

**A First Course
in Abstract Algebra**
Rings, Groups, and Fields
Second Edition

Marlow Anderson
Todd Feil

Contents

Preface	xiii
---------	------

I Numbers, Polynomials, and Factoring

1 The Natural Numbers	3
1.1 Operations on the Natural Numbers	3
1.2 Well Ordering and Mathematical Induction	4
1.3 The Fibonacci Sequence	7
1.4 Well Ordering Implies Mathematical Induction	9
1.5 The Axiomatic Method	9
2 The Integers	15
2.1 The Division Theorem	15
2.2 The Greatest Common Divisor	17
2.3 The GCD Identity	20
2.4 The Fundamental Theorem of Arithmetic	22
2.5 A Geometric Interpretation	24
3 Modular Arithmetic	31
3.1 Residue Classes	31
3.2 Arithmetic on the Residue Classes	34
3.3 Properties of Modular Arithmetic	36
4 Polynomials with Rational Coefficients	41
4.1 Polynomials	41
4.2 The Algebra of Polynomials	43
4.3 The Analogy between \mathbb{Z} and $\mathbb{Q}[x]$	45
4.4 Factors of a Polynomial	47
4.5 Linear Factors	47
4.6 Greatest Common Divisors	49

5	Factorization of Polynomials	55
5.1	Factoring Polynomials	55
5.2	Unique Factorization	57
5.3	Polynomials with Integer Coefficients	59

Section I in a Nutshell	69
--------------------------------	-----------

II Rings, Domains, and Fields

6	Rings	73
6.1	Binary Operations	73
6.2	Rings	74
6.3	Arithmetic in a Ring	80
6.4	Notational Conventions	81
6.5	The Set of Integers is a Ring	82

7	Subrings and Unity	89
7.1	Subrings	89
7.2	The Multiplicative Identity	93

8	Integral Domains and Fields	101
8.1	Zero Divisors	101
8.2	Units	103
8.3	Fields	105
8.4	The Field of Complex Numbers	105
8.5	Finite Fields	110

9	Polynomials over a Field	119
9.1	Polynomials with Coefficients from an Arbitrary Field	119
9.2	Polynomials with Complex Coefficients	121
9.3	Irreducibles in $\mathbb{R}[x]$	124
9.4	Extraction of Square Roots in \mathbb{C}	125

Section II in a Nutshell	135
---------------------------------	------------

III Unique Factorization

10	Associates and Irreducibles	141
10.1	Associates	141
10.2	Irreducibles	142
10.3	Quadratic Extensions of the Integers	144

10.4	Units in Quadratic Extensions	145
10.5	Irreducibles in Quadratic Extensions	149
11	Factorization and Ideals	155
11.1	Factorization for Quadratic Extensions	155
11.2	How Might Factorization Fail?	157
11.3	Ideals	158
11.4	Principal Ideals	160
12	Principal Ideal Domains	169
12.1	Ideals that are not Principal	169
12.2	Principal Ideal Domains	171
13	Primes and Unique Factorization	177
13.1	Primes	177
13.2	UFDs	179
13.3	Expressing Properties of Elements in Terms of Ideals	180
13.4	Ideals in $\mathbb{Z}[\sqrt{-5}]$	183
13.5	A Comparison between \mathbb{Z} and $\mathbb{Z}[\sqrt{-5}]$	183
13.6	All PIDs are UFDs	184
14	Polynomials with Integer Coefficients	189
14.1	The Proof that $\mathbb{Q}[x]$ is a UFD	189
14.2	Factoring Integers out of Polynomials	190
14.3	The Content of a Polynomial	191
14.4	Irreducibles in $\mathbb{Z}[x]$ are Prime	193
15	Euclidean Domains	197
15.1	Euclidean Domains	197
15.2	The Gaussian Integers	199
15.3	Euclidean Domains are PIDs	201
15.4	Some PIDs are not Euclidean	203
	Section III in a Nutshell	207

IV Ring Homomorphisms and Ideals

16	Ring Homomorphisms	211
16.1	Homomorphisms	211
16.2	One-to-one and Onto Functions	214
16.3	Properties Preserved by Homomorphisms	215

16.4	More Examples	216
16.5	Making a Homomorphism Onto	218
17	The Kernel	225
17.1	Ideals	226
17.2	The Kernel	226
17.3	The Kernel is an Ideal	228
17.4	All Pre-images Can Be Obtained from the Kernel	229
17.5	When is the Kernel Trivial?	232
17.6	A Summary and Example	232
18	Rings of Cosets	237
18.1	The Ring of Cosets	237
18.2	The Natural Homomorphism	240
19	The Isomorphism Theorem for Rings	247
19.1	Isomorphism	247
19.2	The Fundamental Isomorphism Theorem	249
19.3	Examples	251
20	Maximal and Prime Ideals	259
20.1	Maximal Ideals	259
20.2	Prime Ideals	262
21	The Chinese Remainder Theorem	271
21.1	Direct Products of Domains	271
21.2	Chinese Remainder Theorem	274
	Section IV in a Nutshell	283
V Groups		
22	Symmetries of Figures in the Plane	287
22.1	Symmetries of the Equilateral Triangle	287
22.2	Permutation Notation	290
22.3	Matrix Notation	292
22.4	Symmetries of the Square	294
23	Symmetries of Figures in Space	299
23.1	Symmetries of the Regular Tetrahedron	300
23.2	Symmetries of the Cube	304

24 Abstract Groups	313
24.1 Definition of Group	314
24.2 Examples of Groups	314
24.3 Multiplicative Groups	316
25 Subgroups	329
25.1 Arithmetic in an Abstract Group	329
25.2 Notation	330
25.3 Subgroups	331
25.4 Characterization of Subgroups	333
26 Cyclic Groups	339
26.1 The Order of an Element	339
26.2 Rule of Exponents	342
26.3 Cyclic Subgroups	345
26.4 Cyclic Groups	347
Section V in a Nutshell	353
 VI Group Homomorphisms and Permutations	
27 Group Homomorphisms	357
27.1 Homomorphisms	357
27.2 Examples	358
27.3 Direct Products	361
28 Group Isomorphisms	367
28.1 Structure Preserved by Homomorphisms	368
28.2 Uniqueness of Cyclic Groups	369
28.3 Symmetry Groups	371
28.4 Characterizing Direct Products	372
29 Permutations and Cayley's Theorem	379
29.1 Permutations	379
29.2 The Symmetric Groups	380
29.3 Cayley's Theorem	383
30 More About Permutations	389
30.1 Cycles	389
30.2 Cycle Factorization of Permutations	391
30.3 Orders of Permutations	394

31 Cosets and Lagrange's Theorem	399
31.1 Cosets	399
31.2 Lagrange's Theorem	401
31.3 Applications of Lagrange's Theorem	404
32 Groups of Cosets	413
32.1 Left Cosets	414
32.2 Normal Subgroups	415
32.3 Examples of Groups of Cosets	417
33 The Isomorphism Theorem for Groups	425
33.1 The Kernel	425
33.2 Cosets of the Kernel	428
33.3 The Fundamental Theorem	429
34 The Alternating Groups	435
34.1 Transpositions	435
34.2 The Parity of a Permutation	436
34.3 The Alternating Groups	438
34.4 The Alternating Subgroup is Normal	439
34.5 Simple Groups	442
35 Fundamental Theorem for Finite Abelian Groups	449
35.1 The Fundamental Theorem	449
35.2 p -groups	452
36 Solvable Groups	455
36.1 Solvability	455
36.2 New Solvable Groups from Old	457
Section VI in a Nutshell	461

VII Constructibility Problems

37 Constructions with Compass and Straightedge	465
37.1 Construction Problems	465
37.2 Constructible Lengths and Numbers	467
38 Constructibility and Quadratic Field Extensions	475
38.1 Quadratic Field Extensions	475
38.2 Sequences of Quadratic Field Extensions	477

38.3	The Rational Plane	479
38.4	Planes of Constructible Numbers	480
38.5	The Constructible Number Theorem	484
39	The Impossibility of Certain Constructions	489
39.1	Doubling the Cube	489
39.2	Trisecting the Angle	490
39.3	Squaring the Circle	493
	Section VII in a Nutshell	499
VIII Vector Spaces and Field Extensions		
40	Vector Spaces I	503
40.1	Vectors	504
40.2	Vector Spaces	505
41	Vector Spaces II	511
41.1	Spanning Sets	511
41.2	A Basis for a Vector Space	514
41.3	Finding a Basis	518
41.4	Dimension of a Vector Space	520
42	Field Extensions and Kronecker's Theorem	527
42.1	Field Extensions	527
42.2	Kronecker's Theorem	528
42.3	The Characteristic of a Field	530
43	Algebraic Field Extensions	537
43.1	The Minimal Polynomial for an Element	537
43.2	Simple Extensions	539
43.3	Simple Transcendental Extensions	544
43.4	Dimension of Simple Algebraic Extensions	545
44	Finite Extensions and Constructibility Revisited	551
44.1	Finite Extensions	551
44.2	Constructibility Problems	556
	Section VIII in a Nutshell	561

IX Galois Theory

45 The Splitting Field	565
45.1 The Splitting Field	566
45.2 Fields with Characteristic Zero	570
46 Finite Fields	577
46.1 Existence and Uniqueness	577
46.2 Examples	580
47 Galois Groups	585
47.1 The Galois Group	585
47.2 Galois Groups of Splitting Fields	588
48 The Fundamental Theorem of Galois Theory	599
48.1 Subgroups and Subfields	599
48.2 Symmetric Polynomials	601
48.3 The Fixed Field and Normal Extensions	602
48.4 The Fundamental Theorem	604
48.5 Examples	607
49 Solving Polynomials by Radicals	615
49.1 Field Extensions by Radicals	615
49.2 Refining the Root Tower	618
49.3 Solvable Galois Groups	622
Section IX in a Nutshell	629
Hints and Solutions	633
Guide to Notation	661
Index	665