The Structure of the REAL NUMBER SYSTEM

THE UNIVERSITY SERIES IN UNDERGRADUATE MATHEMATICS

Editors

John L. Kelley, *University of California*
Paul R. Halmos, *University of Indiana*

PATRICK SUPPES—Introduction to Logic
PAUL R. HALMOS—Finite-Dimensional Vector Spaces, 2nd Ed.
EDWARD J. MCSHANE and TRUMAN A. BOTTS—Real Analysis
JOHN G. KEMENY and J. LAURIE SNELL—Finite Markov Chains
PATRICK SUPPES—Axiomatic Set Theory
PAUL R. HALMOS—Naive Set Theory
JOHN L. KELLEY—Introduction to Modern Algebra
IVAN NIVEN—Calculus: An Introductory Approach, 2nd Ed.
A. SEIDENBERG—Lectures in Projective Geometry
MAYNARD J. MANSFIELD—Introduction to Topology
FRANK M. STEWART—Introduction to Linear Algebra
LEON W. COHEN and GERTRUDE EHRLICH—The Structure of the Real Number System
ELLIOTT MENDELSON—Introduction to Mathematical Logic
HERMAN MEYER—Precalculus Mathematics
ALBERT G. FADELL—Calculus with Analytic Geometry
JOHN L. KELLEY—Algebra: A Modern Introduction
ANNITA TULLER—A Modern Introduction to Geometries
K. W. GRUENBERG and A. J. WEIR—Linear Geometry
HOWARD LEVI—Polynomials, Power Series, and Calculus
ALBERT G. FADELL—Vector Calculus and Differential Equations
EDWARD R. FADELL and ALBERT G. FADELL—Calculus

The Structure of the REAL NUMBER SYSTEM

by

LEON W. COHEN
Professor of Mathematics, University of Maryland

and

GERTRUDE EHRLICH
Associate Professor of Mathematics, University of Maryland

Van Nostrand Reinhold Company
New York Cincinnati Toronto London Melbourne

VAN NOSTRAND REINHOLD COMPANY REGIONAL OFFICES:
Cincinnati New York Chicago Millbrae Dallas

VAN NOSTRAND REINHOLD COMPANY INTERNATIONAL OFFICES:
London Toronto Melbourne

Published by VAN NOSTRAND REINHOLD COMPANY
450 West 33rd Street, New York, N.Y. 10001

Published simultaneously in Canada by
D. VAN NOSTRAND COMPANY (Canada), LTD.

10 9 8 7 6 5 4

PREFACE

The present course of mathematical education in school and college introduces a student rather casually to the various properties of integers, rational numbers, and real numbers as they are needed for arithmetic, algebra, geometry, and calculus. Sometimes the relations among these mathematical structures are sketched as indications of things to come in mathematics. When the student begins graduate study he finds that he is expected to be familiar with the structure of the real number system. If his graduate courses deal explicitly with this system at all, they usually do so in terms of a brief summary. It is then assumed that the student has a usable knowledge of the intricately interwoven properties of set theory, algebra and topology which characterize the system of real numbers. Actually, this assumption is frequently false and a gap is left in the student's knowledge which, if not filled, hinders his development.

This little book, it is hoped, will help fill the gap as a text either for independent study or for a semester course. The exercises in each chapter extend and illustrate the main line of the theory. Some of the exercises are referred to in proofs of theorems. In such cases, we have identified them thus: ●

The authors are indebted to many colleagues for helpful criticism while the manuscript was being used as the basis for a course. Mrs. Mary Gray provided indispensable and sympathetic assistance in typing the several revisions of the manuscript.

LEON W. COHEN
GERTRUDE EHRLICH

June 1963
College Park, Maryland

CONTENTS

CHAPTER 0

INTRODUCTION

Preliminaries. It may just as well be understood that one cannot begin a discussion of mathematics, or even of a portion of mathematics, at the beginning. One may look for such a beginning by setting down, in the conventional manner, undefined terms, unproved propositions, and a proof scheme. The hope that a tidy mathematics might be deducible in this way is implicit in Euclid's geometry. The search for an axiomatic system which might provide a foundation for all of mathematics and a proof of its own consistency continued through the first third of this century.

But there were essential difficulties. The operation of a formal mathematical system requires some instructions stated in a language outside the system. It has been known since 1932 that, even if such instructions are admitted as understood, no system adequate for the most familiar part of mathematics, the arithmetic of the whole numbers, can be proved to be consistent. Thus, one must be content to begin somewhere in the middle, using the axiomatic method, in spite of its limitations, as a means of organizing portions of mathematical knowledge.

The real number system has strong claims to a central position in mathematics. It is the point of departure for the vast field of mathematics called "analysis." Together with its subsystems, the real number system provides models and techniques for much of set theory, algebra, geometry, and topology. It was the critical study of the real numbers, requiring the re-examination and reconstruction of logic, which finally ended the hope of finding a beginning. Because the germ of so much mathematics lies concealed within the real numbers, we hope that this book will serve not only as an introduction but as an invitation to mathematics.

As concepts are defined in the following pages, examples will be

given either to illustrate or to motivate them. The examples will be drawn from familiar mathematical discourse as well as from non-mathematical experience. Strictly, the only examples of mathematics are concepts and relations expressed in the terms, axioms, and theorems of mathematics. In fact, however, these constituents of mathematics are usually abstracted from experience, and experience includes what may be called familiar mathematics. There seems to be an historical cycle in which the strict mathematics of one epoch becomes the familiar mathematics on the basis of which a stricter, more inclusive, mathematics is later formalized. From this point of view it is not strange that the familiar Cartesian plane serves as an example motivating the definition of a Cartesian product in terms of which the Cartesian plane is formally defined. Put briefly, the problem as to which of "abstraction", "experience", is "chicken", "egg" is not resolved.

Set Theory. The fundamental concepts of mathematics may be expressed in the terminology of set theory. We collect in this chapter some facts of the theory of sets which will be used later.*

The terms "set" and "element of a set" will not be defined. Although the mathematical objects treated in this book will all be sets, we shall, in some contexts, explicitly refer to a set as a "set of sets." Sets will usually be denoted by capital letters; but when a set occurs as an element of another set, we may denote it by a small letter. We write "$a \in A$" if a is an element of A, "$a \notin A$" if a is not an element of A, and denote by the symbol "$\{a, b, c, \ldots\}$" the set whose elements are $a, b, c, \ldots$. (If $A \in B$ and $B \in C$, it does not follow that $A \in C$. For example, if the United Nations is a set whose elements are the member nations, and a nation is a set whose elements are its citizens, then Dieudonné is an element of France, France is an element of the United Nations, but Dieudonné is not an element of the United Nations.)

AXIOM OF EXISTENCE *There is a set.*

AXIOM OF IDENTITY *If A, B are sets then A and B are the same set if and only if every element of A is an element of B, and every element of B is an element of A.*

* A more extensive account of the subject at an appropriate level is found in *Naive Set Theory*, by P. Halmos (D. Van Nostrand Co., Inc., Princeton, N.J., 1960), from which we take some of our undefined terms, axioms, and definitions.

We write "$A = B$" if A and B are the same set, "$A \neq B$" if A and B are not the same set. At times, we shall find it convenient to use the symbol for an element of a set repeatedly. Thus, for example, the symbols "$\{a, a, a, b\}$," "$\{a, a, b\}$," "$\{a, b\}$" will all denote the same set.

DEFINITION 0.1 Set B is a *subset* of set A if $b \in A$ for all elements b of B. If B is a subset of A, we write "$B \subset A$" or "$A \supset B$". If $B \subset A$ and $B \neq A$, then B is a *proper subset* of A.

For example, the set of all even integers is a proper subset of the set of all integers. The set of all Caucasians is a proper subset of the set of all human beings. The set consisting of Great Britain and $\sqrt{2}$ is a proper subset of the set consisting of Great Britain, $\sqrt{2}$, and the moon.

•*Exercise* 0.1 If A is a set, then $A \subset A$.

•*Exercise* 0.2 If A, B are sets, then $A = B$ if and only if $A \subset B$ and $B \subset A$.

•*Exercise* 0.3 If A, B, C are sets such that $A \subset B$ and $B \subset C$, then $A \subset C$.

We observe that, in the examples of subsets given above, each subset is determined by a condition imposed on the elements of the original set. The subset of all even integers is determined by the condition "x is even" imposed on x, where x is an integer; the subset of all Caucasians by the condition "x is Caucasian" imposed on x, where x is a human being; the subset consisting of Great Britain and $\sqrt{2}$ by the condition "x is Great Britain or $\sqrt{2}$" imposed on x, where x is Great Britain, $\sqrt{2}$, or the moon.

AXIOM OF SPECIFICATION *If A is a set and $Q(x)$ is a condition, then there is a subset B of A whose elements are exactly those elements x of A for which the condition $Q(x)$ holds.*

The subset B is said to be *determined* (or *specified*) by the condition $Q(x)$. By the Axiom of Identity, if B and B' are subsets of A determined by a condition $Q(x)$, then $B = B'$. We shall say: "a unique subset B of A is determined by $Q(x)$", and write

$$B = \{x \mid Q(x), x \in A\}, \text{ or simply } B = \{x \mid Q(x)\}.$$

THEOREM 0.1 *There is a set which has no elements.*

PROOF: By the Axiom of Existence, there is a set. Let A be a set, and let $Q(x)$ be the condition: "$x \notin A$". By the Axiom of Specification, there is a subset E of A consisting of all elements x of A which satisfy the condition "$x \notin A$". Since no element of A satisfies this condition, the set E has no elements.

A set which has no elements is called an *empty set.*

THEOREM 0.2 *If E and E' are empty sets, then $E = E'$.*

PROOF: Suppose $E \neq E'$. Then one of the following statements must be true:

(1) There is an element $x \in E$ such that $x \notin E'$.
(2) There is an element $x \in E'$ such that $x \notin E$.

But both of these statements are false, since neither E nor E' has any elements. It follows that $E = E'$.

In view of Theorem 0.2, we shall speak of "*the* empty set". We denote this set by "$\varnothing$".

Exercise 0.4 If A is any set, then $\varnothing \subset A$.

It is useful to have available certain ways of combining sets to form new sets.

AXIOM OF UNIONS *If C is a set of sets,* then there is a set B such that $x \in B$ if $x \in A$ for some $A \in C$.*

THEOREM 0.3 *If C is a set of sets, then there is a unique set Σ such that $x \in \Sigma$ if and only if $x \in A$ for some $A \in C$.*

PROOF: By the Axiom of Unions there is a set B such that $x \in B$ if $x \in A$ for some $A \in C$. By the Axiom of Specification, there is a unique subset Σ of B determined by the condition "$x \in A$ for some $A \in C$". (Note: Σ does not depend on the choice of B. Why?)

DEFINITION 0.2 The set Σ of Theorem 0.3 is called the *union* of the sets A of C. We write "$\bigcup_{A \in C} A$" for Σ.

* *Caution:* A set C of *all* sets is inadmissible! For, the condition $Q(x)$: "x is a set in C such that $x \notin x$" specifies a subset D of C whose elements x do not contain themselves as elements. But if $D \in D$, then $D \notin D$; and if $D \notin D$, then $D \in D$. This contradiction is unavoidable if a "set of all sets" is admitted.

If A and B are sets, we have as yet nothing to tell us if there is a set with A and B as elements. This is embarrassing if we wish to consider the union of A and B. The following axiom permits us to do so.

AXIOM OF PAIRS *If A and B are sets, there is a set C such that $A \in C$ and $B \in C$.*

Now, by the Axiom of Specification, there is a subset of C consisting of just A and B. This set $\{A, B\}$ is called a *pair*. If $A = B$, then the pair $\{A, B\} = \{A, A\} = \{A\}$ is called the *singleton* of A.

Exercise 0.5 If A and B are sets, then there is a set which is the union of A and B. We denote the union of A and B by the symbol: "$A \cup B$".

Exercise 0.6

(a) If A and B are sets, $A \cup B = B \cup A$.

(b) If A, B, C are sets, $A \cup (B \cup C) = (A \cup B) \cup C$.

Exercise 0.7 Let C be a set. If $\Sigma = \bigcup_{A \in C} A$, then

(1) $A \subset \Sigma$ for all $A \in C$.

and

(2) $\Sigma \subset B$ for every set B such that $A \subset B$ for all $A \in C$.

Exercise 0.8 Let C be a set. If Σ is a set satisfying the conditions:

(1) $A \subset \Sigma$ for all $A \in C$

and

(2) $\Sigma \subset B$ for every set B such that $A \subset B$ for all $A \in C$,

then $\Sigma = \bigcup_{A \in C} A$.

In the sense of Exercises 0.7 and 0.8, the union of the sets A in a set C is the "smallest" set which includes all the sets A as subsets.

THEOREM 0.4 *If C is a set of sets, then there is a unique set Π such that $x \in \Pi$ if and only if $x \in A$ for all $A \in C$.*

PROOF: The condition $Q(x)$: "$x \in A$ for all $A \in C$" determines a unique subset of the set $\bigcup_{A \in C} A$. This is the required set Π.

DEFINITION 0.3 The set Π of Theorem 0.4 is called the *intersection* of the sets A of C. We write "$\bigcap_{A \in C} A$" for Π.

Exercise 0.9 If A and B are sets, then there is a set which is the intersection of A and B.

We denote the intersection of A and B by the symbol: "$A \cap B$". If $A \cap B = \emptyset$, we say that A and B are *disjoint.*

Exercise 0.10

(a) If A and B are sets, $A \cap B = B \cap A$.
(b) If A, B, C are sets, $A \cap (B \cap C) = (A \cap B) \cap C$.
(c) If A, B, C are sets, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Exercise 0.11 Let C be a set. If $\Pi = \bigcap_{A \in C} A$, then

(1) $\Pi \subset A$ for all $A \in C$

and

(2) $B \subset \Pi$ for every set B such that $B \subset A$ for all $A \in C$.

Exercise 0.12 Let C be a set. If Π is a set satisfying the conditions:

(1) $\Pi \subset A$ for all $A \in C$

and

(2) $B \subset \Pi$ for every set B such that $B \subset A$ for all $A \in C$, then $\Pi = \bigcap_{A \in C} A$.

In the sense of Exercises 0.11 and 0.12, the intersection of the sets A in a set C is the "largest" set which is a subset of every $A \in C$.

Exercise 0.13 If A, B are sets, then $A \subset B$ if and only if $A \cup B = B$.

Exercise 0.14 If A is a set, then $A \cap B = A$ for all subsets B of a set C if and only if $A = \emptyset$.

Exercise 0.15 If A is a set, then $A \cup B = B$ for all subsets B of a set C if and only if $A = \emptyset$.

We shall use "$A - B$" to denote $\{x \mid x \in A \text{ and } x \notin B\}$

Exercise 0.16

(a) $A - B = A - (A \cap B)$
(b) $A - B = \emptyset$ if and only if $A \subset B$.

AXIOM OF POWERS *If A is a set, there is a set $P(A)$ (called the power set of A) whose elements are the subsets of A.*

For example, the power set of the set whose elements are a, b, c is the set whose elements are

$$\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{b, c\},\ \{c, a\},\ \{a, b, c\}.$$

Exercise 0.17 The power set of a set of n elements contains 2^n elements.

If $a \in A$, then one of the subsets of A is the singleton $\{a\}$. We note that if $a \in A$, then $\{a\} \subset A$ and $\{a\} \in P(A)$. If $a \in A$ and $b \in B$, then the pair $\{a, b\}$ is a subset of $A \cup B$ and an element of $P(A \cup B)$.

A very useful concept is that of "ordered pair". The coordinates (x, y) of a point in the plane, for example, form an ordered pair. To specify a point P in the plane, it is sufficient to state which two numbers will serve as the coordinates of P and which one of these two numbers will be the x-coordinate. In the symbol (3, 2), the x-coordinate is *singled out* by being written first. A definition of "ordered pair" which makes use of the idea of singling out one of the elements of a pair without presupposing any notion of "first" or "second" was given by Norbert Wiener:

> DEFINITION 0.4 If $a \in A$ and $b \in B$, then the *ordered pair* (a, b) is the set $\{\{a\}, \{a, b\}\}$ consisting of the pair $\{a, b\}$ and the singleton $\{a\}$.*

This definition has the advantage of presupposing only the set axioms so that such concepts as order and mapping can later be defined in terms of "ordered pair" without danger of circularity.

The most important fact about Definition 0.4 is that the ordered pairs so defined behave exactly as ordered pairs should:

> THEOREM 0.5 *Two ordered pairs* (a, b) *and* (a', b') *are equal if and only if* $a = a'$, *and* $b = b'$.

PROOF: If $a = a'$ and $b = b'$, then, by the Axiom of Identity,

$$(1)\quad \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}.$$

Conversely, suppose that (1) holds. If $a = b$, then, by Definition 0.4, and by the agreement on notation (page 3),

$$(a, b) = (a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\} = \{\{a'\}, \{a', b'\}\}.$$

* We note that if $a = b$, then $(a, b) = (a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$. This result may seem strange, but it does no harm.

By the Axiom of Identity, $a = a' = b'$. Since $a = b$, $a = a'$ and $b = b'$. If $a \neq b$, then, by the Axiom of Identity, $\{a, b\} \neq \{a'\}$. Hence

$$\{a, b\} = \{a', b'\}, \quad \text{and} \quad \{a\} = \{a'\}.$$

But then $a = a'$ and $b = b'$.

THEOREM 0.6 *If A and B are non-empty sets, then there is a set C consisting of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

PROOF: Each ordered pair $(a, b) = \{\{a\}, \{a, b\}\}$ is a subset of the power set $P(A \cup B)$. By the Axiom of Specification, the condition "x is an ordered pair (a, b) with $a \in A$ and $b \in B$" determines a subset C of the power set $P(P(A \cup B))$ of $P(A \cup B)$. The set C consists of all ordered pairs (a, b) with $a \in A$ and $b \in B$.

DEFINITION 0.5 The set C of Theorem 0.6 is called the *Cartesian product* of A and B. We denote it by "$A \times B$".

Example 1: If A and B are both the set of all real numbers, then $A \times B$ is the Cartesian plane. (The term "Cartesian product" is taken from this example.)

Example 2: If A is the set of all real numbers and B is the set of all integers, then $A \times B$ is the subset of the Cartesian plane consisting of all points lying on the lines $y = n$ where n is any integer.

Example 3: If A is the set of all positive integers and B is the set of all integers, then $A \times B$ is the set of all lattice points in the right half-plane.

Exercise 0.18

(a) If A, B, C are non-empty sets, then

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

(b) There are sets A, B, C such that

$$A \times (B \times C) \neq (A \times B) \times C.$$

Hint: use the fact that $\emptyset \neq \{\emptyset\}$.

(c) $A \times B = B \times A$ if and only if $A = B$.

In fact, the following statements are equivalent:

$$\begin{aligned} A \times B &\subset B \times A \\ B \times A &\subset A \times B \\ A \times B &= B \times A \\ A &= B. \end{aligned}$$

Relations, Mappings, Binary Operations. If A and B are sets, then a condition $Q(x)$ determines, by the Axiom of Specification, a subset R of $A \times B$ consisting of all ordered pairs $x = (a, b)$ for which the condition holds. Such a condition expresses what, in ordinary language, is called a relation between a and b. Examples are "a is less than b", "a equals b", "a is divorced from b". In mathematics it is convenient to identify the set R with the relation. In fact, if R is any subset of $A \times B$, one may think of the condition $Q(x)$: "$x \in R$" as expressing a relation between a and b, where $x = (a, b)$.

DEFINITION 0.6 A *binary relation* is a subset R of a Cartesian product $A \times B$. If $R \subset A \times A$, we call R a binary relation *in* A. If $(a, b) \in R$, we may write "$a\,R\,b$".

DEFINITION 0.7 Let R be a binary relation defined in a set A. Then,

(a) R is *reflexive* if $a\,R\,a$ holds for all $a \in A$.
(b) R is *symmetric* if $b\,R\,a$ holds whenever $a\,R\,b$ holds for $a, b \in A$.
(c) R is *transitive* if $a\,R\,c$ holds whenever $a\,R\,b$ and $b\,R\,c$ both hold for $a, b, c \in A$.
(d) R is *anti-symmetric* if $a = b$ whenever $a\,R\,b$ and $b\,R\,a$ both hold for $a, b \in A$.
(e) R satisfies the *law of trichotomy* if, for any $a, b \in A$, exactly one of $a\,R\,b$, $b\,R\,a$, and $a = b$ holds.

DEFINITION 0.8 If a binary relation R in a set A is reflexive, symmetric, and transitive, then it is called an *equivalence relation* in A.

The familiar numerical equality is an example of an equivalence relation. A further example is the number theoretic relation of congruence: in the set A of all integers, we may define a binary relation R such that $a\,R\,b$ holds if and only if 3 is a divisor of $b - a$. Since 3 is a divisor of $a - a$ for every $a \in A$, R is reflexive. If 3 is a divisor of $a - b$, then 3 is a divisor of $b - a$. Thus, R is symmetric. Suppose that 3 is a divisor of $b - a$ and also of $c - b$. Then 3 is a divisor of $(b - a) + (c - b) = c - a$. Thus, R is transitive. But then R is an equivalence relation in A. If $a\,R\,b$ holds for two integers a and b, we say that a is congruent to b modulo

3, and write "$a \equiv b \bmod 3$". For any non-zero integer m, an equivalence relation "congruence modulo m" may be similarly defined.

DEFINITION 0.9 If R is an equivalence relation defined in a set A, and a is any element of A, then the set C_a consisting of all $x \in A$ such that $x \, R \, a$ holds is called an *equivalence class* with respect to the relation R.

Let us determine the equivalence classes in the set A of all integers with respect to the relation "congruence modulo 3". The integers congruent to 0 modulo 3 form an equivalence class. The elements of this class are the multiples of 3, i.e., the integers expressible as $3k$ for some integer k. The integers congruent to 1 modulo 3 form another equivalence class. This class consists of all integers expressible as $3k + 1$ for some integer k. The integers congruent to 2 modulo 3 form a third equivalence class. This class consists of all integers expressible as $3k + 2$ for some integer k. However, every integer is expressible as $3k$, $3k + 1$, or $3k + 2$ for some integer k. Hence the three classes we have listed contain all the integers, and the set A, with respect to the relation "congruence modulo 3", is the union of three equivalence classes no two of which have any elements in common. This illustrates a very important general principle.

THEOREM 0.7 *If R is an equivalence relation in a set A, then A is the union of pairwise disjoint equivalence classes.*

PROOF: We show first that the set A is the union of all its equivalence classes. If $a \in A$, then $a \in C_a$ since $a \, R \, a$ holds, because of the reflexivity of R. But then A is a subset of $\bigcup_{a \in A} C_a$ which, in turn, is a subset of A. Hence $A = \bigcup_{a \in A} C_a$.

We show next that for $a, b \in A$, the equivalence classes C_a and C_b are either disjoint or equal. If $C_a \cap C_b \neq \emptyset$, there is an $x \in A$ satisfying $x \, R \, a$ and $x \, R \, b$. But then $a \, R \, x$ holds since R is symmetric, and hence $a \, R \, b$ holds since R is transitive. Now, if $a' \in C_a$, then from $a' \, R \, a$ and $a \, R \, b$ we have $a' \, R \, b$. Hence, $C_a \subset C_b$. Similarly, we may show that $C_b \subset C_a$. But then $C_a = C_b$.

It follows that A is the union of mutually disjoint equivalence classes.

The equivalence classes with respect to a relation R form a subset of the power set of A.

DEFINITION 0.10 If R is an equivalence relation in a set A, the set A/R of all equivalence classes with respect to R is called the *factor set of A modulo R.*

Exercise 0.19 If A is the union of pairwise disjoint non-empty subsets, then there is an equivalence relation R in A such that the given subsets form the factor set A/R.

For any set C, the set

$$\{(A, B) \mid A \subset B \text{ and } A, B \in P(C)\}$$

is a binary relation in $P(C)$. This relation is called "set inclusion". By Exercises 0.1, 0.2, and 0.3, it is reflexive, anti-symmetric, and transitive.

DEFINITION 0.11 If a binary relation in a set A is reflexive, anti-symmetric, and transitive, it is called a *partial order relation.*

The relation " $\leqq$ " for real numbers and the relation "is a divisor of" for positive integers are further examples of partial order relations.

Finally, " $<$ " for real numbers is an example of a third kind of relation.

DEFINITION 0.12 A binary relation R defined in a set A is called an *order relation* in A if it is transitive and satisfies the law of trichotomy. A set in which is defined an order relation is called an *ordered set.*

An important special kind of binary relation is called a *mapping.*

DEFINITION 0.13 If A and B are non-empty sets, then a *mapping F of A into B* (or: a *function F on A to B*) is a subset F of $A \times B$ satisfying the conditions:

(1) for each $a \in A$, $(a, b) \in F$ for some $b \in B$;
(2) if $(a, b) \in F$ and $(a, b') \in F$, then $b = b'$.

The sets A and B are, respectively, *domain* and *co-domain* of F. The set $B_F = \{b \mid (a, b) \in F\}$ is the *range* (or *image*) of F. If

$B_F = B$, then F is a mapping of A *onto* B. If $(a, b) \in F$ and $(a', b) \in F$ cannot both hold unless $a = a'$, then F is *one-to-one* (1–1).*

If F is a mapping of A into B, and $(a, b) \in F$, we write $b = F(a)$. Then for every $a \in A$ there is exactly one $b \in B$ such that $b = F(a)$. Conversely, if with every element $a \in A$, we associate in some manner exactly one element $F(a)$ belonging to B, then the set of all ordered pairs $(a, F(a))$ is clearly a mapping of A into B.

THEOREM 0.8 *Two mappings F and G of A into B are equal if and only if $F(a) = G(a)$ for every $a \in A$.*

PROOF: If $F = G$ and $(a, F(a)) \in F$, then $(a, F(a)) \in G$. But then, since $(a, G(a)) \in G$, we have $F(a) = G(a)$. (Thus far, we have used only the inclusion $F \subset G$.)

Conversely, if $F(a) = G(a)$ for every $a \in A$, then for each $(a, F(a)) \in F$, we have $(a, F(a)) = (a, G(a)) \in G$, so that $F \subset G$. Similarly, $G \subset F$. But then $F = G$.

Examples of mappings:

(1) If A is the set consisting of 2, -2, and 3, and B is the set of all positive integers, then the set F consisting of (2, 4), $(-2, 4)$, and (3, 9) is a mapping of A into B. This mapping may be described by the equation $F(a) = a^2$. In this case, F is neither 1–1 nor does it map A *onto* B.

(2) If we omit the pair $(-2, 4)$ from the set F in Example 1, we obtain a mapping F' of the set consisting of 2 and 3 into the set of all positive integers. This mapping F' is 1–1. (If, on the other hand, we were to add the pair $(2, -4)$ to the set F, we would no longer have a mapping!)

THEOREM 0.9 *If A, B, and C are sets, and if F is a mapping of A into B and G is a mapping of B into C, then there is a unique mapping H of A into C such that $H(a) = G(F(a))$ for every $a \in A$.*

PROOF: Let

$$H = \{(a, c) \mid c = G(F(a)) \text{ for some } a \in A\}.$$

* The following terms are currently coming into use: a mapping of A onto B is called a *surjection*. A 1–1 mapping of A into B is called an *injection*. A 1–1 mapping of A onto B is called a *bijection*.

Then $H \subset A \times C$. If $a \in A$, then $c = G(F(a)) \in C$, since F and G satisfy (1) of Definition 0.13. If $(a, c) \in H$ and $(a, c') \in H$, then $c = G(F(a)) = c'$, since F and G satisfy (2) of Definition 0.13. Hence H is a mapping of A into C. The condition "$c = G(F(a))$ for some $a \in A$" specifies a unique subset of $A \times C$. Thus H is the only mapping with the required properties.

DEFINITION 0.14 If F is a mapping of A into B, and G is a mapping of B into C, then the mapping H of A into C such that $H(a) = G(F(a))$ for every $a \in A$ is called the *composite* GF of F and G.

THEOREM 0.10 *Composition of mappings is associative, i.e., if F maps A into B, G maps B into C, and H maps C into D, then $(HG)F = H(GF)$.*

PROOF: For every $a \in A$, $[(HG)F](a) = (HG)(F(a)) = H(G(F(a)))$. Also for every $a \in A$, $[H(GF)](a) = H((GF)(a)) = H(G(F(a)))$. Hence, by Theorem 0.8, $(HG)F = H(GF)$.

DEFINITION 0.15 If F is a mapping of A into B and G is a mapping of B into A, then G is called an *inverse mapping* for F if $(GF)(x) = G(F(x)) = x$ for all $x \in A$ and $(FG)(y) = F(G(y)) = y$ for all $y \in B$.

THEOREM 0.11 *If F is a 1–1 mapping of A onto B, then F has a unique inverse mapping.*

PROOF: If F is a 1–1 mapping of A onto B, let

$$(1) \quad G = \{(b, a) \mid (a, b) \in F\}.$$

Then $G \subset B \times A$. If $b \in B$, then, since F maps A onto B, $(a, b) \in F$ for some $a \in A$. Hence, $(b, a) \in G$. If $(b, a) \in G$ and $(b, a') \in G$, then $(a, b) \in F$ and $(a', b) \in F$. Since F is 1–1, $a = a'$. Hence G is a mapping of B into A. By (1), $GF(a) = G(F(a)) = a$ for all $a \in A$, and $FG(b) = F(G(b)) = b$ for all $b \in B$. Thus, G is an inverse mapping for F.

Now let G' be any inverse mapping for F. Then, for all $b \in B$, $G'(b) = [G'(FG)](b) = [(G'F)G](b) = G(b)$. Hence $G = G'$.

Exercise 0.20

(1) If F is a 1–1 mapping of A onto B, then the inverse mapping G of F is a 1–1 mapping of B onto A.

(2) If F is a 1–1 mapping of A onto B and G maps B 1–1 onto C, then GF is a 1–1 mapping of A onto C.

Exercise 0.21 If G, G' are mappings of A into B, and F is either

(a) a 1–1 mapping of B into C such that $FG = FG'$

or

(b) a mapping of C onto A such that $GF = G'F$,

then $G = G'$.

Certain operations of familiar mathematics, e.g., addition and multiplication of numbers, vector addition, and multiplication of vectors by scalars, may be interpreted as mappings whose domain is the Cartesian product of two sets.

DEFINITION 0.16 If A, B, and C are sets, then any mapping of a non-empty subset of $A \times B$ into C is called a *binary operation* from $A \times B$ to C. In particular, if $A = B = C$, then any mapping of a non-empty subset of $A \times A$ into A is called a binary operation *in* A. A binary operation whose domain is the whole set $A \times A$ will be called a binary operation *on* A.

A binary operation $\circ$ from $A \times B$ to C associates with each ordered pair (a, b) in a subset of $A \times B$ a unique element $a \circ b$ of C. A binary operation *in* A associates with each ordered pair (a, a') in a subset of $A \times A$ a unique element $a \circ a'$ of A.

Example 1: If A is the set of all mappings of P into Q, and B is the set of all mappings of Q into T, then composition of mappings is a binary operation from $B \times A$ to C where C is the set of all mappings of P into T.

Example 2: If C is any set of sets such that for A, B in C, $A \cup B$ and $A \cap B$ also belong to C, then $\cup$ and $\cap$ are binary operations on C. In particular, if $P(A)$ is the set of all subsets of a given set A, then $\cup$ and $\cap$ are binary operations on $P(A)$.

Example 3: Familiar addition and multiplication of whole numbers are binary operations on the set of all whole numbers; familiar

subtraction and division are binary operations in, but not on, the set of whole* numbers.

Some important properties which a binary operation on a set A may or may not have are given in the following:

DEFINITION 0.17 A binary operation $\circ$ on A is

(a) *associative* if $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c, \in A$,
(b) *commutative* if $a \circ b = b \circ a$ for all $a, b \in A$.

DEFINITION 0.18 If A is a set, and $\circ$, $\circ'$ are binary operations on A, then $\circ'$ is

(1) *left-distributive over* $\circ$ if $a \circ' (b \circ c) = (a \circ' b) \circ (a \circ' c)$ for all $a, b, c \in A$;
(2) *right-distributive over* $\circ$ if $(b \circ c) \circ' a = (b \circ' a) \circ (c \circ' a)$ for all $a, b, c \in A$.
(3) *distributive over* $\circ$ if it is both left and right distributive over $\circ$.

We note that, if $\circ'$ is commutative, (1), (2), and (3) are equivalent.

Familiar addition and multiplication are both commutative and associative; familiar subtraction and division are neither; multiplication is distributive over addition, but addition is not distributive over multiplication.

Exercise 0.22 Which of the conditions of Definition 0.17 and 0.18 apply in Examples 1 and 2 above?

If C is a non-empty subset of A, then any mapping with domain A induces a mapping with domain C, and every binary operation on A induces a binary operation on C.

•*Exercise* 0.23 If F is a mapping of A into B, and C is a non-empty subset of A, then

$$\tilde{F} = \{(a, b) \mid (a, b) \in F \quad \text{and} \quad a \in C\}$$

is a mapping of C into B such that $F(a) = \tilde{F}(a)$ for all $a \in C$.

DEFINITION 0.19 The mapping $\tilde{F}$ of Exercise 0.23 is called the *restriction of the mapping* F to the subset C. If F is a binary operation on A, then the restriction of the mapping F to $C \times C$ is called the *restriction of the operation* F to C.

* We use the expression "whole numbers" to refer to the familiar positive numbers 1, 2, 3, ...

CHAPTER 1

THE NATURAL NUMBERS

Introduction. Familiar mathematics begins with the whole numbers. We give here a system of axioms from which the familiar properties of the whole numbers can be proved as theorems. For guidance in our choice of axioms, we examine the list of whole numbers

$$1, 2, 3, 4, \ldots.$$

We observe that every whole number has one, and only one, successor in the list, and that every whole number except 1 is the successor of one, and only one, whole number. We observe, too, that we can obtain all whole numbers by starting with 1 and taking successive successors. These properties will be reflected in the axiom system we give below.

We begin with a set N and a mapping S of N into N. The elements of N we call *natural numbers*. For $n \in N$, we call $S(n)$ the *successor* of n.

We impose on N and S the following conditions:*

A_1: S is one-to-one;

A_2: The range of S is not N;

A_3: If u is an element of N which is not in the range of S, and M is a subset of N such that (1) $u \in M$ and (2) $S(n) \in M$ whenever $n \in M$, then $M = N$. (Axiom of Induction)

* Axioms A_1, A_2, and A_3 form a slight modification of the axioms usually associated with the name of Peano, but actually introduced by Dedekind (1888).

In the following, we show that there is just one natural number outside the range of S. This natural number will play the role of the whole number 1. In the presence of our axioms, it will be possible to introduce exactly one binary operation with the properties of familiar addition, and exactly one binary operation with the properties of familiar multiplication. Besides these two operations, we also introduce in N an order relation corresponding to the familiar order for whole numbers. Finally, we use the natural numbers in formulating a definition of "finite set", and show how the natural numbers "count" finite sets in a way which corresponds to the familiar process of counting with whole numbers. The set N itself is not a finite set in this sense.

THEOREM 1.1 *There is exactly one natural number which is not the successor of any natural number.*

PROOF: Let N_S be the range of S. By Axiom A_2, there exists a natural number u which is not in N_S. Let $M = \{u\} \cup N_S$. Then $u \in M$ and $S(n) \in M$ for every $n \in M$, since $N_S \subset M$. By Axiom A_3, $M = N$. Hence $N = \{u\} \cup N_S$, and every natural number $n \neq u$ is in N_S, i.e., every natural number except u is the successor of some natural number.

We shall use the familiar symbol "1" to denote the unique non-successor in N.

DEFINITION 1.1 A subset M of N is called an *inductive set* if $S(n) \in M$ whenever $n \in M$.

We can now restate the Axiom of Induction in the form: "If M is an inductive set containing 1, then $M = N$."

Exercise 1.1 $S(n)$ is different from n for all $n \in N$.

Exercise 1.2 The axioms A_1, A_2, and A_3 are independent, i.e., if A_i and A_j are any two of the axioms, there exists a set N_{ij} and a mapping S_{ij} satisfying the two axioms A_i and A_j, but not satisfying the remaining axiom.

One of the most useful applications of the Axiom of Induction is the "recursive definition" of mappings with domain N. (A mapping of N into a set A is sometimes called a sequence in A.)

A mapping F with domain N and range in a set A may be defined by giving an explicit condition which an ordered pair $(n, a) \in N \times A$

must satisfy so that the element a will be $F(n)$. For example, a mapping F with range in N may be defined by the condition $F(n) = S(S(n))$. In many cases, however, it is impractical to specify such a condition explicitly, and it is desirable to define the mapping "recursively". This is done by specifying two things: (i) how to obtain $F(1)$, and (ii) how to obtain $F(S(n))$ from $F(n)$. Conditions under which a mapping so defined exists are given in the following theorem.

THEOREM 1.2 (*Recursion Theorem*). *Let A be a non-empty set. If G is a mapping of A into A and $a \in A$, then there is exactly one mapping F of N into A such that*

$$F(1) = a \quad \text{and} \quad F(S(n)) = G(F(n)) \quad \text{for all} \quad n \in N.$$

PROOF: Let C be the set of all subsets T of $N \times A$ such that

(1) $(1, a) \in T$, and
(2) $(S(n), G(b)) \in T$ if $(n, b) \in T$.

Since $N \times A$ satisfies (1) and (2), C is not empty. The set

(3) $$F = \bigcap_{T \in C} T$$

satisfies (1), (2). Hence $F \in C$ and, by (3), $F \subset T$ for all $T \in C$.

We show that F is the required mapping. Let

$$M = \{n \mid (n, b) \in F \text{ for exactly one } b \in A\}.$$

$1 \in M$. For, since $F \in C$, $(1, a) \in F$. Suppose $(1, b) \in F$ and $b \neq a$. Let $F_b = F - \{(1, b)\}$. Since $(1, b) \neq (1, a) \in F$, $(1, a) \in F_b$. If $(n, c) \in F_b$, then $(S(n), G(c)) \neq (1, b)$, and $(S(n), G(c)) \in F_b$. But then $F_b \in C$ and $F \subset F_b = F - \{(1, b)\}$, a proper subset of F. Contradiction! It follows that $1 \in M$.

If $n \in M$, then there is exactly one $b \in A$ such that $(n, b) \in F$. Since $F \in C$, $(S(n), G(b)) \in F$. Suppose that $(S(n), c) \in F$ for some $c \neq G(b)$, and let $F_c = F - \{(S(n), c)\}$. Since $(S(n), c) \neq (1, a) \in F$, $(1, a) \in F_c$. If $(m, d) \in F_c$, then $(S(m), G(d)) \neq (S(n), c)$. Otherwise, $S(m) = S(n)$, $G(d) = c \neq G(b)$, so that $m = n$, $d \neq b$, and (n, b), $(n, d) \in F$, contrary to the assumption that $n \in M$. But then $(S(m), G(d)) \in F_c$, hence $F_c \in C$, and $F \subset F_c = F - \{(S(n), c)\}$, a proper subset of F. Contradiction! It follows that $S(n) \in M$. Thus, M is an inductive set.

By the Axiom of Induction, $M = N$. For each $n \in N$, there is exactly one $b \in A$ such that $(n, b) \in F$. Hence, F is a mapping of N into A. Since $(1, a) \in F$, $F(1) = a$. By (3), $F(S(n)) = G(b)$ if and only if $F(n) = b$. Hence, $F(S(n)) = G(F(n))$ for all $n \in N$.

If $\overline{F}$ is any mapping of N into A such that

$$\overline{F}(1) = a \quad \text{and} \quad \overline{F}(S(n)) = G(\overline{F}(n)),$$

then $\overline{F}(1) = F(1)$. If $\overline{F}(n) = F(n)$, then, since G is a mapping of A into A, it follows that

$$\overline{F}(S(n)) = G(\overline{F}(n)) = G(F(n)) = F(S(n)).$$

By the Axiom of Induction,

$$\overline{F} = \{(n, \overline{F}(n)) \mid n \in N\} = \{(n, F(n)) \mid n \in N\} = F.$$

Hence F is the only mapping of N into A having the required properties.

Example: If $A = N - \{1\}$, and G is the mapping given by $G(n) = S(S(n))$, then a mapping F of N into A may be defined by

(a) $F(1) = S(1)$,
(b) $F(S(n)) = G(F(n))$ for each $n \in N$.

If the natural numbers,

$$1,\ S(1),\ S(S(1)),\ S(S(S(1)))\ldots,$$

are identified with the familiar whole numbers,

$$1,\ 2,\ 3,\ 4,\ldots,$$

then the conditions we have stated constitute a recursive definition of the sequence 2, 4, 6, 8, ... of all even numbers.

The following more general theorem is useful in some cases.

Generalized Recursion Theorem. Let A be a non-empty set, and let a be an element of A. For each $n \in N$, let G_n be a mapping of A into A. Then there is exactly one mapping F of N into A such that

$$(1) \quad F(1) = a$$

and

$$(2) \quad F(S(n)) = G_n(F(n))$$

for all $n \in N$.

The proof of this theorem may be obtained by a slight modification of the proof of the Recursion Theorem and should be an instructive exercise for the reader. (Note that the Recursion Theorem deals with the special case where the functions G_n are all equal.)

Addition, Multiplication in N. We shall use the Recursion Theorem to prove that there exist in the natural number system two binary operations with the properties of the addition and multiplication of familiar arithmetic.

THEOREM 1.3 *There is exactly one mapping F of $N \times N$ into N such that*

(1) $F(m, 1) = S(m)$ *for all* $m \in N$

(2) $F(m, S(n)) = S(F(m, n))$ *for all* $m, n \in N$.

PROOF: Let m be any element of N. By the Recursion Theorem, with $A = N$, $a = S(m)$, and $G = S$, there is exactly one mapping F_m of N into N such that

(3) $F_m(1) = S(m)$

(4) $F_m(S(n)) = S(F_m(n))$ for all $n \in N$.

But then the set

$$F = \{((m, n), F_m(n)) \mid (m, n) \in N \times N\}$$

is a mapping of $N \times N$ into N. For all $(m, n) \in N \times N$, $F(m, n) = F_m(n)$. By (3),

$$F(m, 1) = F_m(1) = S(m) \text{ for all } m \in N.$$

By (4),

$$F(m, S(n)) = F_m(S(n)) = S(F_m(n)) = S(F(m, n)).$$

Hence F satisfies (1) and (2).

If $\overline{F}$ is any mapping of $N \times N$ into N satisfying (1) and (2), then

$$\overline{F}(m, 1) = S(m) = F(m, 1) \text{ for each } m \in N.$$

For all $(m, n) \in N \times N$ such that $\overline{F}(m, n) = F(m, n)$, we have

$$\overline{F}(m, S(n)) = S(\overline{F}(m, n)) = S(F(m, n)) = F(m, S(n)).$$

But then for each $m \in N$, the set $N_m = \{n \mid \overline{F}(m, n) = F(m, n)\}$ is equal to N since N_m is an inductive set containing 1. Hence for all $(m, n) \in N \times N$, $\overline{F}(m, n) = F(m, n)$, and $F = \overline{F}$.

Since F is a mapping of $N \times N$ into N, it is a binary operation on N (Definition 0.16).

DEFINITION 1.2 We write "$m + n$" for $F(m, n)$, where F is the mapping of Theorem 1.3, and use the familiar name "addition" for the binary operation "$+$".

We can now restate Theorem 1.3:

THEOREM 1.3$^+$ *There is a unique binary operation on* $\boldsymbol{N}$ *(called addition) such that*

(1^+) $m + 1 = S(m)$ *for each* $m \in \boldsymbol{N}$,

(2^+) $m + S(n) = S(m + n)$ *for each* $m, n \in \boldsymbol{N}$.

Exercise 1.3 If $m, n, p \in \boldsymbol{N}$, and $m + p = n + p$, then $m = n$ (Cancellation Law for Addition).

•*Exercise* 1.4 For $m, n \in \boldsymbol{N}$, $m + n \neq n$.

The familiar addition of whole numbers is both associative and commutative. We show that the addition operation we have introduced in the natural number system has both of these properties.

THEOREM 1.4 *Addition in* $\boldsymbol{N}$ *is associative.*

PROOF: Let P be the set of all $p \in \boldsymbol{N}$ such that $(m + n) + p = m + (n + p)$ holds for all $m, n \in \boldsymbol{N}$. Then $1 \in P$, since $(m + n) + 1 = S(m + n) = m + S(n) = m + (n + 1)$, by properties (1) and (2) of addition. If $p \in P$, then $(m + n) + p = m + (n + p)$ for all m, $n \in \boldsymbol{N}$. Hence $(m + n) + S(p) = S((m + n) + p) = S(m + (n + p)) = m + S(n + p) = m + (n + S(p))$, by (2^+). Thus, P is an inductive set containing 1. By the Axiom of Induction, $P = \boldsymbol{N}$.

THEOREM 1.5 *Addition in* $\boldsymbol{N}$ *is commutative.*

PROOF: We first show that $m + 1 = 1 + m$ for all $m \in \boldsymbol{N}$.

Let $M = \{m \mid m + 1 = 1 + m\}$. Then $1 \in M$ since $1 + 1 = 1 + 1$. If $m \in M$, then $S(m) + 1 = (m + 1) + 1 = (1 + m) + 1 = 1 + (m + 1) = 1 + S(m)$ so that $S(m) \in M$. But then $M = \boldsymbol{N}$. Now let

$$P = \{n \mid m + n = n + m \text{ for all } m \in \boldsymbol{N}\}.$$

Then $1 \in P$, since $m + 1 = 1 + m$ for all $m \in \boldsymbol{N}$. If $n \in P$, then $m + S(n) = m + (n + 1) = m + (1 + n) = (m + 1) + n = n + (m + 1) = n + (1 + m) = (n + 1) + m = S(n) + m$. But then $S(n) \in P$, and, by A_3, $P = \boldsymbol{N}$.

•*Exercise* 1.5 For all $m, n \in \boldsymbol{N}$, $m + n \neq m$.

Exercise 1.6 Define $2 = S(1)$, $3 = S(2)$, $4 = S(3)$, $5 = S(4)$, $6 = S(5)$, and prove

$$1 + 1 = 2,$$
$$2 + 4 = 3 + 3 = 6.$$

The associative property of addition was obtained first, and was used in establishing the commutative property. This is not accidental, since associativity was built into the addition operation by imposing conditions (1^+) and (2^+), so that $m + (n + 1) = m + S(n) = S(m + n) = (m + n) + 1$. In introducing a second binary operation, we bear in mind the behavior of 1 in familiar multiplication, and the relationship of multiplication to addition.

THEOREM 1.6 *There is exactly one mapping K of $\boldsymbol{N} \times \boldsymbol{N}$ into $\boldsymbol{N}$ such that*

(1) $K(m, 1) = m$ *for each* $m \in \boldsymbol{N}$,
(2) $K(m, S(n)) = K(m, n) + m$ *for each* $m, n \in \boldsymbol{N}$.

PROOF: Let m be any element of $\boldsymbol{N}$. By the Recursion Theorem, with $A = \boldsymbol{N}$, $G(k) = k + m$ for each $k \in \boldsymbol{N}$, and $a = m$, there is exactly one mapping K_m of $\boldsymbol{N}$ into $\boldsymbol{N}$ such that

(3) $K_m(1) = m$,
(4) $K_m(S(n)) = K_m(n) + m$ for all $n \in \boldsymbol{N}$.

But then the set

$$K = \{((m, n), K_m(n)) \mid (m, n) \in \boldsymbol{N} \times \boldsymbol{N}\}$$

is a mapping of $\boldsymbol{N} \times \boldsymbol{N}$ into $\boldsymbol{N}$. For all $(m, n) \in \boldsymbol{N} \times \boldsymbol{N}$, $K(m, n) = K_m(n)$. By (3),

$$K(m, 1) = K_m(1) = m \text{ for all } m \in \boldsymbol{N}.$$

By (4),

$$K(m, S(n)) = K_m(S(n)) = K_m(n) + m = K(m, n) + m.$$

Hence, K satisfies (1) and (2).

If $\overline{K}$ is any mapping of $\boldsymbol{N} \times \boldsymbol{N}$ into $\boldsymbol{N}$ satisfying (1) and (2), then

$$\overline{K}(m, 1) = m = K(m, 1) \text{ for all } m \in \boldsymbol{N}.$$

For all $(m, n) \in \boldsymbol{N} \times \boldsymbol{N}$ such that $\overline{K}(m, n) = K(m, n)$ we have

$$\overline{K}(m, S(n)) = \overline{K}(m, n) + m = K(m, n) + m = K(m, S(n)).$$

But then, for each $m \in \boldsymbol{N}$, the set

$$N_m = \{n \mid \overline{K}(m, n) = K(m, n)\} = \boldsymbol{N},$$

since N_m is an inductive set containing 1. Hence for each $(m, n) \in \boldsymbol{N} \times \boldsymbol{N}$, $\overline{K}(m, n) = K(m, n)$, and $\overline{K} = K$.

Since K is a mapping of $\boldsymbol{N} \times \boldsymbol{N}$ into $\boldsymbol{N}$, it is a binary operation on $\boldsymbol{N}$ (Definition 0.16).

DEFINITION 1.3 We write "$m \cdot n$" or "mn" for $K(m, n)$, where K is the mapping of Theorem 1.6, and use the familiar name "multiplication" for the binary operation "$\cdot$".

We can now restate Theorem 1.6:

THEOREM 1.6′ *There is a unique binary operation on* $\boldsymbol{N}$ *(called multiplication), such that*

(1′) $m \cdot 1 = m$ *for each* $m \in \boldsymbol{N}$

(2′) $m \cdot S(n) = m \cdot n + m$ *for each* $m, n \in \boldsymbol{N}$.

THEOREM 1.7 *Multiplication in* $\boldsymbol{N}$ *is left-distributive over addition, i.e., for all* $m, n, p \in \boldsymbol{N}$, $m(n + p) = mn + mp$.

PROOF: Let P be the set of all $p \in \boldsymbol{N}$ such that $m(n + p) = mn + mp$ for all $m, n \in \boldsymbol{N}$. By (1′) and (2′), $m(n + 1) = m \cdot S(n) = mn + m = mn + m \cdot 1$ for all $m, n \in \boldsymbol{N}$. Hence, $1 \in P$.

If $p \in P$, then $m(n + S(p)) = m \cdot S(n + p) = m(n + p) + m = (mn + mp) + m = mn + (mp + m) = mn + m \cdot S(p)$, so that $S(p) \in P$.

Hence P is an inductive set containing 1, and $P = \boldsymbol{N}$.

THEOREM 1.8 *Multiplication in* $\boldsymbol{N}$ *is associative.*

PROOF: Let P be the set of all $p \in \boldsymbol{N}$ such that $(mn)p = m(np)$ for all $m, n \in \boldsymbol{N}$. By (1′), $(mn)1 = mn = m(n1)$ for all $m, n \in \boldsymbol{N}$. Hence $1 \in P$. If $p \in P$, then $(mn)S(p) = (mn)p + mn = m(np) + mn = m(np + n) = m(nS(p))$, by (2′), so that $S(p) \in P$. Hence P is an inductive set containing 1, and $P = \boldsymbol{N}$.

THEOREM 1.9 *Multiplication in* $\boldsymbol{N}$ *is right-distributive over addition, i.e., for all* $m, n, p \in \boldsymbol{N}$, $(m + n)p = mp + np$.

PROOF: Let P be the set of all $p \in \boldsymbol{N}$ such that $(m + n)p = mp + np$ for all $m, n \in \boldsymbol{N}$. Then $(m + n)1 = m + n = m1 + n1$. Hence $1 \in P$. If $p \in P$, then $(m + n)S(p) = (m + n)p + (m + n) = (mp + np) + (m + n) = mp + [np + (m + n)] = mp + [(m + n) + np] = [mp + (m + n)] + np = [(mp + m) + n] + np = (m \cdot S(p) + n) + np = m \cdot S(p) + (n + np) = m \cdot S(p) + (np + n) = m \cdot S(p) + n \cdot S(p)$. Thus, $S(p) \in P$, and P is an inductive set containing 1. But then $P = \boldsymbol{N}$.

THEOREM 1.10 *Multiplication in* $\boldsymbol{N}$ *is commutative.*

PROOF: We first show that $m \cdot 1 = 1 \cdot m$ for all $m \in \boldsymbol{N}$. Let

$$M = \{m \mid m \cdot 1 = 1 \cdot m\}.$$

Then $1 \in M$, since $1 \cdot 1 = 1 \cdot 1$. If $m \in M$, then

$$1 \cdot S(m) = 1(m + 1) = 1 \cdot m + 1 = m \cdot 1 + 1 = m + 1 = S(m)$$

and, by the definition of multiplication, $S(m) \cdot 1 = S(m)$. Hence $S(m) \in M$, and so $M = \boldsymbol{N}$. Now let

$$P = \{n \mid m \cdot n = n \cdot m \text{ for all } m \in \boldsymbol{N}\}.$$

Then $1 \in P$, since $m \cdot 1 = 1 \cdot m$ for all $m \in \boldsymbol{N}$. If $n \in P$, then

$$m \cdot S(n) = mn + m = nm + 1m = (n + 1)m = S(n)m.$$

Hence, $S(n) \in P$ and $P = \boldsymbol{N}$.

Groupoids; Semigroups. The set $\boldsymbol{N}$ of all natural numbers, together with addition and multiplication, serves to illustrate certain abstract mathematical structures which we now define.

DEFINITION 1.4

(a) If $\circ$ is a binary operation on a set G, then the couple* $\langle G, \circ \rangle$ is called a *groupoid*.

* As a mere matter of convenience we refer to mappings whose domains are $\{1, 2\}$, $\{1, 2, 3\}$, $\{1, 2, 3, 4\}$ as couples, triples, and quadruples, respectively, and denote them by $\langle a_1, a_2 \rangle$, $\langle a_1, a_2, a_3 \rangle$, $\langle a_1, a_2, a_3, a_4 \rangle$, where a_i is the image of i. Any one of these may be called a *system*. A more general definition of a "tuple" appears at the end of this chapter.

(b) A groupoid $\langle G, \circ \rangle$ is called a *semigroup* if the operation $\circ$ is associative.

(c) A semigroup whose operation is commutative is called a *commutative semigroup.*

The results of Theorems 1.4, 1.5, 1.8, and 1.10 may be summarized briefly:

THEOREM 1.11 *$\langle \boldsymbol{N}, + \rangle$ and $\langle \boldsymbol{N}, \cdot \rangle$ are commutative semigroups.*

Exercise 1.7 Let A be any non-empty set, M_A the set of all mappings of A into itself, and $\circ$ the operation *composition of mappings* (Definition 0.14). (a) Prove that $\langle M_A, \circ \rangle$ is a semigroup. (b) Prove that the semigroup M_A is not commutative when A contains more than one element.

DEFINITION 1.5 If $\langle G, \circ \rangle$ is a groupoid and $e \in G$, then

(a) e is a *left identity relative to* $\circ$ if $e \circ x = x$ for all $x \in G$;

(b) e is a *right identity relative to* $\circ$ if $x \circ e = x$ for all $x \in G$;

(c) e is a (*two-sided*) *identity relative to* $\circ$ if $e \circ x = x \circ e = x$ for all $x \in G$.

Since $1 \cdot n = n \cdot 1 = n$ for all $n \in \boldsymbol{N}$, the natural number 1 serves as an identity relative to multiplication in the semigroup $\langle \boldsymbol{N}, \cdot \rangle$. In the semigroup $\langle \boldsymbol{N}, + \rangle$, there is no identity relative to addition, since $m + n \neq n$ for all $m, n \in \boldsymbol{N}$ (Exercise 1.4).

THEOREM 1.12 *A groupoid $\langle G, \circ \rangle$ contains at most one (two-sided) identity relative to $\circ$.*

PROOF: If e and f are identities relative to $\circ$, then $e \circ f = f = e$.

We shall use this theorem on several occasions to prove that a groupoid has only one identity. The theorem implies, for example, that there is no natural number $f \neq 1$ such that $fn = nf = n$ for all $n \in \boldsymbol{N}$.

Order in N. If one whole number is less than another, then the second can be obtained by adding a whole number to the first. For the set $\boldsymbol{N}$ of natural numbers we have

THEOREM 1.13 *If T is the subset of $\boldsymbol{N} \times \boldsymbol{N}$ consisting of all (m, n) such that $m + p = n$ for some $p \in \boldsymbol{N}$, then T is an order relation in $\boldsymbol{N}$.*

PROOF: Since T is a subset of $N \times N$, it is a binary relation in N. To show that T is an order relation (Definition 0.12) we show that

(1) If $m, n \in N$, then one and only one of the statements

$$m = n \qquad (m, n) \in T \qquad (n, m) \in T$$

is true (trichotomy).

(2) If $(m, n) \in T$ and $(n, p) \in T$, then $(m, p) \in T$ (transitivity).

For each $m \in N$, let M_m be the set of all $n \in N$ such that one of the statements in (1) is true. We show that $M_m = N$ for all $m \in N$. By Theorem 1.1, either $m = 1$ or $m = p + 1$ for some $p \in N$. Hence either $m = 1$, or $(1, m) \in T$. In either case $1 \in M_m$. Now assume $n \in M_m$. If $m = n$, then $S(n) = m + 1$. Hence, $(m, S(n)) \in T$ and $S(n) \in M_m$. If $(m, n), \in T$, then $m + p = n$ for some $p \in N$ and $m + S(p) = S(n)$. Hence, $(m, S(n)) \in T$ and $S(n) \in M_m$. If $(n, m) \in T$, then $n + p = m$ for some $p \in N$. But $p = 1$ or $p = S(q)$ for some $q \in N$. In the first case, $S(n) = m$, while in the second case, $S(n) + q = n + S(q) = m$ and $(S(n), m) \in T$. In either case, $S(n) \in M_m$. By the Axiom of Induction, $M_m = N$ for all $m \in N$. Now if $m, n \in N$, then $n \in M_m$ and at least one of the statements of (1) is true.

It remains to be shown that for $m, n \in N$ not more than one of the statements of (1) is true. If $m = n$ and $(m, n) \in T$, then $m + p = n = m$ for some $p \in N$. If $m = n$ and $(n, m) \in T$, then $n + q = m = n$ for some $q \in N$. If $(m, n) \in T$ and $(n, m) \in T$, then $m + p = n$ and $n + q = m$ for some $p, q \in N$. Hence, $m + (p + q) = (m + p) + q = n + q = m$. In each case, we have a contradiction, since $m + t \neq m$ for $m, t \in N$ (Exercise 1.5). Hence not more than one of the statements in (1) is true for any $m, n \in N$. This completes the proof of (1).

By the hypothesis of (2) there are $r, s \in N$ such that

$$m + r = n, \qquad n + s = p.$$

Hence,

$$m + (r + s) = (m + r) + s = n + s = p$$

and $(m, p) \in T$. This proves (2).

DEFINITION 1.6 We write "$m < n$" ("$n > m$") for "$(m, n) \in T$", where T is the order relation of Theorem 1.13, and we read "m is less than n" ("n is greater than m"). If $n = m + p$, we write "$p = n - m$" and observe that "$n - m$" is defined for $m, n \in \boldsymbol{N}$ only if $m < n$.

We can now restate Theorem 1.13:

(1) If $m, n \in \boldsymbol{N}$, then just one of $m = n$, $m < n$, $n < m$ ($m = n$, $n > m$, $m > n$) is true (trichotomy).
(2) If $m < n$ and $n < p$ then $m < p$ (if $n > m$ and $p > n$, then $p > m$) (transitivity).

Exercise 1.8 For $m, n, p \in \boldsymbol{N}$, if $mp = np$, then $m = n$ (cancellation law).

• *Exercise* 1.9 For $m, n, p \in \boldsymbol{N}$,

(a) $m < n$ if and only if $m + p < n + p$,
(b) $mp < np$ if and only if $m < n$,
(c) $m < mp$ or $m = mp$.

We note that, according to (a) and (b) of Exercise 1.9, the order in $\boldsymbol{N}$ is not disturbed by either of the binary operations in $\boldsymbol{N}$.

DEFINITION 1.7 A system $\langle A, \circ, < \rangle$ such that

(1) $\langle A, \circ \rangle$ is a semigroup;
(2) $<$ is an order relation in A; and
(3) if $a < b$ in A, then $a \circ c < b \circ c$ for all $c \in A$

is called an *ordered semigroup.*

THEOREM 1.14 *$\langle \boldsymbol{N}, +, < \rangle$ and $\langle \boldsymbol{N}, \cdot, < \rangle$ are ordered semigroups.*

The order in $\boldsymbol{N}$ may be used to define subsets of $\boldsymbol{N}$. Examples: The set of all $n \in \boldsymbol{N}$ such that $S(1) < n$; the set of all $n \in \boldsymbol{N}$ such that $n < S(m)$ for some $m \in \boldsymbol{N}$. It is convenient to introduce notation for stating such definitions.

Notation: We write

"$m \leqq n$" for "$m < n$ or $m = n$",
"$m < n < p$" for "$m < n$ and $n < p$",
"$m \leqq n < p$" for "$m \leqq n$ and $n < p$",
"$m < n \leqq p$" for "$m < n$ and $n \leqq p$",
"$m \leqq n \leqq p$" for "$m \leqq n$ and $n \leqq p$".

Exercise 1.10 "$\leqq$" is a partial order relation in N in the sense of Definition 0.11.

A first element for a subset of N is defined as follows:

DEFINITION 1.8 If $M \subset N$ and there is some $p \in M$ such that

$$p \leqq m \text{ for all } m \in M,$$

then p is called a *first element* (*least element*) of M.

•*Exercise* 1.11 If $M \subset N$ and p and q are first elements of M, then $p = q$.

Thus, if M has a first element, it has only one first element. We shall speak of *the* first element of M.

Some familiar examples of ordered sets do not have first elements. The present moment is earlier than all future moments. The set of all future moments does not have an earliest moment. We shall see that every non-empty subset of N has a first element.

THEOREM 1.15 *1 is the first element of N.*

PROOF: If $m \in N$, then $m = 1$ or $m = S(p) = p + 1$ for some $p \in N$. If $m = p + 1$, then $1 < m$ by Definition 1.6. Hence, $1 \leqq m$ for all $m \in N$. By Definition 1.8 and Exercise 1.11, 1 is the (unique) first element of N.

COROLLARY *If M is a subset of N such that $1 \in M$, then 1 is the first element of M.*

THEOREM 1.16 *If $n \in N$, then the set of all $m \in N$ such that $n < m < S(n)$ is empty.*

PROOF: If $n < m$ in N, then there is some $p \in N$ such that

$$m = n + p.$$

By Theorem 1.1, $p = 1$ or $p = S(q)$ for some $q \in N$. If $p = 1$ then

$$m = n + 1 = S(n),$$

and $m < S(n)$ is false by trichotomy. If $p = S(q)$ then

$$m = n + (q + 1) = (n + 1) + q \quad \text{and} \quad S(n) < m.$$

Hence, again by trichotomy, $m < S(n)$ is false. But then the set of all $m \in N$ such that $n < m < S(n)$ is empty.

DEFINITION 1.9 For $n \in N$, the *initial segment* I_n is the set of all $m \in N$ such that $m \leqq n$.

THEOREM 1.17 *If M is a subset of N such that*

(1) $I_1 \subset M$,

(2) $S(n) \in M$ *whenever* $I_n \subset M$,

then $M = N$.

PROOF: By the definition of I_n and Theorem 1.16,

$$I_{S(n)} = I_n \cup \{S(n)\}.$$

Hence, by (2),

(3) If $I_n \subset M$ then $I_{S(n)} \subset M$.

By (1), (3), and the Axiom of Induction, $I_n \subset M$ for all $n \in N$. Since $n \in I_n$, $N \subset M$ and, since $M \subset N$ by hypothesis, $M = N$.

Since the hypothesis of (2) in Theorem 1.17 asserts "more" than the hypothesis "$n \in M$" of (2) in the Axiom of Induction, the hypothesis—consisting of (1) and (2)—of Theorem 1.17 asserts "less" than the hypothesis of the Axiom of Induction. But the conclusion, "$M = N$", of Theorem 1.17 is also the conclusion of the Axiom of Induction. In this sense Theorem 1.17 is "stronger" than the Axiom of Induction. Theorem 1.17 is sometimes referred to as the Second Principle of Induction.

THEOREM 1.18 *Every non-empty subset of N contains a first element.*

PROOF: We prove the equivalent statement: If $M \subset N$ and M contains no first element, then M is empty. Let K be the set of all natural numbers not in M. Since $1 \leqq n$ for all $n \in N$ and M contains no first element,

(1) $1 \in K$.

Further,

(2) If $I_n \subset K$, then $S(n) \in K$.

For, if $p \in M$, then $p \notin I_n$, since $I_n \subset K$. Hence, $n < p$ and, by Theorem 1.16, $S(n) \leqq p$. Since M contains no first element, $S(n) \notin M$. Hence, $S(n) \in K$.

By (1), (2), and the Second Principle of Induction (Theorem 1.17), $K = N$, and M is empty.

Generalized Associative and Commutative Laws. To simplify our work with sums and products in N and in the systems we introduce later, we define a composite of n elements in an arbitrary semigroup G and prove the generalized associative law, and, in case the operation in G is commutative, the generalized commutative law. These theorems will allow us to rearrange and reassociate freely the terms in sums and the factors in products.

DEFINITION 1.10 If G is a semigroup, and (b_h) is a sequence of elements in G, then the *n-composite* $\mathop{\mathsf{P}}_{h=1}^{n} b_h$ is defined* by

$$\mathop{\mathsf{P}}_{h=1}^{1} b_h = b_1$$

$$\mathop{\mathsf{P}}_{h=1}^{n+1} b_h = \left(\mathop{\mathsf{P}}_{h=1}^{n} b_h\right) b_{n+1}.$$

If, for $b \in G$, $b_h = b$ for all $h \leqq n$, we write b^n for $\mathop{\mathsf{P}}_{h=1}^{n} b_h$. When the usual notations "$+$" and "$\cdot$" are used for addition and multiplication, P will be replaced by $\sum$ or $\prod$, respectively.

THEOREM 1.19 (GENERALIZED ASSOCIATIVE LAW) *Let (b_h) be any sequence of elements from a semigroup G, and, for $n \in N$, $k \in I_n$, let $F = F_k^n$ be a mapping of I_k into I_n such that*

(1) $n_1 < n_2 < \ldots < n_k = n$,

where

$$n_j = F(j) \quad \text{for} \quad j = 1, 2, \ldots, k.$$

Then

(2) $$\mathop{\mathsf{P}}_{h=1}^{n} b_h = \mathop{\mathsf{P}}_{j=1}^{k} Q_j,$$

where

$$Q_1 = \mathop{\mathsf{P}}_{h=1}^{n_1} b_h$$

and

$$Q_j = \mathop{\mathsf{P}}_{h=n_{j-1}+1}^{n_j} b_h \quad \text{for} \quad j = 2, \ldots, k.$$

* This definition is an application of the Generalized Recursion Theorem. What are A, a, the mappings G_n and F in this case? (cf. page 19).

PROOF: Let M be the set of all $n \in N$ such that (2) holds for all $k \in I_n$ and all mappings F_k^n satisfying (1).

Now, $1 \in M$, since from $n = 1$ it follows that $k = 1$, and $F = F_1^1$ is the identity mapping on $I_1 = \{1\}$. Hence

$$\prod_{h=1}^{n} b_h = \prod_{h=1}^{1} b_h = b_1 = Q_1 = \prod_{j=1}^{1} Q_j = \prod_{j=1}^{k} Q_j.$$

Suppose $I_n \subset M$, and F_k^{n+1} is any mapping of I_k into I_{n+1} satisfying (1). If $k = 1$, then $n_1 = n + 1$, and

$$\prod_{j=1}^{k} Q_j = Q_1 = \prod_{h=1}^{n_1} b_h$$

so that (2) is satisfied and $n + 1 \in M$. If $k > 1$, then

$$Q_k = \prod_{h=n_{k-1}+1}^{n+1} b_h = \left(\prod_{h=n_{k-1}+1}^{n} b_h\right) b_{n+1}.$$

Since $n_{k-1} \in I_n$,

$$\prod_{j=1}^{k} Q_j = \left(\prod_{j=1}^{k-1} Q_j\right) Q_k = \left(\prod_{h=1}^{n_{k-1}} b_h\right)\left[\left(\prod_{h=n_{k-1}+1}^{n} b_h\right) b_{n+1}\right].$$

But then

$$\prod_{j=1}^{k} Q_j = \left(\prod_{h=1}^{n_{k-1}} b_h \prod_{h=n_{k-1}+1}^{n} b_h\right) b_{n+1},$$

by the associativity of the operation in G. Since $n \in M$,

$$\prod_{j=1}^{k} Q_j = \left(\prod_{h=1}^{n} b_h\right) b_{n+1} = \prod_{h=1}^{n+1} b_h, \quad \text{by Definition 1.10.}$$

Thus, (2) is satisfied and $n + 1 \in M$. By the second induction principle, $M = N$.

THEOREM 1.20 (GENERALIZED COMMUTATIVE LAW) *Let (b_h) be any sequence of elements from a commutative semigroup G, and, for $n \in N$, let $F = F_n$ be a 1–1 mapping of I_n onto itself. Then*

$$(1) \quad \prod_{h=1}^{n} b_h = \prod_{h=1}^{n} b_{n_h} \text{ where } n_h = F(h) \text{ for } h \in I_n.$$

PROOF: Let M be the set of all $n \in N$ such that (1) holds for each 1–1 mapping F of I_n onto itself.

If $n = 1$, then $I_n = I_1$ and F is the identity mapping on I_1. Hence, $\prod_{k=1}^{1} b_k = b_1 = b_{n_1} = \prod_{k=1}^{1} b_{n_k}$, and $1 \in M$. Suppose $n \in M$, and $F = F_{n+1}$ is a 1–1 mapping of I_{n+1} onto itself. If $b_{n_{n+1}} = b_{n+1}$, then, since $n \in M$,

$$\prod_{k=1}^{n+1} b_k = \left(\prod_{k=1}^{n} b_k\right) b_{n+1} = \left(\prod_{k=1}^{n} b_{n_k}\right) b_{n_{n+1}} = \prod_{k=1}^{n+1} b_{n_k},$$

so that $n + 1 \in M$. If $b_{n+1} = b_{n_l}$ for $1 \leqq l \leqq n$, then $\prod_{k=1}^{n+1} b_{n_k} = \prod_{k=1}^{l} b_{n_k} \prod_{k=l+1}^{n+1} b_{n_k}$, by Theorem 1.19. Since multiplication in G is commutative,

$$\prod_{k=1}^{n+1} b_{n_k} = \prod_{k=l+1}^{n+1} b_{n_k} \prod_{k=1}^{l} b_{n_k}.$$

If $l = 1$, then

$$\prod_{i=1}^{n+1} b_{n_k} = \left(\prod_{k=2}^{n+1} b_{n_k}\right) b_{n_1} = \left(\prod_{k=1}^{n} b_{n'_k}\right) b_{n+1},$$

where $n'_k = n_{k+1}$ for $k = 1, \ldots, n$. Since $n \in M$,

$$\prod_{k=1}^{n+1} b_{n_k} = \left(\prod_{k=1}^{n} b_k\right) b_{n+1} = \prod_{k=1}^{n+1} b_k.$$

If $l > 1$, then

$$\prod_{k=1}^{n+1} b_{n_k} = \prod_{k=l+1}^{n+1} b_{n_k} \left(\prod_{k=1}^{l-1} b_{n_k} b_{n+1}\right)$$

$$= \left(\prod_{k=l+1}^{n+1} b_{n_k} \prod_{k=1}^{l-1} b_{n_k}\right) b_{n+1} = \left(\prod_{k=1}^{l-1} b_{n_k} \prod_{k=l}^{n} b_{n'_k}\right) b_{n+1}.$$

Counting. The familiar process of counting uses the whole numbers as a standard set of tags. If the elements of a set A can be tagged with the whole numbers from 1 to n, the set is said to have n elements. The usefulness of this process lies in the fact that a set which can be tagged with the whole numbers from 1 to n cannot also be tagged with the whole numbers from 1 to m unless $n = m$.

The remaining theorems of this chapter reflect these facts in the system of natural numbers.

THEOREM 1.21 *There exists no* 1–1 *mapping of any initial segment* I_n *onto a proper subset of* I_n.

PROOF: Let M be the set of all $n \in N$ such that there is no 1–1 mapping of the initial segment I_n onto any of its proper subsets. Then $1 \in M$, since the only proper subset of $I_1 = \{1\}$ is the empty set, and the empty set is not the range of any mapping.

Suppose $n \in M$, and let F be a 1–1 mapping of $I_{S(n)}$ onto some proper subset K of $I_{S(n)}$. Then exactly one of the following is true:

(1) $S(n) \in K$ and $F(S(n)) = S(n)$.
(2) $S(n) \in K$ and $F(S(n)) \neq S(n)$.
(3) $S(n) \notin K$.

If (1) is true, let

$$F' = \{(m, F(m)) \mid m \in I_n\}.$$

Then F' is a 1–1 mapping of I_n onto $K - \{S(n)\}$, which is a proper subset of I_n, since K is a proper subset of $I_{S(n)}$. This is impossible, since $n \in M$.

If (2) is true, then $F(S(n)) = t \neq S(n)$ and $F(k) = S(n)$ for some $k \neq S(n)$. Then the set

$$F'' = \{(m, F(m)) \mid m \neq k, S(n)\} \cup \{(k, t), (S(n), S(n))\}$$

is a 1–1 mapping of $I_{S(n)}$ onto K for which (1) is true. But this has been shown to be impossible.

If (3) is true, then $K \subset I_n$ and the set

$$F''' = F - \{(S(n), F(S(n))\}$$

is a 1–1 mapping of I_n onto $K - \{F(S(n))\}$. But $K - \{F(S(n))\}$ is a proper subset of I_n, since $F(S(n)) \in K$ and, by (3), $K \subset I_n$. This is impossible, since $n \in M$.

Hence, $S(n) \in M$ and the theorem follows by the Axiom of Induction.

Exercise 1.12 A subset K of N is an initial segment if and only if

(a) $n \in K$ whenever $S(n) \in K$,
(b) there exists $m \in K$ such that $S(m) \notin K$.

Exercise 1.13 If $n \neq m$, there is no 1–1 mapping of I_n onto I_m.

Exercise 1.14 If N' is the set consisting of all successors in N, then N' is a proper subset of N and there is a 1–1 mapping of N onto N'.

DEFINITION 1.11 For $n \in N$, the set

$$T_n = \{m \mid m \geqq n \text{ in } N\}$$

is called a *terminal segment* of N.

Exercise 1.15

(a) If T_n is a terminal segment of N, then there exists a 1–1 mapping of T_n onto a proper subset of T_n.

(b) A non-empty subset H of N is a terminal segment if and only if $S(n) \in H$ whenever $n \in H$, i.e., if and only if H is an inductive set.

DEFINITION 1.12 A set X is *finite* if it is empty or if there is a 1–1 mapping of some initial segment I_n onto X.

THEOREM 1.22 *If X is a finite set, then there exists no 1–1 mapping of X onto a proper subset Y of X.*

PROOF: If $X = \emptyset$, then X cannot be the domain of any mapping. Suppose $X \neq \emptyset$. Since X is finite, there exists a 1–1 mapping F of I_n onto X for some $n \in N$. If G is a 1–1 mapping of X onto a proper subset Y of X, then, by Exercise 0.20, $H = F^{-1}GF$ is a 1–1 mapping of I_n into I_n. Let x be an element of X which is not in the range Y of G, and suppose $m = F^{-1}(x)$, where $m \in N$. Then m does not belong to the range of H. For, if $m = H(k) = (F^{-1}GF)(k)$ for $k \in I_n$, then $(F^{-1}GF)(k) = F^{-1}(x)$, hence $GF(k) = G(F(k)) = x$. This is impossible since x does not belong to the range of G. But then H is a 1–1 mapping of I_n onto a proper subset of I_n.

By Theorem 1.21, such a mapping does not exist.

•*Exercise* 1.16

(a) Every initial segment is finite.

(b) No terminal segment is finite.

(c) The set N of all natural numbers is not finite.

(d) Every subset of a finite set is finite.

•*Exercise* 1.17

(a) If A and B are finite sets, then $A \cup B$ and $A \cap B$ are finite sets.

(b) If K is a finite set of finite sets A, then $\bigcup_{A \in K} A$ is finite, and $\bigcap_{A \in K} A$ is finite.

(c) Does (b) generalize to arbitrary sets K of finite sets A?

•*Exercise* 1.18 If $<$ is an order relation in a set A, then for every non-empty finite subset B there are elements x and y in B such that $x \leqq z \leqq y$ for all $z \in B$. The elements x and y are called, respectively, the minimum and maximum element of B. (We shall write $x = \min B$, $y = \max B$.)

Our definition of "finite set" reflects the physical process of counting in which objects are successively picked out of a set and tagged with the whole numbers up to some number n. It may be asked whether a set which is not finite can be tagged using *all* of the whole numbers, or, formally, whether there is a 1–1 mapping of the set $\boldsymbol{N}$ of all natural numbers onto any non-finite set. We shall show that the answer to this question is "no". However, if an additional axiom is added to our set theory, we can prove the following weaker statement: for every non-finite set X, there is a 1–1 mapping of $\boldsymbol{N}$ onto some *subset* of X. The axiom we wish to add asserts the possibility of choosing an element from each of the sets belonging to any non-finite set of non-empty sets. The usefulness of such an axiom may be suggested by the following example. If we were given a non-finite collection of pairs of shoes, we would have no difficulty in selecting one shoe from each pair: we could, for instance, choose the *left* shoe of each pair. If, on the other hand, we had a non-finite collection of pairs of socks, we would experience great difficulty in specifying how a sock was to be selected from each pair, since the socks in a pair are usually indistinguishable. The axiom, introduced by Zermelo, is called the

AXIOM OF CHOICE *If X is a non-empty set, then there exists a mapping T of $P(X) - \{\emptyset\}$ into X such that $T(Y) \in Y$ for all $Y \in P(X) - \{\emptyset\}$. (The mapping T is called a* choice function *for X.)*

Using the Axiom of Choice, we can now prove

THEOREM 1.23 *If a set X is not finite, then there is a* 1–1 *mapping of $\boldsymbol{N}$ onto some subset of X.*

PROOF: Let T be a choice function for X and let Q be the set of all finite subsets of X. Since X is not finite, $X - Y \neq \phi$ for any $Y \in Q$, and $T(X - Y) \in X - Y$, by the Axiom of Choice. If $Y \in Q$, let

$$G(Y) = Y \cup \{T(X - Y)\}.$$

By Exercise 1.17, $G(Y) \in Q$ for all $Y \in Q$. Hence the set

$$G = \{(Y, G(Y)) \mid Y \in Q\}$$

is a mapping of Q into Q.

By the Recursion Theorem, there is a mapping F of $\boldsymbol{N}$ into Q such that $F(1) = \{T(X)\}$, and

(1) $F(S(n)) = G(F(n)) = F(n) \cup \{T(X - F(n))\}$ for all $n \in \boldsymbol{N}$.

Now,

(2) if $m \leqq n$ in $\boldsymbol{N}$, then $F(m) \subset F(n)$.

For, let

$$M = \{n \mid F(m) \subset F(n) \text{ for all } m \leqq n\}.$$

Then $1 \in M$. Suppose that $n \in M$. If $m \leqq S(n)$, then either $m \leqq n$ or $m = S(n)$. If $m \leqq n$, then by (1), (2), and the assumption that $n \in M$,

$$F(m) \subset F(n) \subset F(S(n)) = F(n) \cup \{T(X - F(n))\}.$$

If $m = S(n)$, then $F(m) = F(S(n))$. Hence $S(n) \in M$ and, by the Axiom of Induction, $M = \boldsymbol{N}$.

The set

$$H = \{(n, T(X - F(n)) \mid n \in \boldsymbol{N}\}$$

is a mapping of $\boldsymbol{N}$ into X. The mapping H is 1–1. For, if $m < n$ then $S(m) \leqq n$ and by (1) and (2),

$$H(m) = T(X - F(m)) \in F(S(m)) \subset F(n),$$

while $H(n) \notin F(n)$, since

$$H(n) = T(X - F(n)) \in X - F(n).$$

Hence, if $m \neq n$, then $H(m) \neq H(n)$, by trichotomy.

THEOREM 1.24 *If a set X is not finite, then there exists a 1–1 mapping of X onto a proper subset Z of X.*

PROOF: By Theorem 1.23, there exists a 1–1 mapping H of $\boldsymbol{N}$ onto a subset Y of X. Let

(1) $G(x) = HSH^{-1}(x)$ for $x \in Y$,

(2) $G(x) = x$ for $x \in X - Y$.

Then $G = \{(x, G(x)) \mid x \in X\}$ is a 1–1 mapping of X into X. For, if $x_1, x_2 \in Y$ and $G(x_1) = G(x_2)$, then $x_1 = x_2$ by (1), since H, S, and H^{-1} are 1–1 mappings; and if $x_1, x_2 \in X - Y$, and $G(x_1) = G(x_2)$, then $x_1 = x_2$, by (2). If $x_1 \in Y$ and $x_2 \in X - Y$, then

$G(x_1) \neq G(x_2)$, since $G(x_1) \in Y$ and $G(x_2) \in X - Y$. The range of G is a proper subset of X. For, if $H(1) = G(x)$ for some $x \in X$, then $x \in Y$ and $G(x) = HSH^{-1}(x) = H(1)$, so that $SH^{-1}(x) = S(H^{-1}(x)) = 1$, and this is impossible since 1 is not in the range of S.

DEFINITION 1.13 A set X is *infinite* if there exists a 1–1 mapping of X onto a proper subset of itself.

•*Exercise* 1.19 A set is finite if and only if it is not infinite.

DEFINITION 1.14 A set A is called *denumerable* if there is a 1–1 mapping of N onto A.

Exercise 1.20

(a) Every denumerable set is infinite.
(b) Every infinite set contains a denumerable subset.

THEOREM 1.25 *Every subset of* N *is finite or denumerable.*

PROOF: Let A be an infinite subset of N. For each $m \in N$, the set

$$A_m = \{n \mid m < n \text{ and } n \in A\}$$

is infinite and, therefore, not empty. Let $G(m)$ be the first element of A_m. Then

(1) $m < G(m)$ for each $m \in A$

and $G = \{(m, G(m)) \mid m \in A\}$ is a mapping of A into A.

Let $\overline{n}$ be the first element of A. By the Recursion Theorem, there is a mapping F of N into A such that

$$F(1) = \overline{n}$$

and

(2) $F(n + 1) = G(F(n))$ for all $n \in N$.

By (1) and (2), $F(n) < G(F(n)) = F(n + 1)$ for all $n \in N$. By the Axiom of Induction, it follows that $F(n) < F(m)$ if $n < m$. Therefore F is a 1–1 mapping, and its range, $A_F = \{F(n) \mid n \in N\}$, is a denumerable subset of A.

But $A = A_F$. Otherwise, there is some $h \in A - A_F$. Since A_F is an infinite set, $N_h = \{n \mid h < F(n)\} \neq \emptyset$. Let j be the first element of N_h. Since $F(1) = \overline{n} \leqq h < F(j)$, $1 < j$. Hence $j = k + 1$ for some $k \in N$. Since $h \notin A_F$ and $F(k) < F(k + 1)$,

$$F(k) < h < F(k + 1).$$

This is impossible since, by (1) and (2),

$$F(k + 1) = G(F(k)) \leqq h.$$

Exercise 1.21 A subset of a denumerable set is denumerable or finite.

•*Exercise* 1.22 If F is a mapping of a denumerable set A onto a set B, then B is denumerable or finite.

The set $N \times N$ can be represented in various ways as a union of disjoint subsets. If for each m,

$$A_m = \{(m, n) \mid n \in N\},$$

then $N \times N = \bigcup_{m \in N} A_m$ and $A_m \cap A_n = \emptyset$ if $m \neq n$. If for each n,

$$B_n = \{(m, n) \mid m \in N\}$$

then $N \times N = \bigcup_{n \in N} B_n$ and $B_m \cap B_n = \emptyset$ if $m \neq n$. The sets A_m, B_n are represented, respectively, by the rows and columns in Fig. 1.

	B_1	B_2	B_3	B_n
A_1	(1, 1)	(1, 2)	(1, 3)	(1, n) ...
A_2	(2, 1)	(2, 2)	(2, 3) ...	(2, 4) ...
A_3	(3, 1)	(3, 2)	(3, 3) ...	(3, n) ...
	.			.
	.			.
	.			.
A_m	(m, 1)	(m, 2)	(m, 3) ...	(m, n) ...
	.			.
	.			.
	.			.

FIG. 1

Each of the sets A_m and B_n is denumerable, and $N \times N$ is thus represented in two ways as the union of a denumerable set of denumerable sets.

The set $N \times N$ can also be represented as the union of a denumerable set of finite sets R_n whose elements lie on the diagonals indicated in Fig. 1. The sets R_n can be arranged as indicated in Fig. 2.

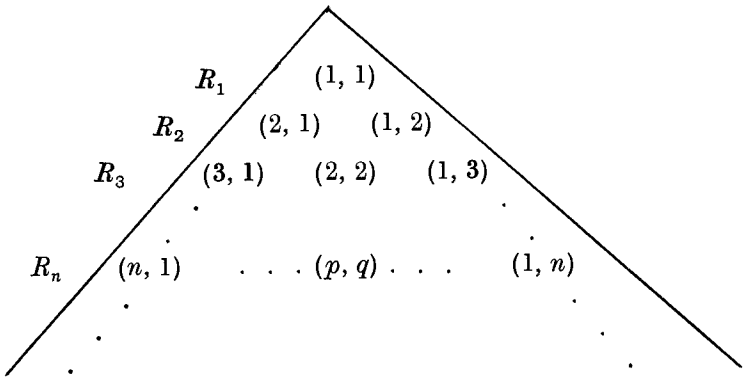


FIG. 2

A precise definition of the sets R_n is given in the proof of Theorem 1.26.

THEOREM 1.26 *$N \times N$ is denumerable.*

PROOF: For each $(p, q) \in N \times N$ there is exactly one $n \in N$ such that $p + q = n + 1$. For each $n \in N$, let

$$R_n = \{(p, q) \mid p + q = n + 1\}.$$

Then

$$N \times N = \bigcup_{n \in N} R_n$$

and

$$R_n \cap R_m = \emptyset \text{ if } n \neq m.$$

There is a 1–1 mapping F'_n of I_n onto R_n such that

$$F'_n(q) = (n + 1 - q, q).$$

For each $n \in N$ let σ_n denote the sum $\sum_{h=1}^{n} h$ of the natural numbers $h \leqq n$. Then there is a 1–1 mapping F''_{n+1} of $I_{\sigma_{n+1}} - I_{\sigma_n}$ onto I_{n+1} such that

$$F''_{n+1}(\sigma_n + q) = q.$$

If $F_{n+1} = F'_{n+1}F''_{n+1}$, then F_{n+1} is a 1–1 mapping of $I_{\sigma_{n+1}} - I_{\sigma_n}$ onto R_{n+1} for each $n \in N$.

Let $J_1 = I_1$, and $J_{n+1} = I_{\sigma_{n+1}} - I_{\sigma_n}$ for each $n \in N$, and let F_1 be the mapping of J_1 onto R_1. Then

$$N = \bigcup_{n \in N} J_n,$$

$$J_n \cap J_m = \emptyset \text{ if } n \neq m,$$

and

$$F = \bigcup_{n \in N} F_n$$

is a 1–1 mapping of N onto $N \times N$.

Exercise 1.23

(a) If K is a denumerable set of non-empty finite sets, then $\bigcup_{A \in K} A$ is denumerable.

Hint: If the sets of K are A_n, $n \in N$, and $B_1 = A_1$, $B_{n+1} = A_{n+1} - (A_{n+1} \cap \bigcup_{j \in I_n} A_j)$, then $B_m \cap B_n = \emptyset$ for $m \neq n$, and $\bigcup_{n \in N} B_n = \bigcup_{A \in K} A$.

(b) Obtain Theorem 1.26 from (a).

Exercise 1.24 Define equivalence relations in $N \times N$ such that the corresponding equivalence classes are, respectively, the sets A_m, B_n in Fig. 1, and the sets R_n in Fig. 2.

Theorem 1.27 *If C is a denumerable set of denumerable sets, then $B = \bigcup_{A \in C} A$ is denumerable.*

Proof: There is a 1–1 mapping T of N onto C. If $T(m) = A_m$ for each $m \in N$, then

$$B = \bigcup_{m \in N} A_m$$

For each $m \in N$ there is a 1–1 mapping F_m of N onto A_m. If $F_m(n) = a_{m,n}$ then

$$A_m = \{a_{m,n} \mid n \in N\}$$

and

$$B = \{a_{m,n} \mid m, n \in N\}.$$

The set $H = \{((m, n), a_{m,n}) \mid (m, n) \in N \times N\}$ is a mapping of $N \times N$ onto B. (The mapping H need not be 1–1 since the sets A_m need not be disjoint.)

Since $N \times N$ is denumerable (Theorem 1.26), the set B is either finite or denumerable (Exercise 1.22). But B is not finite, since it contains A_m, an infinite set. Hence, B is denumerable.

A set A is "more numerous" than a set B if there is a 1–1 mapping of B into A, but there is no 1–1 mapping of B onto A. In this sense, the set N of all natural numbers is more numerous than any

initial segment I_n. Hence, a denumerable set is more numerous than any finite set. More generally, an infinite set, since it contains a denumerable subset (Theorem 1.23), is more numerous than any finite set. It has been shown (Theorem 1.27) that the union of a denumerable set of denumerable sets A_n is denumerable, hence not more numerous than any of the A_n. The following theorem shows that, given any non-empty set A, there is a set more numerous than A.

THEOREM 1.28 *If A is a non-empty set, then there is a* 1–1 *mapping of A into the set $P(A)$ of all subsets of A, but there is no mapping at all of A onto $P(A)$.*

PROOF: The set $\{\{a\} \mid a \in A\}$ is a subset of $P(A)$ and the set $\{(a, \{a\}) \mid a \in A\}$ is a 1–1 mapping of A into $P(A)$.

Suppose there is a mapping F of A onto $P(A)$. Since the set $B = \{a \mid a \notin F(a)\} \in P(A)$ and F maps A onto $P(A)$, there is some $b \in A$ such that $F(b) = B$. Thus, $b \notin F(b)$ if and only if $b \in B$. This is impossible, since $F(b) = B$. Hence there is no mapping of A onto $P(A)$.

COROLLARY $P(N)$ is not denumerable.

Indexing; Tuples; I-products. In many mathematical contexts, the following concepts are quite useful:

If F is a mapping of a set I onto a set X and, for each $\nu \in I$, x_ν denotes $F(\nu)$, then the elements ν of I may be called *indices* for X, the set I may be called an *index set*, and the mapping F itself may be called an *I-tuple*, designated by $\langle x_\nu \mid \nu \in I \rangle$, or simply by $\langle x_\nu \rangle$. The elements x_ν may be referred to as the *components* of the I-tuple F.

In particular, if I is an initial segment I_n in N, then a mapping F of $I = I_n$ onto any set X is often called an *n-tuple*, and is designated by $\langle x_1, \ldots, x_n \rangle$. (If $n = 2$, 3, or 4, the terms *couple*, *triple*, and *quadruple* are customarily used to refer to the corresponding n-tuple.) If I is the set N itself, then a mapping of $I = N$ onto a set X is called a *sequence*.

If X is a set of sets, and F is an I-tuple $\langle X_\nu \rangle$ whose components are the elements of X, then a mapping T of I into $\bigcup_{\nu \in I} X_\nu$ such that $T(\nu) \in X_\nu$ for each $\nu \in I$ may be called an *I-tuple over $\langle X_\nu \rangle$*. Thus, if x_ν designates $T(\nu)$ for each $\nu \in I$, then T is an I-tuple $\langle x_\nu \rangle$ such

that $x_\nu \in X_\nu$ for each $\nu \in I$. In particular, if X is a singleton $\{A\}$, then $\langle X_\nu \rangle$ is an I-tuple whose components are all equal to A, and an I-tuple $T = \langle x_\nu \rangle$ over $\langle X_\nu \rangle$ is an I-tuple whose components x_ν are all elements of $A = \bigcup_{A \in \{A\}} A$. Such an I-tuple is referred to more simply as an I-tuple over A, since it depends only on I and A.

In general, the set of all I-tuples $T = \langle x_\nu \rangle$ over an I-tuple $\langle X_\nu \rangle$ of sets may be referred to as *the I-product over* $\langle X_\nu \rangle$. Thus, for example, if $I = I_2$, and $\langle X_1, X_2 \rangle$ is a couple of sets, then the set of all couples $\langle x_1, x_2 \rangle$, $x_1 \in X_1$, $x_2 \in X_2$, is the I_2-product over the couple $\langle X_1, X_2 \rangle$.

Now, couples are not ordered pairs as defined in Chapter 0 since the ordered pair (x, y) is the set $\{\{x\}, \{x, y\}\}$, while the couple $\langle x, y \rangle$ is the set of ordered pairs: $\{(1, x), (2, y)\}$. However, by Theorem 0.8 on equality of mappings, two I-tuples $T = \langle x_\nu \rangle$ and $T' = \langle x'_\nu \rangle$ are equal if and only if they agree in each component. Since couples and ordered pairs share this important property, they may, in most contexts, be used interchangeably. The I_2-product over a couple $\langle A, B \rangle$ of sets $A = X_1$ and $B = X_2$ may then be identified with the Cartesian product $A \times B$ as defined in Chapter 0. The term Cartesian product is indeed quite commonly used to refer to any I-product.

CHAPTER 2

THE INTEGERS

Preliminaries. The system $\langle N, +, \cdot, < \rangle$, where N is the set of all natural numbers, reflects the properties of the familiar whole numbers with respect to addition, multiplication, and order. Since $m + p \neq m$ for all $m, p \in N$, there are no natural numbers corresponding to zero or to the negative whole numbers. We will construct from N a set Z whose elements we call integers and will define in Z an addition, $(+_Z)$, a multiplication $(\cdot_Z)$ and an order $(<_Z)$ in such a way that Z will reflect the properties of the familiar positive, zero, and negative whole numbers. The resulting system $\langle Z, +_Z, \cdot_Z, <_Z \rangle$ will be an extension of $\langle N, +, \cdot, < \rangle$ in the sense that there exists a 1–1 mapping of N into Z which "preserves" addition, multiplication, and order. The integers will correspond to the "signed whole numbers".

We observe that every signed whole number can be represented in a variety of ways as a difference of two whole numbers (e.g., $+3 = 4 - 1 = 10 - 7 = 12 - 9$; $-2 = 1 - 3 = 5 - 7 = 18 - 20$), and that two such differences are equal when their "cross-sums" are equal (e.g., $4 + 7 = 10 + 1$; $1 + 7 = 5 + 3$). To reflect these properties of the signed whole numbers, we define an integer as an equivalence class of ordered pairs of natural numbers (corresponding to the differences of whole numbers), such that (m, n) and (p, q) are equivalent if the "cross-sums" $m + q$ and $p + n$ are equal.

THEOREM 2.1 *There is an equivalence relation Q in $N \times N$ such that $(m, n)\ Q\ (p, q)$ holds whenever $m + q = p + n$ in N.*

PROOF: Since the set $Q = \{((m, n), (p, q)) \mid m + q = p + n;\ m, n, p, q \in N\}$ is a subset of $(N \times N) \times (N \times N)$, Q is a binary relation in $N \times N$ (Definition 0.6). Since $m + n = m + n$,

$((m, n), (m, n)) \in Q$, and Q is reflexive. If $((m, n), (p, q)) \in Q$, then $m + q = p + n$. Hence, $p + n = m + q$, so that $((p, q), (m, n)) \in Q$ and Q is symmetric. Finally, if $((m, n), (p, q))$ and $((p, q), (r, s)) \in Q$, then $m + q = p + n$ and $p + s = r + q$. But then

$$(m + q) + s = (p + n) + s = (p + s) + n = (r + q) + n.$$

Hence, $q + (m + s) = q + (r + n)$ and, by the cancellation law in N, $m + s = r + n$, so that $((m, n), (r, s)) \in Q$. Thus, Q is transitive. By Definition 0.8, Q is an equivalence relation.

DEFINITION 2.1 We write "$(m, n) \sim (p, q)$" for "$((m, n), (p, q)) \in Q$" and read "$\sim$" as "is equivalent to". For each $(m, n) \in N \times N$, $C_{(m,n)}$ is the set of all $(p, q) \in N \times N$ such that $(p, q) \sim (m, n)$. An *integer* is an equivalence class $C_{(m,n)}$. We write "Z" for the set of all integers and "a", "b", "c", ... for elements of Z.

The set Z of all integers is the factor set $(N \times N)/Q$, where Q is the subset of $(N \times N) \times (N \times N)$ defined in Theorem 2.1 (Definition 0.10).

Addition in Z. The ordered pairs of natural numbers which constitute an integer correspond to the differences of whole numbers associated with a signed whole number. Termwise addition of differences associated with two signed numbers gives a difference associated with their sum—for example,

$$+3 + (-2) = (4 - 1) + (1 - 3) = (4 + 1) - (1 + 3).$$

This suggests that *componentwise* addition of ordered pairs belonging to two integers should give an ordered pair belonging to the sum of the integers, i.e. that the sum of $a = C_{(m, n)}$ and $b = C_{(p, q)}$ should be the integer $c = C_{(m+p, n+q)}$. We shall show that c is independent of the choice of $(m, n) \in a$ and $(p, q) \in b$.

THEOREM 2.2 *If* $(m', n') \sim (m, n)$ *and* $(p', q') \sim (p, q)$, *then*

$$(m + p, n + q) \sim (m' + p', n' + q').$$

PROOF: By hypothesis and Definition 2.1, $m' + n = m + n'$ and $p' + q = p + q'$. Hence, by the properties of addition in N,

$$\begin{aligned}(m + p) + (n' + q') &= (m + n') + (p + q') \\ &= (m' + n) + (p' + q) = (m' + p') + (n + q),\end{aligned}$$

and, by Definition 2.1, $(m + p, n + q) \sim (m' + p', n' + q')$.

THEOREM 2.3 *There is a binary operation F in $\mathbf{Z}$ such that*

$$F(a, b) = C_{(m+p,\ n+q)}$$

if $(m, n) \in a$ and $(p, q) \in b$.

PROOF: The set

$$F = \{((a, b),\ C_{(m+p,\ n+q)}) \mid (m, n) \in a;\ (p, q) \in b;\ a, b \in \mathbf{Z}\}$$

is a subset of $(\mathbf{Z} \times \mathbf{Z}) \times \mathbf{Z}$. For each $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ there are $(m, n) \in a$, $(p, q) \in b$, and $c = C_{(m+p,\ n+q)}$ such that $((a, b), c) \in F$. If $(m', n') \in a$, $(p', q') \in b$, and $c' = C_{(m'+p',\ n'+q')}$ then $(m', n') \sim (m, n)$, $(p', q') \sim (p, q)$ and, by Theorem 2.2, $(m + p, n + q) \sim (m' + p', n' + q')$. Hence, by Definition 2.1, $c' = c$, and F is a mapping of $\mathbf{Z} \times \mathbf{Z}$ into $\mathbf{Z}$, by Definition 0.13. By Definition 0.16, F is a binary operation in $\mathbf{Z}$ and $F(a, b) = c$.

DEFINITION 2.2 We call the binary operation F of Theorem 2.3 *addition* in $\mathbf{Z}$ and write $a +_{\mathbf{Z}} b = F(a, b)$ for all $a, b \in \mathbf{Z}$. (We omit the subscript and write $a + b$ if no confusion arises in the context.)

THEOREM 2.4 $\langle \mathbf{Z}, +_{\mathbf{Z}} \rangle$ *is a commutative semigroup with identity.*

PROOF:

(1) Addition in $\mathbf{Z}$ is associative.

If $a, b, c \in \mathbf{Z}$, then $a = C_{(m,\ n)}$, $b = C_{(p,\ q)}$, $c = C_{(r,\ t)}$ for some $m, n, p, q, r, t \in N$. By Definition 2.2, Theorem 2.3, and the associativity of addition in N,

$$\begin{aligned} a +_{\mathbf{Z}} (b +_{\mathbf{Z}} c) &= C_{(m,\ n)} +_{\mathbf{Z}} C_{(p+r,\ q+t)} \\ &= C_{(m+p,\ n+q)} +_{\mathbf{Z}} C_{(r,\ t)} \\ &= (a +_{\mathbf{Z}} b) +_{\mathbf{Z}} c. \end{aligned}$$

(2) Addition in $\mathbf{Z}$ is commutative.

If $a, b \in \mathbf{Z}$, then $a = C_{(m,\ n)}$, $b = C_{(p,\ q)}$ for some $m, n, p, q \in N$. By Definition 2.2, Theorem 2.3, and the commutativity of addition in N,

$$\begin{aligned} a +_{\mathbf{Z}} b = F(a, b) &= C_{(m+p,\ n+q)} \\ &= C_{(p+m,\ q+n)} = F(b, a) = b +_{\mathbf{Z}} a. \end{aligned}$$

(3) $\mathbf{Z}$ contains a unique identity for addition.

If $a = C_{(m,\ n)}$ is any element of $\mathbf{Z}$, then

$$a + C_{(1,\ 1)} = C_{(m+1,\ n+1)}.$$

Since $(m + 1) + n = m + (n + 1)$ by the properties of addition in N, $(m + 1, n + 1) \sim (m, n)$. Hence, by Definition 2.1,

$$C_{(m+1,\ n+1)} = C_{(m,\ n)},$$

and so

$$a + C_{(1,\ 1)} = a.$$

Therefore, $C_{(1,\ 1)}$ is an identity for $\boldsymbol{Z}$. By Theorem 1.12, there is only one identity.

Notation: We write "0" for the identity for addition in $\boldsymbol{Z}$ and read it as "zero".

THEOREM 2.5 *If $a \in \boldsymbol{Z}$, then there is exactly one element $a' \in \boldsymbol{Z}$ such that $a +_{\boldsymbol{Z}} a' = a' +_{\boldsymbol{Z}} a = 0$.*

PROOF: If $a = C_{(m,\ n)} \in \boldsymbol{Z}$ and $a' = C_{(n,\ m)}$ then

$$a +_{\boldsymbol{Z}} a' = C_{(m+n,\ n+m)}.$$

Since $(q, q) \sim (1, 1)$ for all $q \in N$, it follows from Definition 2.1 that $C_{(m+n,\ m+n)} = C_{(1,\ 1)}$. Hence $a +_{\boldsymbol{Z}} a' = a' +_{\boldsymbol{Z}} a = 0$, and a' has the required properties.

If a'' is another element of $\boldsymbol{Z}$ such that

$$a'' + a = a + a'' = 0,$$

then $a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = 0 + a'' = a''$.

Notation: We write "$-a$" for the element a' of Theorem 2.5.

•*Exercise* 2.1

(a) For $a, b \in \boldsymbol{Z}$ there exists a unique $c \in \boldsymbol{Z}$ such that $a = b + c$ in $\boldsymbol{Z}$.

(b) If $a + c = b + c$ in $\boldsymbol{Z}$, then $a = b$ (cancellation law for addition in $\boldsymbol{Z}$).

Notation: We write "$a - b$" for the unique element c such that $a = b + c$ in $\boldsymbol{Z}$.

DEFINITION 2.3 If $\langle A, \circ \rangle$ is a semigroup, e a right, left, or two-sided identity for $\circ$, and $x, y \in A$, then y is called a

(1) *left inverse of x relative to e* if $y \circ x = e$,

(2) *right inverse of x relative to e* if $x \circ y = e$,

(3) *(two-sided) inverse of x relative to e* if $x \circ y = y \circ x = e$.

The element a' of Theorem 2.5 is an inverse of a relative to the identity 0. The proof given above for the uniqueness of the inverse applies in arbitrary semigroups.

THEOREM 2.6 *In a semigroup* $\langle A, \circ \rangle$ *with (two-sided) identity* e, *an element* x *has at most one inverse relative to* e.

PROOF: If x' and x'' are both inverses of x, then $x'' = x'' \circ e = x'' \circ (x \circ x') = (x'' \circ x) \circ x' = e \circ x' = x'$.

We shall use this theorem repeatedly to prove the uniqueness of inverses.

DEFINITION 2.4 If $\langle A, \circ \rangle$ is a semigroup with identity e such that every element of A has an inverse relative to e, then $\langle A, \circ \rangle$ is called a *group*.

Thus, $\langle \boldsymbol{Z}, +_{\boldsymbol{Z}} \rangle$ is a group, while $\langle \boldsymbol{N}, + \rangle$ is not a group. The purpose of our construction of $\boldsymbol{Z}$ was to embed the semigroup $\langle \boldsymbol{N}, + \rangle$ in the group $\langle \boldsymbol{Z}, +_{\boldsymbol{Z}} \rangle$.

The statements of Exercise 2.1 hold in any group.

Exercise 2.2 If $\langle A, \circ \rangle$ is a group, then for any $a, b \in A$, there is a unique element $c \in A$ such that $a \circ c = b$, and there is a unique element $d \in A$ such that $d \circ a = b$.

In fact, the solvability in A of the equations $a \circ x = b$ and $y \circ a = b$ is a necessary and sufficient condition for a semigroup $\langle A, \circ \rangle$ to be a group:

Exercise 2.3 The semigroup $\langle A, \circ \rangle$ is a group if and only if for any $a, b \in A$ there are c, d in A such that $a \circ c = b$ and $d \circ a = b$.

The cancellation laws hold in any group.

Exercise 2.4 If $\langle A, \circ \rangle$ is a group, and $a \circ x = b \circ x$, or $x \circ a = x \circ b$ for $a, b, x \in A$, then $a = b$.

The cancellation laws are not, in general, sufficient to insure that a semigroup is a group. In fact, we shall define another operation "$\cdot_{\boldsymbol{Z}}$" in $\boldsymbol{Z}$ such that $Z' = \boldsymbol{Z} - \{0\}$ forms, under the restriction of $\cdot_{\boldsymbol{Z}}$ to Z', a semigroup $\langle Z', \cdot_{\boldsymbol{Z}} \rangle$ in which the cancellation laws hold, but which is not a group. However, in the case of a finite semigroup, we have

Exercise 2.5 If A is a finite set and $\langle A, \circ \rangle$ is a semigroup in which both cancellation laws hold, then $\langle A, \circ \rangle$ is a group.

The existence of non-commutative groups is illustrated in the following:

Exercise 2.6 For any non-empty set A, let $\bar{M}_A$ be the set of all 1–1 mappings of A onto itself. If "$\circ$" represents the operation "composition of mappings", then $\langle \bar{M}_A, \circ \rangle$ is a group. The group $\langle \bar{M}_A, \circ \rangle$ is non-commutative except when A consists of a single element, or of two elements.

The following rules of calculation in $\langle \boldsymbol{Z}, + \rangle$ are shared by all commutative groups. For convenience, we state them here in "additive" notation.

•*Exercise* 2.7 If $\langle A, + \rangle$ is a commutative group, and "$-a$" and "$a - b$" denote, respectively, the inverse of a and the element $c \in A$ such that $a = b + c$, then for $a, b, c \in A$, the following statements hold:

(1) $-(-a) = a$.
(2) $a + (-b) = a - b$.
(3) $-(a + b) = (-a) + (-b) = -a - b$.
(4) $(a - b) + (b - c) = a - c$.
(5) $-(a - b) = b - a$.

Multiplication in Z. Our definition of multiplication in $\boldsymbol{Z}$ is patterned on the behavior of differences of signed whole numbers under multiplication:

$$(+2)(-3) = (4 - 2)(3 - 6) = (4 \cdot 3 + 2 \cdot 6) - (2 \cdot 3 + 4 \cdot 6).$$

This suggests that the product of $a = C_{(m, n)}$ and $b = C_{(p, q)}$ should be $c = C_{(mp+nq,\ mq+np)}$, provided that c is independent of the choice of $(m, n) \in a$ and $(p, q) \in b$.

THEOREM 2.7 *If* $(m, n) \sim (m', n')$ *and* $(p, q) \sim (p', q')$, *then*

$$(mp + nq,\ mq + np) \sim (m'p' + n'q',\ m'q' + n'p').$$

PROOF: The conclusion of the theorem follows from

(1) $(mp + nq,\ mq + np) \sim (m'p + n'q,\ m'q + n'p)$

and

(2) $(m'p + n'q,\ m'q + n'p) \sim (m'p' + n'q',\ m'q' + n'p')$

by the transitivity of the equivalence relation.

By hypothesis, $m + n' = m' + n$. Hence, by the properties of addition and multiplication in N,

$$\begin{aligned}(mp + nq) + (m'q + n'p) &= (m + n')p + (n + m')q \\ &= (m + n')(p + q)\end{aligned}$$

and

$$\begin{aligned}(m'p + n'q) + (mq + np) &= (m' + n)p + (n' + m)q \\ &= (m + n')(p + q).\end{aligned}$$

Thus, by Definition 2.1, (1) is proved.

By hypothesis, $p + q' = p' + q$. Hence, by the properties of addition and multiplication in N,

$$\begin{aligned}(m'p + n'q) + (m'q' + n'p') &= m'(p + q') + n'(q + p') \\ &= (m' + n')(p + q')\end{aligned}$$

and

$$\begin{aligned}(m'p + n'q') + (m'q + n'p) &= m'(p' + q) + n'(p + q') \\ &= (m' + n')(p + q')\end{aligned}$$

Thus, by Definition 2.1, (2) is proved.

THEOREM 2.8 *There is a binary operation G on $\mathbf{Z}$ such that*

$$G(a, b) = C_{(mp+nq,\ mq+np)}$$

if $(m, n) \in a$ and $(p, q) \in b$.

PROOF: The set

$$G = \{((a, b),\ C_{(mp+nq,\ mq+np)}) \mid (m, n) \in a;\ (p, q) \in b;\ a, b \in \mathbf{Z}\}$$

is a subset of $(\mathbf{Z} \times \mathbf{Z}) \times \mathbf{Z}$. For each $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ there are $(m, n) \in a$, $(p, q) \in b$, and $c = C_{(mp+nq,\ mq+np)}$ such that $((a, b), c) \in G$. If $(m', n') \in a$, $(p', q') \in b$, and $c' = C_{(m'p'+n'q',\ m'q'+n'p')}$, then $(m', n') \sim (m, n)$, $(p', q') \sim (p, q)$ and, by Theorem 2.7, $(m'p' + n'q', m'q' + n'p') \sim (mp + nq, mq + np)$.

Hence, $c = c'$ by Definition 2.1. But then G is a mapping of $\mathbf{Z} \times \mathbf{Z}$ into $\mathbf{Z}$ by Definition 0.13, and by Definition 0.16, G is a binary operation in $\mathbf{Z}$.

DEFINITION 2.5 We call the binary operation G of Theorem 2.8 *multiplication* in $\mathbf{Z}$ and write

$$a \cdot_{\mathbf{Z}} b = G(a, b) \text{ for all } a, b \in \mathbf{Z}.$$

(We omit the subscript and write $a \cdot b$ or ab if no confusion arises in the context.)

THEOREM 2.9 *$\langle \mathbf{Z}, \cdot \rangle$ is a commutative semigroup with identity.*

PROOF: We leave it to the reader to verify that multiplication in $\mathbf{Z}$ is associative and commutative. Hence, $\langle \mathbf{Z}, \cdot \rangle$ is a commutative semigroup. The element $C_{(1+1,\,1)}$ serves as an identity for multiplication since, for $a = C_{(m,\,n)}$,

$$a \cdot_{\mathbf{Z}} C_{(1+1,\,1)} = C_{(m,\,n)} \cdot C_{(1+1,\,1)} = C_{(m(1+1)+n,\; m+n(1+1))} = C_{(m+m+n,\; m+n+n)} = C_{(m,\,n)} = a.$$

By Theorem 1.12, $C_{(1+1,\,1)}$ is the only identity for multiplication.

Notation: We write "$1_{\mathbf{Z}}$" for the identity for multiplication. (If no confusion with "1" in $\mathbf{N}$ is likely, we omit the subscript and write "1".)

THEOREM 2.10 *Multiplication in $\mathbf{Z}$ is distributive over addition.* The proof is left as an exercise.

Rings.

DEFINITION 2.6 A triple $\langle A, +, \cdot \rangle$ is called a *ring* if

(1) $\langle A, + \rangle$ is a commutative group
(2) $\langle A, \cdot \rangle$ is a semigroup, and
(3) $\cdot$ is left and right distributive over $+$.

A ring $\langle A, +, \cdot \rangle$ is called *commutative* if the semigroup $\langle A, \cdot \rangle$ is commutative, and is called a *ring with identity* if the semigroup $\langle A, \cdot \rangle$ has an identity.

We shall sometimes refer to a ring $\langle A, +, \cdot \rangle$ briefly as "the ring A" and to the identity of $\langle A, + \rangle$ as "0_A".

THEOREM 2.11 *The triple $\langle \mathbf{Z}, +_{\mathbf{Z}}, \cdot_{\mathbf{Z}} \rangle$ is a commutative ring with identity.*

PROOF: $\langle \mathbf{Z}, +_{\mathbf{Z}} \rangle$ is a commutative group, by Theorems 2.4 and 2.5; $\langle \mathbf{Z}, \cdot_{\mathbf{Z}} \rangle$ is a commutative semigroup with $1_{\mathbf{Z}}$ as (the unique) identity, by Theorem 2.9, and the multiplication is left and right distributive over addition (Theorem 2.10).

If $\langle A, +, \cdot \rangle$ is any ring, we have the following calculation rules besides those stated in Exercise 2.7 for $\langle A, + \rangle$:

•*Exercise* 2.8 For $a, b, c \in A$,

(1) $a \cdot 0_A = 0_A \cdot a = 0_A$,
(2) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$.
(3) $(-a) \cdot (-b) = a \cdot b$,
(4) $\begin{cases} (-a) \cdot (b+c) = -a \cdot b - a \cdot c, \\ (b + c) \cdot (-a) = -b \cdot a - c \cdot a. \end{cases}$

Exercise 2.9 If M is the set of all 2×2 matrices of integers, where addition in M is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \oplus \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix}$$

and multiplication in M is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \odot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dy & cf + dh \end{pmatrix},$$

then $\langle M, \oplus, \odot \rangle$ is a non-commutative ring with identity.

Order in Z. The familiar integers are positive, negative, or zero. An integer b exceeds an integer a if the difference $b - a$ is positive. This suggests introducing in $\boldsymbol{Z}$ a set of positive elements, and using it to define order.

DEFINITION 2.7 An integer a is called positive if $(m, n) \in a$ for some m, n such that $n < m$ in $\boldsymbol{N}$.

To show that, according to this definition, an integer is positive no matter which ordered pair of natural numbers is used to represent it, we prove

THEOREM 2.12 *If $n < m$ in $\boldsymbol{N}$ and $(p, q) \sim (m, n)$ in $\boldsymbol{N} \times \boldsymbol{N}$, then $q < p$ in $\boldsymbol{N}$.*

PROOF: By hypothesis, $n + h = m$ for some $h \in \boldsymbol{N}$. Also, by hypothesis, $n + p = q + m$. Hence $n + p = q + n + h$ and, by the properties of addition in $\boldsymbol{N}$, it follows that $p = q + h$ and $q < p$ in $\boldsymbol{N}$.

COROLLARY *An integer, a, is positive if and only if $n < m$ for all $(m, n) \in a$.*

THEOREM 2.13 *If $a \in \boldsymbol{Z}$, then one and only one of the following is true:*

(1) *a is positive* (2) $a = 0$ (3) *$-a$ is positive*

PROOF: Suppose $a = C_{(m, n)}$. By Definition 2.7 and Theorem 2.12, a is positive if and only if $n < m$. Since $C_{(1, 1)} = 0$, $a = 0$ if and only if $m = n$. Since $C_{(n, m)} = -C_{(m, n)}$, $-a$ is positive if and only if $m < n$. By the trichotomy of order in N, exactly one of $m < n$, $m = n$, $n < m$ is true. Hence exactly one of (1), (2), (3) is true.

•*Exercise* 2.10 If a, b are positive in Z, then $a + b$ is positive.

THEOREM 2.14 *If T is the set of all elements $(a, b) \in Z \times Z$ such that $b - a$ is positive, then T is an order relation in Z.*

PROOF: If $a, b \in Z$, then $b - a \in Z$ and, by Theorem 2.13, just one of

$$a - b = 0, \qquad a - b \text{ is positive}, \qquad b - a \text{ is positive}$$

holds. Hence, just one of

$$a = b, \qquad (a, b) \in T, \qquad (b, a) \in T$$

holds, and T has the property of trichotomy.

If $(a, b) \in T$ and $(b, c) \in T$, then $b - a$ and $c - b$ are positive and, by Exercise 2.10, $c - a = (c - b) + (b - a)$ is positive and $(a, c) \in T$. Hence, T is transitive. By Definition 0.12, T is an order relation in Z.

Notation: We write "$a <_Z b$" or "$b > a$" (read "a is less than b in Z" or "b is greater than a in Z") if $b - a$ is positive, i.e., if $(a, b) \in T$, where T is the order relation of Theorem 2.14. Usually we omit the subscript and write "$a < b$" or "$b > a$".

We denote by Z^+ the set of all positive integers.

Exercise 2.11 $Z^+ = \{a \mid a > 0 \text{ in } Z\} = \{-a \mid a < 0 \text{ in } Z\}$.

THEOREM 2.15 $Z^+ = \{C_{(S(n), 1)} \mid n \in N\}$.

PROOF:

(1) $\{C_{(S(n), 1)} \mid n \in N\} \subset Z^+$.

For, $1 < S(n)$ for all $n \in N$. Hence $C_{(S(n), 1)} \in Z^+$ for all $n \in N$.

If $a = C_{(p, q)} \in Z^+$, then $q < p$ in N. If $q = 1$, then $p > 1$, hence $p = S(n)$ for $n \in N$, and $a = C_{(S(n), 1)}$. If $p > q > 1$, then $q = 1 + m$ and $p = 1 + m + n$ for some m, $n \in N$. Hence $a = C_{(1+m+n, 1+m)} = C_{(S(n), 1)}$, and

(2) $Z^+ \subset \{C_{(S(n), 1)} \mid n \in N\}$.

The equality follows from (1) and (2).

THEOREM 2.16 *For* $a, b \in \boldsymbol{Z}^+$, $a \cdot b \in \boldsymbol{Z}^+$.

PROOF: If $a, b \in \boldsymbol{Z}^+$, then $a = C_{(S(n),\,1)}$, $b = C_{(S(m),\,1)}$ for $m, n \in N$. Hence

$$ab = C_{(S(n)S(m)+1,\ S(n)+S(m))} = C_{(mn+m+n+1+1,\ n+1+m+1)} = C_{(S(mn),\,1)} \in \boldsymbol{Z}^+.$$

•*Exercise* 2.12 If $a \neq 0$, $b \neq 0$ in $\boldsymbol{Z}$, then $a \cdot b \neq 0$. Hint: Use Theorem 2.16 and the computation rules of Exercise 2.8.

DEFINITION 2.8 If $\langle A, +, \cdot \rangle$ is a commutative ring with identity $1_A \neq 0_A$ such that for $a, b \in A$, $a \cdot b = 0_A$ only if $a = 0_A$ or $b = 0_A$, then $\langle A, +, \cdot \rangle$ is called an *integral domain.**

As an immediate consequence of Exercise 2.12, we have

THEOREM 2.17 $\langle \boldsymbol{Z}, +, \cdot \rangle$ *is an integral domain.*

Exercise 2.13 If in a ring $\langle A, +, \cdot \rangle$ any one of the following statements holds, then the other two hold also:

(1) If $a, b \in A$ and $a \cdot b = 0_A$, then $a = 0_A$ or $b = 0_A$. (A has no non-zero "divisors of zero".)
(2) If $a, b \in A$, $c \neq 0_A$, and $a \cdot c = b \cdot c$, then $a = b$. (Right-cancellation.)
(3) If $a, b \in A$, $c \neq 0_A$, and $c \cdot a = c \cdot b$, then $a = b$. (Left-cancellation.)

Addition of an element, or multiplication by a positive element, do not disturb inequalities in $\boldsymbol{Z}$, nor does cancellation of terms in sums, or of positive factors in products. More precisely, we have

•*Exercise* 2.14 For a, b in $\boldsymbol{Z}$, $a < b$ if and only if (1) $a + c < b + c$ for all $c \in \boldsymbol{Z}$, or (2) $ac < bc$ for all $c \in \boldsymbol{Z}^+$.

DEFINITION 2.9 If "$<$" denotes an order relation in an integral domain $\langle A, +, \cdot \rangle$ such that

(1) for $a < b$ in A, $a + c < b + c$ for all $c \in A$, and
(2) for $a < b$ in A, $a \cdot c < b \cdot c$ for all $c > 0_A$ in A,

then the system $\langle A, +, \cdot, < \rangle$ is called an *ordered integral domain.*

By Theorem 2.17 and Exercise 2.14 we have

* Usage varies. Sometimes commutativity or the existence of an identity for multiplication are not assumed in the definition of an integral domain.

THEOREM 2.18 *$\langle \boldsymbol{Z}, +, \cdot, < \rangle$ is an ordered integral domain.*

Exercise 2.15 Any commutative ring with identity $1 \neq 0$ in which is defined an order relation satisfying (1) and (2) of Definition 2.9 is an integral domain.

DEFINITION 2.10 If $\langle A, +, \cdot \rangle$ is an integral domain, then a subset A^+ of A is called a set of positive elements for A if

(1) $a + b \in A^+$ for all $a, b \in A^+$,
(2) $a \cdot b \in A^+$ for all $a, b \in A^+$,
(3) for $a \in A$, exactly one of the following holds:

$$a \in A^+, \qquad a = 0_A, \qquad -a \in A^+.$$

Exercise 2.16 $\boldsymbol{Z}^+$ is a set of positive elements for $\boldsymbol{Z}$.

THEOREM 2.19 *If $\langle A, +, \cdot \rangle$ is an integral domain and A^+ is a set of positive elements for A, then*

(1) *the subset T of $A \times A$ defined by*

$$T = \{(a, b) \mid b - a \in A^+\}$$

is an order relation in A.

(2) *If we write "$a < b$" ("$b > a$") for "$(a, b) \in T$", then $\langle A, +, \cdot, < \rangle$ is an ordered integral domain.*

(3) $A^+ = \{a \mid a > 0_A\}$

PROOF: If (a, b) and (b, c) are in T, then $b - a$ and $c - b$ are in A^+. Hence, by Definition 2.10 (2),

$$c - a = (c - b) + (b - a) \in A^+$$

Thus, $(a, c) \in T$, and T is transitive.

For $a, b \in A$, exactly one of

$$b - a \in A^+, \qquad b - a = 0, \qquad -(b - a) = a - b \in A^+$$

holds, by Definition 2.10 (3). Thus, T is trichotomous. It follows that T is an order relation in A.

If $(a, b) \in T$, then, for any $c \in A$,

$$b + c - (a + c) = b - a \in A^+.$$

Hence, $(a + c, b + c) \in T$. Further, if $(a, b) \in T$ and $c \in A^+$ then

$$bc - ac = (b - a)c \in A^+$$

by Definition 2.10 (1). Hence, $(ac, bc) \in T$.

Thus, from $a < b$ and $c \in A$, follows $a + c < b + c$, and from $a < b$ and $c \in A^+$ follows $ac < bc$, so that $\langle A, +, \cdot, < \rangle$ is an ordered integral domain.

Exercise 2.17 If $\langle A, +, \cdot, < \rangle$ is an ordered integral domain, then the set

$$A^* = \{a \mid a \in A \text{ and } a > 0_A\}$$

is a set of positive elements for A and the order relation

$$T = \{(a, b) \mid b - a \in A^+\}$$

is the given order in $\langle A, +, \cdot, < \rangle$.

•*Exercise* 2.18

(1) If $\langle A, +, \cdot, < \rangle$ is an ordered integral domain, then for $a \neq 0_A$, $a \cdot a$ is positive in A; the multiplicative identity 1_A is positive.

(2) In the ordered domain Z of integers, $ab = 1$ if and only if $a = b = \pm 1$.

Exercise 2.19 If $\langle A, +, \cdot, < \rangle$ is an ordered integral domain, then A is an infinite set.

•*Exercise* 2.20 The triple $\langle A_k, \oplus, \odot \rangle$, where

(1) k is a positive integer,

(2) A_k is the set of integers, r, such that $0 \leqq r \leqq k - 1$,

(3) addition is defined by

$$r \oplus s = t \in A_k, \text{ where } (r + s) - t \text{ is a multiple of } k \text{ in } \boldsymbol{Z},$$

(4) multiplication is defined by

$$r \odot s = t \in A_k, \text{ where } rs - t \text{ is a multiple of } k \text{ in } \boldsymbol{Z},$$

is a commutative ring with identity.

•*Exercise* 2.21 A *prime* is an integer $k \neq 0, \pm 1$ such that if a, $b \in \boldsymbol{Z}$, and $ab = k$, then $a = \pm 1$ or $b = \pm 1$. The ring $\langle A_k, \oplus, \odot \rangle$, defined in Exercise 2.20 is an integral domain if and only if k is prime. If k is prime, the integral domain $\langle A_k, \oplus, \odot \rangle$ cannot be made into an ordered integral domain.

Embedding. The elements $C_{(S(n),\,1)} \in Z^+$ behave with respect to $+_Z$, $\cdot_Z$, $<_Z$ exactly as the natural numbers n behave with respect to $+$, $\cdot$, $<$, in the sense of the following theorem.

THEOREM 2.20 *The mapping* $E = E_N^Z$ *of* N *into* Z *defined by*

$$E(n) = C_{(S(n),\,1)} \text{ for } n \in N$$

is a $1-1$ *mapping, with range* Z^+, *such that*

(1) $E(m + n) = E(m) +_Z E(n)$,
(2) $E(m \cdot n) = E(m) \cdot_Z E(n)$,
(3) $E(m) <_Z E(n)$ if and only if $m < n$.

PROOF: If $m, n \in N$, then

$$\begin{aligned} E(m) +_Z E(n) &= C_{(S(n),\,1)} +_Z C_{(S(m),\,1)} \\ &= C_{(S(n)+S(m),\,1+1)} = C_{(S(m+n),\,1)} = E(m + n) \end{aligned}$$

and (1) is proved. Also,

$$\begin{aligned} E(m) \cdot_Z E(n) &= C_{(S(n),\,1)} \cdot_Z C_{(S(m),\,1)} \\ &= C_{(S(m)S(n)+1,\ S(m)+S(n))} \\ &= C_{(mn+m+n+1,\ m+n+1+1)} \\ &= C_{(S(mn),\,1)} = E(m \cdot n) \end{aligned}$$

and (2) is proved. Finally,

$$E(m) = C_{(S(m),\,1)} <_Z C_{(S(n),\,1)} = E(n)$$

if and only if

$$\begin{aligned} C_{(S(n),\,1)} - C_{(S(m),\,1)} &= C_{(S(n),\,1)} + C_{(1,\,S(m))} \\ &= C_{(S(S(n)),\ S(S(m)))} \end{aligned}$$

is positive. Hence $E(m) <_Z E(n)$ if and only if $S(S(m)) < S(S(n))$, and $m < n$, in N.

•*Exercise* 2.22: $E_N^Z(1) = 1_Z$.

Isomorphism.

DEFINITION 2.11

(1) If $\circ$ is a binary operation in a set A, and $\circ'$ is a binary operation in a set A', then a 1–1 mapping F of A into (onto) A' is called an $(\circ, \circ')$-*isomorphism* of A into (onto) A' if

$$F(a \circ b) = F(a) \circ' F(b) \text{ for all } a, b \in A.$$

(2) If T is a binary relation in A, and T' is a binary relation in A', then a 1–1 mapping F of A into (onto) A' is called a (T, T')-isomorphism of A into (onto) A' if for $a, b \in A$, aTb is true if and only if $F(a)\ T'\ F(b)$ is true.

We observe that the condition in (1) may also be written as $F(\circ(a, b)) = \circ'(F(a), F(b))$.

If the relations T and T' in (2) are mappings of A into A and of A' into A', respectively, then the condition in (2) may be written $F(T(a)) = T'(F(a))$ for each $a \in A$.

According to Definition 2.11, the mapping $E_N^{\mathbf{Z}}$ of Theorem 2.20 is a $(+, +_{\mathbf{Z}})$-, $(\cdot, \cdot_{\mathbf{Z}})$ -, and $(<, <_{\mathbf{Z}})$-isomorphism of N into $\mathbf{Z}$ (and onto $\mathbf{Z}^+$). We shall say simply that E is an isomorphism of N into $\mathbf{Z}$ preserving addition, multiplication and order, or that N is isomorphic to $\mathbf{Z}^+$ with respect to addition, multiplication, and order.

Notation: In view of the isomorphism $E_N^{\mathbf{Z}}$ and Exercise 2.22, we use interchangeably the symbols

$$C_{(S(n),\,1)} \text{ and } n,$$

$$1_{\mathbf{Z}} \text{ and } 1.$$

DEFINITION 2.12 If there exists an isomorphism of A into A' with respect to a pair of operations or relations (α, α'), then A' is called an *extension* of A with respect to (α, α'). If A' is an extension of A with respect to (α, α'), we say that A can be *isomorphically embedded* in A' with respect to (α, α').

Thus, $\mathbf{Z}$ is an extension of N with respect to $(+, +_{\mathbf{Z}})$, $(\cdot, \cdot_{\mathbf{Z}})$, and $(<, <_{\mathbf{Z}})$, i.e., with respect to addition, multiplication, and order.

Exercise 2.23

(1) The mapping $E_N^{\mathbf{Z}}$ "preserves successors" in the following sense: if

$$S_{\mathbf{Z}} = \{(a, a + 1_{\mathbf{Z}}) \mid a \in \mathbf{Z}^+\} \subset \mathbf{Z}^+ \times \mathbf{Z}^+,$$

then $S_{\mathbf{Z}}$ is a mapping of $\mathbf{Z}^+$ into $\mathbf{Z}^+$ and

$$E(S(n)) = S_{\mathbf{Z}}(E(n)) \text{ for each } n \in N.$$

(2) The system $\langle \mathbf{Z}^+, S_{\mathbf{Z}} \rangle$ satisfies Axioms A_1, A_2, and A_3, where $\mathbf{Z}^+$ and $S_{\mathbf{Z}}$ play the role of N and S, respectively.

Exercise 2.24

(a) Let K be any set, T a mapping of K into itself. If F is a 1–1 mapping of N onto K such that

$$F(S(n)) = T(F(n)) \text{ for all } n \in N$$

(i.e., if F is an (S, T)-isomorphism of N onto K) then the system $\langle K, T \rangle$ satisfies Axioms A_1, A_2, and A_3.

(b) If K is any set, T a mapping of K into itself such that the system $\langle K, T\rangle$ satisfies Axioms A_1, A_2, and A_3, then there exists an (S, T)-isomorphism of N onto K.

(c) If F is an (S, T)-isomorphism of N onto K, and if addition, multiplication, and order are defined in K according to Definitions 1.2, 1.3, and 1.6, then F is an addition, multiplication, and order isomorphism of N onto K.

The statement in (*b*) expresses the *categoricity* of Axioms A_1, A_2, and A_3. A collection of axioms is called *categorical* if any two systems satisfying the axioms are isomorphic with respect to the operations or relations given in the axioms.

Exercise 2.25 For each K_i $(i = 1, 2, 3)$ below, find a mapping T_i such that the system $\langle K_i, T_i\rangle$ will satisfy Axioms A_1, A_2, and A_3. In each case, exhibit an (S, T_i)-isomorphism of N onto K_i, and define addition and multiplication for K_i in the sense of Definitions 1.2 and 1.3.

(1) For fixed $h \in \boldsymbol{Z}$, $K_1 = \{a \mid a \geqq h\}$.
(2) For fixed $h \in \boldsymbol{Z}$, $K_2 = \{a \mid a \leqq h\}$.
(3) For fixed $h \neq 0$ in $\boldsymbol{Z}$, $K_3 = \{hn \mid n \in \boldsymbol{Z}^+\}$.
(4) For fixed $h \neq 0$ in $\boldsymbol{Z}$, and $k \in \boldsymbol{Z}$, $K_4 = \{hn + k \mid n \in \boldsymbol{Z}^+\}$.

Exercise 2.26

(a) For $a \in \boldsymbol{Z}$, there exists no integer, k, such that $a < k < a + 1$.
(b) Every non-empty set of positive integers in $\boldsymbol{Z}$ has a least element.
(c) Every non-empty set of "negative" integers (i.e., integers a such that $-a \in \boldsymbol{Z}^+$) has a greatest element.
(d) If A is any non-empty subset of $\boldsymbol{Z}$, and if A has a least (greatest) element, then every non-empty subset T of A has a least (greatest) element.

•*Exercise* 2.27. An integer a is *even* if $a = 2k$ for some $k \in \boldsymbol{Z}$. An integer a is *odd* if $a = 2k + 1$ for some $k \in \boldsymbol{Z}$.

Prove:

(1) Every integer is either even or odd.
(2) No integer is both even and odd.
(3) For $a \in \boldsymbol{Z}$, a^2 is even if and only if a is even.

Exercise 2.28 If A is an ordered integral domain, A^+ the set of "positive" elements in A, and if every non-empty subset of A^+ has a first element in the sense of the given ordering, then (a) the principle of induction holds in A^+, i.e., if $M \subset A^+$ such that $1_A \in M$ and $a + 1_A \in M$ for every $a \in M$, then $M = A^+$; and (b) there exists an isomorphism of A onto $\boldsymbol{Z}$ preserving addition, multiplication, and order. (This implies that the statements listed below form a categorical set of axioms for $\boldsymbol{Z}$.)

(1) $\langle A, +, \cdot, < \rangle$ is an ordered integral domain.
(2) Every non-empty subset of the set $A^+ = \{a \mid 0_A < a\}$ has a first element.

Exercise 2.29 Show that $\boldsymbol{Z}$ is denumerable, i.e., construct a 1–1 mapping of $\boldsymbol{N}$ onto $\boldsymbol{Z}$. Is there a mapping of $\boldsymbol{N}$ onto $\boldsymbol{Z}$ which preserves addition or multiplication?

CHAPTER 3

RATIONAL NUMBERS—ORDERED FIELDS

Preliminaries. The set $Z' = Z - \{0\}$ forms a semigroup under multiplication. This semigroup is not a group, since, by Exercise 2.18(2), no integer other than ± 1 has a multiplicative inverse relative to the identity 1. We now construct from Z a set, Q, whose elements we call rational numbers, and we define in Q an addition $(+_Q)$, a multiplication $(\cdot_Q)$, and an order $(<_Q)$, in such a way that the system $\langle Q, +_Q, \cdot_Q, <_Q \rangle$ reflects the familiar properties of fractions. This system will be an extension of $\langle Z, +_Z, \cdot_Z, <_Z \rangle$ with respect to addition, multiplication, and order. If we delete from Q the additive identity 0_Q, we obtain a set, Q', which forms a group under multiplication.

Our definition of rational numbers will be based on familar properties of fractions. We observe that two fractions (e.g., $2/4$ and $-3/-6$) are equal when their "cross products" are equal: $2(-6) = (-3)4$. We shall define a rational number as an equivalence class of ordered pairs of integers (corresponding to the fractions) where the equivalence relation is given by equality of cross products.

DEFINITION 3.1 An ordered pair (a, b) of integers is called *admissible* if $b \neq 0$ in Z. We denote by A the set of all admissible ordered pairs of integers.

THEOREM 3.1 *There is an equivalence relation Q in A such that $(a, b)\ Q\ (c, d)$ holds whenever $ad = cb$.*

PROOF: The set

$$Q = \{((a, b), (c, d)) \mid ad = cb \text{ in } Z\}$$

is a subset of $A \times A$. By Definition 0.6, Q is a binary relation in A. Since $ab = ab$, $((a, b), (a, b)) \in Q$ for all $(a, b) \in A$. Hence the

relation, Q, is reflexive. If $((a, b), (c, d)) \in Q$, then $((c, d), (a, b)) \in Q$. Hence Q is symmetric. Finally, if $((a, b), (c, d))$ and $((c, d), (e, f))$ are in Q, then $ad = cb$ and $cf = ed$. By the properties of multiplication in $\boldsymbol{Z}$, $adf = cbf = edb$ and, since $d \neq 0$, $af = eb$. Hence, $((a, b), (e, f)) \in Q$, and the relation, Q, is transitive. By Definition 0.8, Q is an equivalence relation in A.

DEFINITION 3.2 We write "$(a, b) \sim (c, d)$" for "$((a, b), (c, d)) \in Q$" and read "$\sim$" as "is equivalent to". For each $(a, b) \in A$, the equivalence class $C_{(a, b)}$ is the set of all $(c, d) \in A$ such that $(c, d) \sim (a, b)$. A *rational number* is an equivalence class $C_{(a, b)}$. We write "$\boldsymbol{Q}$" for "the set of all rational numbers" and "x", "y", "z", ... for elements of $\boldsymbol{Q}$.

If A and Q are the sets defined in Theorem 3.1, then the factor set, A/Q, is the set of all rational numbers.

Addition and Multiplication in Q. Our definitions of addition and multiplication in $\boldsymbol{Q}$ mirror the properties of the familiar addition and multiplication of fractions. The uniqueness of sums and products will be a consequence of Theorem 3.2.

THEOREM 3.2 *If* $(a, b) \sim (a', b')$ *and* $(c, d) \sim (c', d')$, *then*

(1) $(ad + cb, bd) \sim (a'd' + c'b', b'd')$,

and

(2) $(ac, bd) \sim (a'c', b'd')$.

PROOF: By hypothesis, $ab' = a'b$ and $cd' = c'd$. Hence, by the properties of addition and multiplication in $\boldsymbol{Z}$,

$$\begin{aligned}(ad + cb)(b'd') &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd' + c'b')(bd).\end{aligned}$$

Since $bd \neq 0$ and $b'd' \neq 0$, $(ad + cb, bd) \sim (a'd' + c'b', b'd')$ by Definition 3.2. Also, $(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$, and, since $bd \neq 0$ and $b'd' \neq 0$, $(ac, bd) \sim (a'c', b'd')$.

THEOREM 3.3 *There are binary operations* F *and* G *on* $\boldsymbol{Q}$ *such that, if* $(a, b) \in x$ *and* $(c, d) \in y$, *then*

(1) $F(x, y) = C_{(ad + cb, bd)}$,
(2) $G(x, y) = C_{(ac, bd)}$.

PROOF: The sets

$$F = \{((x, y), C_{(ad+cb,\ bd)}) \mid (a, b) \in x,\ (c, d) \in y;\ x, y \in Q\}$$

and

$$G = \{((x, y), C_{(ac,\ bd)}) \mid (a, b) \in x,\ (c, d) \in y;\ x, y \in Q\}$$

are subsets of $(Q \times Q) \times Q$. Since (a, b) and (c, d) are in A, $(ad + cb, bd)$ and (ac, bd) are in A.

For each $(x, y) \in Q \times Q$, there are $(a, b) \in x$, $(c, d) \in y$, and $z = C_{(ad+cb,\ bd)}$ such that $((x, y), z) \in F$. If $(a', b') \in x$, $(c', d') \in y$, and $z' = C_{(a'd'+c'b',\ b'd')}$, then, from $(a', b') \sim (a, b)$, $(c', d') \sim (c, d)$, and Theorem 3.2, it follows that $(ad + cb, bd) \sim (a'd' + c'b', b'd')$. Hence, by Definition 3.2, $z' = z$. Therefore, F is a mapping of $Q \times Q$ into Q by Definition 0.13, and, by Definition 0.16, F is a binary operation in Q.

For each $(x, y) \in Q \times Q$, there are $(a, b) \in x$, $(c, d) \in y$, and $z = C_{(ac,\ bd)}$ such that $((x, y), z) \in G$. If $(a', b') \in x$, $(c', d') \in y$, and $z' = C_{(a'c',\ b'd')}$, then $(a', b') \sim (a, b)$, $(c', d') \sim (c, d)$, and, by Theorem 3.2, $(ac, bd) \sim (a'c', b'd')$. Hence, $z = z'$ by Definition 3.2. Therefore, G is a mapping of $Q \times Q$ into Q. By Definition 0.16, G is a binary operation in Q.

DEFINITION 3.3 We refer to the binary operations F and G of Theorem 3.3, respectively, as *addition* and *multiplication in* Q and write

$$x +_Q y = F(x, y), \qquad x \cdot_Q y = G(x, y)$$

for all $x, y \in Q$.

We omit the subscript "Q" and even the "$\cdot$" if the context makes it clear that the operations are in Q.

THEOREM 3.4 $\langle Q, +_Q \rangle$ *is a commutative group.*

PROOF:

(1) Addition in Q is commutative.

If $x, y \in Q$, then $x = C_{(a,\ b)}$, $y = C_{(c,\ d)}$ for some admissible (a, b) and (c, d). By Definition 3.3, Theorem 3.3, and the properties of addition and multiplication in Z,

$$\begin{aligned} x +_Q y = F(x, y) &= C_{(ad+cb,\ bd)} \\ &= C_{(cb+ad,\ db)} = F(y, x) = y +_Q x. \end{aligned}$$

(2) Addition in Q is associative.

If $x, y, z \in \boldsymbol{Q}$, then $x = C_{(a, b)}$, $y = C_{(c, d)}$, $z = C_{(e, f)}$ for some admissible (a, b), (c, d), and (e, f). Now, by Definition 3.3, Theorem 3.3, and the properties of addition and multiplication in $\boldsymbol{Z}$,

$$(1)\quad \begin{cases} (ad + cb, bd) \in x +_Q y, \\ ((ad + cb)f + e(bd), (bd)f) \in (x +_Q y) +_Q z, \end{cases}$$

$$(2)\quad \begin{cases} (cf + ed, df) \in y +_Q z, \\ (a(df) + (cf + ed)b, b(df)) \in x +_Q (y +_Q z). \end{cases}$$

Since, in $\boldsymbol{Z}$,

$$(ad + cb)f + e(bd) = a(df) + (cf + ed)b \text{ and } (bd)f = b(fd),$$

it follows from (1) and (2) that the equivalence classes $(x +_Q y) +_Q z$ and $x +_Q (y +_Q z)$ have an element in common. Hence,

$$x +_Q (y +_Q z) = (x +_Q y) +_Q z.$$

(3) $\boldsymbol{Q}$ contains a unique identity for addition. If $x = C_{(a, b)}$ is any element of $\boldsymbol{Q}$, then

$$x + C_{(0, 1)} = C_{(a \cdot 1 + 0 \cdot b,\ b \cdot 1)} = C_{(a, b)} = x.$$

Hence, $C_{(0, 1)}$ is an identity for addition. By Theorem 1.12, there is only one identity.

(4) Every element of $\boldsymbol{Q}$ has a unique inverse with respect to addition. If $x = C_{(a, b)} \in \boldsymbol{Q}$ and $x' = C_{(-a, b)}$, then

$$x +_Q x' = C_{(ab + (-a)b,\ b^2)} = C_{(0, b^2)} = C_{(0, 1)},$$

since $(0, b^2) \sim (0, 1)$. Hence x' is an inverse for x. By Theorem 2.6, x' is the only inverse.

Notation: We write "0_Q" for the identity $C_{(0, 1)}$, "$-x$" for the inverse of x, and "$x - y$" for the element z, such that $x = y + z$ in $\langle \boldsymbol{Q}, +_Q \rangle$.

THEOREM 3.5 *$\langle \boldsymbol{Q}, \cdot_Q \rangle$ is a commutative semigroup with identity.*

PROOF: We leave it to the reader to verify that multiplication is associative and commutative, and note that the element $C_{(1, 1)}$ serves as an identity for multiplication in $\boldsymbol{Q}$.

Notation: We write "1_Q" for the identity $C_{(1, 1)}$.

THEOREM 3.6 *$\langle Q, +_Q, \cdot_Q \rangle$ is a commutative ring with identity.*

PROOF: Since $\langle Q, +_Q \rangle$ is a commutative group and $\langle Q, \cdot_Q \rangle$ is a commutative semigroup with identity, it remains only to be proved that multiplication in Q distributes over addition.

If $x = C_{(a, b)}$, $y = C_{(c, d)}$, and $z = C_{(e, f)}$, then

$$\begin{aligned} x \cdot_Q y +_Q x \cdot_Q z &= C_{(ac, bd)} +_Q C_{(ae, bf)} \\ &= C_{(acbf + aebd,\ b^2df)} \\ &= C_{(acf + aed,\ bdf)} \\ &= C_{(a, b) \cdot_Q (C_{(c, d)} +_Q C_{(e, f)})} = x \cdot_Q (y +_Q z) \end{aligned}$$

since $b \neq 0$ in Z.

THEOREM 3.7 *Every element x in Q other than 0 has a unique inverse with respect to multiplication.*

PROOF: If $x = C_{(a, b)} \in Q$ and $x \neq 0_Q = C_{(0, 1)}$, then $a \neq 0$, since $(0, b) \sim (0, 1)$ for all $b \neq 0$ in Z. If $a \neq 0$, then $x' = C_{(b, a)} \in Q$ and

$$x \cdot_Q x' = G(x, x') = C_{(ab, ba)} = C_{(1, 1)} = 1_Q.$$

Hence, x' is an inverse for x with respect to multiplication in Q. By Theorem 2.6, x' is the only inverse of x.

COROLLARY *The set $Q' = Q - \{0_Q\}$ is a group with respect to multiplication in Q.*

Fields.

DEFINITION 3.4 A system $\langle A, +, \cdot \rangle$ is called a *field* if

(1) $\langle A, +, \cdot \rangle$ is a commutative ring,
(2) $\langle A', \cdot' \rangle$ is a group where $A' = A - \{0_A\}$, "0_A" denotes the identity for the operation $+$, and $\cdot'$ denotes the restriction of the operation $\cdot$ to the set A'.

THEOREM 3.8 *$\langle Q, +_Q, \cdot_Q \rangle$ is a field.*

•*Exercise* 3.1 Every field is an integral domain.

Exercise 3.2 By a construction analogous to that of Q, a field can be constructed from any given integral domain.

Exercise 3.3 The systems $\langle A_k, \oplus, \odot \rangle$ defined in Exercise 2.21 are fields if and only if k is prime.

Notation: If $\langle A, +, \cdot \rangle$ is a field, we write "0_A" and "1_A" (or simply "0", "1") for the additive and multiplicative identities, respectively. If $x \neq 0$, we write "$1/x$" for the multiplicative inverse of x in A, and, generally, "y/x" for the element $z \in A$ such that $xz = y$.

Exercise 3.4 The properties of commutative groups asserted in Exercise 2.7 in additive notation, applied to the group $\langle A', \cdot' \rangle$, where $A' = A - \{0\}$, read as follows:

For all $x, y, z \in A'$,

(1) $1/(1/x) = x$,
(2) $x \cdot (1/y) = x/y$,
(3) $1/xy = (1/x)(1/y) = (1/x)/y$,
(4) $(x/y)(y/z) = x/z$,
(5) $1/(x/y) = y/x$.

Also, for all $x, z \in A$, $y, t \in A'$,

$$x/y + z/t = (xt + zy)/yt.$$

Order. As in the case of $\boldsymbol{Z}$, we begin by introducing a set of positive elements.

Notation: We let $Q^+ = \{x \mid ab >_Z 0_Z \text{ for some } (a, b) \in x\}$.

THEOREM 3.9 *If* $ab >_Z 0_Z$ *and* $(a, b) \sim (c, d)$, *then* $cd >_Z 0_Z$.

PROOF: From $ad = cb$, we have $(cb)(ad) = (cb)(cb)$. Hence, $(ab)(cd) = (cb)(cb)$. By Exercise 2.18, $(cb)(cb) >_Z 0_Z$ in $\boldsymbol{Z}$. But then $(ab)(cd) >_Z 0_Z$ in $\boldsymbol{Z}$ and, since $ab >_Z 0_Z$ in $\boldsymbol{Z}$, we have $cd >_Z 0_Z$ in $\boldsymbol{Z}$ (Exercise 2.14).

COROLLARY $Q^+ = \{x \mid ab > 0 \text{ for all } (a, b) \in x\}$.

THEOREM 3.10 Q^+ *is a set of positive elements for* $\boldsymbol{Q}$.

PROOF: We show that Q^+ satisfies (1), (2), and (3) of Definition 2.10. If $x, y \in Q^+$, then $x = C_{(a, b)}$, $y = C_{(c, d)}$, where $a, b, c, d \in \boldsymbol{Z}$, and

(1) $$ab >_Z 0_Z, \qquad cd >_Z 0_Z.$$

Hence,

$$x + y = C_{(a, b)} + C_{(c, d)} = C_{(ad + cb,\ bd)}.$$

By (1), Theorem 2.16, and Exercise 2.10,

$$(ad + cb)bd = abdd + cdbb >_Z 0_Z.$$

Hence, $x + y \in Q^+$, and (1) of Definition 2.10 is fulfilled.

Also, $x \cdot y = C_{(a,b)} \cdot C_{(c,d)} = C_{(ac,bd)}$, and $(ac)(bd) >_Z 0_Z$, so that $x \cdot y \in Q^+$, and (2) of Definition 2.10 is fulfilled.

Finally, if $x = C_{(a,b)}$, then, by the trichotomy property of order in Z, exactly one of

$$ab >_Z 0_Z \qquad ab = 0_Z \qquad -ab >_Z 0_Z$$

must hold. But, by Theorem 3.9,

$$ab >_Z 0_Z \text{ if and only if } x \in Q^+,$$
$$(-a) \cdot b = -ab >_Z 0_Z \text{ if and only if } C_{(-a,b)} = -x \in Q^+,$$

and, since $b \neq 0_Z$ and Z is an integral domain,

$$ab = 0_Z \text{ if and only if } a = 0_Z, \text{ and } x = C_{(0,b)} = 0_Q.$$

Thus, Q^+ satisfies (3) of Definition 2.10.

By Theorem 2.19 (1), we have

THEOREM 3.11 *The set* $T = \{(x, y) \mid y - x \in Q^+\}$ *is an order relation in* Q.

Notation: We write $x <_Q y$ ($y >_Q x$) if $(x, y) \in T$. We usually omit the subscript Q.

By Theorem 2.19 (2) we have

THEOREM 3.12 $\langle Q, +_Q, \cdot_Q <_Q \rangle$ *is an ordered integral domain.*

DEFINITION 3.5 If $\langle A, +, \cdot, < \rangle$ is an ordered integral domain such that $\langle A, +, \cdot \rangle$ is a field, then $\langle A, +, \cdot, < \rangle$ is called an *ordered field.*

Embedding. We now show that the ordered field $\langle Q, +_Q, \cdot_Q <_Q \rangle$ is an extension of the ordered integral domain $\langle Z, +_Z, \cdot_Z, <_Z \rangle$.

THEOREM 3.13 *The mapping* $E = E_Z^Q$ *of* Z *into* Q *such that for each* $a \in Z$, $E(a) = C_{(a,1)}$, *is an isomorphism of* Z *into* Q *preserving addition, multiplication, and order.*

PROOF: E is a 1–1 mapping of $\boldsymbol{Z}$ into $\boldsymbol{Q}$. For, if $E(a) = E(b)$, then $C_{(a,\,1)} = C_{(b,\,1)}$; hence, $a \cdot 1 = b \cdot 1$, and $a = b$.

For $a, b \in \boldsymbol{Z}$, $E(a + b) = C_{(a+b,\,1)} = C_{(a,\,1)} + C_{(b,\,1)} = E(a) + E(b)$. Thus, E preserves addition.

For $a, b \in \boldsymbol{Z}$, $E(ab) = C_{(ab,\,1)} = C_{(a,\,1)}C_{(b,\,1)} = E(a) \cdot E(b)$. Thus, E preserves multiplication.

For $a, b \in \boldsymbol{Z}$, $a <_{\boldsymbol{Z}} b$ if and only if $b - a \in \boldsymbol{Z}^+$, i.e., if and only if $C_{(b-a,\,1)} = C_{(b,\,1)} - C_{(a,1)} = E(b) - E(a) \in \boldsymbol{Q}^+$, and $E(a) <_{\boldsymbol{Q}} E(b)$.

•*Exercise* 3.5 If F is a 1–1 mapping of an ordered field A into an ordered field B which preserves addition and maps positive elements to positive elements, then F preserves order.

Notations: In view of the embedding isomorphisms $E_{\boldsymbol{N}}^{\boldsymbol{Z}}$ and $E_{\boldsymbol{Z}}^{\boldsymbol{Q}}$, we shall from now on use the same notation for elements of $\boldsymbol{Z}$ and their images in $\boldsymbol{Q}$. Since we have previously used "n" to denote $E_{\boldsymbol{N}}^{\boldsymbol{Z}}(n) = C_{(S(n),\,1)}$ in $\boldsymbol{Z}$, we now use "n" to denote $E_{\boldsymbol{Z}}^{\boldsymbol{Q}}(E_{\boldsymbol{N}}^{\boldsymbol{Z}}(n)) = C_{(n,\,1)}$ in $\boldsymbol{Q}$. We note that $E_{\boldsymbol{Z}}^{\boldsymbol{Q}}(E_{\boldsymbol{N}}^{\boldsymbol{Z}}(1)) = 1_{\boldsymbol{Q}}$, and $E_{\boldsymbol{Z}}^{\boldsymbol{Q}}(0) = 0_{\boldsymbol{Q}}$, so that we are justified in writing 1 and 0 for $1_{\boldsymbol{Q}}$ and $0_{\boldsymbol{Q}}$, respectively. Finally, since for $h \in \boldsymbol{Z}$, $k \neq 0$ in $\boldsymbol{Z}$,

$$C_{(h,\,k)} = C_{(h,\,1)}/C_{(k,\,1)} = E_{\boldsymbol{Z}}^{\boldsymbol{Q}}(h)/E_{\boldsymbol{Z}}^{\boldsymbol{Q}}(k),$$

we write h/k for the rational number $C_{(h,\,k)}$.

We also use "$\boldsymbol{N}$" and "$\boldsymbol{Z}$" to designate, respectively, the images of $\boldsymbol{N}$ and $\boldsymbol{Z}$ in $\boldsymbol{Q}$.

•*Exercise* 3.6 If x, y are rational numbers, then $x = h/n$, $y = k/n$ for some $h, k \in \boldsymbol{Z}$, $n \in \boldsymbol{Z}^+$. If x, y are positive rational numbers, then $x = p/n$, $y = q/n$ for some $p, q, n \in \boldsymbol{Z}^+$.

Exercise 3.7 Show that $\boldsymbol{Q}$ is denumerable, i.e., construct a 1–1 mapping of $\boldsymbol{N}$ onto $\boldsymbol{Q}$. Can such a mapping preserve addition or multiplication?

Ordered Fields. The ordered field of rational numbers plays a fundamental role among all ordered fields. We shall show that the rational field may be isomorphically embedded in every ordered field.

Let $\langle A, +, \cdot, < \rangle$ be an ordered field, and let F be the mapping of $\boldsymbol{N}$ into A defined by

$$F(1) = 1_A$$
$$F(n + 1) = F(n) + 1_A$$

• *Exercise* 3.8(1) The set

$$G = F \cup \{(0, 0_A)\} \cup \{(-n, -F(n)) \mid n \in \boldsymbol{N}\}$$

is a 1–1 mapping of $\boldsymbol{Z}$ into A which preserves addition, multiplication, and order.

Notation: We write $k1_A$, or simply k, for the element $G(k)$ in A.

(2) The set

$$H = \{(h/k, h1_A/k1_A) \mid h/k \in \boldsymbol{Q}\}$$

is a 1–1 mapping of $\boldsymbol{Q}$ into A which preserves addition, multiplication and order. From Exercise 3.8 follows

THEOREM 3.14 *The ordered field of rational numbers may be isomorphically embedded in every ordered field.*

DEFINITION 3.6 We call the elements $h1_A/k1_A$ of an ordered field A *rational elements of* A and denote by "$\boldsymbol{Q}_A$" the set of all rational elements of A.

Absolute Value. For any ordered field $\langle A, +, \cdot, < \rangle$, there is a mapping of A into A which may be used to define *distance* in A.

DEFINITION 3.6 If $\langle A, +, \cdot, < \rangle$ is an ordered field, and F is the mapping of A into A defined by

$$F(x) = \max \{x, -x\},$$

then for $x \in A$, $F(x)$ is called the *absolute value* of x, and is denoted by $|x|$.

(Note: By the trichotomy of the order relation in A, there exists such a mapping.)

In the following, $\langle A, +, \cdot, < \rangle$ is an ordered field.

• *Exercise* 3.9 For $x \in A$, $|x| = |-x| \geqq 0$,

$$x \leqq |x| \quad \text{and} \quad -x \leqq |x|,$$
$$|x| = 0 \text{ if and only if } x = 0.$$

THEOREM 3.15 *For* $x, y \in A$, $|x + y| \leqq |x| + |y|$.

PROOF: By Exercises 3.9 and 2.14, it follows that

$$x + y \leqq |x| + |y| \text{ and } -(x + y) \leqq |x| + |y|.$$

By Definition 3.6, $|x + y|$ is one of $x + y$, $-(x + y)$. Hence,

$$|x + y| \leqq |x| + |y|.$$

• *Exercise* 3.10 For $x, y \in A$, $|xy| = |x| \cdot |y|$, and

$$|x| - |y| \leqq ||x| - |y|| \leqq |x - y|.$$

Dense Orders; Archimedean Orders. In the ordered integral domain, $\boldsymbol{Z}$, there are *consecutive elements*: if a is any integer, then there is no integer between a and $a + 1$. In an ordered field, on the other hand, there is always another element of the field between any two given elements.

DEFINITION 3.7 An order relation $<$ in a set A is called *dense* if, for any a, b such that $a < b$ in A, there is some $c \in A$ such that $a < c < b$.

THEOREM 3.16 *If* $\langle A, +, \cdot, < \rangle$ *is an ordered field, then the order in* A *is dense.*

PROOF: If $a < b$ in A, then

$$2a = a + a < a + b < b + b = 2b.$$

Since $2 = 1_A + 1_A > 0_A$ in A, it follows that $1/2 > 0$ in A, and $a < (a + b)/2 < b$.

COROLLARY *Between any two rational numbers, there is another rational number.*

Exercise 3.11 Between any two elements of an ordered field, there is an infinite number of elements of the field.

Another important property of the order in $\boldsymbol{Q}$ is that every positive element has arbitrarily large integral multiples. This is not true in all ordered fields, as we shall see.

DEFINITION 3.8 An ordered field $\langle A, +, \cdot \rangle$, $<$ is called Archimedean if, for any $a, b \in A$ such that $0 < a < b$ in A, there is some $n \in \boldsymbol{N}$ such that $na \geqq b$.

THEOREM 3.17 $\langle \boldsymbol{Q}, +, \cdot, < \rangle$ *is Archimedean.*

PROOF: If $0 < x < y$, then (Exercise 3.6) there are positive integers p, q, r such that $x = p/r$, $y = q/r$. Then

$$0 < \frac{p}{r} < \frac{q}{r}$$

and

$$\frac{p}{r} \cdot rq = pq \geqq q \geqq \frac{q}{r}.$$

Thus, for $n = rq$, $nx \geqq y$.

•*Exercise* 3.12 Let K be the set of all formal Laurent series $\sum_{-\infty}^{\infty} r_j x^j$, $r_j \in Q$ for each $j \in Z$, such that for negative j only a finite number of coefficients r_j are different from zero.

Define addition in K by

$$\sum_{-\infty}^{\infty} r_j x^j + \sum_{-\infty}^{\infty} s_j x^j = \sum_{-\infty}^{\infty} (r_j + s_j) x^j,$$

multiplication in K by

$$\sum_{-\infty}^{\infty} r_j x^j \cdot \sum_{-\infty}^{\infty} s_j x^j = \sum_{-\infty}^{\infty} \Big(\sum_{p+q=j} r_p s_q \Big) x^j,$$

and order by

$$\sum_{-\infty}^{\infty} r_j x^j < \sum_{-\infty}^{\infty} s_j x^j$$

if there is an integer, k, such that

$$r_j = s_j \text{ for all } j < k$$

and

$$r_k < s_k.$$

Prove: $\langle K, +, \cdot, < \rangle$ is an ordered field whose order is not Archimedean.

In spite of its density, there are *gaps* in the order of Q in a sense described in the next two exercises.

•*Exercise* 3.13 For all $x \in Q$, $x^2 \neq 2$.

Hint: If $x^2 = 2$ for $x \in Q$, there exists a least positive integer, a, such that for some $b \in Q$, $a^2 = 2b^2$. Use the results of Exercise 2.27 to reach a contradiction.

Thus, Q contains no square root of 2 in the familiar sense. Now consider the following sets of rational numbers:

$$X = \{x \mid x < 0 \text{ or } x^2 < 2\}$$
$$Y = \{x \mid x > 0 \text{ and } x^2 > 2\}$$

In X are all negative rational numbers and all positive numbers whose squares are less than 2. In Y are all positive rational numbers whose squares are greater than 2.

•*Exercise* 3.14 If X and Y are the sets just defined, then

(1) X and Y are not empty,
(2) there is no element both in X and in Y,
(3) if $x \in Q$, then $x \in X$ or $x \in Y$,
(4) if $x \in X$ and $y \in Y$, then $x < y$,
(5) there is no largest element in X and no smallest element in Y.

DEFINITION 3.9 If $\langle A, +, \cdot, < \rangle$ is an ordered field, then the ordered pair (X, Y) is a *cut* in A if X and Y are non-empty subsets of A such that

(1) $X \cap Y = \emptyset$,
(2) $X \cup Y = A$,
(3) if $x \in X$, $y \in Y$, then $x < y$.

The sets X and Y are called, respectively, the *lower class* and the *upper class* of the cut.

A cut is a *gap* if its lower class has no greatest element, and its upper class has no smallest element, in A.

We note that the ordered pair (X, Y) of Exercise 3.14 is a cut and, in fact, a gap, in Q due to the absence in Q of a square root of 2. In Chapter 4, we shall embed the ordered field Q in an ordered field R in which there are no gaps. This will be the field of real numbers. In the construction of R, we shall employ sequences of rational numbers. We recall the following definition:

DEFINITION 3.10 A mapping F of N into a set A is called a *sequence* in A. If $F(n) = a_n$ for each n, we write (a_n) for the mapping F. If $a_n = a$ for each n, we write (a) for (a_n).

The following theorem shows that every gap in Q is "quite narrow" and can be "approximated" by sequences of rational numbers. In

extending Q to the field of real numbers, we fill each gap by an equivalence class whose elements are the sequences which approximate the gap.

THEOREM 3.18 *If (X, Y) is a gap in Q, then there are sequences (x_n), (y_n) in Q such that for each $n \in N$,*

$$x_n \in X, \quad y_n \in Y$$

$$y_n - x_n = \frac{1}{n}$$

and

$$|x_m - x_n| < \frac{1}{n}, \; |y_m - y_n| < \frac{1}{n} \text{ in } Q$$

for all $m \geqq n$ in N.

PROOF: Since (X, Y) is a cut, X and Y are not empty. If $x \in X$ and $y \in Y$, then $y - x > 0$ in Q. For each $n \in N$, $1/n > 0$ in Q and, since the order in Q is Archimedean, there is some $k_n \in N$ such that $k_n/n \geqq y - x$ in Q. Since $y \in Y$ and $x + k_n/n \geqq y$, $x + k_n/n$ is an element of Y. Hence, for each $n \in N$, the set

$$M_n = \left\{ m \;\middle|\; x + \frac{m}{n} \in Y \right\}$$

is a non-empty subset of N and contains a first element m_n (Theorem 1.18). Now, for each $n \in N$,

$$x_n = x + \frac{m_n - 1}{n} \in X, \quad y_n = x + \frac{m_n}{n} \in Y,$$

and

$$y_n - x_n = \frac{1}{n}.$$

Since (X, Y) is a cut in Q, $x_n < y_m$ in Q for all $m, n \in N$. Hence

$$x_n < y_m = x_m + \frac{1}{m} \quad \text{and} \quad x_m < y_n = x_n + \frac{1}{n} \text{ for all } m, n \in N.$$

Therefore, for each $n \in N$ and all $m \geqq n$ in N,

$$|x_m - x_n| = \max\{x_m - x_n, x_n - x_m\} < \max\left\{\frac{1}{n}, \frac{1}{m}\right\} = \frac{1}{n}$$

and

$$|y_m - y_n| = \max\{y_m - y_n, y_n - y_m\} < \max\left\{\frac{1}{m}, \frac{1}{n}\right\} = \frac{1}{n}$$

in Q.

Sequences in Ordered Fields. In the following, we let $\langle A, +, \cdot, < \rangle$ be an ordered field. According to Definition 3.10, a sequence in A is a mapping F of N into A. We write (a_n) for F, where $a_n = F(n) \in A$ for each $n \in N$.

DEFINITION 3.11 A sequence (a_n) in A is called *bounded* if there is some $a \in A$ such that

$$|a_n| < a \text{ in } A \text{ for all } n \in N.$$

Exercise 3.15 If (a_n), (b_n) are bounded sequences in A, then $(a_n \pm b_n)$ and $(a_n b_n)$ are bounded sequences in A.

DEFINITION 3.12 A sequence (a_n) in A is called *fundamental* if for each $e > 0$ in A there is some $n_e \in N$ such that

$$|a_n - a_m| < e \text{ in } A \text{ for all } m, n \geqq n_e \text{ in } N.$$

Note that the sequences approximating the gap in Theorem 3.18 are fundamental sequences in Q (Theorem 3.17).

THEOREM 3.19 *If (a_n) is a fundamental sequence in A, then (a_n) is a bounded sequence.*

PROOF: Let e be any positive element of A. Then, by Definition 3.12, there is some $n_e \in N$ such that

(1) $|a_n - a_m| < e$ in A for all $m, n \geqq n_e$ in N.

The finite subset $\{|a_1|, \ldots, |a_{n_e}|\}$ of A contains a maximum element b (Exercise 1.18). Hence,

(2) $|a_n| \leqq b$ in A for $n \leqq n_e$ in N,

and, by (1),

(3) $|a_n| \leqq |a_n - a_{n_e}| + |a_{n_e}| < e + |a_{n_e}|$ in A

for all $n > n_e$ in N.

It follows from (2) and (3), by trichotomy, that

$$|a_n| \leqq e + b \text{ in } A$$

for all $n \in N$.

THEOREM 3.20 *If (a_n) and (b_n) are fundamental sequences in A, then $(a_n + b_n)$ and $(a_n b_n)$ are fundamental sequences.*

PROOF: Let e be any positive element in A. Then $e/2 > 0$ in A and, by hypothesis, there are $n'_e, n''_e \in N$ such that

(1) $|a_n - a_m| < e/2$ in A for all $n, m \geqq n'_e$ in N,

(2) $|b_n - b_m| < e/2$ in A for all $n, m \geqq n''_e$ in N.

Let $n_e = \max\{n'_e, n''_e\}$ in N. Then, by (1) and (2),

$$|(a_n + b_n) - (a_m + b_m)| \leqq |a_n - a_m| + |b_n - b_m| < e/2 + e/2 = e \quad \text{for all } n, m \geqq n_e \text{ in } N.$$

Hence, $(a_n + b_n)$ is a fundamental sequence in A.

By Theorem 3.19, (a_n), (b_n) are bounded sequences, so there are positive elements a and b in A such that

(3) $|a_n| < a$ and $|b_n| < b$ in A for all $n \in N$.

Since $e/2b$ and $e/2a$ are positive in A, there are n'_e, $n''_e \in N$ such that

(4) $|a_n - a_m| < e/2b$ in A for all $m, n \geqq n'_e$ in N

and

(5) $|b_n - b_m| < e/2a$ in A for all $m, n \geqq n''_e$ in N.

Let $n_e = \max\{n'_e, n''_e\}$ in N. By (3), (4), and (5),

$$|a_n b_n - a_m b_m| \leqq |a_n| \cdot |b_n - b_m| + |b_m| \cdot |a_n - a_m| < a \cdot e/2a + b \cdot e/2b = e \text{ in } A \text{ for all } m, n \geqq n_e \text{ in } N.$$

Hence, $(a_n b_n)$ is a fundamental sequence in A.

DEFINITION 3.13 A sequence (a_n) *converges* to a in A if, for each $e > 0$ in A, there is some $n_e \in N$ such that

$$|a_n - a| < e \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

We call a a *limit* of (a_n) in A.

THEOREM 3.21 *A sequence (a_n) has at most one limit in A.*

PROOF: Suppose a' and a'' are both limits of (a_n). Let e be any positive element in A. Then $e/2 > 0$ in A and there are n'_e, n''_e in N such that

$$|a_n - a'| < e/2 \text{ in } A \text{ for all } n \geqq n'_e \text{ in } N,$$

and

$$|a_n - a''| < e/2 \text{ in } A \text{ for all } n \geqq n''_e \text{ in } N.$$

Let $n_e = \max\{n'_e, n''_e\}$ in N. Then

$$|a' - a''| \leqq |a' - a_n| + |a_n - a''| < e \text{ in } A \text{ for all } n \geqq n_e.$$

Since $0 \leqq |a' - a''| < e$ in A for all $e > 0$, $a' = a''$.

Notation: If (a_n) is convergent, we denote its limit by "$L(a_n)$".

•*Exercise* 3.16 If the order in A is Archimedean, then

$$L\left(\frac{1}{n}\right) = 0 \quad \text{and} \quad L\left(\frac{1}{p^n}\right) = 0 \text{ for all } p \neq 1 \text{ in } N.$$

THEOREM 3.22 *If (a_n) is a convergent sequence in A, then (a_n) is a fundamental sequence.*

PROOF: Let $a = L(a_n)$ and let e be any positive element in A. Then $e/2 > 0$ in A, and, since a is the limit of (a_n), there is some $n_e \in N$ such that

$$|a_n - a| < e/2 \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

Hence,

$$|a_n - a_m| \leqq |a_n - a| + |a - a_m| < e \text{ in } A \text{ for all } m, n \geqq n_e \text{ in } N.$$

•*Exercise* 3.17

(1) If (a_n) is a convergent sequence in A, then (a_n) is a bounded sequence.

(2) If $|a_n| \leqq b$ for all $n \in N$ and $L(a_n) = a$, then $|a| \leqq b$.

THEOREM 3.23 *If $L(a_n) = a$ and $L(b_n) = b$ in A, then*

(1) $L(a_n + b_n) = a + b$

and

(2) $L(a_n b_n) = ab$.

PROOF: Let e be any positive element in A. By hypothesis, there are n'_e, n''_e in N such that

(3) $|a_n - a| < e/2$ in A for all $n \geqq n'_e$ in N,
$|b_n - b| < e/2$ in A for all $n \geqq n''_e$ in N.

Let $n_e = \max\{n'_e, n''_e\}$ in N. Then, by (3),

$$|(a_n + b_n) - (a + b)| \leqq |a_n - a| + |b_n - b| < e \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

This proves (1).

By Exercise 3.17 (1), there are a', b' in A such that

$$|a_n| < a' \quad \text{and} \quad |b_n| < b' \text{ for all } n \in N.$$

Let $c = \max\{a', b'\}$ in A. Then $e/2c > 0$ in A and, by hypothesis, there are $\overline{n}_e$, $\overline{\overline{n}}_e$ in N such that

$$(4)\quad \begin{aligned} |a_n - a| &< e/2c \text{ in } A \text{ for all } n \geqq \overline{n}_e \text{ in } N, \\ |b_n - b| &< e/2c \text{ in } A \text{ for all } n \geqq \overline{\overline{n}}_e \text{ in } N. \end{aligned}$$

Let $\tilde{n}_e = \max\{\overline{n}_e, \overline{\overline{n}}_e\}$ in N. Then, by (4) and Exercise 3.18 (2),

$$|a_n b_n - ab| \leqq |a_n||b_n - b| + |b||a_n - a| < a' \frac{e}{2c} + b' \frac{e}{2c} \leqq e \text{ in } A$$
$$\text{for all } n \geqq \tilde{n}_e \text{ in } N.$$

This proves (2).

•*Exercise* 3.18

(1) For all $a \in A$, if $L(a_n) = a$ in A, then $L(|a_n|) = |a|$.

(2) Show that the converse of (1) is false in the field Q.

(3) $L(|a_n|) = 0$ in A if and only if $L(a_n) = 0$.

THEOREM 3.24 *There are non-convergent fundamental sequences in* Q.

PROOF: Let (X, Y) be the gap (associated with "the missing $\sqrt{2}$") of Exercise 3.14. Let (x_n), (y_n) be defined as in Theorem 3.18 for the gap (X, Y). We recall that $y_n = x_n + 1/n < y + 1$ for all $n \in N$, all $y \in Y$. By Exercise 3.16, (x_n) is a fundamental sequence in Q.

But (x_n) is not convergent in Q. Otherwise $L(x_n) = z \in Q$ and, by Theorem 3.23, $L(x_n^2) = z^2$. Now, for each $n \in N$,

$$0 < 2 - x_n^2 < y_n^2 - x_n^2 = (y_n - x_n)(y_n + x_n) < \frac{2y_n}{n} < \frac{2(y+1)}{n}.$$

Since $L(1/n) = 0$ in Q (Exercise 3.16), $L(x_n^2) = 2$ in Q. Hence, by Theorem 3.21, $x^2 = 2$ for $x \in Q$. This is impossible by Exercise 3.13.

Exercise 3.19 Show that the conditions stated below define a sequence (a_n) which is fundamental but not convergent in Q:

$$a_1 = 1$$
$$a_{n+1} = a_n + \frac{b_n}{10^n},$$

where b_n is a non-negative integer such that

$$\left(a_n + \frac{b_n}{10^n}\right)^2 < 2 < \left(a_n + \frac{b_n + 1}{10^n}\right)^2$$

Note: The a_n are "decimal approximations to $\sqrt{2}$".

THEOREM 3.25 *If (a_n) is a fundamental sequence which does not have limit zero in A, then there is a fundamental sequence (b_n) in A such that $L(a_nb_n) = 1$.*

PROOF: Since (a_n) does not have limit zero in A, there is a positive element $\bar{e}$ in A such that for every $n \in N$,

(1) $|a_k| \geqq \bar{e}$ in A for some $k \geqq n$ in N.

Since (a_n) is a fundamental sequence, there is an $\bar{n} \in N$ such that

(2) $|a_m - a_n| < \frac{\bar{e}}{2}$ in A for all $m, n \geqq \bar{n}$ in N.

If, for $\bar{k} > \bar{n}$,

(3) $|a_{\bar{k}}| \geqq \bar{e}$,

then

(4) $|a_n| = |a_{\bar{k}} - (a_{\bar{k}} - a_n)| \geqq |a_{\bar{k}}| - |a_{\bar{k}} - a_n| > \bar{e} - \frac{\bar{e}}{2} = \frac{\bar{e}}{2}$

for all $n \geqq \bar{n}$. Hence, $a_n \neq 0$ for all $n \geqq \bar{n}$.

Now let

(5) $b_1 = 1$ for $n < \bar{n}$
$b_n = 1/a_n$ for $n \geqq \bar{n}$.

Then (b_n) is a sequence in A. If e is any positive element of A, then there is some $n_e \in N$ such that

$$|a_m - a_n| < \frac{\bar{e}^2 e}{4}$$

for all $m, n \geqq n_e$. Hence, by (4) and (5),

$$|b_m - b_n| = \frac{|a_m - a_n|}{|a_m||a_n|} < \frac{\bar{e}^2 e}{4} \cdot \frac{4}{\bar{e}^2} = e$$

for all $m, n \geqq \max(\bar{n}, n_e)$. It follows that (b_n) is a fundamental sequence in A.

Since $a_nb_n = 1$ for all $n \geqq \bar{n}$, $L(a_nb_n) = 1$.

DEFINITION 3.14 A sequence (a_n) in A is called *positive* if, for some positive e in A and some $k \in N$,

$$a_n \geqq e \text{ in } A \text{ for all } n \geqq k \text{ in } N.$$

Exercise 3.20 The sequence $1/n$ in Q is not positive.

THEOREM 3.26 *If (a_n) is a fundamental sequence in A, then exactly one of the following statements is true*:

(1) $L(a_n) = 0$.
(2) (a_n) *is positive.*
(3) $(-a_n)$ *is positive.*

PROOF: We first show that at least one of (1), (2), and (3) is true. Suppose (1) is false. Then there is a positive element e in A such that for each $m \in N$

$$(4) \quad |a_k| \geqq e \text{ in } A \text{ for some } k \geqq m \text{ in } N.$$

Since $e/2 > 0$ in A and (a_n) is a fundamental sequence, there is some $n_e \in N$ such that

$$(5) \quad |a_n - a_m| < e/2 \text{ in } A \text{ for all } m, n \geqq n_e \text{ in } N.$$

By (4), with $m = n_e$,

$$(6) \quad \max\{a_k, -a_k\} = |a_k| \geqq e \text{ in } A \text{ for some } k \geqq n_e \text{ in } N.$$

If $a_k \geqq e$ then, by (5),

$$a_n = a_k - (a_k - a_n) \geqq e - |a_k - a_n| > e/2 \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

Hence, by Definition 3.14, (a_n) is positive and (2) is true. Otherwise, by (6), $-a_k \geqq e$ and, again by (5),

$$-a_n = -a_k - (a_n - a_k) \geqq e - |a_n - a_k| > e/2 \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

Hence, $(-a_n)$ is positive and (3) is true.

Next we show that not more than one of the three statements is true. If $L(a_n) = 0$, then for each $e > 0$ in A there is some n_e in N such that

$$\max\{a_n, -a_n\} = |a_n| < e \text{ in } A \text{ for all } n \geqq n_e \text{ in } N.$$

Hence there is no positive e in A such that, for some $k \in N$, either

$$a_n \geqq e \text{ in } A \text{ for all } n \geqq k \text{ in } N$$

or

$$-a_n \geqq e \text{ in } A \text{ for all } n \geqq k \text{ in } N.$$

Thus if (1) is true, then (2) and (3) are both false. If (2) and (3) are both true, then for some e' and e'', positive in A, and k', $k'' \in N$,

$$a_n \geqq e' \text{ in } A \text{ for all } n \geqq k' \text{ in } N$$

and

$$-a_n \geqq e'' \text{ in } A \text{ for all } n \geqq k'' \text{ in } N.$$

Hence, for $n = \max\{k', k''\}$ in N,

$$0 < e'' \leqq -a_n \leqq -e' < 0 \text{ in } A.$$

But this is impossible.

It follows that exactly one of (1), (2), and (3) must hold.

•*Exercise* 3.21 Let F_A be the set of all fundamental sequences in the ordered field A. Let T be the subset of $F_A \times F_A$ consisting of those $((a_n), (b_n)) \in F_A \times F_A$ for which $(b_n - a_n) \in F_A$ is positive. Show that T is not an order relation in F_A.

Exercise 3.22 A fundamental sequence (a_n) in A is positive if and only if $(|a_n|)$ is positive.

•*Exercise* 3.23 If (a_n) and (b_n) are positive fundamental sequences in A, then $(a_n + b_n)$ and $(a_n b_n)$ are positive in A.

•*Exercise* 3.24 If A and B are ordered fields and F is a 1–1 mapping of A onto B preserving addition, multiplication, and order, then

(1) (a_n) is a fundamental sequence in A if and only if $(F(a_n))$ is a fundamental sequence in B;
(2) $L(a_n) = a$ if and only if $L(F(a_n)) = F(a)$;
(3) (a_n) is a positive sequence in A if and only if $(F(a_n))$ is a positive sequence in B.

•*Exercise* 3.25 If (x_n) is a convergent sequence in an ordered field A, then (x_n) is a positive sequence in A if and only if $L(x_n) > 0$ in A.

CHAPTER 4

THE REAL NUMBERS

Preliminaries. We introduced the integers as equivalence classes of ordered pairs of natural numbers, and the rational numbers as equivalence classes of ordered pairs of integers. In the construction of the real numbers we again begin with the definition of an equivalence relation. In this case, the equivalence relation will be defined in the set of all fundamental rational sequences.

Thus, a real number will be an equivalence class of fundamental rational sequences. By suitable definitions of addition, multiplication, and order, the set $\boldsymbol{R}$ of all real numbers will be made into an ordered field which will be an extension of the ordered field $\boldsymbol{Q}$. The order in $\boldsymbol{R}$ will have no gaps in the sense of Definition 3.9. Equivalently, every fundamental sequence of real numbers will have a limit in $\boldsymbol{R}$, i.e., the converse of Theorem 3.22 (which is false in $\boldsymbol{Q}$, by Theorem 3.24) will hold in $\boldsymbol{R}$.

The Field R. We shall use "F_Q" to denote the set of all fundamental rational sequences.

THEOREM 4.1 *There is an equivalence relation Q in F_Q such that $(x_n)Q(y_n)$ holds whenever $L(x_n - y_n) = 0$.*

PROOF: The set

$$\dot{Q} = \{((x_n), (y_n)) \mid L(x_n - y_n) = 0\}$$

is a subset of $F_Q \times F_Q$. Since $L(x_n - x_n) = L(0) = 0$ for each $(x_n) \in F_Q$, Q is reflexive. If $L(x_n - y_n) = 0$, then $L(-[x_n - y_n]) = L(y_n - x_n) = 0$, so that Q is symmetric.

If $L(x_n - y_n) = 0$ and $L(y_n - z_n) = 0$, then $L(x_n - z_n) = L(x_n - y_n + y_n - z_n) = L([x_n - y_n] + [y_n - z_n]) = L(x_n - y_n) + L(y_n - z_n) = 0$. Hence, Q is transitive.

As usual, we write $(x_n) \sim (y_n)$ if the pair $((x_n), (y_n)) \in Q$, and denote by "$C_{(x_n)}$" the equivalence class containing (x_n).

Exercise 4.1 For $(x_n) \in F_Q$, $L(x_n) = a$ if and only if $(x_n) \sim (a)$.

DEFINITION 4.1 A *real number* is an equivalence class $C_{(x_n)}$ with respect to the equivalence relation Q of Theorem 4.1, where (x_n) is a fundamental rational sequence.

We denote by $\boldsymbol{R}$ the set of all real numbers and note that $\boldsymbol{R}$ is the factor set F_Q/Q. We use $\xi, \eta, \ldots$ to denote real numbers.

Addition and Multiplication in $\boldsymbol{R}$.

THEOREM 4.2 If (x_n), (y_n), (x'_n), $(y'_n) \in F_Q$, $(x_n) \sim (x'_n)$ *and* $(y_n) \sim (y'_n)$, *then*

(1) $(x_n + y_n) \sim (x'_n + y'_n)$

and

(2) $(x_n y_n) \sim (x'_n y'_n)$.

PROOF:

(1) By Theorem 3.23, $L([x_n + y_n] - [x'_n + y'_n]) = L(x_n - x'_n + y_n - y'_n) = L(x_n - x'_n) + L(y_n - y'_n) = 0 + 0 = 0$ in $\boldsymbol{Q}$.

(2) By Theorem 3.19, since (x_n), $(y'_n) \in F_Q$, there exist $a, b \in \boldsymbol{Q}$ such that $|x_n| < a$, $|y'_n| < b$ for all $n \in \boldsymbol{N}$.

By Theorem 3.20, $(x_n y_n)$ and $(x'_n y'_n)$ are fundamental sequences in $\boldsymbol{Q}$.

Since $(x_n) \sim (x'_n)$ and $(y_n) \sim (y'_n)$, there are, for each positive e in $\boldsymbol{Q}$, n'_e and n''_e in $\boldsymbol{N}$ such that

$$|x_n - x'_n| < \frac{e}{2b} \text{ in } \boldsymbol{Q} \text{ for all } n \geqq n'_e \text{ in } \boldsymbol{N}$$

and

$$|y_n - y'_n| < \frac{e}{2a} \text{ in } \boldsymbol{Q} \text{ for all } n \geqq n''_e \text{ in } \boldsymbol{N}.$$

Hence,

$$|x_n y_n - x'_n y'_n| \leqq |x_n||y_n - y'_n| + |y'_n||x_n - x'_n|$$

$$< a \cdot \frac{e}{2a} + b \cdot \frac{e}{2b} = e$$

$$\text{for all } n \geqq n_e = \max\{n'_e, n''_e\} \text{ in } \boldsymbol{N}.$$

Therefore $L(x_n y_n - x'_n y'_n) = 0$ in $\boldsymbol{Q}$ and $(x_n y_n) \sim (x'_n y'_n)$.

THEOREM 4.3 *There are binary operations F and G on $\boldsymbol{R}$ such that, if $(x_n) \in \xi$ and $(y_n) \in \eta$, then*

(1) $F(\xi, \eta) = C_{(x_n + y_n)}$
(2) $G(\xi, \eta) = C_{(x_n y_n)}$.

PROOF: The sets

$$F = \{((\xi, \eta), C_{(x_n + y_n)}) \mid (x_n) \in \xi, (y_n) \in \eta; \xi, \eta \in \boldsymbol{R}\}$$

and

$$G = \{((\xi, \eta), C_{(x_n y_n)}) \mid (x_n) \in \xi, (y_n) \in \eta; \xi, \eta \in \boldsymbol{R}\}$$

are subsets of $(\boldsymbol{R} \times \boldsymbol{R}) \times \boldsymbol{R}$.

If $(\xi, \eta) \in \boldsymbol{R} \times \boldsymbol{R}$, then $\xi = C_{(x_n)}$, $\eta = C_{(y_n)}$ for some $(x_n), (y_n) \in F_Q$. Since $(x_n + y_n) \in F_Q$ by Theorem 3.20, the pair $((\xi, \eta), \zeta) \in F$ where $\zeta = C_{(x_n + y_n)}$. If $((\xi, \eta), \zeta') \in F$, then $\zeta' = C_{(x'_n + y'_n)}$ where $(x'_n) \in \xi$, $(y'_n) \in \eta$. By Theorem 4.2, since $(x'_n) \sim (x_n)$, $(y'_n) \sim (y_n)$, it follows that $(x'_n + y'_n) \sim (x_n + y_n)$ and $\zeta = \zeta'$. Thus F is a mapping of $(\boldsymbol{R} \times \boldsymbol{R})$ into $\boldsymbol{R}$, and hence a binary operation on $\boldsymbol{R}$.

If $(\xi, \eta) \in \boldsymbol{R} \times \boldsymbol{R}$, then $(x_n) \in \xi$ and $(y_n) \in \eta$ for some (x_n), $(y_n) \in F_Q$. By Theorem 3.20, $(x_n y_n) \in F_Q$. Hence, $((\xi, \eta), \zeta) \in G$ where $\zeta = C_{(x_n y_n)}$. If $((\xi, \eta), \zeta') \in G$, then $\zeta' = C_{(x'_n y'_n)}$ where $(x'_n) \in \xi$, $(y'_n) \in \eta$. By Theorem 3.20, since $(x'_n) \sim (x_n)$, $(y'_n) \sim (y_n)$, it follows that $(x_n y_n) \sim (x'_n y'_n)$, and $\zeta = \zeta'$. Thus G is a mapping of $\boldsymbol{R} \times \boldsymbol{R}$ into $\boldsymbol{R}$, and hence a binary operation on $\boldsymbol{R}$.

DEFINITION 4.2 We call the binary operations F and G of Theorem 4.3 *addition in $\boldsymbol{R}$* and *multiplication in $\boldsymbol{R}$*, respectively, and write "$\xi +_{\boldsymbol{R}} \eta$" and "$\xi \cdot_{\boldsymbol{R}} \eta$" for $F(\xi, \eta)$ and $G(\xi, \eta)$. As usual, we shall feel free to omit the subscript "$\boldsymbol{R}$".

THEOREM 4.4 *$\langle \boldsymbol{R}, +_{\boldsymbol{R}}, \cdot_{\boldsymbol{R}} \rangle$ is a field.*

PROOF: We leave to the reader the verification of the associative, commutative, and distributive properties. We note that $C_{(0)}$ serves as the additive identity, $0_{\boldsymbol{R}}$; $C_{(1)}$ as the multiplicative identity, $1_{\boldsymbol{R}}$; and $C_{(-x_n)}$ as the additive inverse $-C_{(x_n)}$ of $C_{(x_n)}$. If $C_{(x_n)} \neq 0_{\boldsymbol{R}}$, then (x_n) is not equivalent to (0), so that (x_n) does not have limit zero in $\boldsymbol{Q}$. By Theorem 3.25, there is a sequence $(y_n) \in F_{\boldsymbol{Q}}$ such that $L(x_n y_n) = 1_{\boldsymbol{Q}}$. Hence, $(x_n y_n) \sim (1)$, and $C_{(x_n)} C_{(y_n)} = C_{(x_n y_n)} = C_{(1)} = 1_{\boldsymbol{R}}$. Thus, $C_{(y_n)}$ is the multiplicative inverse, $\dfrac{1}{C_{(x_n)}}$, of $C_{(x_n)}$. It follows that $\langle \boldsymbol{R}, +_{\boldsymbol{R}}, \cdot_{\boldsymbol{R}} \rangle$ is a field.

Order in $\boldsymbol{R}$. We shall define the positive elements of $\boldsymbol{R}$ as the equivalence classes belonging to positive sequences in $F_{\boldsymbol{R}}$.

Notation: We let $\boldsymbol{R}^+ = \{\xi \mid$ for some $(x_n) \in \xi$, (x_n) is positive$\}$.

THEOREM 4.5 *If $(x_n) \sim (x'_n)$, and (x_n) is a positive sequence, then (x'_n) is a positive sequence.*

PROOF: If (x_n) is a positive sequence, then by Definition 3.14, there are $e > 0$ in $\boldsymbol{Q}$ and $n_e \in \boldsymbol{N}$ such that $x_n \geqq e$ for $n \geqq n_e$. Since $(x_n) \sim (x'_n)$, there is some n'_e in $\boldsymbol{N}$ such that

$$|x'_n - x_n| < \frac{e}{2} \text{ for } n \geqq n'_e \text{ in } \boldsymbol{N}.$$

Hence, $-\dfrac{e}{2} < x'_n - x_n < \dfrac{e}{2}$ for $n \geqq n'_e$. But then, if $\overline{n}_e = \max\{n_e, n'_e\}$ in $\boldsymbol{N}$,

$$x'_n = (x'_n - x_n) + x_n > -\frac{e}{2} + e = \frac{e}{2} > 0 \text{ for all } n \geqq n'_e.$$

Hence (x'_n) is a positive sequence in $\boldsymbol{Q}$.

COROLLARY $\boldsymbol{R}^+ = \{\xi \mid (x_n)$ *is positive for* all $(x_n) \in \xi\}$.

THEOREM 4.6 *$\boldsymbol{R}^+$ is a set of positive elements for $\boldsymbol{R}$.*

PROOF: We show that $\boldsymbol{R}^+$ satisfies (1), (2), and (3) of Definition 2.10.

If $\xi, \eta \in \boldsymbol{R}^+$, then $\xi = C_{(x_n)}$, $\eta = C_{(y_n)}$, where (x_n), (y_n) are positive sequences in $\boldsymbol{Q}$. By Exercise 3.24, $\xi + \eta = C_{(x_n + y_n)} \in \boldsymbol{R}^+$, and $\xi\eta = C_{(x_n y_n)} \in \boldsymbol{R}^+$, so that (1) and (2) are fulfilled.

If $\xi = C_{(x_n)}$, then, by the Corollary of Theorem 4.5,

$\xi \in \boldsymbol{R}^+$ if and only if (x_n) is a positive sequence in $\boldsymbol{Q}$,
$\xi = 0_{\boldsymbol{R}} = C_{(0)}$ if and only if $L(x_n) = 0_{\boldsymbol{Q}}$,
$-\xi = C_{(-x_n)} \in \boldsymbol{R}^+$ if and only if $(-x_n)$ is a positive sequence in $\boldsymbol{Q}$.

Hence, by Theorem 3.26, exactly one of

$$\xi \in \boldsymbol{R}^+, \qquad \xi = 0_{\boldsymbol{R}}, \qquad -\xi \in \boldsymbol{R}^+$$

must hold. Thus, (3) is fulfilled, and $\boldsymbol{R}^+$ is a set of positive elements for $\boldsymbol{R}$.

By Theorem 2.19 (1), we have

THEOREM 4.7 *The set* $T = \{(\xi, \eta) \mid \eta - \xi \in \boldsymbol{R}^+\}$ *is an order relation in* $\boldsymbol{R}$.

Notation: We write "$\xi <_{\boldsymbol{R}} \eta$" ("$\eta >_{\boldsymbol{R}} \xi$") if $(\xi, \eta) \in T$. Usually, we omit the subscript "$\boldsymbol{R}$".

By Theorem 2.19 (2), and Definition 3.5, we have

THEOREM 4.8 $\langle \boldsymbol{R}, +_{\boldsymbol{R}}, \cdot_{\boldsymbol{R}}, <_{\boldsymbol{R}} \rangle$ *is an ordered field.*

Embedding.

THEOREM 4.9 *The mapping* $E = E_{\boldsymbol{Q}}^{\boldsymbol{R}}$ *of* $\boldsymbol{Q}$ *into* $\boldsymbol{R}$ *such that* $E(x) = C_{(x)}$ *is an isomorphism of* $\boldsymbol{Q}$ *into* $\boldsymbol{R}$ *preserving addition, multiplication, and order.*

PROOF: E is a 1–1 mapping of $\boldsymbol{Q}$ into $\boldsymbol{R}$.

For, $C_{(x)} = C_{(y)}$ if and only if $(x) \sim (y)$, i.e., if and only if $x = y$ in $\boldsymbol{Q}$.

If $x, y \in \boldsymbol{Q}$, then

$$E(x + y) = C_{(x+y)} = C_{(x)} +_{\boldsymbol{R}} C_{(y)} = E(x) +_{\boldsymbol{R}} E(y),$$

and

$$E(xy) = C_{(xy)} = C_{(x)} \cdot_{\boldsymbol{R}} C_{(y)} = E(x) \cdot_{\boldsymbol{R}} E(y).$$

Thus, E preserves addition and multiplication.

Also, $x < y$ in $\boldsymbol{Q}$ if and only if $y - x > 0$ in $\boldsymbol{Q}$ so that $(y - x)$ is a positive sequence in $F_{\boldsymbol{Q}}$. On the other hand, $C_{(x)} < C_{(y)}$ in $\boldsymbol{R}$ if and only if $C_{(y)} - C_{(x)} > 0$ in $\boldsymbol{R}$, so that $(y - x)$ is a positive sequence in $F_{\boldsymbol{Q}}$. Thus, $x < y$ in $\boldsymbol{Q}$ if and only if $C_{(x)} <_{\boldsymbol{R}} C_{(y)}$ in $\boldsymbol{R}$, and E preserves order.

As usual, we shall identify Q with its isomorphic image in R and use interchangeably the symbols x and $C_{(x)}$.

•*Exercise* 4.2 For $(x_n) \in \dot{F}_Q$, $|C_{(x_n)}| = C_{(|x_n|)}$.

•*Exercise* 4.3 For every real number $\varepsilon > 0$ in R, there is a rational number e such that $0 < e < \varepsilon$ in R.

•*Exercise* 4.4 A rational sequence (x_n) is fundamental in Q if and only if it is fundamental in R.

Completeness of R. We have shown (Theorem 3.22) that in an ordered field every convergent sequence is fundamental and (Theorem 3.24) that the converse does not hold in the rational field.

DEFINITION 4.3 An ordered field A is called *complete* if every fundamental sequence in A is convergent.

We shall show that R is complete. We first prove that every fundamental rational sequence converges in R.

THEOREM 4.10 *If* $(x_n) \in \xi$, *then* $L(x_n) = \xi$ *in* R.

PROOF: For $\varepsilon > 0$ in R, let e be a rational number such that $0 < e < \varepsilon$. Since (x_n) is fundamental in Q, there is an n_e in N such that

$$|x_m - x_n| < \frac{e}{2} \text{ for all } m, n \geqq n_e.$$

Hence, for all $m, n \geqq n_e$,

$$e - |x_n - x_m| > \frac{e}{2}$$

and for each $n \geqq n_e$, $(y_m) = (e - |x_n - x_m|)$ is a positive fundamental sequence in R. It follows that, for each $n \geqq n_e$,

$$C_{(y_m)} = C_{(e-|x_n - x_m|)} > 0 \text{ in } R.$$

But then

$$|x_n - \xi| = |x_n - C_{(x_m)}| = C_{(|x_n - x_m|)} < C_{(e)} = e < \varepsilon \text{ for all } n \geqq n_e,$$

and

$$L(x_n) = \xi \text{ in } R.$$

COROLLARY 1 *If* $\xi \in R$ *and* $\varepsilon > 0$ *in* R, *there is an* $x \in Q$ *such that* $|\xi - x| < \varepsilon$ *in* R.

PROOF: If $(x_n) \in \xi$, then $\xi = L(x_n)$. Hence, for every $\varepsilon > 0$ in $\boldsymbol{R}$, there is an n_ε in $\boldsymbol{N}$ such that

$$|\xi - x_n| < \varepsilon \text{ in } \boldsymbol{R} \text{ for all } n \geqq n_\varepsilon.$$

In particular, for $x = x_{n_\varepsilon} \in \boldsymbol{Q}$, $|\xi - x| < \varepsilon$, as required.

COROLLARY 2 *If $\xi < \eta$ in $\boldsymbol{R}$, there is a $z \in \boldsymbol{Q}$ such that $\xi < z < \eta$.*

PROOF: By Theorem 3.16, there is a real number ζ such that $\xi < \zeta < \eta$. If $\varepsilon = \min\{\zeta - \xi, \eta - \zeta\}$, then, by Corollary 1, there is a rational number z such that $\xi \leqq \zeta - \varepsilon < z < \zeta + \varepsilon \leqq \eta$.

COROLLARY 3 *$\boldsymbol{R}$ is Archimedean.*

PROOF: For $0 < \xi < \eta$ in $\boldsymbol{R}$, let x, y be rational numbers such that

$$0 < x < \xi < \eta \leqq y < \xi + \eta \text{ in } \boldsymbol{R}.$$

Since $\boldsymbol{Q}$ is Archimedean and the embedding isomorphism preserves addition and order, there is an $n \in \boldsymbol{N}$ such that $nx \geqq y$ in $\boldsymbol{R}$. But then $n\xi > nx \geqq y \geqq \eta$, and $\boldsymbol{R}$ is Archimedean.

•*Exercise* 4.5 If (x_n) is a rational sequence and $x \in \boldsymbol{Q}$, then

$$L(x_n) = x \text{ in } \boldsymbol{Q} \text{ if and only if } L(x_n) = x \text{ in } \boldsymbol{R}.$$

THEOREM 4.11 *$\boldsymbol{R}$ is complete.*

PROOF: Let (ξ_n) be a fundamental sequence in $\boldsymbol{R}$. By Corollary 1, there is, for each $n \in \boldsymbol{N}$, a rational number z_n such that

$$|\xi_n - z_n| < \frac{1}{n}.$$

We show that (z_n) is a fundamental sequence in $\boldsymbol{R}$. Since $\boldsymbol{R}$ is Archimedean (or also by Exercise 4.5), $L(1/n) = 0$ in $\boldsymbol{R}$. Hence, for every $\varepsilon > 0$ in $\boldsymbol{R}$, there is an $n_1 \in \boldsymbol{N}$ such that

$$|\xi_n - z_n| < \frac{1}{n} < \frac{\varepsilon}{3} \text{ for all } n \geqq n_1.$$

Since (ξ_n) is a fundamental sequence, there is an $n_2 \in \boldsymbol{N}$ such that

$$|\xi_m - \xi_n| < \frac{\varepsilon}{3} \text{ for all } m, n \geqq n_2.$$

Hence,

$$|z_m - z_n| \leqq |z_m - \xi_m| + |\xi_m - \xi_n| + |\xi_n - z_n| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$$

for all $m, n \geqq \max\{n_1, n_2\}$. Thus, (z_n) is a fundamental sequence in $\boldsymbol{Q}$. By Theorem 4.10, $L(z_n) = C_{(z_n)} = \xi$ in $\boldsymbol{R}$. Hence, there is an $n_3 \in \boldsymbol{N}$ such that

$$|z_n - \xi| < \frac{2\varepsilon}{3} \text{ for all } n \geqq n_3.$$

But then

$$|\xi_n - \xi| \leqq |\xi_n - z_n| + |z_n - \xi| < \frac{\varepsilon}{3} + \frac{2\varepsilon}{3} = \varepsilon$$

for all $n \geqq \max\{n_1, n_3\}$. Hence, $L(\xi_n) = \xi$.

DEFINITION 4.4 If B is a subset of an ordered set A, then B is *dense in* A if for all a, b in A such that $a < b$ in A, there is some element $c \in B$ such that $a < c < b$.

By Corollary 2 of Theorem 4.10, $\boldsymbol{Q}$ is dense in $\boldsymbol{R}$. The close connection between the "density" of $\boldsymbol{Q}$ in $\boldsymbol{R}$ and the Archimedean property of $\boldsymbol{R}$ is expressed in the following more general theorem:

THEOREM 4.12 *An ordered field* $\langle A, +, \cdot, < \rangle$ *is Archimedean if and only if the subset* $\boldsymbol{Q}_A$ *of all rational elements of* A *is dense in* A.

PROOF: Suppose A is Archimedean. For $a < b$ in A, one of the following holds:

(1) $a = 0 < b$,
(2) $a < b = 0$,
(3) $a < 0 < b$,
(4) $0 < a < b$,
(5) $a < b < 0$.

By Exercise 3.17, $L(1/n) = 0$ in A. Hence if (1) holds, then $a = 0 < 1/n < b$ for some $n \in \boldsymbol{N}$, and if (2) holds, then $a < -1/n < b = 0$ for some $n \in \boldsymbol{N}$. If (3) holds, then 0 is a rational element between a and b. If (4) holds, then there is some $n \in \boldsymbol{N}$ such that

$$(1) \quad 0 < 1/n < b - a,$$

and there is a least $m \in \boldsymbol{N}$ such that

$$(2) \quad b \leqq \frac{m}{n}.$$

Hence $(m - 1)/n < b$. Also,

$$(3) \quad \frac{m-1}{n} = \frac{m}{n} - \frac{1}{n} > b - (b - a) = a.$$

But then

$$(4) \quad a < \frac{m-1}{n} < b.$$

Finally, if (5) holds, then $0 < -b < -a$, and, by (4), there is a rational element r such that

$$-b < r < -a.$$

But then

$$a < -r < b.$$

It follows that Q_A is dense in A (Definition 4.4).

Now suppose Q_A is dense in A. Then, for $0 < a < b$ in A, there are rational elements x and y such that

$$0 < x < a < b < y < a + b.$$

Since Q_A is Archimedean, and the embedding isomorphism (Exercise 3.8) preserves addition and order, there is some $n \in N$ such that

$$nx \geqq y \text{ in } A.$$

Hence, $na > nx \geqq y > b$, and A is Archimedean.

•*Exercise* 4.6 If B and A are ordered fields such that B is dense in A and (a_n) is a sequence in B, then

(1) (a_n) is a fundamental sequence in A if and only if it is a fundamental sequence in B,
(2) $L(a_n) = a$ in A if and only if $L(a_n) = a$ in B,
(3) (a_n) is a positive sequence in A if and only if it is a positive sequence in B.

•*Exercise* 4.7 An ordered field A is Archimedean if and only if every element of A is the limit of a sequence of rational elements of A.

Metric Spaces. We now make precise the remark in Chapter 3 that the function $|a - b|$ on $A \times A$ to A, where A is an ordered field, plays the role of a distance in A.

DEFINITION 4.5 Let S be a set and let D be a mapping of $S \times S$ into R such that

(1) $D(P, Q) \geqq 0$ in R for all $P, Q \in S$ and the equality holds if and only if $P = Q$. (D is non-negative.)
(2) $D(P, Q) = D(Q, P)$ for all $P, Q \in S$. (D is symmetric.)
(3) $D(P, Q) \leqq D(P, V) + D(V, Q)$ for all $P, V, Q \in S$. (D satisfies the triangle inequality.)

The system $\langle S, D \rangle$ is called a *metric space* S, and D is called a *distance function (metric) for* S.

Examples of metric spaces: $\langle Q, \tilde{d} \rangle$, where Q is the rational field and $\tilde{d}(x, y) = |x - y|$.

$\langle R, d \rangle$, where R is the real field and $d(\xi, \eta) = |\xi - \eta|$.

$\langle Q^{(n)}, \tilde{d}^{(n)} \rangle$, where $Q^{(n)}$ is the set of all n-tuples $x^{(n)} = \langle x_1, \ldots, x_n \rangle$, $x_j \in Q$, and $\tilde{d}^{(n)}(x^{(n)}, y^{(n)}) = \left(\sum_{j=1}^{n} (x_j - y_j)^2 \right)^{1/2}$.

$\langle R^{(n)}, d^{(n)} \rangle$, where $R^{(n)}$ is the set of all n-tuples, $\xi^{(n)} = \langle \xi_1, \ldots, \xi_n \rangle$, $\xi_j \in R$, and $d^{(n)}(\xi^{(n)}, \eta^{(n)}) = \left(\sum_{j=1}^{n} (\xi_j - \eta_j)^2 \right)^{1/2}$ (Euclidean space).

$\langle R^{(n)}, \Delta^{(n)} \rangle$, where $\Delta^{(n)}(\xi^{(n)}, \eta^{(n)}) = \max \{ |\xi_j - \eta_j| \mid j = 1, \ldots, n \}$ (Minkowski space).

The embedding of the ordered field Q in the complete ordered field R suggests a method for embedding any metric space in a complete metric space as indicated in the following.

DEFINITION 4.6 A sequence (P_n) in a metric space $\langle S, D \rangle$ is called *fundamental* in S if, for each $\varepsilon > 0$ in R, there is some $n_\varepsilon \in N$ such that

$$D(P_n, P_m) < \varepsilon \text{ in } R \text{ for all } m, n \geqq n_\varepsilon \text{ in } N.$$

DEFINITION 4.7 A sequence (P_n) in a metric space $\langle S, D \rangle$ is *convergent* in S and has $P \in S$ as a *limit* if for each $\varepsilon > 0$ in R there is some $n_\varepsilon \in N$ such that

$$D(P_n, P) < \varepsilon \text{ in } R \text{ for all } m \geqq n_\varepsilon \text{ in } N.$$

We write "$L(P_n) = P$ in S" for "(P_n) has P as a limit".

THEOREM 4.13

(a) *Every sequence convergent in S is fundamental in S.*
(b) *A convergent sequence in S has exactly one limit in S.*

DEFINITION 4.8 A metric space S is *complete* if every sequence fundamental in S is convergent in S.

THEOREM 4.14 *The metric space $Q^{(n)}$ is not complete for any n. The Euclidean metric space $R^{(n)}$ is complete for each n.*

We write F_S for the set of all sequences (P_n) which are fundamental in the metric space S.

THEOREM 4.15 *The set T of all $((P_n), (Q_n)) \in F_S \times F_S$ such that $L(D(P_n, Q_n)) = 0 \in R$ is an equivalence relation in F_S.*

DEFINITION 4.9

(a) We call (P_n) and (Q_n) *equivalent* if $((P_n), (Q_n)) \in T$ and and write "$(P_n) \sim (Q_n)$".
(b) $C_{(P_n)} = \{(Q_n) \mid (Q_n) \sim (P_n)\}$
(c) $S^\star = \{P^\star \mid P^\star = C_{(P_n)} \text{ for some } (P_n) \in F_S\}$
(d) If $P^\star = C_{(P_n)}$, $Q^\star = C_{(Q_n)}$ then $D^\star(P^\star, Q^\star) = L(D(P_n, Q_n)) \in R$.

THEOREM 4.16 *If $(P_n) \sim (P'_n)$ and $(Q_n) \sim (Q'_n)$, then there is exactly one $\xi \in R$ such that*

$$L(D(P_n, Q_n)) = \xi = L(D(P'_n, Q'_n)).$$

PROOF: From the symmetry and triangle properties of the distance function D for the metric space S it follows that

(1) $|D(P_n, Q_n) - D(P_m, Q_m)| \leqq D(P_n, P_m) + D(Q_n, Q_m)$ in R for all $m, n \in N$.

Since (P_n), (Q_n) are fundamental sequences in S, it follows that $(D(P_n, Q_n))$ is a fundamental sequence in R. Since R is complete, there is some ξ in R such that

(2) $L(D(P_n, Q_n)) = \xi$ in R.

Similarly,

(3) $L(D(P'_n, Q'_n)) = \xi'$ in R.

We have also, as in (1),

(4) $|D(P_n, Q_n) - D(P'_n, Q'_n)| \leqq D(P_n, P'_n) + D(Q_n, Q'_n)$ in R for all $n \in N$.

By hypothesis, $L(D(P_n, P'_n)) = 0 = L(D(Q_n, Q'_n))$ in R and so, by (4),

Hence

$$\begin{aligned}\xi - \xi' &= L(\boldsymbol{D}(P_n, Q_n)) - L(\boldsymbol{D}(P'_n, Q'_n)) \\ &= L(\boldsymbol{D}(P_n, Q_n) - \boldsymbol{D}(P'_n, Q'_n)) = 0,\end{aligned}$$

and $\xi = \xi'$.

This theorem enables one to prove that $\boldsymbol{D}^\star$, defined in the next theorem, is a mapping which serves as a distance function for $\boldsymbol{S}^\star$.

THEOREM 4.17 *If* $P^\star = C_{(P_n)}$, $Q^\star = C_{(Q_n)} \in \boldsymbol{S}^\star$ *and* $\boldsymbol{D}^\star(P^\star, Q^\star) = L(\boldsymbol{D}(P_n, Q_n))$ *in* $\boldsymbol{R}$, *then*

(a) $\boldsymbol{D}^\star = \{((P^\star, Q^\star), \boldsymbol{D}^\star(P^\star, Q^\star)) \mid P^\star, Q^\star \in \boldsymbol{S}^\star\}$ *is a mapping of* $\boldsymbol{S}^\star \times \boldsymbol{S}^\star$ *into* $\boldsymbol{R}$.

(b) *The system* $\langle \boldsymbol{S}^\star, \boldsymbol{D}^\star \rangle$ *is a metric space.*

The metric space $\langle \boldsymbol{S}, \boldsymbol{D} \rangle$ may be embedded in the metric space $\langle \boldsymbol{S}^\star, \boldsymbol{D}^\star \rangle$ in the sense of the next theorem.

THEOREM 4.18 *The subset* F *of* $\boldsymbol{S} \times \boldsymbol{S}^\star$ *defined by*

$$F = \{(P, C_{(P)}) \mid P \in \boldsymbol{S}\}$$

is a mapping of $\boldsymbol{S}$ *into* $\boldsymbol{S}^\star$ *such that*

$$\boldsymbol{D}(P, Q) = \boldsymbol{D}^\star(F(P), F(Q))$$

for all $P, Q \in \boldsymbol{S}$.

DEFINITION 4.10 If $\langle \boldsymbol{S}, \boldsymbol{D} \rangle$, $\langle \boldsymbol{S}', \boldsymbol{D}' \rangle$ are metric spaces, and F is a 1–1 mapping of $\boldsymbol{S}$ into $\boldsymbol{S}'$ such that

$$\boldsymbol{D}(P, Q) = \boldsymbol{D}'(F(P), F(Q)),$$

then F is called an *isometry* of $\boldsymbol{S}$ into $\boldsymbol{S}'$.

Thus the mapping $E^{\boldsymbol{R}}_{\boldsymbol{Q}}$ of Theorem 4.9 is an isometry of $\boldsymbol{Q}$ into $\boldsymbol{R}$.

THEOREM 4.19 $\langle \boldsymbol{S}^\star, \boldsymbol{D}^\star \rangle$ *is a complete metric space.*

The proof is analogous to that of Theorem 4.11, where $\boldsymbol{D}^\star$ and $\boldsymbol{D}$ replace "absolute value" in $\boldsymbol{R}$ and $\boldsymbol{Q}$, respectively. One establishes first the analog of Theorem 4.10, proves "density" of $\boldsymbol{S}$ in $\boldsymbol{S}^\star$ in the sense of Corollary 1 of Theorem 4.10, and then proceeds to prove the completeness of $\boldsymbol{S}^\star$ as in Theorem 4.11.

COROLLARY *Every metric space is isometric to a subspace of a complete metric space.*

CHAPTER 5

EQUIVALENT CHARACTERIZATIONS OF $\boldsymbol{R}$

By Theorem 4.11, the ordered field $\boldsymbol{R}$ of real numbers is complete in the sense that every real fundamental sequence has a limit in $\boldsymbol{R}$. By Theorem 4.10, Corollary 3, $\boldsymbol{R}$ is an Archimedean ordered field. The completeness of $\boldsymbol{R}$ is one of several properties of the real number field which play a fundamental role in the theory of real-valued functions, and which have led to important generalizations in mathematics. In this chapter, we single out six properties in addition to completeness, and prove that an ordered field has any one of these properties if and only if it is Archimedean and complete. The ordered field $\boldsymbol{R}$, being Archimedean as well as complete, has all of the properties.

We first introduce some terminology. In the following, $\langle A, +, \cdot, < \rangle$ will be an ordered field.

DEFINITION 5.1

(1) A subset X of A is *bounded above* if there is an element $a \in A$ such that

$$x \leqq a \text{ for all } x \in X.$$

The element a is called an *upper bound* (*majorant*) for X.

(2) A subset X of A is *bounded below* if there is an element $a \in A$ such that

$$a \leqq x \text{ for all } x \in X.$$

The element a is called a *lower bound* (*minorant*) for X.

(3) A subset X of A is *bounded* if it has both an upper bound and a lower bound.

Note: X is bounded if and only if there are elements $a_1, a_2, \in A$ such that

$$a_1 \leqq x \leqq a_2 \text{ for all } x \in X.$$

Exercise 5.1 If $X \subset A$ is bounded above, and $Y = \{x \mid -x \in X\}$, then

(1) Y is bounded below,
(2) a is an upper bound for X if and only if $-a$ is a lower bound for Y.

DEFINITION 5.2 An element a of A is called a *least upper bound* (*supremum*) of $X \subset A$ if

(1) a is an upper bound for X,
(2) $a \leqq u$ for all upper bounds u of X.

An element a of A is called a *greatest lower bound* (*infimum*) of $X \subset A$ if

(1) a is a lower bound for X,
(2) $v \leqq a$ for all lower bounds v of X.

Exercise 5.2 A subset X of A has at most one least upper bound, and at most one greatest lower bound.

Notation: We may write "sup X" for the least upper bound of X and "inf X" for the greatest lower bound of X. If sup $X \in X$ we may write "max X" for "sup X". If inf $X \in X$ we may write "min X" for "inf X".

Exercise 5.3 $a = \max X$ if and only if $x \leqq a \in X$ for all $x \in X$.
$a = \min X$ if and only if $x \geqq a \in X$ for all $x \in X$.

DEFINITION 5.3 A subset X is called an *interval* in A if, for some $a, b \in A$, one of the following holds:

(1) $X = \{x \mid a \leqq x \leqq b\}$
(2) $X = \{x \mid a < x < b\}$
(3) $X = \{x \mid a \leqq x < b\}$
(4) $X = \{x \mid a < x \leqq b\}$

The elements a, b are called *endpoints* of the interval.
The element $b - a$ is *called* the *length* of the interval.
In the first case, we call X a *closed interval* and write $X = [a, b]$.
In the second case, we call X an *open interval* and write $X = (a, b)$.
In the third and fourth cases, X is neither open nor closed. We write $X = [a, b)$ in the third case, and $X = (a, b]$ in the fourth case.

We note that if $b \leqq a$, then (a, b), $[a, b)$, and $(a, b]$ are all empty, if $b < a$, then $[a, b]$ is empty, and if $b = a$, then $[a, b] = \{a\}$.

•*Exercise* 5.4 If $a < b$, then any interval with endpoints a and b is an infinite set.

DEFINITION 5.4 An element $p \in A$ is called an *accumulation point* of $X \subset A$ if $X \cap [(a, b) - \{p\}] \neq \emptyset$ for all open intervals (a, b) containing p.

Exercise 5.5 The element $p \in A$ is an accumulation point of $X \subset A$ if and only if $X \cap (a, b)$ is an infinite set for all open intervals (a, b) containing p.

Exercise 5.6 If $a < b$ in A, then $[a, b]$ is the set of all accumulation points of any interval with end points a and b.

Exercise 5.7 The subset $\{1 - 1/n \mid n = 1, 2, \ldots\}$ of $\boldsymbol{R}$ has 1 as its unique accumulation point. Does this statement generalize to arbitrary ordered fields?

Exercise 5.8 If $X = Y \cup Z \subset \boldsymbol{R}$, where $Y = \{1/n \mid n = 1, 2, \ldots,\}$ and $Z = (1, 2)$, then p is an accumulation point of X if and only if $p = 0$ or $p \in [1, 2]$.

Note: An accumulation point of a set may or may not belong to the set.

•*Exercise* 5.9 For $a \in A$, $a \neq 0_A$, the set $X = \{na \mid n \in N\}$ is an infinite set which has no accumulation point.

DEFINITION 5.5 A subset X of A is *closed* if every accumulation point of X belongs to X.

Exercise 5.10 The subset $X = \{x \mid x = 0 \text{ or } x = 1/n \text{ for } n \in N\}$ of $\boldsymbol{R}$ is closed. Does this statement generalize to arbitrary ordered fields?

•*Exercise* 5.11

(a) If a subset X of A has no accumulation point in A, then X is closed.
(b) No finite subset of A has an accumulation point.
(c) If $Y \subset X \subset A$ and x is an accumulation point of X but not of Y, then x is an accumulation point of $X - Y$.
(d) If $Y \subset X \subset A$ and x is an accumulation point of Y, then x is an accumulation point of X.
(e) The set X of Exercise 5.9 is closed.

•*Exercise* 5.12 If $a < b$, then the closed interval $[a, b]$ is a closed set, and the intervals $[a, b)$, $(a, b]$, and (a, b) are not closed sets.

DEFINITION 5.6 A set B of subsets K of A *covers* $X \subset A$ if for each $x \in X$ there is some $K_x \in B$ such that $x \in K_x$.

Exercise 5.13 If for $a \in A$, $X_a = \{a\}$, then $\{X_a \mid a \in A\}$ covers A.

Exercise 5.14 If $X = [0, 1) \subseteq A$

and

$$Y = \left\{ \left(x - 1, \frac{x + 1}{2} \right) \middle| x \in X \right\},$$

then Y covers X.

Exercise 5.15

(1) For every $e > 0$ in $\boldsymbol{Q}$, the set $B = \{(r - e, r + e) \mid r \in \boldsymbol{Q}\}$ covers $\boldsymbol{R}$.

(2) If A_1 and A_2 are ordered fields such that A_1 is dense in A_2, then for any $e > 0$ in A_1 the set $B = \{(r - e, r + e) \mid r \in A_1\}$ covers A_2.

Equivalent Properties of Ordered Fields. We now list six statements referring to an ordered field $\langle A, +, \cdot, < \rangle$ which we prove to be equivalent, in the sense that for a given ordered field, all of the statements are true if any one of them is true.

Statement I

(a) A is Archimedean, and

(b) every fundamental sequence in A has a limit in A.

Statement II Every non-empty subset of A which is bounded above has a least upper bound in A.

Statement III There are no gaps in A.

Statement IV Every non-empty subset of A which is bounded below has a greatest lower bound in A.

Statement V If X is a bounded, closed subset of A and T is a set of open intervals which covers X, then T has a finite subset S which covers X.

Statement VI Every bounded infinite subset of A has an accumulation point in A.

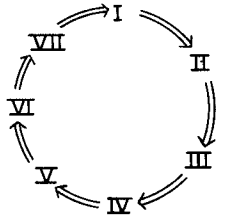
Statement VII

(a) A is Archimedean, and

(b) if, for each $n \in N$, X_n is a closed interval in A, and $X_{n+1} \subset X_n$, then $\bigcap_{n \in N} X_n \neq \emptyset$.

THEOREM 5.1 *In an ordered field* $\langle A, +, \cdot, < \rangle$, *Statements I through VII are equivalent.*

We prove the equivalence by establishing the following cycle of implication:



I IMPLIES II: If A is Archimedean and every fundamental sequence in A has a limit in A, then every non-empty subset of A which is bounded above has a least upper bound in A.

PROOF: Suppose X is a non-empty subset of A, b is an upper bound for X, and $\bar{x} \in X$. Since A is Archimedean, there is, for each $n \in N$, some $\overline{m} \in N$ such that $\bar{x} + \overline{m}/n \geqq b$ in A. Thus, $\bar{x} + \overline{m}/n$ is an upper bound for X. Hence, for each $n \in N$, the set

$$B_n = \{m \mid \bar{x} + m/n \text{ is an upper bound for } X\}$$

is a non-empty subset of N, and (Theorem 1.18) contains a smallest natural number, m_n. Then, for each $n \in N$,

$$(1) \quad y_n = \bar{x} + \frac{m_n}{n} \text{ is an upper bound for } X$$

and

$$(2) \quad x_n = y_n - \frac{1}{n} = \bar{x} + \frac{m_n - 1}{n} \leqq x \text{ in } A \text{ for some } x \in X.$$

Hence

$$x_m < y_n,$$

$$x_m - x_n < y_n - \left(y_n - \frac{1}{n}\right) = \frac{1}{n},$$

and

$$|x_m - x_n| = \max\{x_m - x_n, x_n - x_m\}$$
$$\leqq \max\left\{\frac{1}{n}, \frac{1}{m}\right\} \text{ in } A \text{ for all } m, n \in N.$$

But then, since $L(1/n) = 0$ in the Archimedean ordered field A, (x_n) is a fundamental sequence in A. By hypothesis, (x_n) has a limit a in A.

Now $a = \sup X$. For, a is an upper bound for X. Otherwise, $a < x$ for some $x \in X$. Since $L(x_n) = a$ and $L(1/n) = 0$, there is some $n \in N$ such that

$$x_n - a \leqq |x_n - a| < \frac{x - a}{2} \quad \text{and} \quad \frac{1}{n} < \frac{x - a}{2} \text{ in } A.$$

Then, by (2),

$$y_n = x_n + \frac{1}{n} < \left(a + \frac{x - a}{2}\right) + \frac{x - a}{2} = x \text{ in } A.$$

This is impossible by (1), since $x \in X$. Furthermore, if c is any upper bound for X, then $a \leqq c$ in A. Otherwise, $a - c > 0$ in A. Then, for some $n \in N$,

$$a - x_n \leqq |a - x_n| < a - c \text{ in } A.$$

Hence, by (2), $c < x_n \leqq x$ in A for some $x \in X$. This is impossible, since c is an upper bound for X.

II IMPLIES III: If every non-empty subset of A which is bounded above has a least upper bound in A, then no cut (X, Y) in A is a gap.

PROOF: Suppose (X, Y) is a cut in A. Then X is a non-empty subset of A and every element of the non-empty set Y is an upper bound for X (Definition 5.2). By the hypothesis, there is some $a = \sup X$ in A.

Now, $a = \max X$ or $a = \min Y$. For, since (X, Y) is a cut in A, $a \in X$ or $a \in Y$. If $a \in X$, then $\sup X = a = \max X$. If $a \in Y$, then, since every element of Y is an upper bound for X, $\sup X = a = \min Y$.

III IMPLIES IV: If no cut (X, Y) in A is a gap, then every non-empty subset of A which is bounded below has a greatest lower bound.

PROOF: Suppose B is a non-empty subset of A which is bounded below. Let

(1) $X = \{x \mid x \leqq b \text{ in } A \text{ for all } b \in B\}$,

(2) $Y = A - X$.

Then (X, Y) is a cut in A. For $X \neq \emptyset$ since X is the set of all lower bounds for B, and B is bounded below; $Y \neq \emptyset$ since $b + 1 \in Y$ for all b in the non-empty set B; $X \cup Y = A$ and $X \cap Y = \emptyset$ by (2); and if $x \in X$, $y \in Y$, then $x < y$, since otherwise $y \leqq x \leqq b$ for all $b \in B$, and $y \in X$.

If $b \in X$ for some $b \in B$, then by (1), $b = \max X = \inf B$. If $b \in Y$ for all $b \in B$, and y_0 is smallest in Y, then y_0 is a lower bound for B, and $y_0 \in X$. This is impossible, since $X \cap Y = \emptyset$. Thus, Y has no smallest element. But then, since (X, Y) is not a gap, X has a greatest element x_0, and, by (1), $x_0 = \inf B$.

IV IMPLIES V: If every non-empty subset of A which is bounded below has a greatest lower bound, then every set of open intervals which covers a bounded, closed subset X of A contains a finite subset which covers X.

PROOF: Let X be a closed, bounded subset of A, and let K be a set of open intervals J which covers X. Since X is bounded, there are elements $u, v \in A$ such that $X \subset [u, v]$. Since X is closed, there is for every $y \in [u, v]$, $y \notin X$, an open interval J_y such that $y \in J_y$ and $X \cap J_y$ is empty. Let

$$H = \{J_y \mid y \in [u, v] - X, \quad \text{and} \quad J_y \cap X = \emptyset\}.$$

Then the set $M = K \cup H$ of open intervals $J \in K$ and $J_y \in H$ covers $[u, v]$.

Now let

$$L = \{x \mid x \in [u, v] \text{ and } [x, v] \text{ is covered by a finite subset of } M\}.$$

Since $[v, v]$ is covered by some open interval $T_1 \in K$ if $v \in X$, or by $T_1 = J_v$ if $v \notin X$, it follows that $v \in L$ and L is not empty. Since $u \leqq x$ for all $x \in L$, L is bounded below. By Statement IV, L has a greatest lower bound x_0.

We show that $[x_0, v]$ is covered by a finite subset of M, i.e., $x_0 \in L$. Since $x_0 \in [u, v]$, there is an open interval $T_0 \in M$ such that $x_0 \in T_0$. Let $T_0 = (a, b)$. Then $a < x_0 < b$. Since x_0 is the greatest lower bound of L, there is some $z_0 \in L$ such that $x_0 < z_0 < b$. Since $z_0 \in L$, there is a finite set $\{T_1, \ldots, T_m\} \subset M$ which covers $[z_0, v]$. Hence the finite set $\{T_0, T_1, \ldots, T_m\} \subset M$ covers $[x_0, v]$.

We show next that $x_0 = u$. If $x_0 \neq u$, then $u < x_0$. Since $a < x_0$, $\max\{u, a\} < x_0$. Since the order in A is dense (Theorem 3.16), there is an element $z_1 \in A$ such that

$$u, a \leqq \max\{u, a\} < z_1 < x_0 < b \leqq v.$$

Hence, $z_1 \in [u, v]$, and $[z_1, v]$ is covered by $\{T_0, T_1, \ldots, T_m\}$. Thus, $z_1 \in L$, and $z_1 < x_0$. This is impossible, since x_0 is the greatest lower bound of L.

We have shown that $[u, v]$, and hence the subset X of $[u, v]$, is covered by $\{T_0, T_1, \ldots, T_m\} \subset M = K \cup H$. Since no interval in H contains a point of X, $K \cap \{T_0, T_1, \ldots, T_m\}$ is a finite subset of K which covers X.

V IMPLIES VI: If every set of open intervals which covers a bounded, closed subset X of A contains a finite subset which covers X, then every bounded, infinite subset of A has an accumulation point in A.

PROOF: Let X be a bounded infinite subset of A, and suppose X has no accumulation point. Then X is closed. Suppose $x \in X$. Since x is not an accumulation point of X, there is an open interval J_x such that $X \cap J_x = \{x\}$. The set $K = \{J_x \mid x \in X\}$ covers X. Since X is closed and bounded, there is a finite subset $\overline{K}$ of K which covers X. If $\overline{K} = \{J_{x_1}, \ldots, J_{x_n} \mid n \in N\}$ then for every $x \in X$, there is some $k \in I_n$ such that $x \in J_{x_k}$ and hence $x = x_k$. But then $X = \{x_1, \ldots, x_n\}$, a finite set, contrary to hypothesis.

VI IMPLIES VII: If every bounded, infinite subset of A has an accumulation point in A, then (a) A is Archimedean and (b) if (J_n) is a sequence of closed intervals in A such that $J_{n+1} \subset J_n$ for all $n \in N$, then $\bigcap_{n \in N} J_n \neq \emptyset$.

PROOF: (a) If A is not Archimedean, there exist $a, b \in A$ such that $0 < a < b$ in A, and $a \leqq na < b$ for all $n \in N$. Hence, the set $X = \{na \mid n \in N\}$ is bounded and infinite, and has no accumulation point (Exercise 5.9), contrary to the hypothesis. Thus A is Archimedean.

(b) Suppose $J_n = [a_n, b_n]$ and $J_{n+1} \subset J_n$ for each $n \in N$. Then $a_n \leqq a_{n+1} \leqq b_{n+1} \leqq b_n$ for each n. Let $X = \{a_n \mid n \in N\}$. Since $a_1 \leqq a_n \leqq b_1$ for all $n \in N$, X is a bounded subset of A.

If for some $\bar{n} \in N$, $a_m = a_n$ for all $m \geqq \bar{n}$, then $a_n \leqq a_{\bar{n}} \leqq b_n$ for all n, and $a_{\bar{n}} \in \bigcap_{n \in N} J_n$. Otherwise, for each $n \in N$ there is some $m \in N$ such that $a_m > a_n$. Hence the set X has no greatest element and is therefore an infinite subset of A. By the hypothesis, the bounded, infinite set X has an accumulation point $x \in A$.

If $a_n > x$ for some n, then $a_m \geqq a_n > x$ for all $m \geqq n$. Thus, if $0 < \varepsilon < a_n - x$, the interval $(x - \varepsilon, x + \varepsilon)$ contains only a finite number of points of X. Hence $a_n \leqq x$ for all n. If $b_n < x$ for some n, then $a_m \leqq b_n < x$ for all m. Thus, if $0 < \varepsilon < x - b_n$, the interval $(x - \varepsilon, x + \varepsilon)$ contains no points of X. Hence $x \leqq b_n$ for each n. But then $a_n \leqq x \leqq b_n$ for each n, and $x \in \bigcap_{n \in N} J_n$.

VII IMPLIES I: If (a) A is Archimedcan and if (b) (J_n) is a sequence of closed intervals in A such that $J_{n+1} \subset J_n$ for all $n \in N$, then $\bigcap_{n \in N} J_n \neq \emptyset$, then (a') A is Archimedean and (b') every fundamental sequence in A has a limit in A.

PROOF: (a') holds by (a) of the hypothesis. Suppose (x_n) is a fundamental sequence in A. Then for each $k \in N$ there is some $n_k \in N$ such that

$$(1) \quad x_{n_k} - 1/k < x_n < x_{n_k} + 1/k \text{ in } A \text{ for all } n \geqq n_k \text{ in } N.$$

For each $m \in N$ there are

$$(2) \quad p_m = \max \{n_k \mid k \leqq m \text{ in } N\} \in N,$$
$$(3) \quad a_m = \max \{x_{n_k} - 1/k \mid k \leqq m \text{ in } N\} \in A,$$
$$(4) \quad b_m = \min \{x_{n_k} + 1/k \mid k \leqq m \text{ in } N\} \in A.$$

Then, by (2), (3), and (4)

$$(5) \quad a_m \leqq a_{m+1} < x_n < b_{m+1} \leqq b_m \text{ in } A \text{ for all } m \in N \text{ and all } n \geqq p_{m+1} \text{ in } N.$$

Let $J_m = [a_m, b_m]$ for each $m \in N$. Then, by (5), $J_{m+1} \subset J_m$ for all $m \in N$. Hence, by hypothesis (b), there is some $a \in A$ such that

$$(6) \quad a \in \bigcap_{m \in N} J_m$$

Now $L(x_n) = a$. For, by (1), (3), (4), and (6),

$$(7) \quad x_{n_m} - 1/m \leqq a_m \leqq a \leqq b_m \leqq x_{n_m} + 1/m \text{ in } A \text{ for all } m \in N.$$

By (1),

$$(8) \quad x_{n_m} - 1/m < x_n < x_{n_m} + 1/m \text{ in } A \text{ for all } n \geqq n_m \text{ in } N.$$

Hence, by (7) and (8),

$$(9)\quad |x_n - a| = \max\{x_n - a, a - x_n\} \leqq 2/m \text{ in } A$$

for all $m \in N$ and all $n \geqq n_m$ in N.

Let $e > 0$ in A. By (a), there is some $m \in N$ such that

$$me > 2 \text{ in } A$$

Hence, by (9),

$$|x_n - a| < e \text{ in } A \text{ for all } n \geqq n_m \text{ in } N,$$

and $L(x_n) = a$.

Exercise 5.16 Let K be the set of all Laurent series $\sum_{-\infty}^{\infty} \alpha_j x^j$ where $\alpha_j \in R$ for each j, and for some integer h, $\alpha_j = 0$ if $j < h$. If addition, multiplication and order are defined as in Exercise 3.12, then

(a) K forms a non-Archimedean ordered field which is complete;

(b) A set of "nested" closed intervals—i.e., intervals satisfying the hypotheses of Statement VII (b)—may have an empty intersection. Hint: consider the set of intervals J_n given by $\left[\sum_{j=1}^{\infty} nx^j, \frac{1}{n}\right]$.

We note that, by Exercise 5.16 (a), the Archimedean property (Statement I (a)) is not a consequence of the completeness of an ordered field (Statement I (b)). By Exercise 5.16 (b), Statements I (b) and VII (b) are not equivalent. Examples also exist showing that the Archimedean property (Statement VII (a)) is not a consequence of the "nested intervals" property (Statement VII (b)) (cf. [8]). Thus, the hypothesis that the ordered field is Archimedean is actually needed in Statements I and VII.

Exercise 5.17 Find a counter example in Q to each of Statements I through VII, based on the non-existence in Q of a square root of 2.

Categoricity. We now show that any one of Statements I through VII characterizes R among all ordered fields, or, that the statement "A is an ordered field" together with any one of Statements I through VII forms a categorical set of axioms for the ordered field

of real numbers. Because of the equivalence of the seven statements, it is sufficient to prove that any one of the statements characterizes $\boldsymbol{R}$ among ordered fields.

We first prove:

THEOREM 5.2 *Any Archimedean ordered field can be isomorphically embedded in the ordered field* $\boldsymbol{R}$ *of real numbers.*

PROOF: Let A be an Archimedean ordered field. Let $\boldsymbol{Q}_A$ be the set of all rational elements of A, and let $\tilde{x}$ be the rational element of A which corresponds to $x \in \boldsymbol{Q}$ under the embedding isomorphism of Theorem 3.14.

The set

$$(1) \quad F = \{(L(\tilde{x}_n),\ L(x_n)) \mid (x_n) \in F_Q\}$$

is a 1–1 mapping of A into $\boldsymbol{R}$. For, if $a \in A$, then, by Exercise 4.7, $a = L(\tilde{x}_n)$ for some sequence $(\tilde{x}_n)$ in $\boldsymbol{Q}_A$. Since $(\tilde{x}_n)$ is a fundamental sequence in A (Theorem 3.22), $(\tilde{x}_n)$ is a fundamental sequence in $\boldsymbol{Q}_A$, and (x_n) is a fundamental sequence in $\boldsymbol{Q}$ and in $\boldsymbol{R}$ (Exercises 3.25, 4.6). Since $\boldsymbol{R}$ is complete, $L(x_n) \in \boldsymbol{R}$, and $(a,\ L(x_n)) \in F$. For any $(x_n),\ (y_n) \in F_Q$,

$$(2) \quad L(x_n) = L(y_n) \text{ in } \boldsymbol{R}$$

if and only if (Exercise 4.6)

$$(3) \quad L(x_n - y_n) = 0 \text{ in } \boldsymbol{Q}.$$

But (3) holds if and only if (Exercise 3.25)

$$(4) \quad L(\tilde{x}_n - \tilde{y}_n) = 0 \text{ in } \boldsymbol{Q}_A,$$

and (4) holds if and only if (Exercise 4.6)

$$(5) \quad L(\tilde{x}_n) = L(\tilde{y}_n) \text{ in } A.$$

Thus, (2) and (5) are equivalent, and F is a 1–1 mapping of A into $\boldsymbol{R}$.

By Theorem 3.23, $F(a +_A b) = F(a) +_R F(b)$ and $F(a \cdot_A b) = F(a) \cdot_R F(b)$ for all $a, b \in A$. Thus, F preserves addition and multiplication. If $a = L(\tilde{x}_n)$ is a positive element in A, then $(\tilde{x}_n)$ is a positive sequence in A (Exercise 3.26). By Exercises 3.25 and 3.26, (x_n) is a positive sequence in $\boldsymbol{R}$, and $L(x_n)$ is a positive real number. By Exercise 3.5, F preserves order.

THEOREM 5.3 *Any complete Archimedean ordered field is isomorphic to the ordered field of real numbers.*

PROOF: If A is complete, the mapping F of Theorem 5.2 maps A *onto* $\boldsymbol{R}$. For, if $x = L(x_n)$ in $\boldsymbol{R}$, then $(\tilde{x}_n)$ is a fundamental sequence in A, and, since A is complete, $L(\tilde{x}_n) = a \in A$. But then $x = F(a)$. Hence, F is an isomorphism of the ordered field A onto the ordered field $\boldsymbol{R}$.

COROLLARY *Any ordered field satisfying one of Statements* I *through* VII *is isomorphic to* $\boldsymbol{R}$.

Uncountability of R. Finally, we prove that the ordered field $\boldsymbol{R}$ of real numbers is more numerous than $\boldsymbol{N}$, $\boldsymbol{Z}$, or $\boldsymbol{Q}$.

THEOREM 5.4 $\boldsymbol{R}$ *is not denumerable.*

PROOF: Suppose $\boldsymbol{R}$ is denumerable. Then there is a 1–1 mapping (ξ_n) of $\boldsymbol{N}$ onto $\boldsymbol{R}$.

Let A be the set of all intervals $J = [\xi, \eta] \subset \boldsymbol{R}$ such that $\xi < \eta$ and $\xi_1 \notin J$. Since each J is a proper subset of $\boldsymbol{R}$, there is a largest $k = k(J)$ in $\boldsymbol{N}$ such that

$$\xi_m \notin J \quad \text{for} \quad m \leqq k, \quad \text{and} \quad \xi_{k+1} \in J.$$

For each $J = [\xi, \eta] \in A$, let

$$H_p = \left[\xi + \frac{p(\eta - \xi)}{3},\ \xi + \frac{(p+1)(\eta - \xi)}{3}\right] \quad \text{for} \quad p = 0, 1, 2,$$

and let $G(J) = H_q$ where q is the smallest p for which $\xi_{k(J)+1} \notin H_p$. Then the set $G = \{(J, G(J)) \mid J \in A\}$ is a mapping of A into A such that $G(J) \subset J$ and $k(G(J)) \geqq k(J) + 1$ for each $J \in A$.

Now, $J_1 = [\xi_1 + 1,\ \xi_1 + 2]$ is an element of A, and $k(J_1) \geqq 1$. By the Recursion Theorem, there is a sequence (J_n) in A such that

$$J_1 = [\xi_1 + 1,\ \xi_1 + 2]$$

$$J_{n+1} = G(J_n) \quad \text{for each} \quad n \in \boldsymbol{N}.$$

Then, for each $n \in \boldsymbol{N}$, $J_{n+1} \subset J_n$, and $k(J_n) \geqq n$ since $k(J_1) \geqq 1$ and $k(J_{n+1}) \geqq k(J_n) + 1$. Hence for all $n \in \boldsymbol{N}$, $\xi_m \notin J_n$ if $m \leqq n$. But then $\bigcap_{n \in \boldsymbol{N}} J_n = \phi$. This is impossible since $\boldsymbol{R}$ is a complete Archimedean ordered field.

Exercise 5.18 If x is a real number in the interval $(0, 1]$, prove that x can be represented in exactly one way by a "non-terminating decimal $.a_1a_2a_3 \ldots$," i.e. prove that x is the limit of a unique sequence (u_n) of the form

$$u_1 = \frac{a_1}{10}$$

$$u_n = u_{n-1} + \frac{a_n}{10^n}, \quad n > 1,$$

where $0 \leqq a_n \leqq 9$ and $u_n < x$ for each n.

Exercise 5.19 Using the representation in Exercise 5.18, prove that $(0, 1]$, and hence $\boldsymbol{R}$ (see Ex. 1.21), is non-denumerable.

Hint: suppose $(0, 1]$ is denumerable, and list its elements

$$\begin{array}{ll} x_1\colon & .a_{11}a_{12}a_{13}\ldots \\ x_2\colon & .a_{21}a_{22}a_{23}\ldots \\ x_3\colon & .a_{31}a_{32}a_{33}\ldots \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot \end{array}$$

Construct a non-terminating decimal $.b_1b_2\ldots$ such that $b_n \neq a_{nn}$ for each n, and obtain a contradiction.

CHAPTER 6

THE COMPLEX NUMBERS

The stages in our construction of the real number system may be viewed from the standpoint of the solution of polynomial equations. In the natural number system $\boldsymbol{N}$, an equation of form

$$(1) \quad x + n = m$$

has no root for $n \geqq m$. In the domain $\boldsymbol{Z}$ of integers, any equation of form (1) has a root, but an equation of form

$$(2) \quad ax = b, \quad a \neq 0, \quad a, b \in \boldsymbol{Z},$$

generally has no root in $\boldsymbol{Z}$. (When it does, we say that a is a divisor of b.) This situation is remedied in the field $\boldsymbol{Q}$ of rational numbers where all equations of form

$$(2') \quad px = q, \quad p \neq 0, \quad p, q \in \boldsymbol{Q},$$

have roots. However, for example, an equation of form

$$(3) \quad x^n = z, \quad n \in \boldsymbol{N}, \quad z \in \boldsymbol{Q},$$

may have no root in $\boldsymbol{Q}$. (We have discussed in detail the case $n = 2$, $z = 2$ (Exercise 3.13).)

This situation is partially remedied in the field $\boldsymbol{R}$ of real numbers where any equation of form

$$(3') \quad x^n = \xi, \quad \xi \in \boldsymbol{R},$$

has a root if n is odd, but fails to have a root if n is even and ξ is negative, since even powers in ordered fields are positive. To remedy this situation we construct yet another extension. Our immediate goal shall be to embed $\boldsymbol{R}$ in a field in which the equation

$$(4) \quad x^2 = -1$$

has a root. The resulting field will, in fact, far surpass this goal. For, the field of complex numbers which we are about to construct will have the property that *every* polynomial equation with coefficients in the field has a root* in the field. A field with this property is called *algebraically closed.* The theorem which asserts that the field of complex numbers is algebraically closed is traditionally called the Fundamental Theorem of Algebra, although its proof cannot be accomplished by algebraic means alone. This theorem was first proved by Gauss in his doctoral dissertation. (Gauss later gave at least six additional proofs of the theorem.)

Complex Numbers; Definition.

DEFINITION 6.1 We denote by C the set $R \times R$ of all ordered pairs (ξ, η) of real numbers, write $u, v, w, z, \ldots$ for the elements of C, and call them *complex numbers.*

(Observe that the usual equivalence relation (pp. 43, 60, 80) in this case is simply equality of ordered pairs, so that each equivalence class consists of a single element.)

C as a Field.

THEOREM 6.1 *If, for* $u = (\xi, \eta)$ *and* $v = (\sigma, \tau)$,

$$F(u, v) = (\xi + \sigma, \eta + \tau)$$

and

$$G(u, v) = (\xi\sigma - \eta\tau, \xi\tau + \sigma\eta),$$

then

$$F = \{((u, v), F(u, v)) \mid u, v \in C\}$$

and

$$G = \{((u, v), G(u, v)) \mid u, v \in C\}$$

are binary operations on C.

PROOF: Since two ordered pairs of real numbers are equal if and only if they agree in each component, $F(u, v)$ and $G(u, v)$ are uniquely determined for each $(u, v) \in C \times C$. Hence F and G are mappings of $C \times C$ into C, i.e., they are binary operations on C.

DEFINITION 6.2 We call F and G, respectively, *addition* and *multiplication* on C, write $u +_C v$ for $F(u, v)$ and $u \cdot_C v$ for $G(u, v)$, and omit the subscript "C" most of the time.

* In fact, all of its roots.

THEOREM 6.2 *The system* $\langle \boldsymbol{C}, +_C, \cdot_C \rangle$ *is a field.*

PROOF: We leave to the reader the verification that $\langle \boldsymbol{C}, +_C, \cdot_C \rangle$ is a commutative ring with additive identity $0_C = (0, 0)$ and multiplicative identity $1_C = (1, 0)$. To show that $\boldsymbol{C}$ is, in fact, a field, we observe that if $u = (\xi, \eta) \neq 0_C$, then either $\xi \neq 0$ or $\eta \neq 0$. Hence $\xi^2 + \eta^2$ is a positive real number. But then

$$v = \left(\frac{\xi}{\xi^2 + \eta^2}, \quad \frac{-\eta}{\xi^2 + \eta^2} \right)$$

is an element of $\boldsymbol{C}$, and

$$uv = (\xi, \eta)\left(\frac{\xi}{\xi^2 + \eta^2}, \quad \frac{-\eta}{\xi^2 + \eta^2} \right) = (1, 0) = 1_C.$$

Thus, every non-zero element of $\boldsymbol{C}$ has a multiplicative inverse, and $\langle \boldsymbol{C}, +_C, \cdot_C \rangle$ is a field.

THEOREM 6.3 *The complex numbers* $i = (0, 1)$ *and* $-i = (0, -1)$ *are solutions of the equation* $x^2 = -1_C$.

PROOF: $(\pm i)^2 = i^2 = (0, 1)(0, 1) = (-1, 0) = -1_C$.

Exercise 6.1 The equation $x^2 = -1$ has no solution other than $\pm i$ in $\boldsymbol{C}$.

Exercise 6.2

(1) If $(\xi, \eta) < (\xi', \eta')$ whenever $\xi < \xi'$ or $\xi = \xi'$ and $\eta < \eta'$ in $\boldsymbol{R}$, then $<$ is an order relation in $\boldsymbol{C}$.
(2) Is $\langle \boldsymbol{C}, +, \cdot, < \rangle$ an ordered field?
(3) Is there any order relation, $<$, such that $\langle \boldsymbol{C}, +, \cdot, < \rangle$ is an ordered field?

Embedding.

THEOREM 6.4 *The set*

$$E = E_R^C = \{(\xi, (\xi, 0)) \mid \xi \in \boldsymbol{R}\}$$

is an isomorphism of the field $\langle \boldsymbol{R}, +_R, \cdot_R \rangle$ *into the field* $\langle \boldsymbol{C}, +_C, \cdot_C \rangle$.

PROOF: For every $\xi \in \boldsymbol{R}$, there is exactly one $u \in \boldsymbol{C}$ such that $u = (\xi, 0) = E(\xi)$. Thus, E is a mapping of $\boldsymbol{R}$ into $\boldsymbol{C}$. Since $(\xi, 0) = (\eta, 0)$ only if $\xi = \eta$, E is a 1–1 mapping of $\boldsymbol{R}$ into $\boldsymbol{C}$. Since $E(\xi +_R \eta) = (\xi +_R \eta, 0) = (\xi, 0) +_C (\eta, 0)$, and

$$E(\xi \cdot_R \eta) = (\xi, 0) \cdot_C (\eta, 0) \text{ for all } \xi, \eta \in \boldsymbol{R},$$

E is an isomorphism of $\langle \boldsymbol{R}, +_R, \cdot_R \rangle$ into $\langle \boldsymbol{C}, +_C \cdot_C \rangle$.

In view of Theorem 6.4, we shall write "ξ" for $E(\xi) = (\xi, 0)$ for all $\xi \in \boldsymbol{R}$. This will permit us to express the elements of $\boldsymbol{C}$ in the conventional notation for complex numbers.

THEOREM 6.5 *If $z \in \boldsymbol{C}$, then z can be expressed in one and only one way as $z = \xi + \eta i$, where $\xi, \eta \in \boldsymbol{R}$ and $i = (0, 1)$.*

PROOF: Since $z \in \boldsymbol{C}$, $z = (\xi, \eta)$ for some $\xi, \eta \in \boldsymbol{R}$. Hence $z = (\xi, \eta) = (\xi, 0) + (0, \eta) = (\xi, 0) + (\eta, 0)(0, 1) = \xi + \eta i$.

If $z = \xi' + \eta' i$ for $\xi', \eta' \in \boldsymbol{R}$, then $\xi' + \eta' i = (\xi', 0) + (\eta', 0)(0, 1) = (\xi', 0) + (0, \eta') = (\xi', \eta') = z = (\xi, \eta)$. Hence, $\xi = \xi'$ and $\eta = \eta'$.

C as a Vector Space. The last theorem exemplifies yet another aspect of $\boldsymbol{C}$. Ordered pairs of real numbers, or, equivalently, complex numbers, are traditionally represented as points, or vectors, in the Cartesian plane. Addition of complex numbers, in this representation, corresponds to vector addition, and multiplication of complex numbers by real numbers corresponds to the multiplication of vectors by real scalars. The properties of vectors with respect to these two operations are formalized in the definition of a vector space.

DEFINITION 6.3 If $\langle K, +_K, \cdot \rangle$ is a field, $\langle V, +_V \rangle$ is a commutative group and $\circ$ is a binary operation on $K \times V$ into V, then V *is a vector space* (*linear space*) *over* K if

(1) $\alpha \circ (a +_V b) = \alpha \circ a +_V \alpha \circ b$
(2) $(\alpha +_K \beta) \circ a = \alpha \circ a +_V \beta \circ a$
(3) $(\alpha\beta) \circ a = \alpha \circ (\beta a)$
(4) $1_K \circ a = a$

for all $\alpha, \beta \in K$ and all $a, b \in V$.

The operation $\circ$ is called *scalar multiplication*; the addition in V is called *vector addition*. (Strictly, the system

$$\langle \langle K, +_K, \cdot \rangle, \langle V, +_V \rangle, \circ \rangle$$

is the vector space!)

Exercise 6.3

(1) If K is any field, K_N the set of all sequences (a_n) in K, and if addition and scalar multiplication are defined by

$$(a_n) + (b_n) = (a_n + b_n)$$
$$\alpha \circ (a_n) = (\alpha a_n),$$

then K_N is a vector space over K.

(2) If K is an ordered field, and V is the set
  (a) of all fundamental sequences in K,
  (b) of all convergent sequences in K,
  (c) of all sequences with limit 0 in K,

and the operations are defined as in (1), then, in each case, V is a vector space over K.

DEFINITION 6.4 If V is a vector space over a field K, then the n-tuple $\langle a_1, \ldots, a_n \rangle$ of vectors a_i of V is called a *basis* for V if every vector $v \in V$ has a unique representation

$$v = \sum_{i=1}^{n} \alpha_i a_i$$

where $\alpha_i \in K$ for each $i = 1, \ldots, n$.

DEFINITION 6.5 If V is a vector space over K, and $n \in \boldsymbol{N}$, then V *has dimension* n if it has a basis of n elements.

It is proved in any standard treatment of vector spaces that any two bases of a vector space have the same number of elements, so that the dimension of a finite dimensional vector space is uniquely determined (cf. [2]).

THEOREM 6.6 $\boldsymbol{C}$ *is a two-dimensional vector space over* $\boldsymbol{R}$.

PROOF: We leave to the reader the verification that $\boldsymbol{C}$ satisfies the conditions of Definition 6.3. That $\boldsymbol{C}$ is two-dimensional follows immediately from Theorem 6.5. For, according to Theorem 6.5, $1_C = (1, 0)$ and $i = (0, 1)$ serve as a basis for the vector space $\boldsymbol{C}$ over $\boldsymbol{R}$.

Exercise 6.4 If K is any field, n is a fixed natural number, and the operations are defined componentwise, then the set K_n of all n-tuples over K is an n-dimensional vector space over K.

Exercise 6.5 Every field is a 1-dimensional vector space over itself.

DEFINITION 6.6 If the elements of a vector space V over a field K form a ring $\langle V, +, \cdot \rangle$ such that

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

for all $\alpha \in K$ and all $a, b \in V$, then V is called an *algebra* over K. If the vector space V has dimension n over K, then the algebra V has dimension n over K.

Exercise 6.6 $\boldsymbol{C}$ is an algebra over $\boldsymbol{R}$, of dimension 2.

We state, but do not prove, the following remarkable theorem (Weierstrass-Frobenius Theorem), cf. [18]): Any field which is a finite dimensional algebra over $\boldsymbol{R}$ is isomorphic either to $\boldsymbol{C}$ or to $\boldsymbol{R}$.

$\boldsymbol{C}$ as a Metric Space. Since $\boldsymbol{C}$ cannot be made into an ordered field, the usual definition of absolute value is not possible for complex numbers. However, we shall define a mapping of $\boldsymbol{C}$ into $\boldsymbol{R}$ which shares some of the properties of the absolute value function we defined for ordered fields.

DEFINITION 6.7 If $z = (\xi, \eta) \in \boldsymbol{C}$, then the non-negative real number $\rho(z)$ such that $(\xi^2 + \eta^2) = \rho^2(z)$ is called the *modulus* (absolute value) of z.

•*Exercise* 6.7 The set $\rho = \{(z, \rho(z)) \mid z \in \boldsymbol{C}\}$ is a mapping of $\boldsymbol{C}$ into $\boldsymbol{R}$.

•*Exercise* 6.8

(1) If $z \in \boldsymbol{C}$, then $\rho(z) = 0$ if and only if $z = 0$.
(2) $\rho(-z) = \rho(z)$ for all $z \in \boldsymbol{C}$.
(3) For $z, w \in \boldsymbol{C}$, $\rho(zw) = \rho(z)\rho(w)$.
(4) For $z, w \in \boldsymbol{C}$, $\rho(z + w) \leqq \rho(z) + \rho(w)$.
(5) For $z, w \in \boldsymbol{C}$, $\rho(z - w) \geqq |\rho(z) - \rho(w)| \geqq \rho(z) - \rho(w)$.

THEOREM 6.7 *If, for all* $z, w \in \boldsymbol{C}$, $\boldsymbol{\delta}(z, w) = \rho(z - w)$, *then the set*

$$\boldsymbol{\delta} = \{((z, w), \boldsymbol{\delta}(z, w)) \mid (z, w) \in \boldsymbol{C} \times \boldsymbol{C}\}$$

is a metric on $\boldsymbol{C}$, *and* $\langle \boldsymbol{C}, \boldsymbol{\delta} \rangle$ *is a metric space.*

PROOF: By Exercise 6.7, since $z - w$ is uniquely determined for each $(z, w) \in \boldsymbol{C} \times \boldsymbol{C}$, $\boldsymbol{\delta}$ is a mapping of $\boldsymbol{C} \times \boldsymbol{C}$ into $\boldsymbol{R}$. By Exercise 6.8, (1), $\boldsymbol{\delta}(z, w) \geqq 0$ for all $(z, w) \in \boldsymbol{C} \times \boldsymbol{C}$, and $\boldsymbol{\delta}(z, w) = 0$ if and only if $z = w$. By Exercise 6.8 (2),

$$\boldsymbol{\delta}(z, w) = \rho(z - w) = \rho(w - z) = \boldsymbol{\delta}(w, z) \text{ for all } z, w \in \boldsymbol{C}.$$

By Exercise 6.8, (3),

$$\boldsymbol{\delta}(z, v) + \boldsymbol{\delta}(v, w) = \rho(z - v) + \rho(v - w) \geqq \rho(z - w) = \boldsymbol{\delta}(z, w).$$

Thus, by Definition 4.5, $\boldsymbol{\delta}$ is a metric on $\boldsymbol{C}$, and $\langle \boldsymbol{C}, \boldsymbol{\delta} \rangle$ is a metric space.

Exercise 6.9 The embedding isomorphism E of Theorem 6.4 is an isometry of $(\boldsymbol{R}, \boldsymbol{D})$ (Definition 4.10) into $\langle \boldsymbol{C}, \boldsymbol{\delta} \rangle$.

Exercise 6.10 If $z = (\xi, \eta)$ and $w = (\sigma, \tau)$ then
$\max \{|\xi - \sigma|, |\eta - \tau|\} \leqq \boldsymbol{\delta}(z, w) \leqq \sqrt{2} \max \{|\xi - \sigma|, |\eta - \tau|\}$.

In Chapter 4, we gave definitions of fundamental sequences, convergence, and completeness for metric spaces.

THEOREM 6.8 *$\langle \boldsymbol{C}, \boldsymbol{\delta} \rangle$ is a complete metric space, i.e., every fundamental sequence in $\boldsymbol{C}$ has a limit in $\boldsymbol{C}$.*

PROOF: Let (z_n) be a fundamental sequence in $\boldsymbol{C}$. Then for each $\varepsilon > 0$ there is some $n_\varepsilon \in \boldsymbol{N}$ such that

$$(1) \quad \boldsymbol{\delta}(z_m, z_n) < \varepsilon$$

for all $m, n \geqq n_\varepsilon$ (Definition 4.6). If $z_n = (\xi_n, \eta_n)$ for each n, then, by Exercise 6.10,

$$(2) \quad |\xi_m - \xi_n| \leqq \boldsymbol{\delta}(z_m, z_n) < \varepsilon$$

and

$$(3) \quad |\eta_m - \eta_n| \leqq \boldsymbol{\delta}(z_m, z_n) < \varepsilon$$

for all $m, n \geqq n_\varepsilon$.

Hence, the sequences (ξ_n) and (η_n) are fundamental in $\boldsymbol{R}$. By the completeness of $\boldsymbol{R}$ (Theorem 4.11), there are real numbers ξ, η such that

$$L(\xi_n) = \xi \quad \text{and} \quad L(\eta_n) = \eta.$$

Hence, for every $\varepsilon > 0$, there are natural numbers $n'_\varepsilon, n''_\varepsilon$ such that

$$|\xi_n - \xi| < \frac{\varepsilon}{\sqrt{2}} \text{ for } n \geqq n'_\varepsilon$$

and

$$|\eta_n - \eta| < \frac{\varepsilon}{\sqrt{2}} \text{ for } n \geqq n''_\varepsilon.$$

But then for $n_\varepsilon = \max \{n'_\varepsilon, n''_\varepsilon\}$,

$$\boldsymbol{\delta}(z, z_n) \leqq \sqrt{2} \max \{|\xi - \xi_n|, |\eta - \eta_n|\} < \varepsilon$$

for all $n \geqq n_\varepsilon$.

Hence, the sequence (z_n) converges to $z \in \boldsymbol{C}$.

Bibliography

Completeness is not a property of the bibliography. Where a bracketed number appears in the text, it is a reference to an item in the following list.

1 H. Bachman, Transfinite Zahlen, *Ergebnisse der Math. und ihrer Grenzgebiete*, Neue Folge, Heft 1, Springer Verlag, 1955

2 G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, Macmillan, 1956

3 N. Bourbaki, *Eléments de Mathématique*, Première partie, Livre I, Théorie des Ensembles, Ch. I, II, Hermann, 1954

4 N. Bourbaki, *Eléments de Mathématique*, Première partie, Livre II, Algèbre, Ch. I, Hermann, 1942

5 N. Bourbaki, *Eléments de Mathématique*, Première partie, Livre II, Algèbre, Ch. VI, Hermann, 1952

6 N. Bourbaki, *Eléments de Mathématique*, Première partie, Livre III, Topologie générale, Ch. IV, Nombres réels, 2nd ed., Hermann, 1959

7 N. Bourbaki, *Eléments de Mathématique*, Deuxième partie, Livre II, Algèbre commutative, Ch. II, Hermann, 1952

8 L. W. Cohen and C. Goffman, A theory of transfinite convergence, *Transactions of the Amer. Math. Soc.*, Vol. 66, 1949

9 R. Dedekind, *Was sind und was sollen die Zahlen?* Vierweg, 1898

10 A. Fraenkel, *Abstract Set Theory*, Amsterdam, 1952

11 K. Gödel, Uber die formal unentscheidbaren Sätze der Principia Math. und verwandter Systeme I, *Monatsh. für Math. und Phys.*, Vol. 38, 1931

12 P. Halmos, *Naive Set Theory*, Van Nostrand, 1960

13 N. Jacobson, *Lectures in Abstract Algebra*, Vol. I, Van Nostrand, 1958

14 E. Landau, *Foundations of Analysis*, Chelsea, 1951

15 E. Nagel and J. R. Newman, *Gödel's Proof*, New York Univ. Press, 1958

16 G. Peano, *Notations de logique math.; intr. au Formulaire de Math.*, Turin, 1894

17 G. Peano, *Formulaire de Math.*, 1895–1905

18 L. Pontrjagin, *Topological Groups*, Ch. V, Princeton Univ. Press, 1939

19 B. Russell, *Introduction to Mathematical Philosophy*, Allen & Unwin, 1924

20 B. Russell and A. N. Whitehead, *The Principles of Mathematics*, 2nd ed., Norton, 1938

21 W. Sierpínski, *Leçons sur les nombres transfinis*, Gauthier-Villars, 1950

22 P. Suppes, *Axiomatic Set Theory*, Van Nostrand, 1960

23 B. L. Van der Waerden, *Modern Algebra*, Frederick Ungar Pub. Co., 1953

24 O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, Van Nostrand, 1958

Index