AN INTRODUCTION TO ABSTRACT MATHEMATICAL SYSTEMS

DAVID M. BURTON | University of New Hampshire

ADDISON-WESLEY, READING, MASSACHUSETTS

Printed in the United States of America

Library of Congress Catalog Card No. 65–19237

ADDISON-WESLEY PUBLISHING COMPANY, INC.

READING, MASSACHUSETTS · Palo Alto · London

NEW YORK · DALLAS · ATLANTA · BARRINGTON, ILLINOIS

To my wife and children

THIS BOOK IS IN THE

ADDISON-WESLEY SERIES IN INTRODUCTORY MATHEMATICS

Consulting Editors

RICHARD S. PIETERS AND GAIL S. YOUNG

PREFACE

This little volume is an outgrowth of a series of lectures given by the author in a summer institute for high school teachers of mathematics. The purpose of the course was to improve the participants' understanding of algebraic structure and to acquaint them with some of the basic results of abstract algebra through a formal investigation of various mathematical systems.

In putting these lectures into textbook form, our aim has been to give a presentation which is logically developed, precise, and in keeping with the spirit of the times. Thus a constant level of rigor has been maintained throughout with proofs given in full detail, except for those which parallel proofs given previously. The reader will also find that the text is essentially self-contained. A first chapter on sets and functions is being included to serve as background and to introduce some of the terminology and notations used subsequently. Numerous exercises of varying degree of difficulty are to be found at the end of each section.

It is hoped that the material encountered here will be adaptable to a variety of teaching situations and prove useful not only to the mathematics major but to any adequately prepared student. Indeed, to some extent this has already been the case, for certain mimeographed portions of this text have been successfully employed in a terminal course for liberal arts freshmen. The entire volume would be quite appropriate for a beginning one-semester course in modern algebra or for a reading course in which the student could master the material through independent study.

Many important topics vie for inclusion in a volume of this size, and some choice is obviously imperative. To this end, we merely followed our own taste, condensing or omitting altogether certain of the concepts found in the usual first course in modern algebra. Despite these omissions there remains a broad foundation upon which the reader can build.

New Haven, Conn. D. M. B.
April 1965

CONTENTS

Chapter 1

PRELIMINARY NOTIONS

1-1. THE ALGEBRA OF SETS

The present chapter establishes some of the notations and terminology used throughout the text. It also serves as a brief introduction to the algebras of sets and functions. Inasmuch as this material is intended primarily for background purposes, the reader may prefer to begin with Chapter 2.

The term "set" is intuitively understood to mean a collection of objects having some common characteristic. The objects that make up a given set are called its *elements* or *members*. Sets will generally be designated by capital letters and their elements by small letters. In particular, we shall employ the following notations: Z is the set of integers, Q the set of rational numbers, and $R^{\#}$ the set of real numbers. The symbols Z_{+}, Q_{+}, and $R^{\#}_{+}$ will stand for the positive elements of these sets.

If x is an element of the set A, it is customary to use the notation $x \in A$ and to read the symbol $\in$ as "belongs to." On the other hand, when x fails to be an element of the set A, we denote this by writing $x \notin A$.

There are two common methods of specifying a particular set. First, we may list all of its elements within braces, as with the set $\{-1, 0, 1, 2\}$, or merely list some of its elements and use three dots to indicate the fact that certain elements have been omitted, as with the set $\{1, 2, 3, 4, \ldots\}$. When such a listing is not practical, we may instead indicate a characteristic property whereby we can determine whether or not a given object is an element of the set. More specifically, if $P(x)$ is a statement concerning x, then the set of all elements x for which the statement $P(x)$ is true is denoted by

$$\{x \mid P(x)\}.$$

For example, we might have $\{x \mid x \text{ is an odd integer greater than } 21\}$. Clearly, certain sets may be described both ways:

$$\{0, 1\} = \{x \mid x \in Z \quad \text{and} \quad x^2 = x\}.$$

It is customary, however, to depart slightly from this notation and write $\{x \in A \mid P(x)\}$ instead of $\{x \mid x \in A \text{ and } P(x)\}$.

> **DEFINITION 1–1.** Two sets A and B are said to be *equal*, written $A = B$, if and only if every element of A is an element of B and every element of B is an element of A. That is, $A = B$ provided A and B have the same elements.

Thus a set is completely determined by its elements. For instance,

$$\{1, 2, 3\} = \{3, 1, 2, 2\},$$

since each set contains only the integers 1, 2, and 3. Indeed, the order in which the elements are listed in a set is immaterial, and repetition conveys no additional information about the set.

An *empty set* or *null set*, represented by the symbol $\emptyset$, is any set containing no elements. For instance,

$$\emptyset = \{x \in R^{\#} \mid x^2 < 0\} \qquad \text{or} \qquad \emptyset = \{x \mid x \neq x\}.$$

Any two empty sets are equal, for in a trivial sense they both contain the same elements (namely, none). In effect, then, there is just one empty set, so that we are free to speak of "the empty set $\emptyset$."

The set whose only member is the element x is called *singleton* x and denoted by $\{x\}$:

$$\{x\} = \{y \mid y = x\}.$$

In particular, $\{0\} \neq \emptyset$ since $0 \in \{0\}$.

> **DEFINITION 1–2.** The set A is a *subset* of, or is *contained in* the set B, indicated by writing $A \subseteq B$, if every element of A is also an element of B.

Our notation is designed to include the possibility that $A = B$. Whenever $A \subseteq B$ but $A \neq B$, we will write $A \subset B$ and say that A is a *proper* subset of B.

It will be convenient to regard all sets under consideration as being subsets of some master set U, called the *universe* (universal set, ground set). While the universe may be different in different contexts, it will usually be fixed throughout any given discussion.

There are several immediate consequences of the definition of set inclusion.

THEOREM 1–1. If A, B, and C are subsets of some universe U, then:

(a) $A \subseteq A$, $\emptyset \subseteq A$, $A \subseteq U$.
(b) $A \subseteq \emptyset$ if and only if $A = \emptyset$.
(c) $\{x\} \subseteq A$ if and only if $x \in A$; that is, each element of A determines a subset of A.
(d) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
(e) $A \subseteq B$ and $B \subseteq A$ if and only if $A = B$.

Observe that the result $\emptyset \subseteq A$ follows from the logical principle that a false hypothesis implies any conclusion whatsoever. Thus, the statement, "if $x \in \emptyset$, then $x \in A$," is true since $x \in \emptyset$ is always false.

The last assertion of Theorem 1–1 indicates that a proof of the equality of two specified sets A and B is generally presented in two parts. One part demonstrates that if $x \in A$, then $x \in B$; the other part demonstrates that if $x \in B$, then $x \in A$. An illustration of such a proof will be given later.

We now consider several important ways in which sets may be combined with one another. If A and B are subsets of some universe U, the operations of union, intersection, and difference are defined as follows.

DEFINITION 1–3. The *union* of A and B, denoted by $A \cup B$, is the subset of U defined by

$$A \cup B = \{x \mid x \in A \quad \text{or} \quad x \in B\}.$$

The *intersection* of A and B, denoted by $A \cap B$, is the subset of U defined by

$$A \cap B = \{x \mid x \in A \quad \text{and} \quad x \in B\}.$$

The *difference* of A and B (sometimes called the *relative complement* of B in A), denoted by $A - B$, is the subset of U defined by

$$A - B = \{x \mid x \in A \quad \text{but} \quad x \notin B\}.$$

In the definition of union, the word "or" is used in the "and/or" sense. Thus the statement, "$x \in A$ or $x \in B$" includes the case where x is in both A and B.

The particular difference $U - B$ is called the (absolute) *complement* of B and designated simply by $-B$. If A and B are two nonempty sets whose intersection is empty, that is, $A \cap B = \emptyset$, then they are said to be *disjoint*. We shall illustrate these concepts with an example.

EXAMPLE 1–1. Let the universe be $U = \{0, 1, 2, 3, 4, 5, 6\}$, $A = \{1, 2, 4\}$, and $B = \{2, 3, 5\}$. Then $A \cup B = \{1, 2, 3, 4, 5\}$, $A \cap B = \{2\}$, $A - B = \{1, 4\}$, and $B - A = \{3, 5\}$. Also, $-A = \{0, 3, 5, 6\}$, $-B = \{0, 1, 4, 6\}$. Observe that $A - B$ and $B - A$ are unequal and disjoint.

In the following theorem are listed some simple consequences of the definitions of union, intersection, and complementation.

THEOREM 1–2. If A, B, and C are subsets of some universe U, then:

(a) $A \cup A = A$, $A \cap A = A$;
(b) $A \cup B = B \cup A$, $A \cap B = B \cap A$;
(c) $A \cup (B \cup C) = (A \cup B) \cup C$,
$A \cap (B \cap C) = (A \cap B) \cap C$;
(d) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(e) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$;
(f) $A \cup U = U$, $A \cap U = A$;
(g) $A \cup (-A) = U$, $A \cap (-A) = \emptyset$.

We shall verify the first equality of (d), since its proof illustrates a technique mentioned previously. Suppose that $x \in A \cup (B \cap C)$. Then either $x \in A$ or $x \in B \cap C$. Now, if $x \in A$, then clearly both $x \in A \cup B$ and $x \in A \cup C$, so that $x \in (A \cup B) \cap (A \cup C)$. On the other hand, if $x \in B \cap C$, then $x \in B$ and therefore $x \in A \cup B$; also $x \in C$ and therefore $x \in A \cup C$. The two conditions together imply

$$x \in (A \cup B) \cap (A \cup C).$$

This establishes the inclusion

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C).$$

Conversely, suppose $x \in (A \cup B) \cap (A \cup C)$. Then both $x \in A \cup B$ and $x \in A \cup C$. Since $x \in A \cup B$, either $x \in A$ or $x \in B$; at the same time, since $x \in A \cup C$, either $x \in A$ or $x \in C$. Together, these conditions mean that $x \in A$ or $x \in B \cap C$; that is, $x \in A \cup (B \cap C)$. This proves the opposite inclusion

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

By Part (e) of Theorem 1–1, the two inclusions are sufficient to establish the equality

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

The next theorem relates the operation of complementation to the other operations of set theory.

THEOREM 1-3. Let A and B be subsets of the universe U. Then

(a) $-(A \cup B) = (-A) \cap (-B)$;
(b) $-(A \cap B) = (-A) \cup (-B)$;
(c) if $A \subseteq B$, then $(-B) \subseteq (-A)$;
(d) $-(-A) = A$, $-\emptyset = U$, $-U = \emptyset$.

The first two parts of the above theorem are commonly known as DeMorgan's rules.

One final comment on set theory. It is both desirable and possible to extend our definitions of union and intersection from two sets to any number of sets. Suppose to this end that $\mathcal{A}$ is a nonempty collection of subsets of the universe U. The union and intersection of this arbitrary collection are defined by

$$\cup \mathcal{A} = \{x \mid x \in A \text{ for some set } A \in \mathcal{A}\},$$
$$\cap \mathcal{A} = \{x \mid x \in A \text{ for every set } A \in \mathcal{A}\}.$$

For instance, if $I_n = \{x \in R^\# \mid -1/n \leq x \leq 1/n\}$ for $n = 1, 2, \ldots$ and $\mathcal{A}$ is the collection of all the I_n, then

$$\cup \mathcal{A} = \{x \in R^\# \mid -1 \leq x \leq 1\}, \qquad \cap \mathcal{A} = \{0\}.$$

PROBLEMS

In the following exercises A, B, and C are subsets of some universe U.

1. Prove that $A \cap B \subseteq A \cup B$.
2. Suppose $A \subseteq B$. Show that
   (a) $A \cap C \subseteq B \cap C$ (b) $A \cup C \subseteq B \cup C$
3. Prove that $A - B = A \cap (-B)$, and use this result to verify each of the following identities:
   (a) $A - \emptyset = A$, $\emptyset - A = \emptyset$, $A - A = \emptyset$
   (b) $A - B = A - (A \cap B) = (A \cup B) - B$
   (c) $(A - B) \cap (B - A) = \emptyset$
4. Simplify the following expressions to one of the symbols A, B, $A \cup B$, $A \cap B$, $A - B$.
   (a) $A \cap (A \cup B)$ (b) $A - (A - B)$ (c) $-((A \cap B) \cup (-A))$
5. Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

6. Establish the following results on differences:
   (a) $(A - B) - C = A - (B \cup C)$
   (b) $A - (B - C) = (A - B) \cup (A \cap C)$
   (c) $A \cup (B - C) = (A \cup B) - (C - A)$
   (d) $A \cap (B - C) = (A \cap B) - (A \cap C)$

7. The notion of set inclusion may be expressed either in terms of union or intersection. To see this, prove that
   (a) $A \subseteq B$ if and only if $A \cup B = B$,
   (b) $A \subseteq B$ if and only if $A \cap B = A$.

1-2. FUNCTIONS

From our definition of set equality, $\{a, b\} = \{b, a\}$, since both sets contain the same two elements a and b. That is, no preference is given to one element over the other. When we wish to distinguish one of these elements as being the first, say a, we write (a, b) and call this an ordered pair.

It is possible to give a purely set-theoretic definition of the notion of ordered pair as follows:

DEFINITION 1-4. The *ordered pair* of elements a and b, with first component a and second component b, denoted by (a, b), is the set

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

Note that, according to this definition, a and b are not elements of (a, b) but rather components. The actual elements of the set (a, b) are $\{a, b\}$, the unordered pair involved, and $\{a\}$, that member of the unordered pair which has been selected to be "first." Clearly this agrees with our intuition that an ordered pair should be an entity representing two elements in a given order.

For $a \neq b$, the sets $\{\{a, b\}, \{a\}\}$ and $\{\{b, a\}, \{b\}\}$ are unequal, having different elements, so that $(a, b) \neq (b, a)$. Hence, if a and b are distinct, there are two distinct ordered pairs whose components are a and b: namely, the pairs (a, b) and (b, a). Ordered pairs thus provide a way of handling two things as one while losing track of neither. We emphasize again that there is just one set whose elements are a and b, for $\{a, b\} = \{b, a\}$. As a consequence of Definition 1-4, it can be shown that

$$(a, b) = (c, d) \quad \text{if and only if} \quad a = c,\ b = d.$$

DEFINITION 1–5. The *Cartesian product* of two nonempty sets A and B, designated by $A \times B$, is the set

$$A \times B = \{(a, b) \mid a \in A \quad \text{and} \quad b \in B\}.$$

Whenever we employ the Cartesian product notation, it will be with the understanding that the sets involved are nonempty, even though this may not be explicitly stated at the time. Observe that if the set A contains n elements and B contains m elements, then $A \times B$ has nm elements, which accounts for the use of the word "product" in Cartesian product.

EXAMPLE 1–2. Let $A = \{-1, 0, 1\}$ and $B = \{0, 2\}$. Then

$$A \times B = \{(-1, 0), (-1, 2), (0, 0), (0, 2), (1, 0), (1, 2)\}$$

while

$$B \times A = \{(0, -1), (0, 0), (0, 1), (2, -1), (2, 0), (2, 1)\}.$$

Clearly the sets $A \times B \neq B \times A$. In general, $A \times B = B \times A$ if and only if $A = B$.

We avoid the traditional view of a function as a rule of correspondence and instead give the following definition in terms of ordered pairs.

DEFINITION 1–6. A *function* (or *mapping*) f is a set of ordered pairs such that no two distinct pairs have the same first component. Thus $(x, y_1) \in f$ and $(x, y_2) \in f$ implies $y_1 = y_2$.

The collection of all first components of a function f is called the *domain* of the function and is denoted by D_f, while the collection of all second components is called the *range* of the function and is denoted by R_f. In terms of set notation,

$$D_f = \{x \mid (x, y) \in f \text{ for some } y\},$$
$$R_f = \{y \mid (x, y) \in f \text{ for some } x\}.$$

If f is a function and $(x, y) \in f$, then y is called the *functional value* or *image of f at x* and is denoted by $f(x)$. That is, the symbol $f(x)$ represents the unique second component of that ordered pair of f in which x is the first component.

EXAMPLE 1–3. If the function f is the finite set of ordered pairs

$$f = \{(-1, 0), (0, 0), (1, 2), (2, 1)\},$$

then

$$D_f = \{-1, 0, 1, 2\}, \qquad R_f = \{0, 1, 2\}$$

and we write $f(-1) = 0$, $f(0) = 0$, $f(1) = 2$ and $f(2) = 1$.

Quite often we describe a function by giving a formula for its ordered pairs. For instance, $f = \{(x, x^2 + 2) \mid x \in R^\#\}$. Using the functional value notation, we would then write

$$f(x) = x^2 + 2 \qquad \text{for} \qquad x \in R^\#.$$

DEFINITION 1-7. If $f \subseteq X \times Y$, so that $D_f \subseteq X$ and $R_f \subseteq Y$, then f is referred to as a function from X *into* Y. In particular, if $D_f = X$, we will employ the notation

$$f\colon X \to Y.$$

The function f is said to be *onto* Y, or an *onto function*, whenever f is a function from X into Y and $R_f = Y$. Thus f is onto Y if and only if for each $y \in Y$ there exists some $x \in D_f$ with $(x, y) \in f$, so that $y = f(x)$.

Since functions are sets, we have a ready-made definition of equality of functions: two functions f and g are *equal* if and only if they have the same members. Accordingly, $f = g$ if and only if $D_f = D_g$ and $f(x) = g(x)$ for each element x in their common domain.

Suppose that f and g are two specific functions. The following formulas define functions $f + g, f - g, f \cdot g$ and f/g by specifying the value of these functions at each point of their domain:

$$\left.\begin{aligned} (f + g)(x) &= f(x) + g(x), \\ (f - g)(x) &= f(x) - g(x), \\ (f \cdot g)(x) &= f(x)g(x), \end{aligned}\right\} \qquad \text{where} \qquad x \in D_f \cap D_g,$$

$$(f/g)(x) = f(x)/g(x),$$

$$\text{where} \qquad x \in (D_f \cap D_g) - \{x \in D_g \mid g(x) = 0\}.$$

We term $f + g$, $f - g$, $f \cdot g$ and f/g, the *sum*, *difference*, *product*, and *quotient* of f and g respectively. Clearly the definitions of these functions make sense only when R_f and R_g are subsets of systems in which addition, subtraction, multiplication, and division are permissible.

EXAMPLE 1-4. Suppose $f = \{(x, \sqrt{4 - x^2}) \mid -2 \le x \le 2\}$ and $g = \{(x, 2/x) \mid R^\# - \{0\}\}$, so that $f(x) = \sqrt{4 - x^2}$, $g(x) = 2/x$. Then for $x \in D_f \cap D_g = D_f - \{0\}$,

$$(f + g)(x) = \sqrt{4 - x^2} + \frac{2}{x},$$

$$(f - g)(x) = \sqrt{4 - x^2} - \frac{2}{x},$$

$$(f \cdot g)(x) = (\sqrt{4 - x^2})\,\frac{2}{x},$$

$$(f/g)(x) = \frac{\sqrt{4 - x^2}}{2/x} = \frac{x}{2}\sqrt{4 - x^2}.$$

DEFINITION 1–8. The *composition* of two functions f and g, denoted by $f \circ g$, is the function

$$f \circ g = \{(x, y) \mid \text{for some } z,\ (x, z) \in g \quad \text{and} \quad (z, y) \in f\}.$$

Written in terms of functional values, we have

$$(f \circ g)(x) = f(g(x)), \qquad \text{where} \quad x \in D_g \quad \text{and} \quad g(x) \in D_f.$$

This last notation serves to explain the order of symbols in $f \circ g$; g is written directly beside x, since the functional value $g(x)$ is obtained first. It is apparent from the definition that, so long as $R_g \cap D_f \neq \emptyset$, $f \circ g$ is meaningful. Also, $D_{f \circ g} \subseteq D_g$ and $R_{f \circ g} \subseteq R_f$.

EXAMPLE 1–5. Let

$$f = \{(x, \sqrt{x}) \mid x \in R^{\#}, x \geq 0\}$$

and

$$g = \{(x, 2x + 3) \mid x \in R^{\#}\},$$

so that $f(x) = \sqrt{x}$, $g(x) = 2x + 3$. Then,

$$(f \circ g)(x) = f(g(x)) = f(2x + 3) = \sqrt{2x + 3},$$

where

$$\begin{aligned} D_{f \circ g} = \{x \in D_g \mid g(x) \in D_f\} &= \{x \in R^{\#} \mid 2x + 3 \in D_f\} \\ &= \{x \mid 2x + 3 \geq 0\}. \end{aligned}$$

On the other hand,

$$(g \circ f)(x) = g(f(x)) = g(\sqrt{x}) = 2\sqrt{x} + 3,$$

where

$$\begin{aligned} D_{g \circ f} = \{x \in D_f \mid f(x) \in D_g\} &= \{x \geq 0 \mid \sqrt{x} \in R^{\#}\} \\ &= \{x \mid x \geq 0\}. \end{aligned}$$

One observes that $f \circ g$ is different from $g \circ f$; indeed, rarely does it happen that $f \circ g = g \circ f$.

The next theorem concerns some of the basic properties of the operation of functional composition. Its proof is an exercise in the use of the definitions of this section.

THEOREM 1–4. If f, g, and h are functions for which the following operations are defined, then

(1) $(f \circ g) \circ h = f \circ (g \circ h)$,
(2) $(f + g) \circ h = (f \circ h) + (g \circ h)$,
(3) $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$.

Proof. We establish here only property (3). The other parts of the theorem are obtained in a similar fashion and so are left as an exercise. Observe first that

$$\begin{aligned} D_{(f\cdot g)\circ h} &= \{x \in D_h \mid h(x) \in D_{f\cdot g}\} \\ &= \{x \in D_h \mid h(x) \in D_f \cap D_g\} \\ &= \{x \in D_h \mid h(x) \in D_f\} \cap \{x \in D_h \mid h(x) \in D_g\} \\ &= D_{f\circ h} \cap D_{g\circ h} = D_{(f\circ h)\cdot(g\circ h)}. \end{aligned}$$

Now, for $x \in D_{(f\cdot g)\circ h}$, we have

$$\begin{aligned} [(f \cdot g) \circ h](x) = (f \cdot g)\big(h(x)\big) &= f\big(h(x)\big) \cdot g\big(h(x)\big) \\ &= (f \circ h)(x) \cdot (g \circ h)(x) \\ &= [(f \circ h) \cdot (g \circ h)](x), \end{aligned}$$

which, according to the definition of equality of functions, shows that

$$(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h).$$

DEFINITION 1–9. A function f is termed *one-to-one* if and only if $x_1, x_2 \in D_f$, with $x_1 \neq x_2$, implies $f(x_1) \neq f(x_2)$. That is, distinct elements in the domain have distinct functional values.

When establishing one-to-oneness, it will often prove to be more convenient to use the contrapositive of Definition 1–9:

$$f(x_1) = f(x_2) \quad \text{implies} \quad x_1 = x_2.$$

In terms of ordered pairs, a function f is one-to-one if and only if no two distinct ordered pairs of f have the same second component. Thus the collection of ordered pairs obtained by interchanging the components of the pairs of f also results in a function. This observation indicates the importance of such functions.

More specifically, the *inverse* of a one-to-one function f, symbolized by f^{-1}, is the set of ordered pairs

$$f^{-1} = \{(y, x) \mid (x, y) \in f\}.$$

The function f^{-1} has the properties

$$\begin{aligned} (f^{-1} \circ f)(x) &= x \quad \text{for} \quad x \in D_f, \\ (f \circ f^{-1})(y) &= y \quad \text{for} \quad y \in D_{f^{-1}} = R_f, \end{aligned}$$

so that f^{-1} may be considered the inverse of f with respect to composition.