An Introduction to Modern Algebra

BURTON W. JONES

Modern Algebra

MACMILLAN PUBLISHING CO., INC.
New York

COLLIER MACMILLAN PUBLISHERS
London

Printed in the United States of America

Macmillan Publishing Co., Inc.
866 Third Avenue, New York, New York 10022

Collier-Macmillan Canada, Ltd.

Library of Congress Cataloging in Publication Data

Jones, Burton Wadsworth, (   )
An introduction to modern algebra.

Bibliography: p.
1. Algebra, Abstract. I. Title.
QA162.J66   512'.02   74-3795
ISBN 0-02-361250-9

Printing: 1 2 3 4 5 6 7 8   Year: 5 6 7 8 9 0

An Introduction to **Modern Algebra**

An Introduction to

BURTON W. JONES *The University of Colorado*

To Marian

Preface

This text is intended for junior and senior students in colleges or universities who have the mathematical maturity that a beginning course or two in calculus should impart. It is written at a somewhat lower level than *A Survey of Modern Algebra* by Garrett Birkhoff and Saunders Mac Lane and still lower than *Topics in Algebra* by Israel Herstein and *Modern Algebra* by Bartel van der Waerden. The influence of these three great books on this text is evident.

In writing the book, I have been especially mindful that the student should have a sense of involvement in the development of the subject. To this end, in order to deal with a fundamental concept like a group, for instance, I do not begin by listing a set of postulates but rather show how the idea comes up as an abstraction of a set of properties common to two number systems. In general, if a term is to be defined, I want to make sure that the student has some prior acquaintance with ideas that make the concept meaningful and useful.

I do not usually introduce a new term until I am ready to use it. For instance, the idea of a normal subgroup is not defined when cosets are first introduced nor even when the kernel of a homomorphism is first dealt with. But as soon as it appears that we would be in trouble unless the left and right cosets of the kernel are the same, then the concept of a normal subgroup is forced upon us.

From an algebraist's point of view, the role of ideals in ring theory is probably much more impressive than for unique decomposition into products of prime ideals. But from a less sophisticated point of view, it is when we are faced with the problem of unique decomposition that Dedekind's idea shines in all its brilliance. Similarly, Galois theory, although of fundamental importance in algebra, can be shown to be important to a beginner by its immediate usefulness in the solution of the classical problem of constructions and solutions by radicals.

Special effort is made to keep the student informed about where we are going and why. Tentative exploration often seems useful. Where a somewhat special result is derived, the student is told that it *is* special and where we shall use it later. This information will also guide those teachers who may want to omit certain topics and need to know the price to be paid for such omissions.

Much use is made of numerical examples to lead to ideas and to illustrate concepts that have already been formulated. There are also a number of places where a difficult proof is first shown in a numerical setting, then carried out for a special case in the pattern of the general proof, before finally proving the theorem completely. I feel no compulsion to state a theorem in its most general form.

The exercises are a very important part of the text. Some are routine, to help fix the abstract ideas in concrete situations. A number of proofs of theorems are left to the student so that he can test his knowledge and feel involved in the development of the results. Answers and partial answers are given to selected exercises. Sometimes the answer is merely "yes" or "no," to reassure the student that he is on the right track while leaving the reasons to him. At other times an answer to part of an exercise is given in some detail.

The first three chapters give the basic ideas of groups and fields. An average class should be able to acquire most of this material in a one-semester course that meets three times a week. I would, however, be disappointed not to take some of the topics in the last two chapters, because it is there that the results on groups and fields are really put to work. Furthermore, the last chapter, especially, shows the intimate connection between groups and fields. Students who have some prior knowledge of linear algebra should, in a semester's course, be able to get at least a taste of one of the last two chapters.

In Chapter I we lead up to the abstract idea of a group, then define it, and devote the rest of the chapter to important examples of groups from various parts of mathematics. The purpose is to show the student how ubiquitous the properties of a group are, to help him to become familiar with a group in many of its forms, and to acquire a backlog of experience and examples on which the concepts of the next two chapters can be built. The first four sections are closely interrelated. The fifth and sixth deal with functions and transformations. They all lead up to the idea of a subgroup and what it takes to prove that a subset of a group is a group. Sections 8 and 9 are intimately related. In Section 10 we not only have a rudimentary example of an ideal but derive a result that will be immediately useful. Even the little group from logic is not just a curiosity but concerns itself with the structure of proof. The idea of an abstract group is a simple one (I have taught it to freshmen) but to really appreciate it requires experience; providing this experience is an important aim of this chapter.

Chapter II begins with the idea of an isomorphism. Logically, it might seem more efficient to introduce first the concept of a homomorphism and then specialize it to an isomorphism. But the latter is a simpler concept and much more readily applicable to examples at hand. Cyclic groups are dealt with in detail but only after the student has had experience with more general groups. Since normal subgroups and homomorphisms go together, they are introduced in juxtaposition.

Chapter III begins with the idea of a field because, in my opinion, this is a simpler concept for the beginning student than that of an integral domain or a ring. Another reason for postponing the idea of a ring is that the most accessible example of a ring that is not an integral domain is the set of matrices of some order; and a student without linear algebra in his background might not feel at home with such an illustration. The section on derivatives and separability is introduced, first, because there may be some interest in seeing how a derivative can be defined for polynomials without the idea of a limit, and, second, this section is needed in parts of Chapter VI. It should be pointed out that we treat algebraic extensions only partially in Section 14 because we lack some ideas of a vector space. When a class is familiar with vector spaces, one could give extensions more adequate treatment by introducing at this stage part of Section 2 of Chapter VI.

Chapter IV is a service chapter for those students without any background in linear algebra. The point is that certain topics in linear algebra are needed in the last two chapters, and it would seem awkward to have to refer students to other texts for these results. The chapter begins with the basic idea of a vector space and linear dependence and independence. These are the only parts of Chapter IV that are needed in Chapter VI. Matrices and determinants are used crucially in Section 6 of Chapter V. Otherwise, except for the use of matrices as examples of rings, we do not need them in the rest of the book. Thus the choice of material in this chapter depends on the training of the class and what additional topics in the book they will study.

Chapter V justifies the concept of an ideal by posing the problem of unique decomposition and then solving it. The latter involves, as is there noted, two rather difficult theorems about algebraic fields, which neither the student nor the teacher may want to tackle. In such a case I would prefer, myself, to assume these two theorems and then proceed to solve the problem at hand, since, as I noted earlier, I think the student would be much more impressed with the use of ideals in this connection than for homomorphisms of rings.

But it is true that Section 8 through Theorem 8.7 and Section 9 could be taken up without much of the rest of the chapter.

Chapter VI uses the first three sections of Chapter V but is otherwise independent of its predecessor. Hence a class could omit all but those three sections before proceeding to Chapter VI. The latter is concerned with the related problems of constructions and solutions by radicals. It develops as needed the tool of Galois theory to solve these problems. This chapter ties together most of what has previously been covered in the book: groups, fields, and algebraic extensions of fields.

My indebtedness to the four authors mentioned in the first paragraph of this preface is very great. I especially admire the exploratory point of view from which Herstein wrote his book, and this has influenced my approach to some topics. I should also acknowledge that I have adopted with some enthusiasm the practice of George Simmons in his book on differential equations and have given brief biographical sketches of those mathematicians whose names are linked with the subject and whose ideas underlie the basic theory.

I should like to record my special appreciation of the late Carl B. Allendoerfer, who in many ways encouraged the writing of this book and whose careful and perceptive comments were a crucial influence in its development. I am also grateful to Charles Brase, who, in reading the semifinal version of the manuscript, gave many helpful suggestions. Furthermore, I want to acknowledge the contributions of Miss Kanda Kunze of the University of Arizona and Mrs. Mae Jean Ruehlman of the University of Colorado, who typed the manuscript at various stages. Thanks could not be complete without including the Macmillan staff in their meticulous attention to many details of production.

Boulder, Colorado BURTON W. JONES

Contents

VI. Constructions and Galois Theory 272

I

Definition and Examples of Groups

1. Introduction

In the process of studying any subject, one should stop from time to time to correlate what he has learned. Such coordination is especially useful in mathematics, where the body of knowledge increases rapidly and emphasis shifts. Without such periodic reassessment, what needs to be learned can quickly become unmanageable by sheer volume alone. To achieve such correlation, we shall in this book deal with some fundamental mathematical structures—sets of objects from various parts of the subject that have certain properties in common. When we look at these common properties, we may see relationships not previously perceived. Such a look will increase our insight into known mathematics and will lead into realms that are new to us, although they have important properties in common with the old.

The subject matter of this book is thought of as algebra, but we shall see that it has much in common with parts of analysis and geometry as well. In fact, it is the interplay of various parts of mathematics that lends importance to much of the material presented.

We start with the technical idea of a group because it can be described briefly and has a wealth of application. To work toward this fundamental concept, we first point out a list of properties common to two sets of numbers, and from this abstract the definition of "group." In the rest of the chapter we explore various examples from different parts of mathematics not only to show how being a group can serve as a unifying concept, but also to provide a source for the development of properties of groups that are discussed in later chapters. We postpone until Chapter II consideration of most of the general properties of groups.

2. Definition of a Group

First, let us consider certain properties of two sets of numbers: **Z**, the set of all integers, and **R***, the set of all nonzero real numbers (**R** denotes the real numbers, including zero). To emphasize the relationships, we list the properties in parallel columns.

<table>
<tr><th>Addition of integers, <b>Z</b></th><th>Multiplication of nonzero real numbers <b>R</b>*</th></tr>
<tr><td colspan="2">1. Closure</td></tr>
<tr><td>If b and c are in <b>Z</b>, then $b + c$ and $c + b$ are in <b>Z</b>.</td><td>If b and c are in <b>R</b>*, then $b \cdot c$ and $c \cdot b$ are in <b>R</b>*.</td></tr>
<tr><td colspan="2">2. Associativity</td></tr>
<tr><td>For all a, b, and c in <b>Z</b>, we have $(a + b) + c = a + (b + c)$.</td><td>For all a, b, and c in <b>R</b>*, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.</td></tr>
<tr><td colspan="2">3. Existence of an identity</td></tr>
<tr><td>There is a number 0 in <b>Z</b> such that $0 + a = a + 0 = a$ for all a in <b>Z</b>.</td><td>There is a number 1 in <b>R</b>* such that $1 \cdot a = a \cdot 1 = a$ for all a in <b>R</b>*.</td></tr>
<tr><td colspan="2">4. Existence of an inverse</td></tr>
<tr><td>For each a in <b>Z</b>, there is a number $(-a)$ in <b>Z</b> such that $a + (-a) = (-a) + a = 0$.</td><td>For each a in <b>R</b>*, there is a number a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = 1$. (We also write $1/a$ for a^{-1}.)</td></tr>
</table>

To be sure, these are not the only properties common to addition of integers and multiplication of nonzero real numbers. But we select these because there is a striking parallelism between these two sets of four properties and because we shall see later in this chapter that many other examples of sets also have these properties.

Notice that for multiplication of integers, property 4 fails to hold, since, for example, there is no integer x such that $3x = 1$. On the other hand, the four properties of addition hold if **Z** is replaced by **Q**, the set of rational numbers, **R**, the set of real numbers, or **C**, the set of complex numbers.

Furthermore, the properties of the right-hand column hold if $\mathbf{R}^*$ is replaced by $\mathbf{Q}^*$ or $\mathbf{C}^*$, the respective sets of $\mathbf{Q}$ and $\mathbf{C}$ with zero excluded.

It is also true that the four properties of addition hold if $\mathbf{Z}$ is replaced by $\mathbf{Z}[x]$, the set of polynomials $f(x)$ in x with coefficients in $\mathbf{Z}$. In fact, the coefficients of the polynomials in x could be rational, real, or complex and the properties listed for addition would still hold.

In order to gradually develop a concept that includes both sets with addition and multiplication, respectively, let us look more carefully at the two sets above. Each integer is an element of the set $\mathbf{Z}$ and each nonzero real number an element of $\mathbf{R}^*$. So we start with a set. Then there is a means of combining two elements of the set to get a third, a process we call an *operation*. For the first set above, the operation is addition and, for the second, multiplication. If we denote the operation by $\circ$, we can write

$$s \circ s' = s'',$$

where s, s', and s'' are in the set S. For addition of integers, $\circ$ is $+$, and for multiplication of real numbers it is a raised dot $\cdot$, the symbol for multiplication. Property 2 affirms that the operation is associative.

You may well wonder why we did not include in our list the commutative properties: $a + b = b + a$ and $a \cdot b = b \cdot a$. We have, in fact, purposely avoided this requirement in order to enlarge the scope of the concept of a group. So if the result of the operation is to be allowed to depend on the order, we must consider not just the pair of elements but an *ordered pair*, that is, a pair in which the order makes a difference. Thus we have led up to the following formal definition of a binary operation ("binary" because it combines two elements).

Definition. *Given a set S, we call $\circ$ a* binary operation *on S if it assigns to each ordered pair of elements s and s' of S a unique element s'' of S.*

This operation can be written in at least two ways:

$$s \circ s' = s'' \qquad \text{or} \qquad (s, s') \xrightarrow{\circ} s'',$$

where s, s', and s'' are elements of S.

Since the idea of a binary operation includes closure, we need not mention this property in the formal definition of a group, which follows.

Definition. *Given a nonempty set of elements S and a binary operation $\circ$ on S, then we call S a* group *"under" the operation $\circ$ if the following properties hold:*

1. *The binary operation is* associative; *that is, for every a, b, and c in S,*

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

2. *There is an element e of S such that $e \circ a = a \circ e = a$ for every element a of S. Such an element e is called an* identity *element.* (We shall prove that it is unique.)
3. *To each element b of S there corresponds an element $\bar{b}$ of S such that $b \circ \bar{b} = \bar{b} \circ b = e$, where e is the identity element. Such an element is called an* inverse *of b.* (It can be proved that $\bar{b}$ is uniquely determined by b.)

If you let S be $\mathbf{Z}$ and $\circ$ be $+$, you will see that the integers form a group under addition, whereas if S is $\mathbf{R}^*$ and the operation is multiplication, it follows that the nonzero real numbers form a group under multiplication. Similarly, the sets $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ (rational, real, and complex numbers), as well as $\mathbf{Z}[x]$, form a group under addition; $\mathbf{Q}^*$ and $\mathbf{C}^*$ form a group under multiplication.

There are five other properties common to $\mathbf{Z}$ under addition and $\mathbf{R}^*$ under multiplication, which we list as follows, using the terminology that we have used for the definition of a group.

4. The identity of a group is unique; that is, there is only one identity element in a group.
5. The inverse of any element of a group is unique; that is, each element b has exactly one inverse.
6. If a and b are any elements of a group, then there are unique elements x and y of the group for which $a \circ x = b$ and $y \circ a = b$.
7. The cancellation properties hold: (a) if $a \circ b = a \circ c$, then $b = c$; (b) if $b \circ a = c \circ a$, then $b = c$.
8. The inverse of $a \circ b$ is $\bar{b} \circ \bar{a}$.

First, let us see what these mean for addition of integers. Property 4 affirms that 0 is the only integer z for which $z + a = a + z = a$ for all integers a, and property 5 affirms that every integer has only one negative. Both of these are very obvious. Slightly less obvious is property 6, which maintains that $a + x = b$ and $y + a = b$ are solvable for x and y, no matter what integers a and b are. Property 7 states that $a + b = a + c$ or $b + a = c + a$ implies that $b = c$. Property 8 affirms that the inverse of $a + b$ is $(-b) + (-a)$. You should follow through these same properties for $\mathbf{R}^*$ under multiplication.

Now, these five properties are different from the first three, in that they can be deduced from the first three. This means that whenever we have verified that a system is a group, these properties also hold as extra dividends. So now we proceed to show how property 4 and half of property 6 follow from the group properties, leaving the rest of the proofs as exercises.

To prove property 4, suppose that there are two identity elements e and e' of a group. Then $e \circ e' = e'$ since e is an identity, and $e \circ e' = e$ since e' is an identity. Hence $e = e'$.