ and $\mathfrak{D}_1$:

(10.10) $$x \cdot 0 = 0,$$

(10.11) $$x \cdot (n') = (x \cdot n) + x.$$

The resulting systems will be denoted by $\mathfrak{Z}$ and $\mathfrak{Z}_1$. In these systems we can define, for example, the following arithmetical concepts:

(10.12) $$x \mid y \Leftrightarrow \bigvee_z (y = x \cdot z),$$

(10.13) $$\text{Prime } x \Leftrightarrow x \neq 0 \wedge x \neq 0' \wedge \bigwedge_z (z \mid x \rightarrow (z = 0' \vee z = x)).$$

Gödel has shown, although we have no space for his proof here, that all decidable properties and relations (§5.4), e.g., $z = xy$, are now definable: The system $\mathfrak{Z}$ (or $\mathfrak{Z}_1$) includes the complete recursive theory of numbers.

The (syntactical) consistency of $\mathfrak{Z}_1$ was proved by Gentzen in 1936.

In comparison with the preceding systems, the investigation of $\mathfrak{Z}$ and $\mathfrak{Z}_1$ gives rise to considerably greater difficulties. Consider, for example, the existence of such unsolved number-theoretical problems as the Goldbach conjecture:

(10.14) $$\bigwedge_z (2 \mid z \wedge z \neq 2 \rightarrow \bigvee_{x,y} (\text{Prime } x \wedge \text{Prime } y \wedge z = x + y)).$$

Such problems make it plausible, as is in fact the case, that in these systems the set of consequences is not decidable. The truth of this statement results from the following theorem of Gödel, which is one of the most important discoveries in the whole theory of the foundations of mathematics.

10.5. *The Gödel Incompleteness Theorem:* $\mathfrak{Z}_1$ *Is Incomplete (Even Essentially Incomplete*; cf. End of the Present Subsection)

Although it will be impossible to include many of the details, we wish to give an outline here of the proof of this theorem, partly on account of its great importance, but also in order that the reader may see how an argument which in a natural language leads to a contradiction (namely to the Antinomy of the Liar described in §11.3) can in a formal language be put to good use, namely, to prove the incompleteness of $\mathfrak{Z}_1$.

An important instrument in the proof is the arithmetization described in §5.4, where we have shown that a procedure can be set up whereby the formulas of the language are characterized by their so-called Gödel numbers. Since it is decidable whether or not a given formula is a relevant expression,[36] it is also decidable whether a given natural number is the

[36] A *relevant expression* here is the same as a *relevant* proposition in §4.5.

Gödel number of some relevant expression. Since we have shown in §10.4 that all decidable properties can be defined in $\mathfrak{Z}_1$, there exists a relevant expression $A(x)$ which in the natural interpretation (i.e., the interpretation in which 0 corresponds to zero, and so forth) holds for a natural number if and only if this number is the Gödel number of an expression in $\mathfrak{Z}_1$.

Finite sequences of relevant expressions can be represented by numbers in the same way as the expressions themselves, so that, in particular, proofs can be expressed by numbers, since they are merely special sequences of expressions. Since it is decidable whether a given rule of inference has been correctly used, we can now find a relevant expression $C(p, q)$ which in the natural interpretation is true for p and q if and only if p is the number of a relevant expression H and q is the number of a proof of H in $\mathfrak{Z}_1$.

We now proceed to construct a relevant expression E, containing no free variables, which in the natural interpretation states that E (in other words, the expression itself) is unprovable (cf. the Paradox of the Liar in §11.3). If we assume that E is provable, we then have the following situation: Every model of $\mathfrak{Z}_1$, and consequently also the natural interpretation, satisfies E and therefore states, in contradiction to our assumption, that E is unprovable. On the other hand, if we assume that $\neg E$ is provable, the natural model will satisfy $\neg E$, and therefore falsify E; that is, E is provable, a result which, taken together with the provability of $\neg E$, contradicts the consistency of $\mathfrak{Z}_1$. Thus neither E nor $\neg E$ is provable.

This syntactical result, when reformulated in semantic language, states that neither E nor $\neg E$ is a consequence of $\mathfrak{Z}_1$. In other words, $\mathfrak{Z}_1$ is incomplete, as asserted.

The expression E, which asserts its own unprovability, is constructed as follows: If n is the Gödel number of an expression with exactly one free variable x, let us denote this expression by $A_n(x)$ and call n an A number. We construct the propositional form

(10.15) *x is an A number and y is the Gödel number of a proof of $A_x(x)$.*

By means of the arithmetization, this propositional form can be represented by an expression $B(x, y)$ in $\mathfrak{Z}_1$ with the two free variables x and y. Now let p be the Gödel number of the expression $\wedge_y \neg B(x, y)$. We form the expression $A_p(p)$ obtained by replacing x with p in $A_p(x)$. By (10.15) this expression states: *for every y, the number y is not the Gödel number* of a proof of $A_p(p)$. Thus $A_p(p)$ is a proposition E of the desired kind.

This theorem can obviously be extended to all axiomatic theories that have constructive definitions for their expressions and rules of inference, and that include a sufficiently large part of arithmetic.

The incompleteness theorem has some remarkable consequences:

(1) There exist arithmetical propositions (e.g., E) that are true for the natural numbers but are not provable in $\mathfrak{Z}_1$. It is conceivable, for example, that the Fermat conjecture or the proposition (10.14) is true but cannot be deduced by means of the familiar rules of inference in $\mathfrak{Z}_1$.

(2) From the incompleteness of $\mathfrak{Z}_1$ it follows by §4.6 that $\mathfrak{Z}_1$ *is not monomorphic*. For example, the proposition E is true for the model of the natural numbers but certainly untrue for some other model of $\mathfrak{Z}_1$, since E is not a consequence of $\mathfrak{Z}_1$.

(3) If we introduce into $\mathfrak{Z}$ certain natural rules of inference (it is to be noted that the language in which $\mathfrak{Z}$ is formulated goes beyond the means of expression available in the predicate logic), we can prove, just as for $\mathfrak{Z}_1$, that there exists in $\mathfrak{Z}$ a proposition E such that neither E nor $\neg E$ is deducible. Then we could proceed, again just as for $\mathfrak{Z}_1$ (see above), to prove that $\mathfrak{Z}$ is incomplete, provided we were allowed, as is the case in $\mathfrak{Z}_1$, to replace the concept of provability by the concept of a consequence. But we know that $\mathfrak{Z}$ is complete, as may be proved in exactly the same way as for $\mathfrak{P}$ in §10.2. Thus we have the important result that in $\mathfrak{Z}$, and more generally in the logics of higher order as contrasted with the predicate logic, the concept of a consequence cannot be reduced to an algorithm.

One might think that the incompleteness of $\mathfrak{Z}_1$ could be removed by the introduction of further axioms that would leave the system consistent. But so long as we are dealing with finitely many axioms (or more generally with a decidable schema of axioms), the concept of provability remains decidable, so that the above argument can be applied to the enlarged system of axioms. Thus we are dealing here with an *essential, nonremovable incompleteness*.

These results for $\mathfrak{Z}_1$ and $\mathfrak{Z}_2$ can also be obtained in the following way. We can show that in any sufficiently expressive arithmetical language there always exists, for any given recursively enumerable set (§5.3) M of arithmetical theorems [i.e., arithmetical propositions that are valid in the natural interpretation (§10.5)], an arithmetical proposition E which, together with its negation, does not belong to M. Thus we have:

(*a*) Since the set of deductions in $\mathfrak{Z}_1$ is recursively enumerable (§6.2), the system $\mathfrak{Z}_1$ is incomplete;

(*b*) The system $\mathfrak{Z}$, like $\mathfrak{P}$, is monomorphic and therefore complete (§10.2). Thus the set of deductions in $\mathfrak{Z}$ is not recursively enumerable, and therefore certainly not decidable.

For a system of axioms $\mathfrak{S}$ that includes arithmetic we can also construct, by means of our arithmetization, a proposition W expressing the syntactical consistency of $\mathfrak{S}$. Then the Gödel theorem leads to the result that W

is not deducible in $\mathfrak{S}$, provided $\mathfrak{S}$ is consistent. Consequently, in order to prove the consistency of $\mathfrak{S}$ we must make use of methods that lie outside $\mathfrak{S}$.

10.6. *The Operational Construction of Arithmetic*

In this construction the theorems of arithmetic and of other branches of mathematics are regarded, without reference to any possible semantic interpretation, as statements concerning the application of certain rules of *operation with finite systems*, which may consist of numerals or of concrete objects of any kind. If we study these systems (which are made up of finitely many "atoms" or indivisible systems), we can distinguish them according to their "length," and in this way we necessarily arrive at the conception of a number. By "abstraction" from systems of the same length we obtain the fundamental numbers, which can be uniquely represented by systems such as |, ||, |||, ... (Lorenzen). Propositions, rules of inference, sets, and so forth are again merely systems or "terms" (possibly with certain rules of transition from one system to another). The fundamental rules of operation are given in the form of *algorithms*, on the basis of which further systems and rules can be "deduced." However, this "deducibility" must be of an obviously "constructive" nature; in his "protologic," Lorenzen gives a number of principles of deduction that can be considered constructive.

The operative construction of arithmetic can only be briefly indicated here (see also §5.2). The system for generating the numerals is defined by an algorithm with one axiom and one rule, involving the proper variable e (cf. §5.2):

(10.16) $$|,$$

(10.17) $$\frac{e}{e|}.$$

Equality is defined by the following algorithm (k, l are variables for numerals):

(10.18) $$| = |,$$

(10.19) $$\frac{k = l}{k| = l|}.$$

By various principles of deduction we now realize that:

(10.20) $$k| = l| \to k = l,$$

(10.21) $$k| \neq k,$$

(10.22) $k = l \wedge A(k) \to A(l)$ (so-called principle of equality).

(10.23) $A(|) \wedge \bigwedge_k (A(k) \to A(k|)) \to A(l)$ (so-called principle of induction).

The significance of (10.20) is that the rule

$$\frac{k \mid = l \mid}{k = l} \tag{10.24}$$

is superfluous, i.e., in the algorithm for equality nothing can be deduced with this rule that cannot be deduced without it, as follows from the so-called principle of *inversion:* since $k \mid = l \mid$ can be obtained only from $k = l$, it follows that $k = l$ must also be deducible.

The atom $\wedge$ is introduced by a rule which is identical with the rule for $\wedge$-introduction in §6.4, but the rules in §6.4 for the elimination of $\wedge$ are not required here, since the principle of inversion shows that they are superfluous.

The systems (10.20)–(10.23) correspond to the Peano axioms; but in the present case they are not "postulated" but follow from certain "protological" theorems applied to the arithmetical algorithm.

One advantage of this construction of mathematics lies in the fact that by its very nature it leads only to propositions that can be seen intuitively to be true and therefore cannot involve contradictions.

Exercises for §10

1. On the basis of the axioms (*P*1), (*P*2), (Ind) and (G) prove the following theorem

$$\bigwedge_P (P0 \wedge P0' \wedge \bigwedge_x (Px \to Px'') \to \bigwedge_x Px).$$

2. To (*P*1), (*P*2), (Ind), (*G*), 10.6 and 10.7 adjoin the axioms

$$0^2 = 0$$
$$(x')^2 = x^2 + x + x + 0'.$$

Then show that in the resulting system it is possible to define the relation that holds for x, y and z if and only if $x \cdot y = z$.

Bibliography

Elementary problems in the foundations of arithmetic are discussed in Tarski [1]. For the theory of the systems Z and Z_1 see Russell [1]. On the concept of arithmetic itself see Frege [1].

11. Antinomies

11.1. *Classification of the Antinomies*

A proposition (or a propositional form) together with its negation form a *contradiction*. By an *antinomy* or *paradox* we mean an argument that leads to a contradiction.

It is natural to ask what could be the nature of such an argument. This question is most easily answered if we are dealing with an algorithm, since an antinomy then consists in the deduction of a proposition and of its negation. Since only formal processes are involved here, we speak of a *syntactic antinomy* (for the concepts of syntax and semantics cf. §3.1).

But it can also be the case that an argument which leads to a contradiction is not truly formal but depends on the meaning of the propositions (or of parts of them) that are used in the argument. In this case we speak of a *semantic antinomy*.

Since algorithms in the strict sense of the word are very recent inventions, it is not surprising that syntactic antinomies have been known for a relatively short time. On the other hand, many semantic antinomies were already discussed in antiquity.

If we can deduce a proposition and its negation, then by the rule of $\neg$-elimination (see §6.4) we can deduce *any* proposition. But if we can deduce *everything*, there is no interest in constructing arguments. As a result, we reject any algorithm that leads to a syntactic antinomy. As for semantic arguments leading to a semantic contradiction, we must make up our minds to revise at least one detail of the intuitive truths "inserted" into the argument, but it is often very difficult to accomplish this change in a convincing way.

Syntactic antinomies can also lead, at least indirectly, to a revision of our intuitive ideas. In general, an algorithm is not set up arbitrarily but is based on certain of our intuitive conceptions, which it presents in a concentrated form. Thus, if we find an antinomy in such an algorithm, we must realize either that the conceptions are not adequately represented in the algorithm, or else that they must be rejected, at least to some extent.

We confine ourselves here to a detailed description of two antinomies: the Russell Antinomy, as a characteristic example of a syntactic antinomy, and the Antinomy of the Liar, as a characteristic example of a semantic antinomy.

11.2. *The Russell Antinomy*

We are dealing here with a system of axioms in the language of predicate logic, so that the deductions can be obtained by means of an algorithm. The intuitive conceptions at the basis of this system of axioms are of a set-theoretical nature (cf. §7). Let us describe them briefly: there exists a property defined by the predicate "x is an element of the set y." We represent this predicate by the symbol Exy (that is, we use the symbol Exy of predicate logic to mean $x \in y$). Sets are represented by propositional forms with one variable; for example, the set of even numbers is represented by the propositional form

(11.1) $$2 \mid x,$$

and the set of prime numbers by the propositional form

$$x > 1 \wedge \bigwedge_y (y \mid x \to y = 1 \vee y = x). \tag{11.2}$$

Now if we assume, as seems natural, that every propositional form H with a variable x corresponds to a set y containing exactly those objects which satisfy H, we are led to require as part of our system of axioms that

$$\bigvee_y \bigwedge_x (Exy \leftrightarrow \mathsf{H}). \tag{11.3}$$

It is to be noted that this requirement is not a single axiom but an axiom schema (cf. §4.1), since (11.3) is a prerequisite for every propositional form H containing x (but not y) as a free variable.

The Russell Antinomy now consists of showing that this schema of axioms, within the framework of predicate calculus, leads to a contradiction.

The contradiction is obtained by taking for H the propositional form $\neg\, Exx$. Then the set y, whose existence is required by (11.3) (and whose uniqueness, unimportant here, follows from the principle of extensionality), is *the set consisting of every set that does not contain itself as an element*. But this set y gives rise to a contradiction if we ask whether or not y is a member of itself. For if y is an element of itself, then y, precisely because it is an element of itself, cannot, by definition, be an element of itself. On the other hand, if y is not an element of itself, then, again by the definition of y, it must be an element of itself. Let us deduce the contradiction by a formal argument. In addition to the rules in §6, our set of axioms now includes all the special cases of (11.3) (see the following table).

Line Number	*Flagged Variable*	*Assumptions*	*Assertion*	*Rule Used*
1			$\bigvee_y \bigwedge_x (Exy \leftrightarrow \neg\, Exx)$	axiom
2	y		$\bigwedge_x (Exy \leftrightarrow \neg\, Exx)$	$\vee$-elimination (1)
3			$Eyy \leftrightarrow \neg\, Eyy$	$\wedge$-elimination (2)
4			$Eyy \to \neg\, Eyy$	$\leftrightarrow$-elimination (3)
5			$\neg\, Eyy \to Eyy$	$\leftrightarrow$-elimination (3)
6		Eyy	Eyy	introduction of assumption
7			$Eyy \to Eyy$	elimination of assumption (6)
8		$\neg\, Eyy$	$\neg\, Eyy$	introduction of assumption
9			$\neg\, Eyy \to \neg\, Eyy$	elimination of assumption (8)
10			$Eyy \vee \neg\, Eyy$	excluded middle
11			Eyy	$\vee$-elimination (5, 7, 10)
12			$\neg\, Eyy$	$\vee$-elimination (4, 9, 10)
13			Ezz	$\neg$-elimination (11, 12)
14			$\neg\, Ezz$	$\neg$-elimination (11, 12)

Lines 1–13 provide a finished proof for *Ezz*, and lines 1–14 for $\neg$ *Ezz*, so that the contradiction is proved.[37]

This antinomy indicates that we must in some way revise the set-theoretical conceptions underlying the axioms (11.3). As a result, it is no longer assumed today that *every* propositional form defines a set (cf. §7.6).

11.3. *The Antinomy of the Liar*

This antinomy, already well known in antiquity, makes use of the concept of truth (cf. also §3) and is thus a semantic antinomy. We begin with the stipulation already stated in precise form by Aristotle, that a proposition is true if and only if it describes an actual state of affairs. As a concrete example, let us consider the proposition "it is snowing." Then we can say:

(11.4) "it is snowing" is true if and only if it is snowing.

But this proposition, consisting of the whole of line (11.4), remains true if we replace the proposition "it is snowing" by any other proposition. Thus we are led to recognize the validity of all propositions of the following form:

(11.5) ... is true if and only if---

where in place of "---" we may put an arbitrary proposition, provided that at the same time we put a name of this proposition in place of "...". In order to obtain the Antinomy of the Liar we consider the particular proposition:

(11.6) The proposition that follows "(11.6)" is not true.

In other words, the proposition asserts its own falsity. We now insert this proposition in (11.5) in place of "---" and at the same time we insert a name for this proposition in place of "...". For such a name we choose: "the proposition that follows '(11.6)'." Then as a special case of (11.5) we obtain:

(11.7) The proposition that follows "(11.6)" is true if and only if the proposition that follows "(11.6)" is not true.

But from (11.7) it is easy to obtain a contradiction (cf. the Russell Antinomy starting from line 3 of the proof).

This contradiction cannot be avoided as long as we agree to the following conditions: we accept the Aristotelian criterion of truth (11.5), we admit

[37] We could not stop with line 11 or 12, since they still contain a free occurrence of the flagged variable *y*.

that what is contained in the line (11.6) is a proposition and that "the proposition that follows '(11.6)'" is a name for this proposition, and finally we accept the elementary logical deductions that lead from (11.7) to an actual contradiction.

If now, faced with this contradiction, we ask at what stage we should change our point of view, it would be natural to look first at the Aristotelian criterion of truth (11.5). Yet it must be admitted that proposition (11.5) seems almost self-evident and that we would never have felt any doubt about it if the antinomy had not been brought to our attention. Moreover, we must take note of the fact that in a certain respect we have already made use of this criterion in §3.4, where we discussed the validity, in a certain interpretation, of an elementary propositional form Px_1, ..., x_n. For we can express the Aristotelian criterion, as applied to that special case, in the form:

(11.8) If we replace x by 3 and P by the property of being a prime number, then Px is true if and only if 3 has the property of being a prime number.

The similarity with (11.5) is unmistakable.

But this comparison indicates how we can attack the Antinomy of the Liar. In (11.8) the problem at issue is to define what is meant by saying that a given propositional form is true in a given interpretation. Now the propositional form Px belongs to the language of predicate logic but the desired definition will be given, *not* in the language of predicate logic, but in some other language, namely whatever language we use for talking about predicate logic. Our choice for such a language is everyday English, cautiously used in a somewhat refined form. The predicate "is true" introduced in (11.8) belongs to this everyday language but refers not to propositions of everyday language, but to propositional forms in the language of predicate logic (in conjunction with the given interpretations).

Thus the difference between (11.5) and (11.8) is essentially as follows: in (11.8) we are dealing not only with a given language (the language of predicate logic) but also with a *metalanguage* (everyday English), in which we speak about the first language. The predicate "is true" in (11.8) is a predicate in the metalanguage. But it refers not to propositions in the metalanguage, but to expressions in the first language. In (11.5), on the other hand, there is only *one* language, namely everyday English. The predicate "is true" occurring there belongs to this everyday language and also refers to propositions in the same language.

Now it is easy to see that in (11.8) no antinomy is to be feared (or at any rate we cannot so easily construct one as in the Antinomy of the Liar). For the Antinomy of the Liar is based on a proposition that states its own falsity. But such a situation is not possible (or at any rate not

immediately possible) if we distinguish between language and metalanguage. For in that case we cannot form a proposition that states its own falsity. Such a proposition, call it α, must belong to the metalanguage, since it contains the word "true" (or "false"); but the word "true" in the metalanguage refers to propositions of the initial language and therefore cannot refer to α.

In summary, we may say: we can escape from the Antinomy of the Liar by distinguishing between language and metalanguage and by speaking about the truth of the propositions in a given language—not in that language itself but in a metalanguage. Such distinctions between a formal language and a metalanguage, or a meta-metalanguage and so forth, are common in modern logical investigations. Since the natural languages of the world are "universal" and fail to make this distinction, in the sense that they use the word "true" for arbitrary propositions expressible in them, many investigators consider these natural languages to be inevitably self-contradictory.

As a final remark, let us point out that the other semantic antinomies can be avoided when we make the distinction between language and metalanguage. Consider, for example, the antinomy of the smallest natural number that cannot be described in English in fewer than a hundred words. The antinomy arises from the fact that, precisely in the definition just given, this number has nevertheless been described in fewer than a hundred words. But the above definition refers to all possible descriptions and thus, since it speaks of these descriptions, it must belong to a language that is a metalanguage with respect to the language to which the descriptions belong. Consequently, we obtain *in the metalanguage* a description for the number which is shorter than any possible description *in the initial language*. But this result is not a contradiction.

Exercises for §11

1. An adjective A is said to be *autologic* if A has the property described by A, and otherwise A is *heterologic*. Examples of autologic adjectives are: "seventeenlettered," "English," "pentasyllabic." Consider the word "heterologic." Is it heterologic or autologic? Explain and resolve the antinomy (Grelling's antinomy).
2. If the definition of an object or element m depends on a set M and if m is then assigned to M as an element, the definition of m is said to be *impredicative*.
   (a) Show that the antinomies mentioned in the text make use of impredicative definitions.
   (b) Show that the definition of the least upper bound of a set M of real numbers, as given in real analysis, is impredicative.

Bibliography

On the antinomies in the theory of sets see Beth [1] and Linsky [1].

Bibliography

Bernays, R.: [1] Axiomatic Set Theory. With a historical introduction by Abraham A. Fraenkel. North-Holland Publishing Company, Amsterdam, 1958, VIII + 226 pp.

Beth, E. W.: [1] The Foundations of Mathematics. North-Holland Publishing Company, Amsterdam, 1965, XXVIII + 741 pp.

Bocheński, J. M., [1] A Précis of Mathematical Logic. Translated from the French and German Editions by Otto Bird. D. Reidel, Dordrecht, Holland; Gordon and Breach, New York, VII + 100 pp.

Borsuk, K. and W. Szmielew: [1] Foundations of Geometry. North-Holland Publishing Company, Amsterdam, 1960, XIV + 444 pp.

Carnap, R.: [1] Introduction to Semantics. Harvard University Press, Cambridge, Mass., 1946, 2. Druck, XII + 263 pp.

Carnap, R.: [2] Introduction to Symbolic Logic and its Applications. Dover Publications, Inc., New York, 1958, XIV + 241 pp.

Church, A.: [1] Introduction to Mathematical Logic. Princeton University Press, Princeton, N.J., 1956, IX + 376 pp.

Church, A.: [2] Logic. Article in Encyclopaedia Britannica, Vol. 14. Encyclopaedia Britannica, Ltd., London, Chicago, 1963, pp. 295–305.

Cohen, P. J.: [1] The Independence of the Continuum Hypothesis. Proceedings of the National Academy of Sciences, Vol. 50, pp. 1143–1148 (1963) and Vol. 51, pp. 105–110 (1964).

Cohen, P. J.: [2] Set Theory and the Continuum Hypothesis. W. A. Benjamin, Inc., New York, 1966, VI + 154 pp.

Curry, H. B.: [1] Outlines of a Formalist Philosophy of Mathematics. North-Holland Publishing Company, Amsterdam, 1951, VII + 75 pp.

Curry, H. B.: [2] Foundations of Mathematical Logic. McGraw-Hill Book Company, Inc., New York, 1963, XII + 408 pp.

Davis, M.: [1] Computability and Unsolvability. McGraw-Hill Book Company, Inc., New York, Toronto, London, 1958, XXV + 210 pp.

Fraenkel, A. A.: [1] Abstract Set Theory. North-Holland Publishing Company, Amsterdam, 1953, XII + 479 pp.

Fraenkel, A. A. and Y. Bar-Hillel: [1] Foundations of Set Theory. North-Holland Publishing Company, Amsterdam, 1958, X + 415 pp.

Frege, G.: [1] The Foundations of Arithmetic. Transl. by J. L. Austin. Basil Blackwell, Oxford, 1950, xii + xii^e + XI + XI^e + 119 + 119^e pp.

Frege, G.: [2] Translations from the Philosophical Writings of Gottlob Frege. Edited by P. Geach and M. Black. Basil Blackwell, Oxford, 1952, X + 244 pp.

Goodstein, R. L.: [1] Boolean Algebra. The Macmillan Company, New York, 1963, VI + 140 pp.

Halmos, P. R.: [1] Naive Set Theory. D. Van Nostrand Company, Inc., Princeton N.J., 1960, VII + 104 pp.

Hermes, H.: [1] Enumerability, Decidability, Computability. Springer-Verlag, Berlin, Heidelberg, New York, 1965, IX + 245 pp.

Heyting, A.: [1] Intuitionism. North-Holland Publishing Company, Amsterdam, 1956, VIII + 132 pp.

Hilbert, D. and W. Ackermann: [1] Principles of Mathematical Logic. Chelsea Publishing Co., New York, 1950, XII + 172 pp.
Kalish, D. and R. Montague: [1] Logic. Techniques of Formal Reasoning. Harcourt, Brace & World, Inc., New York, 1964, X + 350 pp.
Keene, G. B.: [1] Abstract Sets and Finite Ordinals. Pergamon Press, Oxford, 1961, X + 106 pp.
Kleene, S. C.: [1] Introduction to Metamathematics. D. Van Nostrand Company, Inc., Princeton, N.J., 1952, X + 550 pp.
Kleene, S. C.: [2] Mathematical Logic. John Wiley & Sons, Inc., New York, 1967, XIII + 398 pp.
Kneale, W. and M. Kneale: [1] The Development of Logic. Clarendon Press, Oxford, 1962, VIII + 761 pp.
Kneebone, G. T.: [1] Mathematical Logic and the Foundations of Mathematics. D. Van Nostrand Company Limited, Princeton, N. J., 1963, XIV + 435 pp.
Kreisel, G.: [1] Mathematical Logic. Lectures on Modern Mathematics, Vol. III (edited by T. L. Saaty), pp. 95–195. John Wiley & Sons, Inc., New York, 1965.
Linsky, L. (editor): [1] Semantics and the Philosophy of Language. The University of Illinois Press, Urbana, 1952, IX + 289 pp.
Lorenzen, P.: [1] Formal Logic. D. Reidel Publishing Company, Dordrecht, 1965, VIII + 123 pp.
Nagel, E., and J. R. Newman: [1] Gödel's Proof. New York University Press, New York, 1958, IX + 118 pp.
Novikov, P. S.: [1] Elements of Mathematical Logic. Oliver & Boyd, Edinburgh, 1964, XI + 296 pp.
Quine, W. V.: [1] Elementary Logic. Ginn and Company, Boston, 1941, VI + 170 pp.
Quine, W. V.: [2] Mathematical Logic. Harper & Row, New York, 1962, XII + 346 pp.
Robinson, A.: [1] Introduction to Model Theory and to the Metamathematics of Algebra. North-Holland Publishing Company, Amsterdam, 1963, IX + 284 pp.
Rosenbloom, P. C.: [1] The Elements of Mathematical Logic. Dover Publications, Inc., New York, 1950, IV + 214 pp.
Rosser, J. B.: [1] Logic for Mathematicians. McGraw-Hill Book Company, Inc., New York, 1953, XIV + 530 pp.
Russell, B.: [1] Introduction to Mathematical Philosophy. The Macmillan Co., New York, 1924, VIII + 208 pp.
Sierpiński, W.: [1] Cardinal and Ordinal Numbers. Państwowe Wydawnictwo Naukowe, Warsaw, 1958, 487 pp.
Suppes, P.: [1] Introduction to Logic. D. Van Nostrand Company, Inc., Princeton, N.J., 1957, XVIII + 312 pp.
Suppes, P.: [2] Axiomatic Set Theory. D. Van Nostrand Company, Inc., Princeton, N.J., 1960, XII + 265 pp.
Tarski, A.: [1] Introduction to Logic and to the Methodology of Deductive Sciences. Oxford University Press, New York, 1941, XVIII + 239 pp.
Tarski, A.: [2] Logic, Semantics, Metamathematics. Clarendon Press, Oxford, 1956, XIV + 471 pp.
Wang, H.: [1] A Survey of Mathematical Logic. North-Holland Publishing Company, Amsterdam, 1964, X + 651 pp.
Wilder, R. L.: [1] Introduction to the Foundations of Mathematics. Second edition. John Wiley & Sons, Inc., New York, 1965, XII + 327 pp.