

Contents

Preface xi

Preliminaries 1

- 0.1 Basics 1
- 0.2 Properties of the Integers 4
- 0.3 $\mathbb{Z} / n\mathbb{Z}$: The Integers Modulo n 8

Part I – GROUP THEORY 13

Chapter 1 Introduction to Groups 16

- 1.1 Basic Axioms and Examples 16
- 1.2 Dihedral Groups 23
- 1.3 Symmetric Groups 29
- 1.4 Matrix Groups 34
- 1.5 The Quaternion Group 36
- 1.6 Homomorphisms and Isomorphisms 36
- 1.7 Group Actions 41

Chapter 2 Subgroups 46

- 2.1 Definition and Examples 46
- 2.2 Centralizers and Normalizers, Stabilizers and Kernels 49
- 2.3 Cyclic Groups and Cyclic Subgroups 54
- 2.4 Subgroups Generated by Subsets of a Group 61
- 2.5 The Lattice of Subgroups of a Group 66

Chapter 3	Quotient Groups and Homomorphisms	73
3.1	Definitions and Examples	73
3.2	More on Cosets and Lagrange's Theorem	89
3.3	The Isomorphism Theorems	97
3.4	Composition Series and the Hölder Program	101
3.5	Transpositions and the Alternating Group	106
Chapter 4	Group Actions	112
4.1	Group Actions and Permutation Representations	112
4.2	Groups Acting on Themselves by Left Multiplication—Cayley's Theorem	118
4.3	Groups Acting on Themselves by Conjugation—The Class Equation	122
4.4	Automorphisms	133
4.5	The Sylow Theorems	139
4.6	The Simplicity of A_n	149
Chapter 5	Direct and Semidirect Products and Abelian Groups	152
5.1	Direct Products	152
5.2	The Fundamental Theorem of Finitely Generated Abelian Groups	158
5.3	Table of Groups of Small Order	167
5.4	Recognizing Direct Products	169
5.5	Semidirect Products	175
Chapter 6	Further Topics in Group Theory	188
6.1	p -groups, Nilpotent Groups, and Solvable Groups	188
6.2	Applications in Groups of Medium Order	201
6.3	A Word on Free Groups	215

Part II – RING THEORY 222

Chapter 7	Introduction to Rings	223
7.1	Basic Definitions and Examples	223
7.2	Examples: Polynomial Rings, Matrix Rings, and Group Rings	233
7.3	Ring Homomorphisms and Quotient Rings	239
7.4	Properties of Ideals	251
7.5	Rings of Fractions	260
7.6	The Chinese Remainder Theorem	265

Chapter 8 Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains 270

- 8.1 Euclidean Domains 270
- 8.2 Principal Ideal Domains (P.I.D.s) 279
- 8.3 Unique Factorization Domains (U.F.D.s) 283

Chapter 9 Polynomial Rings 295

- 9.1 Definitions and Basic Properties 295
- 9.2 Polynomial Rings over Fields I 299
- 9.3 Polynomial Rings that are Unique Factorization Domains 303
- 9.4 Irreducibility Criteria 307
- 9.5 Polynomial Rings over Fields II 313
- 9.6 Polynomials in Several Variables over a Field and Gröbner Bases 315

Part III – MODULES AND VECTOR SPACES 336

Chapter 10 Introduction to Module Theory 337

- 10.1 Basic Definitions and Examples 337
- 10.2 Quotient Modules and Module Homomorphisms 345
- 10.3 Generation of Modules, Direct Sums, and Free Modules 351
- 10.4 Tensor Products of Modules 359
- 10.5 Exact Sequences—Projective, Injective, and Flat Modules 378

Chapter 11 Vector Spaces 408

- 11.1 Definitions and Basic Theory 408
- 11.2 The Matrix of a Linear Transformation 415
- 11.3 Dual Vector Spaces 431
- 11.4 Determinants 435
- 11.5 Tensor Algebras, Symmetric and Exterior Algebras 441

Chapter 12 Modules over Principal Ideal Domains 456

- 12.1 The Basic Theory 458
- 12.2 The Rational Canonical Form 472
- 12.3 The Jordan Canonical Form 491

Part IV – FIELD THEORY AND GALOIS THEORY 509

Chapter 13 Field Theory 510

- 13.1 Basic Theory of Field Extensions 510
- 13.2 Algebraic Extensions 520
- 13.3 Classical Straightedge and Compass Constructions 531
- 13.4 Splitting Fields and Algebraic Closures 536
- 13.5 Separable and Inseparable Extensions 545
- 13.6 Cyclotomic Polynomials and Extensions 552

Chapter 14 Galois Theory 558

- 14.1 Basic Definitions 558
- 14.2 The Fundamental Theorem of Galois Theory 567
- 14.3 Finite Fields 585
- 14.4 Composite Extensions and Simple Extensions 591
- 14.5 Cyclotomic Extensions and Abelian Extensions over \mathbb{Q} 596
- 14.6 Galois Groups of Polynomials 606
- 14.7 Solvable and Radical Extensions: Insolvability of the Quintic 625
- 14.8 Computation of Galois Groups over \mathbb{Q} 640
- 14.9 Transcendental Extensions, Inseparable Extensions, Infinite Galois Groups 645

**Part V – AN INTRODUCTION TO COMMUTATIVE RINGS,
ALGEBRAIC GEOMETRY, AND
HOMOLOGICAL ALGEBRA 655**

Chapter 15 Commutative Rings and Algebraic Geometry 656

- 15.1 Noetherian Rings and Affine Algebraic Sets 656
- 15.2 Radicals and Affine Varieties 673
- 15.3 Integral Extensions and Hilbert's Nullstellensatz 691
- 15.4 Localization 706
- 15.5 The Prime Spectrum of a Ring 731

**Chapter 16 Artinian Rings, Discrete Valuation Rings, and
Dedekind Domains 750**

- 16.1 Artinian Rings 750
- 16.2 Discrete Valuation Rings 755
- 16.3 Dedekind Domains 764

Chapter 17	Introduction to Homological Algebra and Group Cohomology	776
17.1	Introduction to Homological Algebra—Ext and Tor	777
17.2	The Cohomology of Groups	798
17.3	Crossed Homomorphisms and $H^1(G, A)$	814
17.4	Group Extensions, Factor Sets and $H^2(G, A)$	824

**Part VI – INTRODUCTION TO THE REPRESENTATION
THEORY OF FINITE GROUPS 839**

Chapter 18	Representation Theory and Character Theory	840
18.1	Linear Actions and Modules over Group Rings	840
18.2	Wedderburn’s Theorem and Some Consequences	854
18.3	Character Theory and the Orthogonality Relations	864
Chapter 19	Examples and Applications of Character Theory	880
19.1	Characters of Groups of Small Order	880
19.2	Theorems of Burnside and Hall	886
19.3	Introduction to the Theory of Induced Characters	892

Appendix I:	Cartesian Products and Zorn’s Lemma	905
--------------------	--	------------

Appendix II:	Category Theory	911
---------------------	------------------------	------------

Index	919
--------------	------------

Preface to the Third Edition

The principal change from the second edition is the addition of Gröbner bases to this edition. The basic theory is introduced in a new Section 9.6. Applications to solving systems of polynomial equations (elimination theory) appear at the end of this section, rounding it out as a self-contained foundation in the topic. Additional applications and examples are then woven into the treatment of affine algebraic sets and k -algebra homomorphisms in Chapter 15. Although the theory in the latter chapter remains independent of Gröbner bases, the new applications, examples and computational techniques significantly enhance the development, and we recommended that Section 9.6 be read either as a segue to or in parallel with Chapter 15. A wealth of exercises involving Gröbner bases, both computational and theoretical in nature, have been added in Section 9.6 and Chapter 15. Preliminary exercises on Gröbner bases can (and should, as an aid to understanding the algorithms) be done by hand, but more extensive computations, and in particular most of the use of Gröbner bases in the exercises in Chapter 15, will likely require computer assisted computation.

Other changes include a streamlining of the classification of simple groups of order 168 (Section 6.2), with the addition of a uniqueness proof via the projective plane of order 2. Some other proofs or portions of the text have been revised slightly. A number of new exercises have been added throughout the book, primarily at the ends of sections in order to preserve as much as possible the numbering schemes of earlier editions. In particular, exercises have been added on free modules over noncommutative rings (10.3), on Krull dimension (15.3), and on flat modules (10.5 and 17.1).

As with previous editions, the text contains substantially more than can normally be covered in a one year course. A basic introductory (one year) course should probably include: Part I up through Section 5.3, Part II through Section 9.5, Sections 10.1, 10.2, 10.3, 11.1, 11.2 and Part IV. Chapter 12 should also be covered, either before or after Part IV. Additional topics from Chapters 5, 6, 9, 10 and 11 may be interspersed in such a course, or covered at the end as time permits.

Sections 10.4 and 10.5 are at a slightly higher level of difficulty than the initial sections of Chapter 10, and can be deferred on a first reading for those following the text sequentially. The latter section on properties of exact sequences, although quite long, maintains coherence through a parallel treatment of three basic functors in respective subsections.

Beyond the core material, the third edition provides significant flexibility for stu-

dents and instructors wishing to pursue a number of important areas of modern algebra, either in the form of independent study or courses. For example, well integrated one-semester courses for students with some prior algebra background might include the following: Section 9.6 and Chapters 15 and 16; or Chapters 10 and 17; or Chapters 5, 6 and Part VI. Each of these would also provide a solid background for a follow-up course delving more deeply into one of many possible areas: algebraic number theory, algebraic topology, algebraic geometry, representation theory, Lie groups, etc.

The choice of new material and the style for developing and integrating it into the text are in consonance with a basic theme in the book: the power and beauty that accrues from a rich interplay between different areas of mathematics. The emphasis throughout has been to motivate the introduction and development of important algebraic concepts using as many examples as possible. We have not attempted to be encyclopedic, but have tried to touch on many of the central themes in elementary algebra in a manner suggesting the very natural development of these ideas.

A number of important ideas and results appear in the exercises. This is not because they are not significant, rather because they did not fit easily into the flow of the text but were too important to leave out entirely. Sequences of exercises on one topic are prefaced with some remarks and are structured so that they may be read without actually doing the exercises. In some instances, new material is introduced first in the exercises—often a few sections before it appears in the text—so that students may obtain an easier introduction to it by doing these exercises (e.g., Lagrange’s Theorem appears in the exercises in Section 1.7 and in the text in Section 3.2). All the exercises are within the scope of the text and hints are given [in brackets] where we felt they were needed. Exercises we felt might be less straightforward are usually phrased so as to provide the answer to the exercise; as well many exercises have been broken down into a sequence of more routine exercises in order to make them more accessible.

We have also purposely minimized the functorial language in the text in order to keep the presentation as elementary as possible. We have refrained from providing specific references for additional reading when there are many fine choices readily available. Also, while we have endeavored to include as many fundamental topics as possible, we apologize if for reasons of space or personal taste we have neglected any of the reader’s particular favorites.

We are deeply grateful to and we thank the many students and colleagues around the world who, over more than 15 years, have offered valuable comments, insights and encouragement—their continuing support and interest have motivated our writing of this third edition.

David Dummit
Richard Foote
June, 2003