

Contents

Preface — V

1 Groups, Rings and Fields — 1

- 1.1 Abstract Algebra — 1
- 1.2 Rings — 2
- 1.3 Integral Domains and Fields — 3
- 1.4 Subrings and Ideals — 6
- 1.5 Factor Rings and Ring Homomorphisms — 9
- 1.6 Fields of Fractions — 12
- 1.7 Characteristic and Prime Rings — 14
- 1.8 Groups — 16
- 1.9 Exercises — 18

2 Maximal and Prime Ideals — 20

- 2.1 Maximal and Prime Ideals of the Integers — 20
- 2.2 Prime Ideals and Integral Domains — 21
- 2.3 Maximal Ideals and Fields — 23
- 2.4 The Existence of Maximal Ideals — 24
- 2.5 Principal Ideals and Principal Ideal Domains — 25
- 2.6 Exercises — 27

3 Prime Elements and Unique Factorization Domains — 28

- 3.1 The Fundamental Theorem of Arithmetic — 28
- 3.2 Prime Elements, Units and Irreducibles — 34
- 3.3 Unique Factorization Domains — 37
- 3.4 Principal Ideal Domains and Unique Factorization — 40
- 3.5 Euclidean Domains — 43
- 3.6 Overview of Integral Domains — 48
- 3.7 Exercises — 49

4 Polynomials and Polynomial Rings — 51

- 4.1 Degrees, Reducibility and Roots — 51
- 4.2 Polynomial Rings over Fields — 53
- 4.3 Polynomial Rings over Integral Domains — 55
- 4.4 Polynomial Rings over Unique Factorization Domains — 57
- 4.5 Exercises — 63

5 Field Extensions — 65

- 5.1 Extension Fields and Finite Extensions — 65
- 5.2 Finite and Algebraic Extensions — 68

5.3	Minimal Polynomials and Simple Extensions —	69
5.4	Algebraic Closures —	72
5.5	Algebraic and Transcendental Numbers —	73
5.6	Exercises —	76
6	Field Extensions and Compass and Straightedge Constructions —	78
6.1	Geometric Constructions —	78
6.2	Constructible Numbers and Field Extensions —	78
6.3	Four Classical Construction Problems —	80
6.3.1	Squaring the Circle —	81
6.3.2	The Doubling of the Cube —	81
6.3.3	The Trisection of an Angle —	81
6.3.4	Construction of a Regular n -Gon —	82
6.4	Exercises —	86
7	Kronecker's Theorem and Algebraic Closures —	88
7.1	Kronecker's Theorem —	88
7.2	Algebraic Closures and Algebraically Closed Fields —	91
7.3	The Fundamental Theorem of Algebra —	96
7.3.1	Splitting Fields —	97
7.3.2	Permutations and Symmetric Polynomials —	97
7.4	The Fundamental Theorem of Symmetric Polynomials —	104
7.5	Skew Field Extensions of $\mathbb{C}$ and the Frobenius Theorem —	107
7.6	Exercises —	111
8	Splitting Fields and Normal Extensions —	113
8.1	Splitting Fields —	113
8.2	Normal Extensions —	115
8.3	Exercises —	118
9	Groups, Subgroups and Examples —	119
9.1	Groups, Subgroups and Isomorphisms —	119
9.2	Examples of Groups —	121
9.3	Permutation Groups —	124
9.4	Cosets and Lagrange's Theorem —	127
9.5	Generators and Cyclic Groups —	132
9.6	Exercises —	138
10	Normal Subgroups, Factor Groups and Direct Products —	140
10.1	Normal Subgroups and Factor Groups —	140
10.2	The Group Isomorphism Theorems —	144
10.3	Direct Products of Groups —	148

10.4	Finite Abelian Groups —	149
10.5	Some Properties of Finite Groups —	154
10.6	Automorphisms of a Group —	158
10.7	Exercises —	160
11	Symmetric and Alternating Groups —	161
11.1	Symmetric Groups and Cycle Decomposition —	161
11.2	Parity and the Alternating Groups —	164
11.3	The Conjugation in S_n —	167
11.4	The Simplicity of A_n —	168
11.5	Exercises —	171
12	Solvable Groups —	172
12.1	Solvability and Solvable Groups —	172
12.2	The Derived Series —	176
12.3	Composition Series and the Jordan–Hölder Theorem —	177
12.4	Exercises —	179
13	Group Actions and the Sylow Theorems —	181
13.1	Group Actions —	181
13.2	Conjugacy Classes and the Class Equation —	182
13.3	The Sylow Theorems —	184
13.4	Some Applications of the Sylow Theorems —	188
13.5	Exercises —	192
14	Free Groups and Group Presentations —	193
14.1	Group Presentations and Combinatorial Group Theory —	193
14.2	Free Groups —	194
14.3	Group Presentations —	199
14.3.1	The Modular Group —	201
14.4	Presentations of Subgroups —	208
14.5	Geometric Interpretation —	210
14.6	Presentations of Factor Groups —	217
14.7	Decision Problems —	217
14.8	Group Amalgams: Free Products and Direct Products —	218
14.9	Exercises —	220
15	Finite Galois Extensions —	221
15.1	Galois Theory and the Solvability of Polynomial Equations —	221
15.2	Automorphism Groups of Field Extensions —	221
15.3	Finite Galois Extensions —	224
15.4	The Fundamental Theorem of Galois Theory —	225

15.5	Exercises —	234
16	Separable Field Extensions —	235
16.1	Separability of Fields and Polynomials —	235
16.2	Perfect Fields —	236
16.3	Finite Fields —	238
16.4	Separable Extensions —	239
16.5	Separability and Galois Extensions —	242
16.6	The Primitive Element Theorem —	246
16.7	Exercises —	248
17	Applications of Galois Theory —	249
17.1	Field Extensions by Radicals —	249
17.2	Cyclotomic Extensions —	253
17.3	Solvability and Galois Extensions —	254
17.4	The Insolvability of the Quintic Polynomial —	255
17.5	Constructibility of Regular n -Gons —	261
17.6	The Fundamental Theorem of Algebra —	263
17.7	Exercises —	264
18	The Theory of Modules —	267
18.1	Modules over Rings —	267
18.2	Annihilators and Torsion —	271
18.3	Direct Products and Direct Sums of Modules —	272
18.4	Free Modules —	274
18.5	Modules over Principal Ideal Domains —	277
18.6	The Fundamental Theorem for Finitely Generated Modules —	280
18.7	Exercises —	284
19	Finitely Generated Abelian Groups —	286
19.1	Finite Abelian Groups —	286
19.2	The Fundamental Theorem: p -Primary Components —	287
19.3	The Fundamental Theorem: Elementary Divisors —	288
19.4	Exercises —	294
20	Integral and Transcendental Extensions —	295
20.1	The Ring of Algebraic Integers —	295
20.2	Integral Ring Extensions —	298
20.3	Transcendental Field Extensions —	302
20.4	The Transcendence of e and π —	307
20.5	Exercises —	310

21	The Hilbert Basis Theorem and the Nullstellensatz — 312
21.1	Algebraic Geometry — 312
21.2	Algebraic Varieties and Radicals — 312
21.3	The Hilbert Basis Theorem — 314
21.4	The Nullstellensatz — 315
21.5	Applications and Consequences of Hilbert's Theorems — 316
21.6	Dimensions — 319
21.7	Exercises — 324
22	Algebras and Group Representations — 325
22.1	Group Representations — 325
22.2	Representations and Modules — 326
22.3	Semisimple Algebras and Wedderburn's Theorem — 334
22.4	Ordinary Representations, Characters and Character Theory — 342
22.5	Burnside's Theorem — 350
22.6	Exercises — 354
23	Algebraic Cryptography — 356
23.1	Basic Algebraic Cryptography — 356
23.1.1	Cryptosystems Tied to Abelian Groups — 356
23.1.2	Cryptographic Protocols — 364
24	Non-Commutative Group Based Cryptography — 369
24.1	Group Based Methods — 369
24.2	Initial Group Theoretic Cryptosystems—The Magnus Method — 372
24.2.1	The Wagner–Magyarik Method — 374
24.3	Free Group Cryptosystems — 375
24.4	Non-Abelian Digital Signature Procedure — 379
24.5	Password Authentication Using Combinatorial Group Theory — 380
24.5.1	General Outline of the Authentication Protocol — 382
24.5.2	Free Subgroup Method — 382
24.5.3	General Finitely Presented Group Method — 383
24.6	The Strong Generic Free Group Property — 384
24.6.1	Security Analysis of the Group Randomizer Protocols — 389
24.6.2	Implementation of a Group Randomizer System Protocol — 390
24.7	A Secret Sharing Scheme Using Combinatorial Group Theory — 390
24.8	Ko–Lee and Anshel–Anshel–Goldfeld Protocols — 393
24.8.1	The Ko–Lee Protocol — 394
24.8.2	The Anshel–Anshel–Goldfeld Protocol — 396

XII — Contents

Bibliography — 403

Index — 407