MODERN ALGEBRA WITH APPLICATIONS

Second Edition

WILLIAM J. GILBERT
University of Waterloo
Department of Pure Mathematics
Waterloo, Ontario, Canada

W. KEITH NICHOLSON
University of Calgary
Department of Mathematics and Statistics
Calgary, Alberta, Canada

A JOHN WILEY & SONS, INC., PUBLICATION

MODERN ALGEBRA
WITH APPLICATIONS

PURE AND APPLIED MATHEMATICS

A Wiley-Interscience Series of Texts, Monograph, and Tracts

Founded by RICHARD COURANT
Editors: MYRON B. ALLEN III, DAVID A. COX, PETER LAX
Editors Emeriti: PETER HILTON, HARRY HOCHSTADT, JOHN TOLAND

A complete list of the titles in this series appears at the end of this volume.

MODERN ALGEBRA WITH APPLICATIONS

Second Edition

WILLIAM J. GILBERT
University of Waterloo
Department of Pure Mathematics
Waterloo, Ontario, Canada

W. KEITH NICHOLSON
University of Calgary
Department of Mathematics and Statistics
Calgary, Alberta, Canada

A JOHN WILEY & SONS, INC., PUBLICATION

Cover: Still image from the applet KaleidoHedron, Copyright © 2000 by Greg Egan, from his website http://www.netspace.net.au/∼gregegan/. The pattern has the symmetry of the icosahedral group.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Gilbert, William J., 1941–
Modern algebra with applications / William J. Gilbert, W. Keith Nicholson.—2nd ed.
p. cm.—(Pure and applied mathematics)
Includes bibliographical references and index.
ISBN 0-471-41451-4 (cloth)
1. Algebra, Abstract. I. Nicholson, W. Keith. II. Title. III. Pure and applied mathematics (John Wiley & Sons : Unnumbered)

QA162.G53 2003
512—dc21

2003049734

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE TO THE FIRST EDITION

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.

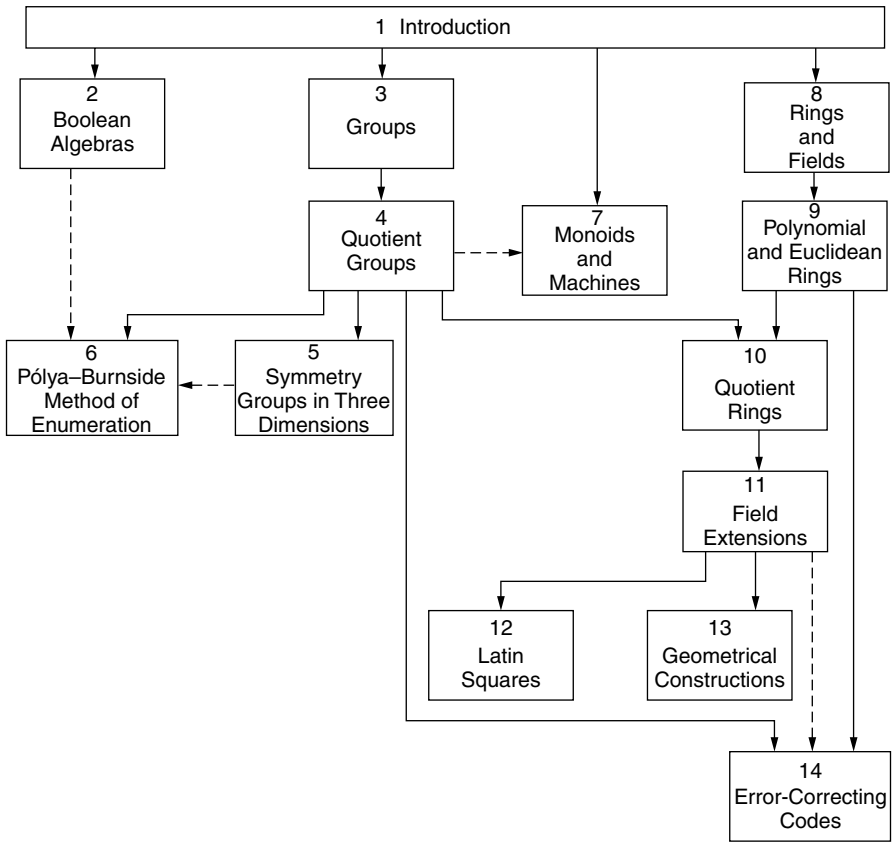


Figure P.1. Structure of the chapters.

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 ends of chapters. Answers to the odd-numbered exercises are given at the back of the book.

Figure P.1 illustrates the interdependence of the chapters. A solid line indicates a necessary prerequisite for the whole chapter, and a dashed 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.

Waterloo, Ontario, Canada WILLIAM J. GILBERT
April 1976

PREFACE TO THE SECOND EDITION

In addition to improvements in exposition, the second edition contains the following new items:

- New shorter proof of the parity theorem using the action of the symmetric group on the discriminant polynomial
- New proof that linear isometries are linear, and more detail about their relation to orthogonal matrices
- Appendix on methods of proof for beginning students, including the definition of an implication, proof by contradiction, converses, and logical equivalence
- Appendix on basic number theory covering induction, greatest common divisors, least common multiples, and the prime factorization theorem
- New material on the order of an element and cyclic groups
- More detail about the lattice of divisors of an integer
- New historical notes on Fermat's last theorem, the classification theorem for finite simple groups, finite affine planes, and more
- More detail on set theory and composition of functions
- 26 new exercises, 46 counting parts
- Updated symbols and notation
- Updated bibliography

February 2003

WILLIAM J. GILBERT
W. KEITH NICHOLSON

LIST OF SYMBOLS

$\mathbb{A}$	Algebraic numbers, 233
A_n	Alternating group on n elements, 70
$\mathbb{C}$	Complex numbers, 4
$\mathbb{C}^*$	Nonzero complex numbers, 48
C_n	Cyclic group of order n, 58
$C[0, \infty)$	Continuous real valued functions on $[0, \infty)$, 173
D_n	Dihedral group of order $2n$, 58
$\mathbb{D}_n$	Divisors of n, 22
$d(u, v)$	Hamming distance between u and v, 269
deg	Degree of a polynomial, 166
e	Identity element of a group or monoid, 48, 137
e_G	Identity element in the group G, 61
$\mathrm{E}(n)$	Euclidean group in n dimensions, 104
F	Field, 4, 160
$\mathcal{F}_n$	Switching functions of n variables, 28
$\mathrm{Fix}g$	Set of elements fixed under the action of g, 125
$\mathrm{FM}(A)$	Free monoid on A, 140
$\gcd(a, b)$	Greatest common divisor of a and b, 184, 299
$\mathrm{GF}(n)$	Galois field of order n, 227
$\mathrm{GL}(n, F)$	General linear group of dimension n over F, 107
$\mathbb{H}$	Quaternions, 177
I	Identity matrix, 4
I_k	$k \times k$ identity matrix, 277
$\mathrm{Im}\, f$	Image of f, 87
$\mathrm{Ker}\, f$	Kernel of f, 86
$\mathrm{lcm}(a, b)$	Least common multiple of a and b, 184, 303
$\mathcal{L}(\mathbb{R}^n, \mathbb{R}^n)$	Linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^n$, 163
$M_n(R)$	$n \times n$ matrices with entries from R, 4, 166
$\mathbb{N}$	Nonnegative integers, 55
NAND	NOT-AND, 28, 36
NOR	NOT-OR, 28, 36
$\mathrm{O}(n)$	Orthogonal group of dimension n, 105
$\mathrm{Orb}\, x$	Orbit of x, 97

$\mathbb{P}$	Positive integers, 3
$\mathcal{P}(X)$	Power set of X, 8
$\mathbb{Q}$	Rational numbers, 6
$\mathbb{Q}^*$	Nonzero rational numbers, 48
Q	Quaternion group, 73
$\mathbb{R}$	Real numbers, 2
$\mathbb{R}^*$	Nonzero real numbers, 48
$\mathbb{R}^+$	Positive real numbers, 5
$S(X)$	Symmetric group of X, 50
S_n	Symmetric group on n elements, 63
$\mathrm{SO}(n)$	Special orthogonal group of dimension n, 108
Stab x	Stabilizer of x, 97
$\mathrm{SU}(n)$	Special unitary group of dimension n, 108
$\mathrm{T}(n)$	Translations in n dimensions, 104
$\mathrm{U}(n)$	Unitary group of dimension n, 108
$\mathbb{Z}$	Integers, 5
$\mathbb{Z}_n$	Integers modulo n, 5, 78
$\mathbb{Z}_n^*$	Integers modulo n coprime to n, 102
$\delta(x)$	Dirac delta function, or remainder in general division algorithm, 172, 181
Λ	Null sequence, 140
$\emptyset$	Empty set, 7
$\phi(n)$	Euler ϕ-function, 102
$\star$	General binary operation *or* concatenation, 2, 140
$*$	Convolution, 168, 173
$\circ$	Composition, 49
Δ	Symmetric difference, 9, 29
$-$	Difference, 9
$\wedge$	Meet, 14
$\vee$	Join, 14
$\subseteq$	Inclusion, 7
$\leqslant$	Less than or equal, 23
$\Rightarrow$	Implies, 17, 293
$\Leftrightarrow$	If and only if, 18, 295
$\cong$	Isomorphic, 60, 172
$\equiv \bmod n$	Congruent modulo n, 77
$\equiv \bmod H$	Congruent modulo H, 79
$\lvert X\rvert$	Number of elements in X, 12, 56
$\lvert G : H\rvert$	Index of H in G, 80
R^*	Invertible elements in the ring R, 188
a'	Complement of a in a boolean algebra, 14, 28
a^{-1}	Inverse of a, 3, 48
$\overline{A}$	Complement of the set A, 8
$\cap$	Intersection of sets, 8
$\cup$	Union of sets, 8

$\in$	Membership in a set, 7
$A-B$	Set difference, 9
$\|\mathbf{v}\|$	Length of $\mathbf{v}$ in $\mathbb{R}^n$, 105
$\mathbf{v} \cdot \mathbf{w}$	Inner product in $\mathbb{R}^n$, 105
V^T	Transpose of the matrix V, 104
$\square$	End of a proof or example, 9
(a)	Ideal generated by a, 204
$(a_1 a_2 \dots a_n)$	n-cycle, 64
$\begin{pmatrix} 1\ 2 \dots n \\ a_1 a_2 \dots a_n \end{pmatrix}$	Permutation, 63
$\binom{n}{r}$	Binomial coefficient $n!/r!(n-r)!$, 129
$F(a)$	Smallest field containing F and a, 220
$F(a_1, \dots, a_n)$	Smallest field containing F and $a_1, \dots, a_n$, 220
(n, k)-code	Code of length n with messages of length k, 266
$(X, \star)$	Group or monoid, 5, 48, 137
$(R, +, \cdot)$	Ring, 156
$(K, \wedge, \vee, ')$	Boolean algebra, 14
$[x]$	Equivalence class containing x, 77
$[x]_n$	Congruence class modulo n containing x, 100
$R[x]$	Polynomials in x with coefficients from R, 167
$R[[x]]$	Formal power series in x with coefficients from R, 169
$R[x_1, \dots, x_n]$	Polynomials in $x_1, \dots, x_n$ with coefficients from R, 168
$[K : F]$	Degree of K over F, 219
X^Y	Set of functions from Y to X, 138
$R^{\mathbb{N}}$	Sequences of elements from R, 168
$\langle a_i \rangle$	Sequence whose ith term is a_i, 168
$G \times H$	Direct product of G and H, 91
$S \times S$	Direct product of sets, 2
S/E	Quotient set, 77
G/H	Quotient group or set of right cosets, 83
R/I	Quotient ring, 206
$a\|b$	a divides b, 21, 184, 299
$l//m$	l is parallel to m, 242
Ha	Right coset of H containing a, 79
aH	Left coset of H containing a, 82
$I + r$	Coset of I containing r, 205

1

INTRODUCTION

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 -1 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 at most four. However, 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 today. Perhaps the most useful mathematical tool 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 with Applications, *Second Edition*, by William J. Gilbert and W. Keith Nicholson
ISBN 0-471-41451-4

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. The 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 extend the common number systems naturally 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 1.1, 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. 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.

If S is a set, the **direct product** $S \times S$ consists of all ordered pairs (a, b) with $a, b \in S$. Here the term *ordered* means that $(a, b) = (a_1, b_1)$ if and only if $a = a_1$ and $b = b_1$. For example, if we denote the set of all real numbers by $\mathbb{R}$, then $\mathbb{R} \times \mathbb{R}$ is the euclidean plane.

Using this terminology, 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)

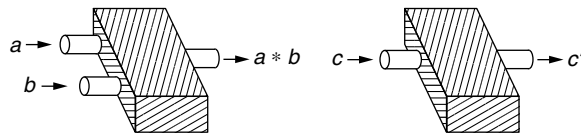


Figure 1.1

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', $\overline{c}$, c^{-1}, or $(-c)$.

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

Addition, multiplication, and subtraction are all binary operations on $\mathbb{R}$ 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 $\mathbb{R}$ because division by zero is undefined. However, division is a binary operation on $\mathbb{R} - \{0\}$, the set of nonzero real numbers.

A binary operation on a finite set can often be presented conveniently 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 $c \star b = a$.

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 1.2 illustrates the composition of two such symmetries to form a third symmetry.

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

TABLE 1.1. Binary Operation on $\{a, b, c\}$

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

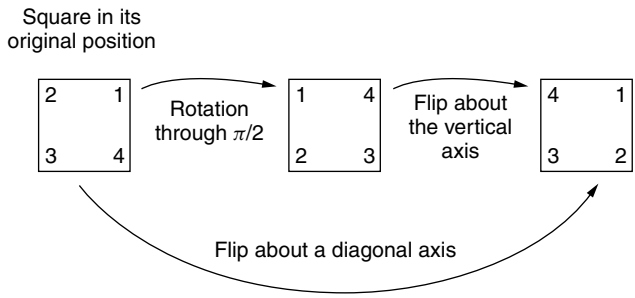


Figure 1.2. Composition of symmetries of a square.

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 $\mathbb{R}$ of real numbers. 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 $M_n(\mathbb{R})$. Matrix multiplication is an associative operation on $M_n(\mathbb{R})$, 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 with multiplicative inverses 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 $(F, +, \cdot)$.

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, $\mathbb{C}$, contains the set of real numbers, $\mathbb{R}$, as a subset. The operations of addition and multiplication on $\mathbb{C}$ restrict to the same operations on $\mathbb{R}$, and therefore $(\mathbb{R}, +, \cdot)$ is a substructure of $(\mathbb{C}, +, \cdot)$.

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 $f: S \to T$ 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, $\mathbb{Z}$, under the operation of addition and the set of positive real numbers, $\mathbb{R}^+$, under multiplication. The function $f: \mathbb{Z} \to \mathbb{R}^+$ defined by $f(x) = e^x$ is a morphism from $(\mathbb{Z}, +)$ to $(\mathbb{R}^+, \cdot)$. 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 $f: S \to T$, 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 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, $(\mathbb{Z}, +, \cdot)$, under the congruence relation modulo n, is the set of integers modulo n, $(\mathbb{Z}_n, +, \cdot)$ (see Appendix 2).

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 $(\mathbb{Z}, +, \cdot)$ 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 only elements with multiplicative inverses. A standard construction will produce the field of fractions of the integers, which is the rational number system $(\mathbb{Q}, +, \cdot)$, and we show that this is the smallest field containing $(\mathbb{Z}, +, \cdot)$. We can now divide by nonzero elements in $\mathbb{Q}$ and solve every linear equation of the form $ax = b$ $(a \neq 0)$. However, not all quadratic equations have solutions in $\mathbb{Q}$; for example, $x^2 - 2 = 0$ has no rational solution.

The next step is to extend the rationals to the real number system $(\mathbb{R}, +, \cdot)$. The construction of the real numbers requires the use of nonalgebraic concepts such as Dedekind cuts or Cauchy sequences, and we will not pursue this, being content to assume that they have been constructed. Even though many polynomial equations have real solutions, there are some, such as $x^2 + 1 = 0$, that do not. We show how to extend the real number system by adjoining a root of $x^2 + 1$ to obtain the complex number system $(\mathbb{C}, +, \cdot)$. The complex number system is really the end of the line, because Carl Friedrich Gauss (1777–1855), in his doctoral thesis, proved that any nonconstant polynomial with real or complex coefficients has a root in the complex numbers. This result is now known as the *fundamental theorem of algebra*.

However, the classical number system can be generalized in a different way. We can look for fields that are not subfields of $(\mathbb{C}, +, \cdot)$. An example of such a field is the system of integers modulo a prime p, $(\mathbb{Z}_p, +, \cdot)$. All the usual operations of addition, subtraction, multiplication, and division by nonzero elements can be performed in $\mathbb{Z}_p$. We show that these fields can be extended and that for each prime p and positive integer n, there is a field $(GF(p^n), +, \cdot)$ with p^n elements. These finite fields are called **Galois fields** after the French mathematician Évariste Galois. We use Galois fields in the construction of orthogonal latin squares and in coding theory.

2

BOOLEAN ALGEBRAS

A boolean algebra is a good example of a type of algebraic structure in which the symbols usually represent nonnumerical objects. This algebra is modeled after the algebra of subsets of a set under the binary operations of union and intersection and the unary operation of complementation. However, boolean algebra has important applications to switching circuits, where each symbol represents a particular electrical circuit or switch. The origin of boolean algebra dates back to 1847, when the English mathematician George Boole (1815–1864) published a slim volume entitled *The Mathematical Analysis of Logic*, which showed how algebraic symbols could be applied to logic. The manipulation of logical propositions by means of boolean algebra is now called the *propositional calculus*.

At the end of this chapter, we show that any finite boolean algebra is equivalent to the algebra of subsets of a set; in other words, there is a boolean algebra isomorphism between the two algebras.

ALGEBRA OF SETS

In this section, we develop some properties of the basic operations on sets. A set is often referred to informally as a collection of objects called the elements of the set. This is not a proper definition—*collection* is just another word for *set*. What is clear is that there are **sets**, and there is a notion of being an **element** (or member) of a set. These fundamental ideas are the primitive concepts of set theory and are left undefined.* The fact that a is an element of a set X is denoted $a \in X$. If every element of X is also an element of Y, we write $X \subseteq Y$ (equivalently, $Y \supseteq X$) and say that X is *contained* in Y, or that X is a **subset** of Y. If X and Y have the same elements, we say that X and Y are **equal sets** and write $X = Y$. Hence $X = Y$ if and only if both $X \subseteq Y$ and $Y \subseteq X$. The set with no elements is called the **empty set** and is denoted as $\emptyset$.

* Certain basic properties of sets must also be assumed (called the *axioms* of the theory), but it is not our intention to go into this here.

Modern Algebra with Applications, *Second Edition*, by William J. Gilbert and W. Keith Nicholson
ISBN 0-471-41451-4

Let X be any set. The set of all subsets of X is called the **power set** of X and is denoted by $\mathcal{P}(X)$. Hence $\mathcal{P}(X) = \{A | A \subseteq X\}$. Thus if $X = \{a, b\}$, then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, X\}$. If $X = \{1, 2, 3\}$, then $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}$.

If A and B are subsets of a set X, their **intersection** $A \cap B$ is defined to be the set of elements common to A and B, and their **union** $A \cup B$ is the set of elements in A or B (or both). More formally,

$$A \cap B = \{x | x \in A \text{ and } x \in B\} \quad \text{and} \quad A \cup B = \{x | x \in A \text{ or } x \in B\}.$$

The **complement** of A in X is $\overline{A} = \{x | x \in X \text{ and } x \notin A\}$ and is the set of elements in X that are not in A. The shaded areas of the **Venn diagrams** in Figure 2.1 illustrate these operations.

Union and intersection are both **binary operations** on the power set $\mathcal{P}(X)$, whereas complementation is a **unary operation** on $\mathcal{P}(X)$. For example, with $X = \{a, b\}$, the tables for the structures $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), {}^-)$ are given in Table 2.1, where we write A for $\{a\}$ and B for $\{b\}$.

Proposition 2.1. The following are some of the more important relations involving the operations $\cap$, $\cup$, and $^-$, holding for all $A, B, C \in \mathcal{P}(X)$.

(i) $A \cap (B \cap C) = (A \cap B) \cap C$.
(ii) $A \cup (B \cup C) = (A \cup B) \cup C$.
(iii) $A \cap B = B \cap A$.
(iv) $A \cup B = B \cup A$.
(v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(vi) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(vii) $A \cap X = A$.
(viii) $A \cup \emptyset = A$.
(ix) $A \cap \overline{A} = \emptyset$.
(x) $A \cup \overline{A} = X$.
(xi) $A \cap \emptyset = \emptyset$.
(xii) $A \cup X = X$.
(xiii) $A \cap (A \cup B) = A$.
(xiv) $A \cup (A \cap B) = A$.

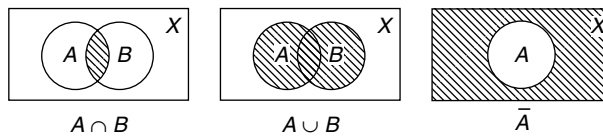


Figure 2.1. Venn diagrams.

TABLE 2.1. Intersection, Union, and Complements in $\mathcal{P}(\{a, b\})$

$\cap$	$\emptyset$	A	B	X
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
A	$\emptyset$	A	$\emptyset$	A
B	$\emptyset$	$\emptyset$	B	B
X	$\emptyset$	A	B	X

$\cup$	$\emptyset$	A	B	X
$\emptyset$	$\emptyset$	A	B	X
A	A	A	X	X
B	B	X	B	X
X	X	X	X	X

Subset	Complement
$\emptyset$	X
A	B
B	A
X	$\emptyset$

(xv) $A \cap A = A$.
(xvi) $A \cup A = A$.
(xvii) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
(xviii) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.
(xix) $\overline{X} = \emptyset$.
(xx) $\overline{\emptyset} = X$.
(xxi) $\overline{\overline{A}} = A$.

Proof. We shall prove relations (v) and (x) and leave the proofs of the others to the reader.

$$\begin{aligned}
\text{(v)}\quad A \cap (B \cup C) &= \{x | x \in A \text{ and } x \in B \cup C\} \\
&= \{x | x \in A \text{ and } (x \in B \text{ or } x \in C)\} \\
&= \{x | (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\} \\
&= \{x | x \in A \cap B \text{ or } x \in A \cap C\} \\
&= (A \cap B) \cup (A \cap C).
\end{aligned}$$

The Venn diagrams in Figure 2.2 illustrate this result.

$$\begin{aligned}
\text{(x)}\quad A \cup \overline{A} &= \{x | x \in A \text{ or } x \in \overline{A}\} \\
&= \{x | x \in A \text{ or } (x \in X \text{ and } x \notin A)\} \\
&= \{x | (x \in X \text{ and } x \in A) \text{ or } (x \in X \text{ and } x \notin A)\}, \text{ since } A \subseteq X \\
&= \{x | x \in X \text{ and } (x \in A \text{ or } x \notin A)\} \\
&= \{x | x \in X\}, \text{ since it is always true that } x \in A \text{ or } x \notin A \\
&= X. \qquad \square
\end{aligned}$$

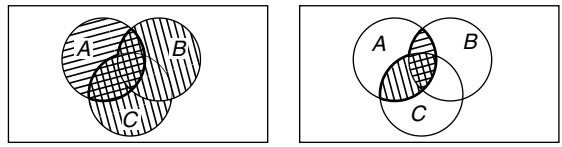
Relations (i)–(iv), (vii), and (viii) show that $\cap$ and $\cup$ are associative and commutative operations on $\mathcal{P}(X)$ with identities X and $\emptyset$, respectively. The only element with an inverse under $\cap$ is its identity X, and the only element with an inverse under $\cup$ is its identity $\emptyset$.

Note the duality between $\cap$ and $\cup$. If these operations are interchanged in any relation, the resulting relation is also true.

Another operation on $\mathcal{P}(X)$ is the **difference** of two subsets. It is defined by

$$A - B = \{x | x \in A \text{ and } x \notin B\} = A \cap \overline{B}.$$

Since this operation is neither associative nor commutative, we introduce another operation $A \Delta B$, called the **symmetric difference**, illustrated in Figure 2.3,



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

Figure 2.2. Venn diagrams illustrating a distributive law.

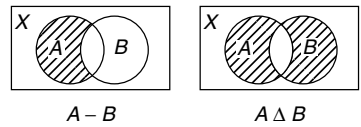


Figure 2.3. Difference and symmetric difference of sets.

defined by

$$A\Delta B = (A \cap \overline{B}) \cup (\overline{A} \cap B) = (A \cup B) - (A \cap B) = (A - B) \cup (B - A).$$

The symmetric difference of A and B is the set of elements in A or B, but not in both. This is often referred to as the **exclusive OR function** of A and B.

Example 2.2. Write down the table for the structure $(\mathcal{P}(X), \Delta)$ when $X = \{a, b\}$.

Solution. The table is given in Table 2.2, where we write A for $\{a\}$ and B for $\{b\}$. □

Proposition 2.3. The operation Δ is associative and commutative on $\mathcal{P}(X)$; it has an identity $\emptyset$, and each element is its own inverse. That is, the following relations hold for all $A, B, C \in \mathcal{P}(X)$:

(i) $A\Delta(B\Delta C) = (A\Delta B)\Delta C$. (ii) $A\Delta B = B\Delta A$.
(iii) $A\Delta\emptyset = A$. (iv) $A\Delta A = \emptyset$.

Three further properties of the symmetric difference are:

(v) $A\Delta X = \overline{A}$. (vi) $A\Delta\overline{A} = X$.
(vii) $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Proof. (ii) follows because the definition of $A\Delta B$ is symmetric in A and B. To prove (i) observe first that Proposition 2.1 gives

$$\begin{aligned}\overline{B\Delta C} &= \overline{(B \cap \overline{C}) \cup (\overline{B} \cap C)} = (\overline{B} \cup C) \cap (B \cup \overline{C}) \\ &= (\overline{B} \cap B) \cup (\overline{B} \cap \overline{C}) \cup (C \cap B) \cup (C \cap \overline{C}) \\ &= (B \cap C) \cup (\overline{B} \cap \overline{C}).\end{aligned}$$

TABLE 2.2. Symmetric Difference in $\mathcal{P}(\{a, b\})$

Δ	$\emptyset$	A	B	X
$\emptyset$	$\emptyset$	A	B	X
A	A	$\emptyset$	X	B
B	B	X	$\emptyset$	A
X	X	B	A	$\emptyset$