

Contents

Preface **xiii**

Acknowledgments **xvii**

Chapter 0 Background **1**

- 0.1 Sets and Maps 1
- 0.2 Equivalence Relations and Partitions 7
- 0.3 Properties of \mathbb{Z} 10
- 0.4 Complex Numbers 24
- 0.5 Matrices 31

Part A

Group Theory

Chapter 1 Groups **39**

- 1.1 Examples and Basic Concepts 39
- 1.2 Subgroups 50
- 1.3 Cyclic Groups 56
- 1.4 Permutations 62

Chapter 2 Group Homomorphisms **74**

- 2.1 Cosets and Lagrange's Theorem 74
- 2.2 Homomorphisms 81
- 2.3 Normal Subgroups 88
- 2.4 Quotient Groups 94
- 2.5 Automorphisms 103

Chapter 3	Direct Products and Abelian Groups	108
3.1	Examples and Definitions	108
3.2	Computing Orders	113
3.3	Direct Sums	116
3.4	Fundamental Theorem of Finite Abelian Groups	122
Chapter 4	Group Actions	131
4.1	Group Actions and Cayley's Theorem	131
4.2	Stabilizers and Orbits in a Group Action	137
4.3	Burnside's Theorem and Applications	142
4.4	Conjugacy Classes and the Class Equation	148
4.5	Conjugacy in S_n and Simplicity of A_5	153
4.6	The Sylow Theorems	159
4.7	Applications of the Sylow Theorems	165
Chapter 5	Composition Series	172
5.1	Isomorphism Theorems	172
5.2	The Jordan-Hölder Theorem	178
5.3	Solvable Groups	184

Part B

Rings and Fields

Chapter 6	Rings	193
6.1	Examples and Basic Concepts	193
6.2	Integral Domains	199
6.3	Fields	202
Chapter 7	Ring Homomorphisms	210
7.1	Definitions and Basic Properties	210
7.2	Ideals	215
7.3	The Field of Quotients	224

Chapter 8	Rings of Polynomials	232
8.1	Basic Concepts and Notation	232
8.2	The Division Algorithm in $F[x]$	239
8.3	More Applications of the Division Algorithm	245
8.4	Irreducible Polynomials	250
8.5	Cubic and Quartic Polynomials	260
8.6	Ideals in $F[x]$	266
8.7	Quotient Rings of $F[x]$	269
8.8	The Chinese Remainder Theorem for $F[x]$	273
Chapter 9	Euclidean Domains	279
9.1	Division Algorithms and Euclidean Domains	279
9.2	Unique Factorization Domains	286
9.3	Gaussian Integers	294
Chapter 10	Field Theory	299
10.1	Vector Spaces	299
10.2	Algebraic Extensions	308
10.3	Splitting Fields	322
10.4	Finite Fields	334
Chapter 11	Geometric Constructions	341
11.1	Constructible Real Numbers	341
11.2	Classical Problems	352
11.3	Constructions with Marked Ruler and Compass	357
11.4	Cubics and Quartics Revisited	363
Chapter 12	Galois Theory	371
12.1	Galois Groups	371
12.2	The Fundamental Theorem of Galois Theory	383
12.3	Galois Groups of Polynomials	398
12.4	Geometric Constructions Revisited	415
12.5	Radical Extensions	423

Chapter 13 Historical Notes 433

From Ahmes the Scribe to Omar Khayyam 433

From Gerolamo Cardano to C. F. Gauss 439

From Evariste Galois to Emmy Noether 445

Part C
Selected Topics

Chapter 14 Symmetries 453

Linear Transformations 453

Isometries 459

Symmetry Groups 464

Platonic Solids 466

Subgroups of the Special Orthogonal Group 468

Further Reading 472

Chapter 15 Gröbner Bases 475

Lexicographic Order 475

A Division Algorithm 478

Dickson's Lemma 482

The Hilbert Basis Theorem 485

Gröbner Bases and the Division Algorithm 486

Further Reading 488

Chapter 16 Coding Theory 490

Linear Binary Codes 490

Error Correction and Coset Decoding 494

Standard Generator Matrices 497

The Syndrome Method 499

Cyclic Codes 505

Further Reading 502

Chapter 17	Boolean Algebras	507
	Lattices	507
	Boolean Algebras	511
	Circuits	517
	<i>Further Reading</i>	520
Answers and Hints to Selected Exercises		525
Bibliography		539
Index		541