Modern Algebra with Applications

Modern Algebra with Applications

WILLIAM J. GILBERT
University of Waterloo

A WILEY-INTERSCIENCE PUBLICATION
JOHN WILEY & SONS
New York • London • Sydney • Toronto

Library of Congress Cataloging in Publication Data:

Gilbert, William J 1941–
Modern algebra with applications.

"A Wiley-Interscience publication."
Bibliography: p.
Includes index.
1. Algebra, Abstract. I. Title.

QA162.G53 512′.02 76-22756
ISBN 0-471-29891-3

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Preface

Until recently the applications of modern algebra were mainly confined to other branches of mathematics. However, the importance of modern algebra and discrete structures to many areas of science and technology is now growing rapidly. It is being used extensively in computing science, physics, chemistry, and data communication as well as in new areas of mathematics such as combinatorics. We believe that the fundamentals of these applications can now be taught at the junior level. This book therefore constitutes a one-year course in modern algebra for those students who have been exposed to some linear algebra. It contains the essentials of a first course in modern algebra together with a wide variety of applications.

Modern algebra is usually taught from the point of view of its intrinsic interest, and students are told that applications will appear in later courses. Many students lose interest when they do not see the relevance of the subject and often become skeptical of the perennial explanation that the material will be used later. However, we believe that, by providing interesting and nontrivial applications as we proceed, the student will better appreciate and understand the subject.

We cover all the group, ring, and field theory that is usually contained in a standard modern algebra course; the exact sections containing this material are indicated in the Table of Contents. We stop short of the Sylow theorems and Galois theory. These topics could only be touched on in a first course, and we feel that more time should be spent on them if they are to be appreciated.

In Chapter 2 we discuss Boolean algebras and their application to switching circuits. These provide a good example of algebraic structures whose elements are nonnumerical. However, many instructors may prefer to postpone or omit this chapter and start with the group theory in Chapters 3 and 4. Groups are viewed as describing symmetries in nature and in mathematics. In keeping with this view, the rotation groups of the regular solids are investigated in Chapter 5. This material provides a good starting point for students interested in applying group theory to physics and chemistry. Chapter 6 introduces the Pólya-Burnside method of enumerating equivalence classes of sets of symmetries and provides a very practical application of group theory to combinatorics. Monoids are becoming more important algebraic structures today; these are discussed in Chapter 7 and are applied to finite-state machines.

The ring and field theory is covered in Chapters 8–11. This theory is motivated by the desire to extend the familiar number systems to obtain the Galois fields and to discover the structure of various subfields of the real and complex numbers. Groups are used in Chapter 12 to construct Latin squares, whereas Galois fields are used to construct orthogonal Latin squares. These can be used to design statistical experiments. We also indicate the close relationship between orthogonal Latin squares and finite geometries. In Chapter 13 field extensions are used to show that some famous geometrical constructions, such as the trisection of an angle and the squaring of the circle, are impossible to perform using only a straightedge and compass. Finally, Chapter 14 gives an introduction to coding theory using polynomial and matrix techniques.

We do not give exhaustive treatments of any of the applications. We only go so far as to give the flavor without becoming too involved in technical complications. The interested reader may delve further into any topic by consulting the books in the bibliography.

It is important to realize that the study of these applications is not the only reason for learning modern algebra. These examples illustrate the varied uses to which algebra has been put in the past, and it is extremely likely that many more different applications will be found in the future.

One cannot understand mathematics without doing numerous examples. There are a total of over 600 exercises of varying difficulty, at the end of the chapters. Answers to the odd-numbered exercises are given at the back of the book.

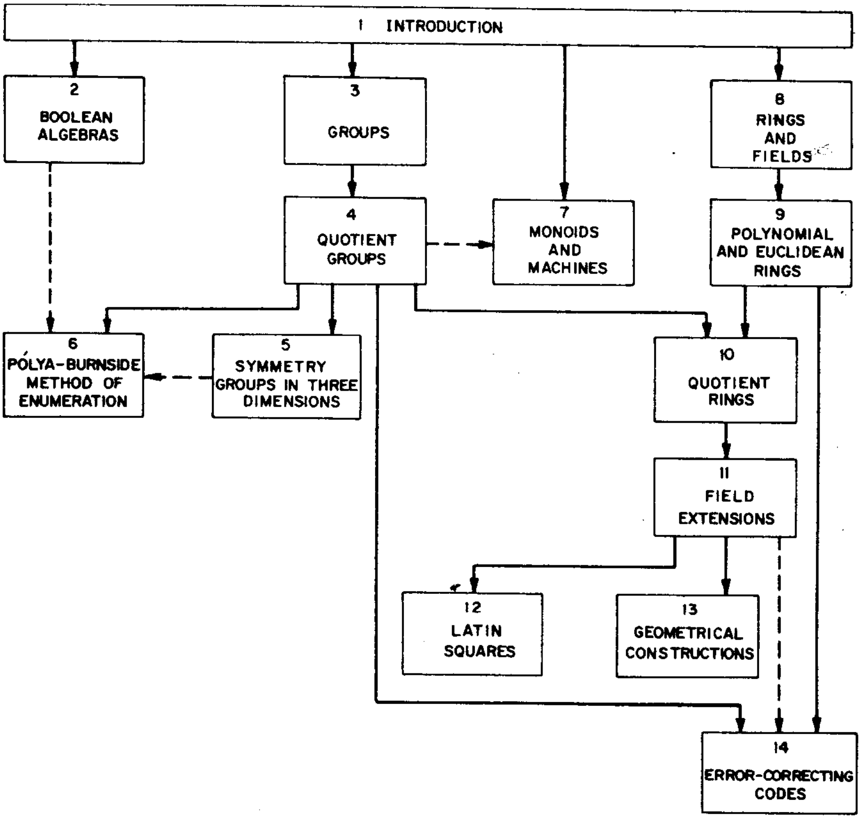

1 INTRODUCTION
2 BOOLEAN ALGEBRAS
3 GROUPS
8 RINGS AND FIELDS
4 QUOTIENT GROUPS
7 MONOIDS AND MACHINES
9 POLYNOMIAL AND EUCLIDEAN RINGS
6 PÓLYA-BURNSIDE METHOD OF ENUMERATION
5 SYMMETRY GROUPS IN THREE DIMENSIONS
10 QUOTIENT RINGS
11 FIELD EXTENSIONS
12 LATIN SQUARES
13 GEOMETRICAL CONSTRUCTIONS
14 ERROR-CORRECTING CODES

Figure 0.01. The prerequisite structure of the chapters.

Figure 0.01 illustrates the interdependence of the various chapters. A solid line indicates a necessary prerequisite for the whole chapter, and a dotted line indicates a prerequisite for one section of the chapter. Since the book contains more than sufficient material for a two-term course, various sections or chapters may be omitted. The choice of topics will depend on the interests of the students and the instructor. However, to preserve the essence of the book, the instructor should be careful not to devote most of the course to the theory, but should leave sufficient time for the applications to be appreciated.

I would like to thank all my students and colleagues at the University of Waterloo, especially Harry Davis, D. Ž. Djoković, Denis Higgs, and Keith Rowe, who offered helpful suggestions during the various stages of the manuscript. I am very grateful to Michael Boyle, Ian McGee, Juris Stepŕans, and Jack Weiner for their help in preparing and proofreading the preliminary versions and the final draft. Finally, I would like to thank Sue Cooper, Annemarie DeBrusk, Lois Graham, and Denise Stack for their excellent typing of the different drafts, and Nadia Bahar for tracing all the figures.

WILLIAM J. GILBERT

Waterloo, Ontario, Canada
April 1976

Contents

Those sections that constitute the core of a modern algebra course are indicated by the symbol†

Introduction 1

Algebra can be defined as the manipulation of symbols. Its history falls into two distinct parts, with the dividing date being approximately 1800. The algebra done before the nineteenth century is called "classical algebra," whereas most of that done later is called "modern algebra" or "abstract algebra."

Classical Algebra

The technique of introducing a symbol, such as x, to represent an unknown number in solving problems was known to the ancient Greeks. This symbol could be manipulated just like the arithmetic symbols until a solution was obtained. *Classical algebra* can be characterized by the fact that each symbol *always* stood for a number. This number could be integral, real, or complex. However, in the seventeenth and eighteenth centuries, mathematicians were not quite sure whether the square root of minus one was a number. It was not until the nineteenth century and the beginning of modern algebra that a satisfactory explanation of the complex numbers was given.

The main goal of classical algebra was to use algebraic manipulation to solve polynomial equations. Classical algebra succeeded in producing algorithms for solving all polynomial equations in one variable of degree less than or equal to four. It was shown by Niels Henrik Abel (1802–1829), by modern algebraic methods, that it was not always possible to solve a polynomial equation of degree five or higher in terms of nth roots. Classical algebra also developed methods for dealing with linear equations containing several variables, but little was known about the solution of nonlinear equations.

Classical algebra provided a powerful tool for tackling many scientific problems, and it is still extremely important for working out today's problems. Perhaps the mathematical tool most useful in science, engineering, and the social sciences is the method of solution of a system of linear equations together with all its allied linear algebra.

Modern Algebra

In the nineteenth century, it was gradually realized that mathematical symbols did not necessarily have to stand for numbers; in fact, it was not necessary that they stand for anything at all! From this realization emerged what is now known as *modern algebra* or *abstract algebra*.

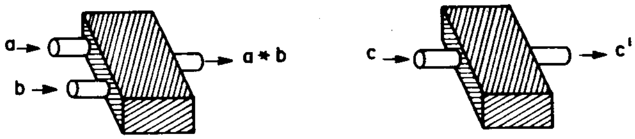
For example, the symbols could be interpreted as symmetries of an object, as the position of a switch, as an instruction to a machine, or as a way to design a statistical experiment. The symbols could be manipulated using some of the usual rules for numbers. For example, the polynomial $3x^2+2x-1$ could be added to and multiplied by other polynomials without ever having to interpret the symbol x as a number.

Modern algebra has two basic uses. Its first is to describe patterns or symmetries that occur in nature and in mathematics. For example, it can describe the different crystal formations in which certain chemical substances are found and can be used to show the similarity between the logic of switching circuits and the algebra of subsets of a set. The second basic use of modern algebra is to naturally extend the common number systems to other useful systems.

Binary Operations

The symbols that are to be manipulated are elements of some set, and the manipulation is done by performing certain operations on elements of that set. Examples of such operations are addition and multiplication on the set of real numbers.

As shown in Figure 1.01, we can visualize an operation as a "black box" with various inputs coming from a set S and one output, which combines the inputs in some specified way.



Binary operation

Unary operation

Figure 1.01

If the black box has two inputs, the operation combines *two* elements of the set to form a third. Such an operation is called a binary operation. If there is only one input, the operation is called unary. An example of a unary operation is finding the reciprocal of a nonzero real number.

A *binary operation*, $\star$, on a set S is really just a particular function from $S \times S$ to S. We denote the image of the pair (a,b) under this function by $a \star b$. In other words, the binary operation $\star$ assigns to any two elements a and b of S the element $a \star b$ of S. We often refer to an operation $\star$ as being *closed* to emphasize that each element $a \star b$ belongs to the set S and not to a possibly larger set. Many symbols are used for binary operations; the most common are $+$, $\cdot$, $-$, $\circ$, $\div$, $\cup$, $\cap$, $\wedge$ and $\vee$.

A *unary operation* on S is just a function from S to S. The image of c under a unary operation is usually denoted by a symbol such as c', $\bar{c}$, c^{-1} or $(-c)$.

Let $\mathbf{P} = \{1,2,3,\ldots\}$ be the set of positive integers. Addition and multiplication are both binary operations on $\mathbf{P}$, because, if $x,y \in \mathbf{P}$, then $x+y$ and $x \cdot y \in \mathbf{P}$. However, subtraction is *not* a binary operation on $\mathbf{P}$ because, for instance, $1-2 \notin \mathbf{P}$. Other natural binary operations on $\mathbf{P}$ are exponentiation and the greatest common divisor, since, for any two positive integers x and y, x^y and $\mathrm{GCD}(x,y)$ are well-defined elements of $\mathbf{P}$.

Let $\mathbf{R}$ be the set of all real numbers. Addition, multiplication, and subtraction are all binary operations on $\mathbf{R}$ because $x+y$, $x \cdot y$, and $x-y$ are real numbers for every pair of real numbers x and y. The symbol $-$ stands for a binary operation when used in an expression such as $x-y$, but it stands for the unary operation of taking the negative when used in the expression $-x$. Division is not a binary operation on $\mathbf{R}$ because division by zero is undefined. However, division is a binary operation on $\mathbf{R}-\{0\}$, the set of nonzero real numbers.

A binary operation on a finite set can often be conveniently presented by means of a *table*. For example, consider the set $T=\{a,b,c\}$, containing three elements. A binary operation $\star$ on T is defined by Table 1.1. In this table, $x\star y$ is the element in row x and column y. For example, $b\star c=b$ and $c\star b=a$.

Table 1.1. A binary operation on $\{a,b,c\}$

$\star$	a	b	c
a	b	a	a
b	c	a	b
c	c	a	b

One important binary operation is the composition of symmetries of a given figure or object. Consider a square lying in a plane. The set S of symmetries of this square is the set of mappings of the square to itself that preserve distances. Figure 1.02 illustrates the composition of two such symmetries to form a third symmetry.

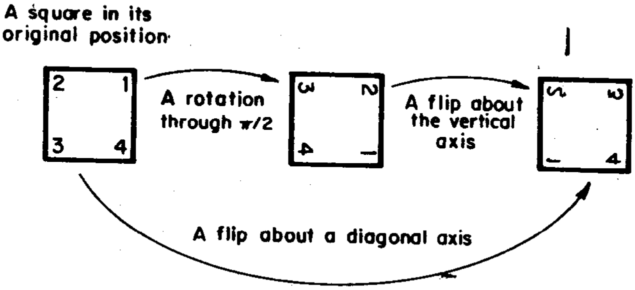

A square in its original position
2
1
3
4
A rotation through $\pi/2$
3
2
4
1
A flip about the vertical axis
2
3
1
4
A flip about a diagonal axis

Figure 1.02. Composition of symmetries of a square.

Most of the binary operations we use have one or more of the following special properties. Let $\star$ be a binary operation on a set S. This operation is called *associative* if $a\star(b\star c)=(a\star b)\star c$ for all $a,b,c\in S$. The operation $\star$ is called *commutative* if $a\star b=b\star a$ for all $a,b\in S$. The element $e\in S$ is said to be an *identity* for $\star$ if $a\star e=e\star a=a$ for all $a\in S$.

If $\star$ is a binary operation on S that has an identity e, then b is called the *inverse* of a with respect to $\star$ if $a\star b=b\star a=e$. We usually denote the inverse of a by a^{-1}; however, if the operation is addition, the inverse is denoted by $-a$.

If $\star$ and $\circ$ are two binary operations on S, then $\circ$ is said to be *distributive* over $\star$ if $a\circ(b\star c)=(a\circ b)\star(a\circ c)$ and $(b\star c)\circ a=(b\circ a)\star(c\circ a)$ for all $a,b,c\in S$.

Addition and multiplication are both associative and commutative operations on the set of real numbers, **R**. The identity for addition is 0, whereas the multiplicative identity is 1. Every real number, a, has an inverse under addition, namely, its negative, $-a$. Every nonzero real number a has a multiplicative inverse, a^{-1}. Furthermore, multiplication is distributive over addition because $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ and $(b+c)\cdot a=(b\cdot a)+(c\cdot a)$; however, addition is not distributive over multiplication because $a+(b\cdot c)\neq(a+b)\cdot(a+c)$ in general.

Denote the set of $n\times n$ real matrices by $\mathcal{M}(n\times n;\mathbf{R})$. Matrix multiplication is an associative operation on $\mathcal{M}(n\times n;\mathbf{R})$ but it is not commutative (unless $n=1$). The matrix I, whose (i,j)th entry is 1 if $i=j$ and 0 otherwise, is the multiplicative identity. Matrices that have inverses under multiplication are called *nonsingular*.

Algebraic Structures

A set, together with one or more operations on the set, is called an *algebraic structure*. The set is called the *underlying set* of the structure. Modern algebra is the study of these structures; in later chapters, we examine various types of algebraic structures. For example, a field is an algebraic structure consisting of a set **F** together with two binary operations, usually denoted by + and $\cdot$, that satisfy certain conditions. We denote such a structure by $(\mathbf{F},+,\cdot)$.

In order to understand a particular structure, we usually begin by examining its *substructures*. The underlying set of a substructure is a subset of the underlying set of the structure, and the operations in both structures are the same. For example, the set of complex numbers, **C**, contains the set of real numbers, **R**, as a subset . The operations of addition and multiplication on **C** restrict to the same operations on **R**, and therefore $(\mathbf{R},+,\cdot)$ is a substructure of $(\mathbf{C},+,\cdot)$.

Two algebraic structures of a particular type may be compared by means of structure-preserving functions called morphisms. This concept of morphism is one of the fundamental notions of modern algebra. We encounter it among every algebraic structure we consider.

More precisely, let $(S,\star)$ and $(T,\circ)$ be two algebraic structures consisting of the sets S and T, together with the binary operations $\star$ on S and $\circ$ on T. Then a function $f\colon S\to T$ is said to be a *morphism* from $(S,\star)$ to $(T,\circ)$ if, for every $x,y\in S$,

$$f(x\star y)=f(x)\circ f(y).$$

If the structures contain more than one operation, the morphism must preserve all these operations. Furthermore, if the structures have identities, these must be preserved too.

As an example of a morphism, consider the set of all integers, $\mathbf{Z}$, under the operation of addition and the set of positive real numbers, $\mathbf{R}_{>0}$, under multiplication. The function $f:\mathbf{Z}\rightarrow\mathbf{R}_{>0}$ defined by $f(x)=e^x$ is a morphism from $(\mathbf{Z},+)$ to $(\mathbf{R}_{>0},\cdot)$. Multiplication of the exponentials e^x and e^y corresponds to addition of their exponents x and y.

A vector space is an algebraic structure whose underlying set is a set of vectors. Its operations consist of the binary operation of addition and, for each scalar λ, a unary operation of multiplication by λ. A function $f:S\rightarrow T$, between vector spaces, is a morphism if $f(\mathbf{x}+\mathbf{y})=f(\mathbf{x})+f(\mathbf{y})$ and $f(\lambda\mathbf{x})=\lambda f(\mathbf{x})$ for all vectors $\mathbf{x}$ and $\mathbf{y}$ in the domain S and all scalars λ. Such a vector space morphism is usually called a *linear transformation*.

A morphism preserves some, but not necessarily all, of the properties of the domain structure. However, if a morphism between two structures is a bijective function (that is, one-to-one and onto), it is called an *isomorphism*, and the structures are called *isomorphic*. Isomorphic structures have identical properties, and they are indistinguishable from an algebraic point of view. For example, two vector spaces of the same finite dimension over a field $\mathbf{F}$ are isomorphic.

One important method of constructing new algebraic structures from old ones is by means of equivalence relations. If $(S,\star)$ is a structure consisting of the set S with the binary operation $\star$ on it, the equivalence relation $\sim$ on S is said to be compatible with $\star$ if, whenever $a\sim b$ and $c\sim d$, it follows that $a\star c\sim b\star d$. Such a compatible equivalence relation allows us to construct a new structure called the *quotient structure*, whose underlying set is the set of equivalence classes. For example, the quotient structure of the integers, $(\mathbf{Z},+,\cdot)$, under the congruence relation modulo n, is the set of integers modulo n, $(\mathbf{Z}_n,+,\cdot)$.

Extending Number Systems

In the words of Leopold Kronecker (1823–1891), "God created the natural numbers; everything else was man's handiwork." Starting with the set of natural numbers under addition and multiplication, we show how this can be extended to other algebraic systems that satisfy properties not held by the natural numbers. The integers $(\mathbf{Z},+,\cdot)$ is the smallest system containing the natural numbers, in which addition has an identity (the zero) and every element has an inverse under addition (its negative). The integers have an identity under multiplication (the element 1), but 1 and -1 are the