Introduction to

Abstract Algebra

W. Keith Nicholson

Introduction to Abstract Algebra

W. Keith Nicholson
University of Calgary

PWS Publishing Company ■ Boston

PWS
Publishing Company

20 Park Plaza
Boston, Massachusetts 02116

Permission has been granted for images of mathematicians by The Historical Picture Service for de Fermat, Cayley, Noether, Kronecker, and Galois; by The Smithsonian Institution for Lagrange (#4683U-N), Gauss (#4683U-M), Abel (#60277-P), and Cauchy (#55574); by The University of Oslo for Sylow; and by The Seeley G. Mudd Manuscript Library at Princeton University for Wedderburn.

Library of Congress Cataloging-in-Publication data
Nicholson, W. Keith
Introduction to abstract algebra/W. Keith Nicholson
p. cm.
Includes bibliography and index.
ISBN 0-534-93189-8
1. Algebra. I. Title.
QA1542.2H35 1993 92-23168 CIP
512.9—dc20

This book is printed on recycled, acid-free paper.

Printed in the United States of America
93 94 95 96 97—10 9 8 7 6 5 4 3 2

Acquisitions Editor: Steve Quigley
Editorial Assistant: Christian Gal
Production Editor: S. London
Manufacturing Coordinator: Ellen Glisker
Interior Designer: S. London
Cover Designer: Eve Mendelsohn Lehmann
Cover Artist: Masaaki Noda
Interior Illustrator: Scientific Illustrators
Compositor: Techset Composition Ltd.
Cover Printer: Henry N. Sawyer, Inc.
Printer and Binder: Arcata Graphics/Halliday

The Prindle, Weber and Schmidt Series in Mathematics

Althoen and Bumcrot, *Introduction to Discrete Mathematics*
Bean, Sharp, and Sharp, *Precalculus*
Boye, Kavanaugh, and Williams, *Elementary Algebra*
Boye, Kavanaugh, and Williams, *Intermediate Algebra*
Burden and Faires, *Numerical Analysis*, Fifth Edition
Cass and O'Connor, *Fundamentals with Elements of Algebra*
Cullen, *Linear Algebra and Differential Equations*, Second Edition
Dick and Patton, *Calculus, Volume I and Volume II*
Dick and Patton, *Technology in Calculus: A Sourcebook of Activities*
Eves, *In Mathematical Circles*
Eves, *Mathematical Circles Squared*
Eves, *Return to Mathematical Circles*
Faires and Burden, *Numerical Methods*
Fletcher, Hoyle, and Patty, *Foundations of Discrete Mathematics*
Fletcher and Patty, *Foundations of Higher Mathematics*, Second Edition
Fraser, *Intermediate Algebra: An Early Functions Approach*
Gantner and Gantner, *Trigonometry*
Geltner and Peterson, *Geometry for College Students*, Second Edition
Gilbert and Gilbert, *Elements of Modern Algebra*, Third Edition
Gobran, *Beginning Algebra*, Fifth Edition
Gobran, *Intermediate Algebra*, Fourth Edition
Gordon, *Calculus and the Computer*
Hall, *Algebra for College Students*, Second Edition
Hall, *Beginning Algebra*
Hall, *College Algebra with Applications*, Third Edition
Hall, *Intermediate Algebra*
Hartfiel and Hobbs, *Elementary Linear Algebra*
Huff and Peterson, *College Algebra Activities for the TI-81 Graphics Calculator*
Humi and Miller, *Boundary-Value Problems and Partial Differential Equations*
Kaufmann, *Elementary Algebra for College Students*, Fourth Edition
Kaufmann, *Intermediate Algebra for College Students*, Fourth Edition
Kaufmann, *Elementary and Intermediate Algebra: A Combined Approach*
Kaufmann, *Algebra for College Students*, Fourth Edition
Kaufmann, *Algebra with Trigonometry for College Students*, Third Edition
Kaufmann, *College Algebra*, Second Edition
Kaufmann, *Trigonometry*
Kaufmann, *College Algebra and Trigonometry*, Second Edition
Kaufmann, *Precalculus*, Second Edition
Kennedy and Green, *Prealgebra for College Students*
Laufer, *Discrete Mathematics and Applied Modern Algebra*
Lavoie, *Discovering Mathematics*
Nicholson, *Elementary Linear Algebra with Applications*, Second Edition
Nicholson, *Introduction to Abstract Algebra*
Pence, *Calculus Activities for Graphic Calculators*
Pence, *Calculus Activities for the TI-81 Graphic Calculator*
Plybon, *An Introduction to Applied Numerical Analysis*
Powers, *Elementary Differential Equations*
Powers, *Elementary Differential Equations with Boundary-Value Problems*

Proga, *Arithmetic and Algebra*, Third Edition
Proga, *Basic Mathematics*, Third Edition
Rice and Strange, *Plane Trigonometry*, Sixth Edition
Rogers, Haney, and Laird, *Fundamentals of Business Mathematics*
Schelin and Bange, *Mathematical Analysis for Business and Economics*, Second Edition
Sgroi and Sgroi, *Mathematics for Elementary School Teachers: Problem Solving Investigations*
Swokowski and Cole, *Fundamentals of College Algebra*, Eighth Edition
Swokowski and Cole, *Fundamentals of Algebra and Trigonometry*, Eighth Edition
Swokowski and Cole, *Fundamentals of Trigonometry*, Eighth Edition
Swokowski and Cole, *Algebra and Trigonometry with Analytic Geometry*, Eighth Edition
Swokowski, *Precalculus: Functions and Graphs*, Sixth Edition
Swokowski, *Calculus*, Fifth Edition
Swokowski, *Calculus*, Fifth Edition, Late Trigonometry Version
Swokowski, *Calculus of a Single Variable*
Tan, *Applied Finite Mathematics*, Third Edition
Tan, *Calculus for the Managerial, Life, and Social Sciences*, Second Edition
Tan, *Applied Calculus*, Second Edition
Tan, *College Mathematics*, Second Edition
Trim, *Applied Partial Differential Equations*
Venit and Bishop, *Elementary Linear Algebra*, Alternate Second Edition
Venit and Bishop, *Elementary Linear Algebra*, Third Edition
Wiggins, *Problem Solver for Finite Mathematics and Calculus*
Willard, *Calculus and Its Applications*, Second Edition
Wood and Capell, *Arithmetic*
Wood and Capell, *Intermediate Algebra*
Wood, Capell, and Hall, *Developmental Mathematics*, Fourth Edition
Zill, *Calculus*, Third Edition
Zill, *A First Course in Differential Equations*, Fifth Edition
Zill and Cullen, *Elementary Differential Equations with Boundary-Value Problems*, Third Edition
Zill and Cullen, *Advanced Engineering Mathematics*

The Prindle, Weber and Schmidt Series in Advanced Mathematics

Brabenec, *Introduction to Real Analysis*
Ehrlich, *Fundamental Concepts of Abstract Algebra*
Eves, *Foundations and Fundamental Concepts of Mathematics*, Third Edition
Keisler, *Elementary Calculus: An Infinitesimal Approach*, Second Edition
Kirkwood, *An Introduction to Real Analysis*
Patty, *Foundations of Topology*
Ruckle, *Modern Analysis: Measure Theory and Functional Analysis with Applications*
Sieradski, *An Introduction to Topology and Homotopy*

Preface

This book is a self-contained introduction to the basic structures of abstract algebra: groups, rings, and fields. It is designed to be used in a one- or two-semester course (see the chapter summaries that follow) and may also serve for self-study. In addition, it contains several optional sections on special topics and applications.

Because many students will not have had much experience with abstract thinking, I introduce a number of important concrete examples (complex numbers, two-by-two matrices, integers modulo n, and permutations) at the beginning and refer to them throughout the book. I chose these examples for their importance and intrinsic interest and also because the student can do actual computations almost immediately even though the examples are, in the student's view, quite abstract. Thus they provide a bridge to the abstract theory and serve as prototype examples of the abstract structures themselves. For example, the student will encounter composition and inverses of permutations before having to fit these notions into the general framework of group theory.

I also emphasize the axiomatic development of these structures. Modern algebra provides one of the best illustrations of the power of abstraction to strip concrete examples of nonessential aspects, so as to reveal similarities between ostensibly different objects and to suggest that a theorem about one structure may have an analogue for a different structure. Achieving this sort of facility with abstraction is one of the goals of the book, which goes hand in hand with another goal: to teach the student how to do proofs. The proofs of most theorems are at least as important for the techniques as for the theorems themselves. Hence, whenever possible, I introduce techniques and use them in examples before giving them in the general case as a proof. This approach explains the large number of examples (nearly 500) in the book.

Of course, a generous supply of exercises is essential if this subject is to have a lasting impact on students, and the book contains nearly 1500 exercises (many with separate parts). Computational exercises appear first for the most part, and the exercises are more or less in ascending order of difficulty. Hints are given for the less straightforward problems. On the whole, I do not use exercises to develop results that are needed later in the text, so not all exercises need to be solved in order to continue with the book. Answers are provided to odd-numbered (parts of) computational exercises and to selected theoretical exercises.

An increasing number of students of abstract algebra come from outside mathematics, and, for many of them, the lure of pure abstraction is not as strong as for mathematicians. Therefore, I include applications of the theory that make the subject more meaningful and lively for these students (and for the mathematicians!). These include cryptography, linear codes, cyclic and BCH codes, and combinatorics, as well as "theoretical" applications within mathematics, such as the impossibility of the classical geometric constructions. The inclusion of short historical notes and biographies should help the reader put the material into perspective. In the same spirit, some classical "gems" appear in optional sections (one example is the elegant proof of the fundamental theorem of algebra in Section 6.6, using the structure theorem for symmetric polynomials). In addition, I convey the modern flavor of the subject by mentioning some of the unsolved problems in abstract algebra and by occasionally stating more advanced theorems that extend beyond the results of the book.

Apart from that, the material is quite standard. The aim is to reveal the basic facts about groups, rings, and fields and to give the student the working tools for further study. The level of exposition rises slowly throughout the text, and no prior knowledge of abstract algebra is required. Even linear algebra is not needed. Except for a few well-marked instances, the aspects of linear algebra that are needed are developed in the text. Calculus is completely unnecessary. Some preliminary topics that are needed are covered in Chapter 0 (including complex numbers and two-by-two matrices).

Although the chapters are necessarily arranged in a linear order, this is by no means true of the contents, and the student (as well as the instructor) should keep the chapter dependency diagram on page xiv in mind. A glance at that diagram shows that Chapters 1–4 are the core of the book but that there is enough flexibility in the remaining chapters to accommodate an instructor who wants to include more than just the basics. The jump from Chapter 6 to Chapter 10 deserves mention. The student has a choice at the end of Chapter 6: either change the subject and do some more group theory or continue with fields in Chapter 10 (solvable groups are adequately reviewed in Section 10.3, so Chapter 9 is not necessary).

The chapter summaries that follow and the chapter dependency diagram can assist in the preparation of a course syllabus. Our course of 36 lectures touches Sections 0.3 and 0.4 lightly and then covers Chapters 1–4, except for Sections 1.5, 2.11, 3.5, and 4.4–4.6.

FEATURES

This book offers the following significant features:

- Self-contained treatment
- Preliminary material available in Chapter 0 for self-study or review
- Integers modulo n and permutations done first as a bridge to abstraction
- Nearly 500 worked examples to guide the student
- Wide variety of exercises with selected answers
- Gradual increase in level throughout the text
- Applications to number theory, combinatorics, geometry, coding, and equations
- Flexibility in syllabus construction and choice of optional topics (see chapter dependency diagram)
- Historical notes and biographies
- Several special topics (for example, symmetric polynomials, nilpotent groups, and finite-dimensional algebras)
- Solutions manual containing answers or solutions to all exercises

CHAPTER SUMMARIES

Chapter 0 ***Preliminaries*** This chapter should be viewed as a primer on mathematics, as it consists of material essential to any mathematics major. The treatment is self-contained. I personally let students read Sections 0.1 and 0.2 on their own, I touch the highlights in Sections 0.3 and 0.4, and review Section 0.5 briefly (our students have had elementary linear algebra so I omit Section 0.6).

Chapter 1 ***Integers and Permutations.*** This chapter covers the fundamental properties of the integers and the two prototype examples of rings and groups: the integers modulo n and the permutation group S_n. These are done naïvely and allow the students to do ring and group calculations in a concrete setting.

Chapter 2 ***Groups.*** This chapter gives the basic facts of group theory, including cyclic groups, Lagrange's theorem, normal subgroups, factor groups, homomorphisms, and the isomorphism theorem. An optional application to linear codes is included. Section 2.7 on groups of motions is also optional.

Chapter 3 ***Rings.*** The basic properties of rings are developed: integral domains, characteristic, rings of quotients, ideals, factorization, homomorphisms, and the isomorphism theorem. The analogy between these notions and the corresponding group-theoretic concepts is noted.

Chapter 4 ***Polynomials.*** After the usual elementary facts are developed, irreducible polynomials are discussed and the unique factorization of polynomials over a field is proved. Then factor rings of polynomials over a field are described and

some finite fields are constructed. In an optional section, symmetric polynomials are discussed and the fundamental structure theorem is proved.

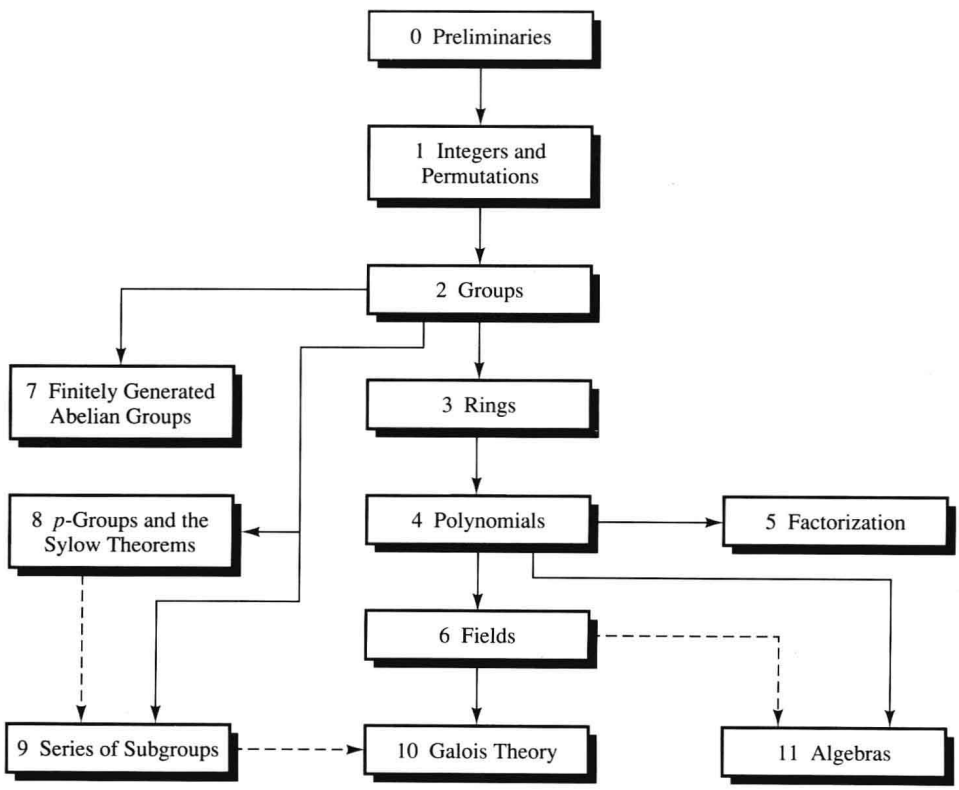
Chapter 5 ***Factorization in Integral Domains.*** Unique factorization domains are characterized in terms of irreducibles and primes, and the fact that the property is inherited by polynomial rings is proved. Principal ideal domains and Euclidean domains are discussed. The chapter is self-contained, and the material presented is not required elsewhere.

Chapter 6 ***Fields.*** After a minimal amount of vector space theory is developed, splitting fields are constructed and used to completely describe finite fields. This topic is a direct continuation of Section 4.3. In optional sections, the classical results on geometric constructions are derived, the fundamental theorem of algebra is proved, and the theory of cyclic (and BCH) codes is developed.

Chapter 7 ***Finitely Generated Abelian Groups.*** The fundamental theorem for finite abelian groups is proved and then extended to the finitely generated case. This material is self-contained and is not required elsewhere.

Chapter 8 ***p-Groups and the Sylow Theorems.*** This chapter is a direct continuation of Section 2.10. The class equation is given and is used to prove Cauchy's theorem and to derive the basic properties of p-groups. Then group actions

Chapter Dependency Diagram



A broken arrow indicates minor dependency.

are introduced, motivated by the class equation and an extended Cayley theorem, and used to prove the Sylow theorems. An optional application to combinatorics is also included.

Chapter 9. ***Series of Subgroups.*** The chapter begins with composition series and the Jordan–Hölder theorem. Then solvable series are introduced, including the derived series, and the basic properties of solvable groups are proved. Finally, central series are discussed and nilpotent groups are characterized as direct products of p-groups. Sections 9.1 and 9.2 depend on Chapter 8 only in the statement of some results, and so could be studied before Chapter 8.

Chapter 10 ***Galois Theory.*** Galois groups of field extensions are defined, separable elements are introduced, and the main theorem of Galois theory is proved. Then the fact that polynomials of degree 5 or more are not solvable in radicals is proved. All this requires only Chapter 6 (the reference to solvable groups in Section 10.3 is adequately reviewed there). Finally, cyclotomic polynomials are discussed and used, with the class equation, to prove Wedderburn's theorem that every finite division ring is a field.

Chapter 11 ***Algebras.*** Finite-dimensional algebras are defined and the regular representation is given. Then the Wedderburn structure theorems are derived. Chapter 6 is needed only for the notion of dimension in a vector space.

ACKNOWLEDGMENTS

I express my appreciation to the following people for their useful comments and suggestions:

F. Doyle Alexander
Stephen F. Austin State University

Steve Benson
Saint Olaf College

Paul M. Cook II
Furman University

Ronald H. Dalla
Eastern Washington University

Robert Fakler
University of Michigan—Dearborn

Robert M. Guralnick
University of Southern California

Edward K. Hinson
University of New Hampshire

Ron Hirschorn
Queen's University

David L. Johnson
Lehigh University

William R. Nico
California State University - Hayward

Kimmo I. Rosenthal
Union College

Erik Shreiner (deceased)
Western Michigan University

S. Thomeier
Memorial University

Marie A. Vitulli
University of Oregon

Thanks also go to Steve Quigley for his generous assistance throughout the project, to Susan London, and to the editorial and production staff at PWS-KENT. Special thanks go to Mark Nicholson for his excellent job of typing the manuscript and to Jason Nicholson for preparing the solutions manual. Finally, I want to thank my wife, Kathleen, for her constant support.

W. Keith Nicholson

Notation used in the Text

Symbol	Description	First Used
$\Rightarrow$	implication	2
$\neg$	negation of a statement	3
$\Leftrightarrow$	logical equivalence	4
$\in$	set membership	6
$\subseteq$	set containment	7
$\subset$	proper set containment	7
$\mathbb{N}$	set of natural numbers	7
$\mathbb{Z}$	set of integers	7
$\mathbb{Q}$	set of rational numbers	7
$\mathbb{R}$	set of real numbers	7
$\mathbb{C}$	set of complex numbers	7
$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$	positive elements in these sets	7
$\|A\|$	number of elements in set A	8
$\varnothing$	empty set	8
$\cup$	union of sets	8, 9
$\cap$	intersection of sets	8, 9
A^c	complement of a set A	10
$A - B$	difference set	11
(a, b)	ordered pair	11
$A \times B$	Cartesian product of sets A and B	11, 12
$(a_1, a_2, \ldots, a_n)$	ordered n-tuple	12
$\alpha: A \to B$ $A \xrightarrow{\alpha} B$	mapping α from A to B	14, 15
$\alpha(x)$	image of x under mapping α	15
$\operatorname{im} \alpha$	image of the mapping α	17
$\alpha\beta$	composite of mappings α and β	18
1_A	identity mapping on set A	19
α^{-1}	inverse of mapping α	20
$\equiv$	equivalence relation	24
$[a]$	equivalence class of a	24
$A_{\equiv}$	quotient set of an equivalence $\equiv$	27
$\operatorname{re} z$	real part of z	31
$\operatorname{im} z$	imaginary part of z	31
$\bar{z}$	conjugate of a complex number z	32
$\|z\|$	absolute value of z	32
$e^{i\theta}$	notation for $\cos\theta + i \sin\theta$	35

Symbol	Description	First Used
$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$	$m \times n$ matrix	40
I, I_n	identity matrix	43
$\det A$	determinant of a square matrix A	45
$n!$	n factorial	51
$\binom{n}{r}$	binomial coefficient	52
$d \mid n$	d is a divisor of n	61
$\gcd(m, n)$ $\gcd(n_1, \ldots, n_r)$	greatest common divisor	62, 68
$\operatorname{lcm}(m, n)$ $\operatorname{lcm}(n_1, \ldots, n_r)$	least common multiple	68
$a \equiv b \pmod{n}$	congruence modulo n	74
$\bar{a}$	residue class of an integer a	74
$\mathbb{Z}_n$	integers modulo n	74
S_n	symmetric group of degree n	87, 90
$\begin{pmatrix} 1 & 2 \cdots & n \\ \sigma 1 & \sigma 2 \cdots & \sigma n \end{pmatrix}$	permutation σ in S_n	87
ε	identity permutation in S_n	88
$(k_1\, k_2 \cdots k_n)$	cycle permutation in S_n	92
$\operatorname{sgn} \sigma$	sign of permutation σ	101
$\mathbb{C}^0$	circle group	115
U_n	group of nth roots of unity	115
M^*	groups of units of M	116
S_X	group of permutations of X	117
$GL_n(R)$	general linear group over R	118
C_n	cyclic group of order n	121
K_4	Klein 4-group	123
$SL_n(R)$	special linear group over R	127
$Z(G)$	center of group G	128
$\langle g \rangle$	cyclic subgroup generated by g	134
$\lvert g \rvert$	order of group element g	137
$\langle X \rangle$	subgroup generated by X	143
$\operatorname{aut} G$	automorphism group of G	151
$\operatorname{inn} G$	inner automorphism group of G	152
Ha, aH	right, left cosets	159
$\lvert G : H \rvert$	index of subgroup H in G	163

Symbol	Description	First Used
D_n	dihedral group	164
$H \lhd G$	H is a normal subgroup of G	177
Q	quaternion group	181
G/K	factor group of G by K	189
G'	derived (commutator) subgroup of G	192
$\ker \alpha$	kernel of α	203
B^n	set of binary n-tuples	214
$F(X, R)$	ring of functions $X \to R$	234
$M_n(R)$	ring of $n \times n$ matrices over R	236
$R[x]$	ring of polynomials in x over R	237
$\deg p(x)$	degree of $p(x)$	237
$\operatorname{char} R$	characteristic of a ring R	238
$\mathbb{H}$	quaternions	254
R^1	ring extension of a general ring R	282
$a \sim b$	associates in an integral domain	362
$\operatorname{span}\{v_1, \ldots, v_n\}$	space spanned by $v_1, \ldots, v_n$	391
$\dim V$	dimension of vector space V	394
$[E:F]$	dimension of E over a subfield F	399
$F(u_1, \ldots, u_n)$	field generated over F by $u_1, \ldots, u_n$	400
$\mathrm{GF}(p^n)$	Galois field of order p^n	422
class a	conjugacy class of a	475
$N(X)$	normalizer of X	476
core H	core of a subgroup H	484
$G \cdot x$	orbit of x generated by G	488
$S(x)$	stabilizer of x	488
length G	composition length of G	511
$\mathrm{gal}(E:F)$	Galois group of E over F	534

Contents

† This is an optional section.

† This is an optional section.