Introduction to Modern Algebra

Revised Edition

NEAL H. McCOY

Introduction to Modern Algebra

Revised Edition

NEAL H. McCOY

Gates Professor of Mathematics
Smith College

ALLYN AND BACON, INC. BOSTON

Library of Congress Catalog Card Number: 68–15225

Printed in the United States of America

Third Printing . . . . . May, 1969

Introduction to Modern Algebra

Dedicated to the memory of my son

PAUL

Preface

When the first edition of this book came out in 1960 there were only three or four other texts available in English for use in undergraduate courses in abstract algebra. The increased recognition of the importance of this subject in the training of mathematicians and of teachers of mathematics may be indicated by the fact that some twenty additional texts have appeared since that time.

This book requires somewhat less mathematical sophistication on the part of the student than do most of the other available texts. As was true for the first edition, this revised edition is intended to be understandable by students who have had little or no background in abstract mathematics and are just beginning the study of abstract algebra.

The general organization and style have not been changed in any essential way. Although some sections and even a few chapters have been modified only slightly or not at all, there have been some fairly substantial changes in content and emphasis. The principal changes which have been introduced in this edition are the following.

Mappings, especially homomorphisms, are introduced fairly early and emphasized throughout. Although the elementary number systems still occupy a central place in the early part of the book, the real numbers are treated very briefly instead of in full detail. Groups are presented before polynomials, although the order of these two chapters could be reversed with no particular difficulty. The study of groups is carried through normal subgroups, quotient groups, and the fundamental theorem on group homomorphisms. A short chapter on ideals and quotient rings then carries the theory of rings to approximately the same point; that is, through the fundamental theorem on ring homomorphisms. Finally, the chapter on linear transformations and matrices has been rewritten and expanded somewhat.

Many of the lists of exercises have been extended, particularly by the addition of some more difficult ones. In my classes, I have often used some of these as "optional exercises" with which to challenge the better students.

A minor change has been the adoption of what is becoming almost standard notation, namely, $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ for, respectively, the ring of integers, the ring of integers modulo n, and the fields of rational numbers, real numbers, and complex numbers.

Professor Robert J. Smith gave the final manuscript a careful reading, and I am indebted to him for catching a number of slips and also for some valuable suggestions which have improved the accuracy or the clarity at several points in the text.

I am greatly indebted to my former colleague and long-time friend, Professor Richard E. Johnson, who offered to read the proofs of this book when he learned that I was unable to read them at the time the task needed to be done. Although I accept the responsibility for those slips which may possibly remain, I am most grateful for his generous and unselfish assistance.

Northampton, Mass. NEAL H. MCCOY

From the Preface to the First Edition

This book is designed as a text for a *first* course in modern abstract algebra. Since many students find such a course fairly difficult, it has been my goal to make the exposition as clear and simple as possible but, at the same time, sufficiently precise and thorough to furnish an honest introduction to the methods and results of abstract algebra.

I have taught a preliminary version of this book to a Smith College class at the undergraduate level, and Professor W. H. Durfee has taught about half of it to a Mount Holyoke College class at the same level. In addition, I have taught various preliminary versions of parts of the first few chapters in three Summer Institutes for High School Teachers, two at the State University of Iowa and one at Randolph-Macon Woman's College, and also in an Academic Year Institute at the University of North Carolina. I am greatly indebted to all those former students who by their questions and difficulties have helped to improve the exposition in various ways. Professor Durfee also made several valuable suggestions as a result of his experience in teaching part of the material.

It would not be possible to list all of those to whom I am indebted in a direct or indirect way. However, I would like to mention a special indebtedness to my colleague, Professor R. E. Johnson. Although, for the most part, I did not discuss with him the choice

of topics or the way in which they were to be presented, nevertheless, over the years we have had many discussions on various topics in abstract algebra and on the pedagogical problems involved in teaching this subject matter. Accordingly, he has had a substantial, although partially indirect, influence on this book. I have also taught his excellent text in this same field and have been consciously influenced by it in certain ways, and no doubt have been unconsciously influenced in other ways as well. In addition, I am grateful to him for substantial help in reading the galley proofs.

Finally, it is a pleasure to express my appreciation to my wife, Ardis, without whose inspiration and encouragement this book would never have been written.

Northampton, Mass. NEAL H. MCCOY

Contents

1

Some Fundamental Concepts

The outstanding characteristic of modern algebra, and indeed also of many other branches of modern mathematics, is its extensive use of what is known as the axiomatic or postulational method. The method itself is not new, since it was used by Euclid (about 300 B.C.) in his construction of geometry as a deductive science. However, in many ways the modern viewpoint is quite different from Euclid's, and the power of the method did not become apparent until this century.

We shall not attempt to give here any description or analysis of the postulational method, but the material of the next few chapters will illustrate the ideas involved. This first brief chapter will present a few basic concepts to be used repeatedly, and will introduce some convenient notation. Although the reader may have previously met some, or even all, of these concepts, they are so fundamental for our purposes that it seems desirable to start off by presenting them in some detail. Many more illustrations of each concept will appear in later chapters.

1.1 Sets

The concept of *set* (class, collection, aggregate) is fundamental in mathematics as it is in everyday life. A related concept is that of *element* of a set. We make no attempt to define these terms but shall presently give some examples that will illustrate the sense in which they are being used.

First of all, we may say that a set is made up of elements. In order to give an example of a set we need, therefore, to exhibit its elements or to give some rule that will specify its elements. We shall often find it convenient to denote sets by capital letters and elements of sets by lower-case letters. If a is an element of the set A, we may indicate this fact by writing $a \in A$ (read, "a is an element of A"). Also, $a \notin A$ will mean that a is not an element of the set A. If both a and b are elements of the set A, we may write $a, b \in A$.

If P is the set of all positive integers, $a \in P$ means merely that a is a positive integer. Certainly, then, it is true that $1 \in P$, $2 \in P$, and so on. If B is the set of all triangles in a given plane, $a \in B$ means that a is one of the triangles in this plane. If C is the set of all books in the Library of Congress, then $a \in C$ means that a is one of these books. We shall presently give other examples of sets.

If $a, b \in A$ and we write $a = b$, it is always to be understood that these are identical elements of A. Otherwise expressed, a and b are merely different symbols designating the same element of A. If $a, b \in A$ and it is not true that $a = b$, we may indicate this fact by writing $a \neq b$ and may say that a and b are *distinct* elements of A.

If A and B are sets with the property that every element of A is also an element of B, we call A a *subset* of B and write $A \subseteq B$ (read, "A is contained in B"). Perhaps we should point out that for every set A it is true that $A \subseteq A$ and hence, according to our definition, one of the subsets of A is A itself. If $A \subseteq B$ and also $B \subseteq A$, then A and B have exactly the same elements and we say that these sets are *equal*, and indicate this by writing $A = B$. If it is not true that $A = B$, we may write $A \neq B$. If $A \subseteq B$ and $A \neq B$, then we say that A is a *proper subset* of B and indicate this fact by the notation $A \subset B$ (read, "A is properly contained in B"). Clearly, $A \subset B$ means that every element of A is an element of B and, moreover, B contains at least one element which is not an element of A.

Sometimes, as has been the case so far, we may specify a set by stating in words just what its elements are. Another way of specifying a set is to exhibit its elements. Thus, $\{x\}$ indicates the set which consists of the single element x, $\{x, y\}$ the set consisting of the two elements x and y, and so on. We may write $A = \{1, 2, 3, 4\}$ to mean that A is the set whose elements are the positive integers 1, 2, 3, and 4. If P is the set of all positive integers, by writing

$$K = \{a \mid a \in P, a \text{ divisible by } 2\},$$

we shall mean that K consists of all elements a having the properties indicated after the vertical bar, that is, a is a positive integer and is divisible by 2. Hence, K is just the set of all *even* positive integers. We may also write

$$K = \{2, 4, 6, 8, \cdots\},$$

the dots indicating that all even positive integers are included in this set. As another example, if

$$D = \{a \mid a \in P, a < 6\},$$

then it is clear that $D = \{1, 2, 3, 4, 5\}$.

Whenever we specify a set by exhibiting its elements, it is to be understood that the indicated elements are distinct. Thus, for example, if we write $B = \{x, y, z\}$, we mean to imply that $x \neq y$, $x \neq z$, and $y \neq z$.

For many purposes, it is convenient to allow for the possibility that a set may have no elements. This fictitious set with no elements we shall call the *empty set*. According to the definition of subset given above, the empty set is a subset of every set. Moreover, it is a proper subset of every set except the empty set itself. The empty set is often designated by $\varnothing$, and thus we have $\varnothing \subseteq A$ for every set A.

If A and B are sets, the elements that are in both A and B form a set called the *intersection* of A and B, denoted by $A \cap B$. Of course, if A and B have no elements in common, $A \cap B = \varnothing$.

If A and B are sets, the set consisting of those elements which are elements either of A or of B (or of both), is a set called the *union* of A and B, denoted by $A \cup B$.

As examples of the concepts of intersection and union, let $A = \{1, 2, 3\}$, $B = \{2, 4, 5\}$, and $C = \{1, 3, 6\}$. Then we have $A \cap B = \{2\}$, $A \cap C = \{1, 3\}$, $B \cap C = \varnothing$, $A \cup B = \{1, 2, 3, 4, 5\}$, $A \cup C = \{1, 2, 3, 6\}$, and $B \cup C = \{1, 2, 3, 4, 5, 6\}$.

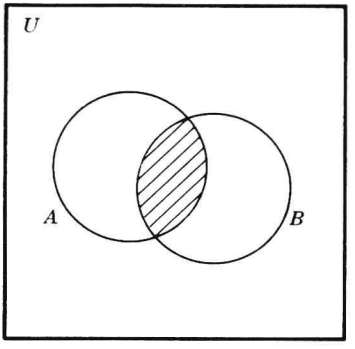
Although we have defined the intersection and the union of only *two* sets, it is easy to extend these definitions to any number of sets, as follows. The *intersection* of any number of given sets is the set consisting of those elements which are in all the given sets, and the *union* is the set consisting of those elements which are in at least one of the given sets.

If A, B, and C are sets, each of the following is an immediate consequence of the various definitions which we have made:

$A \cap B \subseteq A$ and $A \cap B \subseteq B$.

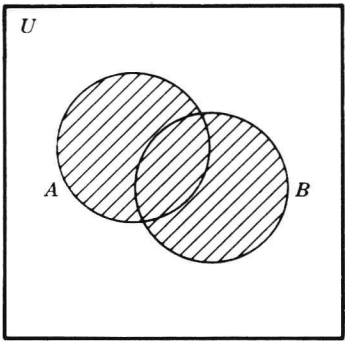
$A \subseteq A \cup B$ and $B \subseteq A \cup B$.
$A \cap B = A$ if and only if $A \subseteq B$.
$A \cup B = A$ if and only if $B \subseteq A$.
If $B \subseteq C$, then $A \cup B \subseteq A \cup C$ and $A \cap B \subseteq A \cap C$.

In working with sets, so-called Venn diagrams are sometimes used to give a purely symbolic, but convenient, geometric indication of the relationships involved. Suppose, for the moment, that all sets being considered are subsets of some fixed set U. In Figures 1 and 2,



$A \cap B$

Figure 1



$A \cup B$

Figure 2

the points within the square represent elements of U. If A and B are subsets of U, then the elements of A and B may be represented by the points within indicated circles (or any other closed regions). The intersection and the union of the sets A and B are then represented in an obvious way by the shaded regions in Figures 1 and 2, respectively.

Of course, the use of a Venn diagram is not meant to imply anything about the nature of the sets being considered, whether or not indicated intersections are nonempty, and so on. Moreover, such a diagram cannot in itself constitute a proof of any fact, but it may be quite helpful in suggesting a proof.

Let us make the following remarks by way of emphasis. A problem of frequent occurrence is that of proving the equality of two sets. Suppose that C and D are given sets and it is required to prove that $C = D$. By definition of equality of sets, we need to show that $C \subseteq D$ and $D \subseteq C$. Sometimes one or both of these conditions follow easily from given facts. If not, the standard procedure is to start with an arbitrary element of C and show that it is an element of D, and

then do the same thing with C and D interchanged. When we write "let $x \in C$" or "if $x \in C$," we mean that x is to represent a completely arbitrary element of the set C. Hence, to show that $C \subseteq D$, we only need to show that "if $x \in C$, then $x \in D$." Of course, any other symbol could be used in place of x. Let us now give an example by way of illustration.

Example. If A, B, and C are sets, prove that

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

Solution. First, let us take advantage of the opportunity to give another illustration of a Venn diagram. If we think of the meaning of $A \cup (B \cap C)$ as consisting of all elements of A together with all elements that are in both B and C, we see that the set $A \cup (B \cap C)$ may be represented by the shaded portion of the Venn

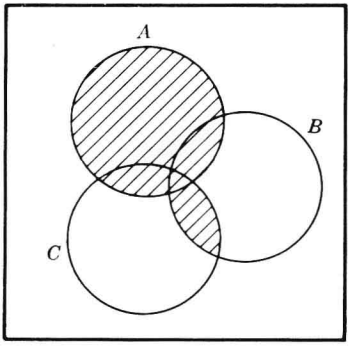


Figure 3

diagram in Figure 3. We leave it to the reader to verify that this same shaded region also represents the set $(A \cup B) \cap (A \cup C)$.

We now proceed to give a formal proof of the required formula. Clearly, $B \cap C \subseteq B$, so $A \cup (B \cap C) \subseteq A \cup B$. Similarly, $B \cap C \subseteq C$, and hence $A \cup (B \cap C) \subseteq A \cup C$. It follows that

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

and we have obtained inclusion one way. To obtain inclusion the other way, let $x \in (A \cup B) \cap (A \cup C)$ and let us show that $x \in A \cup (B \cap C)$. Now $x \in A \cup B$ and also $x \in A \cup C$. If $x \in A$,