Contents

Preface xiii

Translator's Note xvi

Notation xvii

List of Symbols xvii

Chapter 1. Introduction 1

1.1. Pythagorean Triples 1

1.2. Pell's Equation 3

1.3. Fermat's Last Theorem 4

1.4. Congruences 8

1.5. Public Key Cryptology 11

1.6. Quadratic Residues 12

1.7. Prime Numbers 22

1.8. The Prime Number Theorem 26

1.9. Exercises 31

Chapter 2. The Geometry of Numbers 35

2.1. Binary Quadratic Forms 35

2.2. Complete Decomposable Forms of Degree n 37

2.3. Modules and Orders 39

2.4. Complete Modules in Finite Extensions of P 43
2.5. The Integers of a Quadratic Field 45
2.6. Further Examples of Determining a $\mathbb{Z}$-Basis for the Ring of Integers of a Number Field 46
2.7. The Finiteness of the Class Number 47
2.8. The Group of Units 48
2.9. The Start of the Proof of Dirichlet's Unit Theorem 50
2.10. The Rank of $\mathfrak{l}(E)$ 51
2.11. The Regulator of an Order 55
2.12. The Lattice Point Theorem 55
2.13. Minkowski's Geometry of Numbers 57
2.14. Application to Complete Decomposable Forms 62
2.15. Exercises 64

Chapter 3. Dedekind's Theory of Ideals 65
3.1. Basic Definitions 66
3.2. The Main Theorem of Dedekind's Theory of Ideals 68
3.3. Consequences of the Main Theorem 71
3.4. The Converse of the Main Theorem 73
3.5. The Norm of an Ideal 74
3.6. Congruences 76
3.7. Localization 78
3.8. The Decomposition of a Prime Ideal in a Finite Separable Extension 80
3.9. The Class Group of an Algebraic Number Field 84
3.10. Relative Extensions 88
3.11. Geometric Interpretation 93
3.12. Different and Discriminant 94
3.13. Exercises 101

Chapter 4. Valuations 103

4.1. Fields with Valuation 104

4.2. Valuations of the Field of Rational Numbers and of a Field of Rational Functions 110

4.3. Completion 112

4.4. Complete Fields with Respect to a Discrete Valuation 114

4.5. Extension of a Valuation of a Complete Field to a Finite Extension 121

4.6. Finite Extensions of a Complete Field with a Discrete Valuation 124

4.7. Complete Fields with a Discrete Valuation and Finite Residue Class Field 129

4.8. Extension of the Valuation of an Arbitrary Field to a Finite Extension 132

4.9. Arithmetic in the Compositum of Two Field Extensions 137

4.10. Exercises 137

Chapter 5. Algebraic Functions of One Variable 141

5.1. Algebraic Function Fields 142

5.2. The Places of an Algebraic Function Field 144

5.3. The Function Space Associated to a Divisor 149

5.4. Differentials 154

5.5. Extensions of the Field of Constants 158

5.6. The Riemann–Roch Theorem 160

5.7. Function Fields of Genus 0 164

5.8. Function Fields of Genus 1 167

5.9. Exercises 169

Chapter 6. Normal Extensions 171

6.1. Decomposition Group and Ramification Groups 172

6.2. A New Proof of Dedekind's Theorem on the Different 176

6.3. Decomposition of Prime Ideals in an Intermediate Field 178

6.4. Cyclotomic Fields 180

6.5. The First Case of Fermat's Last Theorem 184
6.6. Localization 188
6.7. Upper Numeration of the Ramification Group 190
6.8. Kummer Extensions 195
6.9. Exercises 199

Chapter 7. L-Series 203
7.1. From the Riemann ζ-Function to the Hecke L-Series 204
7.2. Normalized Valuations 207
7.3. Adeles 209
7.4. Ideles 212
7.5. Idele Class Group and Ray Class Group 214
7.6. Hecke Characters 217
7.7. Analysis on Local Additive Groups 219
7.8. Analysis on the Adele Group 223
7.9. The Multiplicative Group of a Local Field 227
7.10. The Local Functional Equation 230
7.11. Calculation of $\rho(c)$ for $K = \mathbb{R}$ 232
7.12. Calculation of $\rho(c)$ for $K = \mathbb{C}$ 234
7.13. Computation of the ρ-Factors for a Nonarchimedean Field 236
7.14. Relations Among the ρ-Factors 239
7.15. Analysis on the Idele Group 240
7.16. Global Zeta Functions 243
7.17. The Dedekind Zeta Function 247
7.18. Hecke L-Series 251
7.19. Congruence Zeta Functions 252
7.20. Exercises 257

Chapter 8. Applications of Hecke L-Series 259
8.1. The Decomposition of Prime Numbers in Algebraic Number Fields 259
8.2. The Nonvanishing of the L-Series at $s = 1$ 262

8.3. The Distribution of Prime Ideals in an Algebraic Number Field 266
8.4. The Generalized Riemann Hypothesis 270
8.5. Exercises 273

Chapter 9. Quadratic Number Fields 275
9.1. Quadratic Forms and Orders in Quadratic Number Fields 275
9.2. The Class Number of Imaginary Quadratic Number Fields 282
9.3. Continued Fractions 285
9.4. Periodic Continued Fractions 290
9.5. The Fundamental Unit of an Order of a Real Quadratic Number Field 295
9.6. The Character of a Quadratic Number Field 301
9.7. The Arithmetic Class Number Formula 303
9.8. Computing the Gaussian Sum 310
9.9. Exercises 313

Chapter 10. What Next? 315
10.1. Absolutely Abelian Extensions 316
10.2. The Class Field of the Ray Class Group 317
10.3. Local Class Field Theory 321
10.4. Formulation of Class Field Theory Using Ideles 322
10.5. Exercises 324

Appendix A. Divisibility Theory 325
A.1. Divisibility in Monoids 325
A.2. Principal Ideal Domains 328
A.3. Euclidean Domains 330
A.4. Finitely Generated Modules over a Principal Ideal Domain 331
A.5. Modules over Euclidean Domains 338
A.6. The Arithmetic of Polynomials over Rings 340

Appendix B. Trace, Norm, Different, and Discriminant 341

Appendix C. Harmonic Analysis on Locally Compact Abelian Groups 345

C.1. Topological Groups 345

C.2. The Pontryagin Duality Theorem 346

C.3. The Haar Integral 347

C.4. The Restricted Direct Product 350

C.5. The Poisson Summation Formula 356

References 359

Index 363