

Contents

| | |
|--|-----------|
| Preface | v |
| 1 Groups, Rings and Fields | 1 |
| 1.1 Abstract Algebra | 1 |
| 1.2 Rings | 2 |
| 1.3 Integral Domains and Fields | 4 |
| 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 | 17 |
| 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 | 27 |
| 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 | 35 |
| 3.3 Unique Factorization Domains | 38 |
| 3.4 Principal Ideal Domains and Unique Factorization | 41 |
| 3.5 Euclidean Domains | 45 |
| 3.6 Overview of Integral Domains | 51 |
| 3.7 Exercises | 51 |
| 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 | 58 |
| 4.5 Exercises | 65 |

| | | |
|----------|--|------------|
| 5 | Field Extensions | 66 |
| 5.1 | Extension Fields and Finite Extensions | 66 |
| 5.2 | Finite and Algebraic Extensions | 69 |
| 5.3 | Minimal Polynomials and Simple Extensions | 70 |
| 5.4 | Algebraic Closures | 74 |
| 5.5 | Algebraic and Transcendental Numbers | 75 |
| 5.6 | Exercises | 78 |
| 6 | Field Extensions and Compass and Straightedge Constructions | 80 |
| 6.1 | Geometric Constructions | 80 |
| 6.2 | Constructible Numbers and Field Extensions | 80 |
| 6.3 | Four Classical Construction Problems | 83 |
| 6.3.1 | Squaring the Circle | 83 |
| 6.3.2 | The Doubling of the Cube | 83 |
| 6.3.3 | The Trisection of an Angle | 83 |
| 6.3.4 | Construction of a Regular n -Gon | 84 |
| 6.4 | Exercises | 89 |
| 7 | Kronecker's Theorem and Algebraic Closures | 91 |
| 7.1 | Kronecker's Theorem | 91 |
| 7.2 | Algebraic Closures and Algebraically Closed Fields | 94 |
| 7.3 | The Fundamental Theorem of Algebra | 100 |
| 7.3.1 | Splitting Fields | 100 |
| 7.3.2 | Permutations and Symmetric Polynomials | 101 |
| 7.4 | The Fundamental Theorem of Algebra | 105 |
| 7.5 | The Fundamental Theorem of Symmetric Polynomials | 109 |
| 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 | 125 |
| 9.4 | Cosets and Lagrange's Theorem | 128 |
| 9.5 | Generators and Cyclic Groups | 133 |
| 9.6 | Exercises | 139 |

| | |
|---|------------|
| 10 Normal Subgroups, Factor Groups and Direct Products | 141 |
| 10.1 Normal Subgroups and Factor Groups | 141 |
| 10.2 The Group Isomorphism Theorems | 146 |
| 10.3 Direct Products of Groups | 149 |
| 10.4 Finite Abelian Groups | 151 |
| 10.5 Some Properties of Finite Groups | 156 |
| 10.6 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 Conjugation in S_n | 167 |
| 11.4 The Simplicity of A_n | 168 |
| 11.5 Exercises | 170 |
| 12 Solvable Groups | 171 |
| 12.1 Solvability and Solvable Groups | 171 |
| 12.2 Solvable Groups | 172 |
| 12.3 The Derived Series | 175 |
| 12.4 Composition Series and the Jordan–Hölder Theorem | 177 |
| 12.5 Exercises | 179 |
| 13 Groups Actions and the Sylow Theorems | 180 |
| 13.1 Group Actions | 180 |
| 13.2 Conjugacy Classes and the Class Equation | 181 |
| 13.3 The Sylow Theorems | 183 |
| 13.4 Some Applications of the Sylow Theorems | 187 |
| 13.5 Exercises | 191 |
| 14 Free Groups and Group Presentations | 192 |
| 14.1 Group Presentations and Combinatorial Group Theory | 192 |
| 14.2 Free Groups | 193 |
| 14.3 Group Presentations | 198 |
| 14.3.1 The Modular Group | 200 |
| 14.4 Presentations of Subgroups | 207 |
| 14.5 Geometric Interpretation | 209 |
| 14.6 Presentations of Factor Groups | 212 |
| 14.7 Group Presentations and Decision Problems | 213 |
| 14.8 Group Amalgams: Free Products and Direct Products | 214 |
| 14.9 Exercises | 216 |

| | |
|--|-----|
| 15 Finite Galois Extensions | 217 |
| 15.1 Galois Theory and the Solvability of Polynomial Equations | 217 |
| 15.2 Automorphism Groups of Field Extensions | 218 |
| 15.3 Finite Galois Extensions | 220 |
| 15.4 The Fundamental Theorem of Galois Theory | 221 |
| 15.5 Exercises | 231 |
| 16 Separable Field Extensions | 233 |
| 16.1 Separability of Fields and Polynomials | 233 |
| 16.2 Perfect Fields | 234 |
| 16.3 Finite Fields | 236 |
| 16.4 Separable Extensions | 238 |
| 16.5 Separability and Galois Extensions | 241 |
| 16.6 The Primitive Element Theorem | 245 |
| 16.7 Exercises | 247 |
| 17 Applications of Galois Theory | 248 |
| 17.1 Applications of Galois Theory | 248 |
| 17.2 Field Extensions by Radicals | 248 |
| 17.3 Cyclotomic Extensions | 252 |
| 17.4 Solvability and Galois Extensions | 253 |
| 17.5 The Insolvability of the Quintic | 254 |
| 17.6 Constructibility of Regular n -Gons | 259 |
| 17.7 The Fundamental Theorem of Algebra | 261 |
| 17.8 Exercises | 263 |
| 18 The Theory of Modules | 265 |
| 18.1 Modules Over Rings | 265 |
| 18.2 Annihilators and Torsion | 270 |
| 18.3 Direct Products and Direct Sums of Modules | 271 |
| 18.4 Free Modules | 273 |
| 18.5 Modules over Principal Ideal Domains | 276 |
| 18.6 The Fundamental Theorem for Finitely Generated Modules | 279 |
| 18.7 Exercises | 283 |
| 19 Finitely Generated Abelian Groups | 285 |
| 19.1 Finite Abelian Groups | 285 |
| 19.2 The Fundamental Theorem: p -Primary Components | 286 |
| 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 Hilbert Nullstellensatz | 315 |
| 21.5 Applications and Consequences of Hilbert's Theorems | 317 |
| 21.6 Dimensions | 320 |
| 21.7 Exercises | 325 |
| 22 Algebraic Cryptography | 326 |
| 22.1 Basic Cryptography | 326 |
| 22.2 Encryption and Number Theory | 331 |
| 22.3 Public Key Cryptography | 335 |
| 22.3.1 The Diffie–Hellman Protocol | 336 |
| 22.3.2 The RSA Algorithm | 337 |
| 22.3.3 The El-Gamal Protocol | 339 |
| 22.3.4 Elliptic Curves and Elliptic Curve Methods | 341 |
| 22.4 Noncommutative Group based Cryptography | 342 |
| 22.4.1 Free Group Cryptosystems | 345 |
| 22.5 Ko–Lee and Anshel–Anshel–Goldfeld Methods | 349 |
| 22.5.1 The Ko–Lee Protocol | 350 |
| 22.5.2 The Anshel–Anshel–Goldfeld Protocol | 350 |
| 22.6 Platform Groups and Braid Group Cryptography | 351 |
| 22.7 Exercises | 356 |
| Bibliography | 359 |
| Index | 363 |