

Contents

Preface	v
1. Fundamental Results and Algorithms in Dedekind Domains	1
1.1 Introduction	1
1.2 Finitely Generated Modules Over Dedekind Domains	2
1.2.1 Finitely Generated Torsion-Free and Projective Modules	6
1.2.2 Torsion Modules	13
1.3 Basic Algorithms in Dedekind Domains	17
1.3.1 Extended Euclidean Algorithms in Dedekind Domains	17
1.3.2 Deterministic Algorithms for the Approximation Theorem	20
1.3.3 Probabilistic Algorithms	23
1.4 The Hermite Normal Form Algorithm in Dedekind Domains	25
1.4.1 Pseudo-Objects	26
1.4.2 The Hermite Normal Form in Dedekind Domains	28
1.4.3 Reduction Modulo an Ideal	32
1.5 Applications of the HNF Algorithm	34
1.5.1 Modifications to the HNF Pseudo-Basis	34
1.5.2 Operations on Modules and Maps	35
1.5.3 Reduction Modulo \mathfrak{p} of a Pseudo-Basis	37
1.6 The Modular HNF Algorithm in Dedekind Domains	38
1.6.1 Introduction	38
1.6.2 The Modular HNF Algorithm	38
1.6.3 Computing the Transformation Matrix	41
1.7 The Smith Normal Form Algorithm in Dedekind Domains	42
1.8 Exercises for Chapter 1	46
2. Basic Relative Number Field Algorithms	49
2.1 Compositum of Number Fields and Relative and Absolute Equations	49
2.1.1 Introduction	49
2.1.2 Étale Algebras	50
2.1.3 Compositum of Two Number Fields	56
2.1.4 Computing θ_1 and θ_2	59

2.1.5	Relative and Absolute Defining Polynomials	62
2.1.6	Compositum with Normal Extensions	66
2.2	Arithmetic of Relative Extensions	72
2.2.1	Relative Signatures	72
2.2.2	Relative Norm, Trace, and Characteristic Polynomial	76
2.2.3	Integral Pseudo-Bases	76
2.2.4	Discriminants	78
2.2.5	Norms of Ideals in Relative Extensions	80
2.3	Representation and Operations on Ideals	83
2.3.1	Representation of Ideals	83
2.3.2	Representation of Prime Ideals	89
2.3.3	Computing Valuations	92
2.3.4	Operations on Ideals	94
2.3.5	Ideal Factorization and Ideal Lists	99
2.4	The Relative Round 2 Algorithm and Related Algorithms	102
2.4.1	The Relative Round 2 Algorithm	102
2.4.2	Relative Polynomial Reduction	110
2.4.3	Prime Ideal Decomposition	111
2.5	Relative and Absolute Representations	114
2.5.1	Relative and Absolute Discriminants	114
2.5.2	Relative and Absolute Bases	115
2.5.3	Ups and Downs for Ideals	116
2.6	Relative Quadratic Extensions and Quadratic Forms	118
2.6.1	Integral Pseudo-Basis, Discriminant	118
2.6.2	Representation of Ideals	121
2.6.3	Representation of Prime Ideals	123
2.6.4	Composition of Pseudo-Quadratic Forms	125
2.6.5	Reduction of Pseudo-Quadratic Forms	127
2.7	Exercises for Chapter 2	129
3.	The Fundamental Theorems of Global Class Field Theory	133
3.1	Prologue: Hilbert Class Fields	133
3.2	Ray Class Groups	135
3.2.1	Basic Definitions and Notation	135
3.3	Congruence Subgroups: One Side of Class Field Theory	138
3.3.1	Motivation for the Equivalence Relation	138
3.3.2	Study of the Equivalence Relation	139
3.3.3	Characters of Congruence Subgroups	145
3.3.4	Conditions on the Conductor and Examples	147
3.4	Abelian Extensions: The Other Side of Class Field Theory	150
3.4.1	The Conductor of an Abelian Extension	150
3.4.2	The Frobenius Homomorphism	151
3.4.3	The Artin Map and the Artin Group $A_m(L/K)$	152
3.4.4	The Norm Group (or Takagi Group) $T_m(L/K)$	153
3.5	Putting Both Sides Together: The Takagi Existence Theorem	154

3.5.1	The Takagi Existence Theorem	154
3.5.2	Signatures, Characters, and Discriminants	156
3.6	Exercises for Chapter 3	160
4.	Computational Class Field Theory	163
4.1	Algorithms on Finite Abelian groups	164
4.1.1	Algorithmic Representation of Groups	164
4.1.2	Algorithmic Representation of Subgroups	166
4.1.3	Computing Quotients	168
4.1.4	Computing Group Extensions	169
4.1.5	Right Four-Term Exact Sequences	170
4.1.6	Computing Images, Inverse Images, and Kernels	172
4.1.7	Left Four-Term Exact Sequences	174
4.1.8	Operations on Subgroups	176
4.1.9	p -Sylow Subgroups of Finite Abelian Groups	177
4.1.10	Enumeration of Subgroups	179
4.1.11	Application to the Solution of Linear Equations and Congruences	182
4.2	Computing the Structure of $(\mathbb{Z}_K/\mathfrak{m})^*$	185
4.2.1	Standard Reductions of the Problem	186
4.2.2	The Use of \mathfrak{p} -adic Logarithms	190
4.2.3	Computing $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ by Induction	198
4.2.4	Representation of Elements of $(\mathbb{Z}_K/\mathfrak{m})^*$	204
4.2.5	Computing $(\mathbb{Z}_K/\mathfrak{m})^*$	206
4.3	Computing Ray Class Groups	209
4.3.1	The Basic Ray Class Group Algorithm	209
4.3.2	Size Reduction of Elements and Ideals	211
4.4	Computations in Class Field Theory	213
4.4.1	Computations on Congruence Subgroups	213
4.4.2	Computations on Abelian Extensions	214
4.4.3	Conductors of Characters	218
4.5	Exercises for Chapter 4	219
5.	Computing Defining Polynomials Using Kummer Theory .	223
5.1	General Strategy for Using Kummer Theory	223
5.1.1	Reduction to Cyclic Extensions of Prime Power Degree	223
5.1.2	The Four Methods	226
5.2	Kummer Theory Using Hecke's Theorem When $\zeta_\ell \in K$	227
5.2.1	Characterization of Cyclic Extensions of Conductor \mathfrak{m} and Degree ℓ	227
5.2.2	Virtual Units and the ℓ -Selmer Group	229
5.2.3	Construction of Cyclic Extensions of Prime Degree and Conductor \mathfrak{m}	233
5.2.4	Algorithmic Kummer Theory When $\zeta_\ell \in K$ Using Hecke	236
5.3	Kummer Theory Using Hecke When $\zeta_\ell \notin K$	242

5.3.1	Eigenspace Decomposition for the Action of τ	242
5.3.2	Lift in Characteristic 0	248
5.3.3	Action of τ on Units	254
5.3.4	Action of τ on Virtual Units	255
5.3.5	Action of τ on the Class Group	256
5.3.6	Algorithmic Kummer Theory When $\zeta_\ell \notin K$ Using Hecke	260
5.4	Explicit Use of the Artin Map in Kummer Theory When $\zeta_n \in K$	270
5.4.1	Action of the Artin Map on Kummer Extensions	270
5.4.2	Reduction to $\alpha \in U_S(K)/U_S(K)^n$ for a Suitable S	272
5.4.3	Construction of the Extension L/K by Kummer Theory	274
5.4.4	Picking the Correct α	277
5.4.5	Algorithmic Kummer Theory When $\zeta_n \in K$ Using Artin	278
5.5	Explicit Use of the Artin Map When $\zeta_n \notin K$	280
5.5.1	The Extension K_z/K	280
5.5.2	The Extensions L_z/K_z and L_z/K	281
5.5.3	Going Down to the Extension L/K	283
5.5.4	Algorithmic Kummer Theory When $\zeta_n \notin K$ Using Artin	284
5.5.5	Comparison of the Methods	287
5.6	Two Detailed Examples	288
5.6.1	Example 1	289
5.6.2	Example 2	290
5.7	Exercises for Chapter 5	293
6.	Computing Defining Polynomials Using Analytic Methods	297
6.1	The Use of Stark Units and Stark's Conjecture	297
6.1.1	Stark's Conjecture	298
6.1.2	Computation of $\zeta'_{K,S}(0, \sigma)$	299
6.1.3	Real Class Fields of Real Quadratic Fields	301
6.2	Algorithms for Real Class Fields of Real Quadratic Fields	303
6.2.1	Finding a Suitable Extension N/K	303
6.2.2	Computing the Character Values	306
6.2.3	Computation of $W(\chi)$	307
6.2.4	Recognizing an Element of \mathbb{Z}_K	309
6.2.5	Sketch of the Complete Algorithm	310
6.2.6	The Special Case of Hilbert Class Fields	311
6.3	The Use of Complex Multiplication	313
6.3.1	Introduction	314
6.3.2	Construction of Unramified Abelian Extensions	315
6.3.3	Quasi-Elliptic Functions	325
6.3.4	Construction of Ramified Abelian Extensions Using Complex Multiplication	333
6.4	Exercises for Chapter 6	344

7. Variations on Class and Unit Groups	347
7.1 Relative Class Groups	347
7.1.1 Relative Class Group for $i_{L/K}$	348
7.1.2 Relative Class Group for $\mathcal{N}_{L/K}$	349
7.2 Relative Units and Regulators	352
7.2.1 Relative Units and Regulators for $i_{L/K}$	352
7.2.2 Relative Units and Regulators for $\mathcal{N}_{L/K}$	358
7.3 Algorithms for Computing Relative Class and Unit Groups	360
7.3.1 Using Absolute Algorithms	360
7.3.2 Relative Ideal Reduction	365
7.3.3 Using Relative Algorithms	367
7.3.4 An Example	369
7.4 Inverting Prime Ideals	371
7.4.1 Definitions and Results	371
7.4.2 Algorithms for the S -Class Group and S -Unit Group	373
7.5 Solving Norm Equations	377
7.5.1 Introduction	377
7.5.2 The Galois Case	378
7.5.3 The Non-Galois Case	380
7.5.4 Algorithmic Solution of Relative Norm Equations	382
7.6 Exercises for Chapter 7	386
8. Cubic Number Fields	389
8.1 General Binary Forms	389
8.2 Binary Cubic Forms and Cubic Number Fields	395
8.3 Algorithmic Characterization of the Set U	400
8.4 The Davenport–Heilbronn Theorem	404
8.5 Real Cubic Fields	409
8.6 Complex Cubic Fields	418
8.7 Implementation and Results	422
8.7.1 The Algorithms	422
8.7.2 Results	425
8.8 Exercises for Chapter 8	426
9. Number Field Table Constructions	429
9.1 Introduction	429
9.2 Using Class Field Theory	430
9.2.1 Finding Small Discriminants	430
9.2.2 Relative Quadratic Extensions	433
9.2.3 Relative Cubic Extensions	437
9.2.4 Finding the Smallest Discriminants Using Class Field Theory	444
9.3 Using the Geometry of Numbers	445
9.3.1 The General Procedure	445
9.3.2 General Inequalities	451

9.3.3	The Totally Real Case	453
9.3.4	The Use of Lagrange Multipliers	455
9.4	Construction of Tables of Quartic Fields	460
9.4.1	Easy Inequalities for All Signatures	460
9.4.2	Signature (0, 2): The Totally Complex Case	461
9.4.3	Signature (2, 1): The Mixed Case	463
9.4.4	Signature (4, 0): The Totally Real Case	464
9.4.5	Imprimitive Degree 4 Fields	465
9.5	Miscellaneous Methods (in Brief)	466
9.5.1	Euclidean Number Fields	467
9.5.2	Small Polynomial Discriminants	467
9.6	Exercises for Chapter 9	468
10.	Appendix A: Theoretical Results	475
10.1	Ramification Groups and Applications	475
10.1.1	A Variant of Nakayama's Lemma	475
10.1.2	The Decomposition and Inertia Groups	477
10.1.3	Higher Ramification Groups	480
10.1.4	Application to Different and Conductor Computations	484
10.1.5	Application to Dihedral Extensions of Prime Degree ..	487
10.2	Kummer Theory	492
10.2.1	Basic Lemmas	492
10.2.2	The Basic Theorem of Kummer Theory	494
10.2.3	Hecke's Theorem	498
10.2.4	Algorithms for ℓ th Powers	504
10.3	Dirichlet Series with Functional Equation	508
10.3.1	Computing L -Functions Using Rapidly Convergent Series	508
10.3.2	Computation of $F_i(s, x)$	516
10.4	Exercises for Chapter 10	518
11.	Appendix B: Electronic Information	523
11.1	General Computer Algebra Systems	523
11.2	Semi-general Computer Algebra Systems	524
11.3	More Specialized Packages and Programs	525
11.4	Specific Packages for Curves	526
11.5	Databases and Servers	527
11.6	Mailing Lists, Websites, and Newsgroups	529
11.7	Packages Not Directly Related to Number Theory	530
12.	Appendix C: Tables	533
12.1	Hilbert Class Fields of Quadratic Fields	533
12.1.1	Hilbert Class Fields of Real Quadratic Fields	533
12.1.2	Hilbert Class Fields of Imaginary Quadratic Fields ..	538
12.2	Small Discriminants	543

12.2.1 Lower Bounds for Root Discriminants	543
12.2.2 Totally Complex Number Fields of Smallest Discriminant	545
Bibliography	549
Index of Notation	556
Index of Algorithms	564
General Index	569