Contents

Preface — V

1 The Natural, Integral, and Rational Numbers — 1
1.1 Number Theory and Axiomatic Systems — 1
1.2 The Natural Numbers and Induction — 1
1.3 The Integers $\mathbb{Z}$ — 11
1.4 The Rational Numbers $\mathbb{Q}$ — 14
1.5 The Absolute Value in $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ — 17

2 Division and Factorization in the Integers — 20
2.1 The Fundamental Theorem of Arithmetic — 20
2.2 The Division Algorithm and the Greatest Common Divisor — 24
2.3 The Euclidean Algorithm — 27
2.4 Least Common Multiples — 31
2.5 General Greatest Common Divisors and Lowest Common Divisors — 33

3 Modular Arithmetic — 38
3.1 The Ring of Integers Modulo n — 38
3.2 Units and the Euler φ-Function — 42
3.3 RSA Cryptosystem — 45
3.4 The Chinese Remainder Theorem — 46
3.5 Quadratic Residues — 53

4 Exceptional Numbers — 59
4.1 The Fibonacci Numbers — 59
4.1.1 The Golden Rectangle — 67
4.1.2 Squares in Semicircles — 68
4.1.3 Side Length of a Regular 10-Gon — 69
4.1.4 Construction of the Golden Section with Compass and Straightedge — 70
4.2 Perfect Numbers and Mersenne Numbers — 71
4.3 Fermat Numbers — 78

5 Pythagorean Triples and Sums of Squares — 82
5.1 The Pythagorean Theorem — 82
5.2 Classification of the Pythagorean Triples — 84
5.3 Sum of Squares — 88

6 Polynomials and Unique Factorization — 95
6.1 Polynomials over a Ring — 95
6.2 Divisibility in Rings — 99

6.3 The Ring of Polynomials over a Field — 100
6.3.1 The Division Algorithm for Polynomials — 101
6.3.2 Zeros of Polynomials — 103
6.4 Horner-Scheme — 108
6.5 The Euclidean Algorithm and Greatest Common Divisor of Polynomials over Fields — 113
6.5.1 The Euclidean Algorithm for $K[x]$ — 114
6.5.2 Unique Factorization of Polynomials in $K[x]$ — 115
6.5.3 General Unique Factorization Domains — 116
6.6 Polynomial Interpolation and the Shamir Secret Sharing Scheme — 117
6.6.1 Secret Sharing — 117
6.6.2 Polynomial Interpolation over a Field — 117
6.6.3 The Shamir Secret Sharing Scheme — 121

7 Field Extensions and Splitting Fields — 124
7.1 Fields, Subfields and Characteristics — 124
7.2 Field Extensions — 125
7.3 Finite and Algebraic Field Extensions — 130
7.3.1 Finite Fields — 133
7.4 Splitting Fields — 134

8 Permutations and Symmetric Polynomials — 139
8.1 Permutations — 139
8.2 Cycle Decomposition of a Permutation — 142
8.2.1 Conjugate Elements in S_n — 145
8.2.2 Marshall Hall's Theorem — 146
8.3 Symmetric Polynomials — 149
8.4 Some Topics in Group Theory — 154
8.4.1 Cosets and Lagrange's Theorem — 154
8.4.2 Normal Subgroups and Factor Groups — 155
8.4.3 Group Isomorphism Theorems — 156
8.4.4 Solvable Groups — 158
8.4.5 Group Actions and the Sylow Theorems — 160
8.4.6 The Fundamental Theorem of Finitely Generated Abelian Groups — 167

9 Real Numbers — 176
9.1 The Real Number System — 176
9.2 Decimal Representation of Real Numbers — 187
9.3 Periodic Decimal Numbers and the Rational Numbers — 190
9.4 The Uncountability of $\mathbb{R}$ — 192
9.5 Continued Fraction Representation of Real Numbers — 193
9.6 Theorem of Dirichlet and Cauchy's Inequality — 195

9.7 The p-adic Numbers — 197
9.7.1 Normed Fields and Cauchy Completions — 197
9.7.2 The p-adic Fields — 198
9.7.3 The p-adic Norm — 201
9.7.4 The Construction of $\mathbb{Q}_p$ — 202
9.7.5 Ostrowski's Theorem — 203
9.7.6 The p-adic Arithmetic and p-adic Expansions — 204
9.7.7 The p-adic Integers — 209
9.7.8 Principal Ideals, Unique Factorization, and Completeness of $\mathbb{Z}_p$ — 210
9.7.9 Hensel's Lemma and Applications — 212
9.7.10 The Non-Isomorphism of the p-adic Fields — 215

10 The Complex Numbers, the Fundamental Theorem of Algebra, and Polynomial Equations — 219
10.1 The Field $\mathbb{C}$ of Complex Numbers — 219
10.2 The Complex Plane — 223
10.2.1 Geometric Interpretation of Complex Operations — 226
10.2.2 Polar Form and Euler's Identity — 227
10.2.3 Other Constructions of $\mathbb{C}$ — 231
10.2.4 The Gaussian Integers — 231
10.3 The Fundamental Theorem of Algebra — 233
10.3.1 First Proof of the Fundamental Theorem of Algebra — 234
10.3.2 Second Proof of the Fundamental Theorem of Algebra — 237
10.4 Solving Polynomial Equations in terms of Radicals — 239
10.5 Galois Theory and the Solvability of Polynomial Equations in terms of Radicals — 250
10.5.1 Automorphism Groups of Field Extensions — 251
10.5.2 Finite Galois Extensions — 252
10.5.3 The Fundamental Theorem of Galois Theory — 253
10.5.4 Field Extensions by Radicals — 261
10.5.5 Solvability by Radicals and Galois Extensions — 266
10.6 Skew Field Extensions of $\mathbb{C}$ and Frobenius's Theorem — 269

11 Quadratic Number Fields and Pell's Equation — 275
11.1 Algebraic Extensions of $\mathbb{Q}$ — 275
11.2 Algebraic and Transcendental Numbers — 276
11.3 Discriminant and Norm — 278
11.4 Algebraic Integers — 283
11.4.1 The Ring of Algebraic Integers — 284
11.5 Integral Bases — 286
11.6 Quadratic Fields and Quadratic Integers — 288

12 **Transcendental Numbers and the Numbers e and π — 296**
12.1 The Numbers e and π — **296**
12.1.1 Calculation e of π — **299**
12.2 The Irrationality of e and π — **303**
12.3 The Numbers e and π throughout Mathematics — **310**
12.3.1 The Normal Distribution — **310**
12.3.2 The Gamma Function and Stirling's Approximation — **311**
12.3.3 The Wallis Product Formula — **313**
12.4 Existence of a Transcendental Number — **318**
12.5 The Transcendence of e and π — **321**
12.6 An Amazing Property of π and a Connection to Prime Numbers — **330**

13 **Compass and Straightedge Constructions and the Classical Problems — 336**
13.1 Historical Remarks — **336**
13.2 Geometric Constructions — **336**
13.3 Four Classical Construction Problems — **343**
13.3.1 Squaring the Circle (Problem of Anaxagoras 500–428 BC) — **343**
13.3.2 The Doubling of the Cube or the Problem from Deli — **344**
13.3.3 The Trisection of an Angle — **344**
13.3.4 Construction of a Regular n-Gon — **345**

14 **Euclidean Vector Spaces — 350**
14.1 Length and Angle — **350**
14.2 Orthogonality and Applications in $\mathbb{R}^2$ and $\mathbb{R}^3$ — **356**
14.3 Orthonormalization and Closest Vector — **365**
14.4 Polynomial Approximation — **369**
14.5 Secret Sharing Scheme using the Closest Vector Theorem — **371**

Bibliography — 375

Index — 377