Contents

Introduction *page* ix
Before we Begin xiii

Part I Rings 1

1 The Integers 3
1.1 The Well-Ordering Principle and Induction 3
1.2 'Division with Remainder' in $\mathbb{Z}$ 6
1.3 Greatest Common Divisors 7
1.4 The Fundamental Theorem of Arithmetic 12
Exercises 20

2 Modular Arithmetic 22
2.1 Equivalence Relations and Quotients 22
2.2 Congruence mod n 23
2.3 Algebra in $\mathbb{Z}/n\mathbb{Z}$ 26
2.4 Properties of the Operations $+, \cdot$ on $\mathbb{Z}/n\mathbb{Z}$ 29
2.5 Fermat's Little Theorem, and the RSA Encryption System 34
Exercises 39

3 Rings 41
3.1 Definition and Examples 41
3.2 Basic Properties 47
3.3 Special Types of Rings 51
Exercises 57

4 The Category of Rings 59
4.1 Cartesian Products 59
4.2 Subrings 61
4.3 Ring Homomorphisms 64
4.4 Isomorphisms of Rings 69
Exercises 75

© in this web service Cambridge University Press

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Table of Contents
More Information

5 **Canonical Decomposition, Quotients, and Isomorphism Theorems** 77
5.1 Rings: Canonical Decomposition, I 77
5.2 Kernels and Ideals 79
5.3 Quotient Rings 83
5.4 Rings: Canonical Decomposition, II 89
5.5 The First Isomorphism Theorem 91
5.6 The Chinese Remainder Theorem 93
5.7 The Third Isomorphism Theorem 100
Exercises 103

6 **Integral Domains** 106
6.1 Prime and Maximal Ideals 106
6.2 Primes and Irreducibles 110
6.3 Euclidean Domains and PIDs 112
6.4 PIDs and UFDs 117
6.5 The Field of Fractions of an Integral Domain 120
Exercises 126

7 **Polynomial Rings and Factorization** 129
7.1 Fermat's Last Theorem for Polynomials 129
7.2 The Polynomial Ring with Coefficients in a Field 131
7.3 Irreducibility in Polynomial Rings 136
7.4 Irreducibility in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ 139
7.5 Irreducibility Tests in $\mathbb{Z}[x]$ 143
Exercises 148

Part II Modules 151

8 **Modules and Abelian Groups** 153
8.1 Vector Spaces and Ideals, Revisited 153
8.2 The Category of R-Modules 158
8.3 Submodules, Direct Sums 161
8.4 Canonical Decomposition and Quotients 164
8.5 Isomorphism Theorems 168
Exercises 171

9 **Modules over Integral Domains** 174
9.1 Free Modules 174
9.2 Modules from Matrices 181
9.3 Finitely Generated vs. Finitely Presented 187
9.4 Vector Spaces are Free Modules 190
9.5 Finitely Generated Modules over Euclidean Domains 193
9.6 Linear Transformations and Modules over $k[t]$ 197
Exercises 199

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Table of Contents
More Information

10 Abelian Groups 202
10.1 The Category of Abelian Groups 202
10.2 Cyclic Groups, and Orders of Elements 207
10.3 The Classification Theorem 212
10.4 Fermat's Theorem on Sums of Squares 217
Exercises 223

Part III Groups 227

11 Groups—Preliminaries 229
11.1 Groups and their Category 229
11.2 Why Groups? Actions of a Group 235
11.3 Cyclic, Dihedral, Symmetric, Free Groups 241
11.4 Canonical Decomposition, Normality, and Quotients 253
11.5 Isomorphism Theorems 260
Exercises 264

12 Basic Results on Finite Groups 267
12.1 The Index of a Subgroup, and Lagrange's Theorem 267
12.2 Stabilizers and the Class Equation 269
12.3 Classification and Simplicity 274
12.4 Sylow's Theorems: Statements, Applications 276
12.5 Sylow's Theorems: Proofs 280
12.6 Simplicity of $\mathcal{A}_n$ 282
12.7 Solvable Groups 286
Exercises 289

Part IV Fields 293

13 Field Extensions 295
13.1 Fields and Homomorphisms of Fields 295
13.2 Finite Extensions and the Degree of an Extension 299
13.3 Simple Extensions 301
13.4 Algebraic Extensions 307
13.5 Application: 'Geometric Impossibilities' 309
Exercises 314

14 Normal and Separable Extensions, and Splitting Fields 317
14.1 Simple Extensions, Again 317
14.2 Splitting Fields 320
14.3 Normal Extensions 326
14.4 Separable Extensions; and Simple Extensions Once Again 328
14.5 Application: Finite Fields 333
Exercises 337

© in this web service Cambridge University Press www.cambridge.org

15 Galois Theory 340
15.1 Galois Groups and Galois Extensions 340
15.2 Characterization of Galois Extensions 345
15.3 The Fundamental Theorem of Galois Theory 350
15.4 Galois Groups of Polynomials 357
15.5 Solving Polynomial Equations by Radicals 361
15.6 Other Applications 370
Exercises 373

Appendix A Background 377

Appendix B Solutions to Selected Exercises 402

Index of Definitions 461
Index of Theorems 463
Subject Index 465

© in this web service Cambridge University Press