LOGIC OF MATHEMATICS

Zofia Adamowicz
Paweł Zbierski

Wiley Series in Pure and Applied Mathematics
A Wiley-Interscience Series of Texts, Monographs, and Tracts

This page intentionally left blank

LOGIC OF MATHEMATICS

PURE AND APPLIED MATHEMATICS

A Wiley-Interscience Series of Texts, Monographs, and Tracts

Founded by RICHARD COURANT
Editor Emeritus: PETER HILTON
Editors: MYRON B. ALLEN III, DAVID A. COX,
HARRY HOCHSTADT, PETER LAX, JOHN TOLAND

A complete list of the titles in this series appears at the end of this volume.

LOGIC OF MATHEMATICS

A Modern Course of Classical Logic

ZOFIA ADAMOWICZ
Institute of Mathematics of the Polish Academy of Sciences

PAWEŁ ZBIERSKI
Department of Mathematics, Warsaw University

A Wiley-Interscience Publication

JOHN WILEY & SONS, INC.

New York • Chichester • Weinheim • Brisbane • Singapore • Toronto

This text is printed on acid-free paper.

Library of Congress Cataloging in Publication Data:

Adamowicz, Zofia.
Logic of mathematics : a modern course of classical logic / Zofia Adamowicz, Paweł Zbierski.
p. cm. -- (Pure and applied mathematics)
"A Wiley-Interscience publication."
Includes bibliographical references (p. 254–256) and index.
ISBN 0-471-06026-7 (cloth : alk. paper)
1. Logic, Symbolic and mathematical. I. Zbierski, Paweł.
II. Title. III. Series: Pure and applied mathematics
(John Wiley & Sons : Unnumbered)
QA9.A24 1997
511.3--dc20 95-20818

10 9 8 7 6 5 4 3 2 1

PREFACE

In this textbook on mathematical logic, we take the position of a mathematician rather than a logician. We select and discuss the material referring directly to mathematical practice either by applications to other branches of mathematics or by explaining the nature of mathematical reasoning. In our approach, relational structures are given priority over logical languages. In the exposition we treat the subject as any part of mathematics as far the methods and the level of accuracy is concerned.

The book is addressed first of all to students of mathematics and to all mathematicians who want to have some familiarity with this beautiful domain of science. The technical difficulties do not exceed those used in any standard course of, say, abstract algebra. Nevertheless, to understand the book, some mathematical experience seems necessary.

Part I of the book (Chapters 1 through 17) is an introductory course at graduate level. In Chapters 1 to 4 we develop the theory of relational structures with a particular emphasis on Boolean algebras. In Chapters 5 to 7 we introduce and discuss formulas, the truth relation, theories, and models. Chapters 8 to 11, devoted to the notion of proof, culminate in Gödel's completeness theorem. In Chapters 12 to 17 we deal mostly with model theoretic topics such as definability, compactness, ultraproducts, realization, omitting of types, and so on.

Part II (Chapters 18 through 24) consists of famous theorems crucial in the development of mathematical logic. In Chapters 18 to 21 we present Gödel's theory, leading to his celebrated incompleteness theorems. Chapter 22 is devoted to the independence proof of Goodstein's theorem from Peano arithmetic. The next chapter contains Cohen's proof of Tarski's theorem on elimination of quantifiers for the theory of real closed fields. Finally, in Chapter 24 we present the Matiyasevich theorem on diophantine relations giving a solution of the tenth Hilbert problem. All the above theorems are provided with complete and rigorous proofs.

Each chapter ends with a number of exercises. Some of them are easy; those more difficult are supplied with hints. We advise the reader to solve them all.

As in any branch of mathematics, we make use of some set-theoretical apparatus. The introductory chapter contains the set-theoretical notions and theorems (without proofs) used throughout the book.

ZOFIA ADAMOWICZ
PAWEŁ ZBIERSKI

This page intentionally left blank

CONTENTS

Introduction 1

PART I Mathematical Structures and Their Theories

1. Relational Systems 9
2. Boolean Algebras 13
3. Subsystems and Homomorphisms 19
4. Operations on Relational Systems 25
5. Terms and Formulas 30
6. Theories and Models 47
7. Substitution of Terms 55
8. Theorems and Proofs 62
9. Theorems of the Logical Calculus 67
10. Generalization Rule and Elimination of Constants 75
11. The Completeness of the Logical Calculus 79
12. Definability 86
13. Peano Arithmetic 94
14. Skolem–Löwenheim Theorems 104
15. Ultraproducts 111
16. Types of Elements 121
17. Supplementary Questions 136

PART II Selected Topics

18. Defining Functions in $\mathbb{N}$ 147
19. Total Functions 160
20. Incompleteness of Arithmetic 169
21. Arithmetical Consistency 182
22. Independence of Goodstein's Theorem 201
23. Tarski's Theorem 223
24. Matiyasevich's Theorem 233

Guide to Further Reading 252

References 254

Index 257

LOGIC OF MATHEMATICS

This page intentionally left blank

INTRODUCTION

In this introductory chapter we set forth the logical and set-theoretical notation and theorems to be used throughout the book.

Elementary Logic

Mathematical statements (expressing properties of some objects) are called formulas. Given any formulas ϕ and ψ, we can form the following new ones: the negation $\neg\phi$ (not ϕ) the implication $\phi \to \psi$ (if ϕ then ψ), the disjunction $\phi \vee \psi$ (ϕ or ψ), the conjunction $\phi \wedge \psi$ (ϕ and ψ), and the equivalence $\phi \equiv \psi$ (ϕ if and only if ψ). The operational symbols $\neg$, $\to$, $\vee$, $\wedge$ and $\equiv$ are called the (logical) connectives (besides the above there are also other connectives but we shall not use them). Recall that

$\neg\phi$ is true if ϕ is false and $\neg\phi$ is false if ϕ is true;

$\phi \to \psi$ is true except when the antecedent ϕ is true and the consequent ψ is false;

$\phi \vee \psi$ is true if at least one of the factors ϕ, ψ is true, otherwise false;

$\phi \wedge \psi$ is true if both ϕ and ψ are true, otherwise false;

$\phi \equiv \psi$ is true if both ϕ and ψ are true or both false, otherwise false.

The symbols $\forall$ and $\exists$ denote the universal and the existential quantifiers, respectively. Thus, $\forall x\phi$ abbreviates "for every x, ϕ" and $\exists x\phi$ stands for "there exists an x, such that ϕ." The symbols $\forall x{\cdot}\in X\phi$ and $\exists x \in X\phi$ denote, respectively, $\forall x(x \in X \to \phi)$ and $\exists x(x \in X \wedge \phi)$.

Operations on Sets

The membership relation is denoted by $\in$. Thus, $x \in A$ means that an object x belongs to (is an element of) the set A, while $x \notin A$ means that x does not belong to A. For any sets A and B we can form the union $A \cup B$, the intersection $A \cap B$,

and the difference $A \setminus B$. Thus, we have

$$x \in A \cup B \equiv x \in A \vee x \in B,$$
$$x \in A \cap B \equiv x \in A \wedge x \in B,$$
$$x \in A \setminus B \equiv x \in A \wedge x \notin B.$$

The empty set is denoted by $\emptyset$ and the set inclusion (containment) by $\subseteq$. Thus, we have

$$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B).$$

The proper inclusion is defined as follows:

$$A \subsetneq B \equiv A \subseteq B \wedge A \neq B.$$

The power set $P(A)$ of A is the family of all subsets of the set A, $P(A) = \{x\colon\ x \subseteq A\}$. An indexed family of sets is denoted by $\{A_i\colon\ i \in I\}$ and its union and intersection by $\bigcup\{A_i\colon\ i \in I\}$ and $\bigcap\{A_i\colon\ i \in I\}$, or $\bigcup_{i \in I} A_i$ and $\bigcap_{i \in I} A_i$, respectively.

Thus, we have

$$x \in \bigcup_{i \in I} A_i \equiv \exists i \in I(x \in A_i)$$
$$x \in \bigcap_{i \in I} A_i \equiv \forall i \in I(x \in A_i).$$

Sets A, B are said to be disjoint, if $A \cap B = \emptyset$, that is, A and B have no common element. A family $\mathcal{F}$ is called disjoint if it consists of nonempty sets and any two sets $A, B \in \mathcal{F}$ are disjoint.

Functions

The symbols $\mathrm{dom}(f)$ and $\mathrm{rng}(f)$ denote, respectively, the domain (the set of arguments) and the range (the set of values) of a function f. The expression

$$f\colon\ X \longrightarrow Y$$

means that f is a function defined on X, $\mathrm{dom}(f) = X$, and with values in Y, $\mathrm{rng}(f) \subseteq Y$. If $\mathrm{rng}(f) = Y$, we say that f is onto Y, and f is one-to-one, if $a \neq b$ implies $f(a) \neq f(b)$, for any $a, b \in X$.

The symbols $f[A]$ and $f^{-1}[B]$ denote the image of a set A and the counterimage (inverse image) of B, respectively.

Let $f\colon\ X \longrightarrow X$. A subset $A \subseteq X$ is said to be closed under f, if $f[A] \subseteq A$, that is, $f(a) \in A$ for all $a \in A$.

The composition of an $f\colon X \longrightarrow Y$ and a $g\colon Y \longrightarrow Z$ is denoted by gf or $g \circ f$. The restriction of f to a subset $A \subseteq \mathrm{dom}(f)$ is denoted by $f|A$. The symbol N (sometimes ω) denotes the set of natural numbers, that is, nonnegative integers. A k-element sequence, where $k \in N$, is a function defined on the set $\{1, \ldots, k\}$ (or on another k-element set). We write $a = \langle a_1, \ldots, a_k \rangle$, where $a_i = a(i)$ is the value of a at i. Functions F defined on the set N are sometimes called infinite sequences and one denotes F by $\langle F_i\colon i \in N \rangle$.

Products and Relations

The product $A \times B$ of sets A, B is defined as the set of all ordered pairs $\langle a, b \rangle$ with $a \in A$ and $b \in B$. A (binary) relation on A is any subset $r \subseteq A \times A$. It is customary to write $r(a, b)$ or arb instead of $\langle a, b \rangle \in r$ and not $r(a, b)$ or $a \not r b$ instead of $\langle a, b \rangle \notin r$. In the first case we say that r holds for a, b and in the latter that r does not hold for a, b.

The product $A_1 \times \cdots \times A_n$ of any finite number of sets is defined as the set of all n-element sequences $\langle a_1, \ldots, a_n \rangle$ with $a_i \in A_i$, for $i = 1, \ldots, n$. For $n = 2$ this definition is consistent with the previous one, since the two-element sequences can be identified with the ordered pairs in an obvious way. If $A_1 = \cdots = A_n = A$, then $A_1 \times \cdots \times A_n$ is denoted by A^n (and called the nth power of A).

Any subset $r \subseteq A_1 \times \cdots \times A_n$ is called an n-ary (n-argument) relation.

A binary relation $\simeq$ on a set A is called an equivalence, if $\simeq$ is reflexive $[\forall a \in A(a \simeq a)]$, symmetric $[\forall a, b \in A(a \simeq b \to b \simeq a)]$, and transitive $[\forall a, b, c \in A(a \simeq b \wedge b \simeq c \to a \simeq c)]$. The subset

$$[a] = \{x \in A\colon\ x \simeq a\}$$

is called the equivalence (or abstraction) class of a. The family $A/\simeq\ = \{[a]\colon\ a \in A\}$ of all equivalence classes is a partition of A; that is, distinct classes are disjoint and the union of all classes is A.

Orderings

A binary relation $\leq$ is called a partial ordering if it is reflexive $[\forall x \in X(x \leq x)]$, antisymmetric $[\forall x, y \in X(x \leq y \wedge y \leq x \to x = y)]$, and transitive $[\forall x, y \in X(x \leq y \wedge y \leq z \to x \leq z)]$. A partial ordering is linear if, in addition, it is connected: $\forall x, y \in X(x \leq y \vee y \leq x)$. Given orderings $(X, \leq^X)$ and $(Y, \leq^Y)$, a one-to-one function $f\colon X \longrightarrow Y$ is called an order embedding if it satisfies the condition

$$x \leq^X y \quad \text{if and only if} \quad f(x) \leq^Y f(y), \quad \text{for all } x, y \in X.$$

If, in addition, f is onto Y, then f is called an order isomorphism.

The Kuratowski–Zorn Principle

A subfamily $\mathcal{F}_0 \subseteq \mathcal{F}$ of a given family of sets $\mathcal{F}$ is called a chain if we have

$$A \subseteq B \quad \text{or} \quad B \subseteq A,$$

for any $A, B \in \mathcal{F}_0$.

The maximum principle of Kuratowski-Zorn states the following: If $\mathcal{F}$ is a family such that the union $\bigcup\{A_i\colon\ i \in I\}$ of any chain $\{A_i\colon\ i \in I\} \subseteq \mathcal{F}$ belongs to $\mathcal{F}$, then $\mathcal{F}$ has maximal elements (i.e. sets $A \in \mathcal{F}$ such that $A \subsetneq B$ holds for no $B \in \mathcal{F}$).

Now, let $\mathcal{F}$ be an arbitrary family of sets. A choice function for $\mathcal{F}$ is any function g defined on $\mathcal{F}$ such that $g(A) \in A$, for each $A \in \mathcal{F}$. The axiom of choice says that every family $\mathcal{F}$ of nonempty sets has a choice function. In particular, there is always a choice function for the family $P(A) \setminus \{\emptyset\}$, of nonempty subsets of A, where A is any nonempty set.

Definitions by Induction

Let $\mathcal{F}$ be a family of sets. For every function $G\colon\ \mathcal{F} \longrightarrow \mathcal{F}$ there is a family $\{G^n\colon\ n \in N\}$ of all the iterations $G^n = G \circ \cdots \circ G$ (n-times). It follows that for every operation $G\colon\ \mathcal{F} \longrightarrow \mathcal{F}$ and every set $B \in \mathcal{F}$ there exists exactly one sequence $F\colon\ N \longrightarrow \mathcal{F}$ such that $F_0 = B$ and $F_{i+1} = G(F_i)$, for each $i \in N$. Further, it can be proved that for every set B there is a family $\mathcal{F}$ such that $B \subseteq \mathcal{F}$ and $\mathcal{F}^n \subseteq \mathcal{F}$, for every $n \in N$ (the latter property means that $\mathcal{F}$ is closed under formation of finite sequences).

Assume that a sequence $F\colon\ N \longrightarrow \mathcal{F}$ has the following property: For some set D,

$$F_{i+1} \subseteq D \times \bigcup_{n \in N} F_i^n \quad \text{for all } i \in N,$$

that is, F_{i+1} consists of some sequences of the form $\langle d, a_1, \ldots, a_n\rangle$, where $d \in D$ and $a_1, \ldots, a_n \in F_i$. We shall often make use of the following theorem.

Theorem. For an arbitrary function $H\colon\ D \times \bigcup_{n \in N} W^n \longrightarrow W$ and any $h\colon\ F_0 \longrightarrow W$ there exists exactly one function $g\colon\ \bigcup_{i \in N} F_i \longrightarrow W$ such that $g|F_0 = h$ and

$$g(d, a_1, \ldots, a_n) = H(d, g(a_1), \ldots, g(a_n))$$

for each $\langle d, a_1, \ldots, a_n\rangle \in F_i$, $i > 0$. Here, W is an arbitrary set.

Cardinal Arithmetic

The cardinality (power) of a set A is denoted by card A. Thus, card A = card B

means that there exists a one-to-one function f from A onto B and card $A \leq$ card B means that card $A =$ card B_0 for some subset $B_0 \subseteq B$ (which is equivalent to the existence of a one-to-one function g: $A \longrightarrow B$).

A set A is countable, card $A = \omega$, if card $A =$ card N; that is, A is of the same power as the set N of natural numbers. The following rules hold true, for any infinite sets $A_1, \ldots, A_n$:

$$\text{card } (A_1 \cup \cdots \cup A_n) = \text{card } (A_1 \times \cdots \times A_n) = \max\{\text{card } A_1, \ldots, \text{card } A_n\}.$$

If the sets A_i are all of the same power equal to card A for $i \in I$, then

$$\text{card } \bigcup_{i \in I} A_i = \max\{\text{card } I, \text{card } A\}.$$

It follows, for example, that card $\bigcup_{n \in N} A^n =$ card A, for any infinite set A.
The Cantor–Bernstein theorem states the following:

If $A \subseteq B \subseteq C$ and card $A =$ card C, then card $B =$ card $A (=$ card $C)$.

Classes

Intuitively, a class is a collection of objects which is too large (i.e., it has too many elements) to be a set. For example, the collection of all sets is a class, as the Russell paradox shows. Some other examples are the class of all orderings, the class of all groups, the class of all compact spaces. It is convenient to regard sets as classes and classes that are not sets are called then proper classes. Each formula $\phi(x)$ determines the class

$$\mathbb{K}_\phi = \{x : \phi(x)\},$$

consisting of all the xs with the property ϕ. The use of classes of this form is inessential, that is, does not lead out of the ordinary set theory (since statements about $\mathbb{K}_\phi$ can be replaced by equivalent statements about sets only). The union $A \cup B$, the intersection $A \cap B$, and the difference $A \setminus B$ of classes A, B are defined in an obvious way. Notice that

$$\mathbb{K}_\phi \cup \mathbb{K}_\psi = \mathbb{K}_{\phi \vee \psi}, \qquad \mathbb{K}_\phi \cap \mathbb{K}_\psi = \mathbb{K}_{\phi \wedge \psi}, \qquad \mathbb{K}_\phi \setminus \mathbb{K}_\psi = \mathbb{K}_{\phi \wedge \neg \psi}.$$

For a systematic exposition of set theory we refer the reader to Monk [M4], Vaught [V2], and Hayden and Kennison [HK]. An axiomatic theory of classes is developed in Kelley [K1].

This page intentionally left blank

I

MATHEMATICAL STRUCTURES AND THEIR THEORIES

This page intentionally left blank

1

RELATIONAL SYSTEMS

Relational systems (called also relational structures) are in common use in mathematics. Among the most familiar examples of relational systems are groups, rings, fields, linear spaces, modules, and so on. Thus, in any branch of mathematics we are concerned with a particular kind of relational structures (the terms *relational structure* and *relational system* will be used interchangeably). We can even say that relational structures are the main subject of interest in mathematical research.

The main subject of mathematical logic is a connection between semantics and syntax. To put it more directly, mathematical logic investigates the relationship between relational systems and formulas (expressing properties of elements in the system). Hence, relational systems and formulas are two fundamental notions of mathematical logic.

First, we shall be dealing with relational systems. Formulas will be introduced in Chapter 5.

Now we pass to the precise definition. First, let us recall the general notion of a relation with a finite number of arguments.

Let A be an arbitrary nonempty set. For any integer $n \geq 1$ we can form the product

$$A^n = A \times \cdots \times A \quad n \text{ times.}$$

The set A^n consists of all n-termed sequences $\langle a_1, \ldots, a_n \rangle$, where $a_i \in A$ for $i = 1, \ldots, n$.

Every subset $r \subseteq A^n$ is called then an *n-ary relation* on the set A. According to generally accepted notation, we write

$$r(a_1, \ldots, a_n), (r \text{ holds for the } a_1, \ldots, a_n) \quad \text{if } \langle a_1, \ldots, a_n \rangle \in r.$$

and

$$\text{not } r(a_1, \ldots, a_n), (r \text{ does not hold for the } a_1, \ldots, a_n) \quad \text{if } \langle a_1, \ldots, a_n \rangle \notin r.$$

In the case of $n = 1$ the set A^1 can be identified with the set A (identifying the sequence $\langle a \rangle$ with the element a). Consequently, unary relations r on A will be identified with subsets $r \subseteq A$.

We shall often write r^A to indicate that r is a relation on the set A. Every function

$$f\colon\ A^n \longrightarrow A$$

defined on the product A^n and assuming its values in the set A is called also an *n-ary operation* on the set A. Similarly, for relations we shall often write f^A to emphasize that f is an n-ary operation on the set A, for some $n \geq 1$.

A relational system is a nonempty set A jointly with some selected relations and operations on A and some elements of A. More exactly, a relational system $\mathbf{A}$ is given by

1.1 $$\mathbf{A} = \langle A,\ \mathcal{R},\ \mathcal{F},\ C \rangle,$$

where A is a nonempty set called the *universe* of $\mathbf{A}$, $\mathcal{R}$ is a family of finitary relations on A, $\mathcal{F}$ is a family of operations on A, and $C \subseteq A$ is a subset of A. The elements $a \in C$ are called *distinguished elements* of the system $\mathbf{A}$.

As already mentioned, relational systems are also called relational structures. We shall use also shorter terms: *a system* or *a structure*. The definition is due to Tarski [T1].

Now, let us comment on this definition. We pose no limitations on the number of relations, operations, or distinguished elements of $\mathbf{A}$—the families $\mathcal{R}, \mathcal{F}, C$ can be finite or infinite of arbitrary cardinality. It is often convenient to represent $\mathcal{R}, \mathcal{F}, C$ as indexed families. In this case, consequently accepted throughout this book, the system 1.1 can be written in the form

1.2 $$\mathbf{A} = \langle A,\ \{r_i^A :\ i \in I\}, \{f_j^A :\ j \in J\}, \{c_k^A :\ k \in K\} \rangle,$$

for some sets I, J, K of indices. We do not assume that the above enumeration is one-to-one. If $\mathbf{A}$ has finitely many relations, operations, and distinguished elements and, for example, $I = \{1, \ldots, n\}$, $J = \{1, \ldots, m\}$, and $K = \{1, \ldots, l\}$, then we write

$$\mathbf{A} = \langle A,\ r_1^A, \ldots, r_n^A, f_1^A, \ldots, f_m^A, c_1^A, \ldots, c_l^A \rangle.$$

Of course, we shall omit the indices, if there is no fear of misunderstanding. We say that $\mathbf{A}$ is finite or infinite if the universe A is finite or infinite, respectively. More generally, by the cardinality of $\mathbf{A}$, card $\mathbf{A}$, we mean the cardinality of the universe A.

Let us note that some of the sets $\mathcal{R}, \mathcal{F}, C$ can be empty. If, for instance, $\mathcal{F} = C = \emptyset$, then $\mathbf{A}$ has relations only and in this case $\mathbf{A}$ is called a *pure* relational system. If $\mathcal{R} = \emptyset$, that is, $\mathbf{A}$ has operations and (possibly) distinguished elements, then $\mathbf{A}$ is said to be an *algebraic system* or in shortened form, an *algebra*).

Examples

The system $\langle N, \leq \rangle$, of nonnegative integers with the usual ordering is an example of a pure relational system. It belongs to the class $\mathbb{K}_0$ of all linear orderings (i.e., systems $\langle A, \leq^A \rangle$, where the relation $\leq^A$ linearly orders the set A). We have $\mathbb{K}_0 \subseteq \mathbb{K}_1$, where $\mathbb{K}_1$ consists of all systems $\langle X, r \rangle$, where r is a binary relation on X.

Any group $\langle G, \cdot, 1 \rangle$ and any ring $\langle P, +, \cdot, 0, 1 \rangle$ are examples of algebraic systems. The class of all groups is contained in the class of all algebras with one binary operation and one distinguished element.

Similarly, the class of all rings is a subclass of the class of all algebras with two binary operations and two distinguished elements.

The field $\mathbb{R} = \langle R, \leq, +, \cdot, 0, 1 \rangle$ of real numbers with the usual ordering is an example of a general relational system. $\mathbb{R}$ belongs to the class of all ordered fields, that is, systems

$$\langle F, \leq, +, \cdot, 0, 1 \rangle$$

such that the algebra $\langle F, +, \cdot, 0, 1 \rangle$ is a field, the relation $\leq$ linearly orders F and is congruent with the field operations; the latter condition means that for any $a, b \in F$,

$$a \leq b \quad \text{implies} \quad a + x \leq b + x \quad \text{for all } x \in F.$$

and

$$a \leq b \quad \text{implies} \quad a \cdot x \leq b \cdot x, \quad \text{for all } x \geq 0.$$

1.3. The Type of a System

For any relation r on the set A we let $\arg(r)$ denote the number of arguments of r. Similarly, we define $\arg(f)$, for any operation f on A. Thus, for any integer $n \in \omega$, we have

$$\arg(r) = n \quad \text{if and only if} \quad r \subseteq A^n$$

and

$$\arg(f) = n \quad \text{if and only if} \quad \operatorname{dom}(f) = A^n.$$

Let $\mathbf{A}$ be a structure of the form 1.2. The type $\tau = \tau(\mathbf{A})$ of the structure $\mathbf{A}$ is defined as the triple

$$\tau = \langle \langle \arg(r_i^A) : i \in I \rangle, \langle \arg(f_j^A) : j \in J \rangle, K \rangle.$$

Thus, the type of $\mathbf{A}$ says what the arity (i.e., the number of arguments) of any

relation and operation of $\mathbb{A}$ is. Also, τ says whether A has distinguished elements and how they are enumerated. For example, the type of a linear ordering can be described informally as "one binary relation," that of a ring as "two binary operations and two distinguished elements," and so on.

Let us assume now that $\mathbb{A}$ and $\mathbb{B}$ are of the same type τ, that is, $\tau(\mathbb{A}) = \tau(\mathbb{B})$. If $\mathbb{A}$ is such as in 1.2, then it follows that $\mathbb{B}$ has the form

$$\mathbb{B} = \langle B,\ \{r_i^B\colon\ i \in I\}, \{f_j^B\colon\ j \in J\}, \{c_k^B\colon\ k \in K\}\rangle$$

and the equalities

$$\text{1.4} \qquad \arg(r_i^A) = \arg(r_i^B), \qquad \arg(f_j^A) = \arg(f_j^B)$$

hold for all $i \in I$ and $j \in J$, respectively. Thus, any two structures $\mathbb{A}$ and $\mathbb{B}$ of a common type are built up in a similar way, in the sense that 1.4 holds (obviously, besides this, $\mathbb{A}$ and $\mathbb{B}$ can be totally different).

Usually, in a given branch of mathematics we investigate one particular structure (e.g., the ordered ring $\mathbb{Z}$ of integers, the field $\mathbb{C}$ of complex numbers, the three-dimensional Euclidean space) or the whole class of structures having some common properties (e.g., the class of partial orderings, the class of abelian groups, the class of rings of polynomials, the class of Banach spaces). In the latter case the structures under consideration are of some common type τ; that is, they constitute a subclass of the class $\mathbb{K}(\tau)$ consisting of all structures of type τ. We shall see later that any class $\mathbb{K}(\tau)$ has its logical language $L(\tau)$ (defined in Chapter 5), so that the formulas of $L(\tau)$ are interpretable in any structure $\mathbb{A} \in \mathbb{K}(\tau)$.

EXERCISES

1.1. Let τ be an arbitrary type. Show that the class $\mathbb{K}(\tau)$ (of all structures of type τ) contains structures of every (finite or infinite) cardinality ≥ 1. More generally, for every set $A \neq \emptyset$, there is a structure $\mathbb{A} \in \mathbb{K}(\tau)$ with the universe A.

1.2. Let A be a finite set, card $A = n$, and fix an integer $m \geq 1$.

(a) What is the number of systems of the form $\langle A, r\rangle$, with $\arg(r) \leq m$.

(b) What is the number of systems of the form $\langle A, f\rangle$, with $\arg(f) \leq m$.

2

BOOLEAN ALGEBRAS

The notion of a Boolean algebra is strictly connected with the logical calculus. It was introduced by Boole in the mid-ninteenth century and defined in full generality by Huntington in 1904; see [H3]. Later Boolean algebras were studied by Stone in the 1930s; see [S6], [S7]. The study of Boolean algebras is inspired not only by logic but also by other branches of mathematics, for example, set theory, measure theory, algebra, and topology. The main examples of Boolean operations are logical connectives (disjunction, conjunction, negation) and set theoretical operations (union, intersection, complementation).

Let us consider an algebraic system

$$\mathbb{A} = \langle A, +, \cdot, -, \mathbb{0}, \mathbb{1} \rangle$$

in which the operations "$+$" and "$\cdot$" are binary, the operation "$-$" is unary, and the distinguished elements $\mathbb{0}$ and $\mathbb{1}$ are assumed to be distinct. A system of this form is called a *Boolean algebra* if the following conditions hold (for any $a, b, c \in A$):

2.1.

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

The elements $a+b$ and $a\cdot b$ are called the (*Boolean*) sum and product of the elements a, b, respectively, $-a$ is called the *Boolean complementation* of the element a, and $\mathbb{0}$ and $\mathbb{1}$ are called the *zero* and *unit*.

Example. (The power-set algebra). Let $A = P(X)$ be the family of all the subsets of a nonempty set X. The Boolean operations are defined as the usual set theoretical operations

$$a+b = a \cup b, \qquad a\cdot b = a \cap b \quad \text{and} \quad -a = X \setminus a.$$

Moreover, we put $\mathbb{0} = \emptyset$ (the empty set) and $\mathbb{1} = X$. By well-known laws of the algebra of sets, we infer that the so defined power-set algebra $P(X)$ is a Boolean algebra. More generally, any field of sets, that is, a family $R \subseteq P(X)$ containing $\emptyset$ and X and closed under union, intersection, and complementation (with respect to X) is a Boolean algebra. In particular, the two-element family $R = \{\emptyset, X\}$ is a field of sets.

Now we shall derive from the axioms 2.1 some laws that are true in any Boolean algebra.

2.2 $\qquad a + a = a \quad \text{and} \quad a \cdot a = a.$

Proof. We have

$$a = a + \mathbb{0} = a + [a \cdot (-a)] = (a + a)[a + (-a)] = (a + a) \cdot \mathbb{1} = a + a.$$

Similarly,

$$a = a \cdot \mathbb{1} = a \cdot [a + (-a)] = a \cdot a + a \cdot (-a) = a \cdot a. \quad \square$$

Let us note that from 2.2 we get

$$a + \mathbb{1} = \mathbb{1} \quad \text{and} \quad a \cdot \mathbb{0} = \mathbb{0}.$$

Because

$$a + \mathbb{1} = a + [a + (-a)] = (a + a) + (-a) = a + (-a) = \mathbb{1}$$

and

$$a \cdot \mathbb{0} = a \cdot (a \cdot (-a)) = (a \cdot a) \cdot (-a) = a \cdot (-a) = \mathbb{0}.$$

For arbitrary sets a, b, the conditions $a \cup b = b$ and $a \cap b = a$ are equivalent and characterize the inclusion $a \subseteq b$. Similarly, in an arbitrary Boolean algebra we have

2.3 $\qquad$ *The conditions $a + b = b$ and $a \cdot b = a$ are equivalent.*

Proof. Multiplying both sides of the equality $a + b = b$ by a we get

$$a \cdot b = a \cdot (a + b) = (a \cdot a) + (a \cdot b) = a + (a \cdot b) = a \cdot (\mathbb{1} + b) = a \cdot \mathbb{1} = a.$$

Conversely, by adding b to both sides of $a \cdot b = a$, we obtain

$$a + b = a \cdot b + b = (a + \mathbb{1}) \cdot b = \mathbb{1} \cdot b = b. \quad \square$$

The above remarks suggest the following definition.

Definition. In any Boolean algebra we define a binary relation $\leq$ as follows:

$$a \leq b \quad \text{if and only if} \quad a + b = b.$$

By 2.3 we can write

$$a \leq b \text{ if and only if } a \cdot b = a.$$

If the algebra is a field of sets, then the relation $\leq$ coincides with the inclusion. In the general case

2.4 *the relation $\leq$ is a partial ordering.*

Proof. We have $a \leq a$, since always $a + a = a$, by 2.2. Assume that $a \leq b$ and $b \leq a$, that is, $a + b = b$ and $b + a = a$. Hence, we get immediately $a = b$. If $a \leq b$ and $b \leq c$, then

$$a + c = a + (b + c) = a + b + c = b + c = c,$$

and thus $a \leq c$. □

2.5 *From $a \leq b$ it follows that $a + x \leq b + x$ and $a \cdot x \leq b \cdot x$, for all x.*

Proof.

$$(a + x) + (b + x) = (a + b) + (x + x) = b + x$$

and

$$(a \cdot x) \cdot (b \cdot x) = (a \cdot b) \cdot (x \cdot x) = a \cdot x. \quad \square$$

From the already known laws $\mathbb{0} + a = a$ and $a + \mathbb{1} = \mathbb{1}$, we infer

$$\mathbb{0} \leq a \leq 1 \quad \text{for any } a,$$

that is, $\mathbb{0}$ is the least and $\mathbb{1}$ is the greatest element of the algebra.

Now, we prove the "lattice" property of $\leq$.

2.6 $$a + b = \sup\{a, b\} \quad \textit{and} \quad a \cdot b = \inf\{a, b\}.$$

Proof. Since $a + (a + b) = (a + a) + b = a + b$, we have $a \leq a + b$. Similarly, $b \leq a + b$. If x is such that $x \geq a$ and $x \geq b$, then

$$(a + b) + x = a + (b + x) = a + x = x,$$

that is, $a + b \leq x$. Hence, $a + b$ is the least upper bound of the set $\{a, b\}$, that is, $a + b = \sup\{a, b\}$. The other equality can be proved similarly. □

From 2.6, by an easy induction, we infer

$$a_1 + \cdots + a_n = \sup\{a_1, \ldots, a_n\}$$

$$a_1 \cdot \cdots \cdot a_n = \sup\{a_1, \ldots, a_n\}$$

for any elements $a_1, \ldots, a_n \in A$, while for infinite sets $Z \subseteq A$, the bounds $\sup Z$ and $\inf Z$ need not exist.

The following theorem characterizes the Boolean complement.

2.7 *If* $a + x = \mathbb{1}$ *and* $a \cdot x = \mathbb{0}$ *then* $x = -a$.

Proof. Using the assumption $a + x = \mathbb{1}$ we get

$$(-a) + x = [(-a) + x] \cdot (a + x) = (-a) \cdot a + x \cdot a + (-a) \cdot x + x \cdot x$$

$$= (a + (-a)) \cdot x + x = x + x = x,$$

that is, $-a \leq x$. On the other hand, using $a \cdot x = \mathbb{0}$,

$$x \cdot (-a) = x \cdot (-a) + x \cdot a = x \cdot ((-a) + a) = x \cdot \mathbb{1} = x,$$

that is $x \leq -a$. Thus $x = -a$. □

Double complementation acts as identity; that is,

2.8 $$-(-a) = a.$$

Proof. In 2.7 we substitute $-a$ for a and put $x = a$ □

From 2.7 we also get $-\mathbb{1} = \mathbb{0}$ and $-\mathbb{0} = \mathbb{1}$.

The De Morgan rules known from elementary logic or set theory can be stated in Boolean terms as follows:

2.9 $$-(a + b) = (-a)(-b) \quad \textit{and} \quad -(ab) = (-a) + (-b).$$

Proof. To obtain the first equality, substitute $x = (-a)(-b)$ in 2.8, replacing a by $a + b$. The other equality can be proved in a similar way. □

The De Morgan rules 2.9 can be generalized (by an obvious induction) to an arbitrary finite number of elements,

$$-(a_1 + \cdots + a_n) = (-a_1) \cdot \cdots \cdot (-a_n)$$