Contents

Preface xi

1 Matrices
1.1 The Basic Operations . . . 1
1.2 Row Reduction . . . 10
1.3 The Matrix Transpose . . . 17
1.4 Determinants . . . 18
1.5 Permutations . . . 24
1.6 Other Formulas for the Determinant . . . 27
Exercises . . . 31

2 Groups
2.1 Laws of Composition . . . 37
2.2 Groups and Subgroups . . . 40
2.3 Subgroups of the Additive Group of Integers . . . 43
2.4 Cyclic Groups . . . 46
2.5 Homomorphisms . . . 47
2.6 Isomorphisms . . . 51
2.7 Equivalence Relations and Partitions . . . 52
2.8 Cosets . . . 56
2.9 Modular Arithmetic . . . 60
2.10 The Correspondence Theorem . . . 61
2.11 Product Groups . . . 64
2.12 Quotient Groups . . . 66
Exercises . . . 69

3 Vector Spaces
3.1 Subspaces of $\mathbb{R}^n$ . . . 78
3.2 Fields . . . 80
3.3 Vector Spaces . . . 84
3.4 Bases and Dimension . . . 86
3.5 Computing with Bases . . . 91
3.6 Direct Sums . . . 95
3.7 Infinite-Dimensional Spaces . . . 96
Exercises . . . 98

4 Linear Operators
4.1 The Dimension Formula . . . 102
4.2 The Matrix of a Linear Transformation . . . 104

12 Factoring
12.1 Factoring Integers . . . 359
12.2 Unique Factorization Domains . . . 360
12.3 Gauss's Lemma . . . 367
12.4 Factoring Integer Polynomials . . . 371
12.5 Gauss Primes . . . 376
Exercises . . . 378

13 Quadratic Number Fields
13.1 Algebraic Integers . . . 383
13.2 Factoring Algebraic Integers . . . 385
13.3 Ideals in $\mathbb{Z}[\sqrt{-5}]$ . . . 387
13.4 Ideal Multiplication . . . 389
13.5 Factoring Ideals . . . 392
13.6 Prime Ideals and Prime Integers . . . 394
13.7 Ideal Classes . . . 396
13.8 Computing the Class Group . . . 399
13.9 Real Quadratic Fields . . . 402
13.10 About Lattices . . . 405
Exercises . . . 408

14 Linear Algebra in a Ring
14.1 Modules . . . 412
14.2 Free Modules . . . 414
14.3 Identities . . . 417
14.4 Diagonalizing Integer Matrices . . . 418
14.5 Generators and Relations . . . 423
14.6 Noetherian Rings . . . 426
14.7 Structure of Abelian Groups . . . 429
14.8 Application to Linear Operators . . . 432
14.9 Polynomial Rings in Several Variables . . . 436
Exercises . . . 437

15 Fields
15.1 Examples of Fields . . . 442
15.2 Algebraic and Transcendental Elements . . . 443
15.3 The Degree of a Field Extension . . . 446
15.4 Finding the Irreducible Polynomial . . . 449
15.5 Ruler and Compass Constructions . . . 450
15.6 Adjoining Roots . . . 456
15.7 Finite Fields . . . 459
15.8 Primitive Elements . . . 462
15.9 Function Fields . . . 463
15.10 The Fundamental Theorem of Algebra . . . 471
Exercises . . . 472

16 Galois Theory
16.1 Symmetric Functions 477
16.2 The Discriminant 481
16.3 Splitting Fields 483
16.4 Isomorphisms of Field Extensions 484
16.5 Fixed Fields 486
16.6 Galois Extensions 488
16.7 The Main Theorem 489
16.8 Cubic Equations 492
16.9 Quartic Equations 493
16.10 Roots of Unity 497
16.11 Kummer Extensions 500
16.12 Quintic Equations 502
Exercises 505

APPENDIX

Background Material
A.1 About Proofs 513
A.2 The Integers 516
A.3 Zorn's Lemma 518
A.4 The Implicit Function Theorem 519
Exercises 521

Bibliography 523

Notation 525

Index 529