

# Contents

	<b>Preface</b>	<b>v</b>
	<b>Acknowledgments</b>	<b>ix</b>
	<b>Index of Notations</b>	<b>xix</b>
	<b>INTRODUCTION</b>	<b>1</b>
<b>CHAPTER 1.</b>	<b>Unique Factorization Domains, Ideals, and Principal Ideal Domains</b>	<b>5</b>
	1.1. Unique Factorization Domains	5
	1.2. Ideals	6
	1.3. Principal Ideal Domains	8
	Exercises	8
<b>CHAPTER 2.</b>	<b>Commutative Fields</b>	<b>13</b>
	2.1. Algebraic Elements	13
	2.2. Algebraic Extensions, Algebraically Closed Fields	14
	2.3. Algebraic Number Fields	15
	2.4. Characteristic and Prime Fields	15
	2.5. Normal Extensions, Splitting Fields	15
	2.6. Separable Extensions	16
	2.7. Galois Extensions	17
	2.8. Roots of Unity	18
	2.9. Finite Fields	19
	2.10. Trace and Norm of Elements	19
	2.11. The Discriminant	20
	2.12. Discriminant and Resultant of Polynomials	21
	2.13. Inseparable Extensions	23
	2.14. Perfect Fields	23
	2.15. The Theorem of Steinitz	24
	2.16. Orderable Fields	24

2.17.	The Theorem of Artin	25
	Exercises	25
	<b>PART ONE</b>	<b>33</b>
<b>CHAPTER 3.</b>	<b>Residue Classes</b>	<b>37</b>
3.1.	Congruences	37
3.2.	The Group of Invertible Residue Classes	41
3.3.	Finite Abelian Groups	45
	Exercises	49
<b>CHAPTER 4.</b>	<b>Quadratic Residues</b>	<b>61</b>
4.1.	The Legendre Symbol and Gauss' Reciprocity Law	61
4.2.	Gaussian Sums	70
4.3.	The Jacobi Symbol	73
	Exercises	76
	<b>PART TWO</b>	<b>83</b>
<b>CHAPTER 5.</b>	<b>Algebraic Integers</b>	<b>85</b>
5.1.	Integral Elements, Integrally Closed Domains	85
5.2.	Rings of Algebraic Integers	91
5.3.	Arithmetic in the Field of Gaussian Numbers	92
5.4.	Integers of Quadratic Number Fields	97
5.5.	Integers of Cyclotomic Fields	100
	Exercises	101
<b>CHAPTER 6.</b>	<b>Integral Basis, Discriminant</b>	<b>107</b>
6.1.	Finitely Generated Modules	107
6.2.	Integral Basis	114
6.3.	The Discriminant	116
6.4.	Discriminant of Quadratic Fields	117
6.5.	Discriminant of Cyclotomic Fields	118
	Exercises	119
<b>CHAPTER 7.</b>	<b>The Decomposition of Ideals</b>	<b>123</b>
7.1.	Dedekind's Theorem	123
7.2.	Dedekind Domains	128
	Exercises	133
<b>CHAPTER 8.</b>	<b>The Norm and Classes of Ideals</b>	<b>141</b>
8.1.	The Norm of an Ideal	141
8.2.	Classes of Ideals	145
	Exercises	148

<b>CHAPTER 9.</b>	<b>Estimates for the Discriminant</b>	<b>153</b>
9.1.	The Theorem of Minkowski	153
9.2.	Estimates of the Discriminant	158
	Exercises	165
<b>CHAPTER 10.</b>	<b>Units</b>	<b>167</b>
10.1.	Roots of Unity	167
10.2.	Units of Quadratic Fields	169
10.3.	Units of Cyclotomic Fields	175
10.4.	Dirichlet's Theorem	177
	Exercises	184
<b>CHAPTER 11.</b>	<b>Extension of Ideals</b>	<b>189</b>
11.1.	Extension of Ideals	189
11.2.	Decomposition of Prime Numbers in Quadratic Fields	198
11.3.	Decomposition of Prime Numbers in Cyclotomic Fields	202
	Exercises	204
<b>CHAPTER 12.</b>	<b>Algebraic Interlude</b>	<b>207</b>
12.1.	Rings of Fractions	207
12.2.	Traces and Norms in Ring Extensions	213
12.3.	Discriminant of Ring Extensions	226
	Exercises	231
<b>CHAPTER 13.</b>	<b>The Relative Trace, Norm, Discriminant, and Different</b>	<b>233</b>
13.1.	The Relative Trace and Norm of an Ideal	233
13.2.	Relative Discriminant and Different of Algebraic Number Fields	237
	Exercises	256
<b>CHAPTER 14.</b>	<b>The Decomposition of Prime Ideals in Galois Extensions</b>	<b>259</b>
14.1.	Decomposition and Inertia	259
14.2.	The Ramification	264
	Exercises	271
<b>CHAPTER 15.</b>	<b>The Fundamental Theorem of Abelian Extensions</b>	<b>273</b>
15.1.	The Theorem of Kronecker and Weber	273
15.2.	Class Field Theory	282
15.2.1.	The Theory of Hilbert	283
15.2.2.	The Theory of Takagi	283
	Exercises	287

<b>CHAPTER 16. Complements and Miscellaneous Numerical Examples</b>	<b>291</b>
16.1. Some Algorithms	291
16.1.1. Calculation of the Minimal Polynomial, Trace and Norm of an Element	292
16.1.2. Calculation of the Discriminant of a Set $\{x_1, \dots, x_n\}$	293
16.1.3. Determination of an Integral Basis, Ring of Integers and Discriminant	293
16.1.4. Decomposition into Prime Ideals	294
16.2. Complements on Cyclotomic Fields	294
16.3. Some Cubic Fields	300
16.4. Biquadratic Fields	311
16.5. Binomial Extensions	314
16.6. Relative Binomial Extensions	320
16.7. The Class Number of Quadratic Extensions	325
16.8. Prime Producing Polynomials Exercises	330 333
<b>PART THREE</b>	<b>337</b>
<b>CHAPTER 17. Local Methods for Cyclotomic Fields</b>	<b>339</b>
17.1. $p$ -Adic and $\lambda$ -Adic Numbers	339
17.1.1. The $p$ -Adic Numbers	339
17.1.2. The $\lambda$ -Adic Numbers	343
17.2. The $\lambda$ -Adic Exponential and Logarithm	344
17.2.1. Formal Power Series	344
17.2.2. The $\lambda$ -Adic Exponential and Logarithm	349
17.3. The $\lambda$ -Adic Integers Exercises	355 363
<b>CHAPTER 18. Bernoulli Numbers</b>	<b>367</b>
18.1. Algebraic Properties	367
18.1.1. Recurrence for the Bernoulli Numbers	367
18.1.2. Relations of Bernoulli Numbers with Trigonometric Functions	370
18.1.3. Bernoulli Numbers and the Zeta Function	372
18.1.4. Sums of Equal Powers of Successive Natural Numbers	377
18.1.5. Quadratic Identities	380
18.2. Arithmetical Properties	384
18.2.1. The Denominator of the Bernoulli Numbers	384
18.2.2. The Numerator of the Bernoulli Numbers	390
18.2.3. The Congruence of Kummer	392

	Exercises	394
<b>CHAPTER 19.</b>	<b>Fermat's Last Theorem for Regular Prime Exponents</b>	<b>399</b>
19.1.	Regular Primes and the Lemma of Units	399
19.2.	Kummer's Theorem	409
19.3.	Irregular Primes	418
	Exercises	425
<b>CHAPTER 20.</b>	<b>More on Cyclotomic Extensions</b>	<b>429</b>
20.1.	Resolution by Radicals of the Cyclotomic Equation	429
20.2.	The Gaussian Periods	434
20.3.	Lagrange Resolvents and the Jacobi Cyclotomic Function	438
20.4.	On the Decomposition into Prime Ideals of the Cyclotomic Field	447
20.5.	Generation of the Class Group of the Cyclotomic Field	454
	Exercises	458
	<b>PART FOUR</b>	<b>461</b>
<b>CHAPTER 21.</b>	<b>Characters and Gaussian Sums</b>	<b>463</b>
21.1.	Characters of Finite Abelian Groups	463
21.2.	Modular Characters	472
21.3.	Gaussian Sums	478
	Exercises	482
<b>CHAPTER 22.</b>	<b>Zeta-Functions and <math>L</math>-Series</b>	<b>487</b>
22.1.	The Riemann Zeta-Function	487
22.2.	$L$ -Series	493
	Exercises	498
<b>CHAPTER 23.</b>	<b>The Dedekind Zeta-Function</b>	<b>505</b>
23.1.	Asymptotic Expression for the Class Number	505
23.2.	The Dedekind Zeta-Series	513
23.3.	Hecke $L$ -Series	518
	Exercises	519
<b>CHAPTER 24.</b>	<b>Primes in Arithmetic Progressions</b>	<b>523</b>
24.1.	Proof of Dirichlet's Theorem	523
24.2.	Special Cases	529
	Exercises	541
<b>CHAPTER 25.</b>	<b>The Frobenius Automorphism and the Splitting of Prime Ideals</b>	<b>543</b>

25.1.	The Frobenius Automorphism	543
25.2.	Density Results on the Decomposition of Prime Ideals	548
25.3.	The Theorem of Chebotarev	552
25.4.	Bauerian Extensions of Fields Exercises	563 564
<b>CHAPTER 26.</b>	<b>Class Number of Quadratic Fields</b>	<b>567</b>
26.1.	The Quadratic Character Attached to the Quadratic Field	568
26.2.	The $L$ -Series and the Gaussian Sum of the Quadratic Character	573
26.3.	The Class Number Formula and the Distribution of Quadratic Residues Exercises	583 592
<b>CHAPTER 27.</b>	<b>Class Number of Cyclotomic Fields</b>	<b>595</b>
27.1.	The Class Number Formula	595
27.2.	The Two Factors of the Class Number Exercises	599 616
<b>CHAPTER 28.</b>	<b>Miscellaneous Results About the Class Number of Quadratic Fields</b>	<b>617</b>
28.1.	Divisibility Properties	617
28.2.	Quadratic Fields with Class Number 1	636
<b>CHAPTER 29.</b>	<b>Miscellaneous Results About the Class Number of Cyclotomic Fields</b>	<b>639</b>
29.1.	Miscellanea About the Relative Class Number of $\mathbb{Q}(\zeta_p)$	639
29.1.1.	Determinantal Formulas for the Relative Class Number	640
29.1.2.	Upper and Lower Bounds for the Relative Class Number	648
29.1.3.	Cyclotomic Fields with Class Number 1	652
29.1.4.	Growth of the Relative Class Number	653
29.1.5.	Some Divisibility Properties of the Relative Class Number	656
29.2.	Miscellanea About the Real Class Number of Cyclotomic Fields	659
29.3.	The Class Number of $\mathbb{Q}(\zeta_m)$ , $m > 2$ and Miscellaneous Results	661
29.3.1.	The Class Number Formula	661
29.3.2.	Divisibility Properties	662
29.3.3.	Fields with Class Number 1	663
	<b>A Guide for Further Study</b>	<b>665</b>

<b>Bibliography</b>	<b>667</b>
<b>Index of Names</b>	<b>673</b>
<b>Subject Index</b>	<b>677</b>