

Contents

Preface — V

Preface to the second edition — VII

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 — 13
- 1.7 Characteristic and prime rings — 14
- 1.8 Groups — 16
- 1.9 Exercises — 19

2 Maximal and prime ideals — 21

- 2.1 Maximal and prime ideals — 21
- 2.2 Prime ideals and integral domains — 22
- 2.3 Maximal ideals and fields — 24
- 2.4 The existence of maximal ideals — 25
- 2.5 Principal ideals and principal ideal domains — 26
- 2.6 Exercises — 28

3 Prime elements and unique factorization domains — 29

- 3.1 The fundamental theorem of arithmetic — 29
- 3.2 Prime elements, units and irreducibles — 34
- 3.3 Unique factorization domains — 38
- 3.4 Principal ideal domains and unique factorization — 41
- 3.5 Euclidean domains — 44
- 3.6 Overview of integral domains — 50
- 3.7 Exercises — 50

4 Polynomials and polynomial rings — 53

- 4.1 Polynomials and polynomial rings — 53
- 4.2 Polynomial rings over fields — 55
- 4.3 Polynomial rings over integral domains — 57
- 4.4 Polynomial rings over unique factorization domains — 59
- 4.5 Exercises — 65

5	Field extensions — 67
5.1	Extension fields and finite extensions — 67
5.2	Finite and algebraic extensions — 70
5.3	Minimal polynomials and simple extensions — 71
5.4	Algebraic closures — 74
5.5	Algebraic and transcendental numbers — 75
5.6	Exercises — 78
6	Field extensions and compass and straightedge constructions — 81
6.1	Geometric constructions — 81
6.2	Constructible numbers and field extensions — 81
6.3	Four classical construction problems — 84
6.3.1	Squaring the circle — 84
6.3.2	The doubling of the cube — 84
6.3.3	The trisection of an angle — 84
6.3.4	Construction of a regular n -gon — 85
6.4	Exercises — 89
7	Kronecker's theorem and algebraic closures — 93
7.1	Kronecker's theorem — 93
7.2	Algebraic closures and algebraically closed fields — 96
7.3	The fundamental theorem of algebra — 101
7.3.1	Splitting fields — 101
7.3.2	Permutations and symmetric polynomials — 102
7.4	The fundamental theorem of algebra — 106
7.5	The fundamental theorem of symmetric polynomials — 109
7.6	Skew field extensions of $\mathbb{C}$ and Frobenius's theorem — 112
7.7	Exercises — 116
8	Splitting fields and normal extensions — 119
8.1	Splitting fields — 119
8.2	Normal extensions — 121
8.3	Exercises — 124
9	Groups, subgroups, and examples — 125
9.1	Groups, subgroups, and isomorphisms — 125
9.2	Examples of groups — 127
9.3	Permutation groups — 130
9.4	Cosets and Lagrange's theorem — 133
9.5	Generators and cyclic groups — 138
9.6	Exercises — 144

10	Normal subgroups, factor groups, and direct products — 147
10.1	Normal subgroups and factor groups — 147
10.2	The group isomorphism theorems — 151
10.3	Direct products of groups — 155
10.4	Finite Abelian groups — 157
10.5	Some properties of finite groups — 161
10.6	Automorphisms of a group — 165
10.7	Exercises — 167
11	Symmetric and alternating groups — 169
11.1	Symmetric groups and cycle decomposition — 169
11.2	Parity and the alternating groups — 172
11.3	Conjugation in S_n — 174
11.4	The simplicity of A_n — 175
11.5	Exercises — 178
12	Solvable groups — 179
12.1	Solvability and solvable groups — 179
12.2	Solvable groups — 179
12.3	The derived series — 183
12.4	Composition series and the Jordan–Hölder theorem — 185
12.5	Exercises — 186
13	Groups actions and the Sylow theorems — 189
13.1	Group actions — 189
13.2	Conjugacy classes and the class equation — 190
13.3	The Sylow theorems — 192
13.4	Some applications of the Sylow theorems — 196
13.5	Exercises — 200
14	Free groups and group presentations — 201
14.1	Group presentations and combinatorial group theory — 201
14.2	Free groups — 202
14.3	Group presentations — 207
14.3.1	The modular group — 209
14.4	Presentations of subgroups — 215
14.5	Geometric interpretation — 218
14.6	Presentations of factor groups — 221
14.7	Group presentations and decision problems — 222
14.8	Group amalgams: free products and direct products — 223
14.9	Exercises — 225

15	Finite Galois extensions — 227
15.1	Galois theory and the solvability of polynomial equations — 227
15.2	Automorphism groups of field extensions — 228
15.3	Finite Galois extensions — 230
15.4	The fundamental theorem of Galois theory — 231
15.5	Exercises — 240
16	Separable field extensions — 243
16.1	Separability of fields and polynomials — 243
16.2	Perfect fields — 244
16.3	Finite fields — 246
16.4	Separable extensions — 247
16.5	Separability and Galois extensions — 250
16.6	The primitive element theorem — 254
16.7	Exercises — 256
17	Applications of Galois theory — 257
17.1	Applications of Galois theory — 257
17.2	Field extensions by radicals — 257
17.3	Cyclotomic extensions — 261
17.4	Solvability and Galois extensions — 262
17.5	The insolubility of the quintic polynomial — 263
17.6	Constructibility of regular n -gons — 269
17.7	The fundamental theorem of algebra — 271
17.8	Exercises — 273
18	The theory of modules — 275
18.1	Modules over rings — 275
18.2	Annihilators and torsion — 279
18.3	Direct products and direct sums of modules — 280
18.4	Free modules — 282
18.5	Modules over principal ideal domains — 285
18.6	The fundamental theorem for finitely generated modules — 288
18.7	Exercises — 292
19	Finitely generated Abelian groups — 293
19.1	Finite Abelian groups — 293
19.2	The fundamental theorem: p -primary components — 294
19.3	The fundamental theorem: elementary divisors — 295
19.4	Exercises — 301
20	Integral and transcendental extensions — 303

20.1	The ring of algebraic integers —	303
20.2	Integral ring extensions —	305
20.3	Transcendental field extensions —	310
20.4	The transcendence of e and π —	315
20.5	Exercises —	318
21	The Hilbert basis theorem and the nullstellensatz —	319
21.1	Algebraic geometry —	319
21.2	Algebraic varieties and radicals —	319
21.3	The Hilbert basis theorem —	321
21.4	The Hilbert nullstellensatz —	322
21.5	Applications and consequences of Hilbert's theorems —	323
21.6	Dimensions —	326
21.7	Exercises —	330
22	Algebras and group representations —	333
22.1	Group representations —	333
22.2	Representations and modules —	334
22.3	Semisimple algebras and Wedderburn's theorem —	342
22.4	Ordinary representations, characters and character theory —	351
22.5	Burnside's theorem —	358
22.6	Exercises —	362
23	Algebraic cryptography —	365
23.1	Basic cryptography —	365
23.2	Encryption and number theory —	370
23.3	Public key cryptography —	375
23.3.1	The Diffie–Hellman protocol —	376
23.3.2	The RSA algorithm —	377
23.3.3	The El-Gamal protocol —	379
23.3.4	Elliptic curves and elliptic curve methods —	381
23.4	Noncommutative-group-based cryptography —	382
23.4.1	Free group cryptosystems —	384
23.5	Ko–Lee and Anshel–Anshel–Goldfeld methods —	389
23.5.1	The Ko–Lee protocol —	389
23.5.2	The Anshel–Anshel–Goldfeld protocol —	390
23.6	Platform groups and braid group cryptography —	391
23.7	Exercises —	395

Bibliography — 399

Index — 403