Graduate Texts in Mathematics 193

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.

(continued after index)

Henri Cohen

Advanced Topics in Computational Number Theory

Springer

Henri Cohen
Université de Bordeaux 1
Lab. Algorithmique Arithmétique Expérimentale
351, cours de la Libération
33405 Talence
France

Mathematics Subject Classification (1991): 11-01, 11Yxx, 11Y16

Library of Congress Cataloging-in-Publication Data
Cohen, Henri
Advanced topics in computational number theory / Henri Cohen.
p. cm. — (Graduate texts in mathematics ; 193)
Includes bibliographical references and index.
ISBN 978-1-4612-6419-4 ISBN 978-1-4419-8489-0 (eBook)
DOI 10.1007/978-1-4419-8489-0
1. Number theory—data processing. I. Title. II. Series.
QA241.C667 1999
512'.7'0285—dc21 99-20756
Printed on acid-free paper.

Production managed by Terry Kornak; manufacturing supervised by Jerome Basma.
Photocomposed copy prepared by the author using AMS-LaTeX and Springer's `clmono01` macros.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4612-6419-4 SPIN 10708040

Preface

The computation of invariants of algebraic number fields such as integral bases, discriminants, prime decompositions, ideal class groups, and unit groups is important both for its own sake and for its numerous applications, for example, to the solution of Diophantine equations. The practical completion of this task (sometimes known as the Dedekind program) has been one of the major achievements of computational number theory in the past ten years, thanks to the efforts of many people. Even though some practical problems still exist, one can consider the subject as solved in a satisfactory manner, and it is now routine to ask a specialized Computer Algebra System such as Kant/Kash, LiDIA, Magma, or Pari/GP, to perform number field computations that would have been unfeasible only ten years ago.The (very numerous) algorithms used are essentially all described in *A Course in Computational Algebraic Number Theory*, GTM 138, first published in 1993 (third corrected printing 1996), which is referred to here as [Coh0]. That text also treats other subjects such as elliptic curves, factoring, and primality testing.

It is important and natural to generalize these algorithms. Several generalizations can be considered, but the most important are certainly the generalizations to global function fields (finite extensions of the field of rational functions in one variable over a finite field) and to relative extensions of number fields. As in [Coh0], in the present book we will consider number fields only and not deal at all with function fields.

We will thus address some specific topics related to number fields; contrary to [Coh0], there is no attempt to be exhaustive in the choice of subjects. The topics have been chosen primarily because of my personal tastes, and of course because of their importance. Almost all of the subjects discussed in this book are quite new from the algorithmic aspect (usually post-1990), and nearly all of the algorithms have been implemented and tested in the number theory package Pari/GP (see [Coh0] and [BBBCO]). The fact that the subjects are new does not mean that they are more difficult. In fact, as the reader will see when reading this book in depth, the algorithmic treatment of certain parts of number theory which have the reputation of being "difficult" is in fact much *easier* than the theoretical treatment. A case in point is computational class field theory (see Chapters 4 to 6). I do not mean that the proofs become any simpler, but only that one gets a much better grasp on the subject by studying its algorithmic aspects.

As already mentioned, a common point to most of the subjects discussed in this book is that we deal with *relative* extensions, but we also study other subjects. We will see that most of the algorithms given in [Coh0] for the absolute case can be generalized to the relative case.

The book is organized as follows. Chapters 1 and 2 contain the theory and algorithms concerning Dedekind domains and relative extensions of number

fields, and in particular the generalization to the relative case of the round 2 and related algorithms.

Chapters 3, 4, 5, and 6 contain the theory and complete algorithms concerning class field theory over number fields. The highlights are the algorithms for computing the structure of $(\mathbb{Z}_K/\mathfrak{m})^*$, of ray class groups, and relative equations for Abelian extensions of number fields using Kummer theory, Stark's conjectures, and complex multiplication. The reader is warned that Chapter 5 is rather technical but contains a wealth of information useful both for further research and for any serious implementation. The analytic techniques using Stark's conjecture or complex multiplication described in Chapter 6 are fascinating since they construct purely algebraic objects using analytic means.

Chapters 1 through 6 together with Chapter 10 form a homogeneous subject matter that can be used for a one-semester or full-year advanced graduate course in computational number theory, omitting the most technical parts of Chapter 5.

The subsequent chapters deal with more miscellaneous subjects. In Chapter 7, we consider other variants of the notions of class and unit groups, such as relative class and unit groups or S-class and unit groups. We sketch an algorithm that allows the direct computation of relative class and unit groups and give applications of S-class and unit groups to the algorithmic solution of norm equations, due to D. Simon.

In Chapter 8, we explain in detail the correspondence between cubic fields and binary cubic forms, discovered by H. Davenport and H. Heilbronn, and examine the important algorithmic consequences discovered by K. Belabas.

In Chapter 9, we give a detailed description of known methods for constructing tables of number fields or number fields of small discriminant, either by using absolute techniques based on the geometry of numbers or by using relative techniques based either on the geometry of numbers or on class field theory.

In Appendix A, we give and prove a number of important miscellaneous results that can be found scattered in the literature but are used in the rest of the book.

In Appendix B, we give an updated but much shortened version of [Coh0, Appendix A] concerning packages for number theory and other useful electronic information.

In Appendix C, we give a number of useful tables that can be produced using the results of this book.

The book ends with an index of notation, an index of algorithms, and a general index.

The prerequisites for reading this book are essentially the basic definitions and results of algebraic number theory, as can be found in many textbooks, including [Coh0]. Apart from that, this book is almost entirely self-contained. Although numerous references are made to the algorithms con-

tained in [Coh0], these should be considered as "black boxes" and used as such. It would, however, be preferable at some point for the reader to study some of the algorithms of [Coh0]; in particular, those generalized here.

WARNINGS

(1) As usual, neither the author nor Springer-Verlag can assume any responsibility for consequences arising from the use of the algorithms given in this book.

(2) The author would like to hear about errors, typographical or otherwise. Please send e-mail to

`cohen@math.u-bordeaux.fr`

Lists of known errors, both for [Coh0] and for the present book, can be obtained by anonymous ftp from the URL

`ftp://megrez.math.u-bordeaux.fr/pub/cohenbook`

or obtained through the author's home page on the Web at the URL

`http://www.math.u-bordeaux.fr/~cohen`

(3) There is, however, another important warning that is almost irrelevant in [Coh0]. Almost all of the algorithms or the algorithmic aspects presented in this book are new, and most have never been published before or are being published while this book is going to press. Therefore, it is quite possible that major mistakes are present, although this possibility is largely diminished by the fact that almost all of the algorithms have been tested, although not always thoroughly. More likely it is possible that some algorithms can be radically improved. The contents of this book only reflect the knowledge of the author at the time of writing.

Acknowledgments

First of all, I would like to thank my colleagues Francisco Diaz y Diaz and Michel Olivier, with whom I have the pleasure of working every day and who collaborated with me on the discovery and implementation of many of the algorithms described in this book. Second, I would like to thank Jacques Martinet, head of our Laboratoire, who has enormously helped by giving me an ideal working environment and who also has tirelessly answered my numerous questions about most of the subject matter of this book. Third, I thank my former students Karim Belabas, Jean-Marc Couveignes, Denis Simon, and Emmanuel Tollis, who also contributed to part of the algorithms described here, and Xavier Roblot for everything related to Stark's conjectures.

In particular, Karim Belabas is to be thanked for the contents of Chapter 8, which are mainly due to him, for having carefully read the manuscript of this book, and not least for having taken the ungrateful job of managing the Pari software, after making thorough modifications leading to version 2.

I would like to thank several additional people who helped me in the preparation of this book. In alphabetical order, they are Claus Fieker (for Chapter 5), David Ford (for Chapter 2), Eduardo Friedman (for Chapter 7 and Appendix A), Thomas Papanikolaou (for Appendix B and for a lot of TEXnical help), and Michael Pohst (for Chapter 5).

I would also like to thank Mehpare Bilhan and the Middle East Technical University (METU) in Ankara, Turkey, for having given me an opportunity to write a first version of part of the subjects treated in this book, which appeared as an internal report of METU in 1997.

Last but not least, I thank all of our funding agencies, in particular, the C.N.R.S., the Ministry of Education and Research, the Ministry of Defense, the University of Bordeaux I, and the Région Aquitaine.

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 $A_{\mathfrak{m}}(L/K)$ 152
3.4.4 The Norm Group (or Takagi Group) $T_{\mathfrak{m}}(L/K)$ 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 Hecke236
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 Hecke260
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 Theory274
5.4.4 Picking the Correct α 277
5.4.5 Algorithmic Kummer Theory When $\zeta_n \in K$ Using Artin278
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 Artin284
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 ℓth 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