WILEY

Pure and Applied Mathematics: A Wiley-Interscience Series of Texts, Monographs, and Tracts

Modern Algebra with Applications

SECOND EDITION

WILLIAM J. GILBERT

W. KEITH NICHOLSON

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

WILEY-INTERSCIENCE
A JOHN WILEY & SONS, INC., PUBLICATION

PURE AND APPLIED MATHEMATICS

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

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

MODERN ALGEBRA WITH APPLICATIONS

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.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic format.

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

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.

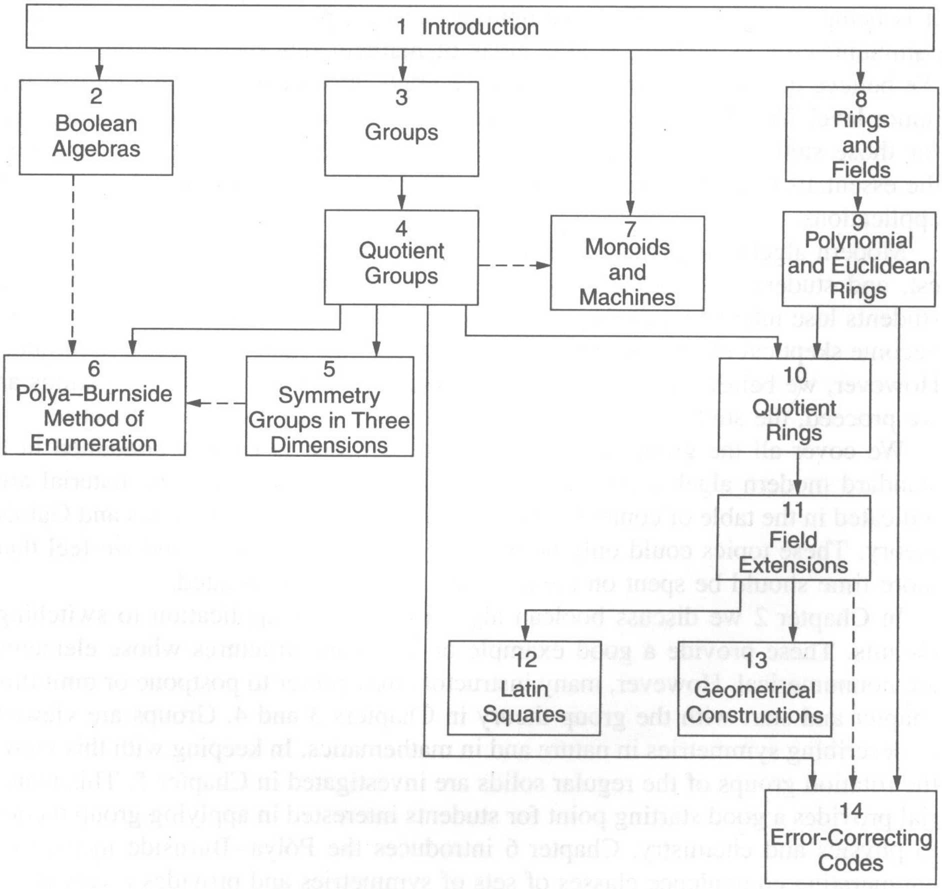
1 Introduction
2 Boolean Algebras
3 Groups
4 Quotient Groups
5 Symmetry Groups in Three Dimensions
6 Pólya–Burnside Method of Enumeration
7 Monoids and Machines
8 Rings and Fields
9 Polynomial and Euclidean Rings
10 Quotient Rings
11 Field Extensions
12 Latin Squares
13 Geometrical Constructions
14 Error-Correcting Codes

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
April 1976

WILLIAM J. GILBERT

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
$\mathscr{P}(X)$	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
$\Vert\mathbf{v}\Vert$	Length of **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
□	End of a proof or example, 9
(a)	Ideal generated by a, 204
$(a_1a_2\ldots a_n)$	n-cycle, 64
$\begin{pmatrix}1\,2\ldots n\\ a_1a_2\ldots a_n\end{pmatrix}$	Permutation, 63
$\binom{n}{r}$	Binomial coefficient $n!/r!(n-r)!$, 129
$F(a)$	Smallest field containing F and a, 220
$F(a_1,\ldots,a_n)$	Smallest field containing F and $a_1,\ldots,a_n$, 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
$R[x_1,\ldots,x_n]$	Polynomials in $x_1,\ldots,x_n$ 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
$a\vert b$	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

CONTENTS

Preface to the First Edition ix

Preface to the Second Edition xiii

List of Symbols xv

1 Introduction 1

Classical Algebra, 1
Modern Algebra, 2
Binary Operations, 2
Algebraic Structures, 4
Extending Number Systems, 5

2 Boolean Algebras 7

Algebra of Sets, 7
Number of Elements in a Set, 11
Boolean Algebras, 13
Propositional Logic, 16
Switching Circuits, 19
Divisors, 21
Posets and Lattices, 23
Normal Forms and Simplification of Circuits, 26
Transistor Gates, 36
Representation Theorem, 39
Exercises, 41

3 Groups 47

Groups and Symmetries, 48
Subgroups, 54

Cyclic Groups and Dihedral Groups, 56
Morphisms, 60
Permutation Groups, 63
Even and Odd Permutations, 67
Cayley's Representation Theorem, 71
Exercises, 71

4 Quotient Groups 76

Equivalence Relations, 76
Cosets and Lagrange's Theorem, 78
Normal Subgroups and Quotient Groups, 82
Morphism Theorem, 86
Direct Products, 91
Groups of Low Order, 94
Action of a Group on a Set, 96
Exercises, 99

5 Symmetry Groups in Three Dimensions 104

Translations and the Euclidean Group, 104
Matrix Groups, 107
Finite Groups in Two Dimensions, 109
Proper Rotations of Regular Solids, 111
Finite Rotation Groups in Three Dimensions, 116
Crystallographic Groups, 120
Exercises, 121

6 Pólya–Burnside Method of Enumeration 124

Burnside's Theorem, 124
Necklace Problems, 126
Coloring Polyhedra, 128
Counting Switching Circuits, 130
Exercises, 134

7 Monoids and Machines 137

Monoids and Semigroups, 137
Finite-State Machines, 142
Quotient Monoids and the Monoid of a Machine, 144
Exercises, 149

8 Rings and Fields 155

Rings, 155
Integral Domains and Fields, 159
Subrings and Morphisms of Rings, 161

New Rings from Old, 164
Field of Fractions, 170
Convolution Fractions, 172
Exercises, 176

9 Polynomial and Euclidean Rings **180**

Euclidean Rings, 180
Euclidean Algorithm, 184
Unique Factorization, 187
Factoring Real and Complex Polynomials, 190
Factoring Rational and Integral Polynomials, 192
Factoring Polynomials over Finite Fields, 195
Linear Congruences and the Chinese Remainder Theorem, 197
Exercises, 201

10 Quotient Rings **204**

Ideals and Quotient Rings, 204
Computations in Quotient Rings, 207
Morphism Theorem, 209
Quotient Polynomial Rings That Are Fields, 210
Exercises, 214

11 Field Extensions **218**

Field Extensions, 218
Algebraic Numbers, 221
Galois Fields, 225
Primitive Elements, 228
Exercises, 232

12 Latin Squares **236**

Latin Squares, 236
Orthogonal Latin Squares, 238
Finite Geometries, 242
Magic Squares, 245
Exercises, 249

13 Geometrical Constructions **251**

Constructible Numbers, 251
Duplicating a Cube, 256
Trisecting an Angle, 257
Squaring the Circle, 259
Constructing Regular Polygons, 259

Nonconstructible Number of Degree 4, 260
Exercises, 262

14 Error-Correcting Codes 264

The Coding Problem, 266
Simple Codes, 267
Polynomial Representation, 270
Matrix Representation, 276
Error Correcting and Decoding, 280
BCH Codes, 284
Exercises, 288

Appendix 1: Proofs 293

Appendix 2: Integers 296

Bibliography and References 306

Answers to Odd-Numbered Exercises 309

Index 323

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