

Contents

Preface	xi
For the student	xi
For the instructor	xi
Note about rings	xiii
Road map	xiii
Acknowledgments	xiv
Unit I: Preliminaries	1
1 Introduction to Proofs	3
1.1 Proving an implication	3
1.2 Proof by cases	4
1.3 Contrapositive	6
1.4 Proof by contradiction	7
1.5 If and only if	8
1.6 Counterexample	9
Exercises	9
2 Sets and Subsets	13
2.1 What is a set?	13
2.2 Set of integers and its subsets	14
2.3 Closure	15
2.4 Showing set equality	17
Exercises	18
3 Divisors	21
3.1 Divisor	21
3.2 GCD theorem	22
3.3 Proofs involving the GCD theorem	23
Exercises	25
Unit II: Examples of Groups	29
4 Modular Arithmetic	31
4.1 Number system \mathbb{Z}_7	31
4.2 Equality in \mathbb{Z}_7	32
4.3 Multiplicative inverses	34
Exercises	37

5 Symmetries	41
5.1 Symmetries of a square	41
5.2 Group properties of D_4	44
5.3 Centralizer	45
Exercises	47
6 Permutations	51
6.1 Permutations of the set $\{1, 2, 3\}$	51
6.2 Group properties of S_n	53
6.3 Computations in S_n	54
6.4 Associative law in S_n (and in D_n)	56
Exercises	56
7 Matrices	61
7.1 Matrix arithmetic	61
7.2 Matrix group $M(\mathbb{Z}_{10})$	62
7.3 Multiplicative inverses	64
7.4 Determinant	65
Exercises	68
Unit III: Introduction to Groups	71
8 Introduction to Groups	73
8.1 Definition of a “group”	73
8.2 Essential properties of a group	76
8.3 Proving that a group is commutative	80
8.4 Non-associative operations	81
8.5 Direct product	81
Exercises	83
9 Groups of Small Size	87
9.1 Smallest group	87
9.2 Groups with two elements	88
9.3 Groups with three elements	90
9.4 Sudoku property	91
9.5 Groups with four elements	92
Exercises	93
10 Matrix Groups	97
10.1 Groups \mathbb{Z}_{10} and U_{10}	97
10.2 Groups $M(\mathbb{Z}_{10})$ and $G(\mathbb{Z}_{10})$	98
10.3 Group $S(\mathbb{Z}_{10})$	100
Exercises	101
11 Subgroups	105
11.1 Examples of subgroups	105
11.2 Subgroup proofs	107
11.3 Center and centralizer revisited	109
Exercises	110

Contents	vii
12 Order of an Element	115
12.1 Motivating example	115
12.2 When does $g^k = \varepsilon$?	116
12.3 Conjugates	118
12.4 Order in an additive group	120
12.5 Elements with infinite order	121
Exercises	122
13 Cyclic Groups, Part I	125
13.1 Generators of the additive group \mathbb{Z}_{12}	125
13.2 Generators of the multiplicative group U_{13}	127
13.3 Matching \mathbb{Z}_{12} and U_{13}	128
13.4 Taking positive and <i>negative</i> powers of g	129
13.5 When the group operation is addition	131
Exercises	132
14 Cyclic Groups, Part II	135
14.1 Why negative powers are needed	135
14.2 Additive groups revisited	136
14.3 $\langle 3 \rangle$ behaves “just like” \mathbb{Z}	137
14.4 Subgroups of cyclic groups	138
Exercises	141
Unit IV: Group Homomorphisms	145
15 Functions	147
15.1 Domain and codomain	147
15.2 One-to-one function	148
15.3 Onto function	149
15.4 When domain and codomain have the same size	152
Exercises	153
16 Isomorphisms	157
16.1 Groups \mathbb{Z}_{12} and $\langle g \rangle$: Elements match up	157
16.2 Groups \mathbb{Z}_{12} and $\langle g \rangle$: Operations match up	158
16.3 Elements with infinite order revisited	161
16.4 Inverse isomorphisms	162
Exercises	164
17 Homomorphisms, Part I	169
17.1 Group homomorphism	169
17.2 Properties of homomorphisms	172
17.3 Order of an element	174
Exercises	175
18 Homomorphisms, Part II	179
18.1 Kernel of a homomorphism	179
18.2 Image of a homomorphism	182
18.3 Partitioning the domain	183

18.4 Finding homomorphisms	184
Exercises	185
Unit V: Quotient Groups	189
19 Introduction to Cosets	191
19.1 Multiplicative group example	191
19.2 Additive group example	193
19.3 Right cosets	195
19.4 Properties of cosets	196
19.5 When are cosets equal?	198
Exercises	200
20 Lagrange's Theorem	205
20.1 Motivating Lagrange's theorem	205
20.2 Proving Lagrange's theorem	207
20.3 Applications of Lagrange's theorem	209
Exercises	211
21 Multiplying/Adding Cosets	213
21.1 Turning a set of cosets into a group	213
21.2 Coset multiplication shortcut	216
21.3 Cosets of $H = 5\mathbb{Z}$ in \mathbb{Z} revisited	217
Exercises	219
22 Quotient Group Examples	223
22.1 Quotient group U_{13}/H revisited	223
22.2 Quotient group U_{37}/H	224
22.3 Quotient group G/H (generalization)	225
Exercises	227
23 Quotient Group Proofs	231
23.1 Sample quotient group proofs	231
23.2 Collapsing G into G/H	234
Exercises	236
24 Normal Subgroups	239
24.1 How does the shortcut fail and work?	239
24.2 Normal subgroups: What and why	241
24.3 Examples of normal subgroups	241
24.4 Normal subgroup test	242
Exercises	245
25 First Isomorphism Theorem	249
25.1 Familiar homomorphism	249
25.2 Another homomorphism	251
25.3 First Isomorphism Theorem	253
25.4 Finding and building homomorphisms	253
Exercises	255

Contents	ix
Unit VI: Introduction to Rings	259
26 Introduction to Rings	261
26.1 Examples and definition	261
26.2 Fundamental properties	264
26.3 Units and zero divisors	266
26.4 Subrings	267
26.5 Group of units	268
Exercises	269
27 Integral Domains and Fields	271
27.1 Integral domains	271
27.2 Fields	273
27.3 Idempotent elements	276
Exercises	277
28 Polynomial Rings, Part I	281
28.1 Examples and definition	281
28.2 Degree of a polynomial	283
28.3 Units and zero divisors	286
Exercises	287
29 Polynomial Rings, Part II	289
29.1 Division algorithm in $F[x]$	289
29.2 Factor theorem	291
29.3 Nilpotent elements	293
Big picture stuff	295
Exercises	295
30 Factoring Polynomials	299
30.1 Examples and definition	299
30.2 Factorable or unfactorable?	301
Big picture stuff	304
Exercises	304
Unit VII: Quotient Rings	309
31 Ring Homomorphisms	311
31.1 Evaluation map	311
31.2 Properties of ring homomorphisms	314
31.3 Kernel and image	315
31.4 Examples and definition of an ideal	316
31.5 Ideals in \mathbb{Z} and in $F[x]$	319
Big picture stuff	319
Exercises	320
32 Introduction to Quotient Rings	323
32.1 From a quotient group to a quotient ring	323
32.2 Role of an ideal in a quotient ring	324
32.3 Quotient ring $\mathbb{Z}_3[x]/\langle x^2 \rangle$	327

32.4	First Isomorphism Theorem for rings	328
	Big picture stuff	329
	Exercises	329
33	Quotient Ring $\mathbb{Z}_7[x]/\langle x^2 - 1 \rangle$	333
33.1	Division algorithm revisited	333
33.2	Another way to reduce in $\mathbb{Z}_7[x]/\langle x^2 - 1 \rangle$	336
33.3	$F[x]/\langle g(x) \rangle$ is <i>not</i> a field	337
33.4	$F[x]/\langle g(x) \rangle$ is a field	338
	Big picture stuff	338
	Exercises	338
34	Quotient Ring $\mathbb{R}[x]/\langle x^2 + 1 \rangle$	343
34.1	Reducing elements in $\mathbb{R}[x]/\langle x^2 + 1 \rangle$	343
34.2	Field of complex numbers	344
34.3	$F[x]/\langle g(x) \rangle$ is a field revisited	347
	Exercises	347
35	$F[x]/\langle g(x) \rangle$ Is/Isn't a Field, Part I	351
35.1	Translate from $F[x]$ to \mathbb{Z}	351
35.2	Translate (back) from \mathbb{Z} to $F[x]$	353
35.3	Proof of Theorem 35.1(b)	355
	Big picture stuff	355
	Exercises	356
36	Maximal Ideals	359
36.1	Examples and definition	360
36.2	Maximality of $\langle g(x) \rangle$	362
	Big picture stuff	364
	Exercises	364
37	$F[x]/\langle g(x) \rangle$ Is/Isn't a Field, Part II	367
37.1	Maximal ideals and quotient rings	367
37.2	Putting it all together	369
37.3	Oh wait, but there's more!	370
37.4	Prime ideals	370
	Exercises	371
A	Proof of the GCD Theorem	373
B	Composition Table for D_4	377
C	Symbols and Notations	379
D	Essential Theorems	381
	Index of Terms	385