

Contents

Preface	xi
Chapter 1. Arithmetic	1
1. Integers	1
1.1. Basic Properties	1
1.2. Induction	2
1.3. Division Algorithm	4
1.4. Divisors	5
1.5. Fundamental Theorem of Arithmetic	8
1.6. Exercises 1.1–1.28	9
2. Modular Arithmetic	13
2.1. Congruence	13
2.2. Congruence Classes	14
2.3. Arithmetic	15
2.4. Structure	16
2.5. Applications	20
2.6. Equivalence Relations	24
2.7. Exercises 1.29–1.72	26
Chapter 2. Groups	33
1. Definitions and Examples	33
1.1. Binary Operations	33
1.2. Definition of a Group	34
1.3. Examples	35
1.4. Exercises 2.1–2.29	41
2. Basic Properties and Order	46
2.1. Exercises 2.30–2.52	48
3. Subgroups and Direct Products	51
3.1. Subgroups	51
3.2. Direct Products	54
3.3. Exercises 2.53–2.91	54
4. Morphisms	59
4.1. Introduction	59
4.2. Definitions and Examples	60
4.3. Basic Properties	62
4.4. Exercises 2.92–2.118	63

5. Quotients	66
5.1. Definitions	66
5.2. Lagrange's Theorem	68
5.3. Normality	69
5.4. Direct Products and the Correspondence Theorem	72
5.5. First Isomorphism Theorem	73
5.6. Exercises 2.119–2.169	74
6. Fundamental Theorem of Finite Abelian Groups	81
6.1. Exercises 2.170–2.188	85
7. The Symmetric Group	89
7.1. Cayley's Theorem	89
7.2. Cyclic Decomposition	90
7.3. Conjugacy Classes	93
7.4. Parity and the Alternating Subgroup	95
7.5. Exercises 2.189–2.229	97
8. Group Actions	103
8.1. Exercises 2.230–2.248	109
9. Sylow Theorems	113
9.1. Exercises 2.249–2.281	118
10. Simple Groups and Composition Series	123
10.1. Simple Groups	123
10.2. Composition Series	126
10.3. Exercises 2.282–2.301	128
Chapter 3. Rings	131
1. Examples and Basic Properties	131
1.1. Definition	131
1.2. Examples	132
1.3. Basic Properties	132
1.4. Subrings	134
1.5. Direct Products	135
1.6. Exercises 3.1–3.39	136
2. Morphisms and Quotients	141
2.1. Morphisms	141
2.2. Ideals	143
2.3. Quotients	144
2.4. Isomorphism Theorem	147
2.5. Exercises 3.40–3.86	147
3. Polynomials and Roots	155
3.1. Division Algorithm	157
3.2. Roots	158
3.3. Rational Root Test	160
3.4. Fundamental Theorem of Algebra	161
3.5. Exercises 3.87–3.129	162

4. Polynomials and Irreducibility	169
4.1. Irreducibility	169
4.2. Polynomials over a Field	169
4.3. Exercises 3.130–3.150	172
5. Factorization	174
5.1. Unique Factorization	175
5.2. Quotient Fields	178
5.3. Unique Factorization in Polynomial Rings	179
5.4. Exercises 3.151–3.172	181
6. Principal Ideal and Euclidean Domains	183
6.1. Principal Ideal Domains	183
6.2. Euclidean Domains	184
6.3. Gaussian Integers	185
6.4. Exercises 3.173–3.201	186
Chapter 4. Field Theory	193
1. Finite and Algebraic Extensions	193
1.1. Vector Spaces	193
1.2. Finite and Algebraic Extensions	196
1.3. Exercises 4.1–4.34	200
2. Splitting Fields	204
2.1. Splitting Fields	204
2.2. Algebraic Closures	208
2.3. Exercises 4.35–4.62	211
3. Finite Fields	215
3.1. Exercises 4.63–4.81	217
4. Galois Theory	219
4.1. Galois Groups	219
4.2. Separability	222
4.3. Galois Correspondence	223
4.4. Exercises 4.82–4.135	229
5. Famous Impossibilities	236
5.1. Compass and Straightedge Constructions	236
5.2. Solvability of Polynomials	239
5.3. Exercises 4.136–4.162	243
6. Cyclotomic Fields	245
6.1. Exercises 4.163–4.179	247
Index	251