

---

# Contents

<i>Preface</i>	v
<b>1 Preliminaries</b>	<b>1</b>
1.1 Basic Ideas of Set Theory . . . . .	2
1.2 Functions . . . . .	7
1.3 Equivalence Relations and Partitions . . . . .	11
1.4 A Note on Natural Numbers . . . . .	14
Review Exercises . . . . .	16
<b>2 Algebraic Structure of Numbers</b>	<b>17</b>
2.1 The Set of Integers . . . . .	18
2.2 Congruences of Integers . . . . .	21
2.3 Rational Numbers . . . . .	28
Review Exercises . . . . .	33
<b>3 Basic Notions of Groups</b>	<b>35</b>
3.1 Definitions and Examples . . . . .	36
3.2 Basic Properties . . . . .	41
3.3 Subgroups . . . . .	45
3.4 Generating Sets . . . . .	48

Review Exercises . . . . .	51
<b>4 Cyclic Groups</b>	<b>53</b>
4.1 Cyclic Groups . . . . .	54
4.2 Subgroups of Cyclic Groups . . . . .	57
Review Exercises . . . . .	63
<b>5 Permutation Groups</b>	<b>65</b>
5.1 Symmetric Groups . . . . .	66
5.2 Dihedral Groups . . . . .	71
5.3 Alternating Groups . . . . .	76
Review Exercises . . . . .	79
<b>6 Counting Theorems</b>	<b>81</b>
6.1 Lagrange's Theorem . . . . .	82
6.2 Conjugacy Classes of a Group . . . . .	87
Review Exercises . . . . .	93
<b>7 Group Homomorphisms</b>	<b>95</b>
7.1 Examples and Basic Properties . . . . .	96
7.2 Isomorphisms . . . . .	99
7.3 Cayley's Theorem . . . . .	105
Review Exercises . . . . .	108
<b>8 The Quotient Group</b>	<b>109</b>
8.1 Normal Subgroups . . . . .	110
8.2 Quotient Groups . . . . .	114
8.3 Fundamental Theorem of Group Homomorphisms . . . . .	119
Review Exercises . . . . .	125
<b>9 Finite Abelian Groups</b>	<b>127</b>
9.1 Direct Products of Groups . . . . .	128
9.2 Cauchy's Theorem . . . . .	133
9.3 Structure Theorem of Finite Abelian Groups . . . . .	137
Review Exercises . . . . .	142

<b>10 Sylow Theorems and Applications</b>	<b>143</b>
10.1 Group Actions . . . . .	144
10.2 Sylow Theorems . . . . .	151
Review Exercises . . . . .	157
<b>11 Introduction to Group Presentations</b>	<b>159</b>
11.1 Free Groups and Free Abelian Groups . . . . .	160
11.2 Generators and Relations . . . . .	165
11.3 Classification of Finite Groups of Small Orders . . . . .	170
Review Exercises . . . . .	175
<b>12 Types of Rings</b>	<b>177</b>
12.1 Definitions and Examples . . . . .	178
12.2 Matrix Rings . . . . .	185
Review Exercises . . . . .	191
<b>13 Ideals and Quotient Rings</b>	<b>193</b>
13.1 Ideals . . . . .	194
13.2 Quotient Rings . . . . .	198
Review Exercises . . . . .	203
<b>14 Ring Homomorphisms</b>	<b>205</b>
14.1 Ring Homomorphisms . . . . .	206
14.2 Direct Products of Rings . . . . .	211
14.3 The Quotient Field of an Integral Domain . . . . .	216
Review Exercises . . . . .	222
<b>15 Polynomial Rings</b>	<b>223</b>
15.1 Polynomial Rings in the Indeterminates . . . . .	224
15.2 Properties of the Polynomial Rings of One Variable . . . . .	228
15.3 Principal Ideal Domains and Euclidean Domains . . . . .	233
Review Exercises . . . . .	237
<b>16 Factorization</b>	<b>239</b>
16.1 Irreducible and Prime Elements . . . . .	240
16.2 Unique Factorization Domains . . . . .	245
16.3 Polynomial Extensions of Factorial Domains . . . . .	253

Review Exercises . . . . .	259
<b>17 Vector Spaces Over an Arbitrary Field</b>	<b>261</b>
17.1 A Brief Review on Vector Spaces . . . . .	262
17.2 A Brief Review on Linear Transformations . . . . .	266
Review Exercises . . . . .	272
<b>18 Field Extensions</b>	<b>273</b>
18.1 Algebraic or Transcendental? . . . . .	274
18.2 Finite and Algebraic Extensions . . . . .	278
18.3 Construction with Straightedge and Compass . . . . .	284
Review Exercises . . . . .	294
<b>19 All About Roots</b>	<b>295</b>
19.1 Zeros of Polynomials . . . . .	296
19.2 Uniqueness of Splitting Fields . . . . .	299
19.3 Algebraically Closed Fields . . . . .	303
19.4 Multiplicity of Roots . . . . .	305
19.5 Finite Fields . . . . .	309
Review Exercises . . . . .	314
<b>20 Galois Pairing</b>	<b>315</b>
20.1 Galois Groups . . . . .	316
20.2 The Fixed Subfields of a Galois Group . . . . .	321
20.3 Fundamental Theorem of Galois Pairing . . . . .	326
Review Exercises . . . . .	331
<b>21 Applications of the Galois Pairing</b>	<b>333</b>
21.1 Fields of Invariants . . . . .	334
21.2 Solvable Groups . . . . .	338
21.3 Insolvability of the Quintic . . . . .	345
Review Exercises . . . . .	350
<b><i>Index</i></b>	<b>351</b>