DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

ALGEBRAIC NUMBER THEORY

SECOND EDITION

$$\forall \quad x, y, z, n \in \mathbb{N}, \quad n > 2, \quad x^n + y^n \neq z^n$$

Richard A. Mollin

CRC Press
Taylor & Francis Group

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

ALGEBRAIC NUMBER THEORY

SECOND EDITION

Richard A. Mollin

University of Calgary

Alberta, Canada

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

R. B. J. T. Allenby and Alan Slomson, How to Count: An Introduction to Combinatorics, Third Edition

Donald Bindner and Martin Erickson, A Student's Guide to the Study, Practice, and Tools of Modern Mathematics

Juergen Bierbrauer, Introduction to Coding Theory

Francine Blanchet-Sadri, Algorithmic Combinatorics on Partial Words

Richard A. Brualdi and Dragoš Cvetković, A Combinatorial Approach to Matrix Theory and Its Applications

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

Charalambos A. Charalambides, Enumerative Combinatorics

Gary Chartrand and Ping Zhang, Chromatic Graph Theory

Henri Cohen, Gerhard Frey, et al., Handbook of Elliptic and Hyperelliptic Curve Cryptography

Charles J. Colbourn and Jeffrey H. Dinitz, Handbook of Combinatorial Designs, Second Edition

Martin Erickson, Pearls of Discrete Mathematics

Martin Erickson and Anthony Vazzana, Introduction to Number Theory

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Mark S. Gockenbach, Finite-Dimensional Linear Algebra

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Second Edition

Jonathan L. Gross, Combinatorial Methods with Computer Applications

Jonathan L. Gross and Jay Yellen, Graph Theory and Its Applications, Second Edition

Jonathan L. Gross and Jay Yellen, Handbook of Graph Theory

David S. Gunderson, Handbook of Mathematical Induction: Theory and Applications

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression, Second Edition

Darel W. Hardy, Fred Richman, and Carol L. Walker, Applied Algebra: Codes, Ciphers, and Discrete Algorithms, Second Edition

Titles (continued)

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

Silvia Heubach and Toufik Mansour, Combinatorics of Compositions and Words

Leslie Hogben, Handbook of Linear Algebra

Derek F. Holt with Bettina Eick and Eamonn A. O'Brien, Handbook of Computational Group Theory

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Neil P. Sigmon, and Ernest L. Stitzinger, Applications of Abstract Algebra with Maple™ and MATLAB®, Second Edition

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

William Kocay and Donald L. Kreher, Graphs, Algorithms, and Optimization

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

C. C. Lindner and C. A. Rodger, Design Theory, Second Edition

Hang T. Lau, A Java Library of Graph Algorithms and Optimization

Elliott Mendelson, Introduction to Mathematical Logic, Fifth Edition

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Richard A. Mollin, Advanced Number Theory with Applications

Richard A. Mollin, Algebraic Number Theory, Second Edition

Richard A. Mollin, Codes: The Guide to Secrecy from Ancient to Modern Times

Richard A. Mollin, Fundamental Number Theory with Applications, Second Edition

Richard A. Mollin, An Introduction to Cryptography, Second Edition

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Carlos J. Moreno and Samuel S. Wagstaff, Jr., Sums of Squares of Integers

Dingyi Pei, Authentication Codes and Combinatorial Designs

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Alexander Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations

Jörn Steuding, Diophantine Analysis

Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

W. D. Wallis, Introduction to Combinatorial Designs, Second Edition

W. D. Wallis and J. C. George, Introduction to Combinatorics

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number: 978-1-4398-4598-1 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

For Kate Mollin

Contents

Preface

This is the second edition of a text that is intended for a one-semester course in algebraic number theory for senior undergraduate and beginning graduate students. The Table of Contents on pages vii–viii is essentially self-descriptive of each chapter's contents, requiring no need for repetition here. What differs from the first edition deserves elucidation. Comments from numerous instructors and students over more than a decade since the first edition appeared have given way to a new style, methodology, and presentation.

The focus has changed from the first edition approach of introducing algebraic numbers and number fields in the first two chapters and leaving ideals until Chapter 3, to the second edition strategy of looking at integral domains, ideals and unique factorization in Chapter 1 and field extensions including Galois theory in Chapter 2. This changes the first edition method of having the entirety of Galois theory relegated to an appendix and bringing it, in this edition, to the main text in a more complete, comprehensive, and involved fashion. Chapter 3 in this edition is devoted to the study of class groups, and as a new feature, not touched in the first edition, we include the study of binary quadratic forms and comparison of the ideal and form class groups, which leads into the general ideal class group discussion and paves the way for the geometry of numbers and Dirichlet's Unit Theorem. In the first edition, this was done in Chapter 2 along with applications to the number field sieve. In this edition, the applications are put into a separate Chapter 4 including the number field sieve in §4.5, introduced via §4.4 on factoring, including Pollard's cubic factoring algorithm, which is more comprehensive than that of the first edition. In turn, §4.1–§4.3 are applications leading to the latter that involve solutions of Diophantine equations including Bachet, Fermat, and prime power representation. This includes Kummer's proof of Fermat's Last Theorem (FLT) for regular primes, Case I, which was put into Chapter 3 in the first edition. This edition maintains the inclusion of Bernoulli numbers, the Riemann zeta function, and connections via von Staudt–Clausen to the infinitude of irregular primes. Applications also appear at the end of Chapter 5 with an overview of primality testing and, as an application of the Kronecker–Weber Theorem, Lenstra's primality test employing the Artin symbol. A special case of this test is presented as the Lucas–Lehmer test for Mersenne primes.

Chapter 5 replaces Chapter 4 of the first edition in its discussion of ideal decomposition in number fields but spreads out the number of sections to more evenly present the material. One feature of the second edition that distinguishes it from the first is that there is much less emphasis on using exercises with the framework of proofs in the main text. Exercises are referenced in the proofs only when they represent material that is routine and more appropriate for a student to do. Throughout the text, this is one of the major changes. In particular, in the proof of the Kronecker–Weber Theorem, as well as in the proofs of the reciprocity laws in Chapter 6, what were exercises in the first edition are now explained in full in the main text. Moreover, exercises in this edition are designed to test and challenge the reader, as well as illustrate concepts both within the main text as well as extend those ideas. For instance, in the exercises for §2.1, Galois theory is expanded from the number field case to finite fields and general fields of characteristic zero which is then invoked in §5.4 to discuss residue class fields and connections with the Frobenius automorphism. Thus, the reader is led at a measured pace through the material to a clear understanding of the pinnacles of algebraic number theory. What is *not* included from the first edition is any separate discussion of elliptic curves. This is done to make the text more self-contained as a one-semester course for which the addition of the latter is better placed in a related course such as given in [54]. Also, the numbering system has changed from the first edition *consecutive* numbering of all objects to the standard method in this edition.

◆ Features of This Text

- The book is ideal for the student since it is *exercise-rich* with over 310 problems. The more challenging exercises are marked with the symbol ✰. Also, complete and detailed solutions to all of the *odd-numbered exercises* are given in the back of the text. Throughout the text, the reader is encouraged to solve exercises related to the topics at hand. Complete and detailed solutions of the *even-numbered exercises* are included in a *Solutions Manual*, which is available from the publisher for the qualified instructor.

- The text is *accessible* to anyone, from the senior undergraduate to the research scientist. The main prerequisites are the basics of a first course in abstract algebra, the fundamentals of an introductory course in elementary number theory, and some knowledge of basic matrix theory. In any case, the appendices, as described below, contain a review of all of the requisite background material. Essentially, the mature student, with a knowledge of algebra, can work through the book without any serious impediment or need to consult another text.

- There are *more than forty mini-biographies* of those who helped develop algebraic number theory from its inception. These are given, unlike the footnote approach of the first edition, in boxed highlighted text throughout, to give a human face to the mathematics being presented, and set so they do not interfere with the flow of the discourse. Thus, the reader has immediate information at will, or may treat them as digressions, and access them later without significantly interfering with the main mathematical text at hand. Our appreciation of mathematics is deepened by a knowledge of the lives of these individuals. I have avoided the current convention of gathering notes at the end of each chapter, since the immediacy of information is more important.

- There are *applications* via factoring, primality testing, and solving Diophantine equations as described above. In §4.5, we also discuss the applications to cryptography.

- The *appendices* are given, for the convenience of the reader, to make the text self-contained. Appendix A is a meant as a convenient *fingertip reference* for *abstract algebra* with an overview of all the concepts used in the main text. Appendix B is an overview of *sequences and series*, including all that is required to develop the concepts. Appendix C consists of the *Greek alphabet with English transliteration.* Students and research mathematicians alike have need of the latter in symbolic presentations of mathematical ideas. Thus, it is valuable to have a table of the symbols, and their English equivalents readily at hand. Appendix D has a table of numerous *Latin phrases* and their *English equivalents*, again important since many Latin phrases are used in mathematics, and historically much mathematics was written in Latin such as Bachet's Latin translation of Diophantus' Greek book *Arithmetica.*

- The *list of symbols* is designed so that the reader may determine, at a glance, on which page the first defining occurrence of a desired notation exists.

- The *index* has over *two thousand entries*, and has been devised in such a way to ensure that there is maximum ease in getting information from the text. There is maximum cross-referencing to ensure that the reader will find ease-of-use in extracting information to be paramount.

- The *bibliography* has over seventy entries for the reader to explore concepts not covered in the text or to expand knowledge of those covered. This includes a page reference for each and every citing of a given item, so that no guesswork is involved as to where the reference is used.

- The Web page cited in the penultimate line will contain a file for comments, and any typos/errors that are found. Furthermore, comments via the e-mail address on the bottom line are also welcome.

◆ **Acknowledgments** The author is grateful for the proofreading done by the following people: John Burke (U.S.A.), Bart Goddard (U.S.A.), Sebastian Linder, and Matt Tesarski (Canada—both students of mine in 2010), Keith Matthews (Australia), Anitha Srinivasan (India), Gopala Srinivasan (India), and Thomas Zapplachinski (Canada—former student, now cryptographer in the field).

Richard Mollin, Calgary, Canada
website: http://www.math.ucalgary.ca/~ramollin/
email: ramollin@math.ucalgary.ca

About the Author

Richard Anthony Mollin is a professor in the mathematics department at the University of Calgary. Over the past quarter century, he has been awarded six Killam Resident Fellowships. He has written over 200 publications including 12 books in algebra, number theory, and computational mathematics. He is a past member of the Canadian and American Mathematical Societies, the Mathematical Association of America and is a member of various editorial boards. He has been invited to lecture at numerous universities, conferences and scientific society meetings and has held several research grants from universities and governmental agencies. He is the founder of the Canadian Number Theory Association and hosted its first conference and a NATO Advanced Study Institute in Banff in 1988—see [47]–[48].

On a personal note—in the 1970s he owned a professional photography business, *Touch Me with Your Eyes*, and photographed many stars such as Paul Anka, David Bowie, Cher, Bob Dylan, Peter O'Toole, the Rolling Stones, and Donald Sutherland. His photographs were published in *The Toronto Globe* and *Mail* newspapers as well as *New Music Magazine* and elsewhere. Samples of his work can be viewed online at
http://math.ucalgary.ca/∼ramollin/pixstars.html.

His passion for mathematics is portrayed in his writings—enjoyed by mathematicians and the general public. He has interests in the arts, classical literature, computers, movies, and politics. He is a patron and a benefactor of the Alberta Ballet Company, Alberta Theatre Projects, the Calgary Opera, the Calgary Philharmonic Orchestra, and Decidedly Jazz Danceworks. His love for life comprises cooking, entertaining, fitness, health, photography, and travel, with no plans to slow down or retire in the foreseeable future.

Suggested Course Outlines

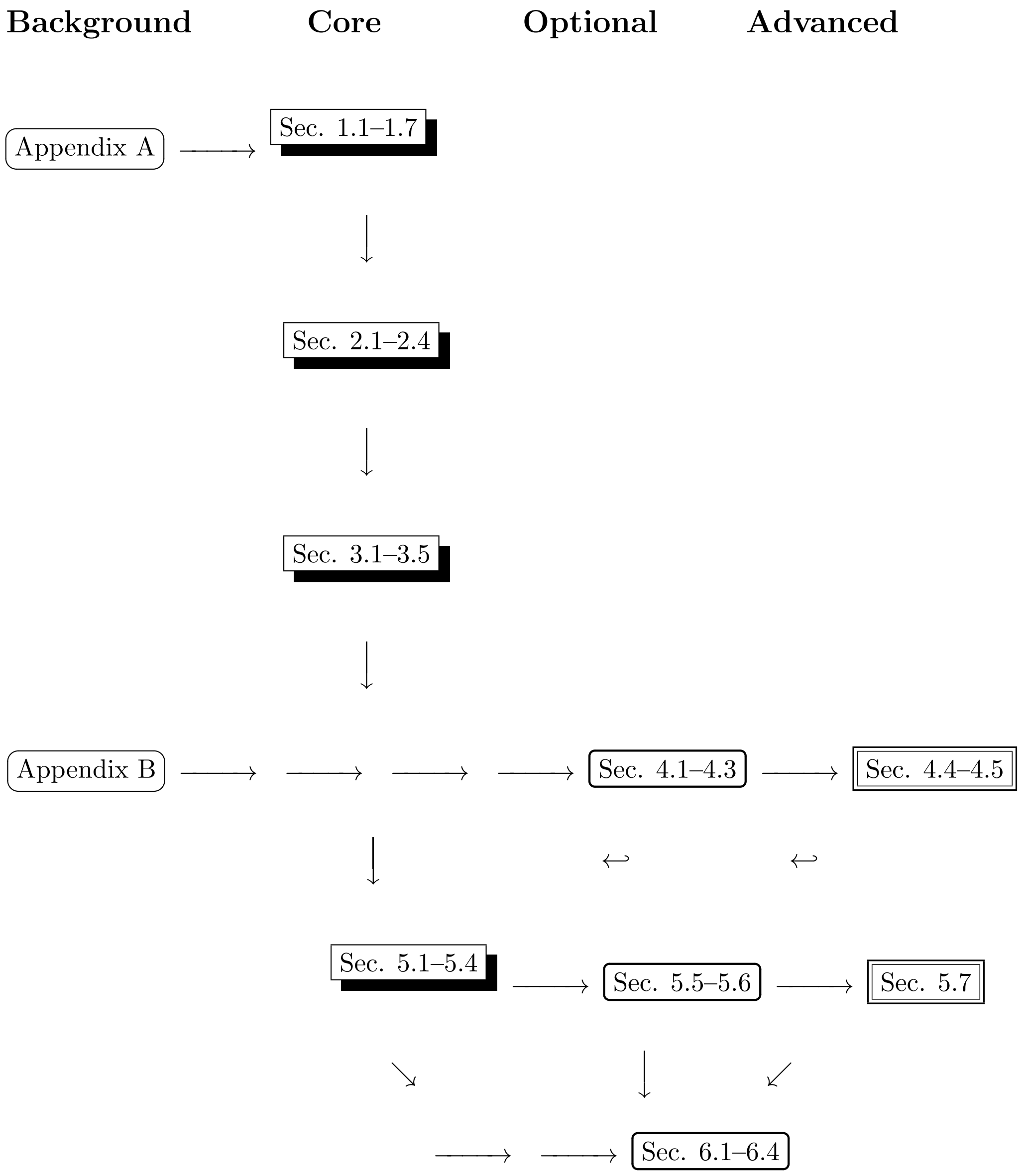
A glance at the Table of Contents will reveal that there is a wealth of material beyond a basic course in algebraic number theory. This section is intended for the instructor, by giving several routes from a course in the basics of algebraic number theory to a more advanced course with numerous applications, as well as other aspects such as Kummer's proof of FLT for regular primes, and advanced reciprocity laws.

Chapters 1 through 3 are essential as a foundation, whereas Chapter 4 is optional, and the instructor may skip it or add any section as an application of the material in the previous chapters. §4.4–§4.5 go together as advanced material on factoring, with §4.4 preparatory material using Pollard's algorithm to set the stage for the description of the number field sieve in §4.5.

In §5.1–§5.4, the groundwork is laid for ramification theory. However, in §5.5, the theory of Kummer extensions and applications to Kummer's proof of FLT for regular primes in the second case may be eliminated from a basic course in algebraic number theory. §5.6 on the proof of the Kronecker–Weber theorem, is a significant application of what has gone before, but is again not necessary for a basic course. §5.7 is an applications section on primality testing.

In a *bare-bones* course, one does not need to proceed into Chapter 6. However, the chapter illustrates some of the pinnacles of algebraic number theory with proofs of the cubic, biquadratic, and Eisenstein reciprocity laws, as well as development of the Stickelberger relation. In a more advanced course, these topics should be included. The following diagram is a schematic flow-chart to illustrate the possible routes for the course, from the most basic course to one filled with applications.

Course Outlines



Chapter 1

Integral Domains, Ideals, and Unique Factorization

> *Take care of your body with steadfast fidelity. The soul must see through these eyes alone, and if they are dim, the whole world is clouded.*
> **Johann Wolfgang von Goethe (1749–1832), German poet, novelist, and dramatist**

In this chapter, we introduce integral domains, and develop the concepts of divisibility, irreducibility, and primes which we apply to Dedekind domains. This preamble allows us to develop Noetherian, principal ideal, and unique factorization domains later in the chapter thereby setting the foundation for the introduction of algebraic number rings and number fields. The reader should be familiar with some basic abstract algebra, such as groups, rings, and fields and their properties, which are reviewed in Appendix A, starting on page 319, for convenience and finger-tip reference.

1.1 Integral Domains

In order to define concepts in the sequel, we will need the following.

Definition 1.1 — Units

An element α in a commutative ring R with identity 1_R is called a *unit* in R when there is a $\beta \in R$ such that $\alpha\beta = 1_R$. The multiplicative group of units in R is denoted by $\mathfrak{U}_R$—see Exercise 1.7 on page 6.

Example 1.1 In $\mathbb{Z}[\sqrt{2}] = R$, $1 + \sqrt{2}$ is a unit, since

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1_R = 1.$$

For the following, recall that a *zero divisor* in a commutative ring R is a nonzero element $\alpha \in R$ such that $\alpha\beta = 0$ where $\beta \neq 0$.

Definition 1.2 — Integral Domains

An *integral domain* is a commutative ring D with identity 1_D, having no zero divisors. In particular, if every nonzero element is a unit, then D is a field.

Application 1.1 — The Cancellation Law

One of the most important properties of an integral domain D is that the *cancellation law* holds, namely if α,β $\in D$ with α nonzero and $\alpha\beta = \alpha\gamma$, then $\beta = \gamma$.

Example 1.2 The ordinary or *rational integers*

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

provide us with our first example of an integral domain.

Example 1.3 For any nonsquare integer n,

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$$

is an example of an integral domain. For example, if $n = -1$, we have the Gaussian integers. Indeed, $n = -1$ yields $\sqrt{-1} = i$ which is an example of a special kind of unit, the generalization of which we now define.

Definition 1.3 — Primitive Roots of Unity

For $m \in \mathbb{N} = \{1, 2, 3, \ldots\}$ *the natural numbers* ζ_m denotes *a primitive* m^{th} *root of unity*, which is a root of $x^m - 1$, but not a root of $x^d - 1$ for any natural number $d < m$.

Example 1.4 With reference to Example 1.3, where $n = -1$, $\sqrt{-1} = i = \zeta_4$ is a primitive fourth root of unity, since it is a root of $x^4 - 1$, but not root of $x^j - 1$ for $j = 1, 2, 3$. Also,

$$\zeta_3 = (-1 + \sqrt{-3})/2$$

is a primitive cube root of unity, since it is a root of $x^3 - 1$, but clearly not a root of $x^2 - 1$ or $x - 1$.

Example 1.5 Suppose that p is a prime and ζ_p is a primitive p-th root of unity. If we set

$$x = \sum_{j=0}^{p-1} \zeta_p^j$$

then

$$x\zeta_p = \sum_{j=0}^{p-1} \zeta_p^{j+1} = \sum_{j=0}^{p-1} \zeta_p^j = x. \tag{1.1}$$

Thus, if $x \neq 0$, dividing through (1.1) by x gives $\zeta_p = 1$, a contradiction. Thus,

$$1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0.$$

This fact will prove useful when discussing notions surrounding roots of unity later in the text—see Exercise 2.25 on page 69, for instance. Also, we generalize this example in Exercise 6.28 on page 310.

Example 1.3 is a motivator for the more general concept, which later turns out to be the so-called "ring of integers of a quadratic field"—see Theorem 1.28 on page 45.

Application 1.2 — Quadratic Domains and Norms

If n is a nonsquare integer, then $\mathbb{Z}[\sqrt{n}]$ is an integral domain as given in Example 1.3, where we note that $\mathbb{Z}[\sqrt{n}]$ is a subset of the field $\mathbb{Q}(\sqrt{n})$. We call domains in $\mathbb{Q}(\sqrt{n})$ *quadratic domains*. There is a slightly larger subset of $\mathbb{Q}(\sqrt{n})$ that is also an integral domain when $n \equiv 1 \pmod 4$—see Exercise 1.1 on page 6

$$\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] \subseteq \mathbb{Q}(\sqrt{n}).$$

Now we may combine Example 1.3 with this application to describe some special quadratic domains as follows. Define

$$\mathbb{Z}[\omega_n] = \{a + b\omega_n : a, b \in \mathbb{Z}\},$$

where

$$\omega_n = \begin{cases} (1+\sqrt{n})/2 & \text{if } n \equiv 1 \pmod 4, \\ \sqrt{n} & \text{if } n \not\equiv 1 \pmod 4. \end{cases}$$

Then $\mathbb{Z}[\omega_n]$ is a *quadratic domain*.

Another concept we will see in greater generality later, but applied here to quadratic domains, is the *quadratic norm* $N : \mathbb{Q}(\sqrt{n}) \mapsto \mathbb{Q}$ via

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2 \in \mathbb{Q}.$$

In particular, by Exercise 1.3

$$\alpha \in \mathfrak{U}_{\mathbb{Z}[\omega_n]} \text{ if and only if } N(\alpha) = \pm 1.$$

We will be using the concept of a norm throughout our discussion to establish properties of, in this case, quadratic domains, or in general, rings of integers, that we have yet to define—see Definition 1.30 on page 36.

The notion of divisibility of elements in an integral domain is a fundamental starting point for understanding how algebraic number theory generalizes the notions of "divisibility," "primality," and related concepts from the integers $\mathbb{Z}$ to other integral domains such as $\mathbb{Z}[\omega_n]$.

Definition 1.4 — Divisors and Trivial Factorizations

If α,$\beta \in D$ an integral domain, then α is said to be a *divisor* of β, if there exists an element $\gamma \in D$ such that $\beta = \alpha\gamma$, denoted by $\alpha \mid \beta$. If α does not divide β, then we denote this by $\alpha \nmid \beta$. If $\beta = \alpha\gamma$, where either $\alpha \in \mathfrak{U}_D$ or $\gamma \in \mathfrak{U}_D$, then this is called a *trivial factorization* of β.

Example 1.6 Consider the notion of units given in Definition 1.1 on page 1 and the illustration given in Example 1.1. Then we have that both $(1+\sqrt{2}) \mid 1$ and $(-1+\sqrt{2}) \mid 1$. Indeed, this may be said to characterize units in D, namely

α is a unit in an integral domain D if and only if $\alpha \mid 1$.

This may be used as an alternative to that of Definition 1.1. The following notion allows for the introduction of a different approach.

Definition 1.5 — Associates

If D is an integral domain and $\alpha,\beta \in D$ with $\alpha \mid \beta$ and $\beta \mid \alpha$, then α and β are said to be *associates*, and we denote this by $\alpha \sim \beta$. If α and β are *not* associates, we denote this by $\alpha \not\sim \beta$.

Example 1.7 From Definition 1.5 and Example 1.6, we see that *α is a unit in an integral domain D if and only if* $\alpha \sim 1$. Furthermore, if $\alpha \sim \beta$ for any $\alpha,\beta \in D$, then there is a unit $u \in D$ such that $\alpha = u\beta$. To see this, since $\alpha \mid \beta$, then there is a $\gamma \in D$ such that $\beta = \gamma\alpha$. Conversely since $\beta \mid \alpha$, there is a $\delta \in D$ such that $\alpha = \delta\beta$. Hence, $\alpha = \delta\beta = \delta\gamma\alpha$, so by the cancellation law exhibited in Application 1.1 on page 2, $1 = \delta\gamma$, so $\delta = \gamma^{-1} = u$ is a unit and $\alpha = u\beta$.

Example 1.8 In $\mathbb{Z}[\sqrt{10}]$, $2+\sqrt{10} \sim 16+5\sqrt{10}$ since

$$16+5\sqrt{10} = (2+\sqrt{10})(3+\sqrt{10}),$$

so $(2+\sqrt{10}) \mid (16+5\sqrt{10})$, and

$$2+\sqrt{10} = (16+5\sqrt{10})(-3+\sqrt{10})$$

so $(16+5\sqrt{10}) \mid (2+\sqrt{10})$.

Example 1.9 Since

$$6 = (4+\sqrt{10})(4-\sqrt{10}),$$

$$\text{then } (4 \pm \sqrt{10}) \mid 6 \text{ in } \mathbb{Z}[\sqrt{10}].$$

Notice that $6 = 2 \cdot 3$ so it appears that 6 does not have a “uniqueness of factorization” in $\mathbb{Z}[\sqrt{10}]$ in some sense that we now must make clear and rigorous. Now we develop the notions to describe this phenomenon which is distinct from $\mathbb{Z}$ where 6 *does* have unique factorization via the Fundamental Theorem of Arithmetic. In fact, in $\mathbb{Z}$, a *prime*, is defined to be an integer p such that the only divisors are ± 1 and $\pm p$. Thus, primes satisfy that

$$\text{if } p \mid ab, \text{ then either } p \mid a \text{ or } p \mid b \tag{1.2}$$

—see [53, Lemma 1.2, p. 32]. Also, primes in $\mathbb{Z}$ satisfy that

$$\text{if } p = ab, \text{ then } a = \pm 1 \text{ or } b = \pm 1. \tag{1.3}$$

The following generalizes property (1.3) to arbitrary integral domains. Then we will discuss property (1.2) and show how (1.2)–(1.3) generalize to similar notions in general integral domains.

Definition 1.6 — Irreducibles

If D is an integral domain and a nonzero, nonunit element $\beta \in D$ satisfies the property that whenever $\beta = \alpha\gamma$, then either $\alpha \in \mathfrak{U}_D$ or $\gamma \in \mathfrak{U}_D$, then β is said to be *irreducible*. In other words, the irreducible elements of D are the nonzero, nonunit elements having only trivial factorizations. If a nonzero, nonunit element of D is not irreducible, it is called a *reducible element*.

Example 1.10 Any prime $p \in \mathbb{Z}$ is irreducible, since its only factorizations are $p = (\pm 1)(\pm p)$. Conversely, if $n \in \mathbb{Z}$ is irreducible, then the only factorizations are trivial so n is prime in $\mathbb{Z}$. In other words, in $\mathbb{Z}$, p is prime if and only if it is irreducible. This fails to be the case in arbitrary integral domains and this provides the fodder for algebraic number theory.

Example 1.11 Consider

$$D = \mathbb{Z}[\sqrt{10}] \text{ and } \beta = 4 + \sqrt{10}.$$

If β is not irreducible, then $\beta = \alpha\gamma$, where neither α nor γ is a unit in $\mathbb{Z}[\sqrt{10}]$. Since

$$N(\beta) = N(\alpha)N(\gamma)$$

by Exercise 1.2 on the next page, then without loss of generality

$$N(\alpha) = N(a + b\sqrt{10}) = 3,$$

where $\alpha = a + b\sqrt{10}$. Thus, $a^2 - 10b^2 = 3$ so the Legendre symbol equality holds:

$$-1 = \left(\frac{3}{5}\right) = \left(\frac{a^2 - 10b^2}{5}\right) = \left(\frac{a^2}{5}\right) = \left(\frac{a}{5}\right)^2 = 1,$$

a contradiction, so $4 + \sqrt{10}$ is irreducible. Similarly, its conjugate $4 - \sqrt{10}$ is irreducible. Via Example 1.9, we have $4 \pm \sqrt{10}$ divides 6 but by Exercise 1.4, $4 \pm \sqrt{10}$ divides neither 2 nor 3. This motivates the next concept, generalizing (1.2).

Definition 1.7 — Primes

If β is a nonzero, nonunit in an integral domain D, then β is called a *prime* if whenever $\beta \mid \alpha\gamma$, then either $\beta \mid \alpha$ or $\beta \mid \gamma$.

Example 1.12 From Example 1.11 we see that $4 \pm \sqrt{10}$ are not primes in $\mathbb{Z}[\sqrt{10}]$. Now we show that $2, 3$ are not primes in $\mathbb{Z}[\sqrt{10}]$ (although they *are* primes in $\mathbb{Z}$). From Example 1.9, 2 and 3 both divide $(4 + \sqrt{10})(4 - \sqrt{10})$. However, by Exercise 1.4 on the following page, neither of them divides $4 \pm \sqrt{10}$, so neither is prime. Yet by Exercise 1.4 both are irreducible. This illustrates the departure, in general integral domains, from the case in $\mathbb{Z}$, where *all* irreducibles are prime as shown in Example 1.10. Yet, the following shows us that primes are always irreducible.

Theorem 1.1 — Primes Are Irreducible

If D is an integral domain and $\beta \in D$ is prime, then β is irreducible.

Proof. Let $\beta \in D$ be prime and suppose that $\beta = \alpha\gamma$. Then *a fortiori*, $\beta \mid \alpha\gamma$ so $\beta \mid \alpha$ or $\beta \mid \gamma$. Without loss of generality, assume that $\beta \mid \alpha$. Then there is a $\delta \in D$ such that $\alpha = \beta\delta$. It follows that $\beta = \alpha\gamma = \beta\delta\gamma$, so by Application 1.1 on page 2, $1 = \delta\gamma$, which makes γ a unit in D. Hence, β is irreducible. □

Remark 1.1 We have seen that the converse of Theorem 1.1 does not hold. Now our task is to determine those integral domains for which it *does* hold. This will involve making precise the notion of "unique factorization" of elements in general integral domains. We begin this delineation in §1.2.

Exercises

1.1. Let n be a nonsquare integer. Prove that if $n \equiv 1 \pmod 4$, then the subring

$$\mathbb{Z}[\omega_n] \subseteq \mathbb{Q}(\sqrt{n})$$

given in Application 1.2 on page 3, is an integral domain. Conclude that $\mathbb{Z}[\sqrt{n}]$, for any nonsquare n, is an integral domain by similar reasoning.

1.2. Prove that norms in quadratic domains are multiplicative, i.e. $N(\alpha\gamma) = N(\alpha)N(\gamma)$.

1.3. Prove that an element α in $\mathbb{Z}[\omega_n]$ is a unit if and only if $N(\alpha) = \pm 1$.

1.4. Prove that in a quadratic domain D, if $\alpha \mid \beta$ in $\mathbb{Z}[\omega_D]$, then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$. Conclude that $4 \pm \sqrt{10}$ are not associates of either 2 or 3 in $\mathbb{Z}[\sqrt{10}]$. Also, conclude that 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{10}]$.

1.5. Let $D = \mathbb{Z}[\omega_n]$ be a quadratic domain and let $\alpha \in D$ satisfy the property that $|N(\alpha)| = p$, a prime in $\mathbb{Z}$. Prove that α is irreducible in D. Provide either a proof or a counterexample to the converse: *If $\alpha \in D$ is an irreducible element, then $|N(\alpha)|$ is a prime in $\mathbb{Z}$.*

1.6. Prove that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

1.7. Prove that the units of an integral domain form a multiplicative abelian group.

1.8. Prove that the relation $\sim$ given in Definition 1.5 on page 4, is an equivalence relation, namely that it is *reflexive*: $a \sim a$, *symmetric*: $a \sim b$ implies $b \sim a$, and *transitive*: if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in D$.

1.9. Prove that in an integral domain D an element α is irreducible if and only if every divisor of α is either an associate of α or a unit.

1.10. If D is a quadratic domain show that if $\alpha,\beta \in D$ with $\alpha \sim \beta$, then $|N(\alpha)| = |N(\beta)|$.

1.11. Is the converse of Exercise 1.10 true? If so prove it, and if not, provide a counterexample.

1.12. Find an $\alpha \in \mathbb{Z}[\sqrt{15}]$ such that $\alpha = \alpha_1\alpha_2 = \beta_1\beta_2$ where α_j, β_j are irreducible for $j = 1, 2$ but neither of α_1, α_2 is an associate of β_j for $j = 1, 2$.

1.13. Apply the question in Exercise 1.12 to $\mathbb{Z}[\sqrt{30}]$.

1.14. Show that $1 + i = 1 + \sqrt{-1}$ is prime in the Gaussian integers $\mathbb{Z}[i]$.

1.15. Find all units in the Gaussian integers $\mathbb{Z}[i]$.

1.16. Prove that $\pm(1+\sqrt{2})^n \in \mathfrak{U}_{\mathbb{Z}[\sqrt{2}]}$ for all $n \in \mathbb{Z}$. Prove that there are no other units in $\mathbb{Z}[\sqrt{2}]$. In other words, show that

$$\mathfrak{U}_{\mathbb{Z}[\sqrt{2}]} = \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}.$$

1.17. If D is an integral domain and $\alpha,\beta \in D$, not both zero, then $\gamma \in D$ is called *a greatest common divisor* (gcd) *of α and β* if the following two conditions are satisfied.

(a) $\gamma \mid \alpha$, and $\gamma \mid \beta$.

(b) If $\sigma \mid \alpha$, and $\sigma \mid \beta$ for some $\sigma \in D$, then $\sigma \mid \gamma$.

Prove that any two gcds must be associates. Also, provide an example of a ring in which elements exist that have no greatest common divisor.

1.2 Factorization Domains

> *Not everything that can be counted counts, and not everything that counts can be counted.* (Attributed)
>
> **Albert Einstein (1879–1955), German-born theoretical physicist**

In this section we explore and solidify the notions of unique factorization in certain integral domains and the intimate connection with the core features of algebraic number theory which this engenders.

Definition 1.8 — Factorization Domains

If D is an integral domain in which every nonzero, nonunit can be represented as a finite product of irreducible elements of D, then D is called a *factorization domain.* A factorization domain in which any nonzero, nonunit can be expressed as a product of irreducibles that is unique up to units and the order of the factors is called a *unique factorization domain* (UFD).

Remark 1.2 Definition 1.8 says that D is a unique factorization domain when the following occurs. Suppose that $\alpha \in D$ is arbitrarily chosen with

$$\alpha = u\gamma_1^{a_1}\gamma_2^{a_2}\cdots\gamma_n^{a_n}$$

where $u \in D$ is a unit, $n, a_j \in \mathbb{N}$ and γ_j is irreducible for $j = 1, 2, \ldots, n$. Then D is a unique factorization domain if any other representation:

$$\alpha = v\kappa_1^{b_1}\kappa_2^{b_2}\cdots\kappa_m^{b_m}$$

where $v \in D$ is a unit, $m, b_j \in \mathbb{N}$, and κ_j is irreducible for $j = 1, 2, \ldots, m$, implies that $m = n$ and after possibly rearranging the γ_j, we have $\gamma_j = \kappa_j$, and $a_j = b_j$ for $j = 1, 2, \ldots, n$.

Now we look at a criterion for a factorization domain to be a unique factorization domain in terms of the concepts we studied in §1.1. This will be the defining feature of such domains in terms of these concepts.

Theorem 1.2 — Unique Factorization—Irreducibles Are Prime

If D is a factorization domain, then D is a unique factorization domain if and only if every irreducible element of D is prime.

Proof. Assume that all such factorizations are unique. If $\alpha \in D$ is irreducible, we must show that α is prime. If $\alpha \bigm| \gamma\beta$, there exists a $\sigma \in D$ such that $\gamma\beta = \alpha\sigma$. Each of β, γ, σ has unique factorization, so write

$$\beta = u\prod_{j=1}^{r}\beta_j, \qquad \gamma = v\prod_{j=1}^{s}\gamma_j, \qquad \sigma = w\prod_{j=1}^{t}\sigma_j,$$

where $u, v, w \in \mathfrak{U}_D$, and each $\beta_j, \gamma_j, \sigma_j$ is irreducible. Thus,

$$\alpha w\prod_{j=1}^{t}\sigma_j = \alpha\sigma = \gamma\beta = vu\prod_{j=1}^{s}\gamma_j\prod_{j=1}^{r}\beta_j.$$

Since α is irreducible, then by unique factorization, α is an associate of one of the β_j or γ_j. In other words, $\alpha \mid \beta$, or $\alpha \mid \gamma$, so α is prime.

Conversely, assume that every irreducible in D is prime. Suppose that

$$u\alpha_1 \cdots \alpha_r = v\beta_1 \cdots \beta_s \text{ for } r \geq s \geq 1, \text{ and } u, v \in \mathfrak{U}_{\mathfrak{O}_F}, \tag{1.4}$$

with α_j, β_j irreducible. We must show that $r = s$, and that each α_j is an associate of some β_k. We use induction on r. If $r = 1$, then $s = 1$, so we are done. Assume that unique factorization holds for all factorizations of length at most $r - 1 \geq 1$. Since $\beta_s \mid u\alpha_1 \cdots \alpha_r$, then $\beta_s \mid \alpha_i$ for some $i \in \{1, 2, \ldots, r\}$, since β_s is not a unit. Thus, β_s is an associate of α_i. Renumber the α_j so that $\alpha_i = \alpha_r$. Thus, by Application 1.1 on page 2, we may cancel the $\alpha_r = \beta_s w$ (where w is a unit) from each side of Equation (1.4) to get

$$u\alpha_1 \cdots \alpha_{r-1} = w^{-1}v\beta_1 \cdots \beta_{s-1}.$$

By the induction hypothesis, $r - 1 = s - 1$, and the α_j are associates of the β_j. The result now follows by induction. □

Remark 1.3 Theorem 1.2 provides the key to understanding unique factorization in integral domains, namely *the failure of unique factorization is the* failure *of (some) set of irreducibles to be prime.*

In Exercise 1.17 on page 6 we defined *greatest common divisors* in integral domains, but there, only sought to find domains *without* gcds. Now we will look at an example of an integral domain where such divisors *always* exist. This provides a motivator for a more general class of domains where there is a "norm" similar to that we found in quadratic domains introduced in Application 1.2 on page 3. These domains are important in our understanding of the basics. First we need to establish a division algorithm. [1.1]We specialize to Gaussian integers as a motivator for what follows. Recall from the definition in Application 1.2 on page 3 that the norm N is defined for any quadratic domain.

Theorem 1.3 — Division Algorithm for Gaussian Integers

Let α,β $\in \mathbb{Z}[i]$ with $\beta \neq 0$. Then there exists σ,δ $\in \mathbb{Z}[i]$ such that

$$\alpha = \beta\sigma + \delta,$$

where $0 \leq N(\delta) < N(\beta)$.

Proof. Let $\alpha/\beta = c + di \in \mathbb{C}$. Set

$$f = \lfloor c + 1/2 \rfloor = Ne(c), \text{ and } g = \lfloor d + 1/2 \rfloor = Ne(d),$$

where $Ne(x)$ is the *nearest integer function.* Here $\lfloor y \rfloor$ is the floor function or greatest integer function—see [53, §2.5]. Hence, there are k,ℓ $\in \mathbb{R}$ such that

$$|k| \leq 1/2, \text{ and } |\ell| \leq 1/2 \tag{1.5}$$

[1.1] The term *algorithm* is derived from the Persian mathematician Mohammed ibn Musa al-Khowarizmi *Mohammed, son of Moses of Kharezm, now Khiva* (circa 790–850 A.D.). His book *Algorithmi de Numero Indorum*, the Latin translation of the no longer extant original Arabic text, was highly influential in bringing the Hindu-Arabic number system to Europe. Shortly after the appearance of these Latin translations, readers began contracting his name to *algorism*, and ultimately *algorithm*, which we use today to mean any methodology following a set of rules to achieve a goal.

with

$$c + di = (f + k) + (g + \ell)i. \tag{1.6}$$

Set

$$\sigma = f + gi \text{ and } \delta = \alpha - \beta\sigma. \tag{1.7}$$

Then it remains to show

$$0 \le N(\delta) < N(\beta).$$

We know that $N(\delta) \ge 0$, since the norm is just a sum of two squares. Now we show that $N(\delta) < N(\beta)$.

By Exercise 1.2 on page 6 (the multiplicativity of the norm), we have

$$N(\delta) = N(\alpha - \beta\sigma) = N((\alpha/\beta - \sigma)\beta)$$

$$= N(\alpha/\beta - \sigma)N(\beta) = N(c + di - \sigma)N(\beta).$$

However, from (1.6)–(1.7), we get

$$c + di - \sigma = c + di - (f + gi) = (c - f) + (d - g)i = k + \ell i.$$

Therefore, by (1.5),

$$N(\delta) = N(k + \ell i)N(\beta) =$$

$$(k^2 + \ell^2)N(\beta) \le ((1/2)^2 + (1/2)^2)N(\beta) \le N(\beta)/2 < N(\beta),$$

as required. □

Remark 1.4 The σ in Theorem 1.3 is called a *quotient* and the δ is called a *remainder* of the division. This follows the notions for the division algorithm in $\mathbb{Z}$.

Remark 1.5 Although Theorem 1.3 gives us a criterion for the existence of an algorithm for division in $\mathbb{Z}[i]$, there is no uniqueness attached to it. In other words, we may have many such representations as the following illustration demonstrates.

Example 1.13 Let $\alpha = 10 + i$ and $\beta = 2 + 5i$, then we may find $\sigma,\delta \in \mathbb{Z}[i]$ using the techniques established in the proof of Theorem 1.3. We have

$$c + di = \frac{\alpha}{\beta} = \frac{10 + i}{2 + 5i} = \frac{(10 + i)(2 - 5i)}{(2 + 5i)(2 - 5i)} = \frac{25}{29} - \frac{48}{29}i,$$

so

$$f = \left\lfloor c + \frac{1}{2} \right\rfloor = \left\lfloor \frac{25}{29} + \frac{1}{2} \right\rfloor = 1 \text{ and } g = \left\lfloor d + \frac{1}{2} \right\rfloor = \left\lfloor -\frac{48}{29} + \frac{1}{2} \right\rfloor = -2.$$

Therefore, $\sigma = 1 - 2i$ and $\delta = \alpha - \beta\sigma = 10 + i - (2 + 5i)(1 - 2i) = -2$. Moreover, we verify

$$N(\delta) = N(-2) = 4 < N(\beta) = N(2 + 5i) = 29$$

with

$$\alpha = 10 + i = (2 + 5i)(1 - 2i) - 2 = \beta\sigma + \delta. \tag{1.8}$$

However, these choices are not unique since we need not follow the techniques of Theorem 1.3. For instance, if we choose $\sigma = 1 - i$ and $\delta = 3 - 2i$, then

$$\alpha = 10 + i = (2 + 5i)(1 - i) + 3 - 2i = \beta\sigma + \delta, \tag{1.9}$$

where $N(\delta) = 13 < 29 = N(2 + 5i) = N(\beta)$. Thus, by (1.8)–(1.9), we see that, when employing the division algorithm for Gaussian integers, the quotient and remainder are not unique.

Now we look at an integral domain where the existence of gcds is guaranteed, namely the Gaussian integers.

Theorem 1.4 — Gaussian GCDs Always Exist

If $\alpha,\beta \in \mathbb{Z}[i] = D$, where at least one of α or β is not zero, then there exists a gcd $\gamma \in \mathbb{Z}[i]$ of α and β.

Proof. Given fixed $\alpha,\beta \in \mathbb{Z}[i]$, not both zero, set

$$\mathcal{S} = \{N(\sigma\alpha + \rho\beta) > 0 : \sigma,\rho \in \mathbb{Z}[i]\},$$

with $\mathcal{S} \neq \varnothing$ since

$$N(\alpha) = N(1 \cdot \alpha + 0 \cdot \beta), \text{ and } N(\beta) = N(0 \cdot \alpha + 1 \cdot \beta) \tag{1.10}$$

at least one of which is not zero and nonnegative, then at least one of them is in $\mathcal{S}$. Thus, we may employ the well-ordering principle—see page 340—to get the existence of an element $\gamma_0 = \sigma_0\alpha + \rho_0\beta$, for which its norm is the least value in $\mathcal{S}$, namely

$$N(\gamma_0) \leq N(\sigma\alpha + \rho\beta) \text{ for all } \sigma,\rho \in \mathbb{Z}[i].$$

Claim 1.1 γ_0 is a greatest common divisor of α and β.

Let $\tau \in \mathbb{Z}[i]$ with $\tau \mid \alpha$ and $\tau \mid \beta$. Then there exists $\delta_1, \delta_2 \in \mathbb{Z}[i]$ such that $\alpha = \tau\delta_1$ and $\beta = \tau\delta_2$. Hence,

$$\gamma_0 = \sigma_0\alpha + \rho_0\beta = \sigma_0\tau\delta_1 + \rho_0\tau\delta_2 = \tau(\sigma_0\delta_1 + \rho_0\delta_2), \tag{1.11}$$

so $\tau \mid \gamma_0$. It remains to show that γ_0 divides both α and β.

Let

$$\kappa = \lambda_1\alpha + \lambda_2\beta \tag{1.12}$$

be such that $N(\kappa) \in \mathcal{S}$. Thus, by Theorem 1.3 on page 8, there exist $\mu,\nu \in \mathbb{Z}[i]$ such that

$$\kappa = \gamma_0\mu + \nu, \tag{1.13}$$

with

$$0 \leq N(\nu) < N(\gamma_0). \tag{1.14}$$

Also, by (1.12)–(1.13),

$$\nu = \kappa - \gamma_0\mu = \lambda_1\alpha + \lambda_2\beta - (\sigma_0\alpha + \rho_0\beta)\mu = (\lambda_1 - \sigma_0\mu)\alpha + (\lambda_2 - \rho_0\mu)\beta,$$

so if $\nu \neq 0$, then $N(\nu) \in \mathcal{S}$. However, by (1.14), this contradicts the minimality of $N(\gamma_0)$ in $\mathcal{S}$, so $\nu = 0$. We have shown that γ_0 divides every element whose norm is in $\mathcal{S}$. In particular, by (1.10)–(1.11), it divides α and β, which secures claim 1.1. Hence, we have the result. □

Now we may look at the promised extension of the idea of a norm from Gaussian integers to a distinguished class of integral domains, which have more general functions describing them.

Definition 1.9 — Euclidean Domains and Functions

If D is an integral domain, then a mapping $\phi : D \mapsto \mathbb{Z}$ is called a *Euclidean function* if it satisfies the two conditions:

(a) If $\alpha \in D$, $\phi(\alpha\beta) \geq \phi(\alpha)$ for all nonzero $\beta \in D$.

(b) If $\alpha,\beta \in D$ with $\beta \neq 0$, there exist $\gamma,\delta \in D$ such that $\alpha = \gamma\beta + \delta$ and $\phi(\delta) < \phi(\beta)$.

When D possesses a Euclidean function then D is called a *Euclidean domain.*

Example 1.14 In $\mathbb{Z}$, $\phi(z) = |z|$, the usual absolute value, is a Euclidean function. Hence, $\mathbb{Z}$ is a Euclidean domain.

Remark 1.6 In Definition 1.9 part (b), we cannot guarantee the uniqueness of the elements γ,δ. However, there are some distinguished domains for which they are unique.

Example 1.15 If F is a field and $D = F[x]$ is the polynomial ring in the indeterminate x, then

$$\phi(f(x)) = \deg(f(x)),$$

the degree of $f(x) \in D$ is a Euclidean function on D. Note that if $f(x) = 0$, the zero polynomial, then

$$\deg(f(x)) = -1$$

by convention. In this case, the values in part (b) of Definition 1.9 are unique—see [61].

We now examine integral domains having Euclidean functions for which the converse of Theorem 1.1 on page 5 holds, since this is a door leading into domains with unique factorizations via Theorem 1.3 on page 8. First we need the following notion.

Definition 1.10 — Field of Quotients

If D is an integral domain, then the field F consisting of all elements of the form $\alpha\beta^{-1}$ for $\alpha,\beta \in D$ with $\beta \neq 0$ is called the *field of quotients* or simply the *quotient field* of D.

Remark 1.7 There is, in actuality, an isomorphic copy of D in F, but in practice it is standard to assume that D is identified with this copy. In the case of a quadratic domain it is clear from Application 1.2 on page 3 that the quotient field of $\mathbb{Z}[\omega_n]$ is $F = \mathbb{Q}(\sqrt{n})$—see Theorem 1.28 on page 45.

Example 1.16 If F is any field, then the quotient field of the polynomial domain $F[x]$ is the field $F(x)$ of rational functions in x. Moreover, the quotient field of $\mathbb{Z}$ is $\mathbb{Q}$.

Definition 1.11 — Norm-Euclidean Quadratic Domains

A quadratic domain D with quotient field F is said to be *norm-Euclidean* if

$$\text{for any } \rho \in F \text{ there exists a } \sigma \in D \text{ such that } |N(\rho - \sigma)| < 1. \tag{1.15}$$

Now we demonstrate that the condition in Definition 1.11 is tantamount to the norm being a Euclidean function.

Theorem 1.5 Let D be a quadratic domain. Then D is a Euclidean domain with respect to the norm function if and only if condition (1.15) holds.

Proof. Suppose that (1.15) holds. If $\alpha,\beta \in D$ with $\beta \neq 0$, then by Exercise 1.2 on page 6

$$|N(\alpha\beta)| = |N(\alpha)||N(\beta)| \geq |N(\alpha)|$$

which is part (a) of Definition 1.9. It remains to show part (b) holds. If $\alpha,\beta \in D$, then by (1.15) there exists a $\sigma \in D$ such that

$$|N(\alpha/\beta - \sigma)| < 1. \tag{1.16}$$

Hence, if we let

$$\delta = \alpha - \sigma\beta,$$

then

$$|N(\delta)| = |N(\alpha - \sigma\beta)| = |N((\alpha/\beta)\beta - \sigma\beta)| = |N(\alpha/\beta - \sigma)| \cdot |N(\beta)| < |N(\beta)|$$

by (1.16) which establishes (b).

Conversely, if N is a Euclidean function on D, then for any $\rho = \alpha/\beta \in \mathbb{Q}(\sqrt{n})$, with $\alpha,\beta \in D$, we have by part (b) of Definition 1.9 that there exist $\gamma,\delta \in D$ such that

$$\alpha = \gamma\beta + \delta \text{ with } N(\delta) < N(\beta).$$

Therefore

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N\left(\frac{\alpha - \gamma\beta}{\beta}\right) = N\left(\frac{\delta}{\beta}\right) < 1.$$

This establishes (1.16) and so the entire result. □

The following turns out to be one of two possible domains $\mathbb{Z}[\sqrt{n}]$ which is norm-Euclidean for n a negative squarefree integer and we look at the positive case as well. (Note that the other $n < 0$ for which we get Euclidean domains are those of the form $\mathbb{Z}[(1 + \sqrt{n})/2]$—see Theorem 1.28.)

Example 1.17 We show that

$$\phi(a + bi) = a^2 + b^2 = N(a + bi)$$

is a Euclidean function on the Gaussian integers $a + bi \in \mathbb{Z}[i] = D$ using Theorem 1.5.

To see that D is norm-Euclidean, select $\rho = q + ri \in \mathbb{Q}(i)$. We must find $\sigma = a + bi \in D$ with

$$|(q - a)^2 + (r - b)^2| < 1.$$

This is accomplished by choosing:

$$a = Ne(q) \text{ and } b = Ne(r) \text{ where } Ne(x) = \lfloor x + 1/2 \rfloor \text{ for any } x \in \mathbb{R}.$$

It can be shown that the only other squarefree $n < 0$ for which $\mathbb{Z}[\sqrt{n}]$ is norm-Euclidean is for $n = -2$. Indeed the a, b chosen above for $n = -1$ will work for $n = -2$ as well. If we allow for ω_n as defined in Application 1.2 on page 3, then $\mathbb{Z}[(1 + \sqrt{n})/2]$ for squarefree $n < 0$ is norm Euclidean if and only if

$$n \in \{-3, -7, -11\}$$

—see [54, Theorem 1.15, p. 34].

The case for positive D is also settled due to the efforts of several mathematicians culminating in the complete solution in the middle of the last century. The positive squarefree integers n for which $\mathbb{Z}[\omega_n]$ is norm-Euclidean are given as follows—see [54, Remark 1.19, Theorem 1.21, p. 50]:

$$n \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Remark 1.8 It can be shown that Theorem 1.4 on page 10 generalizes to any Euclidean domain. In other words, there always exist gcds for elements in Euclidean domains. This comes from the verifiable fact that in a Euclidean domain D with respect to a Euclidean function ϕ, we may select any $\alpha = \alpha_0, \beta = \beta_0 \in D$ with $\alpha_0\beta_0 \neq 0$ and $\beta_0 \not| \alpha_0$ and recursively define $\alpha_j = \beta_j\delta + \gamma_j$ with $\phi(\gamma_j) < \phi(\beta_j)$, where $\alpha_j = \beta_{j-1}$ and $\beta_j = \gamma_{j-1}$. The smallest $n \in \mathbb{N}$ such that $\gamma_n = 0$ yields γ_{n-1} as the gcd of α and β—see [54, Theorem 1.14, p. 33].

Example 1.17 is an example of a more general phenomenon, namely that the converse of Theorem 1.1 on page 5 always holds for Euclidean domains.

Theorem 1.6 — Euclidean Domains Are UFDs
If D is a Euclidean domain then $\alpha \in D$ is irreducible if and only if α is prime.

Proof. First, we establish that D is a factorization domain. By part (a) of Exercise 1.18,

$$\phi(\alpha) = \phi(1_D) \text{ if and only if } \alpha \in \mathfrak{U}_D.$$

In this case α is vacuously a product of irreducible elements. Hence, we may use induction on $\phi(\alpha)$. By Exercise 1.21, $\phi(1_D) \leq \phi(\alpha)$. Assume that $\alpha \notin \mathfrak{U}_D$, and that any $\beta \in D$ with $\phi(\beta) < \phi(\alpha)$ has a factorization into irreducible elements. If α is irreducible, we are done. Assume otherwise. Then $\alpha = \beta\gamma$ for $\beta,\gamma \in D$ and $\beta,\gamma \notin \mathfrak{U}_D$. Thus, by property (a) of Euclidean domains given in Definition 1.9, $\phi(\beta) \leq \phi(\alpha)$, and $\phi(\gamma) \leq \phi(\alpha)$. By part (b) of Exercise 1.18,

$$\phi(\gamma) \neq \phi(\alpha), \text{ and } \phi(\beta) \neq \phi(\alpha).$$

Hence, $\phi(\beta) < \phi(\alpha)$ and $\phi(\gamma) < \phi(\alpha)$ so, by the induction hypothesis, both β and γ have factorizations into irreducibles. Thus, so does α. We have shown that D is a factorization domain.

In view of Theorems 1.1 on page 5 and 1.2 on page 7, we need only show that irreducibles are primes. Suppose that $\alpha|\beta\gamma$ for some $\beta,\gamma \in D$. If $\alpha \nmid \beta$, then given the irreducibility of α, the only common divisors of α and β in D are units. In particular, 1_D is a gcd of α and β. By Exercise 1.19, there exist $\sigma,\delta \in D$ such that $1_D = \sigma\alpha + \delta\beta$. Therefore,

$$\gamma = \sigma\alpha\gamma + \delta\beta\gamma.$$

Since $\alpha|\beta\gamma$, then $\alpha|\gamma$, so α is prime. □

Thus, via Example 1.17 we have the solution for squarefree D.

Corollary 1.1 If $n \in \mathbb{Z}$ is squarefree, then $\mathbb{Z}[\omega_n]$ is a norm-Euclidean domain if and only if

$$n \in \{-1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

The following is immediate from Theorem 1.6 and is implicit in the header thereof. However, the converse of the following result fails to hold—see Exercise 1.25.

Corollary 1.2 If D is a Euclidean domain, then D is a UFD.

Exercises

1.18. Establish the following facts concerning Euclidean functions ϕ on an integral domain D, introduced in Definition 1.9 on page 10.

(a) If $\alpha \sim \beta$ then $\phi(\alpha) = \phi(\beta)$.

(b) If $\alpha \mid \beta$ and $\phi(\alpha) = \phi(\beta)$ then $\alpha \sim \beta$.

(c) $\alpha \in \mathfrak{U}_D$ if and only if $\phi(\alpha) = \phi(1_D)$.

(d) $\phi(\alpha) > \phi(0)$ for all nonzero $\alpha \in D$.

1.19. With reference to Exercise 1.17 on page 6, prove that any common divisor γ of α and β, where α,β are elements of a Euclidean Domain D, may be written in the form

$$\gamma = \sigma\alpha + \delta\beta$$

for some σ,$\delta \in D$.

1.20. Prove that condition (a) in Definition 1.9 on page 10 is equivalent to the condition

(c) If $\alpha \mid \beta$ for α,$\beta \in D$, with $\beta \neq 0$, then $\phi(\alpha) \leq \phi(\beta)$.

1.21. Prove that a Euclidean domain D with Euclidean function ϕ satisfies $\phi(1_D) \leq \phi(\alpha)$ for all nonzero $\alpha \in D$.

1.22. If $\alpha \in D$, a UFD, and $|N(\alpha)|$ is prime, show that α is prime in D.

1.23. Either provide a counterexample to, or prove the converse of the statement in Exercise 1.22.

1.24. Prove that the condition in Definition 1.11 on page 11 is tantamount to the condition: Given α,$\beta \in D$ with $\beta \neq 0$, there exist σ,$\delta \in D$ with $\alpha = \beta\sigma + \delta$ and $|N(\delta)| < |N(\beta)|$.

1.25. An integral domain D is said to be an *almost Euclidean domain* provided that: there exists a function $\phi : D \mapsto \mathbb{N} \cup \{0\}$ called an *almost Euclidean function*, such that

(a) $\phi(0) = 0$ and $\phi(\alpha) > 0$ for $\alpha \neq 0$ in D.

(b) If β is a nonzero element of D then $\phi(\alpha\beta) \geq \phi(\alpha)$ for all $\alpha \in D$.

(c) For any α,$\beta \in D$ with $\beta \neq 0$, one of the following holds.

(i) There exists a $\gamma \in D$ such that $\alpha = \beta\gamma$.

(ii) There exist $x, y \in D$ such that $0 < \phi(\alpha x + \beta y) < \phi(\beta)$.

Prove that an almost Euclidean domain is a UFD.

(*This topic was introduced by Campoli* [9]. *With reference to our discussion herein, he produced integral domains, such as his example*

$$\mathbb{Z}[(-1 - \sqrt{-19})/2]$$

that are UFDs which are not Euclidean domains. Campoli called his example "almost Euclidean." This resulted in the production of counterexamples to the converse of Corollary 1.2 on the previous page. Later Greene [25] *showed that the conditions given above for an almost Euclidean domain are equivalent to being a "Principal Ideal Domain"* (*PID*) *which we will study in* §*1.5 and revisit this topic—see Exercises 1.47–1.48 on page 34. It turns out that Euclidean domains are PIDs which in turn are UFDs. However, neither converse holds. Examples of UFDs that are not PIDs are the hardest to produce and hence the above delineation. More recently, such as in* [31], *almost Euclidean spaces have been used for applications in complexity theory and error-correcting codes.*

1.3 Ideals

> *Intelligence without ambition is a bird without wings.*
> **Salvador Dali (1904–1989), Spanish painter**

In this section we set the stage for the introduction of two types of domains based upon the theory of ideals which will elevate the factorization debate from elements to ideals. This allows us to witness the influence of Dedekind and others on the development of algebraic number theory. Some of the following is adapted from [54].

Definition 1.12 — Ideals

An *R-ideal* is a nonempty subset I of a commutative ring R with identity having the following properties.

(a) If $\alpha,\beta \in I$, then $\alpha+\beta \in I$.

(b) If $\alpha \in I$ and $r \in R$, then $r\alpha \in I$.

Remark 1.9 It is inductively clear that Definition 1.12 implies that if $\alpha_1, \alpha_2, \ldots, \alpha_n \in I$ for any $n \in \mathbb{N}$, then $r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n \in I$ for any $r_1, r_2, \ldots, r_n \in R$. Moreover, if $1 \in I$, then $I = R$. Also, if we are given a set of elements $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ in an integral domain R, then the set of all linear combinations of the α_j for $j = 1, 2, \ldots, n$

$$\left\{\sum_{j=1}^{n} r_j\alpha_j : r_j \in R \text{ for } j = 1, 2, \ldots, n\right\}$$

is an ideal of R denoted by $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. In particular, when $n = 1$, we have the following.

Definition 1.13 — Principal and Proper Ideals

If D is an integral domain and I is a D-ideal, then I is called a *principal* D-ideal if there exists an element $\alpha \in I$ such that $I = (\alpha)$, where α is called a *generator* of I. If $I \neq D$, then I is called a *proper* ideal.

Example 1.18 Let $n \in \mathbb{Z}$ and set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, which is an ideal in $\mathbb{Z}$ and $n\mathbb{Z} = (n) = (-n)$ is indeed a principal ideal. Moreover, it is a proper ideal for all $n \neq \pm 1$.

Example 1.19 In $D = \mathbb{Z}[i]$, (2) and (3) are proper principal ideals. Moreover, the latter is an example of a special type of ideal that we now define—see Example 1.20 on the following page.

Definition 1.14 — Prime Ideals

If D is an integral domain, then a proper D-ideal $\mathcal{P}$ is called a *prime D-ideal* if it satisfies the property that whenever $\alpha\beta \in \mathcal{P}$, for $\alpha,\beta \in D$, then either $\alpha \in \mathcal{P}$ or $\beta \in \mathcal{P}$.

In order to discuss any more features of ideal theory, we need to understand how multiplication of ideals comes into play.

Definition 1.15 — Products of ideals

If D is an integral domain and I, J are D-ideals, then the product of I and J, denoted by IJ, is the ideal in D given by

$$IJ = \{r \in D : r = \sum_{j=1}^{n} \alpha_j \beta_j \text{ where } n \in \mathbb{N}, \text{and } \alpha_j \in I, \beta_j \in J \text{ for } 1 \le j \le n\}.$$

Theorem 1.7 — Criterion for Prime Ideals

If D is an integral domain and I is a proper D-ideal, then I is a prime D-ideal if and only if the following property is satisfied:

$$\text{for any two } D\text{-ideals } J, K, \text{ with } JK \subseteq I, \text{ either } J \subseteq I \text{ or } K \subseteq I. \tag{1.17}$$

Proof. Suppose that (1.17) holds. Then if $\alpha,\beta \in D$ such that $\alpha\beta \in I$, then certainly $(\alpha\beta) = (\alpha)(\beta) \subseteq I$, taking $J = (\alpha)$ and $K = (\beta)$ in (1.17), which therefore implies that $(\alpha) \subseteq I$ or $(\beta) \subseteq I$. Hence, $\alpha \in I$ or $\beta \in I$. We have shown that (1.17) implies I is prime.

Conversely, suppose that I is a prime D-ideal. If (1.17) fails to hold, then there exist D-ideals J, K such that $JK \subseteq I$ but $K \not\subseteq I$ and $J \not\subseteq I$. Let $\alpha \in J$ with $\alpha \notin I$ and $\beta \in K$ with $\beta \notin I$, then $\alpha\beta \in I$ with neither of them being in I, which contradicts Definition 1.14 on the previous page. Hence, (1.17) holds and the result is secured. □

Now we prove a result that links the notion of prime element and prime ideal in the principal ideal case.

Theorem 1.8 — Principal Prime Ideals and Prime Elements

If D is an integral domain and $\alpha \in D$ is a nonzero, nonunit element, then (α) is a prime D-ideal if and only if α is a prime in D.

Proof. Suppose first that (α) is a prime D-ideal. Then for any $\beta,\gamma \in D$ such that $\alpha \mid \beta\gamma$, $\beta\gamma \in (\beta\gamma) \subseteq (\alpha)$. Since (α) is a prime D-ideal, then $\beta \in (\alpha)$ or $\gamma \in (\alpha)$ by Definition 1.14. In other words, $\alpha \mid \beta$ or $\alpha \mid \gamma$, namely α is a prime in D.

Conversely, suppose that α is prime in D. If $\beta,\gamma \in D$ such that $\beta\gamma \in (\alpha)$, then there exists an $r \in D$ with $\beta\gamma = \alpha r$. Since α is prime, then $\alpha \mid \beta$ or $\alpha \mid \gamma$. If $\alpha \mid \beta$, there is an $s \in D$ such that $\beta = \alpha s$, so $\beta \in (\alpha)$. If $\alpha \mid \gamma$, there is a $t \in D$ such that $\gamma = \alpha t$, so $\gamma \in (\alpha)$. We have shown that (α) is a prime D-ideal by Definition 1.14, which completes the proof. □

Example 1.20 In Example 1.19 on the preceding page, (2) and (3) were considered as principal ideals in the Gaussian integers. By Exercises 1.26–1.27 on page 19, 3 is a prime in $\mathbb{Z}[i]$, but 2 is not. Therefore, by Theorem 1.8, (3) is a prime ideal in the Gaussian integers but (2) is not.

Now that we may look at products of ideals, we may we look at the notion of division in ideals in order to link this with elements and primes.

Definition 1.16 — Division of Ideals

If D is an integral domain, then a nonzero D-ideal I is said to *divide a* D-ideal J if there is another D-ideal H such that $J = HI$.

The following shows that division of ideals implies containment.

Lemma 1.1 — To Divide is to Contain
If D is an integral domain and I, J are D-ideals, with $I \mid J$, then $J \subseteq I$.

Proof. Since $I \mid J$, then by Definition 1.16, there is a D-ideal H such that $J = IH$. However, by Definition 1.12 on page 15, $J = IH \subseteq IR \subseteq I$, as required. □

Corollary 1.3 Suppose that D is an integral domain and I is a D-ideal satisfying the property:

$$\text{whenever } I \mid JK \text{ for } D\text{-ideals } J, K, \text{ we have } I \mid J \text{ or } I \mid K. \tag{1.18}$$

Then I is a prime D-ideal.

Proof. Suppose that $I \mid JK$, then by Lemma 1.1, $JK \subseteq I$, and (1.18) implies that either $J \subseteq I$ or $K \subseteq I$. Thus, by Theorem 1.7, I is a prime D-ideal. □

The question now arises as to the validity of the converse of Lemma 1.1 in certain domains. In order to discuss this topic, we must prepare the stage with some essential topics. First of all there are types of ideals which are core to the theory.

Definition 1.17 — Maximal Ideals

In an integral domain D, an ideal M is called *maximal* if it satisfies the property that whenever $M \subseteq I \subseteq D$, for any D-ideal I, then either $I = D$ or $I = M$.

The next concept is necessary to prove our first result about maximal ideals. First note that if I, J are R-ideals, then $I + J$ is necessarily an R-ideal since for any $r \in R$, $\alpha \in I$, $\beta \in J$, $r(\alpha + \beta) \in I + J$ by Definition 1.12 on page 15. We formalize this in the following.

Definition 1.18 — Sums of Ideals Are Ideals

If I, J are ideals in D, a commutative ring with identity, then $I + J = \{\alpha + \beta : \alpha \in I, \beta \in I\}$, is an ideal in D.

We use the above to prove our first result that we need to link maximality with primality.

Theorem 1.9 — Quotients of Prime Ideals Are Integral Domains
If D is an integral domain, then a D-ideal $\mathcal{P}$ is prime if and only if $D/\mathcal{P}$ is an integral domain.

Proof. Suppose that $\mathcal{P}$ is a prime D-ideal. Then $D/\mathcal{P}$ is a commutative ring with multiplicative identity $1_R + \mathcal{P}$ and additive identity $0_R + \mathcal{P}$. We must verify that $D/\mathcal{P}$ has no zero divisors. If $\alpha, \beta \in D$ with $(\alpha + \mathcal{P})(\beta + \mathcal{P}) = 0_R + \mathcal{P} = \mathcal{P}$, then $\alpha\beta + \mathcal{P} = \mathcal{P}$, so $\alpha\beta \in \mathcal{P}$. Since $\mathcal{P}$ is prime, then either $\alpha \in \mathcal{P}$ or $\beta \in \mathcal{P}$. In other words, either $\alpha + \mathcal{P} = 0_R + \mathcal{P}$ or $\beta + \mathcal{P} = 0_R + \mathcal{P}$. We have shown that $D/\mathcal{P}$ has no zero divisors.

Conversely, if $D/\mathcal{P}$ is an integral domain, then $\alpha\beta \in \mathcal{P}$ implies that

$$(\alpha + \mathcal{P})(\beta + \mathcal{P}) = \alpha\beta + \mathcal{P} = 0_R + \mathcal{P}.$$

Thus, having no zero divisors in $D/\mathcal{P}$, either $\alpha + \mathcal{P} = 0_R + \mathcal{P}$ or $\beta + \mathcal{P} = 0_R + \mathcal{P}$. In other words, either $\alpha \in \mathcal{P}$ or $\beta \in \mathcal{P}$, so $\mathcal{P}$ is a prime D-ideal. □

Now we link prime ideals with maximal ones.

Theorem 1.10 — Maximal ideals Are Prime

If D is an integral domain, then every nonzero maximal D-ideal is prime.

Proof. Suppose $M \neq (0)$ is a maximal D-ideal, and $M \mid IJ$ for some D-ideals I, J, with M dividing neither factor. By Lemma 1.1 on the preceding page, there exist $\alpha \in I$ and $\beta \in J$ such that

$$M \mid IJ \mid (\alpha)(\beta)$$

with M dividing neither (α) nor (β), namely $\alpha \notin M$ and $\beta \notin M$. Therefore, by Definition 1.18 on the previous page, $M + (\alpha)$ and $M + (\beta)$ are D-ideals, both of which properly contain M, so $M \neq D$. Hence, by the maximality of M, we have,

$$M + (\alpha) = D = M + (\beta).$$

Therefore,

$$M \subset D = D^2 = (M + (\alpha))(M + (\beta)) \subseteq M^2 + (\alpha)M + (\beta)M + (\alpha)(\beta)M \subseteq M,$$

a contradiction. We have shown that either $M \mid (\alpha)$ or $M \mid (\beta)$. Therefore, by Corollary 1.3 on the preceding page, M is prime. □

The next result tells us when an ideal is maximal with respect to quotients in integral domains.

Theorem 1.11 — Fields and Maximal ideals

If D is an integral domain, then M is a maximal D-ideal if and only if D/M is a field.

Proof. First we need the following fact.

Claim 1.2 D is a field if and only if the only ideals in D are (0) and D.

If D is a field and $I \neq (0)$ is a D-ideal, then there exists a nonzero element $\alpha \in I$. However, since D is a field, then there exists an inverse $\alpha^{-1} \in D$ of α. By Definition 1.12 on page 15, $\alpha\alpha^{-1} = 1_D \in I$, so $I = D$.

Conversely, suppose that the only D-ideals are (0) and D. If $\alpha \in D$ is nonzero, let

$$(\alpha) = \alpha D = I.$$

By hypothesis, $I = D$. Thus, there exists a $\beta \in D$ such that $\beta\alpha = 1_D$, so α is a unit. However, α was chosen as an arbitrary nonzero element in D, so D is a field. This is Claim 1.2.

Suppose that D/M is a field for a given D-ideal M. If $M \subseteq I \subseteq D$ for a D-ideal I, then I/M is an ideal of D/M, so by Claim 1.2, $I/M = (0)$ or $I/M = D/M$. In other words, either $I = D$ or $I = M$, namely M is maximal.

Conversely, if M is maximal, then by Theorem 1.10, either $M = (0)$ or M is prime. If $M = (0)$, then $D/(0) \cong D$ is a field by Claim 1.2, given that (0) is maximal, implying that D has no proper ideals. If M is prime, then by Theorem 1.9 on the preceding page, D/M is an integral domain. Thus, it remains to show that all nonzero elements of D/M have multiplicative inverses, namely that if $\alpha + M \neq M$, then $\alpha + M$ has a multiplicative inverse in D/M. Given $\alpha + M \neq M$, then $\alpha \notin M$. Thus, M is properly contained in the ideal $(\alpha) + M$. Hence, $(\alpha) + M = D$. In other words,

$$1_D = m + r\alpha \text{ for some } m \in M \text{ and } r \in D.$$

Therefore, $1_D - r\alpha = m \in M$, so $1_D + M = r\alpha + M = (r + M)(\alpha + M)$, namely $r + M$ is a multiplicative inverse of $\alpha + M$ in D/M, so D/M is a field. □

Example 1.21 If $D = \mathbb{Z}/n\mathbb{Z}$, where $n \in \mathbb{N}$, then by Theorem 1.11, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n\mathbb{Z}$ is maximal. Later we will see that $\mathbb{Z}$, being a special case of the ring of integers of a number field, always satisfies the property that all prime ideals are maximal—see Definition 1.23 on page 25 and Theorem 1.26 on page 42. Hence, in conjunction with Theorem 1.10, we have

$$\mathbb{Z}/n\mathbb{Z} \text{ is a field if and only if } n\mathbb{Z} \text{ is prime.}$$

Example 1.22 Let F be a field, $r \in F$ is a fixed nonzero element, and

$$I = \{f(x) \in F[x] : f(r) = 0\}.$$

We now demonstrate that I is a maximal ideal in $F[x]$. First, we show that I is indeed an ideal in $F[x]$. If $g(x) \in F[x]$, then for any $f(x) \in I$, $g(r)f(r) = 0$, so $g(x)f(x) \in I$, and clearly $f(r) + h(r) = 0$ whenever $f(x), h(x) \in I$, which shows that I is an $F[x]$-ideal. If we define ϕ to be the map

$$\phi : F[x] \mapsto F[x]/I,$$

given by

$$\phi(f(x)) = f(x) + I,$$

then an easy check shows that $I = \ker(\phi)$—see (A.3) on page 325 in Appendix A, from which it follows that I is maximal, as

$$F \cong F[x]/I.$$

In §1.4, we will use ideal theory developed herein to introduce and explore two distinguished types of domains that set the stage for Dedekind's masterpiece contribution presented in §1.5. This makes way for the foundational building bricks of algebraic number theory in §1.6, where algebraic numbers and numbers fields as generalizations of $\mathbb{Z}$ and $\mathbb{Q}$ are introduced. This provides the springboard to the balance of the text that explores this magnificent edifice of mathematics.

The last section of this chapter, §1.7, is a motivator for Chapter 2 by looking in detail at the least nontrivial extension of $\mathbb{Q}$, namely the quadratic field case, which builds upon the quadratic domains introduced and discussed in §1.2.

Exercises

1.26. Prove that any prime $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$ is a prime in $\mathbb{Z}[i]$.

(*By Corollary 1.1 of Theorem 1.6 on page 13 it only needs to be shown that p is irreducible.*)

1.27. Prove that if $\alpha \in \mathbb{Z}[i]$ and $N_F(\alpha) = p$, where p is prime in $\mathbb{Z}$, then α is a prime in $\mathbb{Z}[i]$ but p is not a prime in $\mathbb{Z}[i]$ and $p \equiv 1 \pmod 4$ or $p = 2$.

1.28. Prove that in an integral domain D with α,$\beta \in D$ nonzero, as ideals $(\alpha) = (\beta)$ if and only if $\alpha\beta^{-1} \in \mathfrak{U}_D$.

1.29. For some indexing set $\mathfrak{J}$, let R be a ring and let $\{R_j : j \in \mathfrak{J}\}$ be any set of subrings of R. Prove that $\cap_{j\in\mathfrak{J}} R_j$ is a subring of R. Also, show that if

$$R_1 \subseteq R_2 \subseteq \cdots \subseteq R_j \subseteq \cdots ,$$

then $\cup_{j\in\mathfrak{J}} R_j$ is a subring of R.

1.4 Noetherian and Principal Ideal Domains

> *Whether you think you can, or you can't—you are right.*
> **Henry Ford (1863–1947), American car manufacturer**

In this section, we use our knowledge of ideals to proceed to build the foundations of algebraic number theory by investigating two kinds of domains that will lead us into the building bricks of algebraic number fields. The following is crucial in the sequel. Some of the following is adapted from [54].

Definition 1.19 — Ascending Chain Condition (ACC)

An integral domain R is said to satisfy the *ascending chain condition* (ACC) if every chain of R-ideals $I_1 \subseteq I_2 \subseteq \cdots I_n \subseteq \cdots$ *terminates*, meaning that there is an $n_0 \in \mathbb{N}$ such that $I_n = I_{n_0}$ for all $n \geq n_0$.

Remark 1.10 An equivalent way of stating the ACC is to say that R does not possess an *infinite strictly ascending* chain of ideals.

The above is a segue to the following important notion that will carry us forward toward our goals—see Biography 1.1 on page 23.

Definition 1.20 — Noetherian Domains

An integral domain R possessing the ACC is called a *Noetherian Domain.*

For the following, the reader is reminded of the general notion of *finite generation* given in Definition A.7 on page 324 in Appendix A. Also, see Remark 1.9 on page 15.

Lemma 1.2 — Finite Generation and Noetherian Domains

If R is an integral domain, then R is a Noetherian Domain if and only if every R-ideal is finitely generated.

Proof. Suppose that every R-ideal is finitely generated. Let

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

be an ascending chain of ideals. It follows from Exercise 1.29 on the previous page that $I = \cup_{i=1}^{\infty} I_j$ is an R-ideal, and since any R-ideal is finitely generated, then there exist $\alpha_j \in R$ for $j = 1, 2, \ldots, d \in \mathbb{N}$ such that

$$I = (\alpha_1, \alpha_2, \ldots, \alpha_d).$$

Therefore, for each $j = 1, 2, \ldots, d$, there is a k_j with $\alpha_j \in I_{k_j}$. Let $n = \max\{k_1, k_2, \ldots, k_d\}$. Then since $I_n \subseteq I$ and $I_{k_j} \subseteq I_n$, given that $k_j \leq n$ for each such j, we have $(\alpha_1, \alpha_2, \ldots, \alpha_d) \subseteq I_n$, which implies that $I \subseteq I_n$. Hence, $I_n = \cup_{i=1}^{\infty} I_j$ and so $I_n = I_j$ for each $j \geq n$. Since the chain terminates, R satisfies the ACC, so is a Noetherian domain.

Conversely, suppose that R is a Noetherian domain. If I is an R-ideal that is not finitely generated, then $I \neq (0)$, so there exists $\alpha_1 \in I$ with $\alpha_1 \neq 0$, and $(\alpha_1) \subset I$. Since $I \neq (\alpha_1)$, given that the former is not finitely generated, then there exists $\alpha_2 \in I$ and $\alpha_2 \notin (\alpha_1)$ so we have

$$(\alpha_1) \subset (\alpha_1, \alpha_2) \subset I.$$

Continuing inductively in this fashion, we get the strictly ascending chain of ideals,

$$(\alpha_1) \subset (\alpha_1, \alpha_2) \subset \cdots \subset (\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \cdots \subset I,$$

contradicting that R is a Noetherian domain. Hence, every R-ideal is finitely generated. □

Corollary 1.4 Let R be a Noetherian domain. Then every nonempty subset of R-ideals contains a maximal element.

Proof. Let $\mathcal{T}$ be the set of ideals with the property that for every ideal I of $\mathcal{T}$, there exists an ideal J of $\mathcal{T}$ with $I \subset J$. If $\mathcal{T} \neq \varnothing$, then by its definition we may construct an infinite strictly ascending chain of ideals in $\mathcal{T}$, contradicting Lemma 1.2. This is the result. □

Immediate from Corollary 1.4 is the following result.

Corollary 1.5 In a Noetherian domain R, every proper R-ideal is contained in a maximal R-ideal.

We need the following concept that is intimately linked to the notion of a UFD, especially when we are dealing with Dedekind domains—see Definition 1.8 on page 7.

Definition 1.21 — Principal Ideal Domain (PID)

An integral domain R in which all ideals are principal is called a *principal ideal domain*, or *PID*.

Theorem 1.12 — PIDs and Noetherian Domains

If R is a PID, then R is a Noetherian domain.

Proof. If we have a nested sequence of R-ideals

$$(\alpha_1) \subseteq (\alpha_2) \subseteq \cdots (\alpha_j) \subseteq \cdots,$$

then it follows from Exercise 1.29 that $\cup_{j=1}^{\infty}(\alpha_j)$ is an R-ideal. Thus, since R is a PID, there exists an $\alpha \in R$ such that $\cup_{j=1}^{\infty}(\alpha_j) = (\alpha)$, so there exists an $n \in \mathbb{N}$ such that $\alpha \in (\alpha_n)$. Therefore,

$$(\alpha_j) = (\alpha_n) = (\alpha)$$

for all $j \geq n$. Thus, the ACC condition of Definition 1.19 is satisfied and R is a Noetherian domain. □

The following strengthens Corollary 1.2 on page 13 and puts Exercise 1.25 on page 14 into clearer focus.

Corollary 1.6 A Euclidean domain is a PID, and so is Noetherian.

Proof. If D is a Euclidean domain, then D has a Euclidean function ϕ by Definition 1.9 on page 10. Let I be a nonzero D-ideal and set

$$\mathcal{S} = \{\phi(\alpha) : \alpha \in I, \alpha \neq 0\}.$$

Given that $I \neq (0)$, $\mathcal{S} \neq \varnothing$. Using the Well-Ordering Principle—see page 340—$\mathcal{S}$ has a least element $\phi(\beta)$ where $\beta \in I$, $\beta \neq 0$. Let $\gamma \in I$ be arbitrary. Then by part (b) of Definition 1.9, there exist $r, q \in D$ with

$$\gamma = q\beta + r \text{ with } \phi(r) < \phi(\beta).$$

By Definition 1.12 on page 15, $r = \gamma - q\beta \in I$, so by the minimality of $\phi(\beta)$, we must have that $r = 0$. Therefore, $\gamma = q\beta$, which implies, since γ was arbitrarily chosen, that $I = (\beta)$. We have shown that every ideal of D is principal (given that the zero ideal is principal as well), so D is a PID. By Theorem 1.12, D is therefore Noetherian. □

Remark 1.11 Note that via Exercise 1.25, Corollary 1.6 is more general than Corollary 1.2 since there are UFDs that are not PIDs and the following shows that Corollary 1.2 follows from Corollary 1.6. Also, see the related Exercise 1.47 on page 34

Theorem 1.13 — PIDs and UFDs

If R is a PID then R is a UFD.

Proof. Let $\mathcal{S}$ be the set of all $\alpha \in R$ such that α is not a product of irreducible elements. If $\mathcal{S} \neq \varnothing$, then by Corollary 1.4 on the preceding page, via Theorem 1.12, $\mathcal{S}$ has a maximal element m. Thus, (m) is a proper ideal (since a unit is vacuously a product of irreducible elements by Definition 1.6 on page 4). Therefore, (m) is contained in a maximal R-ideal (M) for some $M \in R$, by Corollary 1.5 on the preceding page, again via Theorem 1.12. Thus, $M \bigm| m$ and $(M) \neq (m)$ by Theorem 1.10 on page 18. Since M is a product of irreducible elements, there exists an $\alpha \bigm| m$ such that α is irreducible. Therefore, $m = \alpha\beta$ for some $\beta \in R$. If β is a unit, then m is irreducible since associates of irreducibles are also irreducible, a contradiction. Hence, β is not a unit. If $(\beta) \notin \mathcal{S}$, then β is a product of irreducibles, and so is m, a contradiction. Thus, $(\beta) \in \mathcal{S}$. However, $\beta \bigm| m$, so $(m) \subseteq (\beta)$ by Lemma 1.1 on page 17. Also, $(m) \neq (\beta)$ since α is not a unit, given that it is irreducible. Hence, (m) is properly contained in $(\beta) \subseteq \mathcal{S}$, a contradiction to the maximality of (m) in $\mathcal{S}$, so $\mathcal{S} = \varnothing$. This establishes that all nonzero elements of R are expressible as a product of irreducible elements.

We may complete the proof by showing that all irreducible elements are prime and invoke Theorem 1.2 on page 7. Suppose that $r \in R$ is an irreducible element and $r \bigm| \alpha\beta$, $\alpha,\beta \in R$, with r not dividing α. Then by the irreducibility of r, we must have that r and α are relatively prime, namely $R = (r) + (\alpha)$, so there exist $s_1, s_2 \in R$ such that $1_R = rs_1 + \alpha s_2$. Therefore,

$$(\beta) = (rs_1\beta + \alpha s_2\beta) \subseteq (r),$$

since $r \bigm| \alpha\beta$ implies that $(r) \supseteq (\alpha\beta)$, so both $rs_1\beta \in (r)$ and $\alpha s_2\beta \in (r)$. In other words, $r \bigm| \beta$, so r is prime as required. □

Exercises

1.30. In a commutative ring R with identity, an *R-module M is defined to be Noetherian* if every ascending chain of submodules of M *terminates* in the same sense as in Definition 1.19 on page 20. Prove that if N is a submodule of a Noetherian R-module M, then both N and M/N are Noetherian R-modules.

✰ 1.31. With reference to Exercise 1.30, either provide a counterexample to the converse or prove that: if N is a submodule of an R-module M such that both N and M/N are Noetherian R-modules, then M is a Noetherian R-module.

✰ 1.32. If R is a Noetherian ring, prove that any finitely generated R-module is Noetherian.

1.33. Let D_j be integral domains for $j = 1, 2$ with $D_1 \subseteq D_2$. If D_1 is Noetherian and D_2 is finitely generated as a D_1-module, prove that D_2 is a Noetherian domain.

1.34. Prove that $\mathbb{Z}[\sqrt{n}]$ is a Noetherian domain for any nonsquare integer n.

1.35. A commutative ring R with identity is said to satisfy the descending chain condition, denoted by DCC, on ideals if every sequence $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_j \supseteq \cdots$ of R-ideals terminates. In other words, there exists an $n \in \mathbb{N}$ such that $I_j = I_n$ for all $j \geq n$. Prove that R satisfies the DCC if and only if every nonempty collection of ideals contains a minimal element. (Rings of the above type are called *Artinian rings*.)

Biography 1.1 Emmy Amalie Noether (1882–1935) was born in Erlangen, Bavaria, Germany on March 23, 1882. She studied there in her early years and, in 1900, received certification to teach English and French in Bavarian girls' schools. However, she chose a more difficult route, for a woman of that time, namely to study mathematics at university. Women were required to get permission to attend a given course by the professor teaching it. She did this at the University of Erlangen from 1900 to 1902, and passed her matriculation examination in Nürnberg in 1903, after which she attended courses at the University of Göttingen from 1903 to 1904. By 1907, she was granted a doctorate from the University of Erlangen. By 1909, her published works gained her enough notoriety to warrant an invitation to become a member of the *Deutsche Mathematiker-Vereinigung*, and in 1915, she was invited back to Göttingen by Hilbert and Klein. However, it took until 1919 for the university to, grudgingly, obtain her Habilitation,[1.1] and permit her to be on the faculty. In that year she proved a result in theoretical physics, now known as *Noether's Theorem*, praised by Albert Einstein as a penetrating result, which laid the foundations for many aspects of his general theory of relativity. After this, she worked in ideal theory, developing ring theory, which turned out to be of core value in modern algebra.

Her work *Idealtheorie in Ringbereichen*, published in 1921, helped cement this value. In 1924, B.L. van der Waerden published his work *Moderne Algebra*, the second volume of which largely consists of Noether's results. Her most successful collaboration was in 1927 with Helmut Hasse and Richard Brauer on noncommutative algebra. She was recognized for her mathematical achievements through invitations to address the International Mathematical Congress, the last at Zurich in 1932. Despite this, she was dismissed from her position at the University of Göttingen in 1933 due to the Nazi rise to power, given that she was Jewish. She fled Germany in that year and joined the faculty at Bryn Mawr College in the U.S.A. She died at Bryn Mawr on April 14, 1935. She was buried in the Cloisters of the Thomas Great Hall on the Bryn Mawr campus.

[1.1] Habilitation is the highest academic qualification achievable in certain European and Asian countries. Typically Habilitation is earned *after* obtaining a research doctorate (Ph.D.), which is sufficient qualification for a senior faculty position at a university in North America. However, a Habilitation requires a professorial thesis, reviewed by and defended before an academic committee similar to that for a North American Ph.D., but the level of scholarship expected is usually much higher. In practice, for instance in Germany, a Habilitation is required to supervise doctoral students, a post that is known as *Privatdozent* and there are similarly termed appointments in other countries. After serving as Privatdozent, the next step is often appointment as a professor in the faculty in which the candidate sits.

Biography 1.2 Emil Artin (1898–1962) was born on March 3, Vienna, Austria in 1898. He served in the Austrian army in World War I, after which he entered the University of Leipzig. In 1921 he obtained his doctorate, the thesis of which was on quadratic extensions of rational function fields over finite fields. In 1923, he had his Habilitation, allowing him to become Privatdozent at the University of Hamburg—see Footnote 1.1 on the previous page. In 1925, he was promoted to extraordinary professor at Hamburg. In that same year, he introduced the *theory of braids*, which is studied today by algebraists and topologists. In 1928, he worked on rings with minimum condition, the topic of Exercise 1.35 on page 22, which are now called *Artinian rings*. In 1937, Hitler enacted the New Official's Law, which enabled a mechanism for removing not only Jewish teachers from university positions but also those related by marriage. Since Artin's wife was Jewish, although he was not, he was dismissed. In 1937, he emigrated to the U.S.A. and taught at several universities there, including eight years at Bloomingdale at Indiana University during 1938–1946, as well as Princeton from 1946 to 1958. During this time, in 1955, he produced what was, arguably, the catalyst for the later classification of finite simple groups, by proving that the only (then-known) coincidences in orders of finite simple groups were those given by Dickson in his *Linear Groups*. In 1958, he returned to Germany where he was appointed again to the University of Hamburg. Artin's name is attached not only to the aforementioned rings, but also to the reciprocity law that he discovered as a generalization of Gauss's quadratic reciprocity law. One of the tools that he developed to do this is what we now call *Artin L-functions*. He also has the distinction of solving one of Hilbert's famous list of twenty-three problems posed in 1900—see Biography 3.4 on page 94.

He was an outstanding and respected teacher. In fact, many of his Ph.D. students such as Serge Lang, John Tate, and Max Zorn went on to major accomplishments. He also had an interest in astronomy, biology, chemistry, and music. He was indeed an accomplished musician in his own right, playing the flute, harpsichord, and clavichord. He died in Hamburg on December 20, 1962.

1.5 Dedekind Domains

> *Mathematics is the only instructional material that can be presented in an entirely undogmatic way.*
>
> **Max Wilhelm Dehn (1878–1952), German mathematician who introduced one of the first structured elucidations on topology**

§1.4 put us in a position to define a contribution by Dedekind —see Biography 1.3 on page 29. First we need the following notion.

Definition 1.22 — Integral Over a Domain and Integral Closure

If $D \subseteq S$ where D and S are integral domains, then $\alpha \in S$ is said to be *integral* over D if there exists a $d \in \mathbb{N}$, and a polynomial

$$f(x) = x^d + \beta_{d-1}x^{d-1} + \cdots + \beta_1 x + \beta_0 \text{ with } \beta_j \in D \text{ for } j = 0, 1, \ldots, d-1$$

such that $f(\alpha) = 0$.

D is said to be *integrally closed* in S if each element of S that is integral over D is actually in D.

Example 1.23 The integral domain $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, but not in $\mathbb{C}$ since $\sqrt{-1} \in \mathbb{C}$ is integral over $\mathbb{Z}$.

The following will prove to be a useful tool in §1.6, and is of interest in its own right. The reader should solve Exercise 1.40 on page 33 in anticipation of the proof.

Theorem 1.14 — Towers of Integral Domains

If $R \subseteq S \subseteq T$ is a tower of integral domains with S integral over R and $t \in T$ integral over S, then t is integral over R.

Proof. Given that $t \in T$ is integral over S, there exist $s_1, s_2, \ldots, s_n \in S$ such that

$$t^n + s_{n-1}t^{n-1} + \cdots + s_1 t + s_0 = 0.$$

Hence, we have shown that t is integral over $R[s_0, s_1, \ldots, s_n]$. Since $s_j \in S$ is integral over R for $j = 0, 1, \ldots, n-1$, then by part (c) of Exercise 1.40, $R[s_0, s_1, \ldots, s_n]$ is a finitely generated R-module. Since t is integral over $R[s_0, s_1, \ldots, s_n]$, then the same exercise part (d) shows that

$$R[s_0, s_1, \ldots, s_n][t] = R[s_0, s_1, \ldots, s_n, t]$$

is a finitely generated R-module. Hence, by part (e) of the exercise, t is integral over R. □

Now we bring in Dedekind's ideas.

Definition 1.23 — Dedekind Domains

A *Dedekind Domain* is an integral domain D satisfying the following properties.

(A) Every ideal of D is finitely generated.

(B) Every nonzero prime D-ideal is maximal.

(C) D is integrally closed in its quotient field F.

Remark 1.12 Condition (C) says that if $\alpha/\beta \in F$ is the root of some monic polynomial over D, then $\alpha/\beta \in D$, namely $\beta \mid \alpha$ in D. Also, note that by Lemma 1.2 on page 20, Condition (A) may be replaced by the condition that R is a Noetherian domain.

Now we aim at the main goal of this section, which is a unique factorization theorem for ideals. To this end, we first settle conditions for which the converse of Lemma 1.1 on page 17 holds. We require a more general notion of ideal in order to proceed.

Definition 1.24 — Fractional Ideals

Suppose that D is an integral domain with quotient field F. Then a nonempty subset I of F is called a *fractional* D-ideal if it satisfies the following three properties.

1. For any $\alpha,\beta \in I$, $\alpha+\beta \in I$.
2. For any $\alpha \in I$ and $r \in D$, $r\alpha \in I$.
3. There exists a nonzero $\gamma \in D$ such that $\gamma I \subseteq D$.

When $I \subseteq D$, we call I an *integral* D-ideal (which is the content of Definition 1.12 on page 15) to distinguish it from the more general fractional ideal.

Remark 1.13 It is immediate from Definition 1.24 that if I is a fractional D-ideal, then there exists a nonzero $\gamma \in D$ such that $\gamma I = J$ where J is an integral D-ideal.

Example 1.24 Let $D = \mathbb{Z}$, and $F = \mathbb{Q}$. Then the fractional D-ideals are the sets

$$I_q = \{q\mathbb{Z} : q \in \mathbb{Q}^+\}.$$

Since $q\mathbb{Z} = (-q)\mathbb{Z}$, we may restrict attention to the positive rationals $\mathbb{Q}^+$ without loss of generality. Also,

$$I_{q_1} I_{q_2} = q_1 q_2 \mathbb{Z} = I_{q_1 q_2}.$$

We have the isomorphism

$$\mathcal{S} = \{I_q : q \in \mathbb{Q}^+\} \cong \mathbb{Q}^+,$$

as multiplicative groups. The unit element of $\mathcal{S}$ is $\mathbb{Z}$ and the inverse element of $I_q \in \mathcal{S}$ is $(I_q)^{-1} = q^{-1}\mathbb{Z}$. (See Exercise 1.43 on page 33.)

Example 1.24 motivates the following.

Theorem 1.15 — Inverse Fractional Ideals

If D is an integral domain with quotient field F, and I is a fractional D-ideal, then the set

$$I^{-1} = \{\alpha \in F : \alpha I \subseteq D\}$$

is a nonzero fractional D-ideal.

Proof. If $\alpha,\beta \in I^{-1}$, then $\alpha I \subseteq D$ and $\beta I \subseteq D$, so

$$(\alpha+\beta)I \subseteq \alpha I + \beta I \subseteq D,$$

which implies $\alpha+\beta \in I^{-1}$. If $\alpha \in I^{-1}$ and $r \in D$, $\alpha I \subseteq D$, then $r\alpha I \subseteq D$, from which it follows that $r\alpha \in I^{-1}$. Lastly, let γ be a nonzero element of I. Then for any $\alpha \in I^{-1}$, $\alpha I \subseteq D$, so in particular, $\gamma\alpha \in D$. Hence, $\gamma I^{-1} \subseteq D$. This satisfies all three conditions in Definition 1.24. □

Definition 1.25 — Invertible Fractional Ideals
In an integral domain D a fractional D-ideal I is called invertible if

$$I^{-1}I = D,$$

where I^{-1}, given in Theorem 1.15, is called the *inverse* of I.

Now we may return to Dedekind domains and the pertinence of the above to them.

Theorem 1.16 — Invertibility in Dedekind Domains
If D is a Dedekind domain, then every nonzero integral D-ideal is invertible.

Proof. Since D is a Dedekind Domain, then every D-ideal I is finitely generated, so for $I \neq (0)$, there are $\alpha_j \in D$ for $1 \leq j \leq d$ such that $I = (\alpha_1, \alpha_2, \ldots, \alpha_d)$. If $d = 1$, then $I^{-1} = (\alpha_1^{-1})$ and $II^{-1} = D$. Now the result may be extrapolated by induction, and the result is established. □

Corollary 1.7 — To Divide is the Same as to Contain
If D is a Dedekind domain, and I, J are D-ideals, then

$$I \Bigm| J \text{ if and only if } J \subseteq I.$$

Proof. In view of Lemma 1.1, we need only prove one direction. Suppose that

$$J \subseteq I. \tag{1.19}$$

Now let $H = I^{-1}J$, in which case $J = IH$ where H is a D-ideal since by (1.19),

$$I^{-1}J \subseteq I^{-1}I = D,$$

where the equality follows from Theorem 1.16. Thus, $I \bigm| J$, and we have secured the result.□

As a consequence of Corollary 1.7, we see that a prime D-ideal $\mathcal{P}$ in a Dedekind domain D satisfies the same property as prime elements in $\mathbb{Z}$—see Example 1.9 on page 4.

Corollary 1.8 Suppose that D is a Dedekind domain. Then $\mathcal{P}$ is a prime D-ideal if it satisfies the property that for any D-ideals I, J,

$$\mathcal{P} \bigm| IJ \text{ if and only if } \mathcal{P} \bigm| I \text{ or } \mathcal{P} \bigm| J.$$

Proof. By Corollary 1.7, $\mathcal{P} \bigm| IJ$ if and only if $IJ \subseteq \mathcal{P}$ and the latter holds, by (1.17) on page 16, if and only if $I \subseteq \mathcal{P}$ or $J \subseteq \mathcal{P}$, so applying Corollary 1.7 to the latter we get the result. □

We have the following result that mimics the same law for nonzero elements of $\mathbb{Z}$.

Corollary 1.9 — Cancellation Law for Ideals in Dedekind Domains
Let D be a Dedekind domain. If I, J, L are D-ideals with $I \neq (0)$, and $IJ \subseteq IL$, then $J \subseteq L$.

Proof. If $IJ = IL$, then by Theorem 1.16,

$$J = DJ = I^{-1}IJ \subseteq I^{-1}IL = DL = L,$$

as required. □

Now we are ready for the promised unique factorization result.

Theorem 1.17 — Unique Factorization of Ideals

Every proper nonzero ideal in a Dedekind domain D is uniquely representable as a product of prime ideals. In other words, any D-ideal has a unique expression (up to order of the factors) of the form

$$I = \mathcal{P}_1^{a_1}\mathcal{P}_2^{a_2}\ldots\mathcal{P}^{a_n},$$

where the $\mathcal{P}_j$ are the distinct prime D-ideals containing I, and $a_j \in \mathbb{N}$ for $j = 1, 2, \ldots, n$.

Proof. First we must show existence. In other words, we must show that every ideal is indeed representable as a product of primes. Let $\mathcal{S}$ be the set of all nonzero proper ideals that are not so representable.

It follows from Remark 1.12 on page 26 and Corollary 1.4 on page 21 that if $\mathcal{S} \neq \varnothing$, then $\mathcal{S}$ has a maximal member M. By assumption, M cannot be prime and hence not maximal in D, so contained in some maximal prime D-ideal $\mathcal{P}$. Also, $\mathcal{P}$ is maximal by part (B) of Definition 1.23. Hence,

$$D \subseteq \mathcal{P}^{-1} \subseteq M^{-1},$$

which implies

$$M \subseteq M\mathcal{P}^{-1} \subseteq MM^{-1} = D,$$

where the equality follows from Theorem 1.16 on the previous page. We have shown that $M\mathcal{P}^{-1}$ is an integral D-ideal. If $\mathcal{P}^{-1}M = M$, then

$$\mathcal{P}\mathcal{P}^{-1}M = \mathcal{P}M \subseteq \mathcal{P},$$

where the latter inclusion comes from the fact that $\mathcal{P}$ is an ideal. Hence, $M = \mathcal{P}$ by the maximality of $\mathcal{P}$, a contradiction to $M \in \mathcal{S}$. Thus, $\mathcal{P}^{-1}M \neq M$, so $M \subset \mathcal{P}^{-1}M$, namely $\mathcal{P}^{-1}M$ is an integral ideal not in $\mathcal{S}$. This means there are prime ideals $\mathcal{P}_j$ for $j = 1, 2, \ldots d \in \mathbb{N}$ such that

$$\mathcal{P}^{-1}M = \mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_d,$$

which implies

$$M = DM = \mathcal{P}\mathcal{P}^{-1}M = \mathcal{P}\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_d,$$

contradicting that $M \in \mathcal{S}$. We have shown $\mathcal{S} = \varnothing$, thereby establishing existence. It remains to show uniqueness of representation.

Let $\mathcal{P}_j$ and $\mathcal{Q}_k$ be (not necessarily distinct) prime D-ideals such that

$$\mathcal{P}_1\cdots\mathcal{P}_r = \mathcal{Q}_1\cdots\mathcal{Q}_s. \tag{1.20}$$

Hence,

$$\mathcal{P}_1 \supseteq \mathcal{Q}_1\cdots\mathcal{Q}_s,$$

so $\mathcal{Q}_j \subseteq \mathcal{P}_1$ for some $j = 1, 2, \ldots, s$. Without loss of generality, we may assume that $j = 1$, by rearranging the $\mathcal{Q}_j$ if necessary. However, by condition (B) of Definition 1.23, $\mathcal{P}_1 = \mathcal{Q}_1$. Multiplying both sides of (1.20) by $\mathcal{P}_1^{-1}$, we get

$$\mathcal{P}_2\cdots\mathcal{P}_r = \mathcal{Q}_2\cdots\mathcal{Q}_s.$$

Continuing in this fashion, we see that by induction, $r = s$ and $\mathcal{P}_j = \mathcal{Q}_j$ for $1 \leq j \leq s = r$.□

Biography 1.3 Julius Wilhelm Richard Dedekind (1831–1916) was born in Brunswick, Germany on October 6, 1831. There he attended school from the time he was seven. In 1848, he entered the Collegium Carolinum, an educational bridge between high school and university. He entered Göttingen at the age of 19, where he became Gauss' last student, and achieved his doctorate in 1852, the topic being Eulerian integrals. Although he taught in Göttingen and in Zürich, he moved to Brunswick in 1862 to teach at the *Technische Hochschule*, a technical high school. In that year he also was elected to the Göttingen Academy, one of many honours bestowed on him in his lifetime. He maintained this position until he retired in 1894. Dedekind's creation of ideals was published in 1879 under the title *Uber die Theorie der ganzen algebraischen Zahlen.* Hilbert extended Dedekind's ideal theory, which was later advanced further by Emmy Noether. Ultimately this led to the general notion of unique factorization of ideals into prime powers in what we now call *Dedekind domains.* Another of his major contributions was a definition of irrational numbers in terms of what we now call *Dedekind cuts.*He published this work in *Stetigkeit und Irrationale Zahlen* in 1872. He never married, and lived with his sister Julie until she died in 1914. He died in Brunswick on February 12, 1916.

Now we look at PIDs and UFDs in the case of Dedekind domains.

Theorem 1.18 — UFDs are PIDs for Dedekind domains

If R is a Dedekind domain, then R is a UFD if and only if R is a PID.

Proof. In view of Theorem 1.13 on page 22, we need only prove that R is a PID when it is a UFD. Therefore, if there exists an R-ideal that is not principal, then by Theorem 1.17, there exists a prime R-ideal $\mathcal{P}$ that is not principal. Let $\mathcal{S}$ consist of the set of all R-ideals I such that $\mathcal{P}I$ is principal. By Exercise 1.38 on page 33, $\mathcal{S} \neq \varnothing$. By Remark 1.12 on page 26 and Corollary 1.4 on page 21, $\mathcal{S}$ has a maximal element M. Let

$$\mathcal{P}M = (\alpha).$$

If $\alpha = \beta\gamma$ where $\beta \in \mathcal{P}$ is irreducible, then $(\beta) = \mathcal{P}J$ where J is an R-ideal such that $J \bigm| M$, so $J \supseteq M$. By the maximality of M, we have $J = M$, so γ is a unit and α is irreducible. Since $\mathcal{P}$ is not principal, there is a nonzero $\delta \in \mathcal{P} - (\alpha)$, and since $M = (\alpha)$ would imply that $\mathcal{P} = R$, there is a nonzero $\sigma \in M - (\alpha)$. Thus, $\delta\sigma \in \mathcal{P}M \subseteq (\alpha)$, so $\alpha \bigm| \delta\sigma$. However, α divides neither δ nor σ, so α is not prime. This contradicts Theorem 1.2 on page 7. □

The developments in this section allow us to now define gcd and lcm concepts for ideals that mimic those for rational integers.

Definition 1.26 — A gcd and lcm for Ideals

If D is a Dedekind domain, and I, J are D-ideals, then

$$\gcd(I, J) = I + J, \text{ and } \operatorname{lcm}(I, J) = I \cap J.$$

If $\gcd(I, J) = D$, then I and J are said to be *relatively prime.*

Remark 1.14 The notion of relative primality given in Definition 1.26 is the direct analogue for rational integers since $D = (1_D)$ is a principal ideal. This is of course what we mean in $\mathbb{Z}$, since such a pair of integers can have no common divisors. Let us look at this directly.

If I, J are relatively prime, then

$$\gcd(I, J) = I + J = D.$$

If a D-ideal H divides both I and J, then by Corollary 1.7 on page 27, $I \subseteq H$, $J \subseteq H$, so

$$I + J = D \subseteq H,$$

which means that $H = D$. Hence, the only D-ideal that can divide both I and J is $D = (1)$.

The next result is the generalization of the result for rational integers proved in a course in elementary number theory.

Lemma 1.3 — Product of the Ideal-Theoretic gcd and lcm

If D is a Dedekind domain and I, J are D-ideals, then

$$\gcd(I, J) \cdot \operatorname{lcm}(I, J) = (I + J)(I \cap J) = IJ.$$

Proof. By the definition of an ideal, any elements of $I + J$ times any element of $I \cap J$ must be in I and J, so in IJ. Thus,

$$(I \cap J)(I + J) \subseteq IJ.$$

Conversely, any element of IJ is in both I and J, so in $I \cap J$, and trivially in $I + J$. Thus,

$$IJ \subseteq (I \cap J)(I + J),$$

from which the desired equality follows. □

The following exploits our unique factorization result to provide an analogue of the same result for rational integers.

Theorem 1.19 — Prime Factorizations of gcd and lcm of Ideals

Suppose that D is a Dedekind domain and I, J are D-ideals with prime factorizations given, via Theorem 1.17, by

$$I = \prod_{j=1}^{r} \mathcal{P}_j^{a_j}, \text{ and } J = \prod_{j=1}^{r} \mathcal{P}_j^{b_j},$$

where $\mathcal{P}_j$ are prime D-ideals with integers $a_j, b_j \geq 0$. Then

$$\gcd(I, J) = \prod_{j=1}^{r} \mathcal{P}_j^{m_j}, \text{ and } \operatorname{lcm}(I, J) = \prod_{j=1}^{r} \mathcal{P}_j^{M_j},$$

where $m_j = \min(a_j, b_j)$ and $M_j = \max(a_j, b_j)$, for each $j = 1, \ldots, r$.

Proof. Since $\gcd(I, J) = I + J$, then

$$\gcd(I, J) = \prod_{j=1}^{r} \mathcal{P}_j^{a_j} + \prod_{j=1}^{r} \mathcal{P}_j^{b_j} = \prod_{j=1}^{r} \mathcal{P}_j^{m_j}(\prod_{j=1}^{r} \mathcal{P}_j^{a_j - m_j} + \prod_{j=1}^{r} \mathcal{P}_j^{b_j - m_j}).$$

However, for each j, one of $a_j - m_j$ or $b_j - m_j$ is zero, so the right-hand sum is D since the two summands are relatively prime. In other words,

$$\gcd(I, J) = \prod_{j=1}^{r} \mathcal{P}_j^{m_j},$$

as required. Now, by Lemma 1.3, $(I \cap J)(I + J) = IJ$, so

$$IJ = \prod_{j=1}^{r} \mathcal{P}_j^{a_j+b_j} = \prod_{j=1}^{r} \mathcal{P}_j^{m_j}(I \cap J) = (I + J)(I \cap J),$$

so

$$\operatorname{lcm}(I, J) = I \cap J = \prod_{j=1}^{r} \mathcal{P}_j^{a_j+b_j-m_j} = \prod_{j=1}^{r} \mathcal{P}_j^{M_j},$$

and we have the complete result. □

Remark 1.15 Theorem 1.19 tells us that, when D is a Dedekind domain, $\operatorname{lcm}(I, J)$ is actually the largest ideal contained in both I and J, and $\gcd(I, J)$ is the smallest ideal containing both I and J.

The following allows us to compare unique factorization of elements with that of ideals and show where Dedekind's contribution comes into play.

Definition 1.27 — Irreducible Ideals, gcds and lcms

If D is an integral domain, then a D-ideal I is called *irreducible* if it satisfies the property that whenever a D-ideal $J \mid I$, then $J = I$ or $J = D$.

Theorem 1.20 — Irreducible = Prime in Dedekind Domains

If D is a Dedekind domain, and I is a D ideal, then I is irreducible if and only if I is a prime D-ideal.

Proof. Let I be irreducible and let J, K be D-ideals such that $I \mid JK$. Since $\gcd(I, J) \mid I$, then $\gcd(I, J) = I$ or $\gcd(I, J) = D$. If $\gcd(I, J) = I$, then $I + J = I$, which means that

$$I = J = \gcd(I, J).$$

Now suppose that $I \nmid J$. Then $\gcd(I, J) = D$, so there exist $\alpha \in I$ and $\beta \in J$ such that $\alpha + \beta = 1_D$. Therefore, given an arbitrary $\gamma \in K$, $\gamma = \gamma\alpha + \gamma\beta$. Since $I \mid JK$, then by Corollary 1.7 on page 27, $JK \subseteq I$, so $\beta\gamma \in I$ since $\beta\gamma \in JK$. However, $\alpha\gamma \in I$ so $\gamma \in I$. This shows that $K \subseteq I$, so by Corollary 1.7, we have that $I \mid K$. Hence, by Theorem 1.7 on page 16, I is prime.

Conversely, suppose that I is prime. If $I = HJ$ for some nontrivial D-ideals H and J, then either $I|H$ or $I|J$. If $I|H$, there is a D-ideal L such that $H = IL$. Therefore,

$$I = HJ = ILJ.$$

By Corollary 1.9 on page 27, $(1) = D = LJ$. Hence, $J = (1) = D$, so I is irreducible. □

The following is immediate from Theorem 1.20, and is the analogue of the definition of a rational prime.

Corollary 1.10 If D is a Dedekind domain, then I is a prime D-ideal if and only if it satisfies the property that whenever $J \mid I$ for a proper D-ideal J then $I = J$.

Remark 1.16 It follows from Theorem 1.1 on page 5 and Theorem 1.2 on page 7 that the failure of unique factorization in an integral domain D is the failure of irreducible elements to be prime in D. However, since Theorem 1.20 tells us that *irreducible ideals* are the *same* as *prime ideals* in a Dedekind domain, then we have unique factorization restored at the ideal level via Theorem 1.17 on page 28. Thus, the magnitude of of Dedekind's contribution is brought to light by this fact.

We conclude this section with a result that is the generalization of the result for $\mathbb{Z}$. The reader should be familiar with the basics of ring actions such as that covered in Appendix A, pages 326–328.

Theorem 1.21 — Chinese Remainder Theorem for Ideals

Let R be a commutative ring with identity and let $I_1, \ldots, I_r$ be pairwise relatively prime ideals in R. Then the natural map

$$\psi : R/\cap_{j=1}^{r} I_j \mapsto R/I_1 \times \cdots \times R/I_r$$

is an isomorphism.

The above statement is equivalent to saying that if $\beta_1, \beta_2, \ldots, \beta_r \in R$, there exists a $\beta \in R$ such that $\beta - \beta_j \in I_j$ for each $j = 1, 2, \ldots, r$, where β is uniquely determined modulo $\cap_{j=1}^{r} I_j$. The latter means that

$$\text{any } \gamma \text{ satisfying } \gamma - \beta_j \in I_j \text{ for each such } j \text{ implies } \beta - \gamma \in \cap_{j=1}^{r} I_j. \tag{1.21}$$

Proof. Since $\psi(s) = 0$ if and only if $s \in \cap_{j=1}^{r} I_j$, then $\ker(\psi) = (0)$, since the I_j are pairwise relatively prime. It remains to show that ψ is a surjection. Let $\beta_1, \beta_2, \ldots, \beta_r \in R$. We must show that there is a $\beta \in R$ such that $\psi(\beta) = (\beta_1, \ldots, \beta_r)$. This is tantamount to saying: there is a $\beta \in R$ such that $\beta - \beta_k \in I_k$ for each k. Since $I_i + I_j = R$ for all $i \neq j$, then by induction $I_k + \cap_{j \neq k} I_j = R$. Thus, for each such k, there exists an $\alpha_k \in I_k$ and $r_k \in \cap_{j \neq k} I_j$ such that

$$\beta_k = \alpha_k + r_k \text{ with } \beta_k - r_k \in I_k \text{ and } r_k \in I_j \text{ for all } j \neq k.$$

Set $\beta = \sum_{j=1}^{r} r_j$. Then

$$\beta - \beta_k = \sum_{j \neq k} r_j + (r_k - \beta_k) \in I_k,$$

as required. □

Remark 1.17 In Theorem 1.21, we may use the notation

$$\gamma \equiv \beta_j \pmod{I_j},$$

to denote $\gamma - \beta_j \in I_j$. Then (1.21) becomes:

$$\text{any } \gamma \text{ satisfying } \gamma \equiv \beta_j \pmod{I_j} \text{ for } 1 \le j \le r \text{ implies } \beta \equiv \gamma \pmod{\cap_{j=1}^{r} I_j}.$$

Exercises

1.36. Let R be a Dedekind domain. If I, J are R-ideals, prove that there exists an $\alpha \in I$ such that $\gcd((\alpha), IJ) = I$.

1.37. Let R be a Dedekind domain, and let I, J, H be R-ideals. Prove that

$$I(J + H) = IJ + IH.$$

1.38. Let R be a Dedekind domain and I, J nonzero R-ideals. Prove that there is an R-ideal H, relatively prime to J, such that HI is principal.

1.39. Let R be an integral domain with quotient field F. Prove that every invertible fractional R-ideal is a finitely generated R-ideal—see Appendix A pages 323–326.

1.40. Establish each of the following.

(a) If $R \subseteq S \subseteq T$ is a tower of integral domains and $t \in T$ is integral over R, then t is integral over S.

(b) Let R, S be integral domains such that $R \subseteq S$. If $s \in S$, then s is integral over R if and only if $R[s]$ is a finitely generated R-module.

(c) Let R, S be integral domains such that $R \subseteq S$. If $s_1, s_2, \ldots, s_n \in S$ are integral over R, then $R[s_1, s_2, \ldots, s_n]$ is a finitely generated R-module.

(d) If $s \in S$ and there is an integral domain U such that $R[s] \subseteq U \subseteq S$ with U a finitely generated R-module, then s is integral over R and $R[s]$ is a finitely generated R-module.

(e) If $R \subseteq S \subseteq T$ is a tower of integral domains with S integral over R, and $t \in T$ is integral over S, then t is integral over R.

(f) If $R \subseteq S \subseteq T$ is a tower of integral domains with T integral over S and S integral over R, then T is integral over R. (*Transitivity of integrality.*)

1.41. Let R be an integral domain with quotient field F. Prove that every nonzero finitely-generated submodule I of F is a fractional R-ideal.

1.42. Prove that in an integral domain R, the following are equivalent.

(a) Every nonzero fractional R-ideal is invertible.

(b) The set of all fractional R-ideals G forms a multiplicative group.

1.43. Prove that in an integral domain R, the following are equivalent.

(i) R is a Dedekind domain.

(ii) Every proper R-ideal is a unique product of a finite number of prime ideals (up to order of the factors), and each is invertible.

(iii) Every nonzero R-ideal is invertible.

(iv) Every fractional R-ideal is invertible.

(v) The set of all fractional R-ideals forms a multiplicative abelian group.

(*Hint: Use Exercises 1.39–1.42.*)

1.44. Suppose that R is a Dedekind domain with quotient field F and I is an R-ideal. Also, we define:

$$\mathrm{ord}_{\mathcal{P}}(I) = a$$

where $a \geq 0$ is the largest power of the prime ideal $\mathcal{P}$ dividing I. In other words, $\mathcal{P}^a \mid I$ but $\mathcal{P}^{a+1}$ does not divide I. The value $\mathrm{ord}_{\mathcal{P}}(I)$ is called the *order of I with respect to $\mathcal{P}$.* Prove the following.

(a) For R-ideals I, J,

$$\mathrm{ord}_{\mathcal{P}}(IJ) = \mathrm{ord}_{\mathcal{P}}(I) + \mathrm{ord}_{\mathcal{P}}(J).$$

(b) For R-ideals I, J,

$$\mathrm{ord}_{\mathcal{P}}(I + J) = \min(\mathrm{ord}_{\mathcal{P}}(I), \mathrm{ord}_{\mathcal{P}}(J)).$$

(c) For any R-ideal I, there exists an $\alpha \in F$ such that $\mathrm{ord}_{\mathcal{P}}((\alpha)) = \mathrm{ord}_{\mathcal{P}}(I)$ for any prime R-ideal $\mathcal{P} \mid I$.

(*We will have occasion to invoke this new concept when we have developed the tools to study reciprocity laws—see Proposition 6.8 on page 296 and the discussion following it.*)

1.45. Prove that every R-ideal in a Dedekind domain R can be generated by at most two elements.

(*Hint: Use Exercise 1.44.*)

1.46. Prove that D is a Dedekind domain if and only if D is integrally closed, every nonzero prime ideal is maximal, and D is Noetherian.

1.47. With reference to Exercise 1.25 on page 14, prove that an almost Euclidean domain is a PID, and hence Noetherian.

(Note that this is stronger than Exercise 1.25 since there are UFDs that are not PIDs—see Remark 1.11 on page 22.)

1.48. Prove the converse of Exercise 1.47, namely that a PID is almost Euclidean.

(*Hint: Define a function ϕ on the PID such that $\phi(\alpha) = 2^n$ where $n \in \mathbb{N}$ is the number of irreducibles into which α uniquely factors.*)

(*Exercises 1.47–1.48 verify the assertion made in Exercise 1.25 wherein we noted that Greene* [25] *proved: D is almost Euclidean domain if and only if D is a PID.*)

1.49. Determine whether or not

$$\mathcal{I} = \left\{ \frac{n}{2^m} : n, m \in \mathbb{Z}, m \geq 0, n > 0 \right\}$$

is a fractional $\mathbb{Z}$-ideal.

1.50. Let $F = \mathbb{Q}(\sqrt{10})$ and $\mathfrak{O}_F = \mathbb{Z}[\sqrt{10}]$. Find the inverse of the $\mathfrak{O}_F$-ideal

$$I = (6, 2 + \sqrt{10})$$

—see Definition 1.25 on page 27.

1.6 Algebraic Numbers and Number Fields

> *Only a fool learns from his own mistakes. The wise man learns from the mistakes of others.*
>
> **Otto von Bismark (1815–1898), German statesman**

§1.1–§1.5 built the foundation for us to introduce the fundamentals of algebraic number theory. This involves the generalization of the integral domain $\mathbb{Z}$ and its quotient field $\mathbb{Q}$. To see how this is done, we consider the elements of $\mathbb{Z}$ as roots of linear monic polynomials, namely if $a \in \mathbb{Z}$, then a is a root of $f(x) = x - a$. Then we generalize as follows, with some of what follows adapted from [54].

Definition 1.28 — Algebraic Integers
If $\alpha \in \mathbb{C}$ is a root of a monic, integral polynomial of degree d, namely a root of a polynomial of the form

$$f(x) = \sum_{j=0}^{d} a_j x^j = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d \in \mathbb{Z}[x],$$

which is irreducible over $\mathbb{Q}$, then α is called an algebraic integer of degree d.

Example 1.25 $a + b\sqrt{-1} = a + bi$, where $a, b \in \mathbb{Z}$, with $b \neq 0$ is an algebraic integer of degree 2 since it is a root of $x^2 - 2ax + a^2 + b^2$ but not a root of a linear, integral, monic polynomial since $b \neq 0$.

In Definition 1.3 on page 2 we introduced primitive roots of unity which are a distinguished type of algebraic integer. Another special type of algebraic integer is given by the following.

Example 1.26 Numbers of the form $z_0 + z_1\zeta_n + z_2\zeta_n^2 + \cdots + z_{n-1}\zeta_n^{n-1}$, for $z_j \in \mathbb{Z}$ are called *cyclotomic integers* of order n.

Now we develop the generalization of the rational number field as a quotient field of a special ring for which this sets the stage.

Definition 1.29 — Algebraic Numbers and Number Fields
An algebraic number, α, of degree $d \in \mathbb{N}$ is a root of a monic polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$. Denote the subfield of $\mathbb{C}$ consisting of all algebraic *numbers* by $\overline{N}$, and the set of all algebraic *integers* in $\overline{N}$ by $\mathbb{A}$. An *algebraic number field*, or simply *number field*, is of the form

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq \mathbb{C} \text{ with } n \in \mathbb{N} \text{ where } \alpha_j \in \overline{N} \text{ for } j = 1, 2, \ldots, n.$$

An algebraic number of degree $d \in \mathbb{N}$ over a number field F is the root of an irreducible polynomial of degree d over F.

Remark 1.18 If F is a *simple extension*, namely of the form $\mathbb{Q}(\alpha)$, for an algebraic number α, then we may consider this as a vector space over $\mathbb{Q}$, in which case we may say that $\mathbb{Q}(\alpha)$ has dimension d over $\mathbb{Q}$ having basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$. (See Theorem A.4 on page 325. Also, see Exercise 1.51 on page 43 to see that all number fields are indeed simple.)

By Definition 1.29, $\mathbb{Q}$ is the smallest algebraic number field since it is of dimension 1 over itself, and the simple field extension $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and α.

We now demonstrate that $\mathbb{A}$, as one would expect, has the proper structure in $\overline{N}$, which will lead us to a canonical subring of algebraic number fields. If necessary, the reader may review the basics on modules beginning on page 323 in Appendix A.

Theorem 1.22 — The Ring of All Algebraic Integers

$\mathbb{A}$ is a subring of $\overline{N}$.

Proof. It suffices to prove that if $\alpha,\beta \in \mathbb{A}$, then both $\alpha+\beta \in \mathbb{A}$ and $\alpha\beta \in \mathbb{A}$. To this end we need the following.

Claim 1.3 If $\alpha \in \mathbb{A}$, then $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$ is a finitely generated $\mathbb{Z}$-module.

Since $\alpha \in \mathbb{A}$, then there exist $a_j \in \mathbb{Z}$ for $j = 0, 1, \ldots, d-1$ for some $d \geq 1$ such that

$$\alpha^d - a_{d-1}\alpha^{d-1} - \cdots - a_1\alpha - a_0 = 0.$$

Therefore,

$$\alpha^d = a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \cdots + a_1\alpha + a_0 \in \mathbb{Z}\alpha^{d-1} + \cdots + \mathbb{Z}\alpha + \mathbb{Z},$$

and

$$\begin{aligned}\alpha^{d+1} &= a_{d-1}\alpha^d + a_{d-2}\alpha^{d-1} + \cdots + a_1\alpha^2 + a_0\alpha \in \mathbb{Z}\alpha^d + \mathbb{Z}\alpha^{d-1} + \cdots + \mathbb{Z}\alpha^2 + \mathbb{Z}\alpha \\ &\subseteq \mathbb{Z}\alpha^{d-1} + \mathbb{Z}\alpha^{d-2} + \cdots + \mathbb{Z}\alpha + \mathbb{Z}.\end{aligned}$$

Continuing in this fashion we conclude, inductively, that

$$\alpha^c \in \mathbb{Z}\alpha^{d-1} + \mathbb{Z}\alpha^{d-2} + \cdots + \mathbb{Z}\alpha + \mathbb{Z},$$

for any $c \geq d$. However, clearly,

$$\alpha^c \in \mathbb{Z}\alpha^{d-1} + \mathbb{Z}\alpha^{d-2} + \cdots + \mathbb{Z}\alpha + \mathbb{Z},$$

for $c = 1, 2, \cdots, d-1$, so

$$\alpha^c \in \mathbb{Z}\alpha^{d-1} + \mathbb{Z}\alpha^{d-2} + \cdots + \mathbb{Z}\alpha + \mathbb{Z},$$

for any $c \geq 0$. Hence, $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. This completes Claim 1.3.

By Claim 1.3, both $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated. Suppose that $a_1, a_2, \ldots, a_k$ are generators of $\mathbb{Z}[\alpha]$ and $b_1, b_2, \ldots, b_\ell$ are generators of $\mathbb{Z}[\beta]$. Then $\mathbb{Z}[\alpha,\beta]$ is the additive group generated by the a_ib_j for $1 \leq i \leq k$ and $1 \leq j \leq \ell$. Thus, $\mathbb{Z}[\alpha,\beta]$ is finitely generated. Since $\alpha+\beta, \alpha\beta \in \mathbb{Z}[\alpha,\beta] \subseteq \mathbb{A}$ we have secured the theorem. □

Given an algebraic number field F, $F \cap \mathbb{A}$ is a ring in F, by Exercise 1.29 on page 19. This leads to the following.

Definition 1.30 — Rings of Integers

If F is an algebraic number field, then $F \cap \mathbb{A}$ is called the *ring of (algebraic) integers* of F, denoted by $\mathfrak{O}_F$.

With Definition 1.30 in hand, we may now establish a simple consequence of Theorem 1.22.

Corollary 1.11 The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, namely $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

Proof. If $\alpha \in \mathbb{A} \cap \mathbb{Q}$, then $\alpha = a/b$ where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, with $b \neq 0$. Since $\alpha \in \mathbb{A}$, there exists an

$$f(x) = a_0 + \sum_{j=1}^{d} a_j x^j \in \mathbb{Z}[x]$$

with $a_d = 1$, such that $f(\alpha) = 0$. If $d = 1$, then we are done, since $a_0 + \alpha \in \mathbb{Z}$ and $a_0 \in \mathbb{Z}$. If $d > 1$, then

$$a_0 + \sum_{j=1}^{d} a_j \alpha^j \in \mathbb{Z}$$

so

$$\sum_{j=1}^{d} a_j \alpha^j = \sum_{j=1}^{d} \frac{a_j a^j b^{d-j}}{b^d} \in \mathbb{Z}.$$

Therefore, b^d divides $\sum_{j=1}^{d} a_j a^j b^{d-j}$. Since $d > 1$, b divides $\sum_{j=1}^{d-1} a_j a^j b^{d-j}$, so $b \mid a^d$. But $\gcd(a, b) = 1$, so $b = 1$ and $\alpha \in \mathbb{Z}$. □

Corollary 1.12 If F is an algebraic number field, then $\mathbb{Q} \cap \mathfrak{O}_F = \mathbb{Z}$.

Proof. Since $\mathfrak{O}_F \subseteq \mathbb{A}$, then by Corollary 1.11, $\mathbb{Q} \cap \mathfrak{O}_F \subseteq \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$. But clearly $\mathbb{Z} \subseteq \mathbb{Q} \cap \mathfrak{O}_F$, so we have equality. □

Remark 1.19 In order to state the next result, we require a few comments on the notion of *finite generation.* By Definition 1.29 and Claim 1.3 in the proof of Theorem 1.22, we know that for any number field F, $\mathfrak{O}_F$ is finitely generated as a $\mathbb{Z}$-module. Thus, any $\mathfrak{O}_F$-ideal I will have a representation as $I = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ with $\alpha_j \in \mathfrak{O}_F$ for $j = 1, 2, \ldots, d$, and we say that I is *finitely generated.* In the instance where $d = 1$, we are in the case of Definition 1.13 on page 15, namely a principal ideal. Also, see Remark 1.9 on page 15.

Corollary 1.13 If F is a number field, then $\mathfrak{O}_F$ is a Noetherian domain.

Proof. This follows from Remark 1.19 above and Lemma 1.2 on page 20. □

In Definition 1.22 on page 25, we defined integrality over a domain. Now we extend this notion to algebraic numbers and number fields.

Definition 1.31 — Elements Algebraic Over a Domain

If $R \subseteq S$ where R and S are integral domains, then if R is a field and α is integral over R, then α is said to be *algebraic* over R. Also, if every nonconstant polynomial $f(x) \in R[x]$ has a root in R, then R is said to be *algebraically closed.* Moreover, any extension field that is algebraic over R and is algebraically closed is called an *algebraic closure* of R, and it may be shown that an algebraic closure is unique up to isomorphism.

Remark 1.20 In view of Definition 1.29 on page 35, and Definition 1.31 above, we may now restate the notion of an *algebraic number* as a complex number that is algebraic over $\mathbb{Q}$. Moreover, in view of Definition 1.28 on page 35 and Definition 1.31, we see that an *algebraic integer* is a complex number that is integral over $\mathbb{Z}$.

Given an element α that is algebraic over a number field F, Definition 1.31 tells us that there is a monic polynomial $m_{\alpha,F}(x) \in F[x]$ with $m_{\alpha,F}(\alpha) = 0$. We may assume that $m_{\alpha,F}$ has minimal degree. Hence, $m_{\alpha,F}$ must be irreducible, since otherwise, α would be the root of a polynomial of lower degree. Thus chosen, $m_{\alpha,F}(x)$ is called *the minimal polynomial of α over F*. It turns out this polynomial is also unique.

Theorem 1.23 — Minimal Polynomials Are Unique

A number $\alpha \in \mathbb{C}$ is an algebraic number of degree $d \in \mathbb{N}$ over a number field F if and only if α is the root of an unique irreducible monic polynomial

$$m_{\alpha,F}(x) \in F[x].$$

Any $h(x) \in F[x]$ such that $h(\alpha) = 0$ must be divisible by $m_{\alpha,F}(x)$ in $F[x]$.

Proof. If α is an algebraic number of degree d over F, then by Definition 1.29, we may let $f(x) \in F[x]$ be a monic polynomial of minimal degree with $f(\alpha) = 0$, and let $h(x) \in F[x]$ be any other monic polynomial of minimal degree with $h(\alpha) = 0$. Then by the Euclidean algorithm for polynomials (see Theorem A.13 on page 333) there exist $q(x), r(x) \in F[x]$ such that

$$h(x) = q(x)f(x) + r(x), \text{ where } 0 \le \deg(r) < \deg(f) \text{ or } r(x) = 0, \text{ the zero polynomial.}$$

However $f(\alpha) = 0$ so $h(\alpha) = 0 = f(\alpha)$, and $r(\alpha) = 0$, contradicting the minimality of f unless $r(x) = 0$ for all x. Hence, $f(x) \bigm| h(x)$. The same argument can be used to show that $h(x) \bigm| f(x)$. Hence, $h(x) = cf(x)$ for some $c \in F$. However, f and h are monic, so $c = 1$ and $h = f$. This proves that $f(x) = m_{\alpha,F}(x)$ is the unique monic polynomial of α over F. The converse of the first statement follows *a fortiori*.

To prove the second statement, assume that $h(x) \in F[x]$ such that $h(\alpha) = 0$ and use the Euclidean algorithm for polynomials as above to conclude that $m_{\alpha,F}(x) \bigm| h(x)$ by letting $m_{\alpha,F}(x) = f(x)$ in the above argument. □

Corollary 1.14 An irreducible polynomial over an algebraic number field has no repeated roots in $\mathbb{C}$. In particular, all the roots of $m_{\alpha,F}(x)$ are distinct.

Proof. If F is a number field and $f(x) \in F[x]$ is irreducible with a repeated root α, then

$$f(x) = c(x - \alpha)^2 g(x),$$

for some $c \in F$ and $g(x) \in \mathbb{C}[x]$. By Theorem 1.23, $m_{\alpha,F}(x) \bigm| f(x)$ so $f(x) = am_{\alpha,F}(x)$ for some $a \in F$, since f is irreducible. However, $f'(x) = 2c(x - \alpha)g(x) + c(x - \alpha)^2 g'(x)$, where f' is the derivative of f. Hence, $f'(\alpha) = 0$, so by Theorem 1.23, again $m_{\alpha,F}(x) \bigm| f'(x)$, contradicting the minimality of $m_{\alpha,F}(x)$ since $\deg(f') < \deg(f)$. □

Corollary 1.15 If $\alpha \in \mathbb{A}$, then $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$.

Proof. This follows from Definition 1.28 on page 35 and Theorem 1.23. □

Now our goal is to demonstrate that algebraic integers are sufficient to characterize algebraic number fields. First we need the following crucial result.

Lemma 1.4 — Algebraic Numbers as Quotients of Integers

Every algebraic number is of the form α/ℓ where α is an algebraic integer and $\ell \in \mathbb{Z}$ is nonzero.

Proof. By Definition 1.29, if γ is an algebraic number, there exist $a_j \in \mathbb{Q}$ for $j = 0, 1, 2, \ldots, d-1$ such that γ is a root of

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + x^d.$$

Since

$$a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{d-1}\gamma^{d-1} + \gamma^d = 0$$

we may form the least common multiple, ℓ, of the denominators of the a_j for $j = 0, 1, \ldots, d$. Then multiplying through by ℓ,

$$(\ell\gamma)^d + (\ell a_{d-1})(\ell\gamma)^{d-1} + \cdots + (\ell^{d-1} a_1)(\ell\gamma) + \ell^d a_0 = 0.$$

Thus $\ell\gamma$ is the root of a monic integral polynomial, so $\ell\gamma$ is an algebraic integer, say, α. Hence, $\gamma = \alpha/\ell$, with $\alpha \in \mathbb{A}$ and $\ell \in \mathbb{Z}$. □

Corollary 1.16 — Quotient Fields of Number Rings

If F is a number field, then the quotient field of $\mathfrak{O}_F$ is F.

Proof. Let $K = \{\alpha\beta^{-1} : \alpha, \beta \in \mathfrak{O}_F, \beta \neq 0\}$ be the quotient field of $\mathfrak{O}_F$. Suppose that $\gamma = \alpha\beta^{-1} \in K$. Since $\mathfrak{O}_F \subseteq F$, then $\gamma \in F$, so $K \subseteq F$. Now if $\gamma \in F$, then by Lemma 1.4, $\gamma = \alpha/\ell$ where $\alpha \in \mathbb{A}$ and $\ell \in \mathbb{Z}$. However, since $\alpha = \gamma\ell \in F \cap \mathbb{A} = \mathfrak{O}_F$ by Definition 1.30 on page 36, then $\alpha \in \mathfrak{O}_F \subseteq F$, so $K \subseteq F$. Hence, $K = F$. □

Theorem 1.24 — The Primitive Element Theorem for Number Fields

If F is an algebraic number field, then there is an algebraic integer α such that $F = \mathbb{Q}(\alpha)$.

Additionally, if β is algebraic over F with minimal polynomial $m_{\beta,F}(x)$, then

$$|F(\beta) : F| = \deg(m_{\beta,F}).$$

Proof. By Exercise 1.51 on page 43, $F = \mathbb{Q}(\gamma)$ for some algebraic number γ, and by Lemma 1.4, $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha/\ell) = \mathbb{Q}(\alpha)$ or some $\alpha \in \mathbb{A}$.

The second statement will follow if we can show that every element $\delta \in F(\beta)$ is uniquely represented in the form

$$\delta = \sum_{j=0}^{d-1} a_j \beta^j \in F[\beta],$$

where $\deg(m_{\beta,f}(x)) = d$. Since $\delta = f(\beta)/g(\beta)$ with $f(x), g(x) \in F[x]$ and $g(\beta) \neq 0$, then by Theorem 1.23 on the facing page, $m_{\beta,F}(x)$ does not divides $g(x)$. Therefore, $\gcd(g(x), m_{\beta,F}(x)) = 1$, so by Theorem A.13, there exist $s(x), t(x) \in F[x]$ such that $s(x)g(x) + t(x)m_{\beta,F}(x) = 1$. Since $m_{\beta,F}(\beta) = 0$ then $s(\beta) = 1/g(\beta)$. Thus, $\delta = f(\beta)/g(\beta) = f(\beta)s(\beta)$. Let $h(x) = f(x)s(x) \in F[x]$. By Theorem A.13 again, there exist $q(x), r(x) \in F[x]$ such that $h(x) = q(x)m_{\beta,F}(x) + r(x)$ such that $\deg(r) < \deg(m_{\beta,F}(x))$ or $r(x) = 0$. However,

$$\delta = f(\beta)s(\beta) = h(\beta) = q(\beta)m_{\beta,F}(\beta) + r(\beta) = r(\beta).$$

It remains to show that $r(x)$ is unique. Suppose that $v(x) \in F[x]$ such that $\deg(v) \leq d-1$ and $\delta = v(\beta)$. Thus, $r(\beta) - v(\beta) = 0$ so β is a root of $r(x) - v(x) \in F[x]$ contradicting the minimality of $m_{\beta,F}(x)$, whence $r(x) - v(x) = 0$, the zero polynomial, namely $r(x) = v(x)$ as required to secure the second statement. □

Example 1.27 Let $E = \mathbb{Q}(\sqrt{2}, i)$, where $i = \zeta_4 = \sqrt{-1}$ is a primitive fourth root of unity. Then by Exercise 1.53 on page 43,

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right), \text{ and } \zeta_8 = \frac{1+i}{\sqrt{2}}.$$

Example 1.28 If $F = \mathbb{Q}(i)$ and $\alpha = \zeta_8$ is a primitive eight root of unity, then

$$m_{\alpha,F}(x) = x^2 - i$$

is the minimal polynomial of α over F. Moreover, the minimal polynomial of α over $\mathbb{Q}$ is given by

$$m_{\alpha,\mathbb{Q}}(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1,$$

which is an example of the following type of distinguished polynomial.

Definition 1.32 — Cyclotomic Polynomials
If $n \in \mathbb{N}$, then the n^{th} *cyclotomic polynomial* is given by

$$\Phi_n(x) = \prod_{\substack{\gcd(n,j)=1 \\ 1 \le j \le n}} (x - \zeta_n^j),$$

where ζ_n is given by Definition 1.3 on page 2. The degree ofΦ $_n(x)$ is $\phi(n)$, where $\phi(n)$ is the Euler totient—see Definition A.22 on page 342.

Remark 1.21 The reader may think of the term *cyclotomic* as "circle dividing," since the n^{th} roots of unity divide the unit circle into n equal arcs. The cyclotomic polynomial also played a role in Gauss's theory of constructible regular polygons—see [20, §365–§366, pp. 458–460].

Note that since the roots of the n^{th} cyclotomic polynomial are precisely the primitive n^{th} roots of unity, then the degree ofΦ $_n(x)$ is necessarily $\phi(n)$. We now demonstrate the irreducibility of the cyclotomic polynomial.

Theorem 1.25 — Irreducibility of the Cyclotomic Polynomial
For $n \in \mathbb{N}$, $\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x)$, so$\Phi$ $_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. We may let

$$\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x)g(x) \text{ for some } g(x) \in \mathbb{Z}[x]$$

by Theorem 1.23 on page 38.

Claim 1.4 $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) = 0$ for any prime $p \nmid n$.

If $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) \neq 0$, then $g(\zeta_n^p) = 0$, so ζ_n is a root of $g(x^p)$. By Theorem 1.23 again, $g(x^p) = m_{\zeta_n,\mathbb{Q}}(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let

$$f(x) = \sum_j a_j x^j \in \mathbb{Z}[x]$$

have image

$$\overline{f}(x) = \sum_j \overline{a_j} x^j$$

under the natural map

$$\mathbb{Z}[x] \mapsto (\mathbb{Z}/p\mathbb{Z})[x].$$

Thus,

$$\overline{g}(x^p) = \overline{m}_{\zeta_n,\mathbb{Q}}(x)\overline{h}(x).$$

However, $\overline{g}(x^p) = \overline{g}^p(x)$ since $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$. Therefore, $0 = \overline{g}(\zeta_n^p) = (\overline{g}(\zeta_n))^p = \overline{g}(\zeta_n)$. Since$\Phi$ $_n(x) \bigm| (x^n - 1)$, then

$$x^n - 1 = \Phi_n(x)k(x) = m_{\zeta_n,\mathbb{Q}}(x)g(x)k(x),$$

for some $k(x) \in \mathbb{Z}[x]$. Therefore, in $\mathbb{Z}/p\mathbb{Z}[x]$,

$$x^n - \overline{1} = \overline{x^n - 1} = \overline{m}_{\zeta_n,\mathbb{Q}}(x)\overline{g}(x)\overline{k}(x).$$

Since $\overline{g}$ and $\overline{m}_{\zeta_n,\mathbb{Q}}$ have a common root ζ_n, then $x^n - \overline{1}$ has a repeated root. However, this is impossible by irreducibility criteria for polynomials over finite fields, since $p \nmid n$, (see Corollary A.8 on page 332 where we see:

$$x^n - \overline{1} \text{ is irreducible if and only if } \gcd(x^n - \overline{1}, x^{p^i} - x) = 1 \text{ for } 1 \le i \le \lfloor n/2 \rfloor).$$

We have established Claim 1.4, namely that ζ_n^p is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ for any prime $p \nmid n$. Repeated application of the above argument shows that y^p is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ whenever y is a root. Hence, ζ_n^j is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ for all j relatively prime to n such that $1 \le j < n$. Thus, $\deg(m_{\zeta_n,\mathbb{Q}}) \ge \phi(n)$. However, $m_{\zeta_n,\mathbb{Q}}(x) \bigm| \Phi_n(x)$ so

$$m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x),$$

as required. □

Corollary 1.17 For $n \in \mathbb{N}$, $|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \phi(n)$.

Proof. By Theorems 1.24–1.25, in view of Definition 1.32, the result follows. □

At this juncture, we look at general properties of units in rings of integers, in keeping with one of the themes of this section.

Proposition 1.1 Let $\alpha \in \mathbb{A}$. Then the following are equivalent.

(a) α is a unit.

(b) $\alpha \bigm| 1$ in $\mathbb{A}$.

(c) If $F = \mathbb{Q}(\alpha)$, then $m_{\alpha,F}(0) = \pm 1$.

Proof. The equivalence of (a) and (b) comes from Definition 1.1 on page 1. Now assume that α is a unit. Then, by Exercise 1.52 on page 43,

$$m_{\alpha,F}(0) = (-1)^d \prod_{j=1}^{d} \alpha_j = \pm 1$$

if and only if $\alpha \in \mathfrak{U}_F$, so (a) and (c) are equivalent. □

One of our main goals is the following result that leads us toward a unique factorization theory for ideals in rings of algebraic integers. In order to state it we need the following result which is motivated by Example 1.18 on page 15.

Lemma 1.5 — $\mathfrak{O}_\mathbf{F}$-Ideals Intersecting $\mathbb{Z}$

If F is a number field and I is a nonzero $\mathfrak{O}_F$-ideal, then $I \cap \mathbb{Z}$ contains a nonzero element of $\mathbb{Z}$.

Proof. Let $\alpha \in I$ where $\alpha \neq 0$ and consider $m_{\alpha,\mathbb{Q}}(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$, where $a_j \in \mathbb{Z}$ for all $j = 0, 1, \ldots, d-1$ by Corollary 1.15 on page 38. If $d = 1$, then $a_0 = -\alpha \neq 0$, and if $d > 1$, then $a_0 \neq 0$ since $m_{\alpha,\mathbb{Q}}(x)$ is irreducible in $\mathbb{Q}[x]$ by Corollary 1.15. Hence,

$$a_0 = -a_1\alpha - \cdots - a_{d-1}\alpha^{d-1} - \alpha^d \in I$$

as required. □

Theorem 1.26 — Rings of Integers are Dedekind Domains

If F is an algebraic number field, then $\mathfrak{O}_F$ is a Dedekind domain.

Proof. By Corollary 1.13 on page 37 (in view of the comment on condition (A) in Remark 1.12 on page 26), condition (A) of Definition 1.23 on page 25 is satisfied.

Now we show condition (B) holds. Assume that there is a prime $\mathfrak{O}_F$-ideal $\mathcal{P} \neq (0)$ that is not maximal. Therefore, the set $\mathcal{S}$, of all proper $\mathfrak{O}_F$-ideals that strictly contain $\mathcal{P}$, must be nonempty. By Corollary 1.4 on page 21, there is a maximal ideal $M \in \mathcal{S}$ such that $\mathcal{P} \subset M \subset \mathfrak{O}_F$. By Theorem 1.10 on page 18, M is a prime $\mathfrak{O}_F$-ideal. By Lemma 1.5, there exists a nonzero $a \in \mathcal{P} \cap \mathbb{Z}$. By Exercise 1.29 on page 19, $\mathcal{P} \cap \mathbb{Z}$ is a $\mathbb{Z}$-ideal.

Suppose that $ab \in \mathcal{P} \cap \mathbb{Z}$, where $a, b \in \mathbb{Z}$. Since $\mathcal{P}$ is a prime $\mathfrak{O}_F$-ideal, then $a \in \mathcal{P}$ or $b \in \mathcal{P}$ so $a \in \mathcal{P} \cap \mathbb{Z}$ or $b \in \mathcal{P} \cap \mathbb{Z}$, which means that $\mathcal{P} \cap \mathbb{Z}$ is a prime $\mathbb{Z}$-ideal. If $p \in \mathcal{P} \cap \mathbb{Z}$ is a rational prime, then $(p) \subseteq \mathcal{P} \cap \mathbb{Z}$ and (p) is a maximal $\mathbb{Z}$-ideal by Theorem 1.11 on page 18 since $\mathbb{Z}/(p)$ is a field by Example 1.21 on page 19. Hence, since $\mathcal{P} \cap \mathbb{Z} \neq \mathbb{Z}$, we have $(p) = \mathcal{P} \cap \mathbb{Z}$. However, $(p) = \mathcal{P} \cap \mathbb{Z} \subseteq M \cap \mathbb{Z} \subset \mathbb{Z}$, where $1 \notin M$, so $(p) = \mathcal{P} \cap \mathbb{Z} = M \cap \mathbb{Z}$. Since $M \in \mathcal{S}$, then $\mathcal{P} \neq M$, so there exists an $\alpha \in M$ such that $\alpha \notin \mathcal{P}$. Consider

$$m_{\alpha,\mathbb{Q}}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x] \text{ for some } d \in \mathbb{N}.$$

Then $m_{\alpha,\mathbb{Q}}(\alpha) = 0 \in \mathcal{P}$. Now define $\ell \in \mathbb{N}$ to be the least value for which there exist integers b_j such that

$$X = \alpha^\ell + b_{\ell-1}\alpha^{\ell-1} + \cdots + b_1\alpha + b_0 \in \mathcal{P}, \tag{1.22}$$

for $j = 0, 1, \cdots, \ell - 1$. Since $\alpha \in M$, then by properties of ideals,

$$Y = \alpha(\alpha^{\ell-1} + b_{\ell-1}\alpha^{\ell-2} + \cdots + b_1) \in M. \tag{1.23}$$

Since $\mathcal{P} \subset M$, then by (1.22)–(1.23), $X - Y = b_0 \in M$, so $b_0 \in M \cap \mathbb{Z} = \mathcal{P} \cap \mathbb{Z}$. If $\ell = 1$, then $\alpha \in \mathcal{P}$, a contradiction, so $\ell > 1$. Thus, by (1.22),

$$\alpha^\ell + b_{\ell-1}\alpha^{\ell-1} + \cdots + b_1\alpha + b_0 - b_0 = \alpha(\alpha^{\ell-1} + b_{\ell-1}\alpha^{\ell-2} + \cdots + b_1) \in \mathcal{P}.$$

However, since $\mathcal{P}$ is prime and $\alpha \notin \mathcal{P}$, then $\alpha^{\ell-1} + b_{\ell-1}\alpha^{\ell-2} + \cdots + b_1 \in \mathcal{P}$, contradicting the minimality of $\ell > 1$. We have shown $\mathcal{S} = \varnothing$, which establishes that condition (B) of Definition 1.23 holds.

For condition (C), we note that since F is the quotient field of $\mathfrak{O}_F$ by Corollary 1.16 on page 39, then any $\alpha \in F$ is integral over $\mathfrak{O}_F$. Since $\mathfrak{O}_F$ is integral over $\mathbb{Z}$, then by part (e) of Exercise 1.40 on page 33, α is integral over $\mathbb{Z}$. In other words, α is an algebraic integer in F, namely $\alpha \in \mathfrak{O}_F$. Hence, $\mathfrak{O}_F$ is integrally closed and we have part (C) that establishes the entire result. □

Exercises

1.51. Prove that if an algebraic number field F is of the form

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

for $n \in \mathbb{N}$ where α_j for $j = 1, 2, \ldots, n$ are algebraic numbers, then there is an algebraic number γ such that $F = \mathbb{Q}(\gamma)$. (Hence, all algebraic number fields are simple extensions of $\mathbb{Q}$.)

(*Hint: It suffices to prove this for $n = 2$ with $\alpha_1 = \alpha$ and $\alpha_2 = \beta$. Let*

$$m_{\alpha,\mathbb{Q}}(x) = \prod_{j=1}^{d_\alpha}(x - \alpha_j),$$

where the α_j are the conjugates of α over $\mathbb{Q}$, and let

$$m_{\beta,\mathbb{Q}}(x) = \prod_{j=1}^{d_\beta}(x - \beta_j),$$

where the β_j are the conjugates of $\beta_1 = \beta$ over $\mathbb{Q}$. Select $q \in \mathbb{Q}$ with

$$q \neq (\alpha - \alpha_k)/(\beta_j - \beta)$$

for any $k = 1, 2, \ldots, d_\alpha$ and any $j = 1, 2, \ldots, d_\beta$ Also, let

$$\gamma = \alpha + q\beta$$

and

$$f(x) = m_{\alpha,\mathbb{Q}}(\gamma - qx).$$

Prove that β is the only common root of $f(x)$ and $m_{\beta,\mathbb{Q}}(x)$. Show that this implies $\mathbb{Q}(\alpha,\beta\,) \subseteq \mathbb{Q}(\gamma)$. The reverse inclusion is clear.)

1.52. Let F be an algebraic number field. Prove that if $\alpha \in \mathfrak{U}_F$, then $\alpha_j \in \mathfrak{U}_F$ for all $j = 1, 2, \ldots, d$, where $m_{\alpha,F}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$, for some $d \in \mathbb{N}$ is the minimal polynomial of α over F, and α_j are the roots of $m_{\alpha,F}(x)$. Conclude that if F is an algebraic number field, then $\alpha \in \mathfrak{U}_F$ if and only if $\prod_{j=1}^{d} \alpha_j = \pm 1$.

1.53. Referring to Example 1.27 on page 40, prove that

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right),$$

and that if ζ_8 is a primitive eighth root of unity, then it is an odd power of $(1+i)/\sqrt{2}$.

1.54. Prove that

$$x^n - 1 = \prod_{d\,\big|\,n} \Phi_d(x),$$

whereΦ $_d(x)$ is the cyclotomic polynomial given in Definition 1.32 on page 40.

1.7 Quadratic Fields

> *It's not that I'm so smart; it's just that I stay with the problem longer.*
> **Albert Einstein (1879–1955), German-born theoretical physicist**

In this section we use the tools developed in this chapter and apply them to quadratic fields. This is a precursor to the general number field development later in the text and gives an overview of the least nontrivial case of a number field extension of $\mathbb{Q}$.

First we establish the rings of integers for quadratic fields. This extends our discussion begun in Application 1.2 on page 3. Then, we show that a given quadratic field is determined by a unique squarefree integer. We note that if $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$, is irreducible, and $\alpha \in \mathbb{C}$ is a root of $f(x)$, then the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and α is given by adjoining α to $\mathbb{Q}$, denoted by $\mathbb{Q}(\alpha)$, so

$$\mathbb{Q}(\alpha) = \{x + y\alpha : x, y \in \mathbb{Q}\}.$$

This is what we call a *quadratic field*, which we loosely discussed in Application 1.2 on page 3.

Quadratic polynomials with the same squarefree part of the discriminant give rise to the same quadratic field. To see this suppose that:

$$f(x) = x^2 + bx + c \text{ and } g(x) = x^2 + b_1x + c_1 \in \mathbb{Q}[x] \text{ are irreducible,}$$

$$\Delta = b^2 - 4c = m^2D,$$

and

$$\Delta_1 = b_1^2 - 4c_1 = m_1^2D,$$

$$\text{where } m, m_1 \in \mathbb{Z} \text{ and } D \text{ is squarefree.}$$

Then

$$\begin{aligned}\mathbb{Q}(\sqrt{\Delta}) &= \mathbb{Q}(\sqrt{m^2D}) = \mathbb{Q}(m\sqrt{D}) = \mathbb{Q}(\sqrt{D})\\ &= \mathbb{Q}(m_1\sqrt{D}) = \mathbb{Q}\left(\sqrt{m_1^2D}\right) = \mathbb{Q}(\sqrt{\Delta_1}).\end{aligned}$$

Thus, we need the following to clarify the situation on uniqueness of quadratic fields.

Theorem 1.27 — Quadratic Fields Uniquely Determined
If F is a quadratic field, there exists a unique squarefree integer D such that $F = \mathbb{Q}(\sqrt{D})$.

Proof. Suppose that $F = \mathbb{Q}(\alpha)$, where α is a root of the irreducible polynomial $x^2 + bx + c$. By the well-known quadratic formula $\alpha \in \{\alpha_1, \alpha_2\}$, where

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2}, \text{ and } \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Since $\alpha_1 = -\alpha_2 - b$ with $b \in \mathbb{Q}$, then $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha)$. However,

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}\left(\frac{-b + \sqrt{b^2 - 4c}}{2}\right) = \mathbb{Q}(\sqrt{b^2 - 4c}).$$

Let $a = b^2 - 4c = e/f \in \mathbb{Q}$. Then $a \neq d^2$ for any $d \in \mathbb{Q}$ since $x^2 + bx + c$ is irreducible in $\mathbb{Q}[x]$. Without loss of generality we may assume that $\gcd(e, f) = 1$ and f is positive.

Let $ef = n^2 D$, where D is the squarefree part of ef. Hence, $D \neq 1$, and arguing as in the preamble to this theorem, $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{a})$, observing that $\mathbb{Q}(\sqrt{e/f}) = \mathbb{Q}(\sqrt{ef})$. This shows existence. It remains to prove uniqueness.

If D_1 is a squarefree integer such that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_1})$, then $\sqrt{D} = u + v\sqrt{D_1}$ with $u, v \in \mathbb{Q}$. By squaring, rearranging, and assuming that $uv \neq 0$, we get

$$\sqrt{D_1} = \frac{D - u^2 - Dv^2}{2uv} \in \mathbb{Q},$$

which contradicts that D_1 is squarefree. Thus, $uv = 0$. If $v = 0$, then $\sqrt{D} \in \mathbb{Q}$, contradicting the squarefreeness of D. Therefore, $u = 0$ and $D = v^2 D_1$, but again, D is squarefree, so $v^2 = 1$, which yields that $D = D_1$. □

Now we are in a position to determine the ring of integers of an arbitrary quadratic field, which we motivated in Application 1.2 on page 3.

Theorem 1.28 — Rings of Integers in Quadratic Fields

Let F be a quadratic field and let D be the unique squarefree integer such that $F = \mathbb{Q}(\sqrt{D})$. Then

$$\mathfrak{O}_F = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{D}] & \text{if } D \not\equiv 1 \pmod 4. \end{cases}$$

Proof. Let

$$\sigma = \begin{cases} 2 & \text{if } D \equiv 1 \pmod 4, \\ 1 & \text{if } D \not\equiv 1 \pmod 4. \end{cases}$$

Then since $(1 + \sqrt{D})/\sigma$ is a root of $x^2 - 2x/\sigma + (1 - D)/\sigma^2$ we have

$$\mathbb{Z} + \mathbb{Z}\left(\frac{\sigma - 1 + \sqrt{D}}{\sigma}\right) \subseteq \mathfrak{O}_F.$$

It remains to prove the reverse inclusion.

Let $\alpha \in \mathfrak{O}_F \subseteq F$. Then $\alpha = a + b\sqrt{D}$ where $a, b \in \mathbb{Q}$. We may assume that $b \neq 0$, since otherwise we are done, given that

$$\mathbb{Z} \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{\sigma - 1 + \sqrt{D}}{\sigma}\right).$$

Since $\mathfrak{O}_F$ is a ring, then $\alpha' = (a - b\sqrt{D})$, $\alpha + \alpha' = 2a$, and $\alpha\alpha' = a^2 - Db^2$ are all in $\mathfrak{O}_F$. However, the latter two elements are also in $\mathbb{Q}$, and by Corollary 1.12 on page 37, $\mathfrak{O}_F \cap \mathbb{Q} = \mathbb{Z}$, so

$$2a, a^2 - Db^2 \in \mathbb{Z}. \tag{1.24}$$

Case 1.1 $a \notin \mathbb{Z}$.

We must have $a = (2c + 1)/2$ for some $c \in \mathbb{Z}$. Therefore, by (1.24), $4(a^2 - Db^2) \in \mathbb{Z}$, which implies $4Db^2 \in \mathbb{Z}$. However, since D is squarefree, then $2b \in \mathbb{Z}$. (To see this, observe that if $2b = g/f$ where $g, f \in \mathbb{Z}$ with $\gcd(f, g) = 1$, and $f > 1$ is odd, then $4Dg^2 = f^2 h$ for some

$h \in \mathbb{Z}$. Thus, since $\gcd(4g, f) = 1$, $f^2 \bigm| D$ contracting its squarefreeness.) If $b \in \mathbb{Z}$ then, by (1.24), $a \in \mathbb{Z}$, contradicting that $a = (2c+1)/2$. Therefore, $b = (2k+1)/2$ for some $k \in \mathbb{Z}$. Thus,

$$a^2 - Db^2 = \frac{(2c+1)^2}{4} - \frac{D(2k+1)^2}{4} = c^2 + c - (k^2+k)D + \frac{1-D}{4},$$

which implies $(D-1)/4 = c^2 + c - (k^2+k)D - a^2 + Db^2 \in \mathbb{Z}$, hence, $D \equiv 1 \pmod 4$ and:

$$\alpha = \frac{2c+1}{2} + \frac{(2k+1)\sqrt{D}}{2} = (c-k) + \frac{(2k+1)(1+\sqrt{D})}{2}$$

$$\in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{D}}{2}\right) = \mathbb{Z} + \mathbb{Z}\left(\frac{\sigma - 1 + \sqrt{D}}{\sigma}\right).$$

Case 1.2 *$a \in \mathbb{Z}$.*

In this instance, by (1.24), $Db^2 \in \mathbb{Z}$, and arguing as above, since D is squarefree, $b \in \mathbb{Z}$. Hence,

$$\alpha = a + b\sqrt{D} \in \mathbb{Z} + \mathbb{Z}\sqrt{D} = \mathbb{Z} + \mathbb{Z}\left(\frac{\sigma - 1 + \sqrt{D}}{\sigma}\right),$$

which completes the reverse inclusion that secures the theorem. □

Definition 1.33 — Quadratic Field Discriminants
If D is the unique squarefree integer such that $F = \mathbb{Q}(\sqrt{D})$ is a quadratic field, then the discriminant of F is given by

$$\Delta_F = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{if } D \not\equiv 1 \pmod 4. \end{cases}$$

Remark 1.22 Definition 1.33 follows from the fact that the minimal polynomial of F is $x^2 - x + (1-D)/4$ if $D \equiv 1 \pmod 4$, and is $x^2 - D$ if $D \not\equiv 1 \pmod 4$. In §2.3, we will study general number field discriminants and prove the fact, implicit in Definition 1.33, namely$\Delta\ _F \equiv 0, 1 \pmod 4$, holds for any number field F. This is known as *Stickelberger's Theorem*—see Biography 1.4 on page 54 and Theorem 2.10 on page 77.

Example 1.29 Suppose we have an irreducible quadratic polynomial

$$f(x) = ax^2 + bx + c \in \mathbb{Q}[x].$$

Then $\Delta =\ b^2 - 4ac$ is the discriminant not only of $f(x)$, but also the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. By the quadratic formula, the roots of $f(x)$ are given, since $a \neq 0$, by

$$\alpha = \frac{-b + \sqrt{\Delta}}{2a}, \text{ and } \alpha' = \frac{-b - \sqrt{\Delta}}{2a},$$

where α' is called the *algebraic conjugate* of α. By Exercise 1.1 on page 6, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$, which we know is a simplest nontrivial number field, a quadratic field over $\mathbb{Q}$.

The reader will note that some easily verified properties of conjugates are given as follows.

(a) $(\alpha\beta)' = \alpha'\beta'$.

(b) $(\alpha \pm \beta)' = \alpha' \pm \beta'$.

(c) $(\alpha/\beta)' = \alpha'/\beta'$, where $\alpha/\beta = \delta \in \mathbb{Q}(\sqrt{\Delta})$.

Remark 1.23 If $D < 0$ in Theorem 1.28 on page 45, F is called a *complex* (or *imaginary*) quadratic field, and if $D > 0$, F is called a *real* quadratic field. Also, the group of units in a quadratic field forms an abelian group. For real quadratic fields we will learn about this group later, since it is more complicated than the complex case which we now tackle. The reader will recall the notion of groups and notation for a cyclic group, $\langle g\rangle$, generated by an element g—see Definition A.3 on page 320.

Theorem 1.29 — Units in Complex Quadratic Fields
If $F = \mathbb{Q}(\sqrt{D})$ is a complex quadratic field, then

$$\mathfrak{U}_F = \mathfrak{U}_{\mathfrak{O}_F} = \begin{cases} \langle\zeta_6\rangle = \left\langle\frac{1+\sqrt{-3}}{2}\right\rangle & \text{if } D = -3, \\ \langle\zeta_4\rangle = \langle\sqrt{-1}\rangle & \text{if } D = -1, \\ \langle\zeta_2\rangle = \langle -1\rangle & \text{otherwise.} \end{cases}$$

Proof. By Theorem 1.28 we may write $u = a + b\sqrt{D} \in \mathfrak{U}_{\mathfrak{O}_F}$, with $\sigma a, \sigma b \in \mathbb{Z}$ where σ is defined as in the proof of Theorem 1.28. Hence, if $D \not\equiv 1 \pmod 4$, then $a^2 - b^2D = 1$, for some $a, b \in \mathbb{Z}$. If $D < -1$, then $a^2 - b^2D > 1$ for $b \neq 0$. Thus, $b = 0$ for $D \not\equiv 1 \pmod 4$ with $D < -1$. In other words,

$$\mathfrak{U}_{\mathfrak{O}_F} = \langle -1\rangle = \langle\zeta_2\rangle \text{ if } D \equiv 2, 3 \pmod 4 \text{ and } D < -1.$$

Now we assume that $D \equiv 1 \pmod 4$, so $a^2 - Db^2 = 4$ for $a, b \in \mathbb{Z}$. If $D < -4$, then for $b \neq 0$, $a^2 - Db^2 > 4$, a contradiction. Hence, for $D \equiv 1 \pmod 4$ and $D < -4$, $\mathfrak{U}_{\mathfrak{O}_F} = \langle\zeta_2\rangle$. It remains to consider the cases $D = -1, -3$. If $D = -1$, then by Theorem 1.28, $\mathfrak{O}_F = \mathbb{Z}+\mathbb{Z}[i]$, and $a+bi$ is a unit in $\mathfrak{O}_F$ if and only if $a^2+b^2 = 1$. The solutions are $(a, b) \in \{(0\pm 1), (\pm 1, 0)\}$. In other words,

$$\mathfrak{U}_{\mathbb{Q}[i]} = \{\pm 1, \pm i\}.$$

If $D = -3$, then $a^2 + 3b^2 = 4$, so either $a = b = 1$, or $b = 0$ and $a = 2$. Hence, the units are ± 1, $(1 \pm \sqrt{-3})/2$, and $(-1 \pm \sqrt{-3})/2$. However, $1 = \zeta_6^6$ and we have: $-1 = \zeta_6^3$,

$$(1 + \sqrt{-3})/2 = \zeta_6,$$

$$(1 - \sqrt{-3})/2 = \zeta_6^5,$$

$$(-1 + \sqrt{-3})/2 = \zeta_6^2,$$

and

$$(-1 - \sqrt{-3})/2 = \zeta_6^4.$$

Hence,

$$\mathfrak{U}_{\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}} = \langle\zeta_6\rangle,$$

as required. □

Now we look at multiplication of ideals in quadratic fields. If the reader is in need of a reminder about the basics involved in modules and their transition to ideals in the rings of integers in quadratic fields, then see Exercises 1.55–1.58. In any case, see Exercise 1.62 on page 54.

Multiplication Formulas for Ideals in Quadratic Fields

Suppose that

$$F = \mathbb{Q}(\sqrt{D})$$

is a quadratic number field, and $\mathfrak{O}_F$ is its ring of integers–see Theorem 1.28 on page 45. LetΔ_F be the field discriminant given in Definition 1.33 on page 46, and for $j = 1, 2$ with $a_j \in \mathbb{N}, b_j \in \mathbb{Z}$, let

$$I_j = (a_j, (b_j + \sqrt{\Delta_F})/2),$$

be $\mathfrak{O}_F$-ideals. Then

$$I_1 I_2 = (g)\left(a_3, \frac{b_3 + \sqrt{\Delta_F}}{2}\right),$$

where

$$a_3 = \frac{a_1 a_2}{g^2},$$

$$g = \gcd\left(a_1, a_2, \frac{b_1 + b_2}{2}\right),$$

and

$$b_3 \equiv \frac{1}{g}\left(\delta a_2 b_1 + \mu a_1 b_2 + \frac{\nu}{2}(b_1 b_2 + \Delta_F)\right) \pmod{2a_3},$$

where δ, μ, and ν are determined by

$$\delta a_2 + \mu a_1 + \frac{\nu}{2}(b_1 + b_2) = g.$$

Note the above formulas are intended for our context, namely the ring of integers of a quadratic field $\mathfrak{O}_F$, called the *maximal order*. In an order contained in $\mathfrak{O}_F$ that is not maximal, the above does not work unless we restrict to *invertible* ideals. For the details on, and background for, orders in general, see either [49, §1.5] or [50, §3.5]. Also, see Definition 1.25 on page 27 and Exercise 1.43 on page 33.

Example 1.30 Consider$\Delta_F = 40$, with

$$I_1 = (3, 1 + \sqrt{10}) \text{ and } I_2 = (3, -1 + \sqrt{10}),$$

so in the notation of the above description of formulas for multiplication, we have

$$a_1 = a_2 = 3, b_1 = 2 = -b_2, g = 3, \delta = 0 = \nu, \mu = 1, b_3 = 1 \text{ , and } a_3 = 1,$$

so

$$I_1 I_2 = (3, 1 + \sqrt{10})(3, -1 + \sqrt{10}) = (3). \tag{1.25}$$

Hence, the product of I_1 and I_2 is the principal ideal (3) in $\mathbb{Z}[\sqrt{10}] = \mathfrak{O}_F$, and by Theorem 1.8 on page 16, (3) is not a prime ideal in $\mathfrak{O}_F$ since (3) divides $I_1 I_2$ but does not divide either factor. To see this, note that if

$$(3) \mid (3, \pm 1 + \sqrt{10}),$$

then by Lemma 1.1 on page 17,

$$(3, \pm 1 + \sqrt{10}) \subseteq (3),$$

which is impossible since it is easy to show that $\pm 1+\sqrt{10} \notin (3)$. Moreover, by Exercise 1.61 on page 54, I_1 and I_2 *are* prime $\mathfrak{O}_F$-deals.

Example 1.30 motivates a study of prime decomposition of ideals in quadratic fields. For instance, (1.25) is the decomposition of the ideal (3) in $\mathbb{Z}[\sqrt{10}] = \mathfrak{O}_F$ into the product of the two prime ideals I_1 and I_2. In what follows, we have a complete description. The notation (D/p) in the following denotes the Legendre symbol—see Definition A.23 on page 342. Also, the symbol $N(\mathcal{P})$ will denote the norm of a quadratic ideal as defined in Exercise 1.58 on page 54.

Theorem 1.30 — Prime Decomposition in Quadratic Fields
If $\mathfrak{O}_F$ is the ring of integers of a quadratic field $F = \mathbb{Q}(\sqrt{D})$, and $p \in \mathbb{Z}$ is prime, then the following holds.

$$(p) = p\mathfrak{O}_F = \begin{cases} \mathcal{P}_1\mathcal{P}_2 & \text{if } p > 2, (D/p) = 1, \text{ or } p = 2, D \equiv 1 \pmod 8, \\ & \text{where } \mathcal{P}_j, \text{ are distinct prime } \mathfrak{O}_F\text{-ideals for } j = 1, 2 \\ & \text{and } N(\mathcal{P}_j) = p, \\ \mathcal{P} & \text{if } p > 2, (D/p) = -1, \text{ or } p = 2, D \equiv 5 \pmod 8, \\ & \text{where } \mathcal{P} \text{ is a prime } \mathfrak{O}_F\text{-ideal with } N(\mathcal{P}) = p^2, \\ \mathcal{P}^2 & \text{if } p > 2, p \mid D, \text{ or } p = 2, D \equiv 2, 3 \pmod 4), \\ & \text{where } \mathcal{P} \text{ is a prime } \mathfrak{O}_F\text{-ideal with } N(\mathcal{P}) = p. \end{cases}$$

Proof. For the sake of simplicity of elucidation in the following Cases 1.3–1.5, we present only the instance where $\mathfrak{O}_F = \mathbb{Z}[\sqrt{D}]$ since the proof for $\mathfrak{O}_F = \mathbb{Z}[(1 + \sqrt{D})/2]$ is similar.

Case 1.3 $(D/p) = 1$ for $p > 2$.

The Legendre symbol equality tells us that there exists a $b \in \mathbb{Z}$ such that

$$b^2 \equiv D \pmod p.$$

Also, since $p \nmid D$, then $p \nmid b$. Let

$$\mathcal{P}_1 = (p, b + \sqrt{D}) \text{ and } \mathcal{P}_2 = (p, -b + \sqrt{D}).$$

If $\mathcal{P}_1 = \mathcal{P}_2$, then

$$2b = b + \sqrt{D} - (-b + \sqrt{D}) \in \mathcal{P}_1,$$

so $p \mid 2b$ by the minimality of p as demonstrated in Exercises 1.56–1.58, namely

$$2b \in \mathcal{P}_1 \cap \mathbb{Z} = (p).$$

Thus, $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct $\mathfrak{O}_F$-ideals. By the multiplication formulas given on page 48, we have, in the notation of those formulas, $a_3 = 1$ and $g = p$, so

$$\mathcal{P}_1\mathcal{P}_2 = (p).$$

Case 1.4 $(D/p) = -1$ for $p > 2$.

Let $\alpha\beta \in (p)$, where

$$\alpha = a_1 + b_1\sqrt{D}, \beta = a_2 + b_2\sqrt{D} \in \mathbb{Z}[\sqrt{D}].$$

Suppose that $\beta \notin (p)$. We have

$$\alpha\beta = a_1a_2 + b_1b_2D + (a_2b_1 + a_1b_2)\sqrt{D} = p(x + y\sqrt{D}),$$

for some $x, y \in \mathbb{Z}$. Therefore,

$$a_1a_2 + b_1b_2D = px, \tag{1.26}$$

and

$$a_2b_1 + a_1b_2 = py. \tag{1.27}$$

If $b_1 = 0$, then by (1.26), $p \mid a_1a_2$. If $p \mid a_1$, then $\alpha = a_1 \in (p)$, so by Definition 1.14 on page 15, (p) is an $\mathfrak{O}_F$-prime ideal. If $p \mid a_2$, then $p \nmid b_2$ since $\beta \notin (p)$, so by (1.27) $p \mid a_1$ and we again have that $\alpha \in (p)$. Hence, we may assume that $b_1 \neq 0$. Similarly, we may assume that $a_1 \neq 0$.

Multiplying (1.27) by a_1 and subtracting b_1 times (1.26), we get

$$b_2(a_1^2 - b_1^2D) = p(a_1y - b_1x).$$

If $p \mid (a_1^2 - b_1^2D)$, then there exists a $z \in \mathbb{Z}$ such that $a_1^2 - b_1^2D = pz$. Therefore,

$$-1 = \left(\frac{D}{p}\right) = \left(\frac{b_1^2D}{p}\right) = \left(\frac{a_1^2 - pz}{p}\right) = \left(\frac{a_1^2}{p}\right) = 1,$$

a contradiction. Hence, $p \mid b_2$. By (1.27), this means that $p \mid a_2b_1$. If $p \mid a_2$, then

$$p \mid (a_2 + b_2\sqrt{D}), \text{ so } \beta \in (p),$$

a contradiction to our initial assumption. Thus, $p \mid b_1$, so

$$p \mid (a_1 + b_1\sqrt{D}), \text{ which means that } \alpha \in (p).$$

Case 1.5 $p > 2$ and $p \mid D$.

Let $\mathcal{P} = (p, \sqrt{D})$. Then by the multiplication formulas on page 48, with $a_3 = 1$ and $g = p$ in the notation there, $\mathcal{P}^2 = (p)$. This completes Case 1.5.

It remains to consider the three cases for $p = 2$.

Case 1.6 $p = 2$ and $D \equiv 1 \pmod 8$.

Let

$$\mathcal{P} = \left(2, (1 + \sqrt{D})/2\right) \text{ and } \mathcal{P}_2 = \left(2, (-1 + \sqrt{D})/2\right).$$

Then by the multiplication formulas as used above with $a_3 = 1$ and $g = 2$, we have

$$\mathcal{P}_1\mathcal{P}_2 = (2).$$

If $\mathcal{P}_1 = \mathcal{P}_2$, then

$$(1 + \sqrt{D})/2 + (-1 + \sqrt{D})/2 = \sqrt{D} \in \mathcal{P}_1$$

which is not possible. Thus, $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct. This is Case 1.6.

Case 1.7 $p = 2$ and $D \equiv 5 \pmod 8$.

Let $\alpha\beta \in (2)$, where

$$\alpha = (a_1 + b_1\sqrt{D})/2, \beta = (a_2 + b_2\sqrt{D})/2 \in \mathbb{Z}[(1+\sqrt{D})/2],$$

with a_j and b_j of the same parity for $j = 1, 2$. Suppose that $\beta \notin (2)$. We have

$$\alpha\beta = \frac{a_1a_2 + b_1b_2D + (a_2b_1 + a_1b_2)\sqrt{D}}{4} = 2\left(\frac{x + y\sqrt{D}}{2}\right) = x + y\sqrt{D},$$

where $x, y \in \mathbb{Z}$ are of the same parity. Thus,

$$a_1a_2 + b_1b_2D = 4x, \tag{1.28}$$

and

$$a_2b_1 + a_1b_2 = 4y. \tag{1.29}$$

Multiplying (1.29) by a_1 and subtracting b_1 times (1.28), we get

$$b_2(a_1^2 - b_1^2D) = 4(ya_1 - xb_1).$$

If $a_1^2 - b_1^2D$ is even, then either a_1 and b_1 are both odd or both even. In the former case,

$$1 \equiv a_1^2 \equiv b_1^2D \equiv 5 \pmod 8,$$

a contradiction, so they are both even. Hence,

$$\alpha = 2\left(\frac{a_1/2 + (b_1/2)\sqrt{D}}{2}\right) \in (2),$$

so (2) is a prime $\mathfrak{O}_F$-ideal by Definition 1.14. If b_2 is even, then by (1.29), $2 \mid a_2b_1$. If $2 \mid a_2$, then

$$\beta = 2\left(\frac{a_2/2 + (b_2/2)\sqrt{D}}{2}\right) \in (2),$$

contradicting our initial assumption. Hence, b_1 is even and so a_1 is even since they must be of the same parity. As above, this implies that $\alpha \in (2)$. Thus, (2) is prime. This completes Case 1.7.

Case 1.8 $p = 2$ and $D \equiv 2 \pmod 4$.

Let $\mathcal{P} = (2, \sqrt{D})$, which is an $\mathfrak{O}_F$-ideal by Exercise 1.61 on page 54. Moreover, $\mathcal{P}^2 = (2)$, by the multiplication formulas on page 48 with $a_3 = 1$ and $g = 2$.

Case 1.9 $p = 2$ and $D \equiv 3 \pmod 4$.

Let $\mathcal{P} = (2, 1 + \sqrt{D})$, which is an $\mathfrak{O}_F$-ideal by Exercise 1.61. Moreover, as in Case 1.8,

$$\mathcal{P}^2 = (2).$$

This completes all cases. □

Remark 1.24 Although we have not developed the full decomposition theory for ideals in general number fields, we will be able to talk about decomposition of ideals in quadratic fields. The following terminology will be suited to the more general case—see §5.1—so we introduce it here. Suppose that $F = \mathbb{Q}(\sqrt{D})$ is a quadratic number field,Δ_F is given as in Definition 1.33 on page 46, and (Δ_F/p) denotes the Kronecker symbol—see Definition A.25 on page 343. If $p \in \mathbb{Z}$ is a prime, then

$$(p) \text{ is said to } \textit{split} \text{ in } F \text{ if and only if } \left(\frac{\Delta_F}{p}\right) = 1,$$

$$(p) \text{ is said to } \textit{ramify} \text{ in } F \text{ if and only if } \left(\frac{\Delta_F}{p}\right) = 0,$$

and

$$(p) \text{ is said to be } \textit{inert} \text{ in } F \text{ if and only if } \left(\frac{\Delta_F}{p}\right) = -1.$$

Note, as well, that from the proof of Theorem 1.30, when $(p) = \mathcal{P}_1\mathcal{P}_2$, namely when (p) splits, then $\mathcal{P}_2$ is the *conjugate* of $\mathcal{P}_1$. This means that if $\mathcal{P}_1 = (p, b+\sqrt{D})$ then $\mathcal{P}_2 = (p, -b+\sqrt{D})$.

Example 1.31 In Example 1.30 on page 48, with$\Delta_F = 40$, we saw that

$$(3) = I_1I_2 = (3, 1+\sqrt{10})(3, -1+\sqrt{10}),$$

where

$$\left(\frac{\Delta_F}{3}\right) = \left(\frac{40}{3}\right) = 1,$$

so (3) splits in $\mathbb{Q}(\sqrt{10})$ into the two prime $\mathbb{Z}[\sqrt{10}]$-ideals I_1 and I_2.

In Examples 1.19 on page 15 and 1.20 on page 16, we saw that (2) is not a prime ideal in $\mathbb{Z}[i]$ and that (3) is a prime $\mathbb{Z}[i]$-ideal. Since $(2) = (1+i)^2$, where

$$\mathcal{P} = (2, 1+i) = (1+i) = (2, 1-i) = (1-i)$$

is a prime $\mathbb{Z}[i]$-ideal, then (2) is ramified in $F = \mathbb{Q}(i)$, where

$$\left(\frac{\Delta_F}{2}\right) = \left(\frac{-4}{2}\right) = 0.$$

Also, (3) is a prime ideal and we see that

$$\left(\frac{\Delta_F}{3}\right) = \left(\frac{-4}{3}\right) = -1,$$

so (3) is inert in F.

The following illustration shows that the converse of Lemma 1.1 on page 17 does not hold in general and that the multiplication formulas, on page 48, do not necessarily hold if we do not have the ring of integers of a quadratic field in which to work.

Example 1.32 If $R = \mathbb{Z}[\sqrt{5}]$, then $I = (2, 1+\sqrt{5})$ is an R-ideal by Exercise 1.57, and clearly $(2) = (2, 2\sqrt{5}) \subseteq I$. If $I \mid (2)$, then there exists an R-ideal J such that $(2) = IJ$. Thus, J has a representation $J = (a, b+c\sqrt{D})$ with $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$, $0 \le b < a$, such that $c \mid a$, $c \mid b$, and $ac \mid (b^2 - c^2D)$. Moreover, $J \mid (2)$, so by Lemma 1.1, $(2) \subseteq J$, so there exist

$x, y \in \mathbb{Z}$ such that $2 = ax + (b + c\sqrt{D})y$. Therefore, $y = 0$ and $a \mid 2$. If $a = 1$, then $I = (2)$, which means that $1 + \sqrt{5} \in (2)$, a contradiction, so $a = 2$. If $b = 1$, then $c = 1$, so

$$I^2 = (2). \tag{1.30}$$

However, by considering the multiplication of basis elements for I we see that

$$I^2 = (4, 2(1 + \sqrt{5}), 6 + 2\sqrt{5}) = (4, 2(1 + \sqrt{5})),$$

where the last equality follows since $6 + 2\sqrt{5}$ is a linear combination of the other basis elements so is redundant. Thus,

$$I^2 = (4, 2(1 + \sqrt{5})) = (2)(2, 1 + \sqrt{5}) = (2)I,$$

and combining this with (1.30), we get $(2) = (2)I$, which implies $2(1 + \sqrt{5}) \in (2)$, again a contradiction. We have shown both that although $(2) \subset I$, I does not divide (2), and that the multiplication formulas for ideals in R fail to hold. Note, that R is not the ring of integers of a quadratic field by Theorem 1.28 on page 45. Indeed, by Corollary 1.7 on page 27, R is not a Dedekind domain. For instance, (2) is a prime R-ideal but, by the above, is not maximal, contradicting part (B) of Definition 1.23 on page 25. (*R is what is known as an* order *in $\mathfrak{O}_F = \mathbb{Z}[(1 + \sqrt{5})/2]$ for $F = \mathbb{Q}(\sqrt{5})$ and I is an example of an ideal in R which is not* invertible *in R—see* [49, Chapter 1, pp. 23–30]. *As we saw in Theorem 1.16 on page 27, all integral ideals in a Dedekind domain are invertible. Thus, the multiplication formulas work in $\mathfrak{O}_F$, but not in arbitrary orders where invertibility is not guaranteed.*)

Exercises

1.55. Suppose that G is an additive abelian group, and that R is a commutative ring with identity 1_R which satisfy each of the following axioms:

(a) For each $r \in R$ and $g, h \in G$, $r(g + h) = (rg) + (rh)$.

(b) For each $r, s \in R$ and $g \in G$, $(r + s)g = (rg) + (sg)$.

(c) For each $r, s \in R$ and $g \in G$, $r(sg) = (rs)g$.

(d) For each $g \in G$, $1_R \cdot g = g$.

Then G is a (two-sided) *module* over R, or for our purposes, simply an R-module. Prove that (in general) being a $\mathbb{Z}$-module is equivalent to being an additive abelian group.

1.56. Let $R = \mathbb{Z}[\omega_D]$, $D \in \mathbb{Z}$ not a perfect square, and $\omega_D = (\sigma - 1 + \sqrt{D})/\sigma$, with $\sigma = 1$ if $D \not\equiv 1 \pmod 4$ and $\sigma = 2$ otherwise—see Application 1.2 on page 3. Then every $\mathbb{Z}$-submodule of R has a representation in the form

$$I = [a, b + c\omega_D]$$

where $a, c \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $0 \le b < a$. Moreover, a is the smallest natural number in I and c is the smallest natural number such that $b + c\omega_D \in I$ for any $b \in \mathbb{Z}$. (Note that when $c = 1$, I is called *primitive.*)

1.57. With reference to Exercise 1.56, prove that $I = (a, b + c\omega_D)$ is an R-ideal if and only if $c \mid a$, $c \mid b$, and

$$(\sigma b + c(\sigma - 1))^2 \equiv c^2 D \pmod{\sigma^2 ac}. \tag{1.31}$$

(Note that we use the square brackets for $\mathbb{Z}$-modules and the round brackets for ideals.)

1.58. With reference to Exercise 1.56, prove that the $\mathbb{Z}$-module $[a, b + c\omega_D]$ for $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$, is an R-ideal $(a, b + c\omega_D)$ if and only if $c \mid a$, $c \mid b$, and (1.31) is satisfied. (Here a is the smallest natural number in I, called the *norm* of I, denoted by $N(I)$.)

1.59. Let $[\alpha,\beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ and $[\gamma,\delta] = \gamma\mathbb{Z} + \delta\mathbb{Z}$ be two $\mathbb{Z}$-modules, with $\alpha, \beta, \gamma, \delta \in R$, where R is given in Exercise 1.56. Prove that $[\alpha,\beta] = [\gamma,\delta]$ if and only if

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = X \begin{pmatrix} \gamma \\ \delta \end{pmatrix},$$

where $X \in \mathrm{GL}(2, \mathbb{Z})$, which is the *general linear group* of 2×2-matrices with entries from $\mathbb{Z}$, namely, those 2×2-matrices A such that $\det(A) = \pm 1$, also called *unimodular* matrices. (*Note that, in general,* $\mathrm{GL}(n, \mathbb{Z})$ *is the general linear group of* $n \times n$ *matrices with entries from* $\mathbb{Z}$.)

1.60. With reference to Exercise 1.56, prove that if $\alpha \in R$, and $I = (a,\alpha)$ is an R-ideal, then $I = (a, na \pm \alpha)$ for any $n \in \mathbb{Z}$.

1.61. Let F be a quadratic number field and let $\mathcal{P} = (p, (b + \sqrt{\Delta_F})/2)$ be an $\mathfrak{O}_F$-ideal where $p \in \mathbb{N}$ is prime. Prove that $\mathcal{P}$ is a prime $\mathfrak{O}_F$-ideal.

1.62. Verify the multiplication formulas on page 48.

Biography 1.4 Ludwig Stickelberger (1850–1936) was born on May 18, 1850 in the canton of Schaffenhausen, Switzerland as the son of a pastor. In 1867 he graduated from a gymnasium,[a] from which he went to study at the University of Heidelberg. Later he went to the University of Berlin to study under Karl Weierstrass (1815–1897), achieving his doctorate in 1874. His thesis topic was on transformations of quadratic forms to a diagonal form. Also, in 1874, he received his Habilitation from Polytechnicum in Zurich (now ETH Zurich)—see Footnote 1.1 on page 23. In 1879, he was appointed extraordinary professor in the Albert Ludwigs University of Freiburg, and was promoted to full professor in 1919. In 1924 he returned to Basel. Although he had married in 1895, both his wife and son died in 1918. He died on April 11, 1936, and was buried beside his wife and son in Freiburg.

His publication output was at best modest, but his contributions may be characterized as important contributions to linear algebra, and algebraic number theory, including the theorem that bears his name—see Remark 1.22 on page 46. He coauthored four published papers with Frobenius, three of them on elliptic functions. Stickelberger is best known for two papers. The first, *Verallgemeinerung der Kreisteilung*, generalizes results of Jacobi, Cauchy, and Kummer on Gauss and Jacobi sums. He used these results to find *annihilators of class groups* of abelian extensions of $\mathbb{Q}$. The other, *Über eine neue Eigenschaft der Diskriminante*, shows that the Legendre symbol $(\frac{\Delta_F}{p}) = (-1)^{n-g}$, where the number field F has degree n over $\mathbb{Q}$, and g is the number of prime ideals in $\mathfrak{O}_F$ above p. The latter result implies the quadratic reciprocity law. The results in both papers have been generalized over the years.

[a] The *Gymnasium* in the German education system, is a form of secondary school with a pronounced emphasis on academic achievement. This is comparable to the British former grammar school system or with prep schools in the United States.

Chapter 2

Field Extensions

Good old Watson! You are the one fixed point in a changing age.
spoken by **Sherlock Holmes** *in* **His Last Bow (1917)**, *title story.*
Sir Arthur Conan Doyle (1859–1930)
Scottish-born writer of detective fiction

In this chapter we explore in greater detail the notion of an algebraic number field introduced in Definition 1.29 on page 35, via generalizations thereof, which we develop in §2.1. In particular, this is a foundation for Galois theory, and a generalization of prime decomposition motivated by our coverage of the quadratic case in §1.7, which we generalize to arbitrary number fields in §5.1.

2.1 Automorphisms, Fixed Points, and Galois Groups

Given a number field F, it is possible to define an *embedding* as a ring monomorphism θ of F into $\mathbb{C}$—see Definition A.10 on page 327, and the surrounding discussion, for background. Also, the reader should solve Exercises 2.1–2.6 on pages 62–63 as a precursor, motivator, and adjunct material to the following.

Definition 2.1 — Fixed Points and Isomorphisms

Let $K \subseteq K_1$ be two fields and let θ be an embedding of K into K_1. Then $\alpha \in K$ is called a *fixed point under* θ if $\theta(\alpha) = \alpha$.

Remark 2.1 The name "fixed-point" is appropriate since, in the case where $K = K_1$, θ is an automorphism, so $\theta(\alpha) = \alpha = \theta_1(\alpha)$, where θ_1 is the identity automorphism of K, namely, $\theta_1(\beta) = \beta$ for all $\beta \in K$. The set of all fixed points has a special designation. The reader should be familiar with the material surrounding Remark A.4 on page 327 for the following.

Lemma 2.1 — Fixed Fields

If K is any field, then

$$F = \{\beta \in K : \theta(\beta) = \beta \text{ for all } \theta \in \operatorname{Aut}(K)\}$$

is a field, called the *fixed field of* $\operatorname{Aut}(K)$.

Proof. We have for any automorphisms θ,τ of K, and any β,$\gamma \in F$,

$$\theta(\beta \pm \gamma) = \theta(\beta) \pm \theta(\gamma) = \tau(\beta) \pm \tau(\gamma) = \tau(\beta \pm \gamma).$$

Also,

$$\theta(\beta\gamma) = \theta(\beta)\theta(\gamma) = \tau(\beta)\tau(\gamma) = \tau(\beta\gamma).$$

Since $\theta(\beta) = \tau(\beta)$, then

$$\theta(\beta)^{-1} = \tau(\beta)^{-1} = \tau(\beta^{-1}) = \theta(\beta^{-1}).$$

Hence, sums, products, and inverses of fixed points are fixed points, so F is a subfield of K. □

Lemma 2.2 Distinct embeddings of a field K into a field K_1 are independent. In other words, if θ_j are distinct embeddings of K into K_1, and $\beta_j \in K$ for $j = 1, 2, \ldots, n$, such that

$$\sum_{j=1}^{n} \theta_j(\alpha)\beta_j = 0 \text{ for all } \alpha \in K$$

then $\beta_1 = \beta_2 = \cdots = \beta_n = 0$.

Proof. We use induction on n. If $n = 1$, the result is clear, since θ_1 cannot be the zero map. Assume that the result holds for all natural numbers $k < n$. If

$$\sum_{j=1}^{n} \theta_j(\alpha)\beta_j = 0$$

for all $\alpha \in K$, and $\beta_j \neq 0$ for *some* j, then $\beta_j \neq 0$ for *all* $j = 1, 2, \ldots, n$, by the induction hypothesis. We may multiply through by β_n^{-1} to get

$$\theta_n(\alpha) + \sum_{j=1}^{n-1} \theta_j(\alpha)\beta_j\beta_n^{-1} = 0. \tag{2.1}$$

Since the θ_j are distinct, there exists some $\gamma \in K$ such that $\theta_1(\gamma) \neq \theta_n(\gamma)$. Now multiply (2.1) through by $\theta_n(\gamma)^{-1}$ to get

$$\theta_n(\alpha)\theta_n(\gamma)^{-1} + \sum_{j=1}^{n-1} \theta_j(\alpha)\theta_n(\gamma)^{-1}\beta_j\beta_n^{-1} = 0. \tag{2.2}$$

Since (2.2) holds for all $\alpha \in K$, we may replace α by $\gamma\alpha$ therein to get

$$\theta_n(\alpha) + \sum_{j=1}^{n-1} \theta_j(\alpha\gamma)\theta_n(\gamma)^{-1}\beta_n^{-1}\beta_j = 0,$$

so

$$\theta_n(\alpha) + \sum_{j=1}^{n-1} \theta_j(\alpha)\theta_j(\gamma)\theta_n(\gamma)^{-1}\beta_n^{-1}\beta_j = 0. \tag{2.3}$$

Now subtracting (2.3) from (2.1), we get

$$\sum_{j=1}^{n-1} \theta_j(\alpha)\beta_j\beta_n^{-1}(\theta_j(\gamma)\theta_n(\gamma)^{-1} - 1) = 0.$$

However, $\theta_1(\gamma)\theta_n(\gamma)^{-1} - 1 \neq 0$, since $\theta_1(\gamma) \neq \theta_n(\gamma)$. This provides a dependency relation that contradicts the induction hypothesis, so $\beta_j = 0$ for all j, and the result is complete. □

Theorem 2.1 — Degrees Over Fixed Fields

If $\theta_1, \ldots, \theta_n$ are distinct isomorphisms of a field K into a field K_1, and if F is the fixed field of $\{\theta_1, \ldots, \theta_n\}$, then $|K_1 : F| \geq n$.

Proof. If $|K_1 : F| = m < n$, then let $K_1 = F(\alpha_1, \ldots, \alpha_m)$ and consider the system of homogeneous equations for $i = 1, \ldots, m$:

$$\sum_{j=1}^{n} \theta_j(\alpha_i) x_j = 0.$$

Since $m < n$, then by Theorem A.23 on page 338, there must exist solutions $x_j \in K$, not all zero, to these equations for $j = 1, \ldots, n$. Also, for any $\gamma \in K_1$, there exist $\beta_j \in F$ such that

$$\sum_{j=1}^{m} \beta_j \alpha_j = \gamma.$$

Now, for each $i = 1, \ldots, m$, we have

$$\theta_1(\beta_i) \sum_{j=1}^{n} \theta_j(\alpha_i) x_j = 0.$$

Then, since $\beta_i \in F$, we have $\theta_1(\beta_i) = \theta_j(\beta_i)$. Thus,

$$\sum_{j=1}^{n} \theta_j(\beta_i \alpha_i) x_j = 0.$$

Hence,

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} \theta_j(\beta_i \alpha_i) x_j = \sum_{j=1}^{n} \sum_{i=1}^{m} \theta_j(\beta_i \alpha_i) x_j = \sum_{j=1}^{n} \theta_j(\sum_{i=1}^{m} \beta_i \alpha_i) x_j = \sum_{j=1}^{n} \theta_j(\gamma) x_j.$$

We have exhibited a nontrivial dependency relationship between the θ_j, contradicting Lemma 2.2. □

Corollary 2.1 *If $\theta_1, \ldots, \theta_n$ are distinct automorphisms of a field K, and F is the fixed field of* $\mathrm{Aut}(K)$*, then $|K : F| \geq n$.*

In Exercise 2.6 on page 63 we introduce the notion of an F-isomorphism of a number field K. We now generalize this notion.

Definition 2.2 — Fixing Automorphisms

Let K/F be an extension of fields. If θ is an automorphism of K such that $\theta(\alpha) = \alpha$ for all $\alpha \in F$, then θ is said to *fix* F, or to *leave* F *fixed*, and is called an F*-automorphism of* K.

Lemma 2.3 — Groups and Fixing Automorphisms

Let K/F be an extension of fields. The set of all F-automorphisms of K forms a group, denoted by $\mathrm{Aut}_F(K)$.

Proof. Two F-automorphisms θ_1, θ_2 of a field K may be composed by defining

$$\theta_1\theta_2(\beta) = \theta_1(\theta_2(\beta))$$

for each $\beta \in K$. Then this product is also an automorphism of K. Also, if $\theta(\alpha) = \beta$ for a given F-automorphism θ of K, we define $\theta^{-1}(\beta) = \alpha$ as the mapping that takes β to α, called the inverse of θ, which is also an F-automorphism of K. Thus, for any two F-automorphisms θ_1 and θ_2 of K, $\theta_1\theta_2^{-1}(\beta) = \beta$ for any $\beta \in F$, so $\theta_1\theta_2^{-1}$ is an F-automorphism of K. Thus, the set of all F-automorphisms of K forms a multiplicative abelian group. □

Although it is possible for $\mathrm{Aut}_F(K)$ to be infinite, the situation considered in this text for number fields will always deal with a finite group. Also, in general it is possible for the fixed field of $\mathrm{Aut}_F(K)$ to be bigger than F, as illustrated by the following.

Example 2.1 Let $K = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and $F = \mathbb{Q}$. Then $\mathrm{Aut}_F(K) = \{\theta_1\}$, the identity group consisting of only θ_1 which is the identity automorphism that fixes K pointwise. The reason is that the only possible images of $\sqrt[3]{2}$ are $\zeta_3\sqrt[3]{2} \notin K$ and $\zeta_3^2\sqrt[3]{2} \notin K$, where ζ_3 is a primitive cube root of unity, so both are images in $\mathbb{C} - \mathbb{R}$, since $x^3 - 2 = 0$ has roots $x = \sqrt[3]{2}$, the only real root, as well as $x = \zeta_3\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}^2$, the only complex roots.

The case where F *is* the fixed field of $\mathrm{Aut}_F(K)$ is of particular importance. Thus, we now seek to minimize the bound on the degree given in Theorem 2.1. The following, due to Artin, essentially generalizes Exercise 2.6 on page 63—see Biography 1.2 on page 24.

Theorem 2.2 — Unique Automorphism Groups

Let K/F be an extension of fields and let G be a finite group of automorphisms of K having F as its fixed field. Then

$$|K : F| = |G| = |\mathrm{Aut}_F(K)|,$$

and $G = \mathrm{Aut}_F(K)$.

Proof. Let $G = \{\theta_1, \ldots, \theta_n\}$ with identity automorphism θ_1. If $|K : F| > n$, then there exist $\alpha_j \in K$ for $j = 1, \ldots, n+1$ such that the α_j are linearly independent over F. By Theorem A.23 on page 338, there exists a nontrivial solution for $k = 1, \ldots, n+1$ to the system of equations

$$\sum_{j=1}^{n+1} \theta_k(\alpha_j)x_j = 0, \text{ where } x_j \in K \text{ for } j = 1, \ldots, n+1. \tag{2.4}$$

If there is a solution with all $x_j \in F$, then $\theta_1(\alpha_1) = \alpha_1 = -\sum_{j=2}^{n+1} \theta_k(\alpha_j)x_j$, contradicting the assumed linear independence. Thus, at least one of the values x_j of any given solution cannot be in F. Now select a solution set

$$\{x_j\}_{j=1}^{n+1} = \{\beta_j\}_{j=1}^{n+1}$$

in which there is a maximum possible number of nonzero elements, namely let $m \le n$ be the largest natural number such that

$$\beta_{m+1} = \cdots = \beta_{n+1} = 0$$

and $\beta_r \neq 0$ for any $r \le m$. If $m = 1$, then since $\beta_1\theta_1(\alpha_1) = 0$ and $\theta_1(\alpha_1) = \alpha_1 \neq 0$, then $\beta_1 = 0$, a contradiction to the definition of m. Thus, $m > 1$. Also, without loss of generality, we may select $\beta_m = 1$, since we may multiply through by β_m^{-1} to get another solution. Hence, for $k = 1, \ldots, n$ we have

$$\sum_{j=1}^{m} \theta_k(\alpha_j)\beta_j = \theta_k(\alpha_m) + \sum_{j=1}^{m-1} \theta_k(\alpha_j)\beta_j = 0. \tag{2.5}$$

Without loss of generality, we may assume that $\beta_1 \notin F$. Therefore, there exists θ_ℓ such that

$$\theta_\ell(\beta_1) \neq \beta_1 \text{ for some } \ell = 1, \ldots, n.$$

Applying θ_ℓ to (2.5), we get

$$\theta_\ell\theta_i(\alpha_m) + \sum_{j=1}^{m-1} \theta_\ell\theta_i(\alpha_j)\theta_\ell(\beta_j) = 0,$$

for $i = 1, \ldots, n+1$. Since $\theta_\ell\theta_i = \theta_k$ for some $i = 1, \ldots, n$, this equation becomes

$$\theta_k(\alpha_m) + \sum_{j=1}^{m-1} \theta_k(\alpha_j)\theta_\ell(\beta_j) = 0. \tag{2.6}$$

Subtracting (2.6) from (2.5), we achieve

$$\sum_{j=1}^{m-1} \theta_k(\alpha_j)(\beta_j - \theta_\ell(\beta_j)) = 0.$$

Since $\theta_\ell(\beta_1) \neq \beta_1$, this is a solution to (2.4) having less than m nonzero elements, contradicting the minimality of m. We have shown that $|K : F| \leq n$, and by Theorem 2.1, $|K : F| \geq n$, so we have equality. Also, if there exists a $\theta \in \mathrm{Aut}_F(K)$ such that $\theta \notin G$, then there are $n+1$ distinct automorphisms of K which fix F. Therefore, by Corollary 2.1, $|K : F| \geq n+1$, a contradiction. Thus, $\mathrm{Aut}_F(K) = G$. □

The following encapsulates what is contained in Theorem 2.2—see Biography 2.1 on page 64.

Definition 2.3 —— Galois Groups

The uniquely determined group in Theorem 2.2 is called the *Galois group* of the field extension K/F that is called a *Galois extension*, and $\mathrm{Aut}_F(K)$ is denoted by $\mathrm{Gal}(K/F)$.

The above development is essentially due to Artin. However, we have a parallel development for the number field case for comparison, and will give a broader overview, in Exercises 2.1–2.6 on pages 62–63.

The following links the above with the number field case and shows that the group in Definition 2.3 is the one satisfying the following equivalent conditions. The following also holds in the case where the fields are finite or are any finite extensions of fields of characteristic zero—see Exercises 2.12–2.16 on page 64. The result is a preamble to the fundamental theorem for Galois theory.

Theorem 2.3 — The Galois Group of a Number Field

Let K/F be an extension of number fields. Then the following are equivalent.

(a) The fixed field of $G = \mathrm{Aut}_F(K) = \mathrm{Gal}(K/F)$ is F and $|G| = |K : F|$.

(b) For any $\alpha \in K$, $m_{\alpha,F}(x)$ has all its roots in K.

(c) $K = F(\alpha_1, \alpha_2, \ldots, \alpha_d)$ where α_j are roots of some $f(x) \in F[x]$.

Proof. If (a) holds, then let

$$h(x) = \prod_{\sigma \in G} (x - \sigma(\alpha)) \in K[x].$$

However, the elements of G permute the factors of $h(x)$, so $h(x)$ remains invariant under the action of G. However, since $\sigma = 1_G \in G$, $\alpha - 1_G(\alpha) = 0$ is a factor of $h(\alpha)$, namely α is a root of $h(x)$. Thus, by Theorem 1.23 on page 38, $m_{\alpha,F}(x) \bigm| h(x)$, so all roots of $m_{\alpha,F}(x)$ are in K. Hence, (a) implies (b).

Assume (b) holds. By Exercise 1.51 on page 43, there is an element $\gamma \in K$ such that $K = F(\gamma)$. Since we are assuming that $m_{\gamma,F}(x)$ has all its roots in K, then K is generated by the roots of $m_{\gamma,F}(x)$ since $K = F(\sigma(\gamma))$ for any $\sigma \in G$. We have shown that (b) implies (c).

To complete the logical circle, we show that (c) implies (a). (For the proof of this part, the reader should be quite familiar with Exercise 2.6 on page 63. In particular, be aware of the distinction between the notion of an F-*automorphism* and an F-*isomorphism.* The former implies the latter, but, as Example 2.1 on page 58 shows, in general the latter does not necessarily imply the former.) If σ is an F-isomorphism of K, then $\sigma(\alpha_j) = \alpha_k$ where $j, k \in \{1, 2, \ldots, d\}$, from which it is clear that $\sigma(K) = K$, so σ is an F-*automorphism* of K, namely $\sigma \in \mathrm{Aut}_F(K)$. By Exercise 2.6, the number of F-automorphisms of K is exactly $|K : F| = d$. Suppose that $G = \mathrm{Aut}_F(K)$ fixes $\delta \in K$. Then every element of G is an $F(\delta)$-automorphism of K. By Exercise 2.6 again, the number of $F(\delta)$-automorphisms of K is exactly $|K : F(\delta)|$. Hence, $d \leq |K : F(\delta)|$ which forces $d = |K : F(\delta)|$, namely $\delta \in F$. This shows that F is the fixed field of G, and

$$|G| = |\mathrm{Aut}_F(K)| = |K : F| = |\mathrm{Gal}(K/F)|,$$

which completes the task. □

We conclude this section with the following highlight of Galois theory. See Exercise 2.2 for the definition of a normal extension.

Theorem 2.4 — Fundamental Theorem of Galois Theory

Let K/F be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(K/F)$. If H is a subgroup of G, then denote the fixed field of H by $k(H)$, and if L is an intermediate field in K/F, let $g(L) = \mathrm{Aut}_L(K)$. Then

(a) The mappings $g : L \mapsto g(L)$ from intermediate fields to subgroups of G, and $k : H \mapsto k(H)$ from subgroups of G to (intermediate) fixed fields are inverses of one another. Also,

$$k(H_1) \subseteq k(H_2) \text{ if and only if } g(k(H_1)) = H_1 \supseteq H_2 = g(k(H_2)),$$

namely, they are inclusion reversing. Furthermore,

$$|k(H_2) : k(H_1)| = |H_1 : H_2|.$$

(b) K is Galois over any intermediate field L. Also, L is Galois over F if and only if $g(L) = \mathrm{Aut}_L(K)$ is normal in G. If the latter occurs, then

$$\mathrm{Gal}(L/F) \cong \frac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/L)}.$$

Proof. Let L be an intermediate field between K and F, and let $\alpha \in K$. Then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$, all of whose roots are in K by part (b) of Theorem 2.3. Therefore, all roots of $m_{\alpha,L}(x)$ are in K, so by part (b) of Theorem 2.3 again, K/L is Galois. By part (a) of Theorem 2.3, L is the fixed field of $g(L) = \mathrm{Aut}_L(K)$. In other words, $k(g(L)) = L$. On the other hand, if H is a subgroup of $\mathrm{Gal}(K/F)$, then $H = \mathrm{Gal}(K/k(H))$. In other words, $H = g(k(H))$. We have shown that k and g are bijections and inverses of one another. Lastly, the inclusion reversal is now clear, so we have (a).

Let L be an intermediate field between K and F, and let $\alpha \in L$. Then $m_{\alpha,F}(\beta) = 0$ where $\beta \in K$ if and only if $\beta = \theta(\alpha)$ for some $\theta \in \mathrm{Gal}(K/F)$. By part (b) of Theorem 2.3 one more time, L/F is Galois if and only if $\theta \in \mathrm{Gal}(K/F)$, namely if $\theta(L) \subseteq L$. Now, if $\theta(L) \subseteq L$, $\sigma \in g(L)$ and $\alpha \in L$, then

$$\theta^{-1}\sigma\theta(\alpha) = \theta^{-1}\theta(\alpha) = \alpha,$$

so $\theta^{-1}\sigma\theta \in g(L)$. We have shown that if L/K is Galois, then $g(L)$ is normal in G. Conversely, assume that $g(L)$ is normal in G. If $\alpha \in K$, $\theta \in G$ and $\sigma \in g(L)$, then

$$\sigma\theta(\alpha) = \theta\theta^{-1}\sigma\theta(\alpha) = \theta(\alpha),$$

since $\theta^{-1}\sigma\theta \in g(L)$. Thus, $\theta(\alpha)$ is fixed by $g(L)$ so $\theta(\alpha) \in L$. We have shown that if $g(L)$ is normal in G, then $\theta(L) \subseteq L$. Hence, L/F is Galois.

Finally, we establish the isomorphism given in (b). Let $H = \mathrm{Gal}(L/F)$. Since $\theta(L) \subseteq L$ for all $\theta \in \mathrm{Gal}(K/F)$,

$$\theta|_L \in \mathrm{Aut}_F(L) = \mathrm{Gal}(L/F).$$

Thus, the restriction mapping $\theta \mapsto \theta|_L$ is a homomorphism of G to H with $\ker(\theta|_L) = g(L)$. Since

$$|H| = \frac{|K:F|}{|K:L|} = \frac{|G|}{|g(L)|},$$

then the restriction homomorphism is surjective, so

$$H \cong \frac{G}{g(L)},$$

which completes the proof of the fundamental theorem. □

The following diagram illustrates what Theorem 2.4 asserts.

Diagram 2.1

The mapping g:

Fields Groups

$$\begin{tikzcd}
K \arrow[r] & 1 \\
\cup| & \cap| \\
L \arrow[r] & g(L) \\
\cup| & \cap| \\
M \arrow[r] & g(M) \\
\cup| & \cap| \\
F \arrow[r] & G
\end{tikzcd}$$

The mapping k:

Fields Groups

$$\begin{tikzcd}
k(1) & 1 \arrow[l] \\
\cup| & \cap| \\
k(H) & H \arrow[l] \\
\cup| & \cap| \\
k(J) & J \arrow[l] \\
\cup| & \cap| \\
k(G) & G \arrow[l]
\end{tikzcd}$$

Theorem 2.4 asserts that there is a one-to-one correspondence between the subgroups H of $\mathrm{Gal}(K/F)$ and the intermediate fields L, corresponding elements H and L being such that $L = k(H)$ and $H = g(L)$. This elegant relationship will be used in force in §5.4.

Exercises

2.1. Let α be an algebraic number. Prove that if $F = \mathbb{Q}(\alpha)$ is an algebraic number field of degree d over $\mathbb{Q}$, there exist exactly d embeddings θ_j of F into $\mathbb{C}$ for $j = 1, 2, \ldots, d$. Conclude that $\theta_j(\alpha) = \alpha_j$, for $j = 1, 2, \ldots, d$ are precisely the roots of the minimal polynomial $m_{\alpha,\mathbb{Q}}(x)$ of α over $\mathbb{Q}$.

(*Hint: See Theorem 1.23 on page 38, Theorem 1.24 on page 39, and Application A.1 on page 325.*)

(*The elements $\theta_j(\alpha)$ are called the* conjugates *of α, which is a generalization of the concept for quadratic extensions introduced in Example 1.29 on page 46. Moreover, the fields $\mathbb{Q}(\alpha_j)$ are called the* conjugate fields *of F. Also, α_j for $j = 1, 2, \ldots, d$ are called the* complete set of F-conjugates of α *and $\mathbb{Q}(\alpha_j)$ for such j are called the* conjugate fields of F. *Thus, the F-conjugates of α do not depend on the choice of α such that $F = \mathbb{Q}(\alpha)$. Note that if $\mathbb{Q}(\alpha_j) \subseteq \mathbb{R}$ for all F-conjugates of F, then F is called a* totally real *field and if $\mathbb{Q}(\alpha_j) \subseteq \mathbb{C} - \mathbb{R}$, then F is called* totally complex.)

Exercises 2.2–2.6 all refer to Exercise 2.1 and are intended to develop the notion of embeddings of number fields to complement the topic in this section.

2.2. We define the *field polynomial* of α over F to be

$$f_{\alpha,F}(x) = \prod_{j=1}^{d}(x - \theta_j(\alpha)).$$

Establish each of the following.

(a) Let $\beta \in \mathbb{Q}(\alpha)$ be an algebraic number of degree s over $\mathbb{Q}$. Then $d/s = t \in \mathbb{N}$ and

$$f_{\alpha,F}(x) = (m_{\beta,\mathbb{Q}}(x))^t.$$

Conclude that $\theta_j(\beta)$ for $j = 1, 2, \ldots, s$ are the roots of $m_{\beta,\mathbb{Q}}(x)$, each repeated t times in the factorization of $f(x) \in \mathbb{Q}[x]$.

(b) If $F = \mathbb{Q}(\alpha)$ is a number field of degree d over $\mathbb{Q}$ and there are exactly s distinct conjugate fields $\mathbb{Q}(\alpha_j) = F$, then $d/s = t \in \mathbb{N}$ and each distinct field occurs t times.

(*Hint: To establish $t \in \mathbb{N}$, see* (A.2) *on page 325. For the balance, employ Theorem 1.23 on page 38 and Definition A.15 on page 331.*)

(*When $s = 1$ in part* (b) *above, the field F is said to be* normal over $\mathbb{Q}$. *When we are dealing with a field of characteristic zero or a finite field, then being a Galois extension is tantamount to being a normal extension—see Definition 2.3 on page 59. In the more general case, with which we will not be concerned herein, we refer the reader to* [29], *where one may also find a proof of the last assertion.*)

2.3. Prove that for an algebraic number field F with $\alpha \in \mathfrak{O}_F$, all of the F-conjugates of α are algebraic integers.

2.4. Prove that if α is in a number field F, then all F-conjugates of α are equal if and only if $\alpha \in \mathbb{Q}$.

2.5. Prove that if α is in a number field F, then all the F-conjugates of α are distinct if and only if $F = \mathbb{Q}(\alpha)$.

(*Via Exercise 2.5 and in view of the comments made in Exercise 2.2, we see that when all F-conjugates α_j of α are distinct, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_j)$ for all such j, namely F is Galois over $\mathbb{Q}$. Another way of putting this is that every polynomial $f(x) \in F[x]$ which has a root in F splits completely into linear factors, meaning that F is a* splitting field for f*—see Definition A.17 on page 334.*)

2.6. Let E/F be an extension of number fields and let θ be an embedding of E into $\mathbb{C}$ that fixes F pointwise, namely $\theta(f) = f$ for all $f \in F$. Then θ is called an F-isomorphism of E. If θ is an F-isomorphism of $E = F(\alpha)$, then $\theta(\alpha)$ is called a *conjugate* of α over F. Prove that every embedding of F in $\mathbb{C}$ extends to exactly $|E : F|$ embeddings of E in $\mathbb{C}$. Conclude that there are $|E : F|$ F-isomorphisms of E.

(*Hint: Use induction and employ* (A.2) *on page 325 together with Theorem 1.24 on page 39.*)

(*This exercise deals with one of the classic questions in the theory of field extensions, applied to our number field case. If θ is an isomorphism of a field F and E is a field extension of F, when can θ be extended to an isomorphism of E? Putting it another way, when can we find an isomorphism ϕ of E such that $\phi|_F = \theta$?—see the discussion surrounding the defining notation* (A.5) *on page 327 for a reminder of restriction maps and Theorem A.15 on page 334 for extensions of isomorphisms.*)

2.7. Let α be an algebraic integer and suppose that $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 2$. Prove that

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) \text{ for some squarefree } d \in \mathbb{Z}.$$

2.8. Find the minimal polynomial of

$$\alpha = \sqrt{-2 - 3\sqrt{-5}}$$

over $\mathbb{Q}$ and determine $\mathrm{Gal}(K/\mathbb{Q})$ where $K = \mathbb{Q}(\alpha)$. Conclude that

$$|K : \mathbb{Q}| = 4.$$

2.9. Let $n_1 \neq n_2$ be squarefree integers. Prove that

$$K = \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2}) = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}),$$

and determine $\mathrm{Gal}(K/\mathbb{Q})$.

2.10. For $n_j \in \mathbb{Z}$ be squarefree, distinct, and $n_j \neq 1$ for $j = 1, 2$. Prove that

$$|\mathbb{Q}(\sqrt{n_1} + \sqrt{n_2}) : \mathbb{Q}| = 4.$$

2.11. With reference to Exercise 2.1, suppose that F is a number field with embeddings θ_j such that $\theta_j(F) \subseteq \mathbb{R}$ for $j = 1, 2, \ldots, r_1$. These are called the *real embeddings of F*. The remaining embeddings $\theta_j(F) \subseteq \mathbb{C} - \mathbb{R}$ for $j = 1, 2, \ldots, r_2$, are called the *complex embeddings of F*. Show that $|F : \mathbb{Q}| = r_1 + 2r_2$. In this case $\{r_1, r_2\}$ is called the *signature of F*.

2.12. Prove that the signature, defined in Exercise 2.11, of $\mathbb{Q}(\sqrt[3]{2})$ is $\{r_1, r_2\} = \{1, 1\}$. Show that $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$.

2.13. If F is a field of characteristic p, and $n \in \mathbb{N}$, prove that the map given by $\sigma : F \mapsto F$ defined by $\alpha \mapsto \alpha^{p^n}$ is an $\mathbb{F}_p$ automorphism of F.

2.14. Let $D_1 \subseteq D_2$ be integral domains, $\alpha \in D_2$, and let $f(x) \in D_1[x]$ with $\deg(f) \geq 1$. Establish each of the following.

(a) $(x - \alpha)^2 \mid f(x)$ if and only if $f(\alpha) = 0 = f'(\alpha)$.

(b) If D_1 is a field and $\gcd(f(x), f'(x)) = 1$, then f has no multiple roots in D_2.

(c) If D_1 is a field, $f(x)$ is irreducible in $D_1[x]$, and D_2 contains a root c of $f(x)$, then $f(x)$ has no multiple roots in D_2 if and only if $f'(c) \neq 0$.

(d) If $\deg(f) = n \in \mathbb{N}$, then $f(x)$ has at most n roots in D_2.

2.15. Let F be a finite field with p^n elements. Then F is a splitting field, unique up to isomorphism, of $x^{p^n} - x$ over $\mathbb{F}_p$.

(*Hint: Use Exercises 2.13–2.14.*)

2.16. Prove that Theorem 2.3 on page 59 holds for fields of characteristic zero and for finite fields. Also, show that if K/F is a finite extension of finite fields, then K/F is a Galois extension with $\mathrm{Gal}(K/F)$ being cyclic.

(*Hint: Use Corollary A.10 on page 334 and the discussion surrounding it, as well as Theorem A.16 on page 334 for the first statement. For the second statement, use the first statement in conjunction with Exercises 2.13–2.15,*)

Biography 2.1 Évariste Galois (1811–1832) was born on October 25, 1811 outside Paris in the village of Bourg-la-Reine, where his father was mayor. In 1830, he submitted a paper to the Académie des Sciences. Fourier, who was secretary of the Académie, took the paper home, died shortly thereafter, and the paper was lost. This was not the first misfortune, since in the previous year he had submitted a paper to the Académie through Cauchy, who also lost that paper. Galois again tried to submit a paper to the Académie, this time through Poisson, who rejected the paper as incomprehensible. This paper contained the foundations of what we now call *Galois theory.* Due to his involvement in the revolution of 1830, Galois was imprisoned. After his release, he became involved in a pistol duel, allegedly a politically motivated suicide, and was shot through the intestines. Although he was taken to a hospital, he died the next morning on May 31, 1832, from peritonitis. He was not yet twenty-one. For a detailed explanation of his life and "pointless death" see [62], dedicated to an accounting based on reliable historical documents, rather than the mythologized and inaccurate descriptions often found in the literature.

After his death, Galois' papers made their way ultimately into the hands of Liouville. In September of 1843, Liouville announced to the Académie that he found Galois' work to be correct, concise, and deep. Liouville published Galois' papers in his journal in 1846. Galois' work, relating the solving of equations by radicals to the group of the equation, is of fundamental importance, and may be said to have led to an arithmetical approach to algebra.

2.2 Norms and Traces

But all things must come to dust eventually. No human being, no system, no age is impervious to this law; everything beneath the stars will perish; the hardest rock will be worn away. Nothing endures but words.

—*spoken by Tiro, a Roman scribe, in* **Lustrum**,
by Robert Harris—see [26, Page 11][a]

[a] Although [26] is essentially a work of fiction, Marcus Tullius Tiro actually existed and was a secretary to the Roman orator and statesman Cicero. Indeed, Tiro wrote the book *The Life of Cicero*, which disappeared after the fall of Rome along with most of his literary output. Tiro ostensibly lived to be over one hundred years old and his (shorthand) method of recording has elements that survive to this day including the symbol &, for instance. His method, known as *Notae Tironianae* or more commonly the *Tironian system of shorthand*, was taught in Roman schools and enjoyed widespread use over several centuries.

We introduce some concepts in this section that will be crucial in the development of the theory of integral bases and discriminants in §2.3. In §2.1, in particular Exercises 2.1–2.6 on pages 62–63, we discussed embeddings of an algebraic number field in $\mathbb{C}$. We now use this notion to define two fundamental concepts.

Definition 2.4 — Norms and Traces

Let F be an algebraic number field of degree d over $\mathbb{Q}$, and let θ_j for $j = 1, 2, \ldots d$ be the embeddings of F in $\mathbb{C}$. For each element $\alpha \in F$, set

$$T_F(\alpha) = \sum_{j=1}^{d} \theta_j(\alpha),$$

called the *trace of α from F*, and set

$$N_F(\alpha) = \prod_{j=1}^{d} \theta_j(\alpha),$$

called the *norm of α from F.*

The definition of norm and trace was first given by Dedekind in 1871—see Biography 1.3 on page 29. By Exercise 2.17 on page 68, T_F is additive, and N_F is multiplicative. We will substantially generalize Definition 2.4 later—see Definition 5.2 on page 184.

Example 2.2 Let $F = \mathbb{Q}(\sqrt{13})$, $\alpha = 1 + \sqrt{13}$, and $\beta = (3 + \sqrt{13})/2$. The embeddings of F in $\mathbb{C}$ are

$$\theta_1 : \sqrt{13} \mapsto \sqrt{13}, \text{ and } \theta_2 : \sqrt{13} \mapsto -\sqrt{13},$$

fixing $\mathbb{Q}$ pointwise, namely the $\mathbb{Q}$-isomorphisms of F. Here,

$$N_F(\alpha) = \theta_1(\alpha)\theta_2(\alpha) = (1 + \sqrt{13})(1 - \sqrt{13}) = -12,$$

$$N_F(\beta) = \theta_1(\beta)\theta_2(\beta) = \left(\frac{3 + \sqrt{13}}{2}\right)\left(\frac{3 - \sqrt{13}}{2}\right) = -1,$$

$$T_F(\alpha) = \theta_1(\alpha) + \theta_2(\alpha) = (1 + \sqrt{13}) + (1 - \sqrt{13}) = 2,$$

and

$$T_F(\beta) = \theta_1(\beta) + \theta_2(\beta) = \frac{3+\sqrt{13}}{2} + \frac{3-\sqrt{13}}{2} = 3.$$

Also,

$$N_F(\alpha\beta) = N_F\left((1+\sqrt{13})\left(\frac{3+\sqrt{13}}{2}\right)\right) = N_F(8+2\sqrt{13}) =$$

$$8^2 - 4\cdot 13 = 12 = (-12)(-1) = N_F(\alpha)N_F(\beta),$$

and

$$T_F(\alpha+\beta) = T_F\left((1+\sqrt{13}) + \left(\frac{3+\sqrt{13}}{2}\right)\right) = T_F\left(\frac{5+3\sqrt{13}}{2}\right) =$$

$$5 = 2 + 3 = T_F(\alpha) + T_F(\beta).$$

Example 2.2 illustrates some general properties of norms and traces.

Theorem 2.5 — Properties of Norms and Traces in Subfields

Let F be an algebraic number field of degree n over $\mathbb{Q}$, and $\alpha \in F$ with $|\mathbb{Q}(\alpha):\mathbb{Q}| = d$. If $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ are all of the conjugates of α over $\mathbb{Q}$, namely the roots of $m_{\alpha,F}(x)$, then

$$T_F(\alpha) = \frac{n}{d}\sum_{j=1}^{d}\alpha_j = \frac{n}{d}T_{\mathbb{Q}(\alpha)}(\alpha),$$

and

$$N_F(\alpha) = \left(\prod_{j=1}^{d}\alpha_j\right)^{n/d} = (N_{\mathbb{Q}(\alpha)}(\alpha))^{n/d}.$$

Furthermore,

$$m_{\alpha,\mathbb{Q}}(x) = x^d - T_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)}(\alpha).$$

Proof. Let the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ be given by

$$\phi_j(\alpha) \mapsto \alpha_j \quad (1 \le j \le d),$$

where $\phi_j(q) = q$ for all $q \in \mathbb{Q}$. Thus, by Definition 2.4 on the previous page,

$$T_{\mathbb{Q}(\alpha)}(\alpha) = \sum_{j=1}^{d}\alpha_j, \text{ and } N_{\mathbb{Q}(\alpha)}(\alpha) = \prod_{j=1}^{d}\alpha_j.$$

By Exercise 2.6 on page 63, each of the ϕ_i, for $i = 1, 2, \ldots, d$, extends to exactly n/d embeddings of F in $\mathbb{C}$, which we will denote by

$$\theta_i^{(j)}, \text{ for } j = 1, 2, \ldots, n/d.$$

Therefore,

$$T_F(\alpha) = \sum_{i=1}^{d}\sum_{j=1}^{n/d}\theta_i^{(j)}(\alpha) = \sum_{i=1}^{d}\frac{n}{d}\alpha_i = \frac{n}{d}\sum_{i=1}^{d}\alpha_i,$$

and

$$N_F(\alpha) = \prod_{i=1}^{d}\prod_{j=1}^{n/d}\theta_i^{(j)}(\alpha) = \prod_{i=1}^{d}\alpha_i^{n/d} = \left(\prod_{i=1}^{d}\alpha_i\right)^{n/d}.$$

Finally, in the expansion of

$$m_{\alpha,\mathbb{Q}}(x) = \prod_{i=1}^{d}(x-\alpha_i),$$

we see that the constant term must be

$$\pm\prod_{i=1}^{d}\alpha_i = \pm N_{\mathbb{Q}(\alpha)}(\alpha),$$

whereas the coefficient of x^{d-1} must be

$$-\sum_{i=1}^{d}\alpha_i = -T_{\mathbb{Q}(\alpha)}(\alpha).$$

This completes the proof. □

Corollary 2.2 If $\alpha \in F$, an algebraic number field, then

$$T_F(\alpha) \in \mathbb{Q}, \text{ and } N_F(\alpha) \in \mathbb{Q}.$$

Proof. By Theorem 2.5, we need only show that $N_{\mathbb{Q}(\alpha)}(\alpha), T_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Q}$. However, this is immediate since, by the theorem,

$$m_{\alpha,\mathbb{Q}}(x) = x^d - T_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Q}[x],$$

which secures the result. □

Corollary 2.3 Let $\alpha \in \overline{N}$, and let $m_{\alpha,\mathbb{Q}}(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Then $\alpha \in \mathbb{A}$ if and only if $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Furthermore, if $\alpha \in \mathbb{A}$, then

$$T_F(\alpha) \in \mathbb{Z}, \text{ and } N_F(\alpha) \in \mathbb{Z}.$$

Proof. Suppose that $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$ where $\alpha \in \mathbb{A}$, and α is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$ of least possible degree. Then $m_{\alpha,\mathbb{Q}}(x) \bigm| f(x)$ in $\mathbb{Q}[x]$ by Theorem 1.23 on page 38. However, since $m_{\alpha,\mathbb{Q}}(x)$ is monic, then by Gauss's Lemma A.1 on page 332, we must have $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, so $f(x) = m_{\alpha,\mathbb{Q}}(x)$. Conversely, if $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, then $\alpha \in \mathbb{A}$ by definition.

To prove the final statement we note that by Theorem 2.5,

$$m_{\alpha,\mathbb{Q}}(x) = x^d - T_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)}(\alpha),$$

and by the above $m_{\alpha,\mathbb{Q}}(\alpha) \in \mathbb{Z}$ when $\alpha \in \mathbb{A}$, so the result follows. □

The notions of trace and norm are also linked to the discriminant of a polynomial introduced in Exercise 2.29 on page 69. The reader will be familiar with the details of the following from Example 1.29 on page 46.

Example 2.3 Consider the irreducible quadratic polynomial

$$f(x) = ax^2 + bx + c \in \mathbb{Q}[x],$$

where $a \neq 0$. As mentioned in Example 1.29, the roots of $f(x)$ are given by

$$\alpha = \frac{-b + \sqrt{\Delta}}{2a}, \text{ and } \alpha' = \frac{-b - \sqrt{\Delta}}{2a},$$

where $\Delta = \ b^2 - 4ac$ is the discriminant of the quadratic field $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$—see Theorem 1.27 on page 44 and the discussion surrounding it. Therefore,

$$T_F(\alpha) = T_{\mathbb{Q}(\alpha)}(\alpha) = \alpha + \alpha' = \frac{-b + \sqrt{\Delta}}{2a} + \frac{-b - \sqrt{\Delta}}{2a} = -b/a,$$

and

$$N_F(\alpha) = N_{\mathbb{Q}(\alpha)}(\alpha) = \alpha\alpha' = \left(\frac{-b + \sqrt{\Delta}}{2a}\right)\left(\frac{-b - \sqrt{\Delta}}{2a}\right) = \frac{b^2 - \Delta}{4a^2} = c/a.$$

Hence, the minimal polynomial of α over $\mathbb{Q}$ is $m_{\alpha,\mathbb{Q}}(x) = x^2 - T_F(\alpha)x + N_F(\alpha)$.

Exercises

2.17. With reference to Definition 2.4 on page 65, prove that

$$T_F(\alpha + \beta) = T_F(\alpha) + T_F(\beta), \text{ and } N_F(\alpha\beta) = N_F(\alpha)N_F(\beta),$$

for all α,β $\in F$. Also, prove that for any $q \in \mathbb{Q}$,

$$T_F(q\alpha) = qT_F(\alpha), \text{ and } N_F(q\alpha) = q^d N_F(\alpha).$$

(Thus, in particular, if $\alpha = 1$, then $T_F(q) = q$, and $N_F(q) = q^d$.)

2.18. Let $n \in \mathbb{Z}$ be cubefree (namely $p^3 \nmid n$ for any prime p). Also, let $\alpha = \sqrt[3]{n}$, $F = \mathbb{Q}(\alpha)$, and $m_{\alpha,\mathbb{Q}}(x) = x^3 - n$. Find $\text{disc}(m_{\alpha,\mathbb{Q}})$ by employing Exercise 2.31. Furthermore, set

$$\beta = (\alpha^2 \pm \alpha + 1)/3, \text{ with } n \equiv \pm 1 \pmod 9,$$

where the ± signs correspond as given. Find $T_F(\beta)$, $N_F(\beta)$, and $m_{\beta,\mathbb{Q}}(x)$. Conclude that β is an algebraic integer in F.

(*Fields of the form* $\mathbb{Q}(\sqrt[3]{n})$ *for cube-free* n *are called pure cubic fields.*)

2.19. Let $F = \mathbb{Q}(\sqrt{7})$, and $\alpha = (1 + \sqrt{7})/2$. Find $N_F(\alpha)$, $T_F(\alpha)$, and $m_{\alpha,\mathbb{Q}}(x)$.

2.20. Prove that there are no elements having norm 3 from $\mathbb{Q}(\sqrt{-1})$.

2.21. Let $F = \mathbb{Q}(\sqrt{p})$ where $p \equiv \pm 3 \pmod 8$ is prime. Show that there is no $\alpha \in F$ such that $N_F(\alpha) = 2$.

2.22. Find the minimal polynomial of $\sqrt{-2 - 3\sqrt{-5}}$ over $\mathbb{Q}$.

2.23. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

In Exercises 2.24–2.26, we assume that $F = \mathbb{Q}(\zeta_p)$ *for a prime* p.

2.24. Prove that $T_F(\zeta_p) = -1$, and $N_F(1 - \zeta_p) = p$.

2.25. Prove that $T_F(1-\zeta_p^j)=p$, where $j\in\{1,2,\ldots,p-1\}$.

(*Hint: Use Example 1.5 on page 2.*)

2.26. Let α be an algebraic integer in F. Prove that $T_F(\alpha(1-\zeta_p))\in p\mathbb{Z}$.

2.27. Let $\mathfrak{g}=(1+\sqrt{5})/2$ be the golden ratio. Prove that $\zeta_3\in\mathbb{Q}(\mathfrak{g}+\zeta_3)$.

2.28. Prove that $\mathfrak{g}\in\mathbb{Q}(\mathfrak{g}+\zeta_3)$.

2.28. Let $f(x)=x^4-2$ and let $\alpha=\sqrt[4]{2}$ be a real root of $f(x)$. Prove that $F=\mathbb{Q}(\alpha,i)$ is the splitting field for f over $\mathbb{Q}$. See Definition A.17 on page 334.

The remaining exercises allow us a segue into §2.3, where we generalize the notion of a field discriminant given for quadratic fields in Definition 1.33 on page 46.

2.29. If $f(x)\in F[x]$ where $F\subset\mathbb{C}$ is a field, $\deg(f)=d>1$, and

$$f(x)=a\prod_{j=1}^{d}(x-a_j),a_j\in F,$$

then the *discriminant of* f is defined by

$$\operatorname{disc}(f)=a^{2d-1}\prod_{1\le i<j\le d}(\alpha_i-\alpha_j)^2,$$

where α_j for $j=1,2,\ldots,d$ are the roots of f in $\mathbb{C}$.

Prove that for an odd prime p and a primitive p-th root of unity

$$\operatorname{disc}(m_{\zeta_p,\mathbb{Q}})=\prod_{1\le i<j\le p-1}(\zeta_p^i-\zeta_p^j)^2=(-1)^{(p-1)/2}p^{p-2}.$$

(*Hint: First prove that:* $m_{\zeta_p,\mathbb{Q}}(x)=\sum_{j=0}^{p-1}x^j$.)

2.30. Find the discriminant of the quadratic polynomial f given in Example 2.3 on the facing page by applying Exercise 2.29. Also, show that if m' is the formal derivative, then

$$\operatorname{disc}(m'_{\alpha,\mathbb{Q}}(x))=-N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

2.31. Exercise 2.30 motivates the following more general result. Suppose that $\alpha\in\mathbb{A}$ and $F=\mathbb{Q}(\alpha)$ is an algebraic number field of degree d over $\mathbb{Q}$, and $\alpha=\alpha_1,\alpha_2,\ldots,\alpha_d$ are the conjugates of α over $\mathbb{Q}$. Prove that

$$\operatorname{disc}(m_{\alpha,\mathbb{Q}})=(-1)^{d(d-1)/2}\prod_{j=1}^{d}m'_{\alpha,\mathbb{Q}}(\alpha_j)=(-1)^{d(d-1)/2}N_F(m'_{\alpha,\mathbb{Q}}(\alpha_j)),$$

where $m'_{\alpha,\mathbb{Q}}$ is the formal derivative of $m_{\alpha,\mathbb{Q}}$.

2.3 Integral Bases and Discriminants

> *The mathematician is fascinated with the marvelous beauty of the forms he constructs, and in their beauty he finds everlasting truth.*
> **James Byrnie Shaw (1866–1948), mathematician/philosopher—see [63]**

Given a number field F, we know from Theorem 1.24 on page 39 that there is an algebraic integer α such that $F = \mathbb{Q}(\alpha)$. Moreover, every $\beta \in F$ may be uniquely represented in the form

$$\beta = q_0 + q_1\alpha + \cdots + q_{d-1}\alpha^{d-1} \in \mathbb{Q}[\alpha],$$

where $d = |F : \mathbb{Q}|$. In other words, $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a $\mathbb{Q}$-basis for F. Moreover, since $\mathfrak{O}_F$ is Noetherian by Corollary 1.13 on page 37, then in particular, $\mathfrak{O}_F$ is finitely generated as a $\mathbb{Z}$-module so now we seek a $\mathbb{Z}$-basis for it.

Definition 2.5 — Integral Bases

If $\mathfrak{O}_F$ is the ring of integers of a number field F, a basis for $\mathfrak{O}_F$ over $\mathbb{Z}$, or simply a $\mathbb{Z}$-basis for $\mathfrak{O}_F$, is called an *integral basis* for $\mathfrak{O}_F$.

Remark 2.2 By Exercise 2.32 on page 81, an integral basis for $\mathfrak{O}_F$ in the sense of Definition 2.5 is a basis in the sense of Definition A.7 on page 324.

Example 2.4 If $F = \mathbb{Q}(\sqrt{2})$, then $\mathfrak{O}_F = \mathbb{Z}[\sqrt{2}]$, by Theorem 1.28 on page 45. Thus, $\mathcal{B} = \{1, \sqrt{2}\}$ is an integral basis for F.

Example 2.5 If $F = \mathbb{Q}(\sqrt{13})$, then by Theorem 1.28

$$\mathfrak{O}_F = \mathbb{Z}[(1+\sqrt{13})/2] \neq \mathbb{Z}[\sqrt{13}].$$

Here $\alpha = (1+\sqrt{13})/2$ is a root of $m_{\alpha,\mathbb{Q}}(x) = x^2 - x - 3$, whereas $\beta = \sqrt{13}$ is a root of $x^2 - 13$. Thus, although $\{1, \beta\}$ is a basis for F consisting of algebraic integers, it is not an integral basis for F. An integral basis for F is $\{1, \alpha\}$.

The rings of integers in Examples 2.4–2.5 both have integral bases. Our immediate task is first to verify that *any* ring of integers $\mathfrak{O}_F$ of an algebraic number field F has an integral basis. In order to do this, we first need the following notion. The reader should have familiarity with the basics of matrices and fundamental linear algebra as outlined in Appendix A.

Definition 2.6 — Discriminant of a Basis

Let $F = \mathbb{Q}(\alpha)$ be an algebraic number field with $|F : \mathbb{Q}| = d$. If

$$\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$$

is a $\mathbb{Q}$-basis for F, and $\theta_j \quad (1 \le j \le d)$ are all of the embeddings of F in $\mathbb{C}$, then the discriminant of the basis is given by

$$\operatorname{disc}(\mathcal{B}) = \det(\theta_j(\alpha_i))^2,$$

where *det* denotes the determinant of the matrix with entry $\theta_j(\alpha_i)$ in the i^{th} row and j^{th} column.

In particular, if

$$\mathcal{B} = \{1, \alpha, \ldots, \alpha^{d-1}\},$$

then the determinant of the matrix $(\theta_j(\alpha^{i-1}))$ is called the *Vandermonde determinant* and has value

$$\det(\theta_j(\alpha^{i-1})) = \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i), \tag{2.7}$$

by Exercise 2.33, where $\alpha_k = \theta_k(\alpha)$ is the k^{th} conjugate of α for $k = 1, 2, \ldots, d$.

Example 2.6 In Example 2.4, $\mathcal{B} = \{1, \sqrt{2}\}$ is an integral basis for F, and

$$\theta_1 : \sqrt{2} \mapsto \sqrt{2}, \text{ and } \theta_2 : \sqrt{2} \mapsto -\sqrt{2},$$

are the embeddings of F in $\mathbb{C}$. Thus,

$$\operatorname{disc}(\mathcal{B}) = \det(\theta_j(\alpha^{i-1}))^2 = \det \begin{pmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1(\sqrt{2}) & \theta_2(\sqrt{2}) \end{pmatrix}^2 =$$

$$\det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}^2 = (-2\sqrt{2})^2 = 8.$$

Notice that in Example 2.6, $\operatorname{disc}(\mathcal{B}) = \operatorname{disc}(m_{\alpha,\mathbb{Q}})$, where $m_{\alpha,\mathbb{Q}}(x) = x^2 - 2$—see Exercise 2.35 on page 82. This is an illustration of a more general phenomenon given as follows.

Theorem 2.6 — Discriminants of Bases and Minimal Polynomials
Let $\alpha \in \mathbb{A}$ and suppose that $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then

$$\operatorname{disc}(\mathcal{B}) = \operatorname{disc}(m_{\alpha,\mathbb{Q}}),$$

where $m_{\alpha,\mathbb{Q}}(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$. By (2.7),

$$\operatorname{disc}(\mathcal{B}) = \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i)^2,$$

and by Exercise 2.29 on page 69, this is equal to $\operatorname{disc}(m_{\alpha,\mathbb{Q}})$. □

Now we demonstrate that the discriminants of two bases for a number field form a quotient that is a square of a nonzero rational number.

Theorem 2.7 — Discriminants of Two Bases
Let $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ and $\mathcal{B}_2 = \{\beta_1, \beta_2, \ldots, \beta_d\}$ be two $\mathbb{Q}$-bases for an algebraic number field F. Then

$$\operatorname{disc}(\mathcal{B}_2) = D^2 \operatorname{disc}(\mathcal{B}_1),$$

where $D = \det(q_{k,i}) \in \mathbb{Q}$, $D \neq 0$, and the $q_{k,i} \in \mathbb{Q}$ are determined by

$$\beta_k = \sum_{i=1}^{d} q_{k,i} \alpha_i, \quad (q_{k,i} \in \mathbb{Q}).$$

Moreover, $D \in \mathbb{Z}$ provided that $\mathcal{B}_1$ is an integral basis and $\mathcal{B}_2 \in \mathfrak{O}_F$.

Proof. Let θ_j, $(1 \le j \le d)$ be the embeddings of F in $\mathbb{C}$. The representations $\beta_k = \sum_{i=1}^d q_{k,i}\alpha_i$, imply that

$$\theta_j(\beta_k) = \sum_{i=1}^{d} q_{k,i}\theta_j(\alpha_i),$$

for each $k = 1, 2, \ldots, d$. Hence, we get a matrix equation:

$$\begin{pmatrix} \theta_1(\beta_1) & \theta_2(\beta_1) & \cdots & \theta_d(\beta_1) \\ \theta_1(\beta_2) & \theta_2(\beta_2) & \cdots & \theta_d(\beta_2) \\ \vdots & \vdots & \vdots & \vdots \\ \theta_1(\beta_d) & \theta_2(\beta_d) & \cdots & \theta_d(\beta_d) \end{pmatrix} =$$

$$\begin{pmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,d} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ q_{d,1} & q_{d,2} & \cdots & q_{d,d} \end{pmatrix} \begin{pmatrix} \theta_1(\alpha_1) & \theta_2(\alpha_1) & \cdots & \theta_d(\alpha_1) \\ \theta_1(\alpha_2) & \theta_2(\alpha_2) & \cdots & \theta_d(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \theta_1(\alpha_d) & \theta_2(\alpha_d) & \cdots & \theta_d(\alpha_d) \end{pmatrix}.$$

By taking determinants, and squaring, we get the equation:

$$\mathrm{disc}(\mathcal{B}_2) = D^2 \mathrm{disc}(\mathcal{B}_1),$$

with $D = \det(M)$, where

$$M = \begin{pmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,d} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ q_{d,1} & q_{d,2} & \cdots & q_{d,d} \end{pmatrix},$$

as required. □

Example 2.7 Let $F = \mathbb{Q}(\sqrt{13})$, $\alpha = (1+\sqrt{13})/2$, and $\beta = \sqrt{13}$. In Example 2.5 on page 70, we saw that $\mathcal{B}_1 = \{1, \alpha\}$ and $\mathcal{B}_2 = \{1, \beta\}$ are bases for F, the former being integral, and the latter not integral, but merely a basis over $\mathbb{Q}$. Since

$$\theta_1 : \sqrt{13} \mapsto \sqrt{13}, \text{ and } \theta_2 : \sqrt{13} \mapsto -\sqrt{13}$$

are the embeddings of F in $\mathbb{C}$, then

$$\mathrm{disc}(\mathcal{B}_2) = \det(\theta_j(\beta^i))^2 = \det\begin{pmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1(\sqrt{13}) & \theta_2(\sqrt{13}) \end{pmatrix}^2$$

$$= \det\begin{pmatrix} 1 & 1 \\ \sqrt{13} & -\sqrt{13} \end{pmatrix}^2 = (-2\sqrt{13})^2 = 52,$$

and

$$\mathrm{disc}(\mathcal{B}_1) = \det(\theta_j(\alpha^i))^2 = \det\begin{pmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1(\frac{1+\sqrt{13}}{2}) & \theta_2(\frac{1+\sqrt{13}}{2}) \end{pmatrix}^2$$

$$= \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{13}}{2} & \frac{1-\sqrt{13}}{2} \end{pmatrix}^2 = (-\sqrt{13})^2 = 13.$$

Thus,

$$\mathrm{disc}(\mathcal{B}_2) = 2^2 \mathrm{disc}(\mathcal{B}_1).$$

Here

$$D = 2 = \det \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix},$$

since

$$\beta_1 = 1 = q_{1,1} \cdot \alpha_1 + q_{1,2}\alpha_2 = 1 \cdot 1 + 0 \cdot \alpha,$$

and

$$\beta_2 = \beta = \sqrt{13} = q_{2,1}\alpha_1 + q_{2,2}\alpha_2 = -1 \cdot 1 + 2 \cdot \frac{1+\sqrt{13}}{2}.$$

We are now in a position to relate the notion of discriminant introduced in Definition 2.6 on page 70 with the notions introduced in §2.2. See Exercise 2.1 on page 62 for a reminder of terminology and notions surrounding what follows.

Theorem 2.8 — Discriminants as Traces

If $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is a $\mathbb{Q}$-basis for an algebraic number field $F = \mathbb{Q}(\alpha)$, then

$$\Delta = \mathrm{disc}(\mathcal{B}) = \det(T_F(\alpha_i\alpha_j)) \in \mathbb{Q},$$

and$\Delta \neq 0$. Furthermore, if F is a totally real field, then$\Delta > 0$.

Proof. Since $\Delta = \mathrm{disc}(\mathcal{B}) = \det(\theta_j(\alpha_i))^2$, then from the properties of determinants (see Theorem A.19 on page 336), we get:

$$\det(\theta_j(\alpha_i))^2 = \det\left(\sum_{k=1}^{d} \theta_k(\alpha_i\alpha_j)\right) = \det(T_F(\alpha_i\alpha_j)),$$

so $\Delta = \det(T_F(\alpha_i\alpha_j))$. Therefore, by Corollary 2.2 on page 67,$\Delta \in \mathbb{Q}$. It remains to show that Δ is nonzero and also positive when F is totally real.

Let $\mathcal{B}_1 = \mathcal{B}$. By Theorem 1.24 on page 39,

$$\mathcal{B}_2 = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$$

is a basis for F over $\mathbb{Q}$. Thus, by Theorem 2.7, $\mathrm{disc}(\mathcal{B}_2) = D^2\mathrm{disc}(\mathcal{B}_1)$, where D is given in that theorem. However, by Exercise 2.33 on page 81,

$$\mathrm{disc}(\mathcal{B}_2) = \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i)^2, \tag{2.8}$$

and the α_i are distinct so $\mathrm{disc}(\mathcal{B}_2) \neq 0$. Hence, $\mathrm{disc}(\mathcal{B}_1) \neq 0$.

Since $\mathcal{B}_2$ is a basis for F over $\mathbb{Q}$, then by Theorem 2.7,

$$\mathrm{disc}(\mathcal{B}_1) = d^2\mathrm{disc}(\mathcal{B}_2).$$

However, by (2.8), $\mathrm{disc}(\mathcal{B}_2)$ is a square. Since $\mathrm{disc}(\mathcal{B}_1) \neq 0$, so given that F is totally real, all of the α_j are real, so $\mathrm{disc}(\mathcal{B}_1) > 0$. □

Corollary 2.4 If $\mathcal{B}$ is a basis for F over $\mathbb{Q}$ with $\mathcal{B} \subseteq \mathfrak{O}_F$, then $\mathrm{disc}(\mathcal{B}) \in \mathbb{Z}$.

Proof. This is immediate from Corollary 2.3 on page 67. □

Example 2.8 Consider Example 2.7 again. $F = \mathbb{Q}(\sqrt{13})$ is a totally real field with integral basis

$$\mathcal{B}_1 = \{1, (1+\sqrt{13})/2\} = \{1, \alpha\} = \{\alpha_1, \alpha_2\},$$

and a non-integral $\mathbb{Q}$-basis

$$\mathcal{B}_2 = \{1, \sqrt{13}\} = \{1, \beta\} = \{\beta_1, \beta_2\}.$$

Also, since the matrix

$$(T_F(\alpha_i\alpha_j)) = \begin{pmatrix} T_F(1) & T_F(\alpha) \\ T_F(\alpha) & T_F(\alpha^2) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix},$$

then

$$\operatorname{disc}(\mathcal{B}_1) = \det(T_F(\alpha_i\alpha_j)) = \det \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix} = 13.$$

Also, since we have the matrix

$$(T_F(\beta_i\beta_j)) = \begin{pmatrix} T_F(1) & T_F(\beta) \\ T_F(\beta) & T_F(\beta^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 26 \end{pmatrix},$$

then

$$\operatorname{disc}(\mathcal{B}_2) = 52 = \det(T_F(\beta_i\beta_j)).$$

Corollary 2.5 Let $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be a $\mathbb{Q}$-basis for an algebraic number field F. If $\mathcal{B}_2 = \{\beta_1, \beta_2, \ldots, \beta_d\} \subseteq F$ and

$$\beta_k = \sum_{i=1}^{d} q_{k,i}\alpha_i \text{ for } q_{k,i} \in F, \text{ and } k = 1, 2, \ldots, d,$$

then $\mathcal{B}_2$ is also a basis for F if and only if $\det(q_{k,i}) \neq 0$.

Proof. Suppose that $\det(q_{k,i}) \neq 0$. It suffices to show that the β_k are linearly independent by Theorem A.4 on page 325. If

$$\sum_{k=1}^{d} \gamma_k\beta_k = 0 \quad (\gamma_k \in F),$$

then

$$0 = \sum_{k=1}^{d} \gamma_k \sum_{i=1}^{d} q_{k,i}\alpha_i = \sum_{i=1}^{d} \alpha_i \sum_{k=1}^{d} \gamma_k q_{k,i}.$$

Since the α_i are linearly independent, then

$$\sum_{k=1}^{d} \gamma_k q_{k,i} = 0.$$

Since $\det(q_{k,i}) \neq 0$, then $\gamma_k = 0$ for all $k = 1, 2, \ldots, d$.

Conversely, if $\mathcal{B}_2$ is a basis for F, then by Theorem 2.7 on page 71,

$$\operatorname{disc}(\mathcal{B}_2) = D^2\operatorname{disc}(\mathcal{B}_1).$$

Hence, by Theorem 2.8 the result follows. □

In Example 2.5 on page 70, we saw that a $\mathbb{Q}$-basis for an algebraic number field F, consisting of algebraic integers, need not be an integral basis for F. The problem is that a basis consisting of algebraic integers may span F without spanning $\mathfrak{O}_F$ as a $\mathbb{Z}$-module. We now verify that every algebraic number field does indeed have an integral basis, and that the ring of integers is a free abelian group of rank equal to the degree of the number field over $\mathbb{Q}$.

Theorem 2.9 — Existence of Integral Bases

Every algebraic number field F of degree d over $\mathbb{Q}$ has an integral basis, and $\mathfrak{O}_F$ is a free abelian group of rank d.

Proof. By Lemma 1.4 on page 38, there is a basis for F consisting of elements from $\mathfrak{O}_F$. This establishes existence of such bases. It remains to show that there exists such a basis that is a $\mathbb{Z}$-basis for $\mathfrak{O}_F$.

By Corollary 2.4, the discriminants of such bases are in $\mathbb{Z}$, and by Theorem 2.8, they are nonzero. Hence, we may choose a basis

$$\mathcal{B}_1 = \{\beta_1, \beta_2, \dots, \beta_d\} \subseteq \mathfrak{O}_F$$

for F over $\mathbb{Q}$ such that $|\text{disc}(\mathcal{B}_1)|$ is a minimum. Assume that $\mathcal{B}_1$ is not a $\mathbb{Z}$-basis for $\mathfrak{O}_F$. Therefore, there exists a $\gamma \in \mathfrak{O}_F$ such that

$$\gamma = \sum_{j=1}^{d} q_j \beta_j \quad (q_j \in \mathbb{Q}),$$

and at least one $q_j \notin \mathbb{Z}$. Without loss of generality, assume that $q_1 \notin \mathbb{Z}$. Thus,

$$q_1 = \lfloor q_1 \rfloor + r, \quad (0 < r < 1)$$

where $\lfloor q_1 \rfloor$ is the floor of q_1—see Page 8. Set

$$\delta = \gamma - \lfloor q_1 \rfloor \beta_1 = \sum_{j=1}^{d} q_j \beta_j - \lfloor q_1 \rfloor \beta_1 = r\beta_1 + \sum_{j=2}^{d} q_j \beta_j.$$

The determinant of the matrix:

$$A = \begin{pmatrix} r & q_2 & \cdots & q_d \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is

$$\det(A) = r \neq 0.$$

By Corollary 2.5,

$$\mathcal{B}_2 = \{\delta, \beta_2, \dots, \beta_d\}$$

is a basis for F over $\mathbb{Q}$. Since

$$\text{disc}(\mathcal{B}_2) = r^2 \text{disc}(\mathcal{B}_1),$$

then

$$|\text{disc}(\mathcal{B}_2)| < |\text{disc}(\mathcal{B}_1)|,$$

contradicting the minimality of the discriminant of $\mathcal{B}_1$. Hence, $\mathcal{B}_1$ is an integral basis for F. Therefore, as a $\mathbb{Z}$-module

$$\mathfrak{O}_F = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_d,$$

so $\mathfrak{O}_F$ is a free abelian group of rank d (see Equation (A.4) on page 325, and the discussion preceding it). □

Corollary 2.6 If $\mathcal{B} \subseteq \mathfrak{O}_F$ is a $\mathbb{Q}$-basis for F and $\text{disc}(\mathcal{B})$ is squarefree, then $\mathcal{B}$ is an integral basis for F.

Proof. Let $\mathcal{B} = \{\beta_1, \ldots, \beta_d\}$. By Theorem 2.9, there exists an integral basis $\mathcal{B}_1 = \{\alpha_1, \ldots, \alpha_d\}$ for F. By Theorem 2.7 on page 71,

$$\text{disc}(\mathcal{B}) = D^2\text{disc}(\mathcal{B}_1),$$

where $D = \det(q_{k,i})$, and $q_{k,i}$ is given by

$$\beta_k = \sum_{i=1}^{d} q_{k,i}\alpha_i \quad (q_{k,i} \in \mathbb{Q}).$$

Since $\text{disc}(\mathcal{B})$ is squarefree, then $D = \pm 1$. Therefore, $(q_{k,i}) \in GL_n(\mathbb{Z})$. Thus, by Exercise 2.34 on page 81, $\mathcal{B}$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_F$. Thus, $\mathcal{B}$ is an integral basis for F. □

Example 2.9 Example 2.5 on page 70 provides an example of a squarefree discriminant of an integral basis. However, in Example 2.4, $\mathcal{B} = \{1, \sqrt{2}\}$ is an integral basis for $\mathbb{Q}(\sqrt{2})$, but $\text{disc}(\mathcal{B}) = 8$, so the converse of Corollary 2.6 fails to hold.

Although Example 2.9 shows that the converse of Corollary 2.6 fails to hold, if we have two integral bases for an algebraic number field, then they must have the same discriminant.

Corollary 2.7 Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two integral bases for an algebraic number field F. Then

$$\text{disc}(\mathcal{B}_1) = \text{disc}(\mathcal{B}_2).$$

Proof. By Theorem 2.7,

$$\text{disc}(\mathcal{B}_2) = D^2\text{disc}(\mathcal{B}_1) \tag{2.9}$$

where $D \in \mathbb{Z}$ is given in that theorem. Thus,

$$\text{disc}(\mathcal{B}_1) \,\big|\, \text{disc}(\mathcal{B}_2) \in \mathbb{Z},$$

by Corollary 2.4 on page 73. By reversing the roles of $\mathcal{B}_1$ and $\mathcal{B}_2$, we get

$$\text{disc}(\mathcal{B}_2) \,\big|\, \text{disc}(\mathcal{B}_1) \in \mathbb{Z}.$$

Therefore,

$$\text{disc}(\mathcal{B}_1) = \pm\text{disc}(\mathcal{B}_2).$$

However, by Equation (2.9), the minus sign is not possible. □

Corollary 2.7 essentially tells us that the discriminant of an integral basis for an algebraic number field is an invariant of the field, and it has a name. The following generalizes the notion for the quadratic case given in Definition 1.33 on page 46.

Definition 2.7 — Discriminant of a Field

Let $\mathcal{B}$ be an integral basis for an algebraic number field F. Then the discriminant of F is disc$(\mathcal{B})$, denoted byΔ_F.

Application 2.1 — Quadratic Fields

The ring of integers of a quadratic number field F is given by $\mathfrak{O}_F = \mathbb{Z}[\omega_{\Delta_F}]$ where

$$\omega_{\Delta_F} = \begin{cases} (1+\sqrt{\Delta_F})/2 & \text{if} \quad \Delta_F \equiv 1 \pmod 4, \\ \sqrt{\Delta_F} & \text{if} \Delta_F \not\equiv 1 \pmod 4 \end{cases}$$

is called the *principal surd.* —see Application 1.2 on page 3 and Theorem 1.28 on page 45. Also,

$$D_F = \begin{cases} \Delta_F & \text{if} \Delta_F \equiv 1 \pmod 4, \\ D_F/4 & \text{if} \quad \Delta_F \not\equiv 1 \pmod 4 \end{cases}$$

is called the *radicand* of F.

Example 2.10 Let $F = \mathbb{Q}(\sqrt{19})$. By Theorem 1.28, $\mathcal{B} = \{1, \sqrt{19}\}$ is an integral basis for F. Thus,

$$\Delta_F = \text{disc}(\mathcal{B}) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{19} & -\sqrt{19} \end{pmatrix}^2 = (-2\sqrt{19})^2 = 76 = 4 \cdot 19 = 4D_F.$$

Example 2.11 Let $F = \mathbb{Q}(\sqrt{13})$. Then

$$\mathcal{B} = \{1, (1+\sqrt{13})/2\}$$

is an integral basis for F by Theorem 1.28. Thus,

$$\Delta_F = \text{disc}(\mathcal{B}) = \det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{13}}{2} & \frac{1-\sqrt{13}}{2} \end{pmatrix}^2 = 13 = D_F.$$

Now we provide a generalization of the quadratic version promised in Remark 1.22 on page 46—see Biography 1.4 on page 54.

Theorem 2.10 — Stickelberger's Theorem

If F is an algebraic number field, then

$$\Delta_F \equiv 0, 1 \pmod 4.$$

Proof. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for F, where $|F : \mathbb{Q}| = n$. For each $i = 1, 2, \ldots, n$, let $\alpha_i, \alpha_i^{(2)}, \ldots, \alpha_i^{(n)}$ (not to be confused with the powers of α_i) be all of the conjugates of α_i over $\mathbb{Q}$. By part (d) of Theorem A.19 on page 336 as

$$\sqrt{\Delta_F} = \det(\alpha_i^{(j)})$$

is essentially the sum of $n!$ terms, each one corresponding to an element of the symmetric group S_n, we may set $\sigma(\alpha_i^{(j)}) \in S_n$ as the bijection assigning each $\alpha_i^{(j)}$ to an element of S_n. Therefore, we may refine this sum further in terms of the alternating group A_n as follows.

$$\sqrt{\Delta_F} = \det(\alpha_i^{(j)}) = \sum_{\sigma(\alpha_i^{(j)}) \in A_n} \alpha_i^{(j)} - \sum_{\sigma(\alpha_i^{(j)}) \notin A_n} \alpha_i^{(j)} = e - o,$$

so $e, o \in \mathbb{A}$. By Exercise 2.1 on page 62, we have that, for each embedding θ_j of F in $\mathbb{C}$, $\theta_j(e+o) = e+o$, and $\theta_j(eo) = eo$ so, by Exercise 2.4, $e+o, eo \in \mathbb{Q}$. Thus, by Corollary 1.11 on page 37, $e+o, eo \in \mathbb{Z}$. Therefore,

$$\Delta_F = (e-o)^2 \equiv (e+o)^2 - 4eo \equiv (e+o)^2 \pmod{4},$$

then$\Delta_F \equiv 0, 1 \,(\text{mod } 4)$, as required. □

The above proof was published in 1929 by I. Schur (1875–1941), a student of G. Frobenius—see Biographies 2.3 on page 80 and 2.4 on page 81 .

The next result tells us the effect on the discriminant of a field by the signature given in Exercise 2.11 on page 63. The following also generalizes the last statement of Theorem 2.8 on page 73. This is a result of Kronecker—see Biography 2.2.

Theorem 2.11 — Signatures and Discriminants

If F is an algebraic number field with signature $\{r_1, r_2\}$, then the sign ofΔ_F is $(-1)^{r_2}$. In other words,$\Delta_F > 0$ if and only if half the number of complex embeddings is even.

Proof. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for F, where

$$|F : \mathbb{Q}| = n.$$

Since $\det(\alpha_i^{(j)}) \in \mathbb{C}$, we may write it as

$$\det(\alpha_i^j) = a + b\sqrt{-1} \quad (a, b \in \mathbb{R}).$$

Then $\det\overline{\left(\alpha_i^{(j)}\right)} = a - b\sqrt{-1}$,where the $\overline{x}$ denotes the complex conjugate of x. Since complex conjugation will leave the real rows of the determinant unchanged, and will interchange the $2r_2$ "non-real" rows in pairs corresponding to the conjugate embeddings, the value of $\det\overline{\left(\alpha_i^{(j)}\right)}$ is also $(-1)^{r_2}(a + b\sqrt{-1})$. Therefore,

$$(-1)^{r_2}(a + b\sqrt{-1}) = a - b\sqrt{-1}.$$

If r_2 is even, then comparison of coefficients yields that $b = 0$, and$\Delta_F = a^2 > 0$. If r_2 is odd, then $a = 0$, so

$$\Delta_F = (b\sqrt{-1})^2 = -b^2 < 0,$$

as required. □

Example 2.12 If $F = \mathbb{Q}(\sqrt[3]{2})$, there are two complex embeddings, and one real embedding, namely $r_1 = 1 = r_2$, as seen in Exercise 2.12. Also, from Exercise 2.18 on page 68, it follows that

$$\Delta_F = -27 \cdot 2^2 = -108 = (-1)^{r_2} 108.$$

Biography 2.2 Leopold Kronecker (1823–1891) was born on December 7, 1823 in Liegnitz, Prussia (now Legnica, Poland). In 1841, he entered the University of Berlin and achieved a doctorate under Dirichlet's supervision in 1845. Then he left for Silesia where he became wealthy in banking and real estate. He returned to Berlin in 1855 and remained there for the rest of his life. However, he did not become a professor there until 1883 when his lifelong friend Kummer retired. Kronecker was known as a *finitist*, believing that mathematics would be well-served by consideration of only finite numbers and a finite number of steps. This naturally brought him into conflict with the likes of Cantor. In fact, Kronecker was known for his vigorous personal attacks on anyone with whom he had mathematical disagreements. His contributions were mainly to algebraic number theory, the theory of algebraic equations, and elliptic functions. Along with Kummer and Dedekind, Kronecker is generally considered to be the third father of modern algebraic number theory. He died on December 29, 1891 from bronchial illness.

We conclude this section with an observation, which also serves as a caution, concerning integral bases.

Remark 2.3 In view of Theorem 1.24 on page 39, the reader may be tempted into thinking that $\mathfrak{O}_F = \mathbb{Z}[\alpha]$ where $\alpha \in \mathbb{A}$ for any number field F. In other words, one might be lured into the belief that there is always an integral basis of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$. However, this is false, as the following illustration demonstrates. For criteria when this *does* happen see Exercise 5.48 on page 253.

Example 2.13 The following was first presented in [44]. However, our proof is different and more detailed for the edification of the reader. Let $K = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$, $F = \mathbb{Q}(\sqrt{-14})$, and $\mathcal{O}_F = \mathbb{Z}[\sqrt{-14}]$. We seek to establish that there is no $\beta \in \mathfrak{O}_K$ such that $\mathfrak{O}_K = \mathbb{Z}[\beta]$. First, we show that there is no $\alpha \in \mathfrak{O}_K$ such that $\mathfrak{O}_K = \mathbb{Z}[\alpha, \sqrt{-14}]$. By way of contradiction, suppose there is such an α. Then, in particular,

$$\Delta = \frac{1+\sqrt{-7}}{2} = \gamma_1\alpha + \gamma_2, \text{ where } \Delta \in \mathfrak{O}_K, \gamma_1, \gamma_2 \in \mathcal{O}_F$$

and

$$\sqrt{-14}/\sqrt{-7} = \sqrt{2} = \beta_1\alpha + \beta_2 \text{ where } \sqrt{2} \in \mathfrak{O}_K, \text{ and } \beta_1, \beta_2 \in \mathcal{O}_F.$$

Let θ be the embedding of K in $\mathbb{C}$ given by $\theta : \sqrt{-7} \mapsto -\sqrt{-7}$ and $\theta : \sqrt{-14} \mapsto \sqrt{-14}$. In other words, by Theorem 2.3 on page 59, $\langle\theta\rangle = \mathrm{Gal}(K/F)$, fixing F pointwise. Therefore,

$$\theta(\Delta) = \frac{1-\sqrt{-7}}{2} = \gamma_1\theta(\alpha) + \gamma_2,$$

$$\Delta - \theta(\Delta) = \sqrt{-7} = \gamma_1(\alpha - \theta(\alpha)), \tag{2.10}$$

$$\theta(\sqrt{2}) = -\sqrt{2} = \beta_1\theta(\alpha) + \beta_2,$$

and

$$\sqrt{2} - \theta(\sqrt{2}) = 2\sqrt{2} = \beta_1\alpha + \beta_2 - \beta_1\theta(\alpha) - \beta_2 = \beta_1(\alpha - \theta(\alpha)). \tag{2.11}$$

Squaring (2.10)–(2.11) and taking norms from F:

$$7^2 = N_F(\gamma_1)^2 N_F(\alpha - \theta(\alpha))^2 \text{ and } 2^6 = N_F(\beta_1)^2 N_F(\alpha - \theta(\alpha))^2.$$

It follows from Corollary 2.3 on page 67 that $N_F(\alpha - \theta(\alpha)) = \pm 1$ since $N_F(\alpha - \theta(\alpha)) \in \mathbb{Z}$ and divides both 7^2 and 2^6. Thus, $N_F(\gamma_1) = \pm 7$. However, $\gamma_1 = a + b\sqrt{-14}$ for some $a, b \in \mathbb{Z}$ so $a^2 + 14b^2 = \pm 7$ which is impossible. We have shown that there is no $\alpha \in \mathfrak{O}_K$ such that $\mathfrak{O}_K = \mathbb{Z}[\alpha, \sqrt{-14}]$. Now if there is a $\beta \in \mathfrak{O}_K$ such that $\mathfrak{O}_K = \mathbb{Z}[\beta]$, then by setting $\alpha = \beta - \sqrt{-14} \in \mathfrak{O}_K$, we get $\mathfrak{O}_K = \mathbb{Z}[\alpha, \sqrt{-14}]$, which we have just shown to be impossible.

Biography 2.3 Ferdinand Georg Frobenius (1849–1917) was born on October 26, 1849 in Berlin-Charlottenburg, Prussia (now Germany), the son of a Protestant parson. He began his university studies at Göttingen for one semester, then returned to Berlin. At the University of Berlin, he was instructed by the likes of Kronecker, Kummer, and Weierstrass, the latter being his doctoral supervisor under whom he completed his dissertation in 1870. After some positions at secondary school level, he was appointed to the University of Berlin as an extraordinary professor of mathematics in 1874. Note that Frobenius somehow bypassed the usual requirement for a Habilitation—see Footnote 1.1 on page 23. The consensus is that this breach of usual strictness was due to Weierstrass' influence. In 1875, after only a year at Berlin, Frobenius took a position as ordinary professor at the Eidgenössische Polytechnikum in Zürich. Frobenius worked in Zürich for seventeen years where he married and raised a family. When Kronecker died in 1891, Weierstrass exerted further influence to have Frobenius fill the vacant chair at Berlin. For a quarter century, from 1892, Frobenius was the leading influence in Berlin where he died on August 3, 1917. Among his students were Edmund Landau, Robert Remak, and Issai Schur—see Biography 2.4. It is also noteworthy that Siegel was Frobenius' student from 1915 until his death.

Frobenius contributed to a vast array of mathematical areas, among them being analytic functions in series, linear differential equations, linear forms with integer coefficients, elliptic and Jacobi functions, biquadratic forms, and group theory, to name a very few. In group theory, he extended Sylow's theorems from permutation groups to abstract groups, and provided a proof of the structure theorem for finitely generated abelian groups. But arguably his most influential contribution may have been in the area of group characters which he ultimately linked to representations and essentially gave birth to representation theory of groups. Indeed, in 1911 Burnside wrote up Frobenius' character theory in his book *Theory of Groups of Finite Order.* Later, in other areas, such as quantum mechanics and theoretical physics, Frobenius's group theoretic representations found new applications.

Remark 2.4 Recall that Theorem 1.24 on page 39 is the *primitive element theorem* for algebraic number fields. In other words, any algebraic number field F is generated over $\mathbb{Q}$ by a primitive element $\alpha \in \overline{N}$. Therefore, Example 2.13 shows that *there cannot exist a Primitive Element Theorem for rings of integers* of algebraic number fields. Bases of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ for $\alpha \in \mathbb{A}$ are called *power integral bases*, and $\mathfrak{O}_F = \mathbb{Z}[\alpha]$ is called *monogenic.* Hence, not all rings of integers of algebraic number fields have a power integral basis, namely they are not all monogenic.

Biography 2.4 Issai Schur (1875–1941) was born on January 10, 1875 in Mogilyov, in the province of the same name in what was then the Russian Empire, and is now Belarus. His university education began in Berlin 1894, where Frobenius was one of his teachers early on and ultimately his doctoral advisor—see Biography 2.3. By 1901 he had obtained his doctorate on a topic involving representations of the general linear group over $\mathbb{C}$. His thesis introduced functions that we now call S-functions in honour of Schur's contribution. He began his professional life as a lecturer at Berlin University in 1903, and was ultimately promoted to full professor in Berlin in 1919. He held this position until ousted by the Nazis in 1935. While at Berlin, he directed students in many disparate directions including combinatorics, matrix theory, and soluble groups. Among his doctoral students were both Richard and Alfred Brauer (brothers), Robert Frucht, Bernard Neumann, Richard Rado, and Helmut Wieland. After Schur was dismissed from his chair in 1935, he was also pressured to resign from the Prussian Academy in 1938. The academy had honoured him in 1922 with his election to the august body. In 1939, he left for Palestine, broken by the stress and humiliation he suffered under persecution by the Nazis. Two years later, he died in Tel Aviv, Palestine (now Israel).

Among Schur's achievements was his discovery of what we now call the Schur multiplier. This proved to be well in advance of its time. Indeed, as evidence of this fact, some forty years later Eilenberg and MacLane defined cohomology groups, the second of which having coefficients in $\mathbb{C} - \{0\}$ is actually the Schur multiplier. However, Eilenberg and MacLane were unaware of this fact. Schur was interested in representation theory of groups, which began with his doctoral thesis and culminated many years later in his complete description of rational representations of the general linear group. He also worked on projective representations of groups and group characters. In this area he is known for what we now call Schur's Lemma that says: If R and S are two finite-dimensional irreducible representations of a group G and ϕ is linear map from R to S that commutes with the action of the group, then either ϕ is invertible, or $\phi = 0$.

His interests included Galois groups of certain classes of polynomials such as Hermite polynomials. He also worked in divergent series, function theory, integral equations, and number theory.

Exercises

2.32. Prove that a $\mathbb{Z}$-basis for $\mathfrak{O}_F$ in the sense of Definition 2.5 on page 70 is a basis in the sense of Definition A.7 on page 324.

2.33. Let R be a commutative ring with identity and let $\alpha_1, \ldots, \alpha_d \in R$. Prove that

$$\det(\alpha_j^{i-1}) = \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i).$$

2.34. Let G be a free abelian group of rank n with basis $\{g_1, \ldots, g_n\}$, and suppose that $A = (a_{i,j}) \in \mathcal{M}_{n \times n}(\mathbb{Z})$. Prove that the elements

$$h_i = \sum_{j=1}^{n} a_{i,j} g_j \quad (i = 1, 2, \ldots, n),$$

form a basis for G if and only if $A \in GL_n(\mathbb{Z})$. (See Definition A.18 on page 337.)

2.35. Using Exercise 2.31 on page 69, find $\mathrm{disc}(m_{\alpha,\mathbb{Q}})$ when $\alpha = \sqrt{2}$.

2.36. Let $F = \mathbb{Q}(\sqrt[4]{5}) = \mathbb{Q}(\alpha)$. Find $T_F(\alpha)$, $N_F(\alpha)$, and $\mathrm{disc}(m_{\alpha,\mathbb{Q}})$, where $m_{\alpha,\mathbb{Q}}(x) = x^4 - 5$. Also, show that $\mathrm{disc}(m_{\alpha,\mathbb{Q}}) = N_F(m'_{\alpha,\mathbb{Q}}(\alpha))$

2.37. Let $F = \mathbb{Q}(\sqrt[4]{5}, \zeta_4)$, and $\alpha = \sqrt[4]{5}$. Find $T_F(\alpha)$ and $N_F(\alpha)$.

2.38. Let $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ be a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Prove that

$$\mathrm{disc}(\mathcal{B}) = \mathrm{disc}(m_{\alpha,\mathbb{Q}})$$

where $m_{\alpha,\mathbb{Q}}(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

2.39. Let F be an algebraic number field with $\mathfrak{O}_F = \mathbb{Z}[\alpha]$. Prove that$\Delta\ _F = \mathrm{disc}(m_{\alpha,\mathbb{Q}})$ where $m_{\alpha,\mathbb{Q}}$ is the minimal polynomial of α over $\mathbb{Q}$.

2.40. Let R be a Dedekind domain, and let I be an R-ideal with

$$I = \prod_{j=1}^{r} \mathcal{P}_j^{a_j},$$

for distinct prime R-ideals $\mathcal{P}_j$. Prove that

$$|R/I| = \prod_{j=1}^{r} |R/\mathcal{P}_j|^{a_j}.$$

(*Hint: Use Theorem 1.21 on page 32 and exercises in that section.*)

2.41. If R is a commutative ring, and M is an R-module with N an R-submodule of M, then N is called a *pure submodule* of M if $N \cap rM = rN$ for all $r \in R$. Prove that if N is a direct summand of M, then N is a pure submodule.

2.42. With reference to Exercise 2.41, prove that if $\mathfrak{O}_F \subseteq \mathfrak{O}_K$ for algebraic number fields $F \subseteq K$, then $\mathfrak{O}_F$ is a pure $\mathbb{Z}$-submodule of $\mathfrak{O}_K$. Conclude that any integral basis for F can be extended to an integral basis for K.

2.43. Let F be a number field with basis $\{\beta_1, \beta_2, \ldots, \beta_n\}$ over $\mathbb{Q}$, and let $\alpha \in \mathfrak{O}_F$ be of degree d over $\mathbb{Q}$. Suppose that

$$\alpha\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j \text{ for } i = 1, 2, \ldots, n.$$

Prove that $|N_F(\alpha)| = |\det(a_{i,j})|$.

☆ 2.44. Let F be an algebraic number field with $\alpha \in \mathfrak{O}_F$, $\alpha \neq 0$. Prove that

$$|\mathfrak{O}_F/\langle\alpha\rangle| = |N_F(\alpha)|,$$

where the vertical bars on the left denote the cardinality of the quotient group, considered as free abelian groups, and the vertical bars on the right denote the absolute value of the norm. In particular, this says that if the right-hand side is 1, then as free abelian groups, $\mathfrak{O}_F = \langle\alpha\rangle$.

(*Hint: Show that the quotient of free abelian groups $\mathfrak{O}_F/\langle\alpha\rangle$ is finite by demonstrating that $\mathfrak{O}_F$ and its subgroup $\langle\alpha\rangle$ have the same rank. Then use Exercise 2.43.*)

(*This exercise is a segue into §2.4, where we extend the notion of* norm *from elements to ideals and generalize the notion developed for the quadratic case in §1.7.*)

2.4 Norms of Ideals

> *The mathematician may be compared to a designer of garments, who is utterly oblivious of the creatures whom his garments may fit. To be sure, his art originated in the necessity for clothing such creatures, but this was long ago; to this day a shape will occasionally appear which will fit into the garment as if the garment had been made for it. Then there is no end of surprise and delight!*
>
> *from page 142 of* The Two Realities *in* [63]
>
> **Tobias Dantzig (1884–1956) Baltic, German, American mathematician**

Exercise 2.40 as well as Exercise 2.44 provide a lead-in to the following important notion which will allow us to refine some developments from earlier in the text and will lead us naturally to ideal classes and the class group.

Definition 2.8 — Norms of Ideals

Let F be a number field and let I be an (integral) $\mathfrak{O}_F$-ideal. Then we define the norm of I to be

$$N(I) = |\mathfrak{O}_F/I|.$$

If $\mathfrak{I}$ is a *fractional ideal* of $\mathfrak{O}_F$ then, by Remark 1.13 on page 26, there is a nonzero integral $\mathfrak{O}_F$-ideal I and an element $\alpha \in \mathfrak{O}_F$ such that

$$\mathfrak{I} = \frac{1}{\alpha} I.$$

Then the norm of $\mathfrak{I}$ is given by

$$N(\mathfrak{I}) = \frac{N(I)}{N((\alpha))},$$

where $N(I)$ and $N((\alpha))$ are the norms of the integral ideals I and (α).

Notice that, via Exercise 2.40, we know that $|\mathfrak{O}_F/I|$ is finite. In fact, if

$$I = \prod_{j=1}^{r} \mathcal{P}_j^{a_j},$$

via Theorem 1.17 on page 28, then Exercise 2.40 tells us that

$$N(I) = \prod_{j=1}^{r} |\mathfrak{O}_F/\mathcal{P}_j|^{a_j}.$$

Since we have the prime power

$$|\mathfrak{O}_F/\mathcal{P}_j| = p_j^{f_j}$$

by Exercise 2.49 on page 86, then

$$N(I) = \prod_{j=1}^{r} p_j^{f_j a_j}.$$

Also, by Exercise 2.47, for any nonzero fractional $\mathfrak{O}_F$-ideals $\mathfrak{I}, \mathfrak{J}$,

$$N(\mathfrak{I}\mathfrak{J}) = N(\mathfrak{I})N(\mathfrak{J}).$$

Example 2.14 Let $F = \mathbb{Q}(\sqrt{10})$, with the $\mathfrak{O}_F$-ideals $\mathcal{P} = (2, \sqrt{10})$, $\mathcal{Q} = (3, 1 + \sqrt{10})$, and $\mathcal{Q}' = (3, 1 - \sqrt{10})$. (Recall that $\mathfrak{O}_F = \mathbb{Z}[\sqrt{10}]$ by Theorem 1.28 on page 45.) We will show that $\mathcal{P}$, $\mathcal{Q}$, and $\mathcal{Q}'$ are prime $\mathfrak{O}_F$-ideals, and compute their norms. Notice that by simply multiplying out the basis elements,

$$\mathcal{Q}\mathcal{Q}' = (9, 3(1 - \sqrt{10}), 3(1 + \sqrt{10})).$$

However, $3 = 9 - (3(1 - \sqrt{10}) + 3(1 + \sqrt{10})) \in \mathcal{Q}\mathcal{Q}'$, so $(3) \subseteq \mathcal{Q}\mathcal{Q}'$, and clearly the elements $9, 3(1 - \sqrt{10}), 3(1 + \sqrt{10})$ are in the ideal (3), so

$$(3) = \mathcal{Q}\mathcal{Q}',$$

by Theorem 1.30 on page 49. Similarly, $\mathcal{P}^2 = (4, 2\sqrt{10}, 10)$. However, $2 = 10 - 2 \cdot 4 \in \mathcal{P}^2$, so $(2) \subseteq \mathcal{P}^2$, and certainly the elements $4, 2\sqrt{10}, 10$ are in the ideal (2), so again by Theorem 1.30,

$$(2) = \mathcal{P}^2.$$

Hence,

$$(6) = \mathcal{P}^2\mathcal{Q}\mathcal{Q}', \tag{2.12}$$

so

$$N(\mathcal{P}^2\mathcal{Q}\mathcal{Q}') = N((6)) = 2^2 \cdot 3^2 = 36 = N_F(6). \tag{2.13}$$

Notice that this coincides with the fact given in Exercise 2.44 on page 82 since

$$|\mathfrak{O}_F/(6)| = |\mathfrak{O}_F/\langle 6\rangle| = N_F(6),$$

where the first quotient is that of a ring modulo an ideal, and the second quotient is as a free abelian group modulo a cyclic subgroup. We may also calculate $|\mathfrak{O}_F/\mathcal{P}|$ by counting its elements. Although there are other means of doing this, we explore this avenue for its instructive and illustrative value. First, we observe that $\mathcal{P}$ is maximal, for if

$$u + v\sqrt{10} \notin \mathcal{P} = \{2a + b\sqrt{10} : a, b \in \mathbb{Z}\},$$

then $u \in \mathbb{Z}$ is odd and $v \in \mathbb{Z}$ is arbitrary. Hence, we have the ideal equality,

$$(\mathcal{P}, u + v\sqrt{10}) = \mathbb{Z}[\sqrt{10}],$$

given that $u - 1 + v\sqrt{10} \in \mathcal{P}$, so

$$1 = u - 1 + v\sqrt{10} - (u + v\sqrt{10}) \in (\mathcal{P}, u + v\sqrt{10}).$$

By Theorem 1.10 on page 18, $\mathcal{P}$ is a prime $\mathfrak{O}_F$-ideal. Thus, every element of $\mathbb{Z}[\sqrt{10}]$ is either in $\mathcal{P}$ or is of the form $1 + \alpha$, where $\alpha \in \mathcal{P}$, so $|\mathbb{Z}[\sqrt{10}]/\mathcal{P}| = 2 = N(\mathcal{P})$. A similar argument shows that every element of $\mathbb{Z}[\sqrt{10}]$ is either in $\mathcal{Q}$ or is of one of the forms $3a + b - 1 + b\sqrt{10}$ or $3a + b - 2 + b\sqrt{10}$. Therefore,

$$|\mathbb{Z}[\sqrt{10}]/\mathcal{Q}| = 3 = N(\mathcal{Q}) = N(\mathcal{Q}') = |\mathbb{Z}[\sqrt{10}]/\mathcal{Q}'|.$$

Therefore, by Exercise 2.45 on page 86, $\mathcal{Q}$ is a prime $\mathfrak{O}_F$-ideal. Hence,

$$N(\mathcal{P}\mathcal{Q}) = 6 = N(\mathcal{P}\mathcal{Q}'),$$

from which we could have deduced (2.13).

Observe, as we did in Examples 1.9 and 1.11 on pages 4–5, that

$$6 = (4 + \sqrt{10})(4 - \sqrt{10}) = 2 \cdot 3$$

gives two distinct representations of the element 6 as a product of the irreducible elements $4 + \sqrt{10}$, $4 - \sqrt{10}$, 2, and 3. However, there is unique factorization of the ideals as given in (2.12).

The following employs Example 2.14 to illustrate Exercise 2.47 on the following page.

Example 2.15 Let $I = \mathcal{P}\mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are given in Example 2.14. Via Exercise 2.51,

$$I = \mathcal{P}\mathcal{Q} = (6, 2 - \sqrt{10}),$$

with

$$\mathcal{P}'\mathcal{Q}' = \mathcal{P}\mathcal{Q}' = (6, 2 + \sqrt{10}).$$

Let $\mathfrak{I}$ and $\mathfrak{J}$ be fractional $\mathfrak{O}_F$-ideals given by

$$\mathfrak{I} = \frac{1}{2}I \text{ and } \mathfrak{J} = \frac{1}{3}I'.$$

Then

$$N(\mathfrak{I}\mathfrak{J}) = N(\mathfrak{I})N(\mathfrak{J}) = \left(\frac{N(I)}{N_F(2)}\right)\left(\frac{N(I')}{N_F(3)}\right) = \left(\frac{6}{4}\right)\left(\frac{6}{9}\right) = 1,$$

so

$$\mathfrak{I}\mathfrak{J} = \mathbb{Z}[\sqrt{10}] = \mathfrak{O}_F.$$

The following essentially generalizes Exercise 2.44 on page 82, illustrated in Example 2.14.

Theorem 2.12 — Norms of Ideals and Discriminants

Suppose that F is a number field, and that I is a nonzero integral $\mathfrak{O}_F$-ideal. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis for I. Then

$$N(I)^2 = \frac{\text{disc}(\mathcal{B})}{\Delta_F}.$$

Proof. Let $\mathcal{B}_1 = \{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$-basis of $\mathfrak{O}_F$. Then for each $i = 1, \ldots, n$

$$\alpha_i = \sum_{j=1}^{n} z_{i,j}\beta_j, \quad (z_{i,j} \in \mathbb{Z}).$$

By the same reasoning as in the solution, provided on page 378, of Exercise 2.43,

$$N(I) = |\mathfrak{O}_F/I| = |\det(z_{i,j})|.$$

By Theorem 2.7 on page 71,

$$\text{disc}(\mathcal{B}) = (\det(z_{i,j}))^2\text{disc}(\mathcal{B}_1) = N(I)^2\Delta_F,$$

as required. □

An immediate consequence, which is essentially Exercise 2.44, is the following.

Corollary 2.8 If I is an integral $\mathfrak{O}_F$-ideal with $\alpha \in I$, then $N(I) = |N_F(\alpha)|$ if and only if $I = (\alpha)$.

Example 2.16 If $F = \mathbb{Q}(\sqrt{\Delta_F})$ and $\alpha = (a + b\sqrt{\Delta_F})/2 \in \mathfrak{O}_F$, then

$$N((\alpha)) = |N_F(\alpha)| = \frac{a^2 - b^2\Delta_F}{4}.$$

Example 2.17 By Exercise 2.49, $N(\mathcal{P}) = p^f$ for $f \in \mathbb{N}$, where $\mathcal{P}$ is an integral prime $\mathfrak{O}_F$-ideal, then norms of prime ideals are not necessarily primes in $\mathbb{Z}$—see Exercise 2.50. The exact nature of this power f will be settled when we discuss general ideal decomposition in number fields later in Chapter 5.

Exercises

2.45. Let F be a number field and I a nonzero $\mathfrak{O}_F$-ideal. Prove that if $N(I)$ is prime in $\mathbb{Z}$, then I is prime in $\mathfrak{O}_F$.

2.46. Let F be a number field and I, J nonzero integral $\mathfrak{O}_F$-ideals. Prove that

$$N(IJ) = N(I)N(J).$$

Conclude that if an integral ideal I_1 divides an integral ideal I_2, then $N(I_1) \mid N(I_2)$.

2.47. Let F be a number field and $\mathcal{I}, \mathcal{J}$ nonzero fractional $\mathfrak{O}_F$-ideals. Prove that

$$N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J}).$$

(*Note that, unlike the conclusion in Exercise 2.46, we cannot conclude that $N(\mathcal{J})$ divides $N(\mathcal{I}\mathcal{J})$* in $\mathbb{Z}$. *Example 2.15 on the previous page provides a counterexample to the contrary.*)

2.48. Let F be a number field and I a nonzero $\mathfrak{O}_F$-ideal. Prove that $I \mid (N(I))$, namely that $(N(I)) \subseteq I$.

2.49. Let F be a number field and let $\mathcal{P}$ be a nonzero prime $\mathfrak{O}_F$-ideal. Prove that $N(\mathcal{P}) = p^m$, where $\mathcal{P} \cap \mathbb{Z} = (p)$, for some $m \in \mathbb{N}$, where $m \le |F : \mathbb{Q}|$.

2.50. Suppose that $\alpha \in \mathfrak{O}_F$ is a nonzero nonunit element for a number field F. Prove that if $|N_F(\alpha)| = p$ where p is a prime in $\mathbb{Z}$ then α is a prime in $\mathfrak{O}_F$. Show that the converse fails to hold.

(*Hint: Use Theorems 1.8 on page 16 and 1.30 on page 49 as well as Exercises 2.44 on page 82 and 2.45 above in conjunction with Definition 2.8 on page 83.*)

(*Note that this substantially generalizes Exercises 1.5 on page 6 and 1.22 on page 14 and, in particular, shows that the assumption of UFD in Exercise 1.22 is not necessary. We had to wait until we had the machinery made possible by our developments to this point before we could provide this result since it is quite difficult with only elementary techniques.*)

2.51. Find all ideals in $\mathbb{Z}[\sqrt{10}]$ having norm 6.

2.52. Prove that for a Dedekind domain D, and an integral D-ideal I there are only finitely many integral D-ideals that divide I.

2.53. Let F be a number field and $n \in \mathbb{N}$ arbitrary but fixed. Prove that there exist only finitely many integral $\mathfrak{O}_F$-ideals I with $N(I) = n$.

2.54. Let F be a number field and let I be an integral $\mathfrak{O}_F$-ideal. Suppose that $n \in \mathbb{N}$ is the smallest positive integer in I. Prove that $n \mid N(I)$.

Chapter 3

Class Groups

Of all the ruins that of a noble mind is the most deplorable.
spoken by **Sherlock Holmes** *in* **His Last Bow (1917)** *from* The Dying Detective.
Sir Arthur Conan Doyle (1859–1930)
Scottish-born writer of detective fiction

In this chapter, we begin with the interplay between ideal and form class groups. This allows for a relatively simple proof of the finiteness of the class number in §3.2 for the quadratic case. This relatively easy approach is a segue into the general case involving the geometry of numbers in §3.3. Some of what follows is adapted from [54].

3.1 Binary Quadratic Forms

Lagrange was the first to introduce the theory of quadratic forms—see Biography 3.3 on page 93. The theory was later expanded by Legendre, and greatly magnified even later by Gauss—see Biographies 3.1 on page 89 and 3.5 on page 95. An *integral binary quadratic form* is given by

$$f(x, y) = ax^2 + bxy + cy^2 \text{ with } a, b, c \in \mathbb{Z}. \tag{3.1}$$

For simplicity, we may suppress the variables, and denote f by (a, b, c). The value a is called the *leading coefficient*, the value b is called the *middle coefficient*, and c is called the *last coefficient.* If $\gcd(a, b, c) = 1$, then we say that $f(x, y)$ is a *primitive* form.

The aforementioned three great mathematicians looked at the *representation problem*: Given a binary quadratic form (3.1), which $n \in \mathbb{Z}$ are represented by $f(x, y)$? In other words, for which n do there exist integers x, y such that $f(x, y) = n$? If $\gcd(x, y) = 1$, then we say that n is *properly represented* by $f(x, y)$. For instance, when studying criteria for the representation of a natural number n as sums of two squares, such as in [53, Section 6.1, pp. 243–251], a simple answer can be given. When looking at norm-forms $x^2 + ny^2 = m$, where $m, n \in \mathbb{Z}$, such as in [53, Section 7.1, pp. 265–273], the problem can be given a relatively simple answer for certain m, n. In general, there is no simple complete answer. Moreover, an even more general and difficult problem arises, namely when can an integer be represented by a binary quadratic form from a given set of such forms? The theory of binary quadratic forms deals with this question via the following notion. In the balance of our discussion, we use the term *form* to mean *binary quadratic form.*

Definition 3.1 — Equivalent Binary Quadratic Forms

Two forms $f(x, y)$ and $g(x, y)$ are said to be *equivalent* if there exist integers p, q, r, s, such that

$$f(x, y) = g(px + qy, rx + sy) \text{ and } ps - qr = \pm 1. \tag{3.2}$$

For simplicity, we may denote equivalence of f and g by $f \sim g$. If $ps - qr = 1$, then f and g are said to be *properly equivalent*, and if $ps - qr = -1$, they are said to be *improperly equivalent*. Two forms f and g are said to be in the same *equivalence class* or simply in the *same class*, if f is properly equivalent to g.

Remark 3.1 From Definition 3.1, equivalent forms represent the same integers, and the same is true for proper representation – see Exercise 3.1 on page 94. Moreover, since

$$\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = ps - qr = \pm 1,$$

this means that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}),$$

— see Exercise 1.59 on page 54. Note, as well, that proper equivalence means that $ps - qr = 1$ so

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}),$$

the subgroup of $\mathrm{GL}(2, \mathbb{Z})$ with elements having determinant 1. Properly equivalent forms are said to be related by a *unimodular transformation*, namely $X = px + qy$ and $Y = rx + sy$ with $ps - qr = 1$. Note as well, by Exercise 3.3 on page 94, proper equivalence of forms is an equivalence relation.

The notion of proper and improper equivalence is due to Gauss. Lagrange initiated the idea of equivalence, although he did not use the term. He merely said that one could be "transformed into another of the same kind," but did not make the distinction between the two kinds. Similarly Legendre did not recognize proper equivalence. However, there is a very nice relationship between proper representation and proper equivalence, since as Exercise 3.2 shows, the form $f(x, y)$ properly represents $n \in \mathbb{Z}$ if and only if $f(x, y)$ is properly equivalent to the form $nx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.

Example 3.1 For $f(x, y) = x^2 + 7y^2$, $n = 29 = 1 + 7 \cdot 2^2 = f(1, 2)$, $f(x, y)$ is properly equivalent to $g(x, y) = 29x^2 + 86xy + 64y^2$ since $f(x, y) = g(3x - y, -2x + y)$, where $p = 3, q = -1, r = -2, s = 1$. With reference to Remark 3.1, $X = 3x - y$, $Y = -2x + y$ represents a unimodular transformation.

The following notion is central to the discussion and links equivalent forms in another way.

Definition 3.2 — Discriminants of Forms

The *discriminant* of the form $f(x, y) = ax^2 + bxy + cy^2$ is given by

$$D = b^2 - 4ac.$$

If $D > 0$, then f is called an *indefinite* form. If $D < 0$ and $a < 0$, then f is called a *negative definite* form, and if $D < 0$ and $a > 0$, then f is called a *positive definite* form.

Remark 3.2 By Exercise 3.7 on page 94, if forms f and g have discriminants D and D_1, respectively, and $f(x,y) = g(px+qy, rx+sy)$, then $D = (ps-qr)^2 D_1$. Thus, equivalent forms have the same discriminant. However, forms with the same discriminant are not necessarily equivalent — see Exercise 3.8. Furthermore, if $f(x,y) = ax^2 + bxy + cy^2$, then by completing the square, we get

$$4af(x,y) = (2ax+by)^2 - Dy^2,$$

so when $D > 0$, the form $f(x,y)$ represents both positive and negative integers. This is the justification for calling such forms "indefinite." If $D < 0$ and $a < 0$, then $f(x,y)$ represents only negative integers, thus the reason they are called "negative definite," and if $a > 0$, then they represent only positive integers, whence the term "positive definite." Since we may change a negative definite form into a positive definite one by changing the signs of all the coefficients, it is sufficient to consider only positive definite forms when $D < 0$. *We will, therefore, not consider negative definite forms in any discussion hereafter.*

Biography 3.1 Adrien-Marie Legendre (1752–1833) was born on September 18, 1752, in Paris, France. He was educated at the Collège Mazarin in Paris. During the half decade 1775–1780, he taught along with Laplace (1749–1827) at École Militaire. He also took a position at the Académie des Sciences, becoming first *adjoint* in 1783, then *associé* in 1785, and his work finally resulted in his election to the Royal Society of London in 1787. In 1793, the Académie was closed due to the Revolution, but Legendre was able to publish his phenomenally successful book *Eléments de Géométrie* in 1794, which remained the leading introductory text in the subject for over a century. In 1795, the Académie was reopened as the *Institut National des Sciences et des Arts* and met in the Louvre until 1806. In 1808, Legendre published his second edition of *Théorie des Nombres*, which included Gauss's proof of the Quadratic Reciprocity Law. Legendre also published his three-volume work *Exercises du Calcul Intégral* during 1811–1819. Then his three-volume work *Traité des Fonctions Elliptiques* was published during the period 1825–1832. Therein he introduced the name "Eulerian Integrals" for beta and gamma functions. This work also provided the fundamental analytic tools for mathematical physics, and today some of these tools bear his name, such as *Legendre Functions.* In 1824, Legendre had refused to vote for the government's candidate for the Institute National, and for taking this position his pension was terminated. He died in poverty on January 10, 1833, in Paris.

Congruence properties of the discriminant of a form may provide us with information on representation. For instance, Exercise 3.9 tells us that congruence properties modulo 4 determine when an integer may be represented by forms with discriminant $D \equiv 0, 1 \pmod 4$. Furthermore, this means that we can take the equation $D = b^2 - 4ac$ and let $a = 1$ and $b = 0$ or 1 according to whether $D \equiv 0$ or $1 \pmod 4$, so then $c = -D/4$ or $-(D-1)/4$, respectively. Thus, we get a distinguished form of discriminant D given as follows.

Definition 3.3 — Principal Forms

If $D \equiv 0, 1 \pmod 4$, then $(1, 0, -D/4)$ or $(1, 1, -(D-1)/4)$, respectively, are called *principal forms* of discriminant D.

Remark 3.3 Via Exercise 3.10 on page 94, we see that if $D = -4m$, we get the form $f(x,y) = x^2 + my^2$. As we shall see, these forms are particularly important in the historical development of the representation problem. Indeed, entire books, such as [15] are devoted to discussing this issue. There is a general notion that allows us to look at canonical forms for more illumination of the topic. This is given in the following, which is due to Lagrange.

Definition 3.4 — Reduced Forms

A primitive form $f(x,y) = ax^2 + bxy + cy^2$, of discriminant D, is said to be *reduced* if the following hold.

(a) When $D < 0$ and $a > 0$,

$$|b| \le a \le c, \text{ and if either } |b| = a \text{ or } a = c, \text{ then } b \ge 0. \tag{3.3}$$

(b) When $D > 0$,

$$0 < b < \sqrt{D} \text{ and } \sqrt{D} - b < 2|a| < \sqrt{D} + b. \tag{3.4}$$

Note that since f is positive definite in part (a) of Definition 3.4, then by Definition 3.2 on page 88, both a and c are positive.

With the notion of reduction in hand, we have the following result, which provides us with a unique canonical representative for equivalence classes of positive definite forms.

Theorem 3.1 — Positive Definite and Reduced Forms

Every positive definite form is properly equivalent to a unique reduced form.

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive positive definite form. Let n be the least positive integer represented by f. By Exercise 3.2, there exist $B, C \in \mathbb{Z}$ such that $f \sim g$ properly, where $g(X,Y) = nX^2 + BXY + CY^2$. For any integer z, the transformation $X = x - zy$, $Y = y$ yields

$$g(X,Y) = nx^2 + (B - 2nz)xy + (nz^2 - Bz + C)y^2.$$

If we set $z = Ne\left(\frac{B}{2n}\right)$, the nearest integer to $B/(2n)$, then

$$-\frac{1}{2} < \frac{B}{2n} - z \le \frac{1}{2}, -n \le B - 2nz \le n, \text{ and } |B - 2nz| \le n.$$

Thus, if we set $b_1 = B - 2nz$ and $c_1 = nz^2 - Bz + C$, then

$$g(X,Y) = nx^2 + b_1xy + c_1y^2,$$

where $|b_1| \le n$. Thus, f is properly equivalent to g, g is positive definite, and $g(0,1) = c_1$. Therefore, g represents c_1, which implies $c_1 \in \mathbb{N}$, and $c_1 \ge n$ by the minimality of n. We have shown that f is properly equivalent to a reduced form. The balance of the result will follow from the next result.

Claim 3.1 Any two properly equivalent reduced forms must be identical.

Suppose that the form $f(x,y) = ax^2 + bxy + cy^2$ is reduced and properly equivalent to the reduced form $g(x,y) = Ax^2 + Bxy + Cy^2$ via the transformation

$$g(x,y) = f(px + qy, rx + sy)$$

with $ps - qr = 1$. We may assume without loss of generality that $a \geq A$. Also, a straightforward calculation shows that

$$\begin{aligned} A &= ap^2 + bpr + cr^2, \\ B &= 2apq + b(ps + qr) + 2crs, \\ C &= aq^2 + bqs + cs^2. \end{aligned} \tag{3.5}$$

Furthermore, we have

$$|b| \leq a \leq c. \tag{3.6}$$

Using (3.6) we get,

$$A = ap^2 + bpr + cr^2 \geq ap^2 - |bpr| + cr^2 \geq ap^2 - |bpr| + ar^2 = a(p^2 + r^2) - |bpr|. \tag{3.7}$$

However, since

$$p^2 + r^2 \geq 2|pr|, \tag{3.8}$$

then (3.7) is greater than or equal to $2a|pr| - |bpr| \geq a|pr|$, where the latter inequality follows from (3.6) again. We have shown that

$$A \geq a|pr|. \tag{3.9}$$

However, by assumption $a \geq A$, so $|pr| \leq 1$. If $|pr| = 0$, then

$$A = ap^2 + bpr + cr^2 \geq ap^2 + ar^2 = a(p^2 + r^2) \geq a,$$

so $A = a$. On the other hand, if $|pr| = 1$, then by (3.9), $A \geq a$, so again we get $A = a$.

It remains to show that $B = b$ since, once shown, it follows from Exercise 3.7 on page 94 that $C = c$, since $B^2 - 4AC = b^2 - 4ac$.

Suppose that $c > C$. Then $c > a$ since $C \geq A = a$. If $|pr| = 1$, then by (3.6)–(3.8), using the fact that $cr^2 > ar^2$, we deduce $A > a$, a contradiction. Hence, $|pr| = 0$. If $p = 0$, then using (3.7)–(3.8), we conclude that $A > a$, so $r = 0$. Since $ps - qr = 1$, then $ps = 1$. Moreover, since $|B| \leq A = a$ given that g is reduced, then from (3.6), we get $-a \leq |B| - |b| \leq a$. However, by (3.5), $B = 2apq + b$. It follows that $q = 0$ and $B = b$.

Lastly, suppose that $c < C$. By solving for a, b, c in terms of A, B, C we may reverse the roles of the variables and argue as above to the same conclusion that $B = b$. This completes the proof. □

Remark 3.4 The above says that there is a unique representative for each equivalence class of positive definite binary quadratic forms. Furthermore, by Exercise 3.11 on page 95, when $D < 0$, the number h_D of classes of primitive positive definite forms of discriminant D is finite, and h_D is equal to the number of reduced primitive forms of discriminant D. (Note that we prove $h_D < \infty$ in general for field discriminants in Theorem 3.7 on page 106.)

The case for indefinite forms is not so straightforward. The uniqueness issue, in particular, is complicated since we may have many reduced forms equivalent to one another, and the determination as to which reduced forms are equivalent is more difficult. Yet, we resolve this issue in Theorem 3.5 on page 101.

We conclude this section with a result due to Landau. This result precisely delineates the negative discriminants $D = -4n$ for which $h_D = 1$ and the proof is essentially that of Landau [35].

Biography 3.2 Edmund Landau (1877–1938) was born in Berlin, Germany on February 14, 1877. He studied mathematics at the University of Berlin, where his doctoral thesis, awarded in 1899, was supervised by Frobenius—see Biography 2.3 on page 80. Landau taught at the University of Berlin for the decade 1899–1909. In 1909, when he was appointed as ordinary professor at the University of Göttingen, he had amassed nearly seventy publications. His appointment at Göttingen was as a successor to Minkowski. Hilbert and Klein were also colleagues there—see Biography 3.4 on page 94. He became full professor there until the Nazis forced him out in 1933. On November 19, 1933, he was given permission to work at Groningen, Netherlands, where he remained until he retired on February 7, 1934. He returned to Berlin where he died of a heart attack on February 19, 1938.

Landau's major contributions were in analytic number theory and the distribution of primes. For instance, his proof of the prime number theorem, published in 1903, was much more elementary than those given by Poussin and Hadamard—see [53, §1.9, pp. 65–72] for a detailed overview. He established more than 250 publications in number theory and wrote several books on number theory, which were influential.

Theorem 3.2 — When $\mathbf{h_{-4n} = 1}$ for $\mathbf{n > 0}$

If $n \in \mathbb{N}$, then $h_{-4n} = 1$ if and only if $n \in \{1, 2, 3, 4, 7\}$.

Proof. Suppose that $h_{-4n} = 1$. $f(x, y) = x^2 + ny^2$ is clearly reduced since $a = 1$, $b = 0$, and $c = n \geq 1$ in Definition 3.4 on page 90. The result is clear for $n = 1$, so we assume that $n > 1$.

Case 3.1 n is not a prime power.

There exists a prime $p \mid n$ such that $p^d || n$, for $d \in \mathbb{N}$, where $||$ denotes *proper division*, also commonly called *exactly divides*, namely $p^d \mid n$, but $p^{d+1} \nmid n$ — see [53, Definition 1.3, p. 16] for the general notion. Let $a = \min(p^d, n/p^d)$ and $c = \max(p^d, n/p^d)$. Thus, $\gcd(a, c) = 1$, where $1 < a < c$, since n is not a prime power. Thus, $g(x, y) = ax^2 + cy^2$ is a reduced form of discriminant $-4ac = -4n$, so $h_{-4n} > 1$, given that $f(x, y)$ is also a reduced form of discriminant D, unequal to $g(x, y)$. This completes Case 3.1.

Case 3.2 $n = 2^\ell$ where $\ell \in \mathbb{N}$.

We need to show that $h_{-4n} > 1$ for $\ell \geq 3$. If $\ell = 3$, then $D = -32$ and the form $g(x, y) = 3x^2 + 2xy + 3y^2$ is a reduced form of discriminant $2^2 - 4 \cdot 3 \cdot 3 = -32$ not equal to $f(x, y)$, so we may assume that $\ell \geq 4$. Set

$$g(x, y) = 4x^2 + 4xy + (2^{\ell-2} + 1)y^2,$$

which is primitive since $\gcd(4, 4, 2^{\ell-2} + 1) = 1$, and reduced since $4 < 2^{\ell-2} + 1$. Moreover, the discriminant is

$$D = 4^2 - 4 \cdot 4 \cdot (2^{\ell-2} + 1) = -16 \cdot 2^{\ell-2} = -2^{\ell+2} = -4n,$$

but $g \neq f$. This completes Case 3.2.

Case 3.3 $n = p^k$ where $p > 2$ is prime and $k \in \mathbb{N}$.

Suppose that $n+1$ is not a prime power. Then, as in Case 3.1, we may write $n+1 = ac$, where $1 < a < c$ and $\gcd(a,c) = 1$. Thus,

$$g(x,y) = ax^2 + 2xy + cy^2$$

is a reduced form of discriminant $2^2 - 4ac = 4 - 4(n+1) = -4n$, and $f \neq g$, so $h_{-4n} > 1$.
Lastly, suppose that $n+1 = 2^t$ where $t \in \mathbb{N}$, observing that $n+1 = p^k + 1$ is even. If $t \geq 6$, then

$$g(x,y) = 8x^2 + 6xy + (2^{t-3}+1)y^2$$

is reduced since $8 < 2^{t-3} + 1$, and $\gcd(8, 6, 2^{t-3}+1) = 1$. Also, g has discriminant

$$D = 6^2 - 4 \cdot 8(2^{t-3}+1) = 4 - 4 \cdot 2^t = 4 - 4(n+1) = -4n,$$

and $f \neq g$, so $h_{-4n} > 1$. For $t \leq 5$ we have that $t \in \{1,2,3,4,5\}$ have the corresponding values

$$n \in \{1, 3, 7, 15, 31\}.$$

It remains to exclude $n = 15, 31$.
If $n = 15$, then n is not a prime power so this violates the hypothesis of Case 3.3. If $n = 31$, then the form

$$g(x,y) = 5x^2 + 4xy + 7y^2$$

is reduced since $b = 4 < a = 5 < c = 7$, and is primitive since $\gcd(a,b,c) = 1$. Lastly, the discriminant is

$$D = 4^2 - 4 \cdot 5 \cdot 7 = -4 \cdot 31.$$

This completes Case 3.3, and we are done for this direction of the proof.
For

$$n \in \{1, 2, 3, 4, 7\}$$

we get that $h_{-4n} = 1$ from Exercise 3.13. □

Biography 3.3 Joseph-Louis Lagrange (1736–1813) was born on January 25, 1736 in Turin, Sardinia-Piedmont (now Italy). Although Lagrange's primary interests as a young student were in classical studies, his reading of an essay by Edmund Halley (1656–1743) on calculus converted him to mathematics. While still in his teens, Lagrange became a professor at the Royal Artillery School in Turin in 1755. Lagrange sent Euler some of his work, including methods in the calculus of variations, then called *isoperimetrical problems*. This helped Euler to solve a problem upon which he had been working for years. Ultimately, Lagrange succeeded Euler as director of mathematics at the Berlin Academy of Science in 1766. Most of his time at Berlin was spent on celestial mechanics and the polishing of his masterpiece *Mécanique Analytique* or *Analytical Mechanics*, which was published in Paris in 1788. In this work, he spoke of the science of mechanics as the geometry of four dimensions, three dimensional physical space and one time coordinate. This was exploited by Einstein in 1915, when he developed his general theory of relativity. Lagrange left Berlin in 1787 to become a member of the Paris Academy of Science where he remained for the rest of his professional life. When he was fifty-six, he married a young woman, almost forty years younger than he, the daughter of the astronomer Lemonnier. She became his devoted companion until his death in the early morning of April 10, 1813 in Paris.

Exercises

3.1. Prove that equivalent forms represent the same integers, and the same is true for proper representation.

3.2. Prove that the form $f(x, y)$ properly represents n if and only if $f(x, y)$ is properly equivalent to the form $nx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$.

3.3. Prove that proper equivalence of forms is an equivalence relation, namely that the properties of reflexivity, symmetry, and transitivity are satisfied—see Exercise 1.8 on page 6.

Biography 3.4 David Hilbert (1862–1943) was born in Königsberg, Prussia, which is now Kaliningrad, Russia. He studied at the University of Königsberg where he received his doctorate under the supervision of Lindemann. He was employed at Königsberg from 1886 to 1895. In 1895, he was appointed to fill the chair of mathematics at the University of Göttingen, where he remained for the rest of his life. Hilbert was very eminent in the mathematical world after 1900 and it may be argued that his work was a major influence throughout the twentieth century. In 1900, at the Paris meeting of the Second International Congress of Mathematicians, he delivered his now-famous lecture *The Problems of Mathematics*, which outlined twenty-three problems that continue to challenge mathematicians today. Among these were Goldbach's conjecture and the Riemann hypothesis. Some of the Hilbert problems have been resolved and some have not, such as the two listed. Hilbert made contributions to many branches of mathematics including algebraic number theory, the calculus of variations, functional analysis, integral equations, invariant theory, and mathematical physics. Hilbert retired in 1930 at which time the city of Königsberg made him an honorary citizen. He died on February 14, 1943 in Göttingen.

3.4. Prove that improper equivalence is not an equivalence relation.

3.5. Prove that any form equivalent to a primitive form must itself be primitive.

3.6. Prove that if f represents $n \in \mathbb{Z}$, then there exists a $g \in \mathbb{N}$ such that $n = g^2 n_1$ and f properly represents n_1.

3.7. Suppose that $f \sim g$ where f is a form of discriminant D and g is a form of discriminant D_1, then $D = (ps - qr)^2 D_1 = D_1$ where $f(x, y) = g(px + qy, rx + sy)$.

3.8. Provide an example of forms with the same discriminant that are not equivalent.

3.9. Let $D \equiv 0, 1 \pmod 4$ and let n be an integer relatively prime to D. Prove that if n is properly represented by a primitive form of discriminant D, then D is a quadratic residue modulo $|n|$, and if n is even, then $D \equiv 1 \pmod 8$. Conversely, if n is odd and D is a quadratic residue modulo $|n|$, or n is even and D is a quadratic residue modulo $4|n|$, then $n \in \mathbb{Z}$ is properly represented by a primitive form of discriminant D.

3.10. Let $n \in \mathbb{Z}$ and $p > 2$ be a prime not dividing n. Prove that p is represented by a primitive form of discriminant $-4n$ if and only if the Legendre symbol equality $(-n/p) = 1$ holds.

(*Hint: Use Exercise 3.9.*)

3.11. For a fixed integer $D < 0$, let h_D be the number of classes of primitive positive definite forms of discriminant D. Prove that h_D is finite and is equal to the number of reduced forms of discriminant D.

3.12. Let $n \in \mathbb{N}$ and $p > 2$ be prime with $p \nmid n$. Prove that the Legendre symbol $(-n/p) = 1$ if and only if p is represented by one of the h_{-4n} reduced forms of discriminant $-4n$.

(*Hint: See Exercises 3.10–3.11 and Theorem 3.1 on page 90.*)

3.13. Prove that if $n \in \{1, 2, 3, 4, 7\}$, then $h_{-4n} = 1$.

Biography 3.5 Carl Friederich Gauss (1777–1855) is considered to be among the greatest mathematicians who ever lived. His genius was evident at the age of three, when he corrected an error in his father's bookkeeping. Also, at the age of eight, he astonished his teacher, Büttner, by rapidly adding the integers from 1 to 100 via the observation that the fifty pairs $(j+1, 100-j)$ for $j = 0, 1, \ldots, 49$ each sum to 101 for a total of 5050. By the age of fifteen, Gauss entered Brunswick Collegium Carolinum funded by the Duke of Brunswick to whom Gauss dedicated his masterpiece *Disquisitiones Arithmeticae* [20], published in 1801. In 1795, Gauss entered Göttingen University, and by the age of twenty achieved his doctorate, which contained the *Fundamental Theorem of Algebra*—see Theorem A.18 on page 334. His intimate friend as a student was Farkas (or Wolfgang) Bolyai (1775–1856). Both had tried to prove Euclid's parallel postulate, which is equivalent to the assumption that two converging lines must intersect. Although Bolyai gave up in frustration, Gauss had some ideas which, had he developed, would probably have led to his being credited with the discovery of non-Euclidean geometry, but the honour went to others. Gauss did publish his classic treatise *Disquisitiones circa superficies curvas* in 1827, which may be said to have initiated *differential geometry.* Gauss is credited with having invented two physical objects. One is the *heliotrope*, which worked by reflecting the sun's rays using a small telescope and an array of mirrors. The other, in collaboration with Wilhelm Weber (1804–1891), was the invention of the first operational telegraph.

He is also credited with computing, from some severely limited data, the orbit of *Ceres Ferdinandea*, discovered on January 1, 1801 by Piazzi, an Italian astronomer. Ceres was rediscovered by Zach, an astronomer and friend of Gauss, in June 1801, upon its reappearance from behind the sun, where Piazzi had lost his observation, leading to his small amount of data. Ceres was in virtually the exact position where Gauss had predicted! Although Gauss did not disclose it at the time, he used his method of *least squares approximation* to do the calculation. Indeed, some contend that this calculation is what made Gauss famous—see the MAA award-winning article [67] by Teets and Whitehead. However, in total, Gauss' accomplishments are too vast to discuss here in detail.

Gauss was married twice. He married his first wife, Johanna Ostoff on October 9, 1805. She died in 1809 after giving birth to their second son. His second wife was Johanna's best friend Minna, whom he married in 1810. She bore him three children. Gauss remained a professor at Göttingen until the early morning of February 23, 1855 when he died in his sleep.

3.2 Forms and Ideals

> *Happiness is not an ideal of reason but of imagination.*
>
> *from section two of*
> **Fundamental Principles of the Metaphysics of Ethics (1785)**
> **Immanuel Kant (1724–1804)**
> German philosopher

We study how to "multiply" forms, which is called "composition of forms" and relate it to ideal multiplication, which allows us to prove the finiteness of class numbers, for the quadratic case, in a relatively easy fashion. Also, we intimately link the class group of forms with that of ideals. The quadratic case is made transparent via binary quadratic forms, whereas the general case requires Minkowski's geometry of numbers in §3.3. Therein we prove the general case of finiteness of the ideal class number, motivated by the quadratic case—see Biography 3.6 on page 107.

First we need to develop some new notions. The first result allows us to select a canonical form in each equivalence class. For ease of elucidation, we restrict our attention to discriminants that are field discriminants–see Definition 1.33 on page 46.

Lemma 3.1 — Canonical Forms

Let $F = \mathbb{Q}(\sqrt{\Delta_F})$ be a quadratic field of discriminantΔ_F and let $m \in \mathbb{Z}$. Then every proper equivalence class of forms of discriminantΔ_F contains a primitive form with positive leading coefficient that is relatively prime to m.

Proof. Let $f = (a, b, c) \in C_{\Delta_F}$ and set

$$P_{a,m,c} = \prod_p p$$

where the product ranges over all distinct primes p such that $p \mid a$, $p \mid c$ and $p \mid m$. Also set

$$P_{a,m} = \prod_q q$$

where the product ranges over all distinct primes q such that $q \mid a$, $q \mid m$, but $q \nmid c$, set

$$P_{c,m} = \prod_r r$$

where the product ranges over all distinct primes r such that $r \mid c$, $r \mid m$, but $r \nmid a$, and set

$$S_m = \prod_s s$$

where the product ranges over all distinct primes s such that $s \mid m$ but $s \nmid P_{a,m,c}P_{a,m}P_{c,m}$. Then f represents

$$aP_{a,m}^2 + bP_{a,m}P_{c,m}S_m + c(P_{c,m}S_m)^2 = N. \tag{3.10}$$

Claim 3.2 $\gcd(N, m) = 1$.

Assume that a prime $t \mid N$ and $t \mid m$. Assume first that $t \mid a$. Then

$$t \mid P_{a,m,c}P_{a,m}$$

by the definition of the latter. If $t \mid P_{a,m}$, then by (3.10),

$$t \mid cP_{c,m}S_m.$$

However, $t \nmid P_{c,m}S_m$, so $t \mid c$. This contradicts the fact that $t \mid P_{a,m}$. Hence, $t \nmid P_{a,m}$, so $t \mid P_{a,m,c}$. It follows from (3.10) that

$$t \mid bP_{a,m}P_{c,m}S_m.$$

However, we have already shown that $t \nmid P_{a,m}$ and since $t \mid a$, then $t \nmid P_{c,m}$. Also, $t \mid P_{a,m,c}$, so $t \nmid S_m$, which implies that $t \mid b$. We have shown that $t \mid \gcd(a,b,c)$, contradicting that f is primitive. Hence, our initial assumption was false, namely, we have shown that $t \nmid a$. Therefore,

$$t \mid P_{c,m}S_m$$

by the definition of the latter. However, by (3.10), this implies that $t \mid aP_{a,m}$, a contradiction to what we have already shown. This secures the claim.

By Exercise 3.2 on page 94, Claim 3.2 tells us that f is properly equivalent to the form

$$g(x,y) = Nx^2 + Bxy + Cy^2$$

for some $B, C \in \mathbb{Z}$. If $N > 0$, then we have our result.

If $N < 0$, then by setting $x_0 = Bm\ell + 1$ and $y_0 = -2N\ell m$ for some $\ell \in \mathbb{Z}$,

$$g(x_0,y_0) = Nx_0^2 + Bx_0y_0 + Cy_0^2$$

$$= N(Bm\ell+1)^2 + B(Bm\ell+1)(-2N\ell m) + C(2N\ell m)^2$$

$$= NB^2m^2\ell^2 + 2NBm\ell + N - 2NB^2m^2\ell^2 - 2NB\ell m + 4CN^2\ell^2m^2$$

$$= N(1 - m^2\ell^2(B^2 - 4NC)) = N(1 - m^2\ell^2\Delta_F) = Q,$$

where $Q > 0$ if $N < 0$.

Since f represents

$$Q = N(1 - m^2\ell^2\Delta_F)$$

and Q is relatively prime to m, given that N and $1 - m^2\ell^2\Delta_F$ are relatively prime to m, then Exercise 3.2 gives us the complete result.

□

Now we make the connection with ideals.

Theorem 3.3 — Ideals and Composition of Forms

Suppose that $\mathfrak{O}_F$ is the ring of integers of a quadratic field of discriminantΔ_F and

$$f(x,y) = ax^2 + bxy + cy^2$$

is a primitive form, with $a > 0$, of discriminant$\Delta_F = b^2 - 4ac$. Then

$$I = (a, (-b + \sqrt{\Delta_F})/2)$$

is an $\mathfrak{O}_F$-ideal.

Proof. Since $\Delta_F = b^2 - 4ac$, then $b^2 \equiv \Delta_F \pmod{4a}$, so by Exercise 1.58 on page 54, I is an $\mathfrak{O}_F$-ideal. □

Note that in Theorem 3.3, we must exclude the case $a < 0$ since the norm of an ideal must be positive. This excludes the negative definite case, but in view of Remark 3.2 on page 89, there is no loss of generality. Moreover, in the indefinite case, with $a < 0$, we may circumvent this via the techniques given in the proof of Theorem 3.5 on page 101. In particular, see (3.14) on page 103.

Now we examine a means of associating forms in a unique way that allows us to "compose" them.

Definition 3.5 — United Forms

Two primitive forms $f = (a_1, b_1, c_1)$ and $g = (a_2, b_2, c_2)$ of discriminant D are called *united* if $\gcd(a_1, a_2, (b_1 + b_2)/2) = 1$.

Note that in Definition 3.5, since $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$, then b_1 and b_2 have the same parity so $(b_1 + b_2)/2 \in \mathbb{Z}$.

Theorem 3.4 — United Forms and Uniqueness

If $f = (a_1, b_1, c_1)$ and $g = (a_2, b_2, c_2)$ are united forms of discriminant D, where D is a field discriminant, then there exists a unique integer b_3 modulo $2a_1a_2$ such that

$$b_3 \equiv b_j \pmod{2a_j},\ j = 1, 2$$

and

$$b_3^2 \equiv D \pmod{4a_1a_2}.$$

Proof. This is an immediate consequence of the multiplication formulas for quadratic ideals on page 48. □

Now we are in a position to show how to multiply or compose forms.

Definition 3.6 — Dirichlet Composition[3.1]

Suppose that $f = (a_1, b_1, c_1)$ and $g = (a_2, b_2, c_2)$ are primitive, united forms of discriminant Δ_F whereΔ $_F$ is a field discriminant, $a_3 = a_1a_2$, b_3 is the value given in Theorem 3.4, and

$$c_3 = \frac{b_3^2 - \Delta_F}{4a_3}.$$

Then the *Dirichlet composition* of f and g is the form

$$f \circ g = G = (a_3, b_3, c_3).$$

[3.1] As a point of interest, there is a recent paper—see [4]—that shows how composition of binary quadratic forms leads to parametrizations of cubic, quartic, and quintic number fields. These, in turn, are shown to lead to formulas for counting the number of quartic and quintic number fields of bounded discriminant, as well as yet-to-be-determined connections with exceptional Lie groups and higher rank division algebras, for instance.

Remark 3.5 Note that

$$(a_3, (b_3 + \sqrt{\Delta_F})/2)$$

is an-$\mathfrak{O}_F$-ideal where $F = \mathbb{Q}(\sqrt{\Delta_F})$ by the multiplication formulas given on page 48. This shows the intimate connection between multiplication of quadratic ideals and composition of forms. Indeed, we need not restrict to field discriminants for this to work. We could expand the discussion to *non-maximal orders in quadratic fields* but then the delineation becomes more complicated, since we must rely on special conditions for invertibility of ideals and other considerations, all of which are satisfied in the so-called *maximal order* $\mathfrak{O}_F$. See [49] for the more general approach.

The form G, in Definition 3.6, is a form of discriminant

$$b_3^2 - 4a_3c_3 = b_3^2 - 4a_3(b_3^2 - \Delta_F)/(4a_3) = b_3^2 - b_3^2 + \Delta_F = \Delta_F.$$

Also it is primitive since if a prime $p \mid \gcd(a_3, b_3, c_3)$, then $p \mid a_1$ or $p \mid a_2$. Without loss of generality suppose it divides a_1. Then since $p \mid b_3$, we must have that $p \mid b_1$ since $b_3 \equiv b_1 \pmod{2a_1}$ by Theorem 3.4. However, since $p \mid c_3$ and $b_3^2 - 4a_3c_3 = D$, then $p^2 \mid \Delta_F$. However,Δ_F is a field discriminant so $p = 2$ and$\Delta_F \equiv 0 \pmod 4$ is the only possibility. By Definition 1.33 on page 46,$\Delta_F/4 \equiv 2, 3 \pmod 4$. If$\Delta_F/4 \equiv 2 \pmod 4$, then by Theorem 3.4, $b_3/2$ is even since

$$\left(\frac{b_3}{2}\right)^2 \equiv \frac{\Delta_F}{4} \pmod{a_1a_2},$$

given that $2 \mid a_1$. However, we have

$$\left(\frac{b_3}{2}\right)^2 - a_3c_3 = \frac{\Delta_F}{4}, \tag{3.11}$$

so since $2 \mid a_3$ and $2 \mid c_3$, then $\Delta_F/4 \equiv 0 \pmod 4$, a contradiction. Thus,

$$\Delta_F/4 \equiv 3 \pmod 4,$$

so by (3.11), $b_3/2$ is odd. However, (3.11) implies$\Delta_F/4 \equiv 1 \pmod 4$, a contradiction. We have shown that, indeed, G is a primitive form of discriminantΔ_F.

Remark 3.6 The *opposite* of

$$f = (a, b, c)$$

is

$$f^{-1} = (a, -b, c),$$

which is the *inverse* of f under Dirichlet composition. To see this we note that under the proper equivalence that sends (x, y) to $(-y, x)$, $f^{-1} \sim (c, b, a)$, for which $\gcd(a, c, b) = 1$. This allows us to choose a united form in the class of f^{-1} by Definition 3.5, so we may perform Dirichlet composition to get

$$f \circ f^{-1} = G = \left(ac, b, \frac{b^2 - \Delta_F}{4ac}\right) = (ac, b, 1).$$

Moreover, by Exercise 3.19 on page 107,

$$G \sim (1, 0, \Delta_F/4) \text{ when} \Delta_F \equiv 0 \pmod 4$$

and

$$G \sim (1, 1, (1 - \Delta_F)/4) \text{ when} \Delta_F \equiv 1 \pmod 4.$$

Thus, G is in the principal class by Corollary 3.1 on page 103.

We now need to introduce the ideal class group as a vehicle for defining the form class group since Theorem 3.3 on page 97 gives us the connection.

Definition 3.7 — Equivalence of Ideals

Let $\mathfrak{O}_F$ be the ring of integers of a number field F. Then two $\mathfrak{O}_F$-ideals I, J are said to be in the same *equivalence class* if there exist nonzero α,$\beta \in \mathfrak{O}_F$ such that $(\alpha)I = (\beta)J$ denoted by $I \sim J$.

Remark 3.7 By Theorem 1.26 on page 42 and Exercise 1.42 on page 33, we know that the set of all fractional $\mathfrak{O}_F$-ideals forms a multiplicative abelian group. If we denote this group by I_{Δ_F} and let P_{Δ_F} denote the group of principal fractional ideals, then the quotient group

$$\frac{I_{\Delta_F}}{P_{\Delta_F}} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$$

is called the *class group* of $\mathfrak{O}_F$, and

$$h_{\mathfrak{O}_\mathbf{F}} = |C_{\mathfrak{O}_\mathbf{F}}|,$$

is the ordinary or *wide class number*, which we will show to be finite. (First, we show finiteness in the (easier) quadratic case below—see Corollary 3.4 on page 106—then develop the geometry of numbers for the general case—see Theorem 3.11 on page 116.) Also, the class of an $\mathfrak{O}_F$-ideal I is denoted by $\mathbf{I}$. Thus a product of classes $\mathbf{IJ} = \mathbf{C}$ is the class belonging to any ideal $C = IJ$ formed by multiplying representatives $I \in \mathbf{I}$ and $J \in \mathbf{J}$. The identity element $\mathbf{1}$ is the *principal class*, namely all principal ideals $(\alpha) \sim (1)$, meaning $(\alpha) \in \mathbf{1}$. The existence of inverse classes $\mathbf{I^{-1}}$ for any class $\mathbf{I}$ is guaranteed by Exercise 1.43 and Theorem 1.26, namely $\mathbf{II^{-1}} = \mathbf{1}$. The commutative and multiplicative laws are clear, namely

$$\mathbf{IJ} = \mathbf{JI}, \text{ and } \mathbf{I}(\mathbf{JK}) = (\mathbf{IJ})\mathbf{K}, \text{ for } \mathfrak{O}_F\text{-ideals } \mathbf{I}, \mathbf{J}, \mathbf{K}.$$

Also the (integral) prime ideals are the generators of the class group. To see this let $\mathcal{I}$ be a fractional $\mathfrak{O}_F$-ideal and let $\alpha \in \mathfrak{O}_F$ be a nonzero element such that $\alpha I \subseteq \mathfrak{O}_F$. Then $\alpha\mathcal{I}$ is an integral $\mathfrak{O}_F$-ideal and

$$(\alpha\mathfrak{O}_F)^{-1}(\alpha\mathcal{I}) = \mathcal{I} = \prod_{j=1}^{r} \mathcal{P}_j^{a_j},$$

where the $a_j \in \mathbb{Z}$ are not necessarily positive and the $\mathcal{P}_j$ are distinct prime $\mathfrak{O}_F$-ideals as determined by Theorem 1.17 on page 28.

Note as well, that the *conjugate* ideal I' for I, first mentioned in Remark 1.24 on page 52, satisfies

$$\mathbf{I^{-1}} = \mathbf{I}'$$

—see Exercise 3.20 on page 107. In what follows, we will need to refine this concept a bit in order to be able to include indefinite binary quadratic forms. We let $P^+_{\Delta_F}$ denote the group of principal ideals (α) where $N_F(\alpha) > 0$—see Definition 2.4 on page 65. Then we let

$$\frac{I_{\Delta_F}}{P^+_{\Delta_F}} = \mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$$

known as the *narrow ideal class group*, or sometimes called the *strict* ideal class group. Also,

$$h^+_{\mathfrak{O}_\mathbf{F}} = |C^+_{\mathfrak{O}_\mathbf{F}}|,$$

is the *narrow ideal class number.* Clearly, when F is a complex quadratic field, then $\mathbf{C}_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$, since norms are necessarily positive in this case. In the real case we will learn more as we progress.

Note that in what follows, we use the symbol $\sim$ to denote both equivalence in the *ordinary* ideal class group $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ as well as equivalence of forms, but this will not lead to confusion when taken in context.

We use the symbol $\approx$ to denote *strict* equivalence in $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$. In other words, $I \approx J$ in $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$ when there exist α,$\beta \in \mathfrak{O}_F$ such that

$$(\alpha)I = (\beta)J$$

where $N_F(\alpha\beta) > 0$. The next result shows that this is tantamount to form equivalence.

Theorem 3.5 — Form and Ideal Class Groups

If C_{Δ_F} denotes the set of classes of primitive forms of discriminantΔ $_F$, where F is a quadratic field, then C_{Δ_F} is a group with multiplication given by Dirichlet composition and

$$C^+_{\mathfrak{O}_F} \cong C_{\Delta_F}.$$

Proof. Let $f = (a_1, b_1, c_1)$ and $g = (a_2, b_2, c_2)$, then by Exercises 3.2 and 3.9 on page 94, $g \sim (a_2', b_2', c_2')$ where $\gcd(a_1, a_2') = 1$. Thus, Dirichlet composition is defined so we may assume the f and g to be united, without loss of generality. Let $F = (a_3, b_3, c_3)$ be given as in Definition 3.6 on page 98. Then we know that via the ideal correspondence given in Theorem 3.3 on page 97,

$$(a_1, (b_1 - \sqrt{\Delta_F})/2)(a_2, (b_2 - \sqrt{\Delta_F})/2) = (a_3, (b_3 - \sqrt{\Delta_F})/2), \tag{3.12}$$

via the multiplication formulas on page 48. Thus, by Theorem 3.3 and (3.12), the Dirichlet composition of $f(x, y)$ and $g(x, y)$ corresponds to the product of the corresponding ideal classes, which shows that Dirichlet composition induces a well defined binary operation on C_{Δ_F}.

Note that in what follows, if we have strict equivalence of ideals given by

$$I = (a, (-b + \sqrt{\Delta_F})/2) \approx J = (a', (-b' + \sqrt{\Delta_F})/2), \tag{3.13}$$

then we may replace I by $(aa')I$ and J by $(a^2)J$, so we may assume without loss of generality that $a = a'$. Via Theorem 3.3, we may define a mapping from $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$ to C_{Δ_F} as follows

$$\tau : (a, (-b + \sqrt{\Delta_F})/2) \mapsto f = (a, b, c),$$

where $c = (b^2 - \Delta_F)/(4a)$. Moreover, by the above,

$$\tau(IJ) = \tau(I)\tau(J)$$

since we have shown that ideal multiplication corresponds to form multiplication. To see that τ is well defined, assume that $a' > 0$ and $b' \in \mathbb{Z}$ in (3.13). Thus, since there are δ,$\gamma \in \mathfrak{O}_F$ such that $(\delta)I = (\gamma)J$ where $N_F(\delta\gamma) > 0$ then

$$N_F(\delta/\gamma)N(I) = N(J) = a,$$

so $N_F(\delta/\gamma) = 1$. By Exercise 3.21 on page 107, there is a $\sigma \in \mathfrak{O}_F$ such that $\delta/\gamma = \sigma/\sigma'$. If

$$m_{\sigma,\mathbb{Q}}(x) = ux^2 + vx + w$$

is the minimal polynomial of σ over $\mathbb{Q}$, then it is for σ' as well, so $\tau(\sigma) = \tau(\sigma') = (u, v, w)$. Hence,

$$\tau((\delta/\gamma)I) = \tau((\sigma/\sigma'))\tau(I) = \tau(I).$$

Hence, it suffices to prove that $\tau(I) = \tau(J)$ when $I \sim J$. By Exercise 1.59 on page 54, there exists

$$X = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}),$$

such that

$$\begin{pmatrix} (-b+\sqrt{\Delta_F})/2 \\ a \end{pmatrix} = X\begin{pmatrix} (-b'+\sqrt{\Delta_F})/2 \\ a \end{pmatrix}.$$

Therefore,

$$p\left(\frac{-b'+\sqrt{\Delta_F}}{2}\right) + qa = \frac{-b+\sqrt{\Delta_F}}{2}$$

and

$$r\left(\frac{-b'+\sqrt{\Delta_F}}{2a}\right) + sa = a,$$

from which it follows that $r = 0$, $s = p = 1$, and $b = b' - 2qa$. Hence,

$$ax^2 + bxy + cy^2 = f(x,y) = g(x - qy, y) = a(x-qy)^2 + b'(x-qy)y + c'y^2,$$

so f and g are properly equivalent, namely they are in the same class in C_{Δ_F}, so τ is well defined. Now we establish the isomorphism.

First we show that τ is injective. Let

$$\tau(a, (-b+\sqrt{\Delta_F})/2) = f = (a,b,c) \sim \tau(a', (-b'+\sqrt{\Delta_F})/2) = g = (a', b', c')$$

in C_{Δ_F}. Since

$$(aa')(a, (-b+\sqrt{\Delta_F})/2) \approx (a^2)(a', (-b'+\sqrt{\Delta_F})/2)$$

as $\mathfrak{O}_F$-ideals, then we may assume that $a = a'$ without loss of generality since, if they are not equal, we may change the preimage to make it so as above. Now since

$$f\left(\frac{-b+\sqrt{\Delta_F}}{2a}, 1\right) = 0 = f\left(\frac{-b'+\sqrt{\Delta_F}}{2a}, 1\right),$$

then

$$\text{either } \frac{-b+\sqrt{\Delta_F}}{2a} = \frac{-b'+\sqrt{\Delta_F}}{2a} \text{ or } \frac{-b+\sqrt{\Delta_F}}{2a} = \frac{-b'-\sqrt{\Delta_F}}{2a},$$

given that these are the only two roots of $f(x,1) = ax^2 + bx + c = 0$. However, the latter is impossible by comparing coefficients so the former holds, from which we get that $b = b'$ so $c = c'$. Thus, τ is injective.

Lastly, we show that τ is surjective. Let

$$f(x,y) = ax^2 + bxy + cy^2$$

be a primitive form of discriminantΔ $_F$ and let

$$\alpha = (-b+\sqrt{\Delta_F})/(2a).$$

Then $f(\alpha, 1) = 0$, and $a\alpha \in \mathfrak{O}_F$. Define an $\mathfrak{O}_F$-ideal as follows. Set

$$I = \begin{cases} (a, a\alpha) & \text{if } a > 0, \\ (\sqrt{\Delta_F})(a, a\alpha) & \text{if } a < 0 \text{ and}\Delta_F > 0. \end{cases} \tag{3.14}$$

Therefore, $\tau(I) = (a, b, c)$ in the first instance is clear. In the second instance, we note that $I \approx (a, (-b + \sqrt{\Delta_F})/2)$ so

$$\tau(I) = \tau((a, (-b + \sqrt{\Delta_F})/2)) = (a, b, c).$$

Hence, τ is surjective and the isomorphism is established. □

Corollary 3.1 The identity element of C_{Δ_F} is the class containing the principal form $(1, 0, -\Delta_F/4)$ or $(1, 1, (1 - \Delta_F)/4)$ for$\Delta_F \equiv 0, 1 \pmod 4$, respectively.

Proof. Since

$$\tau(1, \sqrt{\Delta_F}/2) = (1, 0, -\Delta_F/4) \text{ or } \tau(1, (-1 + \sqrt{\Delta_F})/2) = (1, 1, (1 - \Delta_F)/4)$$

depending on congruence modulo 4 ofΔ_F, and the preimages are the identity elements in the principal class of $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$, then the images are clearly the identity elements in the principal class of C_{Δ_F}. □

Remark 3.8 When F is a complex quadratic field, as noted in Remark 3.7 on page 100,

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}^+_{\mathfrak{O}_\mathbf{F}},$$

so by Theorem 3.5 on page 101,

$$C_{\Delta_F} \cong \mathbf{C}_{\mathfrak{O}_\mathbf{F}}.$$

However, *in the real case*, this is not always true. For instance, by Exercise 3.14 on page 106, in the case where$\Delta_F = 12$, $C_{\Delta_F} \neq \{1\}$ and $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ has order 1. Yet by Theorem 3.5,

$$\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} \cong C_{\Delta_F}.$$

Indeed, the case where the field F is real and has a unit of norm -1 or F is complex, then by Exercise 3.17 on page 107, $\mathbf{C}_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}^+_{\mathfrak{O}_\mathbf{F}}$ always holds. When F is *real and has no such unit*, for instance as in the$\Delta_F = 12$ case, then by Exercise 3.16,

$$|\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} : \mathbf{C}_{\mathfrak{O}_\mathbf{F}}| = 2.$$

Note as well, by Theorem 3.5,

$$h^+_{\mathfrak{O}_\mathbf{F}} = h_{\Delta_F},$$

the number of classes of forms of discriminantΔ_F. Also by the above discussion, we have demonstrated the following.

Theorem 3.6 — Class Numbers of Forms and Ideals

IfΔ_F is the discriminant of a quadratic field F, then the class number of the form class group h_{Δ_F}, as well as that of both the wide ideal class group $h_{\mathfrak{O}_\mathbf{F}}$ and the narrow ideal class $h^+_{\mathfrak{O}_\mathbf{F}}$, is related by the following.

$$h_{\Delta_F} = h^+_{\mathfrak{O}_{\mathbf{F}}} = \left[\begin{array}{ll} h_{\mathfrak{O}_{\mathbf{F}}} & \text{if}\Delta_F < 0, \\ h_{\mathfrak{O}_{\mathbf{F}}} & \text{if}\Delta_F > 0 \text{ and there exists a } u \in \mathfrak{U}_F \\ & \text{with } N_F(u) = -1, \\ 2h_{\mathfrak{O}_{\mathbf{F}}} & \text{if}\Delta_F > 0 \text{ and there is } \textit{no } u \in \mathfrak{U}_F \\ & \text{with } N_F(u) = -1. \end{array}\right]$$

We conclude this section with a verification that h_{Δ_F} is finite. To do this we first need the following result.

Lemma 3.2 — A Form of Reduction

IfΔ_F is the discriminant of a quadratic field F, then in each class of C_{Δ_F} there is a form $f = (a, b, c)$ such that

$$|b| \le |a| \le |c|.$$

Proof. Let the form $f = (a_1, b_1, c_1)$ be in an arbitrary class of C_{Δ_F}. We may select an integer a such that $|a|$ is the least value from the set of nonzero integers represented by forms in the class of f. Then there exist $p, r \in \mathbb{Z}$ such that

$$a = a_1p^2 + b_1pr + c_1r^2. \tag{3.15}$$

If $g = \gcd(p, r)$, then a/g^2 is represented by f, contradicting the minimality of $|a|$ unless $g = 1$. Therefore, by the Euclidean algorithm, there exist integers q, s such that $ps - qr = 1$. Also,

$$f(px + qy, rx + sy) = a_1(px + qy)^2 + b_1(px + qy)(rx + sy) + c_1(rx + sy)^2 =$$
$$(a_1p^2 + b_1pr + c_1r^2)x^2 + (2pqa_1 + (ps + qr)b_1 + 2rsc_1)xy + (a_1q^2 + b_1qs + c_1s^2)y^2 =$$
$$ax^2 + Bxy + Cy^2,$$

where the coefficient for x^2 comes from (3.15),

$$B = (2pqa_1 + (ps + qr)b_1 + 2rsc_1),$$

and

$$C = a_1q^2 + b_1qs + c_1s^2.$$

Set $g(x, y) = ax^2 + Bxy + Cy^2$ and we have $f \sim g$ in C_{Δ_F}. We may select an integer m such that

$$|2am + B| \le |a|. \tag{3.16}$$

Thus,

$$g(x + my, y) = a(x + my)^2 + B(x + my)y + Cy^2 =$$
$$ax^2 + (2am + B)xy + (am^2 + Bm + C)y^2 =$$
$$ax^2 + bxy + cy^2,$$

with

$$b = 2am + B,$$

and

$$c = am^2 + Bm + C.$$

Set

$$h(x, y) = ax^2 + bxy + cy^2.$$

Then, since$\Delta_F = b^2 - 4ac$, given that $f \sim g \sim h$, then $c = 0$ implies that$\Delta_F = b^2$, a contradiction to the fact thatΔ_F is a field discriminant. Hence, since $h(0, 1) = c$, then $|c| \ge |a|$ by the minimality of $|a|$. Thus, from (3.16), we have the result. □

Corollary 3.2 Any form of discriminantΔ_F is equivalent to a reduced form of the same discriminant.

Proof. By Theorem 3.1 on page 90, we need only prove the result for$\Delta_F > 0$.

Claim 3.3 We may assume that (a, b, c) satisfies $|a| \leq |c|$ with

$$\sqrt{\Delta_F} - 2|a| < b < \sqrt{\Delta_F}.$$

By Lemma 3.2, we may select a form (a, b, c) such that $|b| \leq |a| \leq |c|$. If $\sqrt{\Delta_F} - 2|a| > b$, then by setting

$$m = \left\lfloor \frac{\sqrt{\Delta_F}}{2c} + \frac{b|c|}{2c} + \varepsilon \right\rfloor,$$

where

$$\varepsilon = \begin{cases} 1 & \text{if } c < 0, \\ 0 & \text{if } c > 0 \end{cases}$$

we get

$$\sqrt{\Delta_F} - 2|c| < -b + 2cm < \sqrt{\Delta_F}.$$

We now show that

$$(a, b, c) \sim (c, -b + 2cm, a - bm + cm^2). \tag{3.17}$$

Via the map τ in Theorem 3.5,

$$\tau : \left(a, \frac{-b + \sqrt{\Delta_F}}{2}\right) \mapsto (a, b, c),$$

and

$$\tau : \left(c, \frac{b - 2cm + \sqrt{\Delta_F}}{2}\right) \mapsto (c, -b + 2cm, a - bm + cm^2),$$

as $\mathfrak{O}_F$-ideals. However, by Exercise 1.60 on page 54

$$\left(c, \frac{b - 2cm + \sqrt{\Delta_F}}{2}\right) = \left(c, \frac{b + \sqrt{\Delta_F}}{2}\right),$$

so

$$\left(c, \frac{b - 2cm + \sqrt{\Delta_F}}{2}\right) \sim \frac{b - \sqrt{\Delta_F}}{2c} \cdot \left(c, \frac{b + \sqrt{\Delta_F}}{2}\right)$$
$$= \left(a, \frac{b - \sqrt{\Delta_F}}{2}\right) = \left(a, \frac{-b + \sqrt{\Delta_F}}{2}\right).$$

Since τ is a bijection, we have established (3.17).
If $|a - bm + cm^2| < |c|$, then we repeat the (finite) process, this time on

$$(c, -b + 2cm, a - bm + cm^2),$$

which must terminate in

$$(A, B, C) \sim (a, b, c)$$

with

$$|A| \leq |C| \text{ and } \sqrt{\Delta_F} - 2|A| < B < \sqrt{\Delta_F}.$$

This is Claim 3.3.

Therefore,

$$0 < \sqrt{\Delta_F} - b < 2|a| \le 2|c| = \frac{|\Delta_F - b^2|}{2|a|} < \left|\sqrt{\Delta_F} + b\right|.$$

Hence, $b > 0$, so $b^2 < \Delta_F$ and $|2a|^2 \le 4|ac| = \Delta_F - b^2 < \Delta_F$, so $2|a| < \sqrt{\Delta_F} < \sqrt{\Delta_F} + b$, from which it follows that (a, b, c) is reduced. □

Theorem 3.7 — $\mathbf{h_{\Delta_F}} < \infty$

If F is a quadratic field with discriminantΔ_F, then h_{Δ_F} is finite.

Proof. Note that by Exercise 3.11 on page 95, we need only consider the case where$\Delta_F > 0$. By Lemma 3.2 on page 104, for any class of C_{Δ_F}, there is a form $f = (a, b, c)$ in the class with

$$|ac| \ge b^2 = \Delta_F + 4ac > 4ac,$$

so $ac < 0$. Moreover, $4a^2 \le 4|ac| = -4ac = \Delta_F - b^2 \le \Delta_F$. Therefore,

$$|a| \le \sqrt{\Delta_F}/2, \tag{3.18}$$

so by Lemma 3.2,

$$|b| \le \sqrt{\Delta_F}/2. \tag{3.19}$$

Hence, by the bounds in (3.18)–(3.19), there can only be finitely many choices for the values a and b for a given discriminantΔ_F. Since $c = (b^2 - \Delta_F)/(4a)$, we have established the result. □

Corollary 3.3 — Positive Definite Forms and Reduction

When$\Delta_F < 0$, then the number of inequivalent positive definite forms with discriminant Δ_F is the same as the number of reduced forms.

Proof. See Exercise 3.11. □

Corollary 3.4 — $\mathbf{h_{\mathfrak{O}_F}} < \infty$

IfΔ_F is the discriminant of a quadratic field F, then $h_{\mathfrak{O}_F}$ is finite.

Proof. This follows from Theorem 3.6 on page 103 and Theorem 3.7. □

Exercises

3.14. Prove that when$\Delta_F = 12$ where $F = \mathbb{Q}(\sqrt{3})$, then the form $f = (-1, 0, 3)$ is not properly equivalent to the form $g = (1, 0, -3)$. This shows that $C_{\Delta_F} \ne \{1\}$. Show, however, that $\mathbf{C_{\mathfrak{O}_F}} = \{\mathbf{1}\}$.

(*Hint: See Corollary 1.1 on page 13 and Theorem 1.18 on page 29.*)

In Exercises 3.15-3.17, assume that Δ_F is the discriminant of a quadratic field F.

3.15. Let F be a real quadratic field and set

$$\alpha = \begin{cases} (1, 0, -\Delta_F/4) & \text{if}\Delta_F \equiv 0 \pmod 4, \\ (1, 1, (1 - \Delta_F)/4) & \text{if}\Delta_F \equiv 1 \pmod 4. \end{cases}$$

Prove that $\alpha \sim -\alpha$ in C_{Δ_F} if and only if $\mathfrak{O}_F$ has a unit u such that $N_F(u) = -1$.

3.16. Let F be a real quadratic field. Assume that $\mathfrak{O}_F$ does *not* have a unit of norm -1. Prove that $|\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} : \mathbf{C}_{\mathfrak{O}_\mathbf{F}}| = 2$.

(*Hint: Use Exercise 3.15.*)

3.17. Prove that $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ if F is either a complex quadratic field or F is a real quadratic field such that $\mathfrak{O}_F$ has a unit u with $N_F(u) = -1$.

(*Hint: Use Exercise 3.15.*)

3.18. Let F be a number field and let $h_{\mathfrak{O}_F}$ be the (wide) class number of F. Prove that if I is an integral $\mathfrak{O}_F$-ideal, then $I^{h_{\mathfrak{O}_F}} \sim 1$.

(*Hint: By Theorem 3.7,* $|h_{\mathfrak{O}_F}| < \infty$.)

3.19. Prove the assertion made in Remark 3.6 on page 99 that $(ac, b, 1) \sim (1, 0, \Delta_F/4)$ when $\Delta_F \equiv 0\,(\text{mod } 4)$ and $(ac, b, 1) \sim (1, 1, (1 - \Delta_F)/4)$ when$\Delta\ \ \equiv 1\,(\text{mod } 4)$.

(*Hint: When* $\Delta_F \equiv 0\,(\text{mod } 4)$*, in Definition 3.1 on page 88, select* $p = b/2$*,* $q = 1$*,* $r = -1$*, and* $s = 0$*, and when* $\Delta_F \equiv 1\,(\text{mod } 4)$ *select* $p = -(1 + b)/2$*,* $q = -1$*,* $r = 1$ *and* $s = 0$.)

3.20. Prove that $\mathbf{I}' = \mathbf{I}^{-1}$ in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$.

(*Hint: Use The Multiplication formulas on page 48.*)

3.21. Let u be a unit in $\mathfrak{O}_F$ such that $N_F(u) = 1$. Prove that there exists an $\alpha \in \mathfrak{O}_F$ such that $\alpha = u\alpha'$, where α' is the algebraic conjugate of α.

(*This exercise represents the quadratic analogue of Hilbert's Theorem 90*—see Biography 3.4 on page 94.)

In §3.3, we will be looking at the work of Minkowski in the geometry of numbers, which opens the door to establishing Dirichlet's celebrated unit theorem.

Biography 3.6 Hermann Minkowski (1864–1909) was born on June 22, 1864 in Alexotas of what was then the Russian empire, but is now Kaunas, Lithuania. He studied at the Universities of Berlin, then Königsberg where he received his doctorate in 1885. Yet, even before this, in 1883, both he and Henry Smith were jointly awarded the Grand Prize by the Academy of Sciences (Paris) for the solution of the problem of representations of an integer as a sum of five squares. Eisenstein knew of a formula for such representations in 1847, but never provided a proof.

Minkowski taught at Bonn, Königsberg, and Zürich, but in 1902, Hilbert created a chair for him at Göttingen where Minkowski stayed for the rest of his life. He pioneered the area we now call the *geometry of numbers.* This led to work on convex bodies and to packing problems. Furthermore, his geometric insights paved the way for modern functional analysis. At age 44, he died from a ruptured appendix on January 12, 1909 in Göttingen. Posthumously, in 1910, his most original work, begun in 1890, was first published as *Geometrie der Zahlen.*

Minkowski's main interests were in pure mathematics, especially continued fractions and quadratic forms. However, he is also known for having laid some groundwork for Einstein's relativity theory by thinking of space and time as linked together in a *four-dimensional space-time continuum*, from which he determined how to treat electrodynamics from a four-dimensional perspective.

3.3 Geometry of Numbers and the Ideal Class Group

> *The human heart likes a little disorder in its geometry.*
> *from chapter 26 of* **Captain Corelli's Mandolin (1994)**
> **Louis de Bernières (1954–)**
> British novelist and short-story writer

In this section, we introduce Minkowski's geometry of numbers in order to prove Dirichlet's celebrated unit theorem, which we use to establish the finiteness of the ideal class number. In §3.2 we used the notion of forms to deduce this finiteness in the quadratic case—see Biographies 3.6 on the previous page and 3.9 on page 121. The reader must be familiar with vector spaces and related notions in Appendix A.

Definition 3.8 — Lattices and Parallelotopes

Let $\ell_1, \ell_2, \ldots, \ell_m \in \mathbb{R}^n$, $m, n \in \mathbb{N}, m \leq n$ be $\mathbb{R}$-linearly independent vectors. If

$$L = \{\ell \in \mathbb{R}^n : \ell = \sum_{j=1}^{m} z_j \ell_j \text{ for some } z_j \in \mathbb{Z}\} = \mathbb{Z}[\ell_1, \ldots, \ell_m],$$

then L is called a *lattice of dimension m in $\mathbb{R}^n$*. When $m = n$, L is called a *full lattice.* In other words, a full lattice L is a free abelian group of rank n having a $\mathbb{Z}$-basis that is also an $\mathbb{R}$-basis for $\mathbb{R}^n$. Furthermore, the set

$$\mathbf{P} = \left\{ \sum_{j=1}^{n} r_j \ell_j : r_j \in \mathbb{R}, 0 \leq r_j < 1 \text{ for } j = 1, 2, \ldots, n \right\}$$

is called the *fundamental parallelotope*, or *fundamental parallelepiped*, or *fundamental domain* of L. An invariant—see Remark 3.9 below—of $\mathbf{P}$ is

$$V(\mathbf{P}) = |\det(\ell_j)|,$$

called the *volume of* $\mathbf{P}$, and also called the *discriminant of* L, denoted by $D(L)$.

Remark 3.9 In Definition 3.8, the term *invariant*, when applied to $\mathbf{P}$ means that, irrespective of which basis we choose for L, the volume of $\mathbf{P}$ remains the same. It is an easy exercise for the reader to verify that the determinant remains the same under change of basis using Exercise 2.34 on page 81. For the reader with a knowledge of measure theory, or Lebesgue measure in $\mathbb{R}^n$, the volume of a so-called *measurable set* $S \subseteq \mathbb{R}^n$ is called the measure of S. This measure can be shown to be the absolute value of the determinant of the matrix with rows ℓ_j for $j = 1, 2, \ldots, n$ for any basis $\{\ell_j\}$ of S. Thus, the Lebesgue measure of S is called the volume of S.

Example 3.2 $\mathbb{Z}^n$ is a full lattice in $\mathbb{R}^n$ for any $n \in \mathbb{N}$. In other words, a free abelian group of rank n in $\mathbb{R}^n$ is a full lattice. Hence, $\mathfrak{O}_F$ is a full lattice in $\mathbb{R}^n$, where $|F : \mathbb{Q}| = n$. Also, note that any lattice of dimension $m \in \mathbb{N}$ is full in $\mathbb{R}^m$.

We will now show that lattices as subsets of $\mathbb{R}^n$ are characterized by the following property. First, we remind the reader that if $s = (s_1, s_2, \ldots, s_n) \in \mathbb{R}^n$, then $|s| \le r$ means that $\sum_{j=1}^n s_j^2 \le r^2$, since $|s| = \left(\sum_{j=1}^n s_j^2\right)^{1/2}$, so $|s_j| \le r$ for each such j.

Definition 3.9 — Discrete Sets

Suppose that $S \subseteq \mathbb{R}^n$, $n \in \mathbb{N}$, $r \in \mathbb{R}^+$, the positive reals, and

$$\mathcal{S}_r = \{s \in \mathbb{R}^n : |s| \le r\}$$

is the *sphere* or *ball* in $\mathbb{R}^n$, with radius r, centered at the origin. Then S is called *discrete* if

$$|S \cap \mathcal{S}_r| < \infty,$$

for all $r \in \mathbb{R}^+$.

Theorem 3.8 — Lattices Are Discrete

Let $L \subseteq \mathbb{R}^n$, $L \ne \varnothing$. Then L is a lattice if and only if L is a discrete, additive subgroup of $\mathbb{R}^n$.

Proof. Let L be a lattice of dimension n, namely a full lattice in $\mathbb{R}^n$. If

$$L = \ell_1\mathbb{Z} \oplus \cdots \oplus \ell_n\mathbb{Z},$$

$\{\ell_1, \ldots, \ell_n\}$ is an $\mathbb{R}$-basis for $\mathbb{R}^n$. Thus, any $\alpha \in \mathbb{R}^n$ can be written in the form

$$\alpha = \sum_{j=1}^n r_j\ell_j \quad (r_j \in \mathbb{R}).$$

If $\alpha \in L \cap \mathcal{S}_r$ for any $r \in \mathbb{R}^+$, then each $r_j \in \mathbb{Z}$ and $|r_j| \le r$ for each $j = 1, 2, \ldots, n$. Hence, there exist only finitely many points in $L \cap \mathcal{S}_r$. In other words, L is discrete.

Conversely, assume that L is a discrete, additive subgroup of $\mathbb{R}^n$. We use induction on n. For $n = 1$, let $\{\ell\}$ be a basis for $\mathbb{R}$, namely $\mathbb{R}^1 = \mathbb{R}\ell$. Since $\mathcal{S}_r \cap L$ is finite for all $r \in \mathbb{R}^+$, there exists a smallest positive value r_1 such that $r_1\ell \in L$. Therefore, $\mathbb{Z}r_1\ell \subseteq L$. Since any $s \in \mathbb{R}$ may be written as $s = \left\lfloor \frac{s}{r_1} \right\rfloor r_1 + s_1r_1$, for some real number s_1 with $0 \le s_1 < 1$, then any $s\ell \in L$ may be written in the form $s\ell = nr_1\ell + s_1r_1\ell$, with $n = \left\lfloor \frac{s}{r_1} \right\rfloor \in \mathbb{Z}$, and $0 \le s_1 < 1$. Therefore, by the minimality of r_1, we must have that $s_1 = 0$, so $L = \mathbb{Z}[r_1\ell]$. This establishes the induction step. Assume the induction hypothesis, namely that any discrete subgroup of $\mathbb{R}^k$ for $k < n$ is a lattice, so we may assume that $L \subseteq \mathbb{R}^n$ is discrete and $L \not\subseteq \mathbb{R}^k$ for any $k < n$. Hence, we may choose a basis $\{\ell_1, \ldots, \ell_n\}$ of $\mathbb{R}^n$ with $\ell_j \in L$ for each $j = 1, 2, \ldots, n$. Set

$$V = \mathbb{R}[\ell_1, \ldots, \ell_{n-1}].$$

By the induction hypothesis,

$$L_V = L \cap V$$

is a lattice of dimension $n-1$. Let $\{\beta_1, \ldots, \beta_{n-1}\}$ be a basis for L_V. Therefore, any element $\gamma \in L$ may be written as

$$\gamma = \sum_{j=1}^{n-1} r_j\beta_j + r_n\ell_n \quad (r_j \in \mathbb{R}).$$

By the discreteness of L, there exist only finitely many such γ with all r_j bounded. Thus, we may choose one with $r_n > 0$, and minimal with respect to $|r_j| < 1$ for all $j \neq n$. Let β_n denote this choice. Thus,

$$\mathbb{R}^n = \mathbb{R}[\beta_1, \ldots, \beta_n].$$

Then for any $\delta \in L$,

$$\delta = \sum_{j=1}^{n} t_j \beta_j \quad (t_j \in \mathbb{R}).$$

Let

$$\sigma = \delta - \sum_{j=1}^{n} \lfloor t_j \rfloor \beta_j = \sum_{j=1}^{n} s_j \beta_j.$$

Therefore, $0 \leq s_j < 1$ for all $j = 1, \ldots, n$. By the minimality of r_n, we must have $s_n = 0$. Hence, $\sigma \in L_V$, so $\delta \in L_V \oplus \mathbb{Z}\beta_n$. This gives us in total that

$$L \subseteq L_V \oplus \mathbb{Z}\beta_n \subseteq L.$$

Therefore, $L = L_V \oplus \mathbb{Z}\beta_n$ is a lattice. □

We also need other fundamental notions from geometry.

Remark 3.10 In what follows, we use the fact that the volume of every bounded convex set exists, called *Blanschke's theorem.*

Definition 3.10 — Bounded, Convex, and Symmetric Sets

A set S in $\mathbb{R}^n$ is said to be *convex* if, whenever $s, t \in S$, the point

$$\lambda s + (1 - \lambda)t \in S$$

for all $\lambda \in \mathbb{R}$ such that $0 \leq \lambda \leq 1$. In other words, S is convex if it satisfies the property that, for all $s, t \in S$, the line segment joining s and t is also in S. The volume of a convex set S is given by the multiple integral

$$V(S) = \int_S \cdots \int dx_1 dx_2 \cdots dx_n$$

carried out over the set S.

A set S in $\mathbb{R}^n$ is said to be *bounded* if there exists a sufficiently large $r \in \mathbb{R}$ such that $|s| \leq r$ for all $s \in S$. Another way of looking at this geometrically is that S is bounded if it can fit into a sphere with center at the origin of $\mathbb{R}^n$ and radius r.

A set S in $\mathbb{R}^n$ is *symmetric*, sometimes called centrally symmetric, provided that, for each $s \in S$, we have $-s \in S$.

Remark 3.11 By Remark 3.10, the integral in Definition 3.10 always exists for convex sets.

Example 3.3 Clearly, ellipses and squares are convex in $\mathbb{R}^2$, but a crescent shape, for instance, is not. Also, an n-dimensional cube

$$S = \{s = (s_1, \ldots, s_n) \in \mathbb{R}^n : -1 \leq s_j \leq 1 \text{ for } j = 1, 2, \ldots, n\}$$

is a bounded, symmetric convex set, as is an n-dimensional unit sphere

$$\{s \in \mathbb{R}^n : |s| \leq 1\}.$$

Before proceeding to the main result, we need a technical lemma.

Lemma 3.3 — Translates and Volume

Let $S \subseteq \mathbb{R}^n$ be a bounded set and let L be an n-dimensional lattice. If the *translates* of S by L, given by

$$S_z = \{s + z : s \in S\},$$

for a given $z \in L$, are pairwise disjoint, namely

$$S_z \cap S_y = \varnothing,$$

for each $y, z \in L$ with $y \neq z$, then

$$V(S) \leq V(\mathbf{P})$$

where $\mathbf{P}$ is a fundamental parallelotope of L.

Proof. Since $\mathbf{P}$ is a fundamental parallelotope of L, we have the following description of S as a disjoint union:

$$S = \cup_{z \in L}(S \cap \mathbf{P}_{-z}),$$

where $\mathbf{P}_{-z} = \{x - z : x \in \mathbf{P}\}$, so it follows that

$$V(S) = \sum_{z \in L} V(S \cap \mathbf{P}_{-z}).$$

Since the translate of the set $S \cap \mathbf{P}_{-z}$ by the vector z is $S_z \cap \mathbf{P}$, then

$$V(S \cap \mathbf{P}_{-z}) = V(S_z \cap \mathbf{P}). \tag{3.20}$$

Therefore,

$$V(S) = \sum_{z \in L} V(S_z \cap \mathbf{P}).$$

If the translates S_z are pairwise disjoint, then so are $S_z \cap \mathbf{P}$. Since $S_z \cap \mathbf{P} \subseteq \mathbf{P}$, then Equation (3.20) tells us that

$$\sum_{z \in L} V(S_z \cap \mathbf{P}) \leq V(\mathbf{P}),$$

so the result is proved. □

Now we are in a position to state the central result of this section.

Theorem 3.9 — Minkowski's Convex Body Theorem

Suppose that L is a lattice of dimension n, and let $V(\mathbf{P})$ be the volume of a fundamental parallelotope $\mathbf{P}$ of L. If S is a symmetric, convex set in $\mathbb{R}^n$ with volume $V(S)$ such that

$$V(S) > 2^n V(\mathbf{P}),$$

there exists an $x \in S \cap L$ such that $x \neq 0$.

Proof. It suffices to prove the result for a bounded set S. To see this, we observe that when S is unbounded, we may restrict attention to the intersection of S with an n-dimensional sphere, centered at the origin, having a sufficiently large radius. Let

$$T = \tfrac{1}{2}S = \{s/2 : s \in S\}.$$

Then

$$V(T) = \frac{V(S)}{2^n} > V(\mathbf{P}).$$

If the translates $T_z = \frac{1}{2}S + z$ were pairwise disjoint, then by Lemma 3.3 on the preceding page, $V(\mathbf{P}) \geq V(T)$, a contradiction. Therefore, there must exist two distinct elements $s, t \in L$ such that

$$(\tfrac{1}{2}S - s) \cap (\tfrac{1}{2}S - t) \neq \varnothing.$$

Let $x, y \in S$ such that $\frac{1}{2}x - s = \frac{1}{2}y - t$. Then $t - s = \frac{1}{2}y - \frac{1}{2}x$. Since S is symmetric, then $-x \in S$, and since S is convex, then $\frac{1}{2}y + \frac{1}{2}(-x) \in S$. Hence, $t - s \in S \cap L$, and $t - s \neq 0$, as required. □

Remark 3.12 Some background to the language used above is in order. The term *convex body* refers to a nonempty, convex bounded and *closed* subset S of $\mathbb{R}^n$. The topological term "closed" means that every *accumulation point* of a sequence of elements in S must also be in S. This is tantamount to saying that S is closed in the topological space $\mathbb{R}^n$, with its natural topology. However, we do not need to concern ourselves here with this, since it is possible to state and prove the result without such topological considerations. It can also be shown that if S is "compact," namely every "cover" (a union of sets containing S) contains a *finite* cover, then it suffices to assume that $V(S) \geq 2^n V(\mathbf{P})$.

In order to prove the next result, we need a geometric interpretation of algebraic numbers in a canonical way. This is based upon the signature of a field given in Exercise 2.11 on page 63.

Definition 3.11 — Canonical Embedding of Number Fields

Let $\{r_1, r_2\}$ be the signature of a number field F. Suppose that $\theta_j(F) \subseteq \mathbb{R}$ for $j = 1, \ldots, r_1$ are the real embeddings of F in $\mathbb{C}$, and $\theta_j(F) \not\subseteq \mathbb{R}$ for $j = r_1 + 1, \ldots, r_1 + r_2$ are half of the complex embeddings of F in $\mathbb{C}$, chosen such that exactly one θ_j is taken from each complex conjugate pair $\theta_j, \overline{\theta_j}$ of such embeddings. Then for each $\alpha \in F$, define

$$\Theta_F : F \mapsto \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

by

$$\Theta_F(\alpha) = (\theta_1(\alpha), \ldots, \theta_{r_1}(\alpha), \theta_{r_1+1}(\alpha), \ldots, \theta_{r_1+r_2}(\alpha)).$$

Remark 3.13 With reference to Definition 3.11,Θ_F is a $\mathbb{Q}$-algebra monomorphism by Exercise 3.29 on page 121. Moreover, we may say more aboutΘ_F as follows.

$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ may be identified with $\mathbb{R}^n$, where $n = r_1 + 2r_2 = |F : \mathbb{Q}|$, since each complex component $\theta_j(\alpha)$ for $j = r_1 + 1, \ldots, r_1 + r_2$ may be replaced by a pair of components $\Re(\theta_j(\alpha)), \Im(\theta_j(\alpha))$ where $\Re(x)$ and $\Im(x)$ are the real and complex coefficients of

$$x = \Re(x) + \Im(x)\sqrt{-1} \in \mathbb{C}.$$

Hence,Θ_F may also be considered as an injection into the real vector space $\mathbb{R}^n$. We will have significantly more to say about this later.

We now provide an application of Minkowski's Convex Body Theorem to the relationship between discriminants and norms of algebraic integers, which will prove to be highly valuable later in the text as well.

Theorem 3.10 — Applications to Norms and Discriminants

Let $\{r_1, r_2\}$ be the signature of a number field F, with $|F : \mathbb{Q}| = n = r_1 + 2r_2$, and let M be a free abelian group ($\mathbb{Z}$-module) of finite index in $\mathfrak{O}_F$, namely $|\mathfrak{O}_F : M| = m \in \mathbb{N}$. Then there exists a nonzero $\alpha \in M$ such that

$$|N_F(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} n! n^{-n} \sqrt{|\Delta_F|} m.$$

Proof. Let $B \in \mathbb{R}^+$, and define a set:

$$S_B(r_1, r_2) = \left\{ (\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum_{j=1}^{r_1} |\alpha_j| + 2 \sum_{j=1}^{r_2} |\beta_j| \leq B \right\}.$$

Clearly S_B is bounded and symmetric. We now verify that it is convex. Let $a, b \in \mathbb{R}$ with $a \geq 0$, $b \leq 1$ and $a + b = 1$. Suppose that

$$(\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}), (\gamma_1, \ldots, \gamma_{r_1}, \delta_1, \ldots, \delta_{r_2}) \in S_B(r_1, r_2).$$

We now show that

$$(a\alpha_1 + b\gamma_1, \ldots, a\,\alpha_{r_1} + b\gamma_{r_1}, a\,\beta_1 + b\delta_1, \ldots, a\,\beta_{r_2} + b\delta_{r_2}) \in S_B(r_1, r_2).$$

We have

$$\sum_{j=1}^{r_1} |a\alpha_j + b\gamma_j| + 2\sum_{j=1}^{r_2} |a\beta_j + b\delta_j| \leq \sum_{j=1}^{r_1} a|\alpha_j| + \sum_{j=1}^{r_1} b|\gamma_j| + 2\sum_{j=1}^{r_2} a|\beta_j| + 2\sum_{j=1}^{r_2} b|\delta_j| \leq$$

$$a\left(\sum_{j=1}^{r_1} |\alpha_j| + 2\sum_{j=1}^{r_2} |\beta_j|\right) + b\left(\sum_{j=1}^{r_1} |\gamma_j| + 2\sum_{j=1}^{r_2} |\delta_j|\right) \leq aB + bB = (a+b)B = B,$$

so $S_B(r_1, r_2)$ is convex.

Claim 3.4

$$V(S_B(r_1, r_2)) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!}.$$

We use a double induction on $r_1$and r_2. For $r_1 = 1$ and $r_2 = 0$, we are looking at the length of the line segment $[-B, B]$ in $\mathbb{R}$, so in this case,

$$V(S_B(1, 0)) = 2B = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!}.$$

If $r_1 = 0$ and $r_2 = 1$, we are (essentially) looking at the disc of radius $B/2$ in $\mathbb{R}^2$ (since $\mathbb{R}^2 \cong \mathbb{C}$). Thus, in this case,

$$V(S_B(0, 1)) = \pi B^2/4 = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!}.$$

This completes the induction step. The induction hypothesis that we assume is

$$V(S_B(m, k)) = 2^m \left(\frac{\pi}{2}\right)^k \frac{B^n}{n!}, \text{ for any } m \leq r_1, \text{ and any } k \leq r_2.$$

First, we calculate $V(S_B(r_1+1, r_2))$. In this case, $S_B(r_1+1, r_2)$ is defined by the relations

$$|\alpha| + \sum_{j=1}^{r_1} |\alpha_j| + 2\sum_{j=1}^{r_2} |\beta_j| \leq B \text{ with } \alpha \in \mathbb{R}, \tag{3.21}$$

and $|\alpha| < B$ since $B \neq 0$. Therefore, using the induction hypothesis,

$$V(S_B(r_1+1, r_2)) = \int_{-B}^{B} V(S_{B-|\alpha|}(r_1, r_2))d\alpha = \frac{2^{r_1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \int_{-B}^{B} (B-|\alpha|)^{r_1+2r_2} d\alpha =$$

$$\frac{2^{r_1+1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \int_{0}^{B} (B-\alpha)^{r_1+2r_2} d\alpha = \frac{2^{r_1+1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \int_{0}^{B} x^{r_1+2r_2} dx,$$

after a simple change of variables and this equals,

$$\frac{2^{r_1+1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \frac{B^{r_1+2r_2+1}}{r_1+2r_2+1} = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!}.$$

To complete the claim, we now calculate $V_B(S(r_1, r_2+1))$. In this case, $S(r_1, r_2+1)$ is given by

$$\sum_{j=1}^{r_1} |\alpha_j| + 2\sum_{j=1}^{r_2} |\beta_j| + 2|\beta| \leq B,$$

where $\beta = x + y\sqrt{-1} \in \mathbb{C}$. Thus, in a similar fashion to the above, using the induction hypothesis, we have

$$V_B(S(r_1, r_2+1)) = \frac{2^{r_1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \int\int_{x^2+y^2 \leq B^2/4} (B - 2\sqrt{x^2+y^2})^{r_1+2r_2} dxdy,$$

and after a change of variables we get that the latter equals

$$\frac{2^{r_1}}{(r_1+2r_2)!}\left(\frac{\pi}{2}\right)^{r_2} \int_0^{B/2}\int_0^{2\pi} (B-2\omega)^{r_1+2r_2}\omega du d\omega =$$

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{(r_1+2r_2)!} \int_0^{B/2} (B-2\omega)^{r_1+2r_2}\omega d\omega.$$

Letting $2\omega = z$ and using integration by parts, we deduce

$$\int_0^{B/2} (B-2\omega)^{r_1+2r_2}\omega d\omega = \frac{B^{r_1+2r_2+2}}{4(r_1+2r_2+1)(r_1+2r_2+2)}.$$

Hence,

$$V_B(S(r_1, r_2+1)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1} \frac{B^{r_1+2r_2+2}}{(r_1+2r_2+2)!},$$

and Claim 3.4 is proved.

Let ϵ be arbitrarily chosen in $\mathbb{R}^+$, and define $B > 0$ by

$$B^n(\epsilon) = B^n = \left(\frac{4}{\pi}\right)^{r_2} n! m\sqrt{|\Delta_F|} + \epsilon. \tag{3.22}$$

Then by Claim 3.4,

$$V(S_B) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{B^n}{n!} = 2^{r_1+r_2} m\sqrt{|\Delta_F|} + \frac{\epsilon 2^{r_1}(\pi/2)^{r_2}}{n!} > (2^{-r_2} m\sqrt{|\Delta_F|})2^n. \tag{3.23}$$

We have one more result to establish that will allow us to invoke Minkowski's Convex Body Theorem via (3.23).

Claim 3.5 $V(\Theta_F(M)) = 2^{-r_2} m\sqrt{|\Delta_F|}$

SinceΘ $_F$ injects $\mathfrak{O}_F$ into $\mathbb{R}^n$ in a natural way—see Remark 3.13 on page 112—thenΘ $_F(\mathfrak{O}_F)$ is a full lattice in $\mathbb{R}^n$. If $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for F, then the $\Theta_F(\alpha_i)$ are $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^n$. Let θ_j for $j = 1, 2, \ldots, n$ be the embeddings of F in $\mathbb{C}$, and let ℓ_i denote the vector,

$$(\theta_1(\alpha_i), \ldots, \theta_{r_1}(\alpha_i), \Re(\theta_{r_1+1}(\alpha_i)), \Im(\theta_{r_1+1}(\alpha_i)), \ldots, \Re(\theta_{r_1+r_2}(\alpha_i)), \Im(\theta_{r_1+r_2}(\alpha_i)).$$

Then with the ℓ_i as row vectors,

$$V(\Theta_F(\mathfrak{O}_F)) = \det(\ell_i) = (2\sqrt{-1})^{-r_2}\det(\theta_j(\alpha_i)) = 2^{-r_2}|\det(\theta_j(\alpha_i))| = 2^{-r_2}\sqrt{|\Delta_F|},$$

since for any $y \in \mathbb{C}$,

$$\Re(y) = (y + \overline{y})/2, \text{ and } \Im(y) = (y - \overline{y})/(2\sqrt{-1}).$$

Now Claim 3.5 follows by induction on m.

By Claim 3.5, there exists a nonzero $\alpha = \alpha(\epsilon)$ in M such thatΘ $_F(\alpha) \in S_B$. Thus, since

$$|N_F(\alpha)| = \prod_{j=1}^{r_1} |\theta_j(\alpha)| \prod_{j=r_1+1}^{r_1+r_2} |\theta_j(\alpha)|^2,$$

then by the Arithmetic-Geometric Mean Inequality given on page 339,

$$|N_F(\alpha)| \le \left[\frac{1}{n}\sum_{j=1}^{r_1}|\theta_j(\alpha)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\theta_j(\alpha)|\right]^n \le \frac{B^n}{n^n},$$

where the last inequality is from Equation (3.21). Therefore, by (3.22),

$$|N_F(\alpha)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} m\sqrt{|\Delta_F|} + \frac{\epsilon}{n^n}. \tag{3.24}$$

Note that if ϵ is in the interval $(0, 1)$, there are only finitely many possibilities for $\alpha = \alpha(\epsilon)$. Hence, there exists an $\alpha_0 \in M$ such that Equation (3.24) holds for all positive ϵ. Thus,

$$|N_F(\alpha_0)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} m\sqrt{|\Delta_F|},$$

as required. □

Theorem 3.10 will be applied below to the problem of proving the finiteness of the cardinality of the class group. Thus, we restate it as follows, in terms of ideals, which we may invoke directly for convenience.

Corollary 3.5 Let F be a number field with $|F : \mathbb{Q}| = n = r_1 + 2r_2$, where $\{r_1, r_2\}$ is the signature of F. Then for any integral $\mathfrak{O}_F$-deal I, there exists a nonzero $\alpha \in I$ such that

$$|N_F(\alpha)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_F|} N(I). \tag{3.25}$$

For what ensues, the reader is reminded of Definition 3.7 and Remark 3.7 on page 100.

Theorem 3.11 — Finiteness of the Ideal Class Group
If F is a number field, then $h_{\mathfrak{O}_F} = |\mathbf{C}_{\mathcal{O}_\mathbf{F}}| < \infty$.

Proof. Via Remark 1.13 on page 26 and Definition 3.7, every ideal class $\mathbf{H}$ of fractional $\mathfrak{O}_F$-ideals H contains an integral $\mathfrak{O}_F$-ideal I. Also, there exists an integral ideal $J \in \mathbf{I^{-1}} \in \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ so $IJ \sim 1$. By Corollary 3.5, there exists a nonzero $\alpha \in J$ such that

$$|N_F(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_F|} N(J).$$

Since $J \mid (\alpha)$, we may set $H = \alpha J^{-1}$, so $H \sim I$ and via Corollary 2.8 on page 85,

$$N(H) = \frac{|N_F(\alpha)|}{N(J)} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_F|}.$$

By Exercise 2.53 on page 86, there are only finitely many integral ideals with a given norm, so there are only finitely many choices for J. Given that $\mathbf{I} = \mathbf{J} = \mathbf{H}$, then there are only finitely many choices for the classes $\mathbf{H}$, namely $|\mathbf{C}_{\mathfrak{O}_\mathbf{F}}| < \infty$. □

Immediately from the proof of Theorem 3.11, we have the following important fact.

Corollary 3.6 If F is a number field whereΔ $_F$ is the discriminant of F and $|F : \mathbb{Q}| = n$ with signature $\{r_1, r_2\}$, then every ideal class in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ contains a nonzero integral ideal I such that

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_F|}. \tag{3.26}$$

The right-hand side of (3.26) is a distinguished quantity.

Definition 3.12 — The Minkowski Bound
If F is a number field, the quantity

$$M_F = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_F|}$$

is called the *Minkowski bound*, where Δ_F is the discriminant of F and $|F : \mathbb{Q}| = n$ with signature $\{r_1, r_2\}$.

Remark 3.14 Corollary 3.6 tells us that every ideal class in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ has a nonzero integral ideal with norm less than M_F. We can say more. Since $N(I) \geq 1$ for any integral ideal, then by Corollary 3.6,

$$|\Delta_F| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2} \tag{3.27}$$

which is Minkowski's lower discriminant bound. Moreover, if $n > 1$, namely for $F \neq \mathbb{Q}$, $|\Delta_F| > 1$. We can say more as follows.

Corollary 3.7 For any number field F with $|F : \mathbb{Q}| = n$,

$$|\Delta_F| > \left(\frac{11}{12}\right)^2 \left(\frac{\pi e^2}{4}\right)^n (2\pi n)^{-1}.$$

Proof. By Stirling's Formula—see Equation (A.7) on page 339—

$$\frac{n^n}{n!} = \frac{e^{-\alpha/(12n)+n}}{\sqrt{2\pi n}},$$

for some $\alpha \in \mathbb{R}$ is located in the interval $(0, 1)$. Using (3.27), and the fact that

$$e^{\alpha/(12n)} < e^{1/12} < \sum_{j=0}^{\infty}\left(\frac{1}{12^j}\right) = 12/11,$$

we get

$$|\Delta_F| > \left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{n^n}{n!}\right)^2 = \left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{e^{n-\alpha/(12n)}}{\sqrt{2\pi n}}\right)^2 >$$

$$\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{11e^n}{12}\right)^2 (2\pi n)^{-1} \geq \left(\frac{11}{12}\right)^2\left(\frac{e^2\pi}{4}\right)^n (2\pi n)^{-1},$$

where the last inequality follows from the fact that

$$\left(\frac{\pi}{4}\right)^{2r_2} \geq \left(\frac{\pi}{4}\right)^n,$$

since $\pi/4 < 1$. □

Corollary 3.8 For a number field F with discriminantΔ $_F$,

$$\lim_{n\to\infty} \min_{|F:\mathbb{Q}|=n} \{|\Delta_F|\} = \infty. \tag{3.28}$$

Proof. Since $(\pi e^2)/4 > 5$, then $((\pi e^2)/4)^n > n$, so by Corollary 3.7 we have the result. □

This fact places us in a position to present the following classical result due to Hermite, who published the result in *Crelle's Journal* in 1857.

Biography 3.7 Charles Hermite (1822–1901) was born on December 24, 1822 in Dieuze, Lorraine, France. He was educated at École Polytechnique, where he later taught. He is perhaps best known for his proof, published in *Comptes Rendus de l'Académie des Sciences* in 1873, that e is a transcendental number. Using similar ideas to those of Hermite, C.L.F. Lindemann (1852–1939) produced a proof appearing in a paper entitled "Über die Zahl π," published in *Mathematische Annalen* in 1882, that π is also transcendental. (Lindemann is also known for having published two invalid "proofs" of FLT in 1901 and 1907.) A number of other mathematical entities bear Hermite's name: Hermitian matrices, Hermite polynomials, Hermite differential equations, and Hermite's formula of interpolation. On the human side, Hermite was a friend and supporter of Georg Cantor, when the latter was suffering his many nervous breakdowns. Also, Poincaré was Hermite's best known student. Hermite died on January 14, 1901 in Paris, France.

Theorem 3.12 — Hermite's Theorem on Discriminants

There are only finitely many number fields having a given discriminant $d \in \mathbb{Z}$.

Proof. By Equation (3.28), for a given $d \in \mathbb{Z}$, there exists a $d_0 \in \mathbb{N}$ such that if $n \geq d_0$, then

$$\left(\frac{11}{12}\right)^2 \left(\frac{\pi e^2}{4}\right)^n (2\pi n)^{-1} > |d|.$$

Therefore, if $|F : \mathbb{Q}| \geq d_0$, then $|\Delta_F| > |d|$. Hence, it suffices to prove that for an arbitrarily chosen but fixed $n, d \in \mathbb{N}$, there exist only finitely many number fields F such that $|\Delta_F| \leq |d|$ and $|F : \mathbb{Q}| = n$. By Remark 3.14 on page 116, the result is true for $|d| = 1$. Assume that $d > 1$. Then the case $r_1 = 1$ and $r_2 = 0$ is impossible. If $r_1 = 0$ and $r_2 = 1$, then $n = 2$, so $F = \mathbb{Q}(\sqrt{D})$ for some *squarefree* $D < 0$. By Definition 1.33 on page 46,$\Delta\ _F = 4D$ or $\Delta_F = D$, so there is at most one quadratic field with$\Delta\ _F = -d$. We may now assume that $r = r_1 + r_2 > 1$. The balance of the proof is devoted to proving the existence of a primitive element for F that comes from a finite set. In other words, we now establish the existence of an $\delta \in F$ such that $F = \mathbb{Q}(\delta)$ with δ in a fixed finite set depending only on d. To this end, we define the following sets, broken down into two cases.

Case 3.4 $r_1 \neq 0$

Define the set $\mathcal{S}_1$ in $\mathbb{R}^n$ by

$$\{(\alpha_1, \ldots, \alpha_{r_1}, \beta_{r_1+1}, \gamma_{r_1+1}, \ldots, \beta_r, \gamma_r) : |\alpha_1| < \sqrt{d+1}, |\alpha_i| < 1$$

$$\text{for } i = 2, 3, \ldots\ldots, r_1, \text{ and } \beta_j^2 + \gamma_j^2 < 1 \text{ for } j = r_1 + 1, \ldots, r\}.$$

We now show that $\mathcal{S}_1$ is convex. Let $a, b \in \mathbb{R}$ with $a \geq 0$, $b \leq 1$, and $a + b = 1$. Suppose that

$$(\alpha_1, \ldots, \alpha_{r_1}, \beta_{r_1+1}, \gamma_{r_1+1}, \ldots, \beta_r, \gamma_r), (\delta_1, \ldots, \delta_{r_1}, \rho_{r_1+1}, \sigma_{r_1+1}, \ldots, \rho_r, \sigma_r) \in \mathcal{S}_1.$$

For $j = 2, 3, \ldots, r_1$, we have

$$|a\alpha_j + b\delta_j| \leq a|\alpha_j| + b|\delta_j| < a + b = 1,$$

$$|a\alpha_1 + b\delta_1| \leq a|\alpha_1| + b|\delta_1| < a\sqrt{d+1} + b\sqrt{d+1} = (a+b)\sqrt{d+1} = \sqrt{d+1},$$

and for $j = r_1 + 1, \ldots, r$,

$$a(\beta_j^2 + \gamma_j^2) + b(\rho_j^2 + \sigma_j^2) < a + b = 1.$$

Hence, $\mathcal{S}_1$ is convex.

Case 3.5 $r_1 = 0$

Define the set $\mathcal{S}_2$ in $\mathbb{R}^n$ by

$$\{(\beta_1, \gamma_1, \ldots, \beta_r, \gamma_r) : |\beta_1| < 1, |\gamma_1| < \sqrt{d+1}, \beta_j^2 + \gamma_j^2 < 1 \text{ for } j = 2, 3, \ldots, r\}.$$

By a similar argument to that given in Case 3.4, $\mathcal{S}_2$ is convex.

By integrating over products of intervals and discs, we get

$$V(\mathcal{S}_1) = 2^{r_1}\pi^{r_2}\sqrt{d+1}, \text{ and } V(\mathcal{S}_2) = 2\pi^{r_2-1}\sqrt{d+1}.$$

Thus,

$$\frac{V(\mathcal{S}_1)}{2^{r_1}\sqrt{|\Delta_F|}} = \frac{2^{r_1}\pi^{r_2}\sqrt{d+1}}{2^{r_1}\sqrt{|\Delta_F|}} > \pi^{r_2} \geq 1,$$

and

$$\frac{V(\mathcal{S}_2)}{\sqrt{|\Delta_F|}} = \frac{2\pi^{r_2-1}\sqrt{d+1}}{\sqrt{|\Delta_F|}} > 2\pi^{r_2-1} > 1,$$

(since $r_2 \neq 0$ in Case 3.5, given that $r_1 = 0$). To see that this is sufficient to invoke Minkowski's Convex Body Theorem, we note that, for $j = 1, 2$, we need

$$V(\mathcal{S}_j) > 2^n V(\Theta(\mathfrak{O}_F)).$$

However, from Claim 3.5 on page 115, $V(\Theta(\mathfrak{O}_F)) = 2^{-r_2}\sqrt{|\Delta_F|}$, so

$$V(\mathcal{S}_1) = 2^{r_1}\pi^{r_2}\sqrt{d+1} > 2^{r_1+r_2}\sqrt{|\Delta_F|} = 2^n V(\Theta(\mathfrak{O}_F)),$$

and

$$V(\mathcal{S}_2) = 2\pi^{r_2-1}\sqrt{d+1} > 2^{r_2}\sqrt{|\Delta_F|} = 2^n V(\Theta(\mathfrak{O}_F)).$$

Hence, we have the existence of a nonzero $\delta_j \in \Theta(\mathfrak{O}_F) \cap \mathcal{S}_j$, for $j = 1, 2$. Let δ be one of them. Since

$$m_{\delta,\mathbb{Q}}(x) = \sum_{j=0}^{k} z_j x^j \in \mathbb{Z}[x]$$

with $|z_j| \leq C_d$, for $j = 1, 2, \ldots, k \in \mathbb{N}$, where C_d is a constant depending only on d, there can only be finitely many such δ. It remains to show that $F = \mathbb{Q}(\delta)$. In Case 3.4, δ_1 is the only conjugate of δ lying outside the unit sphere, since $|N_F(\delta)| < 1$, otherwise, and that is impossible. Similarly, in Case 3.5, $\beta_1 + \gamma_1\sqrt{-1}$, and $\beta_1 - \gamma_1\sqrt{-1}$, with $\gamma_1 \neq 0$, are the only conjugates of δ outside the unit sphere. We have shown that in Cases 3.4–3.5, there exist conjugates of δ distinct from the other conjugates. In other words, δ has n distinct conjugates. Hence, $F = \mathbb{Q}(\delta)$. □

Biography 3.8 Laszlo Rédei (1900–1980) was born on November 15, 1900 near Budapest, Hungary. After graduating, he became a secondary-school teacher until he was appointed professor at the University of Szeged in 1940. He remained there until he moved to Budapest in 1967. He did classical work on 4-invariants of class groups of quadratic fields, as well as explicit construction of Hilbert 2-class fields of quadratic fields, and Euclidean algorithms in quadratic fields. Later, his interests moved mainly into group theory, but he also dabbled in combinatorics and graph theory. He died on November 21, 1980.

Exercises

3.22. Show that Minkowski's Convex Body Theorem cannot be strengthened in the sense that the factor 2^n cannot be replaced by a smaller one.

3.23. Let M be a lattice of dimension n containing the lattice L of dimension n, with $|M : L| = d \in \mathbb{N}$ as $\mathbb{Z}$-modules. Suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for M and $\{\beta_1, \ldots, \beta_n\}$ is a basis for L such that for $i = 1, \ldots, n$,

$$\beta_i = \sum_{j=1}^{n} z_{i,j}\alpha_j \quad (z_{i,j} \in \mathbb{Z}).$$

Prove that $|M : L| = |\det(z_{i,j})|$.

3.24. Let G be a free abelian group of rank n, and let H be a subgroup of G. Prove that G/H is finite if and only if the rank of H is n. Conclude that a subgroup H of a lattice L that has finite index in L must also be a lattice.

3.25. For $j = 1, 2, \ldots, n \in \mathbb{N}$, let

$$F_j(x_1, \ldots, x_n) = r_{1,j}x_1 + r_{2,j}x_2 + \cdots + r_{n,j}x_n, \text{ with } r_{i,j} \in \mathbb{R} \text{ for } i = 1, 2, \ldots, n,$$

called a *linear form*, and let L be a lattice of dimension n with discriminant $D(L)$. Prove that if $c_j \in \mathbb{R}^+$ for $j = 1, 2, \ldots, n$ satisfies the condition

$$c_1c_2 \cdots c_n \geq |\det(r_{i,j})|D(L),$$

where $\det(r_{i,j}) \neq 0$, then there exists a nonzero point $(x_1, x_2, \ldots, x_n)$ of L such that

$$|F_1(x_1, x_2, \ldots, x_n)| \leq c_1$$

and

$$|F_j(x_1, x_2, \ldots, x_n)| \leq c_j \text{ for } j = 2, 3, \ldots, n.$$

(*Hint: Use Minkowski's convex body theorem.*)

(*The result in this exercise is known as Minkowski's* Linearformensatz *or* Theorem on linear forms.)

3.26. Suppose that $r \in \mathbb{R}$. Prove that for any $m \in \mathbb{N}$, there exists a $p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$ such that $0 < q \leq m$ and

$$\left| r - \frac{p}{q} \right| < \frac{1}{qm}.$$

(*Hint: Use Exercise 3.25.*)

(*The result in this exercise has implications for the theory of continued fractions and solutions of Pell's equation in elementary number theory—see* [53, Theorem 5.8, p. 218].)

3.27. Let $k, n, m_j \in \mathbb{N}$ for $j = 1, 2, \ldots, k \leq n$ and $F_1(P), \ldots, F_k(P) \in \mathbb{Z}$ be functions defined for points P in the lattice $\mathbb{Z}^n$. Suppose that for each $j = 1, 2, \ldots, k$,

$$F_j(x) \equiv F_j(y) \pmod{m_j}$$

implies that

$$F_j(x - y) \equiv 0 \pmod{m_j}.$$

Also, suppose that S is a symmetric, convex set in $\mathbb{R}^n$ such that

$$V(S) > 2^n \prod_{j=1}^{k} m_j.$$

Prove that there exists a nonzero point $P \in S \cap \mathbb{Z}^n$ and

$$F_j(P) \equiv 0 \pmod{m_j},$$

for $j = 1, \ldots, k$.

(*Hint: Use Exercise* 3.25.)

(This result was proved by L. Rédei in 1950.)

3.28. Let p be a prime not dividing $m \in \mathbb{Z}$. Prove that there exist integers x_j for $j = 1, 2$ such that $|x_j| \leq \sqrt{p}$, and

$$x_2 \equiv mx_1 \pmod{p}.$$

(Hint: Use Exercise 3.27.)

(*This result is* Thue's Theorem. *See* [53, Theorem 1.23, p. 44] *for an elementary-number-theoretic proof, and see* [53, Biography 1.12, p. 45] *for data on Axel Thue.*)

3.29. Prove that Θ given in Definition 3.11 is a $\mathbb{Q}$-algebra monomorphism.

3.30. Let $k, n, t, m_j \in \mathbb{N}$ for $j = 1, 2, \ldots, k < n$ such that $\prod_{j=1}^{k} m_j < t^k$. Prove that for each system of linear forms $F_j(x_1, \ldots, x_n)$, there exist $y_j \in \mathbb{Z}$, not all zero, such that $|y_j| \leq t^{k/n}$ and

$$F_j(x_1, \ldots, x_n) \equiv 0 \pmod{m_j},$$

for $j = 1, \ldots, k$.

Biography 3.9 Johan Peter Gustav Lejeune Dirichlet (1805–1859) was born on February 13, 1805 in Düren, that is now in Germany but was then in the French Empire. He taught at the University of Breslau (now Wroclaw in Poland) in 1827. Then he taught at the University of Berlin from 1828 to 1855. He was appointed to the Berlin Academy in 1831. In 1855, Dirichlet succeeded Gauss at Göttingen. However, in the summer of 1858, he suffered a heart attack while at a conference in Switzerland. He returned to Göttingen where his illness was compounded by his wife's death from a stroke. He died there on May 5.

Dirichlet made contributions to the proof of Fermat's last theorem in 1825. In 1837, his result on primes in arithmetic progression was published—see [54, Theorem 7.7, p. 258] for a self-contained proof. In 1838, his work on the formula for the class number of quadratic forms appeared. In 1839, he began an investigation of equilibrium of systems and potential theory. This led him to what we now call Dirichlet's problem on harmonic functions with given boundary conditions. In 1863, his work, *Vorlesungen über Zahlentheorie*, contained his celebrated work on ideals and units in algebraic number theory, which is a central topic of this section.

3.31. Suppose that F is a number field and I is an integral $\mathfrak{O}_F$-ideal. Prove that there exists a number field $K = F(\alpha)$ with $\alpha \in \mathbb{A}$ such that $\alpha\mathfrak{O}_K = I\mathfrak{O}_K$.

(*Hint: Use Exercise 3.18 on page 107 and Theorem 1.17 on page 28.*)

3.32. With reference to Exercise 3.31, prove that $\mathfrak{O}_F(\alpha) \cap F = I$.

3.33. With reference to Exercises 3.31–3.32, prove that the following holds. Let $\gamma \in \mathbb{A}$ and $\mathfrak{O}_K$ the ring of integers of any number field K. If

$$\mathfrak{O}_K(\gamma) = \mathfrak{O}_K I,$$

then $\gamma = u\alpha$ for some unit $u \in \mathbb{A}$. (*Exercises 3.31–3.33 show that there is always an extension ring of integers of $\mathfrak{O}_F$ in which any given ideal I becomes principal as an "extended ideal" $\mathfrak{O}_K(\gamma)$. See Corollary 5.21, and Remark 5.8 on page 240 for related notions.*)

3.34. Let F be a real quadratic field with $N_F(\varepsilon_{\Delta_F}) = 1$. Suppose that I is an $\mathfrak{O}_F$-ideal with $I^2 = (\alpha)$ for some $\alpha \in \mathfrak{O}_F$ where $N_F(\alpha) < 0$. Prove that $I \not\sim 1$.

3.4 Units in Number Rings

That low man seeks a little thing to do,
Sees it and does it;
This high man, with a great thing to pursue,
Dies ere he knows it.
That low man goes on adding one to one,
His hundred's soon hit:
This high man, aiming at a million,
Misses an unit.

from l.113 of **A Grammarian's Funeral (1855)**
Robert Browning (1812–1869)
English poet
husband of Elizabeth Barrett Browning

In §3.5, we will establish the celebrated Dirichlet unit theorem. We set the stage in this section by establishing results on the finite component of the unit group, namely the group of roots of unity. Of fundamental importance is the ring of integers of a cyclotomic field. This will become even more transparent later when we establish the Kronecker-Weber Theorem. First however, we need the following crucial result on a compositum of fields due to Hilbert—see Biography 3.4 on page 94. The reader should therefore be familiar with the discussion surrounding Application A.1 on page 325.

Theorem 3.13 — Compositum of Rings of Integers
Suppose that F_j are number fields with number rings $\mathfrak{O}_{F_j}$ and discriminants$\Delta\ _{F_j}$ for $j = 1, 2$ with $\gcd(\Delta_{F_1}, \Delta_{F_2}) = 1$, and

$$K = F_1F_2$$

is the compositum of F_1 and F_2. Then

$$\mathfrak{O}_K = \mathfrak{O}_{F_1}\mathfrak{O}_{F_2}$$

(where $\mathfrak{O}_{F_1}\mathfrak{O}_{F_2}$ consists of all sums $\sum_{j=1}^{n} \alpha_j\beta_j$ for $n \in \mathbb{N}$, $\alpha_j \in \mathfrak{O}_{F_1}$, and $\beta_j \in \mathfrak{O}_{F_2}$.)

Proof. Since $\mathfrak{O}_{F_1}\mathfrak{O}_{F_2}$ is the smallest subring of K containing both $\mathfrak{O}_{F_1}$ and $\mathfrak{O}_{F_2}$, then $\mathfrak{O}_{F_1}\mathfrak{O}_{F_2} \subseteq \mathfrak{O}_K$. Thus, it remains to show that $\mathfrak{O}_K \subseteq \mathfrak{O}_{F_1}\mathfrak{O}_{F_2}$. If

$$\mathcal{B}_j = \{\beta_1^{(j)}, \ldots, \beta_{n_j}^{(j)}\},$$

is an integral basis for F_j, then the set consisting of all n_1n_2 products $\beta_i^{(1)}\beta_j^{(2)}$ is a basis for K over $\mathbb{Q}$ by Exercise 3.36 on page 129. Therefore, $\beta \in \mathfrak{O}_K$ may be represented in the form

$$\beta = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} q_{i,j}\beta_i^{(1)}\beta_j^{(2)},$$

with $q_{i,j} \in \mathbb{Q}$. It suffices to show that $q_{i,j} \in \mathbb{Z}$ for each such i, j. By Exercise 2.6 on page 63, we may let θ_k for $k = 1, 2, \ldots, n_1$ be the embeddings of K in $\mathbb{C}$ that fix F_2 pointwise. Thus, for each such k,

$$\theta_k(\beta) = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} q_{i,j}\theta_k(\beta_i^{(1)})\beta_j^{(2)}.$$

Set

$$x_i = \sum_{j=1}^{n_2} q_{i,j}\beta_j^{(2)},$$

for $i = 1, 2, \ldots, n_1$. Therefore, we have the n_2 equations

$$\theta_k(\beta) = \sum_{i=1}^{n_1} x_i \theta_j(\beta_i^{(1)}),$$

for $k = 1, 2, \ldots, n_2$. We use Cramer's rule, Theorem A.21 on page 337 to solve for the x_i as follows.

$$x_i = z_i / \det(\theta_j(\beta_i^{(1)})).$$

Set

$$y_i = \det(\theta_j(\beta_i^{(1)})).$$

Then $y_i, z_i \in \mathbb{A}$, and $y_i^2 = \Delta_{F_1}$. Thus,

$$x_i \Delta_{F_1} = z_i y_i \in \mathbb{A}.$$

Therefore,

$$x_i \Delta_{F_1} = \sum_{j=1}^{n_2} q_{i,j}\Delta_{F_1}\beta_j^{(2)} \in \mathbb{A} \cap F_2 = \mathfrak{O}_{F_2}.$$

However, $\mathcal{B}_2$ is an integral basis for F_2, so $q_{i,j}\Delta_{F_1} \in \mathbb{Z}$ for each i, j. In other words, $q_{i,j} = m_{i,j}/n_{i,j}$, where $m_{i,j}, n_{i,j} \in \mathbb{Z}$ with $n_{i,j} \bigm| \Delta_{F_1}$. A similar argument shows that $n_{i,j} \bigm| \Delta_{F_2}$. Hence, $n_{i,j} \bigm| \gcd(\Delta_{F_1}, \Delta_{F_2}) = 1$, so $q_{i,j} \in \mathbb{Z}$ for all such i, j and we have the result. □

Theorem 3.14 — The Ring of Integers of a Cyclotomic Field
If $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$, then $\mathfrak{O}_F = \mathbb{Z}[\zeta_n]$.

Proof. We may assume that $n \geq 3$, since the result trivially holds for $n = 1, 2$.

Claim 3.6 $\Delta_F \bigm| n^{\phi(n)}$.

By Theorem 1.25 on page 40, $x^n - 1 = \Phi_n(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$, so we may differentiate both sides to get

$$nx^{n-1} = \Phi_n'(x)g(x) + \Phi_n(x)g(x)'. \tag{3.29}$$

For $x = \zeta_n$, (3.29) yields

$$n\zeta_n^{n-1} = \Phi'(\zeta_n)g(\zeta_n),$$

so by taking norms of both sides,

$$\pm n^{\phi(n)} = N_F(n\zeta_n^{n-1}) = N_F(\Phi_n'(\zeta_n))N_F(g(\zeta_n)).$$

By Definition 2.7 on page 77, Exercise 2.31 on page 69 and Theorems 2.6–2.7 on page 71,

$$\Delta_F \bigm| N_F(\Phi_n'(\zeta_n)),$$

so we have claim 3.6.

Now we establish the theorem for a prime power. Suppose that $n = p^a$ for a prime p.

Claim 3.7 If $\beta \in \mathfrak{O}_F$, then

$$\beta = \sum_{j=1}^{\phi(p^a)} \frac{z_j}{\Delta_F}\alpha_j,$$

where $\alpha_j = (1-\zeta_{p^a})^j$, and $z_j \in \mathbb{Z}$ with$\Delta\ _F \bigm| z_j^2$.

If $\beta = \sum_{j=1}^{\phi(p^a)} q_j\alpha_j$ with $q_j \in \mathbb{Q}$, then for any $i \in \mathbb{N}$ with $1 \le i \le \phi(p^a)$, form

$$\theta_j(\beta) = \sum_{j=1}^{d} q_j\theta_j(\alpha_i),$$

where θ_j is an embedding of F in $\mathbb{C}$ for $1 \le j \le \phi(p^a)$. By Cramer's rule,

$$q_j = z_j/\det(\theta_j(\alpha_i)),$$

where $z_j \in \mathbb{A}$ is determined in Theorem A.21, and $\det^2(\theta_j(\alpha_i)) =\Delta\ _F$. Therefore, $z_j^2 = q_j^2\Delta_F \in \mathbb{A}\cap\mathbb{Q} = \mathbb{Z}$, by Corollary 1.11 on page 37. Hence,$\Delta\ _F \bigm| z_j^2$, which yields Claim 3.7.

Claim 3.8 If $n = p^a$, then $\mathbb{Z}[\zeta_{p^a}] = \mathfrak{O}_F$.

Since $\zeta_{p^a} = 1-(1-\zeta_{p^a})$, then $\mathbb{Z}[1-\zeta_{p^a}] = \mathbb{Z}[\zeta_{p^a}]$, so it suffices to show that $\mathfrak{O}_F = \mathbb{Z}[1-\zeta_{p^a}]$. By Claim 3.6, $|\Delta_F|$ is a power of p. If $\beta \in \mathfrak{O}_F$ but $\beta \notin \mathbb{Z}[1-\zeta_{p^a}]$, then by Claim 3.7, we may assume that

$$\beta = \sum_{j=d}^{\phi(p^a)} \frac{z_j}{p}\alpha_{j-1}, \text{ for some } d \text{ with } 1 \le d \le \phi(p^a),$$

where $p \nmid z_d$. By Exercise 3.35 on page 129, $N_F(1-\zeta_{p^a}) = p$. Thus,

$$\frac{\prod_j(1-\zeta_{p^a}^j)}{(1-\zeta_{p^a})^{\phi(p^a)}} = \frac{N_F(1-\zeta_{p^a})}{(1-\zeta_{p^a})^{\phi(p^a)}} = \frac{p}{(1-\zeta_{p^a})^{\phi(p^a)}} \in \mathfrak{O}_F,$$

since for each natural number j relatively prime to p, we have

$$\frac{1-\zeta_{p^a}^j}{1-\zeta_{p^a}} \in \mathfrak{O}_F.$$

Therefore,

$$\frac{p}{(1-\zeta_{p^a})^d} \in \mathfrak{O}_F,$$

which implies that

$$\frac{\beta p}{(1-\zeta_{p^a})^d} = \frac{\sum_{j=d}^{\phi(p^a)} z_j\alpha_{j-1}}{(1-\zeta_{p^a})^d} = \frac{z_d}{1-\zeta_{p^a}} + \sum_{j=d+1}^{\phi(p^a)} z_j\alpha_{j-d-1} \in \mathfrak{O}_F.$$

In turn, this implies that

$$\frac{z_d}{1-\zeta_{p^a}} = \frac{\beta p}{(1-\zeta_{p^a})^d} - \sum_{j=d+1}^{\phi(p^a)} z_j\alpha_{j-d-1} \in \mathfrak{O}_F.$$

Thus, by Exercise 2.17 on page 68, and Exercise 3.35,

$$N_F(1-\zeta_{p^a}) = p \mid N_F(z_d) = z_d^{\phi(p^a)},$$

so $p \mid z_d$, a contradiction, which establishes Claim 3.8.

Let

$$n = \prod_{j=1}^{b} p_j^{a_j},$$

be the canonical prime factorization of n. Then for $F_j = \mathbb{Q}(\zeta_{p_j^{a_j}})$, we have $\gcd(\Delta_{F_\ell}, \Delta_{F_k}) = 1$, for any $\ell \neq k$ with $1 \leq \ell, k \leq b$, by Claim 3.6. We need one more result to finish the proof.

Claim 3.9 If $F_k = \mathbb{Q}(\zeta_{p^{a_k}})$ and $F_\ell = \mathbb{Q}\zeta_{p^{a_e}})$ for $k \neq \ell$, then $\mathfrak{O}_{F_k}\mathfrak{O}_{F_\ell} = \mathfrak{O}_{F_kF_\ell}$.

By Theorem 3.13 on page 122,

$$\mathbb{Z}[\zeta_{p_\ell^{a_\ell}p_k^{a_k}}] = \mathbb{Z}[\zeta_{p_\ell^{a_\ell}}, \zeta_{p_k^{a_k}}] = \mathbb{Z}[\zeta_{p_\ell^{a_\ell}}]\mathbb{Z}[\zeta_{p_k^{a_k}}] = \mathfrak{O}_{F_\ell}\mathfrak{O}_{F_k} = \mathfrak{O}_{F_\ell F_k}.$$

Hence, by induction using Claim 3.9,

$$\mathfrak{O}_F = \mathbb{Z}[\zeta_n],$$

as required. □

The following is a stronger result than Claim 3.6 on page 123 in the case of a prime power.

Corollary 3.9 — Discriminants of Prime-Power Cyclotomic Fields

If $F = \mathbb{Q}(\zeta_{p^a}) \neq \mathbb{Q}$ where p is prime, then$\Delta_{F} = (-1)^{\phi(p^a)/2}p^{p^{a-1}(a(p-1)-1)}$.

Proof. By Exercise 1.54 on page 43, we have

$$x^{p^a} - 1 = (x^{p^{a-1}} - 1)\Phi_{p^a}(x).$$

Therefore, by taking derivatives,

$$p^a x^{p^a-1} = p^{a-1}x^{p^{a-1}-1}\Phi_{p^a}(x) + (x^{p^{a-1}} - 1)\Phi'_{p^a}(x).$$

Thus,

$$p^a\zeta_{p^a}^{p^a-1} = (\zeta_{p^a}^{p^{a-1}} - 1)\Phi'_{p^a}(\zeta_{p^a}). \tag{3.30}$$

We observe that since $\zeta_{p^a}^{p^a-1}$ is a primitive p^a-th root of unity, we may invoke Exercise 3.35 on page 129 to get, $N_F(\zeta_{p^a}^{p^{a-1}} - 1) = (-1)^{\phi(p^a)}p^{p^{a-1}}$. Hence, by taking norms of both sides of Equation (3.30), we get

$$p^{a\phi(p^a)} = (-1)^{\phi(p^a)}p^{p^{a-1}}N_F(\Phi'_{p^a}(\zeta_{p^a})). \tag{3.31}$$

However, by Exercise 2.39 on page 82, and Exercise 2.31 on page 69,

$$N_F(\Phi'_{p^a}(\zeta_{p^a})) = (-1)^{\phi(p^a)(\phi(p^a)-1)/2}\Delta_F = (-1)^{\phi(p^a)/2}\Delta_F.$$

Thus, via Equation (3.31), we get

$$\Delta_F = (-1)^{\phi(p^a)/2}p^{a\phi(p^a)-p^{a-1}} = (-1)^{\phi(p^a)/2}p^{p^{a-1}(a(p-1)-1)},$$

which is the result. □

We will provide the complete generalization of Corollary 3.9 to the determination of the discriminant of $\mathbb{Q}(\zeta_n)$ for any $n \in \mathbb{N}$ when we have the tools to do so in Theorem 5.14 on page 216.

Before establishing the main result on roots of unity for this section, we need the following result due to Kronecker—see Biography 2.2 on page 79. We we will substantially generalize the following later when we have developed the tools to do so—see Corollary 5.4 on page 200.

Theorem 3.15 — Division of Field Discriminants in Towers

If $\mathbb{Q} \subseteq F \subseteq K$ is an extension of number fields then$\Delta\ _F \Bigm| \Delta_K$.

Proof. By Exercise 2.42 on page 82, any integral basis for K contains an integral basis for F. Let $\{\alpha_1, \ldots, \alpha_d, \alpha_{d+1}, \ldots, \alpha_n\}$ be an integral basis for K where the first d elements provide an integral basis for F. From Exercise 2.6 on page 63, we know that $|F : \mathbb{Q}| = d|n = |K : \mathbb{Q}|$. Also, from that exercise we may arrange the embeddings θ_j, $(1 \leq j \leq n)$ of K in $\mathbb{C}$ in the following manner. Let $\theta_j(\alpha_i) = \alpha_i^{(j)}$, and set $\theta_j(\alpha_1) = \alpha_1^{(j)}$ for $j = 1, 2, \ldots, d$. Also, ensure that, for each $i = 1, 2 \ldots, n$, we have arranged that $\theta_j(\alpha_i) = \theta_k(\alpha_i)$, whenever $j \equiv k \pmod{d}$. This yields the following.

$$\Delta_K = \det(\theta_j(\alpha_i))^2 =$$

$$\det\begin{pmatrix} \alpha_1^{(1)}\cdots\alpha_1^{(d)} & \alpha_1^{(1)}\cdots\alpha_1^{(d)} & \cdots & \alpha_1^{(1)}\cdots\alpha_1^{(d)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_d^{(1)}\cdots\alpha_d^{(d)} & \alpha_d^{(1)}\cdots\alpha_d^{(d)} & \cdots & \alpha_d^{(1)}\cdots\alpha_d^{(d)} \\ \alpha_{d+1}^{(1)}\cdots\alpha_{d+1}^{(d)} & \alpha_{d+1}^{(d+1)}\cdots\cdots & \cdots & \cdots\cdots\alpha_{d+1}^{(n)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{(1)}\cdots\alpha_n^{(d)} & \alpha_n^{(d+1)}\cdots\cdots & \cdots & \cdots\cdots\alpha_n^{(n)} \end{pmatrix}^2,$$

and by subtracting the j^{th} column from the $(kd+j)^{th}$ column for $j = 1, 2, \ldots, d$, and $k = 1, 2, \ldots, n/d - 1$, this equals,

$$\det\begin{pmatrix} \alpha_1^{(1)}\cdots\alpha_1^{(d)} & 0\cdots 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_d^{(1)}\cdots\alpha_d^{(d)} & 0\cdots 0 & \cdots & 0 \\ \alpha_{d+1}^{(1)}\cdots\alpha_{d+1}^{(d)} & \alpha_{d+1}^{(d+1)} - \alpha_{d+1}^{(1)}\cdots\cdots & \cdots & \cdots\cdots\alpha_{d+1}^{(n)} - \alpha_{d+1}^{(d)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{(1)}\cdots\alpha_n^{(d)} & \alpha_n^{(d+1)} - \alpha_n^{(1)}\cdots\cdots & \cdots & \cdots\cdots\alpha_n^{(n)} - \alpha_n^{(d)} \end{pmatrix}^2 = \gamma\Delta_F,$$

where $\gamma \in \mathfrak{O}_K$. However, $\gamma = \Delta_K/\Delta_F \in \mathbb{Q}$, so by Corollary 1.11 on page 37, $\gamma \in \mathbb{Z}$, as required. □

In Definition 1.3 on page 2, we first met the notion of a primitive root of unity. Now we look at the group generated by them. Henceforth, for a number field F, we denote the subgroup of $\mathfrak{U}_{\mathfrak{O}_F}$ consisting of roots of unity by $\mathcal{R}_F$.

Theorem 3.16 — The Group of Roots of Unity

If F is a number field, then every finite subgroup G of the multiplicative group of nonzero elements of F consists of roots of unity, and is cyclic. In particular, $\mathcal{R}_F$ is a finite cyclic group. Moreover, $|\mathcal{R}_F|$ is an even divisor of $2\Delta_F$.

Proof. Suppose that $|G| = n$. It follows from Theorem A.3 on page 321, that there exists an element $\alpha \in G$ such that α has order n and $\beta^n = 1$ for each $\beta \in G$. By Theorem A.18 on page 334, $x^n - 1$ has at most n roots in $\mathbb{C}$, so G has order at most n. Since α has order n and $\alpha, \alpha^2, \ldots, \alpha^n = 1$ are all distinct then $G = \langle \alpha \rangle$, the cyclic group of order n generated by α. In particular, $\mathcal{R}_F$ is a finite cyclic group.

Given that $\{-1, 1\} \subseteq \mathcal{R}_F$, then $2 \bigm| n = |\mathcal{R}_F|$. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical prime factorization of n in $\mathbb{Z}$ and since $\mathbb{Q}(\zeta_{p_j^{a_j}}) \subseteq F$, then by Corollary 3.9 on page 125, and Theorem 3.15,

$$p_j^{p_j^{a_j-1}(a_j(p_j-1)-1)} \bigm| \Delta_F.$$

Therefore,

$$\prod_{j=1}^{k} p_j^{p_j^{a_j-1}(a_j(p_j-1)-1)} \bigm| \Delta_F.$$

If $p_j > 2$, then

$$p_j^{a_j-1}(a_j(p_j - 1) - 1) \geq a_j,$$

and if $p_j = 2$, then

$$p_j^{a_j-1}(a_j(p_j - 1) - 1) \geq a_j - 1,$$

from which the result follows. □

Now we establish a result that will allow the determination of the group of roots of unity in terms of their absolute value. Recall that the absolute value of $\gamma = a + b\sqrt{-1} \in \mathbb{C}$ is given by $|\gamma| = \sqrt{a^2 + b^2} = \sqrt{\gamma\overline{\gamma}}$, where $\overline{\gamma} = a - b\sqrt{-1}$ is the complex conjugate of γ. Sometimes $|\gamma|$ is called the modulus of γ.

Theorem 3.17 — Bounds on Absolute Values

Suppose that F is a number field with embeddings θ_j for $j = 1, 2, \ldots, d = |F : \mathbb{Q}|$ in $\mathbb{C}$, and $r \in \mathbb{R}$ with $r > 0$. Then there exist only finitely many $\alpha \in \mathfrak{O}_F$ such that $|\theta_j(\alpha)| \leq r$ for all $j = 1, 2, \ldots, d$.

Proof. Let

$$M = \max\left\{dr, \binom{d}{2}r^2, \ldots, \binom{d}{j}r^j, \ldots, r^d\right\},$$

and set

$$\mathcal{F} = \left\{ f(x) = x^d + \sum_{j=0}^{d-1} z_j x^j \in \mathbb{Z}[x] : |z_j| \leq M \right\}.$$

Then $|\mathcal{F}| < \infty$. Set

$$\mathcal{S} = \{\alpha \in F : f(\alpha) = 0 \text{ for some } f(x) \in \mathcal{F}\}.$$

Then $|\mathcal{S}| < \infty$, as well. If $\alpha \in F$ with $|\theta_j(\alpha)| \leq r$ for all $j = 1, 2, \ldots, d$, then

$$|s_j(\theta_1(\alpha), \ldots, \theta_d(\alpha))| \leq M,$$

for all $j = 1, 2, \ldots, d$, where the s_j are the elementary symmetric functions given in Definition A.16 on page 333. Since $\alpha \in \mathfrak{O}_F$, then $s_j(\theta_1(\alpha), \ldots, \theta_d(\alpha)) \in \mathbb{Z}$ by Corollaries 1.11 on page 37 and A.9 on page 334. Therefore,

$$\prod_{j=1}^{d} (x - \theta_j(\alpha)) \in \mathcal{F},$$

which implies that $\alpha \in \mathcal{S}$. The result follows. □

The following result is due to Kronecker.

Corollary 3.10 $\alpha \in \mathfrak{R}_F$ if and only if $|\theta_j(\alpha)| = 1$ for all $j = 1, \ldots, d$.

Proof. If $\alpha \in \mathfrak{R}_F$, then $\theta_j(\alpha) \in \mathfrak{R}_F$, since $\theta_j(\alpha)^n = 1$ for some $n \in \mathbb{N}$. Thus, $|\theta_j(\alpha)|^n = 1$, so $|\theta_j(\alpha)| = 1$.

Conversely, by Theorem 3.17, there exist only finitely many $\alpha \in \mathfrak{O}_F$ such that $|\theta_j(\alpha)| = 1$. Since $\alpha^k \in \mathfrak{O}_F$ satisfies $|\alpha^k| = 1$ for all $k \in \mathbb{N}$, then it follows that $\alpha^k = \alpha^\ell$ for some $k < \ell$. Thus, $\alpha^{\ell-k} = 1$, which implies that $\alpha \in \mathfrak{R}_F$, as required. □

We conclude this section with a determination of $\mathfrak{R}_F$ for a prime cyclotomic field F.

Theorem 3.18 — Roots of Unity in Prime Cyclotomic Fields

Let $F = \mathbb{Q}(\zeta_p)$ for $p > 2$ prime. Then

$$\mathfrak{R}_F = \langle -1 \rangle \times \langle \zeta_p \rangle,$$

as a multiplicative group, and every element $u \in \mathfrak{U}_{\mathfrak{O}_F}$ may be written as $u = w\zeta_p^k$ where $w \in \mathbb{R} \cap \mathfrak{U}_{\mathfrak{O}_F}$ and $k \in \mathbb{Z}$.

Proof. By Theorem 3.14 on page 123, $\mathfrak{O}_F = \mathbb{Z}[\zeta_p]$. Clearly, $\langle -1 \rangle \times \langle \zeta_p \rangle \subseteq \mathfrak{R}_F$. If the inclusion is proper, there is a $\zeta_n \in \mathfrak{R}_F$ with $n \nmid 2p$. In particular, it must contain either $\zeta_n = \zeta_{4q}$ where $q \neq p$ is prime or $\zeta_n = \zeta_{p^2}$. However, $\zeta_4 \notin \mathbb{Q}(\zeta_p)$, since otherwise $\zeta_4 \in \{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$, which is not possible. Since the degree of $\mathbb{Q}(\zeta_{p^2})$ over $\mathbb{Q}$ is $p(p-1)$, then the latter cannot hold either. Thus, $\mathfrak{R}_F = \langle -1 \rangle \times \langle \zeta_p \rangle$, as required. Moreover, since there are no more complex units in $\mathfrak{U}_{\mathfrak{O}_F}$, then the last statement of the theorem must hold. □

Example 3.4 Let $F = \mathbb{Q}(\zeta_p)$ for a prime $p > 2$, and set

$$u = \frac{1 - \zeta_p^j}{1 - \zeta_p},$$

so its complex conjugate is

$$\overline{u} = \frac{1 - \zeta_p^{-j}}{1 - \zeta_p^{-1}} = \frac{\zeta_p^{-j}(1 - \zeta_p^j)}{\zeta_p^{-1}(1 - \zeta_p)} = \zeta_p^{1-j} u.$$

Both are units in $\mathfrak{O}_F$ by Exercise 3.37. Thus,

$$u\overline{u} = \left(\frac{1 - \zeta_p^j}{1 - \zeta_p}\right)\left(\frac{1 - \zeta_p^{-j}}{1 - \zeta_p^{-1}}\right) = \zeta_p^{(1-j)} u^2,$$

so if j is odd, then

$$u\overline{u} = (\zeta_p^{(1-j)/2} u)^2.$$

Hence,

$$v = \sqrt{\left(\frac{1 - \zeta_p^j}{1 - \zeta_p}\right)\left(\frac{1 - \zeta_p^{-j}}{1 - \zeta_p^{-1}}\right)} \in \mathbb{R} \cap \mathfrak{U}_{\mathfrak{O}_F}. \tag{3.32}$$

The distinguished units v in Equation (3.32) are called *cyclotomic units*, about which we will learn more later in the text.

Remark 3.15 A result due to Hilbert, which he proved in 1897, says that the numbers

$$\left(\left[\left(1-\zeta_p^{r^{k+1}}\right)\left(1-\zeta_p^{-r^{k+1}}\right)\right]/\left[\left(1-\zeta_p^{r^k}\right)\left(1-\zeta_p^{-r^k}\right)\right]\right)^{1/2},$$

where r is a primitive root modulo p and $k = 0, 1, \ldots, (p-3)/2$, provide a system of independent units in $\mathfrak{U}_{\mathfrak{O}_F}$ for $F = \mathbb{Z}[\zeta_p]$—see Biography 3.4 on page 94. As this chapter progresses, we will learn substantially more about the role of units.

The above shows that even for the relatively simple fields considered, there is somewhat of a difficulty in describing the structure of the units. For the general case, we will need to introduce some geometry to tackle the problem. We do this in §3.5.

Exercises

3.35. Let p be a prime, and $a \in \mathbb{N}$. Prove that $N_F(1-\zeta_{p^a}) = p$, where ζ_{p^a} is a primitive p^a-th root of unity.

3.36. Suppose that $F_j = \mathbb{Q}(\alpha_j)$ are number fields, with $|F_j : \mathbb{Q}| = n_j$ for $j = 1, 2$. Prove that

$$|K : \mathbb{Q}| \le n_1 n_2,$$

where

$$K = F_1 F_2 = \mathbb{Q}(\alpha_1, \alpha_2).$$

Also, show that if

$$\gcd(|F_1 : \mathbb{Q}|, |F_2 : \mathbb{Q}|) = 1,$$

then

$$|K : \mathbb{Q}| = n_1 n_2.$$

Is the converse true?

3.37. Let p be a prime, $n = p^a$ for some $a \in \mathbb{N}$, and $F = \mathbb{Q}(\zeta_n)$. Suppose that $j \in \mathbb{N}$ such that $\gcd(j, p) = 1$. Prove that

$$N_F\left(\frac{1-\zeta_n^j}{1-\zeta_n}\right) = 1, \text{ and}\Phi\ _n(1) = p.$$

3.38. Let $\alpha \in \mathfrak{O}_F$ be prime, where $F = \mathbb{Q}(\zeta_n)$ for $n \in \mathbb{N}$. Suppose that

$$\alpha \mid (\zeta_n^a - \zeta_n^b)$$

for some $a, b \in \mathbb{Z}$. Prove that $\zeta_n^a = \zeta_n^b$.

3.39. Let $n > 2$ be an integer, and set $F = \mathbb{Q}(\zeta_n)$. We know that $\zeta_n \in \mathfrak{U}_{\mathfrak{O}_F}$. Prove that

$$N_F(\zeta_n) = 1.$$

3.40. Let $n \in \mathbb{N}$ with $n > 1$. Prove that

$$\prod_{1 \le j \le n-1} (1 - \zeta_n^j) = n.$$

3.5 Dirichlet's Unit Theorem

> *Experience is the name every one gives to their mistakes.*
> *from act 3 of* **Lady Windermere's Fan (1892)**
> **Oscar Wilde (1854–1900)**
> Anglo-Irish dramatist and poet

In this section, the primary goal is to establish Dirichlet's Unit Theorem, which gives, in an abstract fashion, a complete description of the group of units $\mathfrak{U}_{\mathfrak{O}_F}$ of $\mathfrak{O}_F$ for any number field F.

First, we need a variant of Definition 3.11 on page 112.

Definition 3.13 — Logarithmic Representations and Spaces

Let F be a number field with signature $\{r_1, r_2\}$, where $|F : \mathbb{Q}| = n = r_1 + 2r_2$, and note that $(\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$ is the multiplicative group in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consisting of those elements with *all* co-ordinates nonzero. Define the map

$$\Psi : (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \mapsto \mathbb{R}^{r_1+r_2},$$

by

$$\Psi(\alpha_1, \ldots, \alpha_{r_1}, \alpha_{r_1+1}, \ldots, \alpha_{r_2}) = (\mathfrak{l}_1(\alpha_1), \ldots, \mathfrak{l}_{r_1}(\alpha_{r_1}), \ldots, \mathfrak{l}_{r_2}(\alpha_{r_2})),$$

where

$$\mathfrak{l}_j(\alpha_j) = \begin{cases} \log_e(|\alpha_j|) & \text{if } 1 \le j \le r_1, \\ \log_e(|\alpha_j|^2) & \text{if } r_1 + 1 \le j \le r_1 + r_2. \end{cases}$$

Let the map

$$\mathcal{L}_F : F \mapsto \mathbb{R}^{r_1+r_2},$$

be given via the composition of functions

$$\mathcal{L}_F = \Psi \circ \Theta_F,$$

where$\Theta\ _F$ is given in Definition 3.11. Then for any $\alpha \in F$,

$$\mathcal{L}_F(\alpha) = (\log_e(|\theta_1(\alpha)|), \ldots, \log_e(|\theta_{r_1}(\alpha)|), \log_e(|\theta_{r_1+1}(\alpha)|^2), \ldots, \log_e(|\theta_{r_2}(\alpha)|^2)).$$

$\mathcal{L}_F$ is called the *logarithmic representation*, or *logarithmic map* of F, and $\mathbb{R}^{r_1+r_2}$ is called the *logarithmic space.*

By Exercise 3.41 on page 136, the logarithmic representation $\mathcal{L}_F$ of Definition 3.13 is a homomorphism of the multiplicative group F^* of nonzero elements of F to the additive group of the logarithmic space $\mathbb{R}^{r_1+r_2}$. In fact, this is the reason for introducing logarithms in the first place, namely to link this section with the preceding one in the sense that the group $\mathfrak{U}_{\mathfrak{O}_F}$ is multiplicative, whereas Minkowski's Convex Body Theorem applies to lattices, which are additive. Hence, we now have a method that maps from one scenario to the other via $\mathcal{L}_F$. If we consider the restriction of $\mathcal{L}_F$ to $\mathfrak{U}_{\mathfrak{O}_F}$, we begin to get the picture.

Lemma 3.4 — The Kernel and Image of $\mathcal{L}_\mathbf{F}$

If F is a number field with signature $\{r_1, r_2\}$, then

$$\ker(\mathcal{L}_F) = \mathcal{R}_F,$$

and $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ is a lattice in $\mathbb{R}^{r_1+r_2}$, having dimension less than $r_1 + r_2$.

Proof. Since $\mathcal{L}_F(\alpha) = 0$ if and only if $|\theta_j(\alpha)| = 1$ for all $j = 1, \ldots, r_2$, then by Corollary 3.10 on page 128, $\theta_j(\alpha) \in \mathcal{R}_F$ for all such j. Hence, $\ker(\mathcal{L}_F) = \mathcal{R}_F$. Let $r = r_1 + r_2$ for convenience. Then for $\alpha \in \mathfrak{U}_{\mathfrak{O}_F}$, since

$$\pm 1 = N_F(\alpha) = \prod_{j=1}^{n} \theta_j(\alpha) = \prod_{j=1}^{r_1} \theta_j(\alpha) \prod_{j=r_1+1}^{r_1+r_2} \theta_j(\alpha)\overline{\theta_j(\alpha)} =$$

$$\prod_{j=1}^{r_1} \theta_j(\alpha) \prod_{j=r_1+1}^{r_1+r_2} |\theta_j(\alpha)|^2,$$

then

$$\sum_{j=1}^{r} \mathfrak{l}_j(\alpha) = \log_e(|N_F(\alpha)|) = \log(1) = 0,$$

so

$$\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F}) \subseteq \{(x_1, \ldots, x_r) \in \mathbb{R}^r : \sum_{j=1}^{r_1} x_j + 2 \sum_{j=r_1+1}^{r_1+r_2} x_j = 0\},$$ [3.2]

which has dimension $r - 1$. To prove that $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ is a lattice, we invoke Theorem 3.8 on page 109. By definition, it is an additive subgroup, so we need only prove that it is discrete.

Let $\alpha \in \mathfrak{U}_{\mathfrak{O}_F}$. Then $|\mathcal{L}_F(\alpha)| < r$. For $n \in \mathbb{N}$, set

$$\mathcal{S}_n = \{\alpha \in \mathfrak{U}_{\mathfrak{O}_F} : |\theta_j(\alpha)| \le n \text{ for all } j = 1, 2, \ldots, r\},$$

called a *cube with side n centered at the origin.* Since for each $j = 1, \ldots, r$,

$$|\mathfrak{l}_j(\theta_j(\alpha))| \le \log_e(|\mathcal{L}_F(\alpha)|) < n,$$

then $|\theta_j(\alpha)| < e^n$ for $1 \le j \le r_1$, and $|\theta_j(\alpha)|^2 < e^n$ for $r_1 + 1 \le j \le r$. Hence, $\mathcal{S}_n$ has only finitely many points. However, $\Theta(\mathcal{S}_n)$ is an injection of $\mathcal{S}_n$ into the $r - 1$-dimensional hyperplane. Thus, $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ is a lattice. □

The next step toward the unit theorem is to establish that $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ is actually of dimension $r - 1$ rather than just contained in a hyperplane of that dimension.

Definition 3.14 — Norms of Elements in Logarithmic Space

If F is a number field with signature $\{r_1, r_2\}$, and $\ell \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\ell = (\ell_1, \ldots, \ell_{r_1+r_2})$, then the *norm of ℓ* is given by

$$N_F(\ell) = \prod_{j=1}^{r_1} \ell_j \prod_{j=r_1+1}^{r_1+r_2} |\ell_j|^2.$$

[3.2] This set is an example of a *hyperplane*. In topological language, an *osculating hyperplane* of a convex set $S \subseteq \mathbb{R}^n$ is a hyperplane that has a point of its boundary in common with S, but is disjoint from the interior of S. Recall that the *boundary* of a set S is defined to be the intersection of the closure of S with the closure of its complement, whereas the *interior* of S is the set of all points $s \in S$ for which there exists a disc with center s, contained in S. A fundamental result concerning osculating hyperplanes is the following. If S is a convex set in $\mathbb{R}^n$, and P is a point on its boundary, there exists at least one osculating hyperplane of S containing P.

The term *norm* in Definition 3.14 is appropriate and in keeping with the notion of norm given in Definition 2.4—see (3.33) on page 132. In preparation for the following, the reader is reminded of linear transformations and their matrices as given in Definition A.20 on page 338.

Lemma 3.5 — Linear Transformations and Norms

Suppose that F is a number field with signature $\{r_1, r_2\}$, and let $\ell \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let the map

$$\lambda_\ell : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mapsto \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

be defined by $\lambda_\ell(x) = \ell x$. Then λ_ℓ is a linear transformation and $\det(\lambda_\ell) = N_F(\ell)$.

Proof. Choose the canonical basis for $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, namely $\{v_j\}$ for $j = 1, 2\ldots, n = r_1 + 2r_2$ where $v_j = (0, \ldots 0, 1, 0 \ldots 0)$, where the 1 is in the j^{th} place for $j = 1, 2, \ldots, r_1$, and $v_j = (0, \ldots 0, 1 + \sqrt{-1}, 0 \ldots 0)$ with the $1 + \sqrt{-1}$ in the j^{th} place for $j = r_1 + 1, \ldots, r_1 + r_2$. Thus, if

$$\ell = (\ell_1, \ldots, \ell_{r_1+r_2}) = (\ell_1, \ldots, \ell_{r_1}, m_{r_1+1} + n_{r_1+1}\sqrt{-1}, \ldots, m_{r_2} + n_{r_2}\sqrt{-1}),$$

then the matrix of λ_ℓ is given by the almost diagonal matrix,

$$\begin{pmatrix}
\ell_1 & 0 & 0 & \cdots & & & & & 0 \\
0 & \ell_2 & 0 & \cdots & & & & & 0 \\
\vdots & & \ddots & & & & & & \vdots \\
0 & \cdots & & \ell_{r_1} & & & & & 0 \\
0 & \cdots & & & m_{r_1+1} & -n_{r_1+1} & & & 0 \\
0 & \cdots & & & n_{r_1+1} & m_{r_1+1} & & & 0 \\
\vdots & & & & & & \ddots & & \vdots \\
0 & \cdots & & & & & & m_{r_2} & -n_{r_2} \\
0 & \cdots & & & & & & n_{r_2} & m_{r_2}
\end{pmatrix},$$

whose determinant is given by

$$\prod_{j=1}^{r_1} \ell_j \prod_{j=r_1+1}^{r_1+r_2} (m_j^2 + n_j^2) = \prod_{j=1}^{r_1} \ell_j \prod_{j=r_1+1}^{r_1+r_2} |\ell_j|^2 = N_F(\ell),$$

as required. □

Now we are in a position to establish the dimension of $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$.

Theorem 3.19 — The Dimension of $\mathcal{L}_{\mathbf{F}}(\mathfrak{U}_{\mathfrak{O}_{\mathbf{F}}})$

If F is a number field with signature $\{r_1, r_2\}$, then $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ is a lattice of dimension $r_1 + r_2 - 1$ in $\mathbb{R}^{r_1+r_2}$.

Proof. By Exercise 3.41 on page 136 and Definition 2.4 on page 65, for each $\alpha \in F$,

$$N_F(\Theta(\alpha)) = N_F(\alpha) = \prod_{j=1}^{r_1} \theta_j(\alpha) \prod_{j=r_1+1}^{r_2} \theta_j(\alpha)\overline{\theta_j(\alpha)} = \prod_{j=1}^{r_1} \theta_j(\alpha) \prod_{j=r_1+1}^{r_2} |\theta_j(\alpha)|^2. \tag{3.33}$$

Therefore, for any $\alpha \in \mathfrak{O}_F$, $\Theta_F(\alpha) \in \mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ if and only if $|N_F(\Theta_F(\alpha))| = 1$. Thus, for any $\ell \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $|N_F(\Theta_F(\alpha))| = 1$, we must have $|\det(\lambda_\ell)| = 1$, by Lemma

3.5. Hence, the lattiesΘ $_F(\mathfrak{O}_F)$ and $\lambda_\ell(\Theta_F(\mathfrak{O}_F))$, with $|\det(\lambda_\ell)| = 1$, have the same fundamental parallelotopes with the same volume, namely

$$V(\Theta(\mathfrak{O}_F)) = (V(\lambda_\ell(\Theta(\mathfrak{O}_F)))) = 2^{-r_2}\sqrt{|\Delta_F|},$$

by Claim 3.5 on page 115.

Let $c_j \in \mathbb{R}^+$ for $1 \le j \le r_1 + r_2$, and set

$$\mathcal{S} = \{(\ell_1, \ldots, \ell_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |\ell_j| < c_j \text{ for } 1 \le j \le r_1;\ |\ell_j|^2 < c_j \text{ for } r_1 < j \le r_1 + r_2\}.$$

By the same reasoning as that given in the proof of Theorem 3.12 in Case 3.5 on page 118, we deduce

$$V(\mathcal{S}) = 2^{r_1}\pi^{r_2}\prod_{j=1}^{r_1+r_2} c_j.$$

Now the object is to use Minkowski's Convex Body Theorem to get certain required points in $\lambda_\ell(\theta_F(\mathfrak{O}_F))$. To be able to invoke Minkowski's Theorem, we need

$$V(\mathcal{S}) > 2^n 2^{-r_2}\sqrt{|\Delta_F|} = 2^n V(\lambda_\ell(\Theta_F(\mathfrak{O}_F))). \tag{3.34}$$

To achieve this, we can assume that the c_j were chosen such that (3.34) holds, with $|\det(\lambda_\ell)| = 1$. Therefore, there exists a nonzero $\alpha \in \mathfrak{O}_F$ such that $\lambda_\ell(\Theta_F(\alpha)) \in \mathcal{S}$. Then, for $\ell = (\ell_1, \ldots, \ell_{r_1+r_2})$,

$$\lambda_\ell(\Theta_F(\alpha)) = (\theta_1(\alpha)\ell_1, \ldots, \theta_{r_1+r_2}(\alpha)\ell_{r_1+r_2}),$$

with

$$|\theta_j(\alpha)\ell_j| < c_j \text{ for } 1 \le j \le r_1, \text{ and } |\theta_j(\alpha)\ell_j|^2 < c_j \text{ for } r_1 < j \le r_1 + r_2. \tag{3.35}$$

Since $|\det(\lambda_\ell)| = 1$, then by (3.33)

$$|N_F(\alpha)| = \prod_{j=1}^{r_1}|\theta_j(\alpha)| \prod_{j=r_1+1}^{r_1+r_2}|\theta_j(\alpha)|^2 < \prod_{j=1}^{r_1+r_2} c_j.$$

By Theorem 3.17 on page 127, there exist only finitely many $\alpha \in \mathfrak{O}_F$ such that for all k,

$$|\theta_k(\alpha)| \le \prod_{j=1}^{r_1+r_2} c_j.$$

Let $\{\beta_1, \ldots, \beta_k\}$ be the set formed by α. Then α must be an associate of one of the β_j's since the norms are the same for α and one of the β_j's. Let $\alpha = u_1\beta_t$ for some $t = 1, \ldots, k$, where $u_1 \in \mathfrak{U}_{\mathfrak{O}_F}$. Also, in view of (3.35), $|\theta_j(\alpha)\ell_j| = |\theta_j(u_1)\ell_j\theta_j(\beta_t)| < c_j$, for each $j = 1, \ldots, r_1$, and $|\theta_j(\alpha)\ell_j|^2 = |\theta_j(u_1)\ell_j\theta_j(\beta_t)|^2 < c_j$, for $j = r_1 + 1, \ldots r_1 + r_2$.

Let $a_j = \min_{1\le t\le k}\{|\theta_j(\beta_t)|\}$. Thus, $|\theta_j(u_1)| \cdot |\ell_j| < c_j/a_j \quad (1 \le j \le r_1)$, and $|\theta_j(u_1)| \cdot |\ell_j| < \sqrt{c_j}/a_j \quad (r_1 < j \le r_1 + r_2)$. Now we place a further restriction upon ℓ (other than $|\det(\lambda_\ell)| = 1$), namely we assume that for some $B \in \mathbb{R}^+$,

$$|\ell_1| = \frac{1}{B^{r_1+r_2-1}},$$

and $|\ell_j| = B \quad (2 \le j \le r_1 + r_2)$. Hence,

$$|\theta_1(u_1)| < \frac{B^{r_1+r_2-1}c_1}{a_1}, \qquad |\theta_j(u_1)| < \frac{c_j}{a_jB} \quad (2 \le j \le r_1),$$

and

$$|\theta_j(u_1)| < \frac{\sqrt{c_j}}{Ba_j} \quad (r_1 < j \le r_1 + r_2).$$

We may also assume that B is selected to be sufficiently large so that $|\theta_j(u_1)| < 1$ for all $j \neq 1$. Therefore, $\mathfrak{l}_j(\theta_j(u_1)) < 0$ for all $j = 2, \ldots, r_1 + r_2$. Also, $|N_F(u_1)| = 1$, so by (3.33) on page 132,

$$\sum_{j=1}^{r_1+r_2} \mathfrak{l}_j(\theta_j(u_1)) = 0, \tag{3.36}$$

so

$$\mathfrak{l}_1(\theta_1(u_1)) = -\sum_{j=2}^{r_1+r_2} \mathfrak{l}_j(\theta_j(u_1)) > 0.$$

Continuing in the above fashion, we can manufacture units $u_2, u_3, \ldots, u_{r_1+r_2-1} \in \mathfrak{U}_{\mathfrak{O}_F}$, such that

$$\mathfrak{l}_j(\theta_j(u_i)) < 0 \text{ if } i \neq j, \tag{3.37}$$

and

$$\sum_{j=1}^{r_1+r_2-1} \mathfrak{l}_j(\theta_j(u_i)) > 0 \text{ for all } i = 1, \ldots, r_1 + r_2 - 1, \tag{3.38}$$

where (3.38) follows from the fact that

$$\sum_{j=1}^{r_1+r_2} \mathfrak{l}_j(\theta_j(u_i)) = \log_e(|N_F(\alpha)|) = 0, \text{ and } \mathfrak{l}_{r_1+r_2}(\theta_j(u_i)) < 0,$$

with the first equality stemming from (3.33).

Now we introduce a map that reduces the dimension by one. This will put us within striking distance of the main result. Let $\mathbf{P} : \mathbb{R}^{r_1+r_2} \mapsto \mathbb{R}^{r_1+r_2-1}$ be given by the projection,

$$\mathbf{P}(\ell_1, \ldots, \ell_{r_1+r_2}) \mapsto (\ell_1, \ldots, \ell_{r_1+r_2-1}).$$

Claim 3.10 The vectors $\mathbf{P}(\mathcal{L}_F(u_i))$ for $1 \le i \le r_1 + r_2 - 1$ are $\mathbb{R}$-linearly independent.

Let $M = (m_{i,j}) \in \mathcal{M}_{n \times n}$ be the matrix given by $m_{i,j} = \mathbf{P}(\mathcal{L}_F(u_i))$, and $n = r_1 + r_2 - 1$ for convenience. Hence, $m_{i,j} < 0$ if $i \neq j$, and

$$\sum_{j=1}^{n} m_{i,j} > 0 \text{ for all } i = 1, \ldots, n. \tag{3.39}$$

We will have the result if M is nonsingular. Assume that it is not. Then there exist $r_j \in \mathbb{R}$, not all zero, such that

$$\sum_{j=1}^{n} m_{i,j} r_j = 0 \text{ for all } i = 1, \ldots, n.$$

Let $n_0 \in \mathbb{N}$ with $n_0 \le n$ such that $|r_{n_0}| \ge |r_j|$ for all $j = 1, \ldots, n$, and assume that $r_{n_0} > 0$ (since we may otherwise replace all r_j by $-r_j$). Thus, by (3.39),

$$0 = r_{n_0} m_{n_0,n_0} + \sum_{j \neq n_0} m_{n_0,j} r_j > r_{n_0} m_{n_0,n_0} + \left(\sum_{j \neq n_0} m_{n_0,j} \right) r_{n_0} > 0,$$

a contradiction that establishes Claim 3.10, and hence the entire result. □

Theorem 3.20 — Dirichlet's Unit Theorem

Suppose that F is a number field with signature $\{r_1, r_2\}$, and let $m = |\mathcal{R}_F|$. Then

$$\mathfrak{U}_{\mathfrak{O}_F} \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r_1+r_2-1 \text{ copies}} \times \langle \zeta_m \rangle \cong \langle u_1 \rangle \times \langle u_2 \rangle \times \cdots \times \langle u_{r_1+r_2-1} \rangle \times \langle \zeta_m \rangle,$$

where ζ_m is a primitive m^{th} root of unity. Any such system of units u_j for $j = 1, \ldots, r_1 + r_2 - 1$ is called a *fundamental system of units*.

Proof. By Theorem 3.19 on page 132, there exist units u_j for $j = 1, \ldots, r_1 + r_2 - 1$ such that $\mathcal{L}_F(\mathfrak{U}_{\mathfrak{O}_F})$ has $\mathcal{L}_F(u_j)$ as a $\mathbb{Z}$-basis. Thus, for any $u \in \mathfrak{U}_{\mathfrak{O}_F}$, there exist unique $z_j \in \mathbb{Z}$ such that

$$\mathcal{L}_F(u) = \sum_{j=1}^{r_1+r_2-1} z_j \mathcal{L}_F(u_j).$$

Therefore,

$$\mathcal{L}_F\left(u \prod_{j=1}^{r_1+r_2-1} u^{-z_j}\right) = 0.$$

To complete the proof, we need to show that if $\mathcal{L}_F(v) = 0$ for $v \in \mathfrak{U}_{\mathfrak{O}_F}$, then $v \in \mathcal{R}_F$. However, this is Lemma 3.4 on page 131. □

Application 3.1 —Units in Real Quadratic Fields

A simple application of Theorem 3.20 is to a real quadratic field. Since $r_1 = 2$, and $r_2 = 0$ for $F = \mathbb{Q}(\sqrt{\Delta_F})$, $\mathfrak{U}_{\mathfrak{O}_F} \cong \langle u_1 \rangle \times \langle -1 \rangle$, namely there exists a smallest unit $u_1 > 1$ such that for any $u \in \mathfrak{U}_{\mathfrak{O}_F}$, $u = \pm u_1^a$ for some $a \in \mathbb{Z}$. We denote u_1 by ε_{Δ_F} and call this **the fundamental unit** of $\mathbb{Q}(\sqrt{\Delta_F})$. The uniqueness is given by Dirichlet's Theorem and our insistence that the unit be bigger than 1 as a generator. Since$\Delta_F > 0$, then $\mathcal{R}_F = \langle -1 \rangle = \langle \zeta_2 \rangle$.

Example 3.5 If $F = \mathbb{Q}(\sqrt{\Delta_F})$ for$\Delta_F < 0$, then $r_1 = 0$, and $r_2 = 1$, so $\mathfrak{U}_{\mathfrak{O}_F} = \mathcal{R}_F$ as given by Theorem 1.29 on page 47.

Based upon fundamental systems of units, we now show that determinants of logarithmic representations do not vary. This will allow for the definition of another invariant of a number field F.

Theorem 3.21 — Determinants of Logarithmic Maps

Suppose that F is a number field with signature $\{r_1, r_2\}$, and $\{u_i\}$, $\{v_i\}$ for $i = 1, 2, \ldots, r_1 + r_2 - 1$ are systems of fundamental units. Then $|\det(\mathcal{L}_F(u_i))| = |\det(\mathcal{L}_F(v_i))|$, where $(\mathcal{L}_F(u_i))$ is a matrix with entries $\log_e(|\theta_j(u_i)|)$, and $(\mathcal{L}_F(v_i))$ is a matrix with entries $\log_e(|\theta_j(v_i)|)$, where θ_j are the embeddings of F in $\mathbb{C}$.

Proof. Set $r = r_1 + r_2 - 1$, and assume that $|\mathcal{R}_F| = m$. By Dirichlet's Unit Theorem, we may write, for each $i = 1, \ldots, r$,

$$v_i = \zeta_m^{b_i} \prod_{j=1}^{r} u_j^{a_{i,j}} \quad (b_i, a_{i,j} \in \mathbb{Z}),$$

and

$$u_i = \zeta_m^{c_i} \prod_{j=1}^{r} v_j^{d_{i,j}} \quad (c_i, d_{i,j} \in \mathbb{Z}).$$

By uniqueness of representation of units, $(d_{i,j})^{-1} = (a_{i,j})$, so $\det((a_{i,j})(d_{i,j})) = 1$. Hence, $|\det(a_{i,j})| = |\det(d_{i,j})|$. Since

$$\theta_j(v_i) = \theta_j(\zeta_m^{b_i}) \prod_{k=1}^{r} \theta_j(u_k)^{a_{i,k}},$$

then $\log_e(|\theta_j(v_i)|) = \log_e(|\theta_j(\zeta_m^{b_i})|) + \sum_{k=1}^r a_{i,k} \log_e(|\theta_j(u_k)|) = \sum_{k=1}^r a_{i,k} \log_e(|\theta_j(u_k)|)$, where the last equality follows from Corollary 3.10 on page 128. Hence,

$$|\det(\log_e(|\theta_j(v_i)|))| = |\det(\log_e(|\theta_j(u_i)|))|,$$

so $|\det(\mathcal{L}_F(v_i))| = |\det(\mathcal{L}_F(u_i)|$, which is what we sought. □

Based upon Theorem 3.21, we may now define an invariant of F.

Definition 3.15 — Regulators

Let $\{u_1, \ldots, u_{r_1+r_2-1}\}$ be a fundamental system of units of a number field F having signature $\{r_1, r_2\}$. Then the *regulator* of F is given by

$$\mathfrak{r}_F = |\det(\mathcal{L}_F(u_j))|. \tag{3.40}$$

Computation of the regulator, given in Equation (3.40), of a number field is difficult, since we must know in advance a fundamental system of units. However, for real quadratic fields, knowledge of *the* fundamental unit is sufficient and tables of such units exist (for instance, see [49, Appendix B, pp. 287–312]).

Example 3.6 If $F = \mathbb{Q}(\sqrt{5})$, then $r_1 = 2$, and $r_2 = 0$. Since the fundamental unit is $\varepsilon_5 = (1+\sqrt{5})/2$, then

$$\mathfrak{r}_F = \log_e\left(\frac{1+\sqrt{5}}{2}\right).$$

Exercises

3.41. Prove that the logarithmic representation $\mathcal{L}_F$ of Definition 3.13 is a homomorphism of the the multiplicative group F^* of nonzero elements of F to the additive group of $\mathbb{R}^{r_1+r_2}$.

3.42. Let F be a number field. Prove that $\ker(\mathcal{L}_F) = \mathcal{R}_F$.

3.43. Let F be a real quadratic number field with$\Delta_F \equiv 5 \pmod 8$, and fundamental unit $\varepsilon_{\Delta_F} = (T + U\sqrt{\Delta_F})/2$, where $T, U \in \mathbb{Z}$. Let G be the subgroup of $\mathbb{Z}[\sqrt{\Delta_F}]$ consisting of the positive units. Prove that $G = \langle \varepsilon_{\Delta_F} \rangle$ if and only if T and U are both even.

3.44. With reference to Exercise 3.43, prove that $G = \langle \varepsilon_{\Delta_F}^3 \rangle$ if T and U are odd.

(*This is related to a problem of Eisenstein, namely the determination of criteria for the solvability of the Diophantine equation* $|x^2 - \Delta_F y^2| = 4$ *with* $\gcd(x,y) = 1$ *for* $x, y \in \mathbb{Z}$. *There is an underlying interplay between the two rings* $\mathbb{Z}[\sqrt{\Delta_F}]$, *and* $\mathbb{Z}[(1+\sqrt{\Delta_F})/2]$ *that helps to explain the phenomenon. Solution of the aforementioned Diophantine equation, for* $\Delta_F \equiv 5 \pmod 8$, *is equivalent to* $\varepsilon_{\Delta_F} \notin \mathbb{Z}[\sqrt{\Delta_F}]$. *See* [49, Exercises 2.1.14–2.1.16, pp. 59–61]. Also, see Example 1.32 on page 52.)

Biography 3.10 Ferdinand Gotthold Max Eisenstein (1823–1852) was born on April 16, 1823 in Berlin, Germany. From an early age he suffered from ill health. While still young, he travelled with his parents to Wales and Ireland where he met W.R. Hamilton, who acquainted Eisenstein with the work of Abel. This inspired Eisenstein to study mathematics further, and he enrolled at the University of Berlin upon his return to Germany. Subsequently he produced many papers, twenty-five of which were published in *Crelle's Journal* where Abel had published his pioneering work. Among his achievements was the introduction of generalized Jacobi sums to obtain a proof of the law of biquadratic reciprocity. Gauss had such respect for him that he is purported to have said that there were only three epoch-making mathematicians: Archimedes, Newton, and Eisenstein. However, due to his ill health, Eisenstein was not allowed to fulfill this assessment. Humboldt had collected money for Eisenstein to travel to Sicily to improve his health. However, he died before he could go there. His death occurred, at the age of twenty-nine, from pulmonary tuberculosis on October 11, 1852

If F is a quadratic number field and $I^2 \sim 1$ in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$, then $\mathbf{I}$ is called an ambiguous class *in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$. If $I = (a, (b + \sqrt{\Delta_F})/2)$ is an integral $\mathfrak{O}_F$-ideal, then $I' = (a, (b - \sqrt{\Delta_F})/2)$ is the conjugate ideal of I, which we introduced for prime quadratic ideals in Remark 1.24 on page 52 and illustrated further in Example 2.15 on page 85. Thus, via Exercise 3.20 on page 107, an ambiguous class of $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ is a class $\mathbf{I}$ in which $I \sim I'$. Indeed, for an ambiguous class, $\mathbf{I} = \mathbf{I}^{-1}$. If $I = I'$, then I is called an ambiguous $\mathfrak{O}_F$-ideal. For a prime $p \in \mathbb{Z}$, the maximum elementary abelian p-subgroup of $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ is denoted by $\mathbf{C}_{\mathfrak{O}_F,p}$, if $|\mathbf{C}_{\mathfrak{O}_F,p}| = p^r$, the r is called the p-rank of $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$—see Definition A.3 on page 320. We let $h_{\mathfrak{O}_F,p}$ denote the order of $\mathbf{C}_{\mathfrak{O}_F,p}$.*

Exercises 3.45–3.54 below are devoted to studying these ideal classes, and in particular to establishing Gauss' result on the 2 rank of $\mathfrak{O}_F$—Exercises 3.48 and 3.54. Thus, in these exercises, we are assuming that F is a quadratic number field with discriminant Δ_F.

3.45. Suppose that either$\Delta_F < 0$ or$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = -1$. Prove that every class of $\mathbf{C}_{\mathfrak{O}_F,2}$ has an ambiguous ideal in it.

(*Hint: Use Exercise 3.21 on page 107.*)

☆ 3.46. Let$\Delta_F < 0$ be the discriminant of a quadratic field F over $\mathbb{Q}$, and let ω_{Δ_F} be defined as in Application 2.1 on page 77. Suppose that $I = (a, b \pm \omega_{\Delta_F})$ is an integral $\mathfrak{O}_F$-ideal with $a > 1$, $b \geq 0$, and $N_F(b \pm \omega_{\Delta_F}) < N_F(\omega_{\Delta_F})^2$. Prove that $I \sim 1$ if and only if $a = N_F(b \pm \omega_{\Delta_F})$.

3.47. Suppose that I is an integral $\mathfrak{O}_F$-ideal in a quadratic field $F = \mathbb{Q}(\sqrt{\Delta_F})$. Prove that $N(I) \mid \Delta_F$ if and only if $I = I'$.

☆ 3.48. Suppose that either$\Delta_F < 0$ or$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = -1$ and thatΔ_F is divisible by N distinct primes. Prove that $h_{\mathfrak{O}_F,2} = 2^{N-1}$.

(*Hint: Use Exercises 3.45–3.46.*)

3.49. Assume that$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = 1$. Then by Exercise 3.21, $\varepsilon_{\Delta_F} = \alpha/\alpha'$ for some $\alpha \in \mathfrak{O}_F$. Prove that the only primitive ambiguous $\mathfrak{O}_F$-ideals are (α), $\sqrt{D_F}$, $\mathfrak{O}_F$, and $(\alpha\sqrt{D_F})$, where D_F is the radicand of F defined in Application 2.1 on page 77.

3.50. Suppose that $\alpha \in I$ where I is an $\mathfrak{O}_F$-ideal with $N(I) = |N_F(\alpha)|$. Prove that $I = (\alpha)$.

3.51. If I is a primitive integral $\mathfrak{O}_F$-ideal, prove that $(N(I)) = II'$.

3.52. Assume thatΔ_F has only one prime divisor, namely$\Delta_F = q \equiv 1 \pmod 4$ is prime or $\Delta_F = 8$. Prove that $N_F(\varepsilon_{\Delta_F}) = -1$.

(*Hint: Use Exercises 3.21 on page 107 and 3.47.*)

3.53. Using Exercise 3.52, prove that for any prime $p \equiv 1 \pmod 4$, there exist $x, y \in \mathbb{Z}$ such that $x^2 - py^2 = -1$.

3.54. Assume that$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = 1$. Prove that $h_{\mathfrak{O}_F,2} = 2^{N-2}$.

(*Hint: Use Exercises 3.49–3.52.*)

Let F be a quadratic number field. An $\mathfrak{O}_F$-ideal $I = [N(I), \alpha]$ is called reduced *if it is primitive and there does* not *exist an element $\gamma \in I$ such that both $|\gamma| < N(I)$ and $|\gamma'| < N(I)$. Exercises 3.55–3.61 are in reference to reduction in quadratic number fields.*

✰ 3.55. Prove that if$\Delta_F > 0$, then I is reduced if and only if there is an element $\beta \in I$ such that $I = [N(I), \beta]$, $\quad \beta > N(I)$, and $-N(I) < \beta' < 0$.

(*Note that when $\Delta_F < 0$, then this means that there is no $\gamma \in I$ such that $|\gamma| < N(I)$ where $|\gamma|^2 = \gamma\gamma' = N_F(\gamma)$. The notion of reduction comes from the theory of binary quadratic forms—see Definition 3.4 on page 90.*)

3.56. Prove that if $N(I) < \sqrt{|\Delta_F|/2}$, then I is reduced.

3.57. Prove that if I is reduced, then $N(I) < \sqrt{\Delta_F}$, when F is real, and $N(I) < \sqrt{|\Delta_F|/3}$ when F is complex.

✰ 3.58. Let I be a primitive, ambiguous $\mathfrak{O}_F$-ideal, where$\Delta_F > 0$. Prove that if $N(I) < \sqrt{\Delta_F}$, then either I is reduced, or$\Delta_F \equiv 0 \pmod 4$, and I divides the ideal $(\sqrt{\Delta_F/4})$.

3.59. Let I be a primitive, ambiguous $\mathfrak{O}_F$-ideal, where$\Delta_F > 0$. Prove that there exists a reduced ambiguous ideal J such that $J \sim I$.

3.60. Let I be a reduced ambiguous $\mathfrak{O}_F$-ideal, such that $I \neq (1)$, and$\Delta_F > 0$. If $4 \mid \Delta_F$, then also assume that

$$I \neq \left(2, b + \sqrt{\Delta_F/4}\right), \text{ where } b \equiv \Delta_F/2 \pmod 2.$$

Prove that either $N(I)$ or $N(I)/2$ is a nontrivial factor of the radicand D of F.

(*This exercise underlies the fact that the so-called Continued Fraction Algorithm can be used as a method for factoring—see* [49].)

3.61. Suppose that F is a real quadratic field. Let I be a primitive principal $\mathfrak{O}_F$-ideal, such that $\gcd(N(I), D) = 1$, and $N(I) = n^2$ for some $n \in \mathbb{N}$. Prove that there is an $\mathfrak{O}_F$-ideal J such that $I = J^2$.

Remark 3.16 Note that in Exercises 3.43–3.44, and 3.52–3.53, we are essentially dealing with the solutions of *Pell's equation* $x^2 - Dy^2 = \pm 1$. Euler misattributed a method of solving this equation to John Pell (1611–1685), whence its name. However, another English mathematician, William Brouncker (1601–1665) actually found the method. Lagrange was the first to prove that the positive Pell equation always has infinitely many solutions—see Biography 3.3 on page 93. The above exercises show that the Pell equation is actually about the fundamental unit of a quadratic field. Often, in an elementary number theory course, continued fractions are employed to solve the equation—see [53, §5.3, pp. 232–239] for instance.

Chapter 4

Applications: Equations and Sieves

> *If we could find the answer to that* [why it is that we and the universe exist], *it would be the ultimate triumph of human reason—for then we would know the mind of God.*
>
> *from* **A Brief History of Time (1988)**.
>
> **Stephen Hawking (1942–)**
>
> *English theoretical physicist*

This chapter is devoted to looking at how we may apply the first three chapters to the solutions of Diophantine equations and to factoring via the number field sieve and Pollard's sieve.

4.1 Prime Power Representation

We have looked at representation problems, without calling them such, in Example 2.16 on page 85 for instance. Also, emanating from Theorem 1.30 on page 49, we may expand our understanding by employing it as follows, some of which is adapted from [54].

Recall that by Corollary 3.4 on page 106, we know that $h_{\mathfrak{O}_\mathbf{F}} < \infty$. Also, recall from Application 3.1 on page 135 the definition of ε_{Δ_F} as the fundamental unit of a real quadratic field.

Theorem 4.1 — Prime Representation and $\mathbf{h}_{\mathfrak{O}_\mathbf{F}}$

Let F be a quadratic field with discriminantΔ_F and (wide) class number $h_{\mathfrak{O}_\mathbf{F}}$. Suppose that $p > 2$ is a prime such that $\gcd(\Delta_F, p) = 1$ andΔ_F is a quadratic residue modulo p. Then the following hold.

(a) If either$\Delta_F < 0$ or$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = -1$, then there exist relatively prime integers a, b such that

$$p^{h_{\mathfrak{O}_\mathbf{F}}} = \begin{cases} a^2 - \Delta_F b^2 & \text{if}\Delta_F \equiv 1 \pmod 8, \\ a^2 - \frac{\Delta_F}{4} b^2 & \text{if}\Delta_F \equiv 0 \pmod 4, \\ a^2 + ab + \frac{1}{4}(1 - \Delta_F) b^2 & \text{if}\Delta_F \equiv 5 \pmod 8. \end{cases}$$

(b) If$\Delta_F > 0$ and $N_F(\varepsilon_{\Delta_F}) = 1$, then there exist relatively prime integers a, b such that

$$p^{h_{\mathfrak{O}_\mathbf{F}}} = \begin{cases} \pm(a^2 - \Delta_F b^2) & \text{if} \quad {}_F \equiv 1\,(\mathrm{mod}\ 8)\Delta, \\ \pm(a^2 - \frac{\Delta_F}{4} b^2) & \text{if} \quad {}_F \equiv 0\,(\mathrm{mod}\ 4)\Delta, \\ \pm(a^2 + ab + \frac{1}{4}(1-\Delta_F)b^2) & \text{if} \quad {}_F\Delta \equiv 5\,(\mathrm{mod}\ 8). \end{cases}$$

Proof. By Theorem 1.30, since $p > 2$, then if $(\Delta_F/p) = 1$, we have $(p) = \mathcal{P}_1\mathcal{P}_2$ where $\mathcal{P}_j$ are distinct prime $\mathfrak{O}_F$-ideals for $j = 1, 2$. Thus,

$$(p^{h_{\mathfrak{O}_\mathbf{F}}}) = (p)^{h_{\mathfrak{O}_\mathbf{F}}} = \mathcal{P}_1^{h_{\mathfrak{O}_\mathbf{F}}}\mathcal{P}_2^{h_{\mathfrak{O}_\mathbf{F}}} \sim (1),$$

since ${\mathcal{P}_\mathbf{j}}^{h_{\mathfrak{O}_\mathbf{F}}} \sim (1)$ for $j = 1, 2$ by Exercise 3.18 on page 107. Hence, $\mathcal{P}_j^{h_{\mathfrak{O}_\mathbf{F}}}$ is a principal ideal for $j = 1, 2$. Let

$$\mathcal{P}_1^{h_{\mathfrak{O}_\mathbf{F}}} = \left(\frac{u + v\sqrt{\Delta_F}}{2}\right)$$

where $u \equiv v\,(\mathrm{mod}\ 2)$, if$\Delta$ ${}_F \equiv 1\,(\mathrm{mod}\ 4)$, and u is even ifΔ ${}_F \equiv 0\,(\mathrm{mod}\ 4)$. Then via the proof of Theorem 1.30 we know that $\mathcal{P}_2$ must be the conjugate of $\mathcal{P}_1$, namely

$$\mathcal{P}_2^{h_{\mathfrak{O}_\mathbf{F}}} = \left(\frac{u - v\sqrt{\Delta_F}}{2}\right).$$

Hence,

$$(p^{h_{\mathfrak{O}_\mathbf{F}}}) = \left(\frac{u^2 - \Delta_F v^2}{4}\right),$$

so there exists an $\alpha \in \mathfrak{U}_F$ such that

$$p^{h_{\mathfrak{O}_\mathbf{F}}} = \alpha\left(\frac{u^2 - \Delta_F v^2}{4}\right).$$

However,

$$\alpha = \frac{4p^{h_{\mathfrak{O}_\mathbf{F}}}}{u^2 - \Delta_F v^2} \in \mathbb{Q}.$$

But, by Corollary 1.12 on page 37, $\mathfrak{O}_F \cap \mathbb{Q} = \mathbb{Z}$, so $\alpha \in \mathfrak{U}_\mathbb{Z} = \{\pm 1\}$. Thus,

$$4p^{h_{\mathfrak{O}_\mathbf{F}}} = \pm(u^2 - \Delta_F v^2). \tag{4.1}$$

Claim 4.1 IfΔ ${}_F \equiv 0\,(\mathrm{mod}\ 4)$, then $\gcd(u/2, v) = 1$, and ifΔ ${}_F \equiv 1\,(\mathrm{mod}\ 4)$, $\gcd(u, v) = 1$ or 2.

IfΔ ${}_F \equiv 1\,(\mathrm{mod}\ 4)$, let $q > 2$ be a prime such that $q \mid \gcd(u, v)$. Then there exist integers x, y such that $u = qx$ and $v = qy$, where $x \equiv y\,(\mathrm{mod}\ 2)$. Therefore, by (4.1), $q^2 \mid 4p^{h_{\mathfrak{O}_\mathbf{F}}}$, but $q > 2$ so $q = p$. Hence,

$$\mathcal{P}_1^{h_{\mathfrak{O}_\mathbf{F}}} = (p)\left(\frac{x + y\sqrt{\Delta_F}}{2}\right) = \mathcal{P}_1\mathcal{P}_2\left(\frac{x + y\sqrt{\Delta_F}}{2}\right),$$

which forces $\mathcal{P}_2 \mid \mathcal{P}_1^{h_{\mathfrak{O}_\mathbf{F}}}$, contradicting that $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct $\mathfrak{O}_F$-ideals. We have shown that $\gcd(u, v) = 2^c$ for some integer $c \geq 0$. It follows from (4.1) that $4^c \mid 4$ so $c = 0$ or $c = 1$.

IfΔ ${}_F \equiv 0\,(\mathrm{mod}\ 4)$, and q is a prime such that $q \mid \gcd(u/2, v)$, then there exist integers x, y such that $u = 2qx$ and $v = qy$, so

$$p^{h_{\mathfrak{O}_\mathbf{F}}} = \pm((qx)^2 - (\Delta_F/4)(qy)^2)$$

which forces $p = q$ and this leads to a contradiction as above. This is Claim 4.1.

If$\Delta_F < 0$ then the plus sign holds in (4.1), since $u^2 - \Delta_F v^2 > 0$. When$\Delta_F > 0$ and there exists an $\alpha \in \mathfrak{U}_F$ with $N_F(\alpha) = -1$, we may multiply by

$$N_F(\alpha) = N(r + s\sqrt{\Delta_F}) = r^2 - \Delta_F s^2 = -1$$

to get

$$-(u^2 - \Delta_F v^2) = (r^2 - \Delta_F s^2)(u^2 - \Delta_F v^2) = (ru + \Delta_F sv)^2 - \Delta_F(rv + su)^2.$$

To complete the proof, we need only show how the a, b may be selected to satisfy parts (a)–(b) of our theorem.

When$\Delta_F \equiv 1 \pmod 4$, then by (4.1), if u and v are odd, $4p^{h_{\mathfrak{O}_{\mathbf{F}}}} \equiv 0 \pmod 8$, contradicting that $p > 2$. Thus, by Claim 4.1, $\gcd(u, v) = 2$ so we select $a = u/2$ and $b = v/2$. If $\Delta_F \equiv 0 \pmod 4$, then by Claim 4.1, we may select $a = u/2$ and $b = v$. Lastly, when$\Delta_F \equiv 5 \pmod 8$, since $u \equiv v \pmod 2$, set $u = b + 2a$ and $b = v$ where $a, b \in \mathbb{Z}$. Then (4.1) becomes,

$$\pm 4p^{h_{\mathfrak{O}_{\mathbf{F}}}} = u^2 - \Delta_F v^2 = (b + 2a)^2 - \Delta_F b^2 = 4a^2 + 4ab + (1 - \Delta_F)b^2,$$

so

$$p^{h_{\mathfrak{O}_{\mathbf{F}}}} = \pm(a^2 + ab + \frac{1}{4}(1 - \Delta_F)b^2),$$

which secures our result. □

Remark 4.1 As a counterfoil to Theorem 4.1 on page 139, we note that, by Exercise 3.9 on page 94, ifΔ_F is not a quadratic residue modulo a prime $p > 2$, then there is no binary quadratic form that represents p^k for any positive integer k. Hence, there cannot exist integers (a, b, c) such that $p^k = ax^2 + bxy + cy^2$ for any integers x, y.

Theorem 4.1 has certain value when $h_{\mathfrak{O}_{\mathbf{F}}} = 1$. In particular, we have the following results, the first of which is a special case of Theorem A.27 on page 343.

Corollary 4.1 Let p be a prime. Then there exist relatively prime integers a, b such that

$$p = a^2 + b^2 \text{ if and only if } p = 2 \text{ or } p \equiv 1 \pmod 4.$$

Proof. By Theorems 3.2 on page 92 and 3.6 on page 103, for$\Delta_F = -4$,

$$h_{\mathfrak{O}_{\mathbf{F}}} = h_{\mathbb{Z}[\sqrt{-1}]} = 1.$$

Thus, by Theorem 4.1, if $(\Delta_F/p) = 1$, namely $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for $a, b \in \mathbb{N}$. Since $2 = 1^2 + 1^2$, then we have one direction. Conversely, if $p = a^2 + b^2$, and $p > 2$, then by Exercise 3.9 on page 94, $(-4/p) = (-1/p) = 1$, which implies that $p \equiv 1 \pmod 4$. □

Corollary 4.2 Let p be a prime. Then there exist relatively prime integers a, b such that

$$p = a^2 + 2b^2 \text{ if and only if } p = 2 \text{ or } p \equiv 1, 3 \pmod 8.$$

Proof. First, we know that $(-8/p) = (-2/p) = 1$ if and only if $p \equiv 1, 3 \pmod 8$. By Theorems 3.2 and 3.6, for$\Delta_F = -8$,

$$h_{\mathfrak{O}_{\mathbf{F}}} = h_{\mathbb{Z}[\sqrt{-1}]} = 1.$$

Therefore, by Theorem 4.1, if $(-8/p) = 1$, $p = a^2 + 2b^2$ for $a, b \in \mathbb{N}$. Also, $2 = 0^2 + 2 \cdot 1^2$. Conversely, if

$$p = a^2 + 2b^2, \text{ and } p > 2,$$

then by Exercise 3.9, $(-8/p) = (-2/p) = 1$. □

Corollary 4.3 Let p be a prime. Then there exist relatively prime integers a, b such that

$$p = a^2 + ab + b^2 \text{ if and only if } p = 3 \text{ or } p \equiv 1 \pmod 3.$$

Proof. From Exercise 4.1, $(-3/p) = 1$ if and only if $p \equiv 1 \pmod 3$. By Corollaries 1.1–1.2 on page 13, Theorem 1.28 on page 45, and Theorem 3.6 on page 103, we have that

$$h_{\mathbb{Z}[(1+\sqrt{-3})/2]} = 1.$$

Thus, by Theorem 4.1, if $(\Delta_F/p) = (-3/p) = 1$, then

$$p = a^2 + ab + b^2 \text{ for some integers } a, b.$$

Also $3 = 1^2 + 1 \cdot 1 + 1^2$. Conversely, by Exercise 3.9, if $p > 3$ and $p = a^2 + ab + b^2$, then $(-3/p) = 1$. □

Corollary 4.4 Let p be a prime. Then there exist relatively prime integers a, b such that $p = a^2 + 7b^2$ if and only if $p = 7$ or

$$p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}.$$

Proof. By Exercise 4.2, $(-7/p) = 1$ if and only if

$$p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}.$$

Also, as in the proof of Corollary 4.3, for$\Delta_F = -7$,

$$h_{\mathfrak{O}_\mathbf{F}} = h_{\mathbb{Z}[(1+\sqrt{-7})/2]} = h_{-7} = 1.$$

Therefore, by Theorem 4.1, if $(-7/p) = 1$, $p = a^2 + 7b^2$ for $a, b \in \mathbb{N}$. Also, $7 = 0^2 + 7 \cdot 1^2$. Conversely, if

$$p = a^2 + 7b^2, \text{ and } p \neq 7,$$

then by Exercise 3.9, $(-7/p) = 1$. □

Exercises

4.1. Prove that $(-3/p) = 1$ for a prime $p > 3$ if and only if $p \equiv 1 \pmod 3$.

(*Hint: You may use* (A.11) on page 342.)

4.2. Prove that $(-7/p) = 1$ for an odd prime p if and only if $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$.

In Exercises 4.3–4.6, use the techniques of Corollary 4.3 to solve the representation problems.

4.3. Prove that a prime p is representable in the form

$$p = a^2 + ab + 3b^2 \text{ for relatively prime } a, b \in \mathbb{Z}$$

if and only if

$$p = 11 \text{ or } p \equiv 1, 3, 5, 9, 15, 21, 23, 25, 27, 31 \pmod{44}.$$

4.4. Prove that a prime p is representable in the form

$$p = a^2 + ab + 5b^2 \text{ for relatively prime } a, b \in \mathbb{N}$$

if and only if $p = 19$ or

$$p \equiv 1, 5, 7, 9, 11, 17, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73 \pmod{76}.$$

4.5. Prove that a prime p is representable in the form

$$p = a^2 + ab + 11b^2 \text{ for relatively prime } a, b \in \mathbb{Z}$$

if and only if $p = 43$ or

$$p \equiv 1, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81,$$

$$83, 87, 95, 97, 99, 101, 103, 107, 109, 111, 117, 121, 127, 133,$$

$$135, 139, 143, 145, 153, 165, 167, 169 \pmod{172}.$$

4.6. Prove that a prime p is representable in the form

$$p = a^2 + ab + 17b^2 \text{ for relatively prime } a, b \in \mathbb{Z}$$

if and only if $p = 67$ or

$$p \equiv 1, 9, 15, 17, 19, 21, 23, 25, 29, 33, 35, 37, 39, 47, 49, 55, 59, 65, 71, 73, 77, 81,$$

$$83, 89, 91, 93, 103, 107, 121, 123, 127, 129, 131, 135, 143, 149, 151, 153, 155,$$

$$157, 159, 163, 167, 169, 171, 173, 181, 183, 189, 193, 199, 205, 207, 211, 215,$$

$$217, 223, 225, 227, 237, 241, 255, 257, 261, 263, 265 \pmod{268}.$$

4.7. From Corollaries 1.1–1.2 on page 13, Theorem 1.28 on page 45, and Theorem 3.6 on page 103,we know that $h_{\mathfrak{O}_\mathbf{F}} = h_{\mathbb{Z}[(1+\sqrt{-163})/2]} = 1$. Thus, Theorem 4.1 on page 139 informs us that odd primes p with $(\Delta_F/p) = (-163/p) = 1$ satisfy that $p = a^2 + ab + 41b^2$ for some relatively prime integers a, b. Show that for $b = 1$, $a^2 + a + 41$ is indeed prime for $a = 0, 1, \ldots, 39$.

(*This is related to a result of Rabinowitsch* [60], *which states that for negative* Δ_F, *with* $\Delta_F \equiv 1 \pmod 4$, *we have that* $h_{\mathfrak{O}_\mathbf{F}} = 1$ *if and only if* $x^2 + x + (1 - \Delta_F)/4$ *is prime for* $x = 0, 1, \ldots, \lfloor |\Delta_F|/4 - 1 \rfloor$. *The reader may now go to Exercises 4.3–4.6 and verify this fact for those values as well.*)

(*See Biography 4.1 on the next page.*)

4.8. Related to the Rabinowitsch result in Exercise 4.7 is the following, known as the *Rabinowitsch–Mollin–Williams* criterion for real quadratic fields–see [46]. If F is a real quadratic field with discriminant$\Delta_F \equiv 1 \pmod 4$, then $|x^2 + x + (1 - \Delta_F)/4|$ is 1 or prime for all $x = 1, 2, \ldots, \lfloor (\sqrt{\Delta_F} - 1)/2 \rfloor$ if and only if $h_{\mathfrak{O}_\mathbf{F}} = 1$ and either $\Delta_F = 17$ or$\Delta_F = n^2 + r \equiv 5 \pmod 8$ where $r \in\{\pm 4, 1\}$–see [50, Theorem 6.5.13, p. 352]. Verify this primality for the values

$$\Delta_F \in \{17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}.$$

(*See Biography 4.2 on the following page.*)

4.9. It is known that for$\Delta_F = -20$, $h_{\mathfrak{O}_\mathbf{F}} = 2$ and $\mathcal{P} = (2, 1+\sqrt{-5})$ is an ideal representing the nonprincipal class. Use the identification given in the proof of Theorem 3.5 on page 101 to prove the following, where $p \neq 5$ is an odd prime.

(a) $p = a^2 + 5b^2$ if and only if $p \equiv 1, 9 \pmod{20}$.

(b) $p = 2a^2 + 2ab + 3b^2$ if and only if $p \equiv 3, 7 \pmod{20}$.

Biography 4.1 The following was taken from a most interesting article about G. Rabinowitsch by Mordell [55]. Mordell writes: "In 1923, I attended a meeting of the American Mathematical Society held at Vassar College in New York State. Someone called Rainich from the University of Michigan at Ann Arbor, gave a talk upon the class number of quadratic fields, a subject in which I was very much interested. I noticed that he made no reference to a rather pretty paper written by Rabinowitz from Odessa and published in *Crelle's Journal.* I commented upon this. He blushed and stammered and said, "I am Rabinowitz." He had moved to the U.S.A. and changed his name.... The spelling of Rabinowitsch in this book coincides with that which appears in Crelle [60].

Biography 4.2 Hugh Cowie Williams was born in London, Ontario, Canada on July 23, 1943. He graduated with a doctorate in computer science from the University of Waterloo in 1969. Since that time, his research interests have been in using computational techniques to solve problems in number theory, and in particular, those with applications to cryptography. He held a Chair under Alberta Informatics Circle of Research Excellence (iCORE) at the University of Calgary (U of C) until 2009. He oversaw the Centre for Information Security and Cryptography (CISaC), a multi-disciplinary research centre at the U of C devoted to research and development towards providing security and privacy in information communication systems. There are also more than two dozen graduate students and post doctoral fellows being trained at the centre. The iCORE Chair is in algorithmic number theory and cryptography (ICANTC), which is the main funder of CISaC. The initial funding from iCORE was $3 million dollars for the first five years and this has been renewed for another five years. In conjunction with this iCORE Chair, Professor Williams had set up a research team in pure and applied cryptography to investigate the high-end theoretical foundations of communications security. Previous to the iCORE chair, Professor Williams was Associate Dean of Science for Research and Development at the University of Manitoba, as well as, Adjunct Professor for the Department of Combinatorics and Optimization at the University of Waterloo. He has an extensive research and leadership background and a strong international reputation for his work in cryptography and number theory. CISaC and ICANTC were acronyms coined by this author, who initiated the application for the Chair, and is currently a member of the academic staff of CISaC, as well as professor at the U of C's mathematics department. This author and Professor Williams have coauthored more than two dozen papers in number theory, and computational mathematics, over the past quarter century.

4.2 Bachet's Equation

> *No enemy is worse than bad advice.*
>
> **Sophocles (c. 496–406 B.C.)**
> Greek dramatist

In this section we look at unique factorization in certain quadratic domains to find solutions of certain Bachet equations, those of the form

$$y^2 = x^3 + k \tag{4.2}$$

where $k \in \mathbb{Z}$—see Biography 4.3 on page 147.

Theorem 4.2 — General Solutions of Bachet's Equation
Let $F = \mathbb{Q}(\sqrt{k})$ be a complex quadratic field with radicand $k < -1$ such that $k \not\equiv 1 \pmod 4$, and $h_{\mathfrak{O}_F} \not\equiv 0 \pmod 3$. Then there are no solutions of (4.2) in integers x, y except in the following cases: there exists an integer u such that

$$(k, x, y) = (\pm 1 - 3u^2, 4u^2 \mp 1, \varepsilon\, u(3 \mp 8u^2)),$$

where the ± signs correspond to the ∓ signs and $\varepsilon = \pm 1$ is allowed in either case.

Proof. Suppose that for k as given in the hypothesis, (4.2) has a solution.

Claim 4.2 $\gcd(x, 2k) = 1$.

Given that $y^2 \equiv 0, 1 \pmod 4$, and $k \equiv 2, 3 \pmod 4$, then

$$x^3 = y^2 - k \equiv 1, 2, 3 \pmod 4.$$

However, $x^3 \equiv 2 \pmod 4$ is not possible. Hence, x is odd. Now let p be a prime such that $p \mid \gcd(x, 2k)$, where $p > 2$ since x is odd. Since k is a radicand, it is squarefree, so

$$p || k = y^2 - x^3. \tag{4.3}$$

However, $p \mid x$ so $p \mid y$, which implies that $p^2 \mid (y^2 - x^3)$, a contradiction to (4.3), that establishes the claim.

By Claim 4.2, there exist integers r, s such that

$$rx + 2ks = 1. \tag{4.4}$$

Claim 4.3 The $\mathfrak{O}_F$-ideals $(y + \sqrt{k})$ and $(y - \sqrt{k})$ are relatively prime.

If the claim does not hold, then there is a prime $\mathfrak{O}_F$-ideal $\mathcal{P}$ dividing both of the given ideals by Theorem 1.19 on page 30. Therefore, by Corollary 1.7 on page 27, $y \pm \sqrt{D} \in \mathcal{P}$. Therefore, $2\sqrt{k} = y + \sqrt{k} - (y - \sqrt{k}) \in \mathcal{P}$, so

$$2\sqrt{k} \cdot \sqrt{k} = 2k \in \mathcal{P}. \tag{4.5}$$

Given that

$$(y + \sqrt{k})(y - \sqrt{k}) = (y^2 - k) = (x^3) = (x)^3,$$

then by Corollary 1.7 again, since $(x)^3 \subseteq \mathcal{P}$, then $\mathcal{P} \bigm| (x)^3$. However, since $\mathcal{P}$ is prime $\mathcal{P} \bigm| (x)$, and once more by Corollary 1.7, we conclude that

$$x \in \mathcal{P}. \tag{4.6}$$

Now we invoke (4.4)–(4.6) to get that both rx and $2ks$ are in $\mathcal{P}$ so $1 = rx + 2ks \in \mathcal{P}$, a contradiction that establishes the claim.

By Theorem 1.26 on page 42, $\mathfrak{O}_F$ is a Dedekind domain, so by Claim 4.4 and Exercise 4.10, there exists an integral $\mathfrak{O}_F$-ideal $\mathcal{J}$ such that $(y + \sqrt{k}) = \mathcal{J}^3$. In other words, $\mathcal{J}^3 \sim 1$, but $h_{\mathfrak{O}_F} \not\equiv 0 \,(\text{mod } 3)$, so by Exercise 4.11, $\mathcal{J} \sim 1$. Thus, by Theorem 1.28 on page 45, there exist $u, v \in \mathbb{Z}$ such that $\mathcal{J} = (u + v\sqrt{k})$. Hence,

$$(y + \sqrt{k}) = (u + v\sqrt{k})^3 = \left([u + v\sqrt{k}]^3\right).$$

By Exercise 1.28 on page 19, there is a unit w in $\mathfrak{O}_F$ such that

$$y + \sqrt{k} = w(u + v\sqrt{k})^3, \tag{4.7}$$

where we observe that since $k \not\equiv 1 \,(\text{mod } 4)$, then 2 does not split in $\mathbb{Q}(\sqrt{k})$—see Remark 1.24 on page 52. Also, by Theorem 1.29 on page 47, $w = \pm 1$. Now we conjugate (4.7) to get

$$y - \sqrt{k} = w(u - v\sqrt{k})^3. \tag{4.8}$$

Hence,

$$x^3 = y^2 - k = (y - \sqrt{k})(y + \sqrt{k}) = w^2(u + v\sqrt{k})^3(u - v\sqrt{k})^3 = (u^2 - v^2k)^3.$$

Therefore,

$$x = u^2 - v^2k. \tag{4.9}$$

Now by adding (4.7)–(4.8), we get

$$2y = w\left[(u + v\sqrt{k})^3 + (u - v\sqrt{k})^3\right] = 2w(u^3 + 3uv^2k), \tag{4.10}$$

and by subtracting (4.8) from (4.7), we get

$$2\sqrt{k} = w\left[(u + v\sqrt{k})^3 - (u - v\sqrt{k})^3\right] = 2w\sqrt{k}(3u^2v + v^3k). \tag{4.11}$$

Hence, from (4.10)–(4.11), we get, respectively, that

$$y = w(u^3 + 3uv^2k) \tag{4.12}$$

and

$$1 = w(3u^2v + v^3k) = wv(3u^2 + v^2k). \tag{4.13}$$

From (4.13), we get that $v = \pm w$, so from (4.9), (4.12)–(4.13), we have,

$$x = u^2 - k,\ y = w(u^3 + 3uk), \text{ and } 1 = \pm(3u^2 + k).$$

It follows that $k = \pm 1 - 3u^2$, $x = 4u^2 \mp 1$, and $y = \varepsilon(3u \mp 8u^3)$, where $\varepsilon = \pm 1$ is allowed in either case. Therefore, the two cases are encapsulated in the following

$$(k, x, y) = (\pm 1 - 3u^2, 4u^2 \mp 1, \varepsilon\, u(3 \mp 8u^2))$$

and

$$x^3 + k = (4u^2 \mp 1)^3 \pm 1 - 3u^2 = 64u^6 \mp 48u^4 + 9u^2 = (\varepsilon u(3 \mp 8u^2))^2 = y^2,$$

as required. □

As special cases, we get the following two celebrated results—see Biographies 4.4 and 4.5 on page 148.

Application 4.1 —Euler's Solution of Bachet's Equation

The only solutions with $x, y \in \mathbb{Z}$ of (4.2) for $k = -2$ are $x = 3$ and $y = \pm 5$.

Application 4.2 —Fermat's Solution of Bachet's Equation

The only solutions with $x, y \in \mathbb{Z}$ of (4.2) for $k = -4$ are

$$(x, y) \in \{(5, \pm 11), (2, \pm 2)\}.$$

Remark 4.2 Note that in Theorem 4.2, u is odd when $k = 1 - 3u^2$ and u is even when $k = -1 - 3u^2$ by the hypothesis that $k \not\equiv 1 \pmod 4$, and the fact that k is a radicand, which precludes that $k \equiv 0 \pmod 4$—see Application 2.1 on page 77.

See Exercises 4.13–4.14 for more illustrations. Also, see Exercise 4.15 for results similar to Theorem 4.2 on page 145 for the case where $k > 0$.

Biography 4.3 Claude Gasper Bachet de Méziriac (1581–1638) was born in Bourg-en-Bresse in Savoy that was a region variously allied with France, Italy, or Spain. In his early years, he was educated by the Jesuits. Indeed, after both his parents died when he was only six, the Jesuit Order took care of him in a house belonging to the duchy of Savoy. Later, he studied with the Jesuits in Lyon, France, and Milan, Italy. He also spent time in Paris and Rome. His principal income was generated by his luxurious estate at Bourg-en-Bresse. In 1620, he married and had seven children. By the 1630s, he developed a sequence of health problems including rheumatism and gout. He died on February 26, 1638.

Bachet's contribution to mathematics was as a writer of books on mathematical puzzles, which were seminal in that later books on recreational mathematics were modeled after his. In 1612, for instance, he published *Problèmes plaisans et delectables qui se font par les nombres*, the last edition published in 1959! His puzzles were largely arithmetical, such as number systems other than base 10. Also, he was fond of card tricks, magic square problems, watch-dial puzzles depending on numbering schemes, and what we would call today *think-of-a-number* problems. As noted in this section, he also contributed to number theory, being perhaps best known for his Latin translation of Diophantus's Greek book *Arithmetica*, in which Fermat wrote his now famous Last Theorem marginal notes—see Biography 4.5 on the next page.

Exercises

4.10. Suppose that I, J are nonzero integral R-ideals where R is a Dedekind domain with I and J relatively prime—see Definition 1.26 on page 29. Prove that if K is an R-ideal and $n \in \mathbb{N}$ such that $IJ = K^n$, then there exist R-ideals $\mathfrak{I}$, $\mathfrak{J}$ such that $I = \mathfrak{I}^n, J = \mathfrak{J}^n$, and $K = \mathfrak{I}\mathfrak{J}$.

(*Hint: use Theorem 1.17 on page 28.*)

4.11. Let $\mathfrak{O}_F$ be the ring of integers of an algebraic number field F with class number $h_{\mathfrak{O}_F}$. Prove that if I is an integral $\mathfrak{O}_F$-ideal such that $I^n \sim 1$ for some $n \in \mathbb{N}$ with $\gcd(h_{\mathfrak{O}_F}, n) = 1$, then $I \sim 1$.

4.12. Show that the only rational integer solutions of $y^2 = x^3 - 1$ are $x = 1$ and $y = 0$ using unique factorization in $\mathbb{Z}[i]$.

4.13. Suppose that p is a prime of the form $p = u^2 + 13v^2$ for some $u, v \in \mathbb{N}$. Find all solutions to $y^2 = p^{3m} - 13$, for $m \in \mathbb{N}$ if any exist.

(*Note that* 13 *is the smallest value of* $|k|$ *of the form* $|k| = 1 + 3u^2$ *such that the hypothesis of Theorem 4.2 is satisfied. Also,* $h_{\mathbb{Z}[\sqrt{-13}]} = 2$.)

4.14. Find all solutions of $y^2 = x^3 - 193$ if they exist.

(*With reference to Exercise 4.13, the next smallest* $|k|$ *of the form* $|k| = 1 + 3u^2$ *such that the hypothesis of Theorem 4.2 is satisfied is* $|k| = 193$. *Also,* $h_{\mathbb{Z}[\sqrt{-193}]} = 4$.)

4.15. Suppose that $k \in \mathbb{N}$ is a radicand of a real quadratic field $F = \mathbb{Q}(\sqrt{k})$ and $k \not\equiv 1 \pmod 4$, such that $h_{\mathfrak{O}_F} \not\equiv 0 \pmod 3$, with F having fundamental unit ε_k—see Application 3.1 on page 135. Let $\varepsilon = \varepsilon_k$ if ε_k has norm 1, and $\varepsilon = \varepsilon_k^2$ otherwise, and set $\varepsilon = T + U\sqrt{k}$. Prove that (4.2) on page 145 has no solutions if $k \equiv 4 \pmod 9$ and $U \equiv 0 \pmod 9$.

(*Hint: Assume there is a solution* (x, y) *to* (4.2). *Then you may assume that* $y + \sqrt{k} = w(u + v\sqrt{k})^3$ *for a unit* $w \in \mathfrak{O}_F$ *and some* $u, v \in \mathbb{Z}$, *since the argument is the same as in the proof of Theorem 4.2.*)

(*Note that more results for* $k > 0$ *of this nature, which typically involve congruences on* T *and* U, *may be found, for instance, in Mordell's classic text* [56] *on Diophantine equations.*)

Biography 4.4 Leonard Euler (1707–1783) was a Swiss mathematician who studied under Jean Bernoulli (1667–1748)—see Biography 4.7 on page 161. Euler was extremely prolific. In his lifetime, he is estimated to have written over eight hundred pages a year. He published over five hundred papers during his lifetime, and another three hundred and fifty have appeared posthumously. It took almost fifty years for the Imperial Academy to finish publication of his works after his death. Euler had spent the years 1727–1741 and 1766–1783 at the Imperial Academy in St. Petersburg under the invitation of Peter the Great. Euler lost the sight in his right eye in 1735, and he was totally blind for the last seventeen years of his life. Nevertheless, his phenomenal memory (having the entire *Aeneid* committed to memory for example) made the difference, and so his mathematical output remained high. In fact, about half of his works were written in those last seventeen years. He died on September 18, 1783.

Biography 4.5 Pierre de Fermat was not a professional mathematician, and published none of his discoveries. In fact, he was a lawyer. However, he did correspond with other mathematicians such as Pascal, de Bessy, and Mersenne. It is from this correspondence that we know about much of his work. Moreover, Fermat's son found his copy of Bachet's translation of Diophantus' *Arithmetica*, in which he had written margin notes—see Biography 4.3 on the preceding page. These were published by his son, so we now have a further record of Fermat's work.

4.3 The Fermat Equation

All animals are equal but some animals are more equal than others.
from chapter 10 of **Animal Farm (1945)**
George Orwell (Eric Blair) (1903–1950)
English novelist

In this section, we look at *Fermat's Last Theorem* (FLT), and its related *prime Fermat equation*

$$x^p + y^p + z^p = 0. \tag{4.14}$$

It suffices to solve (4.14) in order to solve the general Fermat equation $x^n + y^n = z^n$ for $n \in \mathbb{N}$. As is now well-known, FLT was solved by Andrew Wiles—see [54, Theorem 10.4, p. 365] for a proof that is given in one paragraph at the end of the book.

We begin with the anchor case where $p = 3$, provided by Gauss—see Biography 3.5 on page 95—then move to the larger picture provided by Kummer—see Biography 4.9 on page 164. The following result employs not only the unique factorization in a quadratic domain $\mathbb{Z}[\zeta_3]$ (where ζ_3 is a primitive cube root of unity) but also Fermat's method of *infinite descent*. This method involves assuming the existence, in natural numbers, of a solution to a given problem and constructing new solutions using smaller natural numbers; and then from the new ones other solutions using still smaller natural numbers, and so on. Since this process cannot go on indefinitely for natural numbers, then the initial assumption must have been false.

Theorem 4.3 — Gauss's Proof of FLT for p = 3

There are no solutions of

$$\alpha^3 + \beta^3 + \gamma^3 = 0$$

for nonzero $\alpha, \beta, \gamma \in \mathfrak{O}_F = \mathbb{Z}[\zeta_3]$, where $F = \mathbb{Q}(\zeta_3)$. In particular, there are no solutions to

$$x^3 + y^3 = z^3,$$

in nonzero rational integers x, y, z.

Proof. We assume that there are nonzero $\alpha, \beta, \gamma \in \mathfrak{O}_F$ such that

$$\alpha^3 + \beta^3 + \gamma^3 = 0,$$

and achieve a contradiction. Without loss of generality, we may assume that

$$\gcd(\alpha,\beta) = \gcd(\alpha,\gamma) = \gcd(\beta,\gamma) = 1,$$

—see Exercise 1.17 on page 6 and Remark 1.8 on page 13. Let

$$\lambda = 1 - \zeta_3 = \frac{3 - \sqrt{-3}}{2},$$

—see Example 1.4 on page 2. Then $N_F(\lambda) = \lambda\lambda' = 3$, where $\lambda' = (3 + \sqrt{-3})/2$ is the algebraic conjugate of λ. Therefore, by Corollaries 1.1–1.2 on page 13 and Exercise 1.22 on page 14, λ is prime in $\mathfrak{O}_F$. We will achieve the desired contradiction by an infinite descent argument. This is not done directly, but rather we get a contradiction to the equation $\alpha^3 + \beta^3 + \lambda^{3n}\rho^3 = 0$. Thus, we first show that the latter equation holds. We require two claims. Note that congruence of elements follows the development in §1.5 on ideals, namely $\sigma \equiv \omega \pmod{\nu}$ means $\nu \mid (\sigma - \omega)$ in $\mathfrak{O}_F$—see Remark 1.17 on page 32, as well as Exercises 4.25–4.32 on pages 163–164 for further developments.

Claim 4.4 If $\lambda \nmid \delta \in \mathfrak{O}_F$, then $\delta \equiv \pm 1 \,(\mathrm{mod}\ \lambda)$.

Let $\delta = a + b\zeta_3$, where $a, b \in \mathbb{Z}$. Then $\delta = u + v\lambda$, where $u, v \in \mathbb{Z}$. If $\lambda | u$, then $\delta \equiv 0$ $(\mathrm{mod}\ \lambda)$, a contradiction, so $\lambda \nmid u$. Since $\lambda|3$, then $3 \nmid u$, so $u \equiv \pm 1 \,(\mathrm{mod}\ 3)$ in $\mathbb{Z}$. Thus, there is a $t \in \mathbb{Z}$ such that

$$\delta = \pm 1 + 3t + v\lambda.$$

But $\lambda|3$, so there exists a $\sigma \in \mathfrak{O}_F$ such that

$$\delta = \pm 1 + t\sigma\lambda + v\lambda = \pm 1 + \lambda(t\sigma + v).$$

In other words, $\delta \equiv \pm 1 \,(\mathrm{mod}\ \lambda)$, which is Claim 4.4.

Claim 4.5 If $\lambda \nmid \delta \in \mathfrak{O}_F$, then $\delta^3 \equiv \pm 1 \,(\mathrm{mod}\ \lambda^4)$.

By Claim 4.4, we may assume that $\delta \equiv 1 \,(\mathrm{mod}\ \lambda)$ since the other case is similar. Therefore, $\delta = 1 + \lambda\sigma$ for some $\sigma \in \mathfrak{O}_F$. Thus,

$$\delta^3 - 1 = (\delta - 1)(\delta - \zeta_3)(\delta - \zeta_3^2) = \lambda\sigma(\lambda\sigma + 1 - \zeta_3)(\lambda\sigma + 1 - \zeta_3^2) =$$

$$\lambda\sigma(\lambda\sigma + \lambda)(\lambda\sigma + \lambda(1 + \zeta_3)) = \lambda^3\sigma(\sigma + 1)(\sigma - \zeta_3^2), \tag{4.15}$$

where the last equality follows from the fact that $\sum_{j=0}^{2} \zeta_3^j = 0$, given in Example 1.5 on page 2. Since

$$\zeta_3^2 - 1 = (\zeta_3 + 1)(\zeta_3 - 1) = (\zeta_3 + 1)\lambda,$$

then $\zeta_3^2 \equiv 1 \,(\mathrm{mod}\ \lambda)$, so since $\delta \equiv 1 \,(\mathrm{mod}\ \lambda)$, then by (4.15),

$$0 \equiv (\delta^3 - 1)\lambda^{-3} \equiv \sigma(\sigma + 1)(\sigma - \zeta_3^2) \equiv \sigma(\sigma + 1)(\sigma - 1) \pmod{\lambda}.$$

Hence,

$$\delta^3 \equiv 1 \pmod{\lambda^4},$$

and we have Claim 4.5.

Claim 4.6 $\lambda \mid \alpha\beta\gamma$.

Suppose that $\lambda \nmid \alpha\beta\gamma$. Then by Claim 4.5,

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4},$$

from which it follows that $\lambda^4 \mid 1$ or $\lambda^4 \mid 3$. The former is impossible since λ is prime, and the second is impossible since

$$3 = (1 - \zeta_3)(1 - \zeta_3^2) = (1 - \zeta_3)^2(1 + \zeta_3) = \lambda^2(1 + \zeta_3),$$

and $1 + \zeta_3$ is a unit, so not divisible by λ^2. This contradiction establishes Claim 4.6.

By Claim 4.6, we may assume without loss of generality that $\lambda \mid \gamma$. However, by the gcd condition assumed at the outset of the proof, $\lambda \nmid \alpha$, and $\lambda \nmid \beta$. Let $n \in \mathbb{N}$ be the highest power of λ dividing γ. In other words, assume that

$$\gamma = \lambda^n\rho, \text{ for some } \rho \in \mathfrak{O}_F \text{ with } \lambda \nmid \rho.$$

Thus, we have

$$\alpha^3 + \beta^3 + \lambda^{3n}\rho^3 = 0. \tag{4.16}$$

We now use Fermat's method of infinite descent to complete the proof. First we establish that $n > 1$. If $n = 1$, then by Claim 4.4,

$$-\lambda^3\rho^3 = \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}.$$

The signs on the right cannot be the same since $\lambda \nmid 2$. Therefore,

$$-\lambda^3\rho^3 \equiv 0 \pmod{\lambda^4},$$

forcing $\lambda \mid \rho$, a contradiction that shows $n > 1$. Given the above, the following claim, once proved, will yield the full result by descent.

Claim 4.7 If Equation (4.16) holds for $n > 1$, then it holds for $n - 1$.

Let

$$X = \frac{\beta + \alpha\zeta_3}{\lambda}, Y = \frac{\beta\zeta_3 + \alpha}{\lambda}, \text{ and } Z = \frac{(\beta+\alpha)\zeta_3^2}{\lambda}.$$

Observe that $X, Y, Z \in \mathfrak{O}_F$ by Corollary 1.1 on page 13, Equation (4.16), and the fact that $\zeta_3 \equiv 1 \pmod{\lambda}$. Also, by Example 1.5, $\sum_{j=0}^2 \zeta_3 = 0$,

$$X + Y + Z = 0, \tag{4.17}$$

and

$$XYZ = \frac{\beta^3 + \alpha^3}{\lambda^3} = \left(\frac{-\lambda^n\rho}{\lambda}\right)^3 = \lambda^{3n-3}(-\rho)^3,$$

so $\lambda^{3n-3} \mid XYZ$, but $\lambda^{3n} \nmid XYZ$, since $\lambda \nmid \rho$. Also, since

$$\beta = -\zeta_3 X + \zeta_3^2 Y, \text{ and } \alpha = \zeta_3 Z - X,$$

then by the gcd condition assumed at the outset of the proof, we have

$$\gcd(X, Y) = \gcd(X, Z) = \gcd(Y, Z) = 1.$$

Hence, each of X, Y, and Z is an associate of a cube in $\mathfrak{O}_F$. Also, we may assume without loss of generality that $\lambda^{3n-3} \mid Z$. By unique factorization in $\mathfrak{O}_F$, we may let $X = u_1\xi^3$, $Y = u_2\eta^3$, and $Z = u_3\lambda^{3n-3}\nu^3$ for some $\xi, \eta, \nu \in \mathfrak{O}_F$, and $u_j \in \mathfrak{U}_{\mathfrak{O}_F}$ for $j = 1, 2, 3$. Therefore, from (4.17),

$$\xi^3 + u_4\eta^3 + u_5\lambda^{3n-3}\nu^3 = 0, \tag{4.18}$$

where $u_j = u_1^{-1}u_{j-2}$ for $j = 4, 5$. Therefore, $\xi^3 + u_4\eta^3 \equiv 0 \pmod{\lambda^3}$. By Claim 4.5

$$\xi^3 \equiv \pm 1 \pmod{\lambda^4}, \text{ and } \eta^3 \equiv \pm 1 \pmod{\lambda^4}.$$

Hence,

$$\pm 1 \pm u_4 \equiv 0 \pmod{\lambda^3}.$$

Since the only choices for u_4 are ± 1, $\pm\zeta_3$, and $\pm\zeta_3^2$, then the only values that satisfy the last congruence are $u_4 = \pm 1$, since $\lambda^3 \nmid (\pm 1 \pm \zeta_3)$, and $\lambda^3 \nmid (\pm 1 \pm \zeta_3^2)$. If $u_4 = 1$, then Equation (4.18) provides a validation of Claim 4.7. If $u_4 = -1$, then replacing η by $-\eta$ provides a validation of the claim. This completes the proof. □

Theorem 4.3 is the lynchpin case for the next result. The following uses factorization in *prime cyclotomic fields* $F = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity for a prime $p > 2$ when $p \nmid h_{\mathfrak{O}_F}$, in which case p is called a *regular* prime. The proof is due to Kummer and is an application of techniques we have learned thus far.

In the following, we note that for historical reasons and for convenience, FLT is usually broken down into two cases. Case I is that $p \nmid xyz$ and Case II is that $p|xyz$—see Theorem 5.22 on page 240.

Theorem 4.4 — Kummer's Proof of FLT for Regular Primes–Case I
Let p be an odd prime such that $p \nmid h_{\mathfrak{O}_F}$ for $F = \mathbb{Q}(\zeta_p)$. Then if $p \nmid xyz$, the Fermat equation (4.14) on page 149 has no integer solution $xyz \neq 0$.

Proof. Assume that (4.14) has a solution $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$. We may assume that $x, y, z \in \mathbb{Z}$ are pairwise relatively prime, and we may write (4.14) as the *ideal* equation

$$\prod_{j=0}^{p-1}(x + \zeta_p^j y) = (z)^p. \tag{4.19}$$

Claim 4.8 *$(x + \zeta_p^j y)$ and $(x + \zeta_p^k y)$ are relatively prime for $0 \leq j \neq k \leq p-1$.*

Let $\mathcal{P}$ be a prime $\mathfrak{O}_F$-ideal dividing both of the above ideals. Therefore, $\mathcal{P}$ divides

$$(x + \zeta_p^k y) - (x + \zeta_p^j y) = y\zeta_p^k(1 - \zeta_p^{j-k}).$$

By Exercise 3.37 on page 129, $\lambda = 1 - \zeta_p$ and $1 - \zeta_p^{j-k}$ are associates for $j \neq k$, and by Exercise 3.39, ζ_p^k is a unit, so $\mathcal{P} \mid (y\lambda)$. By primality, $\mathcal{P} \mid (y)$ or $\mathcal{P} \mid (\lambda)$. If $\mathcal{P} \mid (y)$, then $\mathcal{P} \mid (z)$ from (4.19). Since $\gcd(y, z) = 1$, there exist $u, v \in \mathbb{Z}$ such that $uy + vz = 1$. Since $y, z \in \mathcal{P}$, then $1 \in \mathcal{P}$, a contradiction. Hence, $\mathcal{P} \mid (\lambda)$. By Exercise 2.24 on page 68 and Corollary 2.8 on page 85,

$$N((\lambda)) = N_F(\lambda) = p.$$

Thus, by Exercise 2.45 on page 86, (λ) is a prime $\mathfrak{O}_F$-ideal. Therefore, $\mathcal{P} = (\lambda)$, so $(\lambda) \mid (z)$. By Exercise 2.46, $N_F(\lambda) \mid N_F(z)$. However, by Corollary 1.17 on page 41, $N_F(z) = z^{p-1}$, so $p = N_F(\lambda) \mid z$, contradicting the hypothesis. This completes Claim 4.8.
By Claim 4.8 and Theorem 1.17 on page 28,

$$(x + \zeta_p y) = I^p,$$

for some $\mathfrak{O}_F$-ideal I. Since $p \nmid h_{\mathfrak{O}_F}$, then by Exercise 4.11 on page 147, $I \sim 1$. Hence, there exists an $\alpha \in \mathfrak{O}_F$ such that

$$x + \zeta_p y = u_1 \alpha^p,$$

where $u_1 \in \mathfrak{U}_{\mathfrak{O}_F}$. By Theorem 3.18 on page 128, $u_1 = w\zeta_p^k$ for some $k \in \mathbb{Z}$ and $w \in \mathbb{R} \cap \mathfrak{U}_{\mathfrak{O}_F}$. Therefore,

$$x + \zeta_p y = w\zeta_p^k \alpha^p. \tag{4.20}$$

By Exercise 4.32 on page 164 there exists a $z_1 \in \mathbb{Z}$ such that $\alpha \equiv z_1 \,(\text{mod } (\lambda))$. By taking norms on the latter, we get

$$\alpha^p - z_1^p = \prod_{j=0}^{p-1}(\alpha - \zeta_p^j z_1).$$

Since $\zeta_p \equiv 1 \,(\text{mod } (\lambda))$, then for each $j = 0, 1, \ldots, p-1$,

$$\alpha - \zeta_p^j z_1 \equiv \alpha - z_1 \pmod{(\lambda)}.$$

Hence,

$$\alpha^p \equiv z_1^p \pmod{(\lambda)^p},$$

so (4.20) becomes

$$x + \zeta_p y \equiv w z_1^p \zeta_p^k \pmod{(\lambda)^p}.$$

However, $(p) = (\lambda)^{p-1}$ by Exercise 4.19 on page 162, so

$$x + \zeta_p y \equiv w z_1^p \zeta_p^k \pmod{(p)}.$$

Since ζ_p^k is a unit, then

$$\zeta_p^{-k}(x + \zeta_p y) \equiv w z_1^p \pmod{(p)}. \tag{4.21}$$

By taking complex conjugates in (4.21), we get

$$\zeta_p^{k}(x + \zeta_p^{-1} y) \equiv w z_1^p \pmod{(p)}. \tag{4.22}$$

Subtracting (4.22) from (4.21), we get

$$\zeta_p^{-k}x + \zeta_p^{1-k}y - \zeta_p^{k}x - \zeta_p^{k-1}y \equiv 0 \pmod{(p)}. \tag{4.23}$$

Claim 4.9 $2k \equiv 1 \,(\text{mod } p)$.

If $p \bigm| k$, then $\zeta_p^k = 1$, so (4.23) becomes

$$0 \equiv y(\zeta_p - \zeta_p^{-1}) \equiv y\zeta_p^{-1}(\zeta_p^2 - 1) \equiv y\zeta_p^{-1}(\zeta_p - 1)(\zeta_p + 1) \equiv y\zeta_p^{-1}\lambda(\zeta_p + 1) \pmod{(p)}.$$

However, by Exercise 4.20, $1 + \zeta_p \in \mathfrak{U}_{\mathfrak{O}_F}$, so

$$y\lambda \equiv 0 \pmod{(p)}.$$

Also, by Exercise 4.19,

$$(p) = (\lambda)^{p-1},$$

and $p \geq 3$, so $\lambda \bigm| y$. Taking norms on the latter and using Exercise 2.46 again, we get that $p \bigm| y$, contradicting the hypothesis. Therefore, $k \not\equiv 0 \,(\text{mod } p)$. By (4.23) there exists an $\alpha_1 \in \mathfrak{O}_F$ such that

$$\alpha_1 p = x\zeta_p^{-k} + y\zeta_p^{1-k} - x\zeta_p^{k} - y\zeta_p^{k-1}. \tag{4.24}$$

By Exercise 4.21, $k \not\equiv 1 \,(\text{mod } p)$. Since $k \not\equiv 0, 1 \,(\text{mod } p)$, then

$$\alpha_1 = \frac{x}{p}\zeta_p^{-k} + \frac{y}{p}\zeta_p^{1-k} - \frac{x}{p}\zeta_p^{k} - \frac{y}{p}\zeta_p^{k-1}. \tag{4.25}$$

By Theorem 3.14 on page 123,

$$\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$$

is a $\mathbb{Z}$-basis of $\mathfrak{O}_F$. Thus, if all exponents $-k$, $1-k$, k and $k-1$ are incongruent modulo p, then $x/p \in \mathbb{Z}$, contradicting the hypothesis. Thus, two of the aforementioned exponents are congruent modulo p. The only possibility remaining after excluding $k \equiv 0, 1 \,(\text{mod } p)$ is

$$2k \equiv 1 \pmod{p}.$$

This establishes Claim 4.9.

Hence, (4.24) becomes

$$\alpha_1 p \zeta_p^k = x + y\zeta_p - x\zeta_p^{2k} - y\zeta_p^{2k-1} = (x - y)\lambda.$$

By taking norms and applying Exercise 2.46 one more time, we get $p \bigm| (x - y)$, namely

$$x \equiv y \pmod{p}.$$

Thus, by (4.14)

$$y \equiv z \pmod{p}$$

as well. Therefore, since $p \nmid x$,

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \pmod{p}.$$

Thus, $p = 3$, which was eliminated in Theorem 4.3, so we have completed the proof. □

Now that we have completed Kummer's verification of Case I of FLT for regular primes, we turn our attention to *irregular primes* namely those primes p such that $p \mid h_{\mathfrak{O}_F}$. We are interested in the number of them. Kummer stated that there are infinitely many regular primes. In [66], published in 1964, Siegel made this more precise by conjecturing that approximately $e^{-1/2}$ of all primes are regular, namely in the asymptotic sense using natural density, about 60.75% of primes are regular. However, at the time of the writing of this book, this still has not been proved. That there are infinitely many irregular primes is known, proved by K.L. Jensen in 1915, and this is the focus of our next result. The mechanism for so doing requires an equivalent definition of an irregular prime necessitating the introduction of more celebrated numbers.

First, we need to introduce the following, which first appeared in the posthumous work *Ars Conjectandi* by Jacob (Jacques) Bernoulli in 1713—see Biography 4.7 on page 161. Also, the reader should be familiar with the background on the basics concerning series—see Appendix B.

Definition 4.1 — Bernoulli Numbers

In the Taylor series, for a complex variable x,

$$F(x) = \frac{x}{e^x - 1} = \sum_{j=0}^{\infty} \frac{B_j x^j}{j!},$$

the coefficients B_j are called the *Bernoulli numbers.*

Example 4.1 Using the recursion formula given in Exercise 4.16 on page 161, we calculate the first few Bernoulli numbers:

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	$-1/2$	$1/6$	0	$-1/30$	0	$1/42$	0	$-1/30$	0	$5/66$

n	11	12	13	14	15	16	17	18	19
B_n	0	$-691/2730$	0	$7/6$	0	$-3617/510$	0	$43867/798$	0

Example 4.1 suggests that $B_{2n+1} = 0$ for all $n \in \mathbb{N}$ and this is indeed the case—see Exercise 4.23 on page 162.

Suppose that x, s are complex variables and set

$$F(s,x) = \frac{se^{xs}}{e^s - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{s^n}{n!}, \text{ for } |s| < 2\pi. \tag{4.26}$$

Then by comparing coefficients of x^n in

$$\sum_{n=0}^{\infty} B_n(x) \frac{s^n}{n!} = F(s,x) = F(s)e^{xs} = \sum_{n=0}^{\infty} B_n \frac{s^n}{n!} \sum_{j=0}^{\infty} x^j \frac{s^j}{j!},$$

we get the following.

Definition 4.2 — Bernoulli Polynomials
For $x \in \mathbb{C}$,

$$B_n(x) = \sum_{j=0}^{n} \binom{n}{j} B_j x^{n-j},$$

called the n-th *Bernoulli polynomial.*

Example 4.2 Using the recursion formula in Exercise 4.16 again, we calculate the first few Bernoulli polynomials:

$$B_0(x) = 1, B_1(x) = x - \frac{1}{2}, B_2(x) = x^2 - x + \frac{1}{6},$$
$$B_3(x) = x^3 - \frac{3}{2}x = x(x-1)\left(x - \frac{1}{2}\right),$$
$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30},$$
$$B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x.$$
$$B_6(x) = x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}.$$

The following is Kummer's notion of a regular prime which is equivalent to the one given on page 154. Recall that a rational number $q = a/b$ is written in *lowest terms* when $\gcd(a, b) = 1$.

Definition 4.3 — Bernoulli Numbers, Regular, and Irregular Primes
An odd prime number p is said to be a regular prime if p does not divide the numerator of any of the Bernoulli numbers B_n when B_n is written in lowest terms for $n = 2, 4, 6, \ldots, p-3$.

We need the following result by Jacob Bernoulli on sums of n-th powers and Bernoulli polynomials.

Lemma 4.1 — Bernoulli Numbers, Polynomials, and Sums of Powers
For every nonnegative $n \in \mathbb{Z}$ and $k \in \mathbb{N}$,

$$S_n(k) = \sum_{j=1}^{k-1} j^n = \frac{B_{n+1}(k) - B_{n+1}}{n+1} = \frac{1}{n+1} \sum_{j=0}^{n} \binom{n+1}{j} B_j k^{n+1-j}.$$

Proof. Since $F(s, x) - F(s, x-1) = se^{s(x-1)}$, then

$$\frac{B_{n+1}(x) - B_{n+1}(x-1)}{n+1} = (x-1)^n. \tag{4.27}$$

Adding (4.27) for $x = 1, 2, \ldots k$, we get the result. □

In order to obtain a crucial result on Bernoulli numbers, which is the final lead-up to proving the infinitude of irregular primes, we need to establish a realtionship between Bernoulli numbers and the *Riemann zeta function*

$$\zeta(s) = \sum_{j=1}^{\infty} j^{-s} \text{ for } s \in \mathbb{C} \text{ with } \Re(s) > 1,$$

where $\Re(s) = a$ is the real part of $s = a + b\sqrt{-1}$ for $a, b \in \mathbb{R}$—see [53, §1.9, pp. 65–72] as well as the development in Appendix B on pages 352–354. This was established by Euler as follows.

Theorem 4.5 — Bernoulli Numbers and the Riemann Zeta Function
For $k \in \mathbb{N}$,

$$\zeta(2k) = \frac{(2\pi)^{2k}}{2(2k)!}|B_{2k}|.$$

Proof. First we note that by putting $x = 0$ in Equation (4.26) and adding $s/2$ to both sides, we get (where coth denotes the hyperbolic cotangent):

$$\frac{s}{2}\left(\frac{e^s+1}{e^s-1}\right) = \frac{s}{2}\coth\left(\frac{s}{2}\right) = \sum_{k=0}^{\infty} B_{2k}\frac{s^{2k}}{(2k)!} \tag{4.28}$$

observing that $B_1 = -1/2$ is the only nonzero, odd-indexed Bernoulli number. Then by setting $s = 2ix$ in (4.28), we get

$$x\cot x = 1 + \sum_{k=1}^{\infty}(-1)^k B_{2k}\frac{2^{2k}x^{2k}}{(2k)!}, \tag{4.29}$$

recalling that $e^{ix} = \cos x + i\sin x$, so $\cos x = (e^{ix} + e^{-ix})/2$ and $\sin x = (e^{ix} - e^{-ix})/(2i)$. Secondly, from the known infinite product expansion for the sine function

$$\sin(x) = x\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2\pi^2}\right), \tag{4.30}$$

—see Application B.2 on page 354—we take the logarithmic derivative of (4.30) to achieve,

$$x\cot(x) = 1 + 2\sum_{n=1}^{\infty}\frac{x^2}{x^2 - n^2\pi^2}. \tag{4.31}$$

To proceed, we need the following.

Claim 4.10 For $x \in \mathbb{C}$,

$$\frac{x^2}{x^2 - n^2\pi^2} = -\sum_{k=1}^{\infty}\frac{x^{2k}}{n^{2k}\pi^{2k}}.$$

We have

$$-\sum_{k=1}^{\infty}\frac{x^{2k}}{n^{2k}\pi^{2k}} = 1 - \sum_{k=0}^{\infty}(n\pi/x)^{-2k} = 1 - \lim_{N\to\infty}\sum_{k=0}^{N}\left[\left(\frac{n\pi}{x}\right)^{-2}\right]^k.$$

However, by Theorem B.4 on page 347 this equals

$$1 - \lim_{N\to\infty}\left(\frac{\left(\left(\frac{n\pi}{x}\right)^{-2}\right)^{N+1} - 1}{\left(\frac{n\pi}{x}\right)^{-2} - 1}\right) = 1 + \frac{1}{\left(\frac{n\pi}{x}\right)^{-2} - 1} = \frac{x^2}{x^2 - n^2\pi^2},$$

which is Claim 4.10.

Now by plugging the result of Claim 4.10 into (4.31), and equating the result with (4.29), we get

$$1+\sum_{k=1}^{\infty}(-1)^k B_{2k}\frac{2^{2k}x^{2k}}{(2k)!}=1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{x^{2k}}{n^{2k}\pi^{2k}},$$

so

$$(-1)^{k+1}B_{2k}\frac{2^{2k-1}x^{2k}}{(2k)!}=\sum_{n=1}^{\infty}\frac{x^{2k}}{n^{2k}\pi^{2k}}=\frac{x^{2k}}{\pi^{2k}}\sum_{n=1}^{\infty}\frac{1}{n^{2k}}=\frac{x^{2k}}{\pi^{2k}}\zeta(2k).$$

Since $(-1)^{k+1}B_{2k}>0$, then this implies the desired result,

$$|B_{2k}|\frac{(2\pi)^{2k}}{2(2k)!}=\zeta(2k).$$

□

Corollary 4.5 For $n\in\mathbb{N}$,

$$\lim_{n\to\infty}\left|\frac{B_{2n}}{2n}\right|=\infty.$$

Proof. By Theorem 4.5,

$$|B_{2n}|>\frac{2(2n)!}{(2\pi)^{2n}},$$

given that $\zeta(2n)>1$. Since $(2n)!>(2n/e)^{2n}$, by Stirling's formula given in (A.7) on page 339, then

$$|B_{2n}|>2\left(\frac{n}{\pi e}\right)^{2n},$$

and the result follows. □

We are now ready for a key result in our pursuit to establish the infinitude of irregular primes. For convenience, we introduce the following notion.

Definition 4.4 — p-Integers and Rational Congruences

If $q\in\mathbb{Q}$, and $p\in\mathbb{Z}$ is a prime, then $q=a/b$ for $a,b\in\mathbb{Z}$ written in lowest terms is called a p-integer provided that $p\nmid b$. For any $n\in\mathbb{N}$, a congruence

$$q_1\equiv q_2 \pmod{n} \text{ with } q_1,q_2\in\mathbb{Q}$$

means that q_1-q_2, written in lowest terms, is a rational number with numerator divisible by n.

Remark 4.3 The term *p-integer* comes from the notion of a *p-adic integer*, which we will not study *per se* in this text since we are concentrating on a *global* approach—see [54, Chapter 6] for an introduction to p-adic analysis.

The reader can easily verify that for any rational number q_1 with denominator prime to n, there exists a unique rational integer r_2 with $0\le r_2\le n-1$ such that

$$q_1\equiv r_2 \pmod{n}.$$

The following result was proved independently by T. Clausen and C. von Staudt. Clausen was described by Gauss as a man of "outstanding talents." The following was communicated to Gauss by von Staudt, who published a proof in 1840. Just prior to this, Clausen had published a statement of the result—see Biographies 4.6 on page 159 and 4.8 on page 162.

Theorem 4.6 — von Staudt–Clausen
Let p be a prime and $n \in \mathbb{N}$ even. If $(p-1) \nmid n$, then B_n is a p-integer. If $(p-1) \mid n$, then pB_n is a p-integer, and

$$pB_n \equiv -1 \pmod{p}.$$

Proof. We use induction on n. Since $B_2 = 1/6$, then the denominator of B_2 is not divisible by p unless $p = 2, 3$. If $p = 3$, then $pB_2 = 1/2$ is a p-integer, and $pB_n = 1/2 \equiv -1 \,(\text{mod } 3)$. If $p = 2$, then $pB_2 = 1/3$ is a p-integer, and $pB_2 = 1/3 \equiv -1 \,(\text{mod } 2)$. This is the induction step. Now we use the fact given in Lemma 4.1 on page 155, for our case, namely

$$(k+1)S_k(p) = \sum_{j=0}^{k} \binom{k+1}{j} B_j p^{k+1-j}.$$

Therefore,

$$pB_k = S_k(p) - \frac{1}{k+1} \sum_{j=0}^{k-1} \binom{k+1}{j} p^{k-j} pB_j, \tag{4.32}$$

where pB_j for $j < k$ is a p-integer. Consider

$$\frac{1}{k+1} \binom{k+1}{j} p^{k-j}, \tag{4.33}$$

which is divisible by $p = 2$, given that $j < k$, since $k+1$ is odd. If $p > 2$, then write (4.33) as

$$\frac{1}{k+1} \binom{k+1}{k+1-j} p^{k-j} = \frac{k(k-1)\cdots(j+1)}{(k+1-j)!} p^{k-j},$$

where the last equality follows, via (4.33), from the symmetry property in Pascal's triangle, $\binom{k+1}{k+1-j} = \binom{k+1}{j}$—see [53, Exercise 1.15, p. 14]. We have that

$$p^r \mid (k+1-j)!, \tag{4.34}$$

where

$$r = \sum_{\ell=1}^{\infty} \left\lfloor \frac{k+1-j}{p^\ell} \right\rfloor < \sum_{\ell=1}^{\infty} \frac{k+1-j}{p^\ell} = \frac{k+1-j}{p-1} \le \frac{k+1-j}{2} \le k-j,$$

with the second equality following from Theorem B.4 on page 347. Therefore,

$$\frac{p^{k-j}}{(k+1-j)!}$$

is a p-integer, so from (4.32) and (4.34),

$$\frac{p^{k-j}}{(k+1-j)!} \equiv 0 \pmod{p}.$$

Hence, pB_k is a p-integer, so

$$pB_k \equiv S_k(p) \pmod{p}. \tag{4.35}$$

Also, if $(p-1) \mid k$, then $x^k \equiv 1 \,(\text{mod } p)$, for $1 \le x \le p-1$. Therefore,

$$S_k(p) = \sum_{x=1}^{p-1} x^k \equiv \sum_{x=1}^{p-1} 1 = p-1 \pmod{p},$$

so

$$S_k(p) \equiv -1 \pmod{p} \text{ if } (p-1) \mid k. \tag{4.36}$$

On the other hand, if $(p-1) \nmid k$, then let g be a primitive root modulo p. Thus,

$$S_k(p) = \sum_{x=1}^{p-1} x^k \equiv \sum_{\ell=0}^{p-2} g^{\ell k} = \frac{g^{(p-1)k}-1}{g^k-1} \pmod{p},$$

where the last equality comes from Theorem B.4 again. Therefore, since $g^{p-1} \equiv 1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{p}$, then

$$S_k(p) \equiv 0 \pmod{p} \text{ if } (p-1) \nmid k. \tag{4.37}$$

Comparing (4.35) and (4.37), we see that $pB_k \equiv 0 \pmod{p}$ when $(p-1) \nmid k$, so B_k is a p-integer. Similarly, comparing (4.35) and (4.36), we get that $pB_k \equiv -1 \pmod{p}$, when $(p-1) \mid k$. □

Biography 4.6 Carl Georg Christian von Staudt (1798–1867) was born in the Imperial Free City of Rothenburg (now Rothenburg ob der Tauber, Germany) on January 24, 1798. He attended Gauss's alma mater, Göttingen, from 1818 to 1822, the year in which he received his doctorate in astronomy from Erlangen, Bavaria (now Germany). In 1827, he became Professor of Mathematics at the Polytechnic School at Nuremburg, and in 1835 at the University of Erlangen. One of his feats was the demonstration of how to construct a regular polygon of seventeen sides (a 17-gon) using only compasses. Then he turned his attention to Jacob Bernoulli's numbers described above. However, he is principally known for his work in geometry. In 1847, he published *Geometrie der Lage*, which was on projective geometry. His work showed that projective geometry did not need to have reference to magnitude or number. He died on June 1, 1867 in Erlangen.

Corollary 4.6 If $p > 2$ is prime and $n \in \mathbb{N}$ is even with $n \le p-1$, then

$$pB_n \equiv S_n(p) \pmod{p^2}.$$

Proof. In the proof of Theorem 4.6, if $n \le p-1$, then $p-1$ does not divide any $k < n$. Therefore, all B_k for $k < n$ are p-integers. Hence, every term on the right-hand side of (4.32) is divisible by p^2. □

The last result required for putting together the machinery necessary to establish the infinitude of irregular primes is due to Kummer.

Theorem 4.7 — Kummer's Congruence

If p is a prime and $n \in \mathbb{N}$ is even with $(p-1) \nmid n$, then B_n/n is a p-integer, and

$$\frac{B_{n+p-1}}{n+p-1} \equiv \frac{B_n}{n} \pmod{p}.$$

In this case, we say that the values B_n/n have period length $p-1$ modulo p when $(p-1) \nmid n$.

Proof. Let g be a primitive root modulo p with $1 < g < p$, and set

$$F(x) = \frac{gx}{e^{gx}-1} - \frac{x}{e^x-1} = \sum_{n=1}^{\infty} \frac{B_n(g^n-1)}{n!}x^n, \tag{4.38}$$

where the last equality comes from Definition 4.1 on page 154. We may also write, via Theorem B.4 on page 347 and the Binomial Theorem,

$$F(x) = x\sum_{j=0}^{\infty} a_j(e^x-1)^j, \tag{4.39}$$

where each a_j is a p-integer, by (4.38). Also, since the $(e^x-1)^j$ are each linear combinations of the expressions:

$$e^{kx} = \sum_{\ell=0}^{\infty} \frac{k^\ell}{\ell!}x^\ell, \tag{4.40}$$

and since $k^{\ell+p-1} \equiv k^\ell \pmod p$ by Fermat's Little Theorem, then (4.39) becomes, via (4.40),

$$F(x) = x\sum_{n=0}^{\infty} \frac{b_n}{n!}x^n, \tag{4.41}$$

where the b_n are p-integers. Comparing coefficients of x^n in (4.38) and (4.41), we get

$$\frac{B_n(g^n-1)}{n!} = \frac{b_{n-1}}{(n-1)!},$$

so

$$\frac{B_n}{n}(g^n-1) = b_{n-1}.$$

Since $(p-1) \nmid n$, then $g^n \not\equiv 1 \pmod p$, so the values g^n-1 have period length $p-1$ by Fermat's Little Theorem. Also, since the b_n are p-integers, then B_n/n are p-integers, and have period length $p-1$, when $(p-1) \nmid n$. □

Theorem 4.8 — Infinitude of Irregular Primes

There exist infinitely many irregular primes.

Proof. Let $p_1, p_2, \cdots, p_r$ be irregular primes for $r \in \mathbb{N}$. It suffices to prove the existence of an irregular prime $p \neq p_j$ for any $j = 1, 2, \ldots, r$. Let

$$n = s\prod_{j=1}^{r}(p_j-1) \equiv 0 \pmod 2,$$

where $s \in \mathbb{N}$ may be chosen sufficiently large so that $|B_n/n| > 1$, by Corollary 4.5 on page 157. Let p be a prime dividing the numerator of B_n/n, in lowest terms. If $(p-1) \mid n$, then by Theorem 4.6, p divides the denominator of B_n, a contradiction. Hence, $(p-1) \nmid n$, and $p \nmid 2\prod_{j=1}^{r} p_j$. Suppose that $n = q(p-1)+t$, where $2 \le t \le p-3$. By Theorem 4.7 on the preceding page,

$$\frac{B_t}{t} \equiv \frac{B_n}{n} \pmod p.$$

Since $B_n/n \equiv 0 \pmod p$, then $B_t/t \equiv 0 \pmod p$. By Definition 4.3 on page 155, p is irregular, and we are done. □

One conclusion from the results of this section and the relatively recent proof of FLT using elliptic curves is that the manifold attempts to prove it are far more valuable and far-reaching than the relevance of FLT itself. In fact, it may be said that the very existence of algebraic number theory itself is due to the deep and fertile ideas generated by such attempts to prove FLT.

Biography 4.7 Jacob Bernoulli (1654–1705) was born on December 27, 1654 in Basel, Switzerland. He was one of ten children of Nicolaus and Margaretha Bernoulli. His brother Johann (1667–1748) was the tenth child of the union, and the two brothers had an influence on each other's mathematical development. Jacob was the first to explore the realms of mathematics, and being the pioneer in the family in this regard, he had no tradition to follow as did his brothers after him. In 1681, Bernoulli travelled to the Netherlands where he met the mathematician Hudde, then to England where he met with Boyle and Hooke. This began a correspondence with numerous mathematicians that continued over several years. In 1683, he returned to Switzerland to teach at the University in Basel. He studied the work of leading mathematicians there and cultivated an increasing love of mathematics. Jacob's first seriously important work was in his 1685 publications on logic, algebra, and probability. In 1689, he published significant work on infinite series and on his law of large numbers. The latter is a mathematical interpretation of probability as relative frequency. This means that if an experiment is carried out for a large number of trials, then the relative frequency with which an event occurs equals the probability of the event. By 1704, Jacob had published five works on infinite series containing such fundamental results such as that $\sum_{j=1}^{\infty} 1/j$ diverges—see Exercise 4.17. Although Jacob thought he had discovered the latter, it had been already discovered by Mengoli some four decades earlier. In 1690, Jacob published an important result in the history of mathematics by solving a differential equation using, in modern terms, *separation of variables.* This was the first time that the term *integral* was employed with its proper meaning for integration. In 1692, he investigated curves, including the logarithmic spiral, and in 1694, conceived of what we now call the *lemniscate of Bernoulli.* By 1696, he had solved what we now call the *Bernoulli equation*: $y' = p(x)y + q(x)y^n$. Eight years after his death, the *Ars Conjectandi* was published in 1713, a book in which the Bernoulli numbers first appear—see Definition 4.1 on page 154. In the book, they appear in his discussion of exponential series. Jacob held his chair at Basel until his death on August 16, 1705, when it was filled by his brother Johann. Jacob was always enthralled with the logarithmic spiral mentioned above. Indeed, he requested that it be carved on his tombstone with the (Latin) inscription *I shall arise the same though changed.*

Exercises

4.16. Prove the following *recursion formula for Bernoulli numbers* for $n \in \mathbb{N}$,

$$\sum_{i=0}^{n-1} \binom{n}{i} B_i = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1, \end{cases}$$

where $\binom{n}{i}$ is the binomial coefficient.

(*Hint: Use the fact that* $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.)

4.17. Prove that $\sum_{j=1}^{\infty}(1/j)$ diverges.

(*Hint: Assume* $\sum_{j=1}^{\infty}(1/j) = d \in \mathbb{R}$ *and reach a contradiction.*)

4.18. Prove that, from Definition 4.2 on page 155,

$$B_n(1) = \begin{cases} 1/2 & \text{if } n = 1, \\ B_n & \text{if } n > 1. \end{cases}$$

(*Hint: Use Exercise 4.16.*)

Biography 4.8 Thomas Clausen (1801–1885) was born in Snogebaek, Denmark on January 16, 1801. Clausen took care of the livestock of a local priest, who in turn taught Latin, Greek, and astronomy to him. Clausen became an assistant at the Altona Observatory in 1824, then later he went to the Optical Institute in Munich. His lack of any significant duties there left him with ample time to study mathematics and astronomy. However, his suffering from a degree of mental illness caused him to leave Munich and return to Altona. For the next two years he engaged in what many consider to be the best research of his life. In 1842, he was appointed to the observatory in Dorpat (now Tartu), Estonia. Then two years after that, he received his Ph.D. under the supervision of F.W. Bessel (1784–1846). In 1866, he was appointed director of the Dorpat Observatory, a post which he held until his retirement in 1872. During his lifetime he published more than one-hundred and fifty papers in the areas of mathematics, astronomy, and geophysics. Among his achievements was the factoring of the sixth Fermat number[a] in 1854 (see [71, p. 99] for a discussion of Clausen's factoring method). He also found a new method for factoring numbers in general. He died on May 23, 1885 in Dorpat.*)*

[a] Recall that a Fermat number is one of the form $F_n = 2^{2^n} + 1$ for any $n \in \mathbb{N}$.

4.19. Let $p > 2$ be prime, and set $\lambda = 1 - \zeta_p$, where ζ_p is a primitive p^{th} root of unity. Prove that the following ideal equation holds

$$(\lambda)^{p-1} = (p).$$

4.20. Let $p > 2$ be prime, and let ζ_p be a primitive p^{th} root of unity. Prove that $1+\zeta_p \in \mathfrak{U}_{\mathfrak{O}_F}$, where $F = \mathbb{Q}(\zeta_p)$.

4.21. Show that $k \not\equiv 1 \pmod{p}$ in Claim 4.9 on page 153 of the proof of Theorem 4.4.

4.22. Establish the following derivative formula for Bernoulli polynomials,

$$B'_{n+1}(x) = (n+1)B_n(x).$$

(*Hint: Replace the* x *by* $x+1$ *in Equation* (4.27) *on page 155 and differentiate with respect to* x.)

4.23. Prove that the Bernoulli numbers $B_n = 0$ for $n > 1$ an odd integer. (*Hint: Use Definition 4.1 on page 154.*)

4.24. Compute the Bernoulli numbers B_n for even n where $8 \le n \le 24$.

4.25. Let F be a number field and I a nonzero $\mathfrak{O}_F$-ideal. In Remark 1.17 on page 32 we talked about congruence modulo an ideal, which we further develop here. If $\alpha,\beta \in I$, we say that α and β are *congruent modulo I* if $\alpha - \beta \in I$, denoted by

$$\alpha \equiv \beta \pmod{I}.$$

We call all those $\alpha \in \mathfrak{O}_F$ which are congruent to each other a *residue class modulo I*. Prove that the number of residue classes is equal to $N(I)$.

Note: The balance of the exercises in this section are in reference to Exercise 4.25.

4.26. Let R be a Dedekind domain. Prove that if $\gcd(\alpha, I) = 1$, then for any $\beta \in R$, there is a $\gamma \in R$, uniquely determined modulo I, such that

$$\alpha\gamma \equiv \beta \pmod{I}.$$

Furthermore, prove that this congruence is solvable for some $\gamma \in \mathfrak{O}_F$ if and only if $\gcd(\alpha, I) \bigm| (\beta)$.

4.27. In view of Exercise 4.26, two elements of $\mathfrak{O}_F$ that are congruent modulo I have the same gcd with I. Hence, this is an invariant of the class, since it is a property of the whole residue class. We denote the *number of residue classes relatively prime to I*, by the symbol $\mathbf{\Phi}(I)$. Let I, J be relatively prime $\mathfrak{O}_F$-ideals. Prove that

$$\mathbf{\Phi}(I) = N(I) \prod_{\mathcal{P} \bigm| I} \left(1 - \frac{1}{N(\mathcal{P})}\right),$$

where the product runs over all distinct prime divisors of I. Conclude, in particular that if I, J are relatively prime $\mathfrak{O}_F$-ideals, then

$$\mathbf{\Phi}(IJ) = \mathbf{\Phi}(I)\mathbf{\Phi}(J).$$

4.28. Suppose that $I = \prod_{j=1}^{r} \mathcal{P}_j^{a_j}$, where the $\mathcal{P}_j$ are distinct $\mathfrak{O}_F$-ideals. Prove that

$$\mathbf{\Phi}(I) = N(I) \prod_{j=1}^{r} \left(1 - \frac{1}{N(\mathcal{P}_j)}\right).$$

Note that when $F = \mathbb{Q}$, then $\mathbf{\Phi}$ is the ordinary Euler totient function ϕ.

4.29. Let $\alpha_j \in \mathfrak{O}_F$ for $j = 1 \ldots, d$, and let $\mathcal{P}$ be a prime $\mathfrak{O}_F$-ideal. Prove that the polynomial congruence

$$f(x) = x^d + \alpha_1 x^{d-1} + \cdots + \alpha_{d-1}x + \alpha_d \equiv 0 \pmod{\mathcal{P}}$$

has at most d solutions $x \in \mathfrak{O}_F$ that are incongruent modulo $\mathcal{P}$, or else $f(\alpha) \equiv 0 \pmod{\mathcal{P}}$ for all $\alpha \in \mathfrak{O}_F$. (We also allow the case where $\deg(f) = 0$, in which case $f(x) = \alpha_0 \equiv 0 (\text{mod } \mathcal{P})$ means that $\alpha_0 \in \mathcal{P}$.)

4.30. Prove that the residue classes modulo I, relatively prime to I, form an abelian group under the multiplication given by $(a + I)(b + I) = ab + I$. Prove that this group has order $\mathbf{\Phi}(I)$. In particular, show that if I is a prime $\mathfrak{O}_F$-ideal, then the group is cyclic.

4.31. Suppose that I is a nonzero $\mathfrak{O}_F$-ideal and $\alpha \in \mathfrak{O}_F$ is relatively prime to I. Prove that

$$\alpha^{\Phi(I)} \equiv 1 \pmod{I},$$

called *Euler's Theorem for Ideals.* Conclude that if $I = \mathcal{P}$ is a prime $\mathfrak{O}_F$-ideal, then

$$\alpha^{N(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}},$$

called *Fermat's Little Theorem for Ideals.*

4.32. Let $\mathcal{P}$ be a nonzero prime $\mathfrak{O}_F$-ideal, and let $\alpha \in \mathfrak{O}_F$. Prove that there exists a $z \in \mathbb{Z}$ such that $\alpha \equiv z \,(\text{mod } \mathcal{P})$ if and only if $\alpha^p \equiv \alpha \,(\text{mod } \mathcal{P})$, where $(p) = \mathcal{P} \cap \mathbb{Z}$.

Biography 4.9 Eduard Kummer (1810–1893) was born on January 29, 1810 in Sorau, Brandenburg, Prussia (now Germany). He entered the University of Halle in 1828. By 1833, he was appointed to a teaching post at the Gymnasium in Liegniz which he held for 10 years. In 1836, he published an important paper in *Crelle's Journal* on hypergeometric series, which led to his correspondence with Jacobi and Dirichlet, who were impressed with his talent. Indeed, upon Dirichlet's recommendation, Kummer was elected to the Berlin academy in 1839, and was Secretary of the Mathematics Section of the Academy from 1863 to 1878. In 1842, with the support of Dirichlet and Jacobi, Kummer was appointed to a full professorship at the University of Breslau, now Wroclaw, in Poland. In 1843, Kummer was aware that his attempts to prove Fermat's Last Theorem were flawed due to the lack of unique factorization in general. He introduced his "ideal numbers" that was the basis for the concept of an ideal, thus allowing the development of ring theory, and a substantial amount of abstract algebra later on. In 1855, Dirichlet left Berlin to succeed Gauss at Göttingen, and recommended to Berlin that they offer the vacant chair to Kummer, which they did. In 1857, the Paris Academy of Sciences awarded Kummer the Grand Prize for his work. In 1863, the Royal Society of London elected him as a Fellow. He died in Berlin on May 14, 1893.

Although Kummer may be best known for his failed attempt to prove FLT and the mathematics that derived from it, there are some not-so-well-known results that bear his name. For instance, in 1864 he published the discovery, now called the *Kummer surface*, that is a fourth order surface, based upon the singular surface of the quadratic line complex. This surface has sixteen isolated conical double points and sixteen singular tangent planes. This discovery emanated from his algebraic approach to geometric problems involving ray systems that had been studied by Sir William Rowan Hamilton (1805–1865).

4.4 Factoring

> *The thing which is the most outstanding and chiefly to be desired by all healthy and good and well-off persons, is leisure with honour.*
>
> *from chapter 98 of* **Pro Sestio**
> **Cicero (Marcus Tullius Cicero) (106–43 B.C.)**
> Roman orator and statesman
> —see the quotation on page 65.

The problem of factoring rational integers has taken on significant importance in the modern era. To a great extent, this is due to the increased need for security in the transmission of sensitive data such as military or banking communications. The theory that is behind all of this is called *cryptography*, the study of methods for sending messages in secret, namely in *enciphered* or *disguised* form to a recipient who has the knowledge to remove the disguise or *decipher* it. The RSA cryptosystem, for instance, is based upon the presumed difficulty of factoring—see [51] for details on RSA and other cryptosystems. (Think of a *cryptosystem*, also called a *cipher*, as a method for enciphering and deciphering.) Herein we will be concerned with the applications of algebraic number theory to such important problems as factoring, but not to the cryptographic descriptions themselves, which may be found in an introductory text on cryptography such as [51].

It is somewhat surprising that long-standing problems such as Fermat's Last Theorem have fallen to the sword of mathematical intellect, yet we still cannot do something as seemingly simple as that of factoring a 200-digit integer in reasonable computational time. However, this is the case. Factoring is intrinsically difficult. However, even this latter statement has only historical validation in the sense that a plethora of mathematicians and computer scientists have worked diligently to try to get efficient algorithms for factoring and, for all the work done, we have not advanced very far. However, there is no *proof* that verifies the intractability of factoring.

In this section, we will look at two closely allied factoring algorithms. We first look at some elementary facts about factoring that will historically lead into our algorithms that are the feature of this section.

◆ **The Integer Factoring Problem—(IFP)**

Given $n \in \mathbb{N}$, find primes p_j for $j = 1, 2, \dots, r \in \mathbb{N}$ with $p_1 < p_2 < \cdots < p_r$ and $e_j \in \mathbb{N}$ for $j = 1, 2, \dots, r$, such that

$$n = \prod_{j=1}^{r} p_j^{e_j}.$$

A simpler problem than the IFP is the notion of *splitting* of $n \in \mathbb{N}$, which means the finding of factors $r, s \in \mathbb{N}$ such that $1 < r \leq s$ such that $n = rs$. In order to solve the IFP for any integer, one merely splits n, then splits n/r and s if they are both composite, and so on until we have a complete factorization.

Trial Division: The oldest method of splitting n is *trial division*, by which we mean dividing n by all primes up to $\sqrt{n}$. For $n < 10^8$, or within that neighbourhood, this is not an unreasonable method in our computer-savvy world. However, for larger integers, we need more elaborate methods.

Fermat Factoring: If we have an $n \in \mathbb{N}$ such that

$$x^2 \equiv y^2 \pmod{n} \text{ with } x \not\equiv \pm\, y \pmod{n} \text{ for some } x, y \in \mathbb{Z}, \tag{4.42}$$

then n is necessarily composite since $\gcd(x-y,n)$ provides a nontrivial factor of n. This idea was known to Fermat who, in 1643, developed a method of factoring based upon the following observation.

If $n = rs$ is an odd natural number with $1 < r < \sqrt{n}$, then

$$n = a^2 - b^2 \text{ where } a = (r+s)/2 \text{ and } b = (s-r)/2.$$

Thus, in order to find a factor of n, we need only look at values $x = y^2 - n$ for

$$y = \lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots, (n-1)/2$$

until a perfect square is found. This is called *Fermat's difference of squares method.*

Euler's Factoring Method: This method applies only to integers of the form

$$n = x^2 + ay^2 = z^2 + aw^2,$$

where $x \neq z$ and $y \neq w$. In other words, n can be written in two distinct ways in this special form for a given nonzero value of $a \in \mathbb{Z}$. Then

$$(xw)^2 \equiv (n - ay^2)w^2 \equiv -ay^2w^2 \equiv (z^2 - n)y^2 \equiv (zy)^2 \pmod{n},$$

from which we may have a factor of n, namely, provided that $xw \not\equiv \pm\, zy \pmod{n}$. In this case, the (nontrivial) factors of n are given by $\gcd(xw \pm yz, n)$.

The Euler method essentially is predicated on the congruence (4.42), but unlike the Fermat method, not all integers have even one representation in the form $n = x^2 + ay^2$.

Legendre's Factoring Method: This method is a precursor to what we know today as *continued fraction methods for factorization*—see [51]. Legendre reasoned in the following fashion. Instead of looking at congruences of the form (4.42), he looked at those of the form

$$x^2 \equiv \pm py^2 \pmod{n} \text{ for primes } p, \tag{4.43}$$

since a solution to (4.43) implies that $\pm p$ is a quadratic residue of all prime factors of n. For instance, if the residue is 2, then all prime factors of n are congruent to $\pm 1 \pmod{8}$ (since it is a fact from elementary number theory that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{8}$—see (A.10) on page 342). Therefore, he would have halved the search for factors of n. Legendre applied this method for various values of p, thereby essentially constructing a quadratic sieve by getting many residues modulo n. (A *sieve* may be regarded as any process whereby we find numbers via searching up to a prescribed bound and eliminating candidates as we proceed until only the desired solution set remains. A [general] *quadratic* sieve is one in which about half of the possible numbers being sieved are removed from consideration, a technique used for hundreds of years as a scheme for eliminating impossible cases from consideration.) This allowed him to eliminate potential prime divisors that sit in various linear sequences, as with the residue 2 example above. He realized that if he could achieve enough of these, he could eliminate primes up to $\sqrt{n}$, thereby effectively developing a test for primality.

The linchpin of Legendre's method is the continued fraction expansion of $\sqrt{n}$, since he was simply finding *small* residues modulo n. Legendre was essentially building a sieve on the prime factors of n, which did not let him predict, for a given prime p, a different residue to yield a square. This meant that if he found a solution to $x^2 \equiv py^2 \pmod{n}$, he could not predict a solution, $w^2 \equiv pz^2 \pmod{n}$, *distinct* from the former. If he had been able to do this, he would have been able to combine them as

$$(xw)^2 \equiv (pzy)^2 \pmod{n}$$

and have a factor of n *provided that* $xw \not\equiv \pm\, pzy \pmod{n}$ since we are back to congruence (4.42).

In the 1920s, one individual expanded the idea, described above, of attempting to match the primes to create a square. We now look at his important influence.

Kraitchik's Factoring Method: Maurice Kraitchik determined that it would suffice to find a *multiple* of n as a difference of squares in attempting to factor it—see Biography 4.10 on page 173. For this purpose, he chose a polynomial of the form, $kn = ax^2 \pm by^2$, for some integer k, which allowed him to gain control over finding two distinct residues at a given prime to form a square, which Legendre could not do. In other words, Kraitchik used quadratic polynomials to get the residues, then multiplied them to get squares (not a square times a small number). Kraitchik developed this method over a period of more than three decades, a method later exploited by D.H. Lehmer and R.E. Powers—see [37]). They employed Kraitchik's technique but obtained their residues as Legendre had done.

In the early 1980s, Carl Pomerance was able to fine tune the parameters in Kraitchik's method described above—see [59]. We describe that process below but first need some notions used therein to be defined.

An important role in factorization is played by the following notion, which we will need as part of the algorithm to be described.

Definition 4.5 — Smooth Integers

A rational integer z is said to be smooth with respect to $y \in \mathbb{Z}$, or simply y-smooth, if all prime factors of z are less than or equal to y.

Remark 4.4 The term *factor base* means the choice of a suitable set of rational primes over which we may factor a set of integers. Also, if $\mathcal{F} = \{p_1, p_2, \ldots, p_k\}$ is a factor base, then from knowledge about the distribution of smooth integers close to $\sqrt{n}$, the optimal k is known to be one that is chosen to be

$$k \approx \sqrt{\exp(\sqrt{\log(n)\log\log(n)})}. \tag{4.44}$$

Now we are ready to describe the sieve.

Application 4.3 — The Quadratic Sieve (QS) Algorithm

(1) Choose a *factor base* $\mathcal{F} = \{p_1, p_2, \ldots, p_k\}$, where the p_j are primes for $j = 1, 2, \ldots, k \in \mathbb{N}$.

(2) For each nonnegative integer j, let $t = \pm j$. Compute

$$y_t = (\lfloor\sqrt{n}\rfloor + t)^2 - n$$

until $k + 2$ such values are found that are p_k-smooth. For each such t,

$$y_t = \pm \prod_{i=1}^{k} p_i^{a_{i,t}}, \tag{4.45}$$

and we form the binary $k + 1$-tuple,

$$\mathfrak{v}_t = (v_{0,t}, v_{1,t}, v_{2,t}, \ldots, v_{k,t}),$$

where $v_{i,t}$ is the least nonnegative residue of $a_{i,t}$ modulo 2 for $1 \le i \le k$, $v_{0,t} = 0$ if $y_t > 0$, and $v_{0,t} = 1$ if $y_t < 0$.

(3) Obtain a subset $\mathcal{S}$ of the values of t found in step (2) such that for each $i = 0, 1, 2, \ldots, k$,

$$\sum_{t \in \mathcal{S}} v_{i,t} \equiv 0 \pmod{2}. \tag{4.46}$$

In this case,

$$x^2 = \prod_{t \in \mathcal{S}} x_t^2 \equiv \prod_{t \in \mathcal{S}} y_t = y^2 \pmod{n},$$

where $x_t = \lfloor \sqrt{n} \rfloor + t$, so $\gcd(x \pm y, n)$ provides a nontrivial factor of n if $x \not\equiv \pm\, y \pmod{n}$.

In step (2), we have that $y_t \equiv x_t^2 \pmod{n}$. Thus, if a prime $p \mid y_t = x_t^2 - n$, we have $x_t^2 \equiv n \pmod{p}$. Thus, we must exclude from the factor base any primes p for which there is no solution $x \in \mathbb{Z}$ to the congruence $x^2 \equiv n \pmod{p}$. In other words, we exclude from the factor base any primes p for which n is *not* a quadratic residue modulo p.

Example 4.3 Let $n = 60377$. From Equation (4.44) on page 167, $k = 13$, so we choose the first thirteen primes for which n is a quadratic residue. They comprise our factor base $\mathcal{F} = \{2, 7, 11, 23, 29, 31, 37, 41, 53, 59, 61, 67, 71\}$. In the table below, we see, by inspection, that a subset $\mathcal{S}$ of the values of t such that $\sum_{t \in \mathcal{S}} v_{i,t} \equiv 0 \pmod{2}$ for each $i = 0, 1, 2, \ldots, 13$ is $\mathcal{S} = \{-1, -3, -6, -22\}$. (Note that $\lfloor \sqrt{n} \rfloor = 245$ in this case.) Thus,

$$\prod_{t \in \mathcal{S}} x_t^2 = 244^2 \cdot 242^2 \cdot 239^2 \cdot 223^2 \equiv 50885^2 \equiv x^2 \pmod{60377},$$

and

$$\prod_{t \in \mathcal{S}} y_t = 2^6 \cdot 7^2 \cdot 11^4 \cdot 29^2 \cdot 37^2 \equiv 25408^2 \equiv y^2 \pmod{60377}.$$

By computing both of the values,

$$\gcd(x - y, n) = \gcd(50885 - 25408, 60377) = 349$$

and

$$\gcd(x + y, n) = \gcd((50885 + 25408, 60377) = 173,$$

we get that $n = 60377 = 173 \cdot 349$.

t	x_t	y_t	$\mathfrak{v}_t$
-1	244	-29^2	$(1,0,0,0,0,0,0,0,0,0,0,0,0,0)$
-3	242	$-7^2 \cdot 37$	$(1,0,0,0,0,0,0,1,0,0,0,0,0,0)$
3	248	$7^2 \cdot 23$	$(0,0,0,0,1,0,0,0,0,0,0,0,0,0)$
-4	241	$-2^3 \cdot 7 \cdot 41$	$(1,1,1,0,0,0,0,0,1,0,0,0,0,0)$
4	249	$2^3 \cdot 7 \cdot 29$	$(0,1,1,0,0,1,0,0,0,0,0,0,0,0)$
-6	239	$-2^3 \cdot 11 \cdot 37$	$(1,1,0,1,0,0,0,1,0,0,0,0,0,0)$
6	251	$2^6 \cdot 41$	$(0,0,0,0,0,0,0,0,1,0,0,0,0,0)$
7	252	$53 \cdot 59$	$(0,0,0,0,0,0,0,0,0,1,1,0,0,0)$
-10	235	$-2^5 \cdot 7 \cdot 23$	$(1,1,1,0,1,0,0,0,0,0,0,0,0,0)$
11	256	$7 \cdot 11 \cdot 67$	$(0,0,1,1,0,0,0,0,0,0,0,0,1,0)$
-16	229	$-2^8 \cdot 31$	$(1,0,0,0,0,0,1,0,0,0,0,0,0,0)$
16	261	$2^6 \cdot 11^2$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
-20	225	$-2^3 \cdot 23 \cdot 53$	$(1,1,0,0,1,0,0,0,0,1,0,0,0,0)$
-22	223	$-2^3 \cdot 11^3$	$(1,1,0,1,0,0,0,0,0,0,0,0,0,0)$
22	267	$2^5 \cdot 11 \cdot 31$	$(0,1,0,1,0,0,1,0,0,0,0,0,0,0)$

Some elementary linear algebra underlies the solution to a factorization problem using the QS as depicted in Example 4.3. By ensuring that there are $k+2$ vectors $\mathfrak{v}_t$ in a $k+1$-dimensional vector space $\mathbb{F}_2^{k+1}$, we guarantee that there is a linear dependence relation among the $\mathfrak{v}_t$. In other words, we ensure the existence of the set $\mathcal{S}$ in step (3) of the algorithm such that congruence (4.46) holds. There is no guarantee that $x \not\equiv \pm\, y \pmod n$, but there are usually several dependency relations among the $\mathfrak{v}_t$, so there is a high probability that at least one of them will yield an (x, y) pair such that $x \not\equiv \pm\, y \pmod n$. The problem, of course, is that for "large" smoothness bounds B, we need a lot of congruences before we may be able to get these dependency relations.

The first successful implementation of the QS in which a serious number was factored occurred in 1983 when J. Gerver [21] factored a 47-digit number. Then, in 1984, the authors of [16] factored a 71-digit number.

The QS has been employed using an approach called *factoring by electronic mail.* This is a term used by Lenstra and Manasse in [40] to mean the distribution of the Quadratic Sieve operations to hundreds of physically separated computers all over the world, and in 1988 they used this approach to factor a 106-digit number. Indeed, it is this *parallel computing* that picks up the time.

In 1994, the authors of [2] factored the RSA-129 number[4.1] by using the electronic mail factoring technique with over 1600 computers and more than 600 researchers around the globe. The unit of time measurement for factoring is called a *mips year*, which is defined as being tantamount to the computational power of a computer rated at one *million instructions per second* (mips) and used for one year, which is equivalent to approximately $3 \cdot 10^{13}$ instructions. For instance, factoring the RSA-129 challenge number required 5000 mips years, and in 1989 the aforementioned factorization of the 106-digit number needed 140 mips years.

Now we are ready to present an algorithm that is closely tied to the QS, and is also a precursor for the number field sieve presented in §4.5. This algorithm involves factoring using certain cubic integers, namely the integers from

$$\mathfrak{O}_F = \mathbb{Z}[\sqrt[3]{-2}] = \mathbb{Z}[\sqrt[3]{2}]$$

(since $\sqrt[3]{-2} = -\sqrt[3]{2}$, which is the ring of integers of

$$F = \mathbb{Q}(\sqrt[3]{-2}) = \mathbb{Q}(\sqrt[3]{2}),$$

by Exercise 4.33 on page 173). In this section, we will show how we may employ these cubic integers in $\mathbb{Z}[\sqrt[3]{-2}]$ to factor integers in $\mathbb{Z}$. Some of what follows is adapted from [54].

We begin with a motivating example.

Example 4.4 We look at how to factor the fifth Fermat number

$$F_5 = 2^{32} + 1.$$

For convenience, set $\alpha = \sqrt[3]{-2}$. First, notice that

$$2F_5 = x^3 + 2, \text{ where } x = 2^{11},$$

and that

$$N_F(x - \alpha) = x^3 + 2, \text{ with } x - \alpha \in \mathbb{Z}[\alpha].$$

[4.1] Integers with n digits that are a product of two primes of approximately the same size are denoted by RSA-n, called an *RSA challenge number*.

In fact, by Exercise 4.35 on page 173, any $\beta = a + b\alpha + c\alpha^2$ has norm

$$N_F(\beta) = a^3 - 2b^3 + 4c^3 + 6abc. \tag{4.47}$$

By Exercise 4.34, there is a prime $\beta \in \mathbb{Z}[\alpha]$ such that $\beta \mid (x - \alpha)$, so by Exercise 2.46 on page 86,

$$N_F(\beta) \mid N_F(x - \alpha) = x^3 + 2.$$

Hence, we may be able to find a nontrivial factorization of F_5 via norms of certain elements of $\mathbb{Z}[\alpha]$. We do this as follows.

Consider elements of the form $a + b\alpha \in \mathbb{Z}[\alpha]$, for convenience, and sieve over values of a and b, testing for

$$\gcd(N_F(a + b\alpha), F_5) = \gcd(a^3 - 2b^3, F_5) > 1.$$

For convenience, we let a run over the values $1, 2, \ldots, 100$, and b run over the values $b = 1, 2, \ldots 20$. Formal reasons for this approach will be given later. We fix each value of a, and let b run over its range of values. The runs for $1 \le a \le 15$ and $1 \le b \le 20$ yield

$$\gcd(a^3 - 2b^3, F_5) = 1.$$

However, at $a = 16$, $b = 5$, we get

$$\gcd(16^3 - 2 \cdot 5^3, F_5) = 641.$$

In fact,

$$F_5 = 641 \cdot 6700417.$$

We may factor $16 + 5\alpha$ as follows.

$$16 + 5\alpha = (1 + \alpha)(-1 + \alpha)(\alpha)(-9 + 2\alpha - \alpha^2),$$

where $1 + \alpha$ is a unit with norm -1; $-1 + \alpha$ has norm -3; α has norm -2; and

$$\beta = -9 + 2\alpha - \alpha^2$$

has norm -641. This accounts for

$$16^3 - 2 \cdot 5^3 = 2 \cdot 3 \cdot 641,$$

and shows that β is the predicted prime divisor of $x - \alpha$, which gives us the nontrivial factor of F_5.

The method in Example 4.4 works well largely because of the small value of F_5. However, it may not be feasible for larger values to check all of the gcd conditions over a much larger range. The following method of Pollard, which he introduced in 1991 in [58], uses the above notions of factorizations in $\mathbb{Z}[\alpha]$ to factor F_7, which was first accomplished in 1970.

As in the above case, suppose that $n \in \mathbb{N}$ with

$$2n = m^3 + 2.$$

For instance,

$$2F_7 = m^3 + 2$$

where $m = 2^{43}$. Pollard's idea to factor $n = F_7$ involves B-smooth numbers of the form $a + bm$, for some suitable B that will be the number of primes in a prescribed set defined in the algorithm below. Also, $a + b\alpha$ will be B-smooth meaning that its *norm* is B-smooth in the sense of Definition 4.5 on page 167. Thus, if we get a factorization of $a + b\alpha$ in $\mathbb{Z}[\alpha]$, we also get a corresponding factorization of $a + bm$ modulo F_7. To see this, one must understand a notion that we will generalize when we discuss the number field sieve in §4.5. We let

$$\psi : \mathbb{Z}[\alpha] \mapsto \mathbb{Z}/n\mathbb{Z}$$

be a ring homomorphism such that $\psi(\alpha) = m$. Thus, in $\mathbb{Z}/n\mathbb{Z}$,

$$x^3 = -2 = -(1 + 1), \text{ where 1 is the identity of } \mathbb{Z}/n\mathbb{Z}.$$

Hence, ψ is that unique map which is defined element-wise by the following.

$$\psi\left(\sum_{j=0}^{2} z_j\alpha^j\right) = \sum_{j=0}^{2} z_j m^j \in \mathbb{Z}/n\mathbb{Z}, \text{ where } z_j \in \mathbb{Z}.$$

The role of this map ψ in attempting to factor a number n is given by the following.

Suppose that we have a set $\mathcal{S}$ of polynomials

$$g(x) = \sum_{j=0}^{2} z_j x^j \in \mathbb{Z}[x]$$

such that

$$\prod_{g\in\mathcal{S}} g(\alpha) = \beta^2$$

where $\beta \in \mathbb{Z}[\alpha]$, and

$$\prod_{g\in\mathcal{S}} g(m) = y^2,$$

where $y \in \mathbb{Z}$. Then if $\psi(\beta) = x \in \mathbb{Z}$, we have $x^2 \equiv \psi(\beta)^2 \equiv \psi(\beta^2) \equiv \psi\left(\prod_{g\in\mathcal{S}} g(\alpha)\right) \equiv \prod_{g\in\mathcal{S}} g(m) \equiv y^2 \pmod{n}$. In other words, this method finds a pair of integers x, y such that

$$x^2 - y^2 \equiv (x - y)(x + y) \equiv 0 \pmod{n},$$

so we may have a nontrivial factor of n by looking at $\gcd(x - y, n)$.

We now describe the algorithm, but give a simplified version of it, since this is meant to be a simple introduction to the ideas behind the number field sieve. We use a very small value of n as an example for the sake of simplicity, namely $n = 23329$. Note that $2n = 36^3 + 2 = m^3 + 2$. We will also make suitable references in the algorithm in terms of how Pollard factored $n = F_7$.

Application 4.4 — Pollard's Algorithm

Step 1: Compute a *factor base.*

In the case of cubic integers in $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt[3]{-2}]$, we take for $n = 23329$ only the first eleven primes as the factor base, those up to and including 41 (or for $n = F_7$, Pollard chose the first five hundred rational primes) as $\mathcal{FB}_1$, the first part of the factor base, and for the second part, $\mathcal{FB}_2$, we take those primes of $\mathbb{Z}[\alpha]$ with norms $\pm p$, where $p \in \mathcal{FB}_1$. (The reasons behind the choice of the number of primes in $\mathcal{FB}_1$ are largely empirical.) Also, we include the units $-1, 1 + \alpha$, and $1/(1 + \alpha) = -1 + \alpha - \alpha^2$ in $\mathcal{FB}_2$. Here, we have discarded the $\mathbb{Z}[\alpha]$-primes of norm p^2 or p^3, since these cannot divide our n, given that they cannot divide the $a + b\alpha$, with the assumptions we are making.

Step 2: Run the sieve.

In this instance, the sieve involves finding numbers $a+bm$ that are composed of some primes from $\mathcal{FB}_1$. For $n = 23329$, we sieve over values of a from -5 to 5 and values of b from 1 to 10 (or for $n = F_7$, Pollard chose values of a from -4800 to 4800, and values of b from 1 to 2000). Save only coprime pairs (a, b).

Step 3: Look for smooth values of the norm, and obtain factorizations of $a+bx$ and $a+b\alpha$.

Here, smooth values of the norm means that $N = N_F(a+b\alpha) = a^3 - 2b^3$ is not divisible by any primes bigger than those in $\mathcal{FB}_1$. For those (a, b) pairs, factor $a + bm$ by trial division, and eliminate unsuccessful trials. Factor $a + b\alpha$ by computing the norm $N_F(a + b\alpha)$ and using trial division. When a prime p is found, then divide out a $\mathbb{Z}[\alpha]$-prime of norm $\pm p$ from $a + b\alpha$. This will involve getting primes in the factorization of the form $a + b\alpha + c\alpha^2$ where $c \neq 0$. Units may also come into play in the factorizations, and a table of values of $(1 + \alpha)^j$ is kept for such purposes with $j = -2, \cdots, 2$ for $n = 23329$ (or for F_7, one should choose to keep a record of units for $j = -8, -7, \ldots, 8$). Some data extracted for the run on $n = 23329$ is given as follows.

Table 4.1

$a + b\alpha + c\alpha^2$	N	factorization of $a + b\alpha + c\alpha^2$
$5 + \alpha$	$3 \cdot 41$	$(-1 + \alpha)(-1 - 2\alpha - 2\alpha^2)$
$4 + 10\alpha$	$-2^4 \cdot 11^2$	$-(3 + 2\alpha)^2\alpha^4(-1 + \alpha - \alpha^2)^2$
$-1 + \alpha$	-3	$-1 + \alpha$
$-1 - 2\alpha - 2\alpha^2$	-41	$-1 - 2\alpha - 2\alpha^2$
$3 + 2\alpha$	11	$3 + 2\alpha$
α	-2	α
$-1 + \alpha - \alpha^2$	-1	*unit*

Table 4.2

$a + bm + cm^2$	factorization of $a + bm + cm^2$
$5 + m$	41
$4 + 10m$	$2^2 \cdot 7 \cdot 13$
$-1 + m$	$5 \cdot 7$
$-1 - 2m - 2m^2$	$-5 \cdot 13 \cdot 41$
$3 + 2m$	$3 \cdot 5^2$
m	$2^2 \cdot 3^2$
$-1 + m - m^2$	$-13 \cdot 97$

Step 4: Complete the factorization.

By selecting -1 times the first four rows in the third column of Table 4.1, we get a square in $\mathbb{Z}[\alpha]$:

$$\beta^2 = (-1 + \alpha)^2(-1 - 2\alpha - 2\alpha^2)^2(3 + 2\alpha)^2\alpha^4(-1 + \alpha - \alpha^2)^2, \tag{4.48}$$

and correspondingly, since β^2 is also -1 times the first four rows in the first column of Table 4.1, we get:

$$\beta^2 = (5 + \alpha)(-4 - 10\alpha)(-1 + \alpha)(-1 - 2\alpha - 2\alpha^2). \tag{4.49}$$

Then we get a square in $\mathbb{Z}$ from Table 4.2 by applying ψ to (4.49):

$$\psi(\beta^2) = (5 + m)(-4 - 10m)(-1 + m)(-1 - 2m - 2m^2) = 2^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 41^2 = y^2.$$

Also, by applying ψ to β via (4.48), we get:

$$\psi(\beta) = (-1 + m)(-1 - 2m - 2m^2)(3 + 2m)m^2(-1 + m - m^2) \equiv 9348 \pmod{23329},$$

so by setting $x = \psi(\beta)$, we have

$$x^2 = \psi^2(\beta) = \psi(\beta^2) \equiv y^2 \pmod{n}.$$

Since

$$y = 2 \cdot 5 \cdot 7 \cdot 13 \cdot 41 \equiv 13981 \pmod{23329},$$

then $y - x \equiv 4633 \,(\text{mod } 23329)$. However, $\gcd(4633, 23329) = 41$. In fact $23329 = 41 \cdot 569$. Pollard used the algorithm in a similar fashion to find integers X and Y for the more serious factorization $\gcd(X - Y, F_7) = 59649589127497217$. Hence, we have a factorization of F_7 as follows.

$$F_7 = 59649589127497217 \cdot 5704689200685129054721.$$

Essentially, the ideas for factoring using cubic integers above is akin to the notion of the strategy used in the QS method. There, we try to generate sufficiently many smooth quadratic residues of n close to $\sqrt{n}$. In the cubic case, we try to factor numbers that are close to perfect cubes. In §4.5, we will extend these ideas to show how F_9 was factored using the number field sieve, and $\mathbb{Z}[\sqrt[5]{2}]$.

Exercises

4.33. Prove that $\mathbb{Z}[\sqrt[3]{-2}]$ is the ring of integers of $\mathbb{Q}(\sqrt[3]{-2})$.

4.34. Prove that every nonzero ideal in a Dedekind domain R must contain a prime element.

4.35. Prove that (4.47) holds in Example 4.4.

4.36. Use Pollard's method to factor F_6.

In Exercises 4.37–4.39, use the gcd *method described before Pollard's method to find an odd factor of the given integer.*

4.37. $5^{77} - 1$.

4.38. $7^{149} + 1$. (*Hint: Use* $\mathbb{Z}[\sqrt[3]{-7}]$.)

4.39. $3^{239} - 1$. (*Hint: Use* $\mathbb{Z}[\sqrt[3]{3}]$.)

Factor each of the integers in Exercises 4.40–4.43 using the QS method.

4.40. $n = 3191491$.

4.41. $n = 12358397$.

4.42. $n = 42723991$.

4.43. $n = 74299271$.

Biography 4.10 Maurice Borisovich Kraitchik (1882–1957) obtained his Ph.D. from the University of Brussels in 1923. He worked as an engineer in Brussels and later as a Director at the Mathematical Sciences section of the Mathematical Institute for Advanced Studies there. From 1941–1946, he was Associate Professor at the New School for Social Research in New York. In 1946, he returned to Belgium, where he died on August 19, 1957. His work over thirty-five years on factoring methods stands tall today because he devised and used a variety of practical techniques that are found today in computer methods such as the QS method. He is also the author of the popular book *Mathematical Recreations* [34].

4.5 The Number Field Sieve

> *When fortune is lavish of her favours, beware of adversity; events do not always succeed each other in one train of fortunes.*
>
> **Cato the elder (Marcus Porcius Cato) (234 B.C.–149 B.C.)**
>
> Roman statesman, orator, and writer

In §4.4 we provided a motivator for the sieve in this section via Pollard's algorithm, which we showed to be linked to the QS. Some of what follows is adapted from [54].

In 1988, John Pollard circulated a manuscript that contained the outline of a new algorithm for factoring integers, which we studied in §4.4. In 1990, the first practical version of Pollard's algorithm was given in [39], published in 1993, the authors of which dubbed it the *number field sieve.* Pollard had been motivated by a discrete logarithm algorithm given in 1986, by the authors of [13], which employed quadratic fields. Pollard looked at the more general scenario by outlining an idea for factoring certain large integers using number fields. The special numbers that he considered are those large composite natural numbers that are "close" to being powers, namely those $n \in \mathbb{N}$ of the form $n = r^t - s$ for small natural numbers r and $|s|$, and a possibly much larger natural number t. Examples of such numbers, which the number field sieve had some successes factoring, may be found in tables of numbers of the form

$$n = r^t \pm 1, \text{ called } \textit{Cunningham numbers}.$$

However, the most noteworthy success was factorization of the ninth Fermat number $F_9 = 2^{2^9}+1 = 2^{512}+1$ (having 155 decimal digits), by the Lenstra brothers, Manasse and Pollard in 1990, the publication of which appeared in 1993—see [41].

To review some of the history preceding the number field sieve, we observe the following. Prior to 1970, a 25-digit integer was considered difficult to factor. In 1970, the power of the continued fraction method raised this to 50 digits—see [53, §5.4, pp. 240–242]. Once the algorithm was up and running in 1970, legions of 20- to 45-digit numbers were factored that could not be factored before. The first major success was the factorization of the seventh Fermat number

$$F_7 = 2^{2^7} + 1 = 2^{128} + 1,$$

a 39-digit number, which we described via Pollard's method in §4.4. By the mid 1980s, the quadratic sieve algorithm was felling 100-digit numbers. With the dawn of the number field sieve, 150-digit integers were now being tackled. The number field sieve is considered to be asymptotically faster than any known algorithm for the special class of integers of the above special form to which it applies. Furthermore, the number field sieve can be made to work for arbitrary integers. For details, see [7], where the authors refer to the number field sieve for the special number $n = r^t - s$ as the *special number field sieve.* The more general sieve has come to be known as the *general number field sieve.*

Much older than any of the aforementioned ideas for factoring is that attributed to Fermat, namely the writing of n as a difference of two squares. However, this idea was enhanced by Maurice Kraitchik in the 1920s, both approaches we also reviewed in §4.4. To further describe Kraitchik's influence, we review it from a slightly different perspective here. He reasoned it might suffice to find a *multiple of* n as a difference of squares, namely,

$$x^2 \equiv y^2 \pmod{n}, \tag{4.50}$$

so that one of $x-y$ or $x+y$ *could* be divisible by a factor of n. We say *could* here since we fail to get a nontrivial factor of n when $x \equiv \pm y \pmod{n}$. However, it can be shown that if n is divisible by at least two distinct odd primes, then for at least half of the pairs x (modulo n), and y (modulo n), satisfying (4.50) with $\gcd(x, y) = 1$, we will have $1 < \gcd(x-y, n) < n$.

This classical idea of Kraitchik had seeds in the work of Gauss, but Kraitchik introduced it into a new century in the pre-dawn of the computer age. This idea is currently exploited by many algorithms via construction of these (x, y)-pairs. For instance, the QS algorithm uses it. More recently, the number field sieve exploits the idea. To see how this is done, we give a brief overview of the methodology of the number field sieve. This will motivate the formal description of the algorithm.

For $n = r^t - s$ we wish to choose a number field of degree d over $\mathbb{Q}$. The following choice for d is made for reasons (which we will not discuss here), which make it the optimal selection, at least theoretically. (The interested reader may consult [39, Sections 6.2–6.3, pp. 31–32] for the complexity analysis and reasoning behind these choices.) Set

$$d = \left(\frac{(3 + o(1)) \log n}{2 \log \log n} \right)^{1/3}. \tag{4.51}$$

Now select $k \in \mathbb{N}$, which is minimal with respect to $kd \geq t$. Therefore, $r^{kd} \equiv sr^{kd-t} \pmod{n}$. Set

$$m = r^k, \text{ and } c = sr^{kd-t}. \tag{4.52}$$

Then $m^d \equiv c \pmod{n}$. Set

$$f(x) = x^d - c,$$

and let $\alpha \in \mathbb{C}$ be a root of f. Then this leads to a choice of a number field, namely $F = \mathbb{Q}(\alpha)$. Although the number field sieve can be made to work when $\mathbb{Z}[\alpha]$ is *not* a UFD, the assumption that it *is* a UFD simplifies matters greatly in the exposition of the algorithm, so we will make this assumption. Note that once made, this assumption implies that $\mathfrak{O}_F = \mathbb{Z}[\alpha]$. See [39] for a description of the modifications necessary when it is not a UFD.

Now the question of the irreducibility of f arises. If f is reducible over $\mathbb{Z}$, we are indeed lucky, since then $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Z}[x]$, where $0 < \deg(g) < \deg(f)$. Therefore, $f(m) = n = g(m)h(m)$ is a nontrivial factorization of n, and we are done. Use of the number field sieve is unnecessary. However, the probability is high that f is irreducible since *most* primitive polynomials over $\mathbb{Z}$ *are irreducible.* Hence, for the description of the number field sieve, we may assume that f is irreducible over $\mathbb{Z}$.

Since $f(m) \equiv 0 \pmod{n}$, we may define the natural homomorphism,

$$\psi : \mathbb{Z}[\alpha] \mapsto \mathbb{Z}/n\mathbb{Z},$$

given by

$$\alpha \mapsto \overline{m} \in \mathbb{Z}/n\mathbb{Z}.$$

Then

$$\psi \left(\sum_j a_j \alpha^j \right) = \sum_j a_j \overline{m}^j.$$

Now define a set $\mathcal{S}$ consisting of pairs of relatively prime integers (a, b), satisfying the following two conditions:

$$\prod_{(a,b) \in \mathcal{S}} (a + bm) = c^2, \quad (c \in \mathbb{Z}), \tag{4.53}$$

and

$$\prod_{(a,b)\in\mathcal{S}} (a+b\alpha) = \beta^2, \quad (\beta \in \mathbb{Z}[\alpha]). \tag{4.54}$$

Thus, $\psi(\beta^2) = \overline{c}^2$, so $\psi(\beta^2) \equiv c^2 \pmod{n}$. In other words, since $\psi(\beta^2) = \psi(\beta)^2$, then if we set $\psi(\beta) = h \in \mathbb{Z}$, $h^2 \equiv c^2 \pmod{n}$. This takes us back to Kraitchik's original idea, and we may have a nontrivial factor of n, namely $\gcd(h \pm c, n)$ (provided that $h \not\equiv \pm c \pmod{n}$).

The above overview of the number field sieve methodology is actually a special case of an algebraic idea, which is described as follows. Let R be a ring with homomorphism

$$\phi : R \mapsto \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

together with an algorithm for computing nonzero diagonal elements (x, x) for $x \in \mathbb{Z}/n\mathbb{Z}$. Then the goal is to multiplicatively combine these elements to obtain squares in R whose square roots have an image under ϕ not lying in $(x, \pm x)$ for nonzero $x \in \mathbb{Z}/n\mathbb{Z}$. The number field sieve is the special case

$$R = \mathbb{Z} \times \mathbb{Z}[\alpha], \text{ with } \phi(z,\beta) = (\overline{z},\psi(\beta)).$$

Before setting down the details of the formal number field sieve algorithm, we discuss the crucial role played by *smoothness* introduced in Definition 4.5 on page 167. Recall that a smooth number is one with only "small" prime factors. In particular, $n \in \mathbb{N}$ is B-smooth for $B \in \mathbb{R}^+$, if n has no prime factor bigger than B. Smooth numbers satisfy the triad of properties:

(1) They are fairly numerous (albeit sparse).

(2) They enjoy a simple multiplicative structure.

(3) They play an essential role in discrete logarithm algorithms.

If $F = \mathbb{Q}(\alpha)$ is a number field, then by definition

> an algebraic number $a + b\alpha \in \mathbb{Z}[\alpha]$ is B-smooth if $|N_F(a + b\alpha)|$ is B-smooth.

Hence, $a + b\alpha$ is B-smooth if and only if all primes dividing $|N_F(a + b\alpha)|$ are less than B. Thus, the idea behind the number field sieve is to look for small relatively prime numbers a and b such that both $a + \alpha b$ and $a + \overline{m}b$ are smooth. Since $\psi(a + \alpha b) = a + \overline{m}b$, then each pair provides a congruence modulo n between two products. Sufficiently many of these congruences can then be used to find solutions to $h^2 \equiv c^2 \pmod{n}$, which may lead to a factorization of n.

The above overview leaves open the demanding questions as to how we choose the degree d, the integer m, and how the set of relatively prime integers a, b such that Equations (4.53)–(4.54) can be found. These questions may now be answered in the following formal description of the algorithm.

Application 4.5 — The Number Field Sieve Algorithm

Step 1—Selection of a Factor Base and Smoothness Bound

There is a consensus that smoothness bounds are best chosen empirically. However, there are theoretical reasons for choosing such bounds as

$$B = \exp((2/3)^{2/3}(\log n)^{1/3}(\log\log n)^{2/3}),$$

which is considered to be optimal since it is based upon the choice for d as above. See [39, Section 6.3, p. 32] for details. Furthermore, the reasons for this being called a smoothness bound will unfold in the sequel.

Define a set $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$, where the component sets $\mathcal{S}_j$ are given as follows. $\mathcal{S}_1 = \{p \in \mathbb{Z} : p \text{ is prime and } p \leq B\}$,

$$\mathcal{S}_2 = \{u_j : j = 1, 2, \ldots, r_1 + r_2 - 1, \text{ where } u_j \text{ is a generator of } \mathfrak{U}_{\mathfrak{O}_F}\}.$$

(Here $\{r_1, r_2\}$ is the signature of F, and the generators u_j are the generators of the infinite cyclic groups given by Dirichlet's Unit Theorem that we presented as Theorem 3.20 on page 135.) Also,

$$\mathcal{S}_3 = \{\beta = a + b\alpha \in \mathbb{Z}[\alpha] : |N_F(\beta)| = p < B_2 \text{ where } p \text{ is prime}\},$$

where B_2 is chosen empirically. Now we set the factor base as

$$\mathcal{F} = \{a_j = \psi(j) \in \mathbb{Z}/n\mathbb{Z} : j \in \mathcal{S}\}.$$

Also, we may assume $\gcd(a_j, n) = 1$ for all $j \in \mathcal{S}$, since otherwise we have a factorization of n and the algorithm terminates.

Step 2—Collecting Relations and Finding Dependencies

We wish to collect relations (4.53)–(4.54) such that they occur simultaneously, thereby yielding a potential factor of n. One searches for relatively prime pairs (a, b) with $b > 0$ satisfying the following two conditions.

(i) $|a + bm|$ is B-smooth except for at most one additional prime factor p_1, with $B < p_1 < B_1$, where B_1 is empirically determined.

(ii) $a + b\alpha$ is B_2-smooth except for at most one additional prime $\beta \in \mathbb{Z}[\alpha]$ such that $|N_F(\beta)| = p_2$ with $B_2 < p_2 < B_3$, where B_3 is empirically chosen.

The prime p_1 in (i) is called the *large prime*, and the prime p_2 in (ii) is called the *large prime norm*. Pairs (a, b) for which p_1 and p_2 do not exist (namely when we set $p_1 = p_2 = 1$) are called *full relations*, and are called *partial relations* otherwise. In the sequel, we will only describe the full relations since, although the partial relations are more complicated, they lead to relations among the factor base elements in a fashion completely similar to the ones for full relations. For details on partial relations, see [41, Section 5].

First, we show how to achieve relations in Equation (4.53), the "easy" part (relatively speaking). (This is called the *rational part*, whereas relations in Equation (4.54) are called the *algebraic part*.) Then we show how to put the two together. To do this, we need the following notion from linear algebra.

Every $n \in \mathbb{N}$ has an exponent vector $v(n)$ defined by $n = \prod_{j=1}^{\infty} p_j^{v_j}$, where p_j is the j^{th} prime, only finitely many of the v_j are nonzero, and

$$v(n) = (v_1, v_2, \ldots) = (v_j)_{j=1}^{\infty}$$

with an infinite string of zeros after the last significant place. We observe that n is a square if and only if each v_j is even. Hence, for our purposes, the v_j give *too much* information. Thus, to simplify our task, we reduce each v_j modulo 2. Henceforth, then $\overline{v_j}$ means v_j reduced modulo 2. We modify the notion of the exponent vector further for our purposes by letting $B_1 = \pi(B)$, where $\pi(B)$ is the number of primes no bigger than B. Then, with $p_0 = -1$, $a + bm = \prod_{j=0}^{B_1} p_j^{v_j}$ is the factorization of $a + bm$. Set

$$v(a + bm) = (\overline{v_0}, \ldots, \overline{v_{B_1}}),$$

for each pair (a, b) with $a + b\alpha \in \mathcal{S}_3$. The choice of B allows us to make the assumption that $|\mathcal{S}_3| > B_1 + 1$. Therefore, the vectors in $v(a + bm)$ for pairs (a, b) with $a + b\alpha \in \mathcal{S}_3$ exceed the dimension of the $\mathbb{F}_2$-vector space $\mathbb{F}_2^{B_1+1}$. In other words, we have *more than* $B_1 + 1$ vectors in a $B_1 + 1$-dimensional vector space. Therefore, there exist nontrivial linear dependence relations between vectors. This implies the existence of a subset $\mathcal{T}$ of $\mathcal{S}_3$ such that

$$\sum_{a+b\alpha\in\mathcal{T}} v(a + bm) = 0 \in \mathbb{F}_2^{B_1+1},$$

so

$$\prod_{a+b\alpha\in\mathcal{T}} (a + bm) = z^2 \quad (z \in \mathbb{Z}).$$

This solves Equation (4.53).

Now we turn to the algebraic relations in Equation (4.54). We may calculate the norm of $a + b\alpha$ by setting $x = a$ and $y = b$ in the homogeneous polynomial $(-y)^d f(-x/y) = x^d - c(-y)^d$, with $f(x) = x^d - c$. Therefore, $N_F(a + b\alpha) = (-b)^d f(-ab^{-1}) = a^d - c(-b)^d$. Let

$$R_p = \{r \in \mathbb{Z} : 0 \le r \le p - 1, \text{ and } f(r) \equiv 0 \pmod{p}\}.$$

Then for $\gcd(a, b) = 1$, we have $N_F(a + b\alpha) \equiv 0 \,(\text{mod } p)$ if and only if $a \equiv -br \,(\text{mod } p)$, and this r is unique. Observe that by the relative primality of a and b, the multiplicative inverse b^{-1} of b modulo p is defined since, for $b \equiv 0 \,(\text{mod } p)$, there are no nonzero pairs (a, b) with $N_F(a + b\alpha) \equiv 0 \,(\text{mod } p)$.

The above shows that there is a one-to-one correspondence between those $\beta \in \mathbb{Z}[\alpha]$ with $|N_F(\beta)| = p$, a prime and pairs (p, r) with $r \in R_p$. Note that the kernel of the natural map $\psi : \mathbb{Z}[\alpha] \mapsto \mathbb{Z}/p\mathbb{Z}$ is $\ker(\psi) = \langle a + b\alpha\rangle$, the cyclic subgroup of $\mathbb{Z}[\alpha]$ generated by $a + b\alpha$. It follows that $|\mathbb{Z}[\alpha] : \langle a + b\alpha\rangle| = |N_F(a + b\alpha)| = p$, so $\mathbb{Z}[\alpha]/\langle a + b\alpha\rangle$ is a field.

This corresponds to saying that the $\mathbb{Z}[\alpha]$-ideal $\mathcal{P} = (a+b\alpha)$ is a principal, first-degree prime $\mathbb{Z}[\alpha]$-ideal, namely one for which $N_F(\mathcal{P}) = p^1 = p$. Hence, $\mathbb{Z}[\alpha]/\mathcal{P} \cong \mathbb{F}_p$, the finite field of p elements.

The above tells us that in Step 1 of the number field sieve algorithm, the set $\mathcal{S}_3$ essentially consists of the first-degree prime $\mathbb{Z}[\alpha]$-ideals of norm $N_F(\mathcal{P}) \le B_2$. These are the *smooth, degree one, prime* $\mathfrak{O}_F$*-ideals*, namely those ideals whose prime norms are B_2-smooth.

In part (ii) of Step 2 of the algorithm on page 177, the additional prime element $\beta \in \mathbb{Z}[\alpha]$ such that $|N_F(\beta)| = p_2$ with $B_2 < p_2 < B_3$ corresponds to the prime $\mathfrak{O}_F$-ideal $\mathcal{P}_2$ called the *large prime ideal.* Moreover, $\mathcal{P}_2$ corresponds to the pair $(p_2, c\,(\text{mod } p_2))$, where $c \in \mathbb{Z}$ is such that $a \equiv -bc\,(\text{mod } p_2)$, thereby enabling us to distinguish between prime ideals of the same norm. If the large prime in Step 2 does not occur, we write $\mathcal{P}_2 = (1)$. Now, since

$$|a + bm| = \prod_{p\in\mathcal{S}_1} p^{v_p},$$

and

$$|a + b\alpha| = \prod_{u\in\mathcal{S}_2} u^{t_u} \prod_{s\in\mathcal{S}_3} s^{v_s}, \tag{4.55}$$

for nonnegative $t_u, v_s \in \mathbb{Z}$, and since $\psi(a + bm) = \psi(a + b\alpha)$, then

$$\prod_{p\in\mathcal{S}_1} \psi(p)^{v_p} = \prod_{u\in\mathcal{S}_2} \psi(u)^{t_u} \prod_{s\in\mathcal{S}_3} \psi(s)^{v_s},$$

in $\mathbb{Z}/n\mathbb{Z}$. Therefore, we achieve a relationship among the elements of the factor base $\mathcal{F}$, as follows

$$\prod_{u \in \mathcal{S}_2} \psi(u)^{t_u} \prod_{s \in \mathcal{S}_3} \psi(s)^{v_s} \equiv \prod_{p \in \mathcal{S}_1} \psi(p)^{v_p} \pmod{n}. \tag{4.56}$$

Furthermore, we may translate (4.55) ideal-theoretically into the ideal product

$$|a + b\alpha| = \prod_{u \in \mathcal{S}_2} u^{t_u} \prod_{\mathcal{P} \in \mathcal{S}_3} \pi_{\mathcal{P}}^{v_{\mathcal{P}}}, \tag{4.57}$$

where $\mathcal{P}$ ranges over all of the first-degree prime $\mathbb{Z}[\alpha]$-ideals of norm less than B_2, and $\pi_{\mathcal{P}}$ is a generator of $\mathcal{P}$.

Thus, (4.56) gives rise to the identity

$$\prod_{p \in \mathcal{S}_1} \psi(p)^{v_p} = \prod_{u \in \mathcal{S}_2} \psi(u)^{t_u} \prod_{\mathcal{P} \in \mathcal{S}_3} \psi(\pi_{\mathcal{P}})^{v_{\mathcal{P}}}.$$

If $|\mathcal{S}_3| > \pi(B)$, then by applying Gaussian elimination for instance, we can find $x(a,b) \in \{0,1\}$ such that simultaneously

$$\prod_{a+b\alpha \in \mathcal{S}_3} (a + b\alpha)^{x(a,b)} = \left(\left(\prod_{u \in \mathcal{S}_2} u^{\overline{t_u}}\right)\left(\prod_{s \in \mathcal{S}_3} s^{\overline{v_s}}\right)\right)^2,$$

and

$$\prod_{a+b\alpha \in \mathcal{S}_3} (a + bm)^{x(a,b)} = \left(\left(\prod_{p \in \mathcal{S}_1} p^{\overline{v_p}}\right)\right)^2,$$

hold. From this a factorization of n may be gleaned, by Kraitchik's method.

Practically speaking, the number field sieve tasks consist of sieving all pairs (a,b) for $b = b_1, b_2 \ldots, b_n$ for short (overlapping) intervals $[b_1, b_2]$, with $|a|$ less than some given bound. All relations, full and partial, are gathered in this way until sufficiently many have been collected.

The big prize garnered by the number field sieve was the factorization of F_9, the ninth Fermat number, as described in [41]. In 1903, A.E. Western found the prime factor $2424833 = 37 \cdot 2^{16} + 1$ of F_9. Then in 1967, Brillhart determined that $F_9/2424833$ (having 148 decimal digits) is composite by showing that it fails to satisfy Fermat's Little Theorem. Thus, the authors of [41] chose

$$n = F_9/2424833 = \left(2^{512} + 1\right)/2424833.$$

Then they exploited the above algorithm as follows. If we choose d as in Equation (4.51) on page 175, we get that $d = 5$. The authors of [41] then observed that since $2^{512} \equiv -1 \pmod{n}$, then for $h = 2^{205}$, we get $h^5 \equiv 2^{1025} \equiv 2 \cdot \left(2^{512}\right)^2 \equiv 2 \pmod{n}$. This allowed them to choose the map $\psi : \mathbb{Z}[\sqrt[5]{2}] \mapsto \mathbb{Z}/n\mathbb{Z}$, given by $\psi : \sqrt[5]{2} \mapsto 2^{205}$. Here $\mathbb{Z}[\sqrt[5]{2}]$ is a UFD. Then they chose m and c as in Equation (4.52), namely since $r = 2$, $s = -1$, and $t = 512$, then the minimal k with $5k = dk \geq t = 512$ is $k = 103$, and $m = 2^{103}$, so $c = -8 \equiv 2^{5 \cdot 103} \pmod{n}$. This gives rise to $f(x) = x^5 + 8$ with root $\alpha = -\sqrt[5]{2}^3$, and $\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\sqrt[5]{2}]$. Observe that $8F_9 = 2^{515} + 8 = \left(2^{103}\right)^5 + 8$. Thus, $\psi(\alpha) = m = 2^{103} \equiv -2^{615} \equiv -\left(2^{205}\right)^3 \pmod{n}$. Notice that 2^{103} is small in relation to n, and is in fact closer to $\sqrt[5]{n}$. Since

$$\psi(a + b\alpha) = a + 2^{103}b \in \mathbb{Z}/n\mathbb{Z},$$

we are in a position to form relations as described in the above algorithm. Indeed, the authors of [41] actually worked only in the subring $\mathbb{Z}[\alpha]$ to find their relations. The sets they chose from Step 1 are $\mathcal{S}_1 = \{p \in \mathbb{Z} : p \le 1295377\}$,

$$\mathcal{S}_2 = \{-1, -1 + \sqrt[5]{2}, -1 + \sqrt[5]{2}^2 - \sqrt[5]{2}^3 + \sqrt[5]{2}^4\},$$

for units $u_1 = -1$, $u_2 = -1 + \sqrt[5]{2}$, and $u_3 = -1 + \sqrt[5]{2}^2 - \sqrt[5]{2}^3 + \sqrt[5]{2}^4$, and

$$\mathcal{S}_3 = \{\beta \in \mathbb{Z}[\alpha] : |N_F(\beta)| = p \le 1294973, \, p \text{ a prime}\}.$$

The authors began sieving in mid-February of 1990 on approximately thirty-five workstations at Bellcore. On the morning of June 15, 1990 the first of the dependency relations that they achieved turned out to give rise to a trivial factorization! However, an hour later their second dependency relation gave way to a 49-digit factor. This and the 99-digit cofactor were determined by A. Odlyzko to be primes, on that same day. They achieved: $F_9 = q_7 \cdot q_{49} \cdot q_{99}$, where q_j is a prime with j decimal digits as follows: $q_7 = 2424833$,

$$q_{49} = 7455602825647884208337395736200454918783366342657,$$

and $q_{99} = 741640062627530801524787141901937474059940781097519$

$$023905821316144415759504705008092818711693940737.$$

Fermat numbers have an important and rich history, which is intertwined with the very history of factoring itself. Euler was able to factor F_5. In 1880, Landry used an idea attributable to Fermat to factor F_6. As noted above, F_7 was factored by Pollard. Brent and Pollard used a version of Pollard's rho-method to factor F_8 (see [53, pp. 206–208] for a detailed description with examples of the rho-method). As we have shown above, F_9 was factored by the number field sieve. Lenstra's elliptic curve method was used by Brent to factor F_{10} and F_{11}—see [52, pp. 522–524]. Several other Fermat numbers are known to have certain small prime factors, and the smallest Fermat number for which there is no known factor is F_{24}. On March 27, 2010 Michael Vang found the sixth known factor of F_{12}: $17353230210429594579133099699123162989482444520899 \cdot 2^{15} + 1$. On March 26, 2010 David Bessell found the factor of F_{22}: $3853959202444067657533632211 \cdot 2^{24} + 1$. No factor of the 1262612-digit F_{22} was previously known. On February 3, 2010 Tapio Rajala found the factor of F_{14}: $1784180997819127957596374417642156545110881094717 \cdot 2^{16} + 1$. For updates on prime factors of Fermat numbers, see the website:

http://www.prothsearch.net/fermat.html.

Exercises

4.44. Let $n, d \in \mathbb{N}$ and $m = \lfloor n^{1/d} \rfloor$, with $n > 2^{d^2}$. Write n to base m via integers $c_j \in \{0, 1, \ldots, m-1\}$ for $j = 1, 2, \ldots, d$, namely

$$n = \sum_{j=0}^{d} c_j m^j = c_0 + c_1 m + \cdots + c_{d-1} m^{d-1} + c_d m^d.$$

Prove that $c_d = 1$, and $c_{d-1} \le d$. (*The polynomial*

$$f(x) = x^d + c_{d-1} x^{d-1} + \cdots + c_0$$

is the polynomial used in the general number field sieve. See [7].)

4.45. Use the number field sieve to find two prime factors of $2^{153} + 3$.

4.46. Use the number field sieve to find a prime factor of $2^{488} + 1$.

Chapter 5

Ideal Decomposition in Number Fields

At his best, man is the noblest of all animals; separated from law and justice he is the worst.

Aristotle (384–322 B.C.)
Greek philosopher

This chapter builds upon the ideas developed for quadratic fields in Theorem 1.30 on page 49 and the discussion surrounding it. We extend the notions and definitions given in Remark 1.24 on page 52 to arbitrary number fields and link this with the Galois theory developed in §2.1.

5.1 Inertia, Ramification, and Splitting of Prime Ideals

If K/F is an extension of number fields, namely $|K : F| < \infty$, and $|F : \mathbb{Q}| < \infty$, we call K a *relative extension* of F. If $F = \mathbb{Q}$, then K is called an *absolute extension*. Our main interest continues to be the number rings, so we now look at the interplay among the ideals of $\mathfrak{O}_F$ and those of $\mathfrak{O}_K$. We remind the reader of the notation for the class group and discussion surrounding it in Remark 3.7 on page 100. Since $\mathfrak{O}_F \subseteq \mathfrak{O}_K$, we may consider the map

$$\iota_{K/F} : I_{\Delta_F} \mapsto I_{\Delta_K},$$

given by

$$\iota_{K/F} : \mathcal{I} \mapsto \mathcal{I}\mathfrak{O}_K, \tag{5.1}$$

where $\mathcal{I}\mathfrak{O}_K$ is the smallest fractional $\mathfrak{O}_K$-ideal containing $\mathcal{I}$. This consists of all sums $\sum_{j=1}^{n} \alpha_j\beta_j$ with $n \in \mathbb{N}$, $\alpha_j \in \mathcal{I}$, and $\beta_j \in \mathfrak{O}_K$ for $j = 1, 2, \ldots, n$. This is also called the fractional ideal *generated by* $\mathcal{I}$ *in* $\mathfrak{O}_K$. It follows from Theorem 1.17 on page 28, that

$$\mathcal{I}\mathfrak{O}_K = \prod_{j=1}^{r} \mathcal{P}_j^{e_j},$$

where the $\mathcal{P}_j$ are distinct, prime $\mathfrak{O}_K$-ideals, and $e_j \in \mathbb{Z}$ are nonzero, and possibly negative for $j = 1, 2, \ldots, r$. By Exercise 5.1 on page 194,

$$\mathcal{I}\mathfrak{O}_K \cap F = \mathcal{I},$$

and by Exercise 5.2, $\iota_{K/F}$ is a group monomorphism that induces a mapping[5.1]

$$\bar{\iota}_{K/F} : \mathbf{C}_{\mathfrak{O}_\mathbf{F}} \mapsto \mathbf{C}_{\mathfrak{O}_\mathbf{K}}, \tag{5.2}$$

given by

$$\bar{\iota}_{K/F} : \mathbf{I} \mapsto \prod_{j=1}^{r} \mathcal{P}_j^{e_j}.$$

Remark 5.1 We are mainly interested in the case where $\mathcal{I}$ is a prime $\mathfrak{O}_F$-ideal and its decomposition in extension fields, since the prime ideals are the generators of the class group as demonstated in Remark 3.7.

Definition 5.1 — Ramification, Inertia, and Decomposition Numbers
Let K/F be an extension of number fields, and let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal with

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j}, \quad e_j \in \mathbb{N}$$

where the $\mathcal{P}_j$ are distinct, prime $\mathfrak{O}_K$-ideals. We say that the prime $\mathfrak{O}_K$-ideals $\mathcal{P}_j$ *lie over* $\mathfrak{p}$, or are *above* $\mathfrak{p}$. Also, $\mathfrak{p}$ is said to *lie under* the $\mathcal{P}_j$.
The number e_j is called the *ramification index* of $\mathcal{P}_j$ in $\mathfrak{O}_K$, denoted by

$$e_{K/F}(\mathcal{P}_j).$$

Also, $\mathcal{P}_j$ is said to be ramified in $\mathfrak{O}_K$ if $e_{K/F}(\mathcal{P}_j) > 1$, and $\mathfrak{p}$ is also said to be *ramified* in $\mathfrak{O}_K$ as well. Furthermore, $\mathfrak{p}$ is said to be *unramified* in $\mathfrak{O}_K$ provided that $e_{K/F}(\mathcal{P}_j) = 1$ for each $j = 1, 2, \ldots, g$. The number g is called the *decomposition number* of $\mathfrak{p}$ in $\mathfrak{O}_K$, denoted by

$$g_{K/F}(\mathfrak{p}).$$

The degree $|\mathfrak{O}_K/\mathcal{P}_j : \mathfrak{O}_F/\mathfrak{p}|$ is called the *inertial degree*, or *relative degree*, of $\mathcal{P}_j$ in $\mathfrak{O}_K$, denoted by

$$f_{K/F}(\mathcal{P}_j).$$

The fields $\mathfrak{O}_K/\mathcal{P}_j$ and $\mathfrak{O}_F/\mathfrak{p}$ are called the *residue class fields* or simply *residue fields* at $\mathcal{P}_j$ and $\mathfrak{p}$, respectively. Thus, $f_{K/F}(\mathcal{P}_j)$ is the degree of the extension of these finite fields.

A useful fact that we will need in what follows is the next result using the above notions.

Lemma 5.1 Let K/F be an extension of number fields and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal, then there exists exactly one $\mathfrak{O}_F$-ideal $\mathfrak{p}$ lying below $\mathcal{P}$.

Proof. Since $1 \notin \mathcal{P} \cap \mathfrak{O}_F$, then $\mathcal{P} \cap \mathfrak{O}_F$ is an $\mathfrak{O}_F$-ideal with $\mathfrak{O}_F \neq \mathcal{P} \cap \mathfrak{O}_F$, and $\mathcal{P} \cap \mathfrak{O}_F$ is nonzero since $N_{K/F}(\alpha) \in \mathcal{P} \cap \mathfrak{O}_F$ for all $\alpha \in \mathcal{P}$. Also, given that $\mathcal{P} \cap \mathfrak{O}_F \subseteq \mathcal{P}$, then this induces an embedding

$$\psi : \mathfrak{O}_F/(\mathcal{P} \cap \mathfrak{O}_F) \mapsto \mathfrak{O}_K/\mathcal{P},$$

[5.1] The term *induces* here may be interpreted as "gives rise to," which means that the mapping in (5.1) gives rise to the well-defined mapping in (5.2) by moving to quotient groups.

and since $\mathfrak{O}_K/\mathcal{P}$ is a field by Theorems 1.11 on page 18 and 1.26 on page 42, then as a subring embedded in it, $\mathfrak{O}_F/(\mathcal{P}\cap\mathfrak{O}_F)$ must be an integral domain by Theorem 1.9 on page 17, so $\mathcal{P}\cap\mathfrak{O}_F$ is a prime $\mathfrak{O}_F$-ideal. Since

$$\iota_{K/F}(\mathcal{P}\cap\mathfrak{O}_F) = (\mathcal{P}\cap\mathfrak{O}_F)\mathfrak{O}_K \subseteq \mathcal{P}\mathfrak{O}_K\cap\mathfrak{O}_K = \mathcal{P},$$

then $\mathcal{P}$ lies over $\mathcal{P}\cap\mathfrak{O}_F$. If $\mathfrak{p}$ is another prime $\mathfrak{O}_F$-ideal below $\mathcal{P}$, then $\mathfrak{p}\subseteq\mathcal{P}\cap\mathfrak{O}_F$, so $\mathfrak{p}=\mathcal{P}\cap\mathfrak{O}_F$, by Condition B of Definition 1.23 on page 25. □

Example 5.1 Let us consider the ideals in Example 2.14 on page 84. We have the $\mathfrak{O}_K = \mathbb{Z}[\sqrt{10}]$-ideal $(2)\mathbb{Z}[\sqrt{10}] = \mathcal{P}^2$ where $\mathcal{P} = (2,\sqrt{10})$, so the prime ideal (2) in $\mathfrak{O}_F = \mathbb{Z}$ is ramified in $\mathfrak{O}_K$. Since

$$(3)\mathfrak{O}_K = (3, 1+\sqrt{10})(3, 1-\sqrt{10}) = \mathcal{P}\mathcal{P}',$$

then the ramification indices of $\mathcal{P}$ and $\mathcal{P}'$ are 1, so 3 is unramified in $\mathfrak{O}_K$. Its decomposition number is 2. Lastly, $(7)\mathfrak{O}_K = \mathcal{P}$ a prime $\mathfrak{O}_K$-ideal since $|\mathfrak{O}_K/\mathcal{P} : \mathfrak{O}_F/(7)| = 2$, its inertial degree in K.

There is an easier way to determine the relative degrees of primes in extensions via polynomials in certain circumstances by way of Exercise 5.4.

Example 5.2 Let $K = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\alpha)$ and $F = \mathbb{Q}$. Then by Exercise 4.33 on page 173, $\mathfrak{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. For $p = 7$, we have that

$$x^3 - 2 = m_{\alpha,\mathbb{Q}}(x)$$

is irreducible modulo 7. Therefore, $(7)\mathfrak{O}_K = \mathcal{P}$, where $\mathcal{P}$ is an $\mathfrak{O}_K$-prime ideal with $e_{K/F}(\mathcal{P}) = 1 = g_{K/F}(7)$ and $f_{K/F}(\mathcal{P}) = 3$, so 7 is inert in K by Exercise 5.4.
If $p = 29$, then

$$x^3 - 2 \equiv (x+3)(x^2+26x-20) \pmod{29},$$

where $x^2+26x-20$ is irreducible modulo 29 so by Exercise 5.4,

$$(29)\mathfrak{O}_K = \mathcal{P}_1\mathcal{P}_2,$$

where the $f_{K/F}(\mathcal{P}_1) = 1$, and $f_{K/F}(\mathcal{P}_2) = 2$, $e_{K/F}(\mathcal{P}_1) = e_{K/F}(\mathcal{P}_2) = 1$, and $g_{K/F}(29) = 2$. Thus, 29 is unramified in $\mathfrak{O}_K$.
If $p = 31$, then

$$x^3 - 2 \equiv (x-4)(x-7)(x+11) \pmod{31},$$

so by Exercise 5.4,

$$(31)\mathfrak{O}_K = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3,$$

where $e_{K/F}(\mathcal{P}_j) = f_{K/F}(\mathcal{P}_j) = 1$ for $j = 1, 2, 3$, and $g_{K/F}(31) = 3$, so 31 is completely split in $\mathfrak{O}_K$.

Some properties of ramification and inertia are given in the following. In the sequel, a *tower* of number fields $F \subseteq K \subseteq L$ means that F, K, and L are number fields, with L an extension of K, and K an extension of F.

Theorem 5.1 — Transitivity of Ramification and Inertial Degrees
Let $F \subseteq K \subseteq L$ be a tower of number fields, and let $\mathcal{Q}$ be a prime $\mathfrak{O}_L$-ideal above the prime $\mathfrak{O}_K$-ideal $\mathcal{P}$. Then

$$e_{L/K}(\mathcal{Q})e_{K/F}(\mathcal{P}) = e_{L/F}(\mathcal{Q}),$$

and

$$f_{L/K}(\mathcal{Q})f_{K/F}(\mathcal{P}) = f_{L/F}(\mathcal{Q}).$$

Proof. The transitivity of the inertial degrees follows directly from Definition 5.1. To see this, let $\mathfrak{p}$ be the prime $\mathfrak{O}_F$-ideal below $\mathcal{P}$. Then

$$f_{L/K}(\mathcal{Q})f_{K/F}(\mathcal{P}) = |\mathfrak{O}_L/\mathcal{Q} : \mathfrak{O}_K/\mathcal{P}||\mathfrak{O}_K/\mathcal{P} : \mathfrak{O}_F/\mathfrak{p}| =$$

$$|\mathfrak{O}_L/\mathcal{Q} : \mathfrak{O}_F/\mathfrak{p}| = f_{L/F}(\mathcal{Q}).$$

Also, since $\mathfrak{p} \subseteq \mathcal{P} \subseteq \mathcal{Q}$, then

$$e_{L/F}(\mathcal{Q}) = e_{L/K}(\mathcal{Q})e_{K/F}(\mathcal{P}).$$

□

The reader may now recall Theorem 1.30 on page 49, the quadratic case, which we will use in the following illustration—see also Remark 1.24 on page 52.

Example 5.3 Let $L = \mathbb{Q}(\sqrt{-1}, \sqrt{10})$, $K = \mathbb{Q}(\sqrt{10})$, and $F = \mathbb{Q}$. Then by Theorem 1.30, we have for $p = 5$ that

$$p\mathfrak{O}_L = \mathcal{P}_1^2\mathcal{P}_2^2,$$

where $\mathcal{P}_1$ and $\mathcal{P}_2$ are prime $\mathfrak{O}_L$-ideals with $e_{L/K}(\mathcal{P}_1) = e_{L/K}(\mathcal{P}_2) = 1$, and $e_{K/F}(\mathfrak{p}_1) = e_{K/F}(\mathfrak{p}_2) = 2$, where $\mathcal{P}_j \cap \mathfrak{O}_K = \mathfrak{p}_j$ for $j = 1, 2$. Thus,

$$e_{L/F}(\mathcal{P}_j) = e_{L/K}(\mathcal{P}_j)e_{K/F}(\mathfrak{p}_j) = 2.$$

Also, if $p = 3$, then by Theorem 1.30, p is completely split in K and is inert in $\mathbb{Q}(\sqrt{-1})$. Therefore, $3\mathfrak{O}_L = \mathcal{Q}_1\mathcal{Q}_2$, where $\mathcal{Q}_j$ for $j = 1, 2$ are prime $\mathfrak{O}_L$-ideals, and $f_{L/K}(\mathcal{Q}_j) = 2$ for $j = 1, 2$, while $f_{K/F}(\mathfrak{q}_j) = 1$ where $\mathcal{Q}_j \cap \mathfrak{O}_K = \mathfrak{q}_j$. Hence, for $j = 1, 2$,

$$f_{L/F}(\mathcal{Q}_j) = f_{L/K}(\mathcal{Q}_j)f_{K/F}(\mathfrak{q}_j) = 2.$$

We will now develop tools that will allow us to refine our knowledge of the ramification, inertial, and decomposition numbers, especially as we tie them into the theory developed in the preceding chapters. First, we extend the notion of trace and norm.

Definition 5.2 — Relative Norms and Traces of Elements
Let K/F be an extension of number fields with $|K : F| = n$, and let θ_j for $j = 1, 2, \ldots, n$ be all of the F-isomorphisms of K—see Exercise 2.6 on page 63. Let $\alpha \in K$ and set

$$N_{K/F}(\alpha) = \prod_{j=1}^{n} \theta_j(\alpha),$$

called the *relative norm* of α in K/F. Also, set

$$T_{K/F}(\alpha) = \sum_{j=1}^{n} \theta_j(\alpha),$$

called the *relative trace* of α in K/F. Observe that when $F = \mathbb{Q}$, then these notions coincide with those given in Definition 2.4 on page 65, and in this case, we call $N_{K/\mathbb{Q}}$ the *absolute norm* and $T_{K/\mathbb{Q}}$ the *absolute trace.*

Example 5.4 Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$, and $F = \mathbb{Q}(\sqrt{3})$. Then

$$N_{K/F}(5 + \sqrt{-1}) = (5 + \sqrt{-1})(5 - \sqrt{-1}) = 26,$$

and

$$N_{K/\mathbb{Q}}(5 + \sqrt{-1}) = N^2_{K/F}(5 + \sqrt{-1}) = 26^2 = 676.$$

Also,

$$T_{K/F}(5 + \sqrt{-1}) = (5 + \sqrt{-1}) + (5 - \sqrt{-1}) = 10,$$

and

$$T_{K/\mathbb{Q}}(1 + \sqrt{-1}) = 2T_{K/F}(1 + \sqrt{-1}) = 20.$$

Example 5.4 motivates the following, which uses the ideas developed in Exercise 2.6.

Theorem 5.2 — Properties of Relative Norms and Traces
If $F \subseteq K \subseteq L$ is a tower of number fields, then for $\alpha \in L$ the following hold.

(a) $N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha))$, and $N_{L/F}(\alpha) \in F$.

(b) $T_{L/F}(\alpha) = T_{K/F}(T_{L/K}(\alpha))$, and $T_{L/F}(\alpha) \in F$.

(c) If $|L : F(\alpha)| = r$, then

$$N_{L/F}(\alpha) = (N_{F(\alpha)/F}(\alpha))^r, \text{ and } T_{L/F}(\alpha) = r(T_{F(\alpha)/F}(\alpha)).$$

Proof. (a) Let θ_j for $j = 1, 2, \ldots, n = |L : K|$ be all of the K-isomorphisms of L and let ψ_k for $k = 1, 2, \ldots, m = |K : F|$ be all of the F-isomorphisms of K. Then

$$N_{K/F}(N_{L/K}(\alpha)) = \prod_{k=1}^{m} \psi_k(\prod_{j=1}^{n} \theta_j(\alpha)) = \prod_{k=1}^{m}\prod_{j=1}^{n} \psi_k(\theta_j(\alpha)) = N_{L/F}(\alpha),$$

since the $\psi_k\theta_j$ are all distinct and comprise the F-isomorphisms of L. Observe as well that if ψ_1 is the identity embedding of K, then $\theta_j|_K = \psi_1$ for all $j = 1, 2, \ldots, n$, and that ψ_k extends to n embeddings of L into $\mathbb{C}$ for each $k = 1, 2, \ldots, m$.

(b) The property for the trace is proved in a similar fashion to that of (a), employing additivity instead of multiplicativity.

(c) These formulas are proved in the same fashion as that given in the proof of Theorem 2.5 on page 66. □

Example 5.5 Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$, $K = \mathbb{Q}(\sqrt{-1})$, and $F = \mathbb{Q}$. If $\alpha = \sqrt{5} + \sqrt{-1}$, then

$$N_{K/F}(N_{L/K}(\alpha)) = N_{K/F}((\sqrt{5} + \sqrt{-1})(-\sqrt{5} + \sqrt{-1})) = N_{K/F}(-6) = 36 =$$

$$(\sqrt{5} + \sqrt{-1})(-\sqrt{5} + \sqrt{-1})(\sqrt{5} - \sqrt{-1})(-\sqrt{5} - \sqrt{-1}) = N_{L/F}(\alpha).$$

Also,

$$T_{K/F}(T_{L/K}(\alpha)) =$$

$$T_{K/F}((\sqrt{5} + \sqrt{-1}) + (-\sqrt{5} + \sqrt{-1})) = T_{K/F}(2\sqrt{-1}) = 2\sqrt{-1} - 2\sqrt{-1} = 0 =$$

$$(\sqrt{5} + \sqrt{-1}) + (-\sqrt{5} + \sqrt{-1}) + (\sqrt{5} - \sqrt{-1}) + (-\sqrt{5} - \sqrt{-1}) = T_{L/F}(\alpha).$$

If $\beta = 3 + \sqrt{-1}$, then

$$N_{L/F}(\beta) = (N_{K/F}(\beta))^2 = 10^2 = 100,$$

and

$$T_{L/F}(\beta) = 2T_{K/F}(\beta) = 2 \cdot 6 = 12.$$

The following makes use of Lemma 5.1 on page 182 to introduce a new notion.

Definition 5.3 — Relative Norms of Ideals

Let K/F be an extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal above the unique prime $\mathfrak{O}_F$-ideal $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$. Set

$$N^{K/F}(\mathcal{P}) = \mathfrak{p}^{f_{K/F}(\mathcal{P})},$$

and extend to $\mathcal{I} \in I_{\Delta_F}$ via

$$N^{K/F}(\mathcal{I}) = \prod_{j=1}^{n} \mathfrak{p}_j^{a_j f_{K/F}(\mathcal{P}_j)},$$

where

$$\mathcal{I} = \prod_{j=1}^{n} \mathcal{P}_j^{a_j},$$

as a product of distinct prime powers in $\mathfrak{O}_K$ and $\mathcal{P}_j \cap \mathfrak{O}_F = \mathfrak{p}_j$. When $F = \mathbb{Q}$,

$$N^{K/\mathbb{Q}}(\mathcal{I}) = (N(\mathcal{I})),$$

the principal ideal in $\mathbb{Z}$ generated by $N(\mathcal{I})$ as given in Definition 2.8 on page 83. We call $N^{K/\mathbb{Q}}$ the *absolute norm.*

Definition 5.3 tells us, in particular, that $N^{K/F}(\mathcal{I})$ is an $\mathfrak{O}_F$-ideal for any $\mathfrak{O}_K$-ideal $\mathcal{I}$. The reader may develop further properties of the relative norm of ideals by solving Exercises 5.3–5.6.

Example 5.6 Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$, $F = \mathbb{Q}(\sqrt{5})$, and $p = 11$. Then $p\mathfrak{O}_K = \mathcal{P}_1\mathcal{P}_2$, where $\mathcal{P}_j$ for $j = 1, 2$ are distinct prime $\mathfrak{O}_K$-ideals, and $e_{K/F}(\mathcal{P}_j) = 1$, $f_{K/F}(\mathcal{P}_j) = 2$ by Theorem 1.30 on page 49, and Theorem 5.1 on page 184. Hence,

$$N^{K/F}(\mathcal{P}_j) = \mathfrak{p}_j^2, \text{ where } \mathfrak{p}_j = \mathcal{P}_j \cap \mathfrak{O}_F.$$

Also,

$$N^{K/\mathbb{Q}}(\mathcal{P}_j) = (11)^2,$$

since $\mathfrak{p}_j \cap \mathbb{Z} = (11)$.

What is hidden in the development thus far is the relationship between $|K : F|$ and the ramification and inertial degrees.

Theorem 5.3 — Field Degrees, Ramification, and Inertia

Let K/F be an extension of number fields. Suppose that $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal and

$$\mathfrak{p}\mathfrak{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g},$$

where the $\mathcal{P}_j$ are distinct prime $\mathfrak{O}_K$-ideals, and $g = g_{K/F}(\mathfrak{p})$. Then for $e_j = e_{K/F}(\mathcal{P}_j)$, and $f_j = f_{K/F}(\mathcal{P}_j)$,

$$\sum_{j=1}^{g} e_j f_j = |K : F|.$$

Proof. The embedding of $\mathfrak{O}_F$ into $\mathfrak{O}_K$ induces an embedding of the field $\mathfrak{O}_F/\mathfrak{p}$ into the ring $\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K$. We now show that the dimension of the ring as a vector space over the field is indeed $|K:F| = n$, and that this is also the required sum.

Claim 5.1 $|\mathfrak{O}_K/\mathcal{P}_j^{e_j} : \mathfrak{O}_F/\mathfrak{p}| = e_j f_j$.

By Exercise 2.40 on page 82, we have

$$|\mathfrak{O}_K/\mathcal{P}_j^{e_j} : \mathfrak{O}_K/\mathcal{P}_j| = e_j.$$

Therefore,

$$|\mathfrak{O}_K/\mathcal{P}_j^{e_j} : \mathfrak{O}_F/\mathfrak{p}| = |\mathfrak{O}_K/\mathcal{P}_j^{e_j} : \mathfrak{O}_K/\mathcal{P}_j||\mathfrak{O}_K/\mathcal{P}_j : \mathfrak{O}_F/\mathfrak{p}| = e_j f_j,$$

which establishes Claim 5.1.

By Claim 5.1 and Exercise 2.40,

$$|\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K : \mathfrak{O}_F/\mathfrak{p}\mathfrak{O}_F| = \sum_{j=1}^{g} e_j f_j. \tag{5.3}$$

It remains to show that this dimension is also n. First, we show that it is at most n. We do this by demonstrating that any $n+1$ elements of $\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K$ are linearly dependent over $\mathfrak{O}_F/\mathfrak{p}\mathfrak{O}_F$. Let α_j for $j = 1, 2, \ldots, n+1$ be elements of $\mathfrak{O}_K$ and let $\overline{\alpha}_j$ be the corresponding elements of $\mathfrak{O}_F/\mathfrak{p}\mathfrak{O}_F$. Since the α_j are linearly dependent over F, then they are linearly dependent over $\mathfrak{O}_F$ by Lemma 1.4 on page 38. Therefore, there exist $\beta_j \in \mathfrak{O}_F$ not all zero such that

$$\sum_{j=1}^{n+1} \beta_j \alpha_j = 0. \tag{5.4}$$

Claim 5.2 There exists a $\gamma \in F - \mathfrak{O}_F$ with $\gamma(\beta_1, \ldots, \beta_{n+1}) \subseteq \mathfrak{O}_F$, but $\gamma(\beta_1, \ldots, \beta_{n+1}) \not\subseteq \mathfrak{p}$.

By Exercise 1.38 on page 33, there is a non-zero $\mathfrak{O}_F$-ideal I such that $I(\beta_1, \ldots, \beta_{n+1}) = (\alpha)$ for some $\alpha \in \mathfrak{O}_F$. Thus, $I(\beta_1, \ldots, \beta_{n+1}) \not\subseteq \alpha\mathfrak{p}$, since otherwise $\alpha \in \alpha\mathfrak{p}$ implies $1 \in \mathfrak{p}$. Let $\beta \in I$ such that $\beta(\beta_1, \ldots, \beta_{n+1}) \not\subseteq \mathfrak{p}$. Then by setting $\gamma = \beta/\alpha$, we get the claim.

By Claim 5.2, reducing (5.4) modulo $\mathfrak{p}$ yields a nontrivial relation among the α_j. In other words, not all $\beta_j$are zero modulo $\mathfrak{p}$, so the α_j are linearly dependent over $\mathfrak{O}_F/\mathfrak{p}\mathfrak{O}_F$. Hence, we have shown that

$$|\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K : \mathfrak{O}_F/\mathfrak{p}\mathfrak{O}_F| \le n.$$

We conclude by establishing the full equality.

Let $\mathfrak{p} \cap \mathbb{Z} = (p)$, and let $\mathfrak{p}_k$ for $k = 1, 2, \ldots, g_{F/\mathbb{Q}}(p) = g_1$ be all of the prime $\mathfrak{O}_F$-ideals above p. Now we show that $n = n_k = |\mathfrak{O}_K/\mathfrak{p}_k\mathfrak{O}_K : \mathfrak{O}_F/\mathfrak{p}_k|$ for each $k = 1, 2, \ldots, g_1$.

Claim 5.3 $\sum_{j=1}^{g_1} e_{F/\mathbb{Q}}(\mathfrak{p}_j) f_{F/\mathbb{Q}}(\mathfrak{p}_j) = |F:\mathbb{Q}|$.

We have

$$N^{F/\mathbb{Q}}(\mathfrak{p}\mathfrak{O}_F) = \prod_{j=1}^{g_1} (p)^{e_{F/\mathbb{Q}}(\mathfrak{p}_j) f_{F/\mathbb{Q}}(\mathfrak{p}_j)} = (p)^{\sum_{j=1}^{g_1} e_{F/\mathbb{Q}}(\mathfrak{p}_j) f_{F/\mathbb{Q}}(\mathfrak{p}_j)},$$

and by Corollary 2.8 on page 85, this equals

$$|\mathfrak{O}_F/(p)| = (N_F(p)) = (p)^{|F:\mathbb{Q}|}.$$

Since $N^{F/\mathbb{Q}}(\mathfrak{p}\mathfrak{O}_F) = N(\mathfrak{p}) = (|\mathfrak{O}_F : (p)|) = (N_F(p))$ by Definition 5.3 on page 186, this establishes Claim 5.3.

Therefore, since $p\mathfrak{O}_F = \prod_{k=1}^{g_1} \mathfrak{p}_k^{e_{F/\mathbb{Q}}(\mathfrak{p}_k)}$, then using (5.3),

$$N^{K/\mathbb{Q}}(p\mathfrak{O}_K) = \prod_{k=1}^{g_1}(N^{K/\mathbb{Q}}(\mathfrak{p}_k\mathfrak{O}_K))^{e_{F/\mathbb{Q}}(\mathfrak{p}_k)} = \prod_{k=1}^{g_1} N^{F/\mathbb{Q}}(\mathfrak{p}_k)^{n_k e_{F/\mathbb{Q}}(\mathfrak{p}_k)} =$$

$$\prod_{k=1}^{g_1}(p)^{n_k e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k)} = (p)^{\sum_{k=1}^{g_1} n_k e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k)},$$

by Claim 5.1 and Exercise 5.6 on page 195. However, by the same reasoning as in Claim 5.3,

$$N^{K/\mathbb{Q}}(p\mathfrak{O}_K) = (p)^{\sum_{j=1}^{g} e_{K/\mathbb{Q}}(\mathcal{P}_j) f_{K/\mathbb{Q}}(\mathcal{P}_j)} = (p)^{|K:\mathbb{Q}|}.$$

Therefore,

$$|K:\mathbb{Q}| = \sum_{k=1}^{g_1} n_k e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k),$$

so

$$n|F:\mathbb{Q}| = n\sum_{k=1}^{g_1} e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k) = \sum_{k=1}^{g_1} n e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k) \geq$$

$$\sum_{k=1}^{g} n_k e_{F/\mathbb{Q}}(\mathfrak{p}_k) f_{F/\mathbb{Q}}(\mathfrak{p}_k) = |K:\mathbb{Q}| = n|F:\mathbb{Q}|.$$

Thus, $n_k = n$ for each $k = 1, \ldots, g_1$. In particular, for $\mathfrak{p}_k = \mathfrak{p}$, the equality holds. This completes the proof. □

In view of Theorem 5.3, we may extend the notions given in Definition 5.1 as follows.

Definition 5.4 — Inert, Completely Split, and Totally Ramified

Let K/F be an extension of number fields, and let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal with

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j}, \quad e_j \in \mathbb{N}$$

where the $\mathcal{P}_j$ are distinct, prime $\mathfrak{O}_K$-ideals. Then $\mathfrak{p}$ is said to be *completely ramified*, or *totally ramified* in $\mathfrak{O}_K$ whenever

$$e_j = e_{K/F}(\mathcal{P}_j) = |K:F| \text{ for some } j = 1, 2, \ldots, g,$$

so $f_{K/F}(\mathcal{P}_j) = 1 = g_{K/F}(\mathcal{P}_j)$. $\mathfrak{p}$ is said to *split completely*, or to be *completely split* in $\mathfrak{O}_K$ if

$$g = g_{K/F}(\mathfrak{p}) = |K:F|,$$

so $e_{K/F}(\mathcal{P}_j) = 1 = f_{K/F}(\mathcal{P}_j)$. If $f_{K/F}(\mathcal{P}_j) = |K:F|$ for $j = 1, 2, \ldots, g$, then $\mathfrak{p}$ is said to be *inert*[5.2] in $\mathfrak{O}_K$, so $e_{K/F}(\mathcal{P}_j) = 1 = g_{K/F}(\mathcal{P}_j)$.

[5.2] It is a common and accepted abuse of language in the literature to say that $\mathfrak{p}$ ramifies, splits or is inert in K, rather than $\mathfrak{O}_K$.

Example 5.7 Consider the situation given in Example 5.2 on page 183. For $p = 29$,

$$(29)\mathfrak{O}_K = (29)\mathbb{Z}[\sqrt[3]{2}] = \mathcal{P}_1\mathcal{P}_2,$$

for prime $\mathfrak{O}_K$-ideals $\mathcal{P}_1$, and $\mathcal{P}_2$, where $e_{K/\mathbb{Q}}(\mathcal{P}_j) = 1$ for $j = 1, 2$, $f_{K/\mathbb{Q}}(\mathcal{P}_1) = 1$, $f_{K/\mathbb{Q}}(\mathcal{P}_2) = 2$, and $g(29) = 2$. Thus,

$$|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = |K : F| = \sum_{j=1}^{g} e_j f_j = 1 \cdot 1 + 1 \cdot 2 = 3.$$

The reader is reminded of the definition of normal extension given in Exercise 2.2 on page 62. For such extensions, Theorem 5.3 on page 186 is given as follows.

Theorem 5.4 — Normal Extensions, Ramification, and Inertia
Let K/F be a normal extension of number fields, and let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal with

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j},$$

where $g = g_{K/F}(\mathfrak{p})$ and $e_j = e_{K/F}(\mathcal{P}_j)$. Then

$$e_{K/F}(\mathcal{P}_j) = e_{K/F}(\mathcal{P}_k) = e_{K/F}(\mathfrak{p}), \text{ and } f_{K/F}(\mathcal{P}_j) = f_{K/F}(\mathcal{P}_k) = f_{K/F}(\mathfrak{p})$$

for all $j, k \in \{1, 2, \ldots, g\}$. Thus,

$$e_{K/F}(\mathfrak{p}) f_{K/F}(\mathfrak{p}) g_{K/F}(\mathfrak{p}) = n = |K : F|.$$

Proof. The last assertion will follow as an immediate consequence of the initial results via Theorem 5.3.

If we can show that for each $\mathcal{P}_j$ and $\mathcal{P}_k$ for any $j, k \in \{1, 2, \ldots, g\}$, there exists an F-isomorphism θ of K such that $\theta(\mathcal{P}_j) = \mathcal{P}_k$,[5.3] then the initial assertions follow. To see this, suppose that $\theta(\mathcal{P}_1) = \mathcal{P}_k$. Then

$$\mathfrak{p}\mathfrak{O}_K = \theta(\mathfrak{p}\mathfrak{O}_K) = \prod_{j=1}^{g} \theta(\mathcal{P}_j)^{e_j},$$

then $e_1 = e_k$ by uniqueness of factorization of ideals. Also,

$$f_k = |\mathfrak{O}_K/\mathcal{P}_k : \mathfrak{O}_F/\mathfrak{p}| = |\mathfrak{O}_K/\theta(\mathcal{P}_1) : \mathfrak{O}_F/\mathfrak{p}| = |\mathfrak{O}_K/\mathcal{P}_1 : \mathfrak{O}_F/\mathfrak{p}| = f_1.$$

Hence, it remains to show that the $\mathcal{P}_j$ are conjugates over F.

Let θ be any F-isomorphism of K. Since $\mathcal{P}_1^{h_K} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$, then $\alpha \in \mathcal{P}_1$ since $\mathcal{P}_1$ is prime. Since

$$N_{K/F}(\alpha) = \prod_{j=1}^{n} \theta_j(\alpha) \in \mathcal{P}_1,$$

where θ_j for $j = 1, 2, \ldots, n$ are all of the F-isomorphisms of K, then

$$N_{K/F}(\alpha)\mathfrak{O}_K \subseteq \mathfrak{p}\mathfrak{O}_K,$$

[5.3] When this occurs, we say that the $\mathcal{P}_j$ are *conjugates over* F. The reader may easily verify that $\theta(\mathcal{P}_j)$ is a prime $\mathfrak{O}_K$-ideal, so $\theta(\mathcal{P}_j)\cap\mathfrak{O}_F=\mathfrak{p}$ forcing $\theta(\mathcal{P}_j)=\mathcal{P}_k$ for some $k\in\mathbb{N}$—see Exercise 2.40 on page 82.

so $\mathfrak{p}\mathfrak{O}_K \mid N_{K/F}(\alpha)\mathfrak{O}_K$, which in turn implies that $\mathcal{P}_k \mid (N_{K/F}(\alpha))$ for all $k \in \{1, 2, \ldots, n\}$. Thus, for some $\ell \in \{1, 2, \ldots, n\}$, $\theta_\ell(\alpha) \in \mathcal{P}_k$. Therefore,

$$\theta_\ell(\mathcal{P}_1)^{h_K} = \theta_\ell(\alpha)\mathfrak{O}_K \subseteq \mathcal{P}_k,$$

from which it follows that $\theta_\ell(\mathcal{P}_1) = \mathcal{P}_k$ since both $\mathcal{P}_1$ and $\mathcal{P}_k$ are primes. Hence, the $\mathcal{P}_j$ are all conjugates over F. □

The action of the F-isomorphisms of K on the prime $\mathfrak{O}_K$-ideals established in the above proof has a name. We also say that the F-isomorphisms of K *transitively permute* the $\mathcal{P}_j$, or *act transitively* on them. Thus, we have the following immediate consequence.

Corollary 5.1 If K/F is a normal extension of number fields, then the F-isomorphisms of K transitively permute the prime $\mathfrak{O}_K$-ideals above a fixed prime ideal $\mathfrak{p}$ in $\mathfrak{O}_F$.

Example 5.8 Let $p^k > 2$ where p is a rational prime and $k \in \mathbb{N}$. Set $K = \mathbb{Q}(\zeta_{p^k})$ and let $\lambda = 1 - \zeta_{p^k}$. Then $(\lambda) = \lambda\mathfrak{O}_K$ is a principal $\mathfrak{O}_K$-ideal, and is prime since

$$N^{K/\mathbb{Q}}(\lambda\mathfrak{O}_K) = (p),$$

by Corollary 2.8 on page 85 and Exercise 3.35 on page 129. Furthermore, since $p = \mathbf{\Phi}_{p^k}(1) = \prod_j (1 - \zeta_{p^k}^j)$, where the product ranges over all natural numbers $j < p^k$ relatively prime to p, and by Exercise 3.35, we get $p = u\lambda^{\phi(p^k)}$ where $u \in \mathfrak{O}_K$ is a unit. Thus,

$$p\mathfrak{O}_K = (\lambda\mathfrak{O}_K)^{\phi(p^k)},$$

so since $K/\mathbb{Q}$ is normal, we get

$$e_{K/\mathbb{Q}}(p) = \phi(p^k) = |K : \mathbb{Q}|, \text{ and } f_{K/\mathbb{Q}}(p) = 1 = g_{K/\mathbb{Q}}(p).$$

We give an interpretation of the relative norm of an ideal that is similar to the relative norm of an element. We will employ the Galois theory developed in §2.1.

Theorem 5.5 — Ideal Norms as Conjugates

Let K/F be an extension of number fields, and let L be the minimal normal extension of F containing K. Set $H = \text{Gal}(L/F)/\text{Gal}(L/K)$.[5.4] Then for $\mathcal{I} \in I_{\Delta_F}$,

$$N^{K/F}(\mathcal{I})\mathfrak{O}_L = \prod_{\theta \in H} \theta(\mathcal{I}\mathfrak{O}_L).$$

In particular, if K/F is a normal extension, then

$$N^{K/F}(\mathcal{I})\mathfrak{O}_K = \prod_{\theta \in \text{Gal}(K/F)} \theta(\mathcal{I}).$$

Proof. By Exercise 5.3 on page 194, it suffices to prove the result for $\mathcal{I} = \mathcal{P}$, a prime $\mathfrak{O}_K$-ideal. Let $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$. First we prove the result for K/F a normal extension, namely $K = L$. By Theorem 5.4 on the preceding page,

$$\mathfrak{p}\mathfrak{O}_K = (\mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_g)^{ef},$$

[5.4] The reader is cautioned that the set H is not, in general, a group.

where $\mathcal{P} = \mathcal{P}_1$, $e = e_{K/F}(\mathfrak{p})$, $f = f_{K/F}(\mathfrak{p})$, and $g = g_{K/F}(\mathfrak{p})$. Since the F-isomorphisms of K transitively permute the $\mathcal{P}_j$, for $j = 1, 2, \ldots, g$, and since

$$efg = n = |K : F|,$$

then for each such j there are ef of these isomorphisms that send $\mathcal{P}_1$ to $\mathcal{P}_j$. Therefore,

$$\prod_{\theta \in H} \theta(\mathcal{P}) = \prod_{\theta \in \mathrm{Gal}(K/F)} \theta(\mathcal{P}) = \prod_{j=1}^{g} \mathcal{P}_j^{ef} = (\mathfrak{p}\mathfrak{O}_K)^f = N^{K/F}(\mathcal{P})\mathfrak{O}_K.$$

This completes the proof for the case where $K = L$.
In the general case, if $\theta_1\theta_2^{-1} \in H$, then $\theta_1(\mathcal{P}\mathfrak{O}_L) = \theta_2(\mathcal{P}\mathfrak{O}_L)$. Therefore,

$$\left(\prod_{\theta \in H} \theta(\mathcal{P}\mathfrak{O}_L)\right)^{|L:K|} = \prod_{\theta \in \mathrm{Gal}(L/F)} \theta(\mathcal{P}\mathfrak{O}_L) = N^{L/F}(\mathcal{P}\mathfrak{O}_L)\mathfrak{O}_L,$$

by the above case, and by Exercises 5.6–5.7, this equals,

$$N^{K/F}(N^{L/K}(\mathcal{P}\mathfrak{O}_L))\mathfrak{O}_L = N^{K/F}(\mathcal{P})^{|L:K|}\mathfrak{O}_L = \left(N^{K/F}(\mathcal{P})\mathfrak{O}_L\right)^{|L:K|},$$

and the desired result follows. □

Corollary 5.2 Assuming the hypothesis of Theorem 5.5, let $\mathcal{I} = (\alpha) \in P_{\Delta_K}$. Then $N^{K/F}(\mathcal{I}) \in P_{\Delta_F}$ is the principal fractional $\mathfrak{O}_F$-ideal generated by $N_{K/F}(\alpha)$.

Proof. From Theorem 5.5, we get

$$N^{K/F}(\mathcal{I})\mathfrak{O}_L = \prod_{\theta \in H} \theta(\mathcal{I}\mathfrak{O}_L) = \prod_{\theta \in H} \theta(\alpha\mathfrak{O}_L) = N_{L/K}(\alpha)\mathfrak{O}_L.$$

Therefore, by Exercise 5.1,

$$N^{K/F}(\mathcal{I}) = N^{K/F}(\mathcal{I})\mathfrak{O}_L \cap K = N_{K/F}(\alpha)\mathfrak{O}_L \cap K = N_{K/F}(\alpha)\mathfrak{O}_K,$$

which is the required result. □

Example 5.9 Let $K = \mathbb{Q}(\sqrt[3]{2})$, which is not normal over $\mathbb{Q}$ as observed above. However, $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is normal over $\mathbb{Q}$, where ζ_3 is a primitive cube root of unity. In fact, it is the minimal normal extension of $\mathbb{Q}$ containing K. The embeddings of L into $\mathbb{C}$ are $\{1, \theta_1, \theta_2, \theta_1^2, \theta_1\theta_2, \theta_1^2\theta_2\}$ where:

$$\theta_1 : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}, \text{ and } \theta_1 : \zeta_3 \mapsto \zeta_3,$$

$$\theta_2 : \zeta_3 \mapsto \zeta_3^{-1}, \text{ and } \theta_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}.$$

As shown in Example 5.7 on page 189, we have the $\mathfrak{O}_K$-ideal

$$(29)\mathfrak{O}_K = \mathcal{P}_1\mathcal{P}_2,$$

with $f_{K/\mathbb{Q}}(\mathcal{P}_1) = 1 = e_{K/\mathbb{Q}}(\mathcal{P}_j)$ for $j = 1, 2$, and $f_{K/\mathbb{Q}}(\mathcal{P}_2) = 2$. Also, 29 is inert in $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ by Theorem 1.30 on page 49. Therefore, by Theorem 5.1 on page 184,

$$(29)\mathfrak{O}_L = \mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3,$$

where the $\mathcal{Q}_j$ for $j = 1, 2, 3$ are $\mathfrak{O}_L$-ideals with

$$f_{L/K}(\mathcal{Q}_1) = 2, \text{ and } f_{L/K}(\mathcal{Q}_j) = e_{L/K}(\mathcal{Q}_j) = 1, \text{ for } j = 2, 3.$$

Also, here

$$H = \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/K) = \langle\overline{\theta}_1\rangle = \{1, \overline{\theta}_1, \overline{\theta}_1^2\},$$

where $\overline{\theta}_1$ is the image of θ_1 under the natural map that takes $\mathrm{Gal}(L/\mathbb{Q})$ to the set H. Thus, again by Theorem 5.1,

$$\overline{\theta}_1(\mathcal{Q}_1) = \mathcal{Q}_1, \overline{\theta}_1(\mathcal{Q}_2) = \mathcal{Q}_3, \text{ and } \overline{\theta}_1(\mathcal{Q}_3) = \mathcal{Q}_2.$$

Hence,

$$N^{K/\mathbb{Q}}((29)\mathfrak{O}_K)\mathfrak{O}_L = N^{K/\mathbb{Q}}(\mathcal{P}_1\mathcal{P}_2)\mathfrak{O}_L = \prod_{j=1}^{3}\overline{\theta}_1^j(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3) = \mathcal{Q}_1^3\mathcal{Q}_2^3\mathcal{Q}_3^3.$$

Notice that by Definition 5.3 on page 186,

$$N^{K/\mathbb{Q}}((29)\mathfrak{O}_K) = N^{K/\mathbb{Q}}(\mathcal{P}_1\mathcal{P}_2) = N^{K/\mathbb{Q}}(\mathcal{P}_1)N^{K/\mathbb{Q}}(\mathcal{P}_2) =$$

$$(29)^{f_{K/\mathbb{Q}}(\mathcal{P}_1)}(29)^{f_{K/\mathbb{Q}}(\mathcal{P}_2)} = (29) \cdot (29)^2 = (29)^3,$$

which coincides with the new characterization of relative norms for ideals, since

$$N^{K/\mathbb{Q}}((29)\mathfrak{O}_K)\mathfrak{O}_L = 29^3\mathfrak{O}_L = (\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3)^3.$$

If we consider the norm from L, then as in the proof of Theorem 5.5, we get,

$$N^{L/\mathbb{Q}}((29)\mathfrak{O}_L)\mathfrak{O}_L = \prod_{\theta\in\mathrm{Gal}(L/\mathbb{Q})}\theta(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3) =$$

$$\left(\prod_{\theta\in H}\theta(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3)\right)^2 = (\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3)^6.$$

Observe that, since $L/\mathbb{Q}$ is normal, then $e_{L/\mathbb{Q}}(29) = 1$, $f_{L/\mathbb{Q}}(29) = 2$, and $g_{L/\mathbb{Q}}(29) = 3$. Again, by our original Definition 5.3 on page 186, we get

$$N^{L/\mathbb{Q}}(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3) = \prod_{j=1}^{3}N^{L/\mathbb{Q}}(\mathcal{Q}_j) = \prod_{j=1}^{3}(29)^2 = (29)^6,$$

so we achieve, as above, that

$$N^{L/\mathbb{Q}}((29)\mathfrak{O}_L)\mathfrak{O}_L = 29^6\mathfrak{O}_L = (\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3)^6.$$

Yet another way to see this is to use Exercise 5.6 on page 195 and Definition 5.3 to get,

$$N^{L/\mathbb{Q}}(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3) = N^{K/\mathbb{Q}}(N^{L/K}(\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3)) = N^{K/\mathbb{Q}}\left(\prod_{j=1}^{3}N^{L/K}(\mathcal{Q}_j)\right) =$$

$$N^{K/\mathbb{Q}}\left(\mathcal{P}_1^{f_{L/K}(\mathcal{Q}_1)}\mathcal{P}_2^{f_{L/K}(\mathcal{Q}_2)}\mathcal{P}_2^{f_{L/K}(\mathcal{Q}_3)}\right) = N^{K/\mathbb{Q}}(\mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_2) = N^{K/\mathbb{Q}}(\mathcal{P}_1^2\mathcal{P}_2^2) =$$

$$(29)^{2f_{K/\mathbb{Q}}(\mathcal{P}_1)}(29)^{2f_{K/\mathbb{Q}}(\mathcal{P}_2)} = (29)^{2\cdot 1}(29)^{2\cdot 2} = (29)^6.$$

All of the above methods are instructive, but the easiest is to look at Corollary 5.2, from which we get that $N^{K/\mathbb{Q}}((29)\mathfrak{O}_K)$, respectively, $N^{L/\mathbb{Q}}((29)\mathfrak{O}_L)$, is the principal $\mathbb{Z}$-ideal generated by $N_{K/\mathbb{Q}}(29) = 29^3$, respectively, $N_{L/\mathbb{Q}}(29) = 29^6$.

Corollary 5.2 allows us to achieve yet another characterization for the norm of ideals.

Theorem 5.6 — Norms of Ideals Generated by Norms of Elements
Let K/F be an extension of number fields. If $\mathfrak{I} \in I_{\Delta_K}$, then $N^{K/F}(\mathfrak{I})$ is the smallest ideal of I_{Δ_F} which contains all norms $N_{K/F}(\alpha)$ where α ranges over all elements of $\mathfrak{I}$.

Proof. By Corollary 5.2, $N_{K/F}(\alpha) \in N^{K/F}(\mathfrak{I})$ for all $\alpha \in \mathfrak{I}$. It remains to show that the $N_{K/F}(\alpha)$ generate $N^{K/F}(\mathfrak{I})$. First, we assume that $\mathfrak{I}$ is an integral $\mathfrak{O}_K$-ideal.

Claim 5.4 There exist $\alpha,\beta \in \mathfrak{I}$ with $(\alpha) + (\beta) = \mathfrak{I}$.

Suppose that H is an $\mathfrak{O}_K$-ideal relatively prime to $\mathfrak{I} = \prod_{j=1}^{n} \mathfrak{p}_j^{a_j}$, and let

$$\alpha_j \in \mathfrak{p}_j^{a_j} - \mathfrak{p}_j^{a_j+1}.$$

Also, by Exercise 1.38 on page 33, there is an $\mathfrak{O}_K$-ideal I_1 such that $\alpha\mathfrak{O}_K = \mathfrak{I}I_1$ for some $\alpha \in \mathfrak{O}_K$. Then by Theorem 1.21 on page 32, there is a solution $y = \beta$ to the system of congruences

$$y \equiv \alpha_j \pmod{\mathfrak{p}_j^{a_j+1}} \text{ for } j = 1, 2, \dots, n,$$
$$\text{and } y \equiv 1 \pmod{I_1 H}.$$

Therefore, $\beta \in \mathfrak{I}$ and we may set $\beta\mathfrak{O}_K = \mathfrak{I}I_2$ where I_2 is an $\mathfrak{O}_K$-ideal with

$$I_2 + I_1 H\mathfrak{I} = \mathfrak{O}_K \subseteq I_2 + I_1,$$

so $I_1 + I_2 = \mathfrak{O}_K$. Hence,

$$\alpha\mathfrak{O}_K + \beta\mathfrak{O}_K = \mathfrak{I}I_1 + \mathfrak{I}I_2 = \mathfrak{I}(I_1 + I_2) = \mathfrak{I},$$

which secures the claim.

By Claim 5.4, $N^{K/F}(I_1)$ and $N^{K/F}(I_2)$ must be relatively prime since I_1 and I_2 are relatively prime implying that $N^{K/F}(I_1)\mathfrak{O}_K$ and $N^{K/F}(I_2)\mathfrak{O}_K$ are relatively prime. Also,

$$N^{K/F}(\alpha\mathfrak{O}_K) = N^{K/F}(\mathfrak{I})N^{K/F}(I_1),$$

and

$$N^{K/F}(\beta\mathfrak{O}_K) = N^{K/F}(\mathfrak{I})N^{K/F}(I_2).$$

Thus, $N^{K/F}(I_1) = N^{K/F}(\alpha\mathfrak{I}^{-1}\mathfrak{O}_K)$ and $N^{K/F}(I_2) = N^{K/F}(\beta\mathfrak{I}^{-1}\mathfrak{O}_K)$ are relatively prime. Hence,

$$N^{K/F}(\alpha\mathfrak{O}_K) + N^{K/F}(\beta\mathfrak{O}_K) = N^{K/F}(\mathfrak{I})(N^{K/F}(I_1) + N^{K/F}(I_2)) = N^{K/F}(\mathfrak{I}),$$

and this completes the proof for the integral case.

If $\mathfrak{I}$ is any fractional $\mathfrak{O}_K$-ideal, then $\mathfrak{I} = \gamma^{-1}J$ for some $\gamma \in \mathfrak{O}_K$ and some integral $\mathfrak{O}_K$-ideal J by Remark 1.13 on page 26. However,

$$N_{K/F}(\gamma)\gamma^{-1} = \delta \in \mathfrak{O}_K,$$

since $\gamma \mid N_{K/F}(\gamma)$. Thus,

$$\mathfrak{I} = \delta J(\delta\gamma)^{-1}\mathfrak{O}_K = H\sigma^{-1},$$

where $H = \delta J\mathfrak{O}_K$ is an integral $\mathfrak{O}_K$-ideal and

$$\sigma = \delta\gamma = N_{K/F}(\gamma) \in \mathfrak{O}_F.$$

By Exercise 5.3 and the proof for the integral case, the fractional ideal generated by all of the elements $N_{K/F}(\alpha)$ for $\alpha \in \mathfrak{I}$ is

$$\sigma^{-|K:F|}N^{K/F}(H) = N^{K/F}(\sigma^{-1}H) = N^{K/F}(\mathfrak{I}),$$

as required. □

Example 5.10 In Example 5.8, with $K = \mathbb{Q}(\zeta_{p^k})$ and $F = \mathbb{Q}$, we have the principal prime $\mathfrak{O}_K$-ideal $\lambda\mathfrak{O}_K = (\lambda)$, and

$$N^{K/F}(\lambda\mathfrak{O}_K) = (p) = (N_{K/F}(\lambda)).$$

Example 5.11 In Example 5.9, $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$, and

$$N^{K/\mathbb{Q}}((29)\mathfrak{O}_K) = (29)^3 = (N_{K/\mathbb{Q}}(29)).$$

In the next section, we will look at another ideal-theoretic concept called the *different*, which will allow us to say much more about prime decomposition in number fields, especially cyclotomic and pure extensions such as those illustrations given in our closing examples for this section.

Exercises

5.1. Let K/F be an extension of number fields, and let $\mathfrak{I} \in I_{\Delta_K}$. Prove that

$$\mathfrak{I}\mathfrak{O}_K \cap F = \mathfrak{I}.$$

Also, show that if $\mathfrak{I}, \mathfrak{J} \in I_{\Delta_F}$ with $I\mathfrak{O}_K = J\mathfrak{O}_K$, then $\mathfrak{I} = \mathfrak{J}$.

(*Hint: Use Exercises 3.31–3.32 on page 121.*)

5.2. Prove that the mapping $\iota_{K/F}$ given in (5.1) is a group monomorphism that induces the map given in (5.2).

(*Hint: Use Exercise 5.1.*)

5.3. Let K/F be an extension of number fields, and let $\mathfrak{I}, \mathfrak{J} \in I_{\Delta_F}$. Prove that

$$N^{K/F}(\mathfrak{I})N^{K/F}(\mathfrak{J}) = N^{K/F}(\mathfrak{I}\mathfrak{J}).$$

5.4. Let K/F be an extension of number fields and assume that $\mathfrak{O}_K = \mathfrak{O}_F[\alpha]$ for some $\alpha \in \mathfrak{O}_K$. Let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal, and let $\overline{m}_{\alpha,F}(x)$ be the polynomial determined from the minimal polynomial $m_{\alpha,F}(x)$ by reducing its coefficients modulo $\mathfrak{p}$. Suppose further that

$$\overline{m}_{\alpha,F}(x) = \prod_{j=1}^{g} g_j(x)^{e_j}, \quad e_j \in \mathbb{N}$$

where the $g_j(x)$ are distinct irreducible polynomials over the field $\mathfrak{O}_F/\mathfrak{p} = \overline{\mathfrak{O}_F}$. Prove that

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j},$$

where the $\mathcal{P}_j$ are distinct prime $\mathfrak{O}_K$-ideals such that $f_{K/F}(\mathcal{P}_j) = \deg_{\overline{\mathfrak{O}_F}}(g_j)$. Furthermore, show that for each $j = 1, 2, \ldots, g$,

$$\mathcal{P}_j = \mathfrak{p}\mathfrak{O}_K + g_j(\alpha)\mathfrak{O}_K.$$

(*Hint: Use Theorem A.5 on page 328 and Theorem 1.21 on page 32.*)

(*This phenomenon does not always occur, as shown by Example 2.13 on page 79. In other words, $\mathfrak{O}_K$ need not necessarily be of the form $\mathfrak{O}_K = \mathfrak{O}_F[\alpha]$.*)

5.5. Let I and J be nonzero ideals in a Dedekind domain R with quotient field F. Prove that if $I \neq R$, there exists a $\gamma \in F$ such that $\gamma J \subseteq R$, but $\gamma J \not\subseteq I$.

(*Hint: Use Exercise 1.38 on page 33.*)

5.6. Let $F \subseteq K \subseteq L$ be a tower of number fields. Prove that if $\mathcal{I} \in I_{\Delta_L}$, then

$$N^{L/F}(\mathcal{I}) = N^{K/F}(N^{L/K}(\mathcal{I})).$$

5.7. Let K/F be an extension of number fields, and let $\mathcal{I} \in I_{\Delta_F}$. Prove that

$$N^{K/F}(\mathcal{I}) = \mathcal{I}^n,$$

where $n = |K : F|$.

(*Hint: Use Exercise 5.3 and Theorem 5.3 on page 186.*)

5.8. Let K/F be an extension of number fields. Show that there exists a number field L that is a normal extension of F containing K.

(*Hint: Use Theorem 1.24 on page 39.*)

5.9. Let $f(x) \in \mathbb{Z}[x]$ be nonconstant. Prove that there exist infinitely many rational primes p such that $f(x) \equiv 0 \pmod{p}$, for some $x \in \mathbb{Z}$.

(*Hint: Use Theorem A.7 on page 330.*)

5.10. Let K/F be an extension of number fields. Prove that there are infinitely many prime $\mathfrak{O}_F$-ideals that are completely split in $\mathfrak{O}_K$.

(*Hint: Use Theorem 1.24 on page 39.*)

5.11. Prove that there are no inert primes in $\mathbb{Q}(\zeta_{2^n})$ for any $n \in \mathbb{N}$ with $n > 2$.

(*Hint: Use Exercise 5.4 and Theorem 1.30 on page 49*)

5.2 The Different and Discriminant

> *Nothing is so strong as gentleness and nothing is so gentle as real strength.*
>
> **Ralph W. Sockman (1889–1970)**
>
> Senior pastor of the United Methodist Christ Church in New York City

In this section we will develop tools that will allow us to generalize the notion of the discriminant of a number field, and prove more powerful results than those achieved thus far. First, we need the following.

Definition 5.5 — The Dual/Codifferent
Let K/F be an extension of number fields, and let $\mathfrak{I} \in I_{\Delta_F}$. Then

$$\mathfrak{I}^* = \{\beta \in K : T_{K/F}(\beta\mathfrak{I}) \subseteq \mathfrak{O}_F\}$$

is called the *dual* or *codifferent* of $\mathfrak{I}$ over F, where $T_{K/F}(\beta\mathfrak{I}) \subseteq \mathfrak{O}_F$ means $T_{K/F}(\beta\alpha) \in \mathfrak{O}_F$ for all $\alpha \in \mathfrak{I}$.

Lemma 5.2 — The Dual is Fractional
If K/F is an extension of number fields with $\mathfrak{I} \in I_{\Delta_K}$, then $\mathfrak{I}^* \in I_{\Delta_K}$.

Proof. Let $\alpha_1, \alpha_2 \in \mathfrak{I}^*$, and $\beta_1, \beta_2 \in \mathfrak{O}_K$. Then

$$T_{K/F}((\beta_1\alpha_1 + \beta_2\alpha_2)\mathfrak{I}) \subseteq T_{K/F}(\beta_1\mathfrak{I}) + T_{K/F}(\beta_2\mathfrak{I}) \subseteq \mathfrak{O}_F,$$

so $\mathfrak{I}^*$ is an $\mathfrak{O}_K$-module. Since $\mathfrak{I} \in I_{\Delta_K}$, then by Definition 1.24 on page 26, there exists a nonzero $\beta \in \mathfrak{O}_K$ such that $\beta\mathfrak{I} \subseteq \mathfrak{O}_K$. By Definition 5.5, all such β are in $\mathfrak{I}^*$, which must therefore be nonzero.

Claim 5.5 There exists a $\beta^* \in \mathfrak{O}_K$ such that

$$\beta^*\mathfrak{I}^* \subseteq \mathfrak{O}_K.$$

Let $\beta_1, \beta_2, \ldots, \beta_n$ be a basis for K over F with $\beta_j \in \mathfrak{O}_K$ for $j = 1, 2, \ldots, n$, which is allowed by Exercise 2.42 on page 82. Let $\beta \in \mathfrak{I} \cap \mathfrak{O}_K$ be nonzero, and set

$$\beta^* = N_{K/F}(\beta)\det(T_{K/F}(\beta_i\beta_j)).$$

Let

$$\gamma = \sum_{j=1}^{n} \alpha_j\beta_j \in \mathfrak{I}^* \quad (\alpha_j \in F),$$

be arbitrarily chosen. Then

$$T_{K/F}(N_{K/F}(\beta)\gamma\beta_i) \in \mathfrak{O}_F,$$

since $N_{K/F}(\beta)\beta_i \in \mathfrak{O}_K$. However, for each $i = 1, 2, \ldots, n$,

$$T_{K/F}(N_{K/F}(\beta)\gamma\beta_i) = N_{K/F}(\beta)T_{K/F}(\gamma\beta_i) = N_{K/F}(\beta)\sum_{j=1}^{n} \alpha_j T_{K/F}(\beta_i\beta_j).$$

Hence, for each such i, j,

$$\alpha_j N_{K/F}(\beta)\det(T_{K/F}(\beta_i\beta_j)) \in \mathfrak{O}_F,$$

so $\beta^*\gamma \in \mathfrak{O}_K$. This establishes Claim 5.5, from which it follows that $\mathfrak{I}^* \in I_{\Delta_K}$. □

Lemma 5.3 — Properties of the Dual

Let K/F be an extension of number fields, and let $\mathcal{I} \in I_{\Delta_K}$. Then each of the following holds.

(a) $\mathcal{I}\mathcal{I}^* = \mathfrak{O}_K^*$.

(b) If I is an integral $\mathfrak{O}_K$-ideal, then $(I^*)^{-1}$ is an integral $\mathfrak{O}_K$-ideal.

(c) If $\mathcal{J} \in I_{\Delta_K}$ and $\mathcal{I} \subseteq \mathcal{J}$, then $\mathcal{I}^* \supseteq \mathcal{J}^*$.

Proof. Let $\alpha \in \mathcal{I}^*$. Then $T_{K/F}(\alpha\mathcal{I}) \subseteq \mathfrak{O}_F$, so $T_{K/F}(\alpha\mathcal{I}\mathfrak{O}_K) \subseteq \mathfrak{O}_K$. Therefore, $\alpha\mathcal{I} \subseteq \mathfrak{O}_K^*$. In other words, $\alpha \in \mathcal{I}^{-1}\mathfrak{O}_K^*$. We have shown that

$$\mathcal{I}^* \subseteq \mathcal{I}^{-1}\mathfrak{O}_K^*.$$

By reversing the argument, we get that

$$\mathcal{I}^{-1}\mathfrak{O}_K^* \subseteq \mathcal{I}^*.$$

Hence, we have $\mathcal{I}^* = \mathcal{I}^{-1}\mathfrak{O}_K^*$, so

$$\mathcal{I}\mathcal{I}^* = \mathcal{I}\mathcal{I}^{-1}\mathfrak{O}_K^* = \mathfrak{O}_K^*,$$

which is (a). In particular, if $I \subseteq \mathfrak{O}_K$, then $\mathfrak{O}_K \subseteq I^*$. Therefore,

$$(I^*)^{-1} = \mathfrak{O}_K(I^*)^{-1} \subseteq I^*(I^*)^{-1} = \mathfrak{O}_K,$$

which is (b).

For (c) assume that $\mathcal{I} \subseteq \mathcal{J}$. Then for any $\beta \in \mathcal{J}^*$,

$$T_{K/F}(\beta\mathcal{I}) \subseteq T_{K/F}(\beta\mathcal{J}) \subseteq \mathfrak{O}_F.$$

Hence, $\beta \in \mathcal{I}^*$, so $\mathcal{I}^* \supseteq \mathcal{J}^*$. □

By Lemma 5.2, if $\mathcal{I} \in I_{\Delta_K}$, then $\mathcal{I}^* \in I_{\Delta_K}$. In particular, by part (b) Lemma 5.3, if I is an integral $\mathfrak{O}_K$-ideal, then $(I^*)^{-1}$ is an integral $\mathfrak{O}_K$-ideal. In any case, $(\mathcal{I}^*)^{-1}$ is a special kind of ideal.

Definition 5.6 — The Different

Let K/F be an extension of number fields and let $\mathcal{I} \in I_{\Delta_K}$. Then the ideal $(\mathcal{I}^*)^{-1} \in I_{\Delta_K}$ is called the *different of* $\mathcal{I}$ *over* F, denoted by $\mathcal{D}_{K/F}(\mathcal{I})$. If $\mathcal{I} = \mathfrak{O}_K$, then $\mathcal{D}_{K/F}(\mathcal{I})$ is called the *different of the extension* K/F, denoted by $\mathcal{D}_{K/F}$.

We now employ the Galois theory developed in §2.1.

Lemma 5.4 — Properties of the Different

Let $F \subseteq K \subseteq L$ be an extension of number fields. Then each of the following holds.

1. If $\mathcal{I} \in I_{\Delta_K}$, then $\mathcal{D}_{K/F}(\mathcal{I}) = \mathcal{I}\mathcal{D}_{K/F}$.
2. $\mathcal{D}_{L/F} = \mathcal{D}_{L/K}\mathcal{D}_{K/F}$.
3. If K/F is normal, then for any $\sigma \in \text{Gal}(K/F)$, $\mathcal{D}_{K/F}^{\sigma} = \mathcal{D}_{K/F}$. In other words, $\mathcal{D}_{K/F}$ is fixed, also called *invariant* under the action of the Galois group. The notations $\sigma(\mathcal{D}_{K/F})$ and $\mathcal{D}_{K/F}^{\sigma}$ for the action of σ are used interchangeably.

4. If $\mathfrak{I} \in I_{\Delta_F}$ and $\mathfrak{J} \in I_{\Delta_K}$, then $T_{K/F}(\mathfrak{J}) \subseteq \mathfrak{I}$ if and only if $\mathfrak{J} \subseteq \mathfrak{I}\mathfrak{D}_{K/F}^{-1}$.

Proof. For part 1, we use part (a) of Lemma 5.3 on the previous page to get, $(\mathfrak{I}\mathfrak{I}^*)^{-1} = (\mathfrak{O}_K^*)^{-1}$, so

$$(\mathfrak{I}^*)^{-1} = (\mathfrak{I}^{-1})^{-1}(\mathfrak{O}_K^*)^{-1} = \mathfrak{I}(\mathfrak{O}_K^*)^{-1},$$

namely $\mathfrak{D}_{K/F}(\mathfrak{I}) = \mathfrak{I}\mathfrak{D}_{K/F}$.

For part 2, we observe that $\alpha \in \mathfrak{D}_{L/K}^{-1}$ if and only if $T_{L/K}(\alpha) \in \mathfrak{O}_K$ by Definition 5.5 on page 196. In turn the latter is equivalent to

$$\mathfrak{D}_{K/F}^{-1} T_{L/K}(\alpha) \subseteq \mathfrak{D}_{K/F}^{-1}, \tag{5.5}$$

by part (c) of Lemma 5.3. Also, (5.5) holds if and only if

$$T_{K/F}(\mathfrak{D}_{K/F}^{-1} T_{L/K}(\alpha)) = T_{K/F}(T_{L/K}(\alpha\mathfrak{D}_{K/F}^{-1})) = T_{L/F}(\alpha\mathfrak{D}_{K/F}^{-1}) \subseteq \mathfrak{O}_F, \tag{5.6}$$

by part (b) of Theorem 5.2 on page 185. Lastly, (5.6) is equivalent to saying that $\alpha\mathfrak{D}_{K/F}^{-1} \subseteq \mathfrak{D}_{L/F}^{-1}$. We have shown that $\alpha \in \mathfrak{D}_{L/K}^{-1}$ if and only if $\alpha \in \mathfrak{D}_{K/F}\mathfrak{D}_{L/F}^{-1}$, namely $\mathfrak{D}_{L/K}^{-1} = \mathfrak{D}_{K/F}\mathfrak{D}_{L/F}^{-1}$. In other words, $\mathfrak{D}_{L/F} = \mathfrak{D}_{L/K}\mathfrak{D}_{K/F}$.

For part 3, let $\beta \in \mathfrak{O}_K^*$, and $\sigma \in \mathrm{Gal}(K/F)$. Then since $T_{K/F}(\beta\mathfrak{O}_K) \subseteq \mathfrak{O}_F$, we have

$$T_{K/F}(\beta^\sigma\mathfrak{O}_K) = T_{K/F}(\beta\mathfrak{O}_K^{\sigma^{-1}}) = T_{K/F}(\beta\mathfrak{O}_K) \subseteq \mathfrak{O}_F.$$

Therefore, ${\mathfrak{O}_K^*}^\sigma \subseteq \mathfrak{O}_K^*$ for all $\sigma \in \mathrm{Gal}(K/F)$. Similarly, ${\mathfrak{O}_K^*}^{\sigma^{-1}} \subseteq \mathfrak{O}_K^*$, so $\mathfrak{O}_K^* \subseteq {\mathfrak{O}_K^*}^\sigma$. Hence, $\mathfrak{O}_K^* = {\mathfrak{O}_K^*}^\sigma$, namely $\mathfrak{D}_{K/F}^\sigma = \mathfrak{D}_{K/F}$.

Finally, for part 4, $T_{K/F}(\mathfrak{J}) \subseteq \mathfrak{I}$ if and only if $\mathfrak{I}^{-1}T_{K/F}(\mathfrak{J}) = T_{K/F}(\mathfrak{I}^{-1}\mathfrak{J}) \subseteq \mathfrak{O}_F$, which in turn holds if and only if $\mathfrak{I}^{-1}\mathfrak{J} \subseteq \mathfrak{D}_{K/F}^{-1}$, namely when $\mathfrak{J} \subseteq \mathfrak{I}\mathfrak{D}_{K/F}^{-1}$.

□

We now are able to generalize the notion given in Definition 2.7 on page 77.

Definition 5.7 — Discriminant of a Relative Extension

Let K/F be an extension of number fields. Then the *discriminant of* K/F is $N^{K/F}(\mathfrak{D}_{K/F})$, denoted by$\Delta_{K/F}$. In particular,$\Delta_{K/\mathbb{Q}} = (\Delta_K)$ is called the *absolute discriminant of* K.

The reader should now go to Exercise 5.17 on page 212 for an explicit example of the above. An important property of relative discriminants is given as follows.

Lemma 5.5 — Relative Discriminants in Towers

If $F \subseteq K \subseteq L$ is a tower of number fields, then$\Delta_{L/F} = \Delta_{K/F}^{|L:K|} N^{K/F}(\Delta_{L/K})$.

Proof. From part 2 of Lemma 5.4, we have

$$\Delta_{L/F} = N^{L/F}(\mathfrak{D}_{L/K}\mathfrak{D}_{K/F}) = N^{L/F}(\mathfrak{D}_{L/K})N^{L/F}(\mathfrak{D}_{K/F}),$$

where the last equality comes from Exercise 5.3 on page 194. By Exercises 5.6–5.7 the latter equals,

$$N^{K/F}(N^{L/K}(\mathfrak{D}_{L/K}))N^{K/F}(N^{L/K}(\mathfrak{D}_{K/F})) = N^{K/F}(\Delta_{L/K})N^{K/F}(\mathfrak{D}_{K/F}^{|L:K|})$$

$$= N^{K/F}(\Delta_{L/K})N^{K/F}(\mathfrak{D}_{K/F})^{|L:K|} = N^{K/F}(\Delta_{L/K})\Delta_{K/F}^{|L:K|},$$

as required. □

The next result verifies that the absolute discriminant coincides with the notion given in Definition 2.7 as an ideal generator.

Theorem 5.7 — Dual Basis, Different, and Discriminant

Let F be an algebraic number field, and let $\mathcal{I} \in I_{\Delta_F}$ with $\mathbb{Z}$-basis $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and set $\mathcal{B}^* = \{\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*\}$ with $\alpha_j^* \in F$ defined by

$$T_{F/\mathbb{Q}}(\alpha_i \alpha_j^*) = \delta_{i,j},$$

where $\delta_{i,j} = 0$ if $i \neq j$ and $\delta_{i,j} = 1$ if $i = j$.[5.5] Then the set $\mathcal{B}^*$ is an integral basis for $\mathcal{I}^*$, called a dual basis. Furthermore,

$$N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}(\mathcal{I})) = N^{F/\mathbb{Q}}(\mathcal{I})|\Delta_F|.$$

In particular,

$$N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}) = |\Delta_F|.$$

In other words, as ideals,

$$\Delta_{F/\mathbb{Q}} = (\ \Delta_F).$$

Proof. Let A be the matrix with entries $(T_{F/\mathbb{Q}}(\alpha_i \alpha_j))$. From Theorem 2.8 on page 73, we know that $\det(A) \neq 0$. Thus, A is invertible, so $AA^{-1} = I_n$. The diagonal of this identity matrix consists of elements $\alpha_i \alpha_i^* = 1$, where the

$$\alpha_i^* = \sum_{k=1}^{n} \alpha_k \frac{\det(A_{k,i})}{\det(A)} \in F,$$

from Theorem A.22 on page 338. Also, the off-diagonal elements of the identity matrix give us that $\alpha_i \alpha_j^* = 0$, with the $\alpha_j^* \in F$ similarly determined by Theorem A.22. Hence, $T_{F/\mathbb{Q}}(\alpha_j \alpha_j^*) = 1$ and $T_{F/\mathbb{Q}}(\alpha_i \alpha_j^*) = 0$ for $i \neq j$. This establishes the existence of the elements in $\mathcal{B}^*$, and so secures the validity of the first assertion.

Let $\beta \in F$. Then by the definition of the α_j^*, there exist $q_j \in \mathbb{Q}$ such that $\beta = \sum_{j=1}^{n} q_j \alpha_j^*$. Also, for any $\alpha \in \mathcal{I}$, there exist $z_j \in \mathbb{Z}$ such that $\alpha = \sum_{i=1}^{n} z_i \alpha_i$. Thus,

$$T_{F/\mathbb{Q}}(\alpha\beta) = \sum_{i=1}^{n} \sum_{j=1}^{n} q_j z_i \alpha_i \alpha_j^*,$$

so $T_{F/\mathbb{Q}}(\alpha\beta) \subseteq \mathbb{Z}$ exactly when $q_j \in \mathbb{Z}$ for $j = 1, 2, \ldots, n$, so $\mathcal{B}^*$ is an integral basis for $\mathcal{I}^*$.

For the assertion on norms, we first assume that $\mathcal{I} = \mathfrak{O}_F$. By the above, $\mathfrak{O}_F^* = \mathcal{D}_{F/\mathbb{Q}}^{-1}$ has dual basis consisting of the α_j^*. Let $m \in \mathbb{N}$ such that

$$m\alpha_j^* = m_j^* \in \mathfrak{O}_F, \tag{5.7}$$

which is allowed by Lemma 1.4 on page 38. Let $\mathfrak{J} = m\mathcal{D}_{F/\mathbb{Q}}{}^{-1} \subseteq \mathfrak{O}_F$. Then by Corollary 2.8 on page 85,

$$N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}^{-1})^2 = N^{F/\mathbb{Q}}(\mathfrak{J}m^{-1})^2 = N^{F/\mathbb{Q}}(\mathfrak{J})^2 N_{F/\mathbb{Q}}(m)^{-2} = N^{F/\mathbb{Q}}(\mathfrak{J})^2 m^{-2n},$$

and by Theorem 2.12 on page 85, this equals

$$\operatorname{disc}\left(\{m_1^*, m_2^*, \ldots, m_n^*\}\right) \Delta_F{}^{-1} m^{-2n} = \operatorname{disc}\left(\{\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*\}\right) \Delta_F{}^{-1},$$

where the last equality follows from (5.7).

[5.5] The $\delta_{i,j}$ is called the *Kronecker delta.*

To complete the proof, we observe that the following matrix equation holds,

$$(T_{F/\mathbb{Q}}(\alpha_i\alpha_j^*)) = (\theta_j(\alpha_i))(\theta_j(\alpha_i^*))^t,$$

where $\theta_1, \theta_2, \ldots, \theta_n$ are the $\mathbb{Q}$-isomorphisms of F. Hence by the Kronecker delta symbol, this is the identity matrix, so

$$\operatorname{disc}(\alpha_1^*, \ldots, \alpha_n^*) = \operatorname{disc}^{-1}(\alpha_1, \ldots, \alpha_n) = {\Delta_F}^{-1}.$$

We have shown that $N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}})^2 = {\Delta_F}^2$, so

$$N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}) = |\Delta_F|.$$

By part 1 of Lemma 5.4 on page 197, if $\mathcal{I} \in I_{\Delta_F}$, then

$$N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}(\mathcal{I})) = N^{F/\mathbb{Q}}(\mathcal{I}\mathcal{D}_{F/\mathbb{Q}}) = N^{F/\mathbb{Q}}(\mathcal{I})N^{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}}) = N^{F/\mathbb{Q}}(\mathcal{I})|\Delta_F|,$$

as required. □

Corollary 5.3 *Suppose that L is a number field with squarefree discriminant Δ_L. If $\mathbb{Q} \subseteq K \subseteq L$ is a tower of number fields, then $K = \mathbb{Q}$ or $K = L$.*

Proof. By Remark 3.14 on page 116, if $K \neq \mathbb{Q}$, there is a prime $p \mid \Delta_K$. By Lemma 5.5 on page 198, and Theorem 5.7 on the previous page,

$$(p)^{|L:K|} \mid \Delta_{L/\mathbb{Q}} = (\ \Delta_L),$$

contradicting the squarefreeness, so $L = K$. □

Corollary 5.4 *If $\mathbb{Q} \subseteq K \subseteq L$ is a tower of number fields, then*

$${\Delta_K}^{|L:K|} \mid \Delta_L.$$

Proof. By Lemma 5.5,

$${\Delta_{K/\mathbb{Q}}}^{|L:K|} \mid \Delta_{L/\mathbb{Q}},$$

which secures the result. □

The reader will observe that Corollary 5.4 generalizes Kronecker's result given in Theorem 3.15 on page 126.

The following result, which was known to Euler in a different form, is another tool in our quest to establish a fundamental result in the theory of the different that, in turn, will allow us to establish important results in ramification theory in §5.3.

Theorem 5.8 — Generators for the Dual of a Primitive Extension

Let K/F be an extension of number fields, with $K = F(\alpha)$ where $\alpha \in \mathfrak{O}_K$, and set $|K : F| = n$. Then

$$\mathfrak{O}_F[\alpha]^* = \frac{\mathfrak{O}_F[\alpha]}{m'_{\alpha,F}(\alpha)},$$

where $m'_{\alpha,F}$ is the formal derivative of $m_{\alpha,F}$. In other words, $\mathfrak{O}_F[\alpha]^*$ is generated as an $\mathfrak{O}_F$-module by the elements

$$\alpha^j/m'_{\alpha,F}(\alpha) \text{ for } j = 0, 1, 2, \ldots, n-1.$$

Also,

$$T_{K/F}\left(\frac{\alpha^j}{m'_{\alpha,F}(\alpha)}\right) = 0 \text{ for all } j = 0, 1, 2, \ldots, n-2, \tag{5.8}$$

and

$$T_{K/F}\left(\frac{\alpha^{n-1}}{m'_{\alpha,F}(\alpha)}\right) = 1. \tag{5.9}$$

Proof. Let α_j, for $j = 1, 2, \ldots, n$, be the conjugates of α over F, where $\alpha_1 = \alpha$—see Exercise 2.1 on page 62. By applying the Lagrange interpolation formula—see Theorem A.26 on page 342—we get

$$1 = \sum_{i=1}^{n} \frac{m_{\alpha,F}(x)}{m'_{\alpha_i,F}(\alpha)(x-\alpha_i)} = \sum_{i=1}^{n} \frac{m_{\alpha,F}(x)}{m'_{\alpha_i,F}(\alpha)} \sum_{k=0}^{\infty} \frac{\alpha_i^k}{x^{k+1}}, \tag{5.10}$$

where the last equality comes from Theorem B.4 on page 347. Also, if

$$m_{\alpha,F}(x) = x^n + \sum_{k=1}^{n} a_k x^{n-k},$$

then

$$\frac{1}{m_{\alpha,F}(x)} = \frac{1}{x^n} + \sum_{k=1}^{\infty} \frac{a_k}{x^{n+k}}. \tag{5.11}$$

By comparing (5.10)–(5.11), we get (5.8)–(5.9), which also says that

$$T_{K/F}\left(\frac{\alpha^j}{m'_{\alpha,F}(\alpha)}\right) \in \mathfrak{O}_F,$$

so

$$\alpha^j/m'_{\alpha,F}(\alpha) \in \mathfrak{O}_F[\alpha]^*.$$

In other words,

$$\frac{\mathfrak{O}_F[\alpha]}{m'_{\alpha,F}(\alpha)} \subseteq \mathfrak{O}_F[\alpha]^*.$$

It remains to establish the reverse inclusion. Let $y \in \mathfrak{O}_F[\alpha]^*$.
Since the elements $\alpha^j/m'_{\alpha,F}(\alpha)$ for $j = 0, 1, 2, \ldots, n-1$ form a basis for K over F, we may write

$$y = \sum_{j=0}^{n-1} a_j \frac{\alpha^j}{m'_{\alpha,F}(\alpha)}.$$

Therefore,

$$T_{K/F}(y) = \sum_{j=0}^{n-1} a_j T_{K/F}\left(\frac{\alpha^j}{m'_{\alpha,F}(\alpha)}\right) = a_{n-1},$$

by (5.8)–(5.9) established above. Since $y \in \mathfrak{O}_F[\alpha]^*$, then $a_{n-1} \in \mathfrak{O}_F$. Now let

$$m_{\alpha,F}(x) = x^n + \sum_{k=0}^{n-1} b_k x^k, \text{ with } b_k \in \mathfrak{O}_F, \tag{5.12}$$

since $\alpha \in \mathfrak{O}_K$. Thus,

$$T_{K/F}(y\alpha) = \sum_{j=0}^{n-1} a_j T_{K/F}\left(\frac{\alpha^{j+1}}{m'_{\alpha,F}(\alpha)}\right) = a_{n-2} + a_{n-1}T_{K/F}\left(\frac{\alpha^n}{m'_{\alpha,F}(\alpha)}\right),$$

and from (5.12), this equals

$$a_{n-2} - a_{n-1}\left(\sum_{k=1}^{n} b_k T_{K/F}\left(\frac{\alpha^{n-k}}{m'_{\alpha,F}(\alpha)}\right)\right) = a_{n-2} - a_{n-1}b_1.$$

Since $a_{n-2} - a_{n-1}b_1 \in \mathfrak{O}_F$, then $a_{n-2} \in \mathfrak{O}_F$. Continuing in this fashion, we see that all $a_j \in \mathfrak{O}_F$, so $y \in \mathfrak{O}_F[\alpha]$, which completes the reverse inclusion, and hence the entire proof.□

Now we turn to a concept that will help to explain the term *different*.

Definition 5.8 — Different of an Element

Let K/F be an extension of number fields with $K = F(\alpha)$ for $\alpha \in \mathfrak{O}_K$. The *different of* α is $m'_{\alpha,F}(\alpha)$, denoted by

$$\delta_{K/F}(\alpha).$$

The reason for the name “different” in Definition 5.8 is that $m'_{\alpha,F}(\alpha) \neq 0$ exactly when α is *different* from all of its conjugates over F. In other words, $\alpha \neq \theta_j(\alpha)$ for all F-isomorphisms θ_j of K that are not the identity embedding, namely when α is a primitive element over F. Now it is important to compare $\mathfrak{O}_K^*$ with $\mathfrak{O}_F[\alpha]^*$. We know that $\mathfrak{O}_K^* \subseteq \mathfrak{O}_F[\alpha]^* = \mathfrak{O}_F[\alpha]/m'_{\alpha,F}(\alpha)$, since for any $\beta \in \mathfrak{O}_K^*$, we must have $T_{K/F}(\beta\mathfrak{O}_F[\alpha]) \subseteq \mathfrak{O}_F$, given that $\mathfrak{O}_F[\alpha] \subseteq \mathfrak{O}_K$ for $\alpha \in \mathfrak{O}_K$. Now we look at the reverse inclusion from the following perspective.

Definition 5.9 — The Conductor

Let K/F be an extension of number fields, and let R be a subring of $\mathfrak{O}_K$ such that $\mathfrak{O}_F \subseteq R$. Let $\mathfrak{f}_R$ [5.6] be the greatest common divisor of the $\mathfrak{O}_K$-ideals contained in R. We call $\mathfrak{f}_R$ the *conductor of* R *in* $\mathfrak{O}_K$.

Lemma 5.6 — Conductor Characterization

Let K/F be an extension of number fields, and let R be a subring of $\mathfrak{O}_K$ such that $\mathfrak{O}_F \subseteq R$. Then

$$\mathfrak{f}_R = \{\beta \in K : \beta R^* \subseteq \mathfrak{O}_K^*\},$$

and $\mathfrak{f}_R$ is an $\mathfrak{O}_K$-ideal contained in R. In particular, if $R = \mathfrak{O}_F[\alpha]$ for some $\alpha \in \mathfrak{O}_K$, then

$$\mathfrak{f}_\alpha = m'_{\alpha,F}(\alpha)\mathfrak{O}_K^* = \delta_{K/F}(\alpha)\mathfrak{O}_K^*$$

is the conductor of $\mathfrak{O}_F[\alpha]$ in $\mathfrak{O}_K$ and is the largest $\mathfrak{O}_K$-ideal contained in $\mathfrak{O}_F[\alpha]$.

Proof. Set

$$I = \{\beta \in K : \beta R^* \subseteq \mathfrak{O}_K^*\}.$$

For $\beta \in I$, $\gamma \in \mathfrak{O}_K$, we have

$$\gamma\beta R^* \subseteq \gamma\mathfrak{O}_K^* \subseteq \mathfrak{O}_K^*.$$

[5.6] The letter $\mathfrak{f}$ is used here since the origin is in the German language, where the term for conductor is *Führer*.

Therefore, I is an $\mathfrak{O}_K^*$-module. (Observe that if $R \neq \mathfrak{O}_K$, then R^* is an $\mathfrak{O}_F$-module, but not an $\mathfrak{O}_K$-module.) Also, $R^* \subseteq \mathfrak{O}_K^*$, so

$$T_{K/F}(IR^*) \subseteq T_{K/F}(\mathfrak{O}_K^*) \subseteq \mathfrak{O}_F.$$

Therefore, $R^* \subseteq I^*$, so $I \subseteq R \subseteq \mathfrak{O}_K$. This shows that I is an $\mathfrak{O}_K$-ideal contained in R. Consequently, the $\mathfrak{O}_K$-ideal $\mathfrak{f}_R$ divides I.

Suppose that J is an $\mathfrak{O}_K$-ideal in R and $\beta \in R^*$, namely $T_{K/F}(\beta R) \subseteq \mathfrak{O}_F$. Then

$$T_{K/F}(\beta J \mathfrak{O}_K) \subseteq T_{K/F}(\beta R) \subseteq \mathfrak{O}_F.$$

Therefore, $\beta J \subseteq \mathfrak{O}_K^*$, which implies that $J \subseteq I$. Thus, I divides all $\mathfrak{O}_K$-ideals in R, so $I \mid \mathfrak{f}_R$. Hence,

$$I = \mathfrak{f}_R \subseteq R,$$

as required.

Now if $R = \mathfrak{O}_F[\alpha]$, then by the above and the fact that $\mathfrak{O}_K^* \subseteq \mathfrak{O}_F[\alpha]^*$, we get,

$$m'_{\alpha,F}(\alpha)\mathfrak{O}_K^* \subseteq m'_{\alpha,F}(\alpha)\mathfrak{O}_F[\alpha]^* = \mathfrak{O}_F[\alpha] \subseteq \mathfrak{O}_K,$$

where the equality comes from Theorem 5.8 on page 200. Thus, $m'_{\alpha,F}(\alpha)\mathfrak{O}_K^*$ is an $\mathfrak{O}_K$-ideal contained in $\mathfrak{f}_\alpha$. Also, from the proof of Theorem 5.8,

$$T_{K/F}\left(\frac{\mathfrak{O}_F[\alpha]}{m'_{\alpha,F}(\alpha)}\right) \in \mathfrak{O}_F.$$

Therefore, $\mathfrak{O}_F[\alpha]/m'_{\alpha,F}(\alpha) \subseteq \mathfrak{O}_K^*$, but $\mathfrak{f}_\alpha \subseteq \mathfrak{O}_F[\alpha]$ by the first part of the proof, so

$$\mathfrak{f}_\alpha / m'_{\alpha,F}(\alpha) \subseteq \mathfrak{O}_K^*.$$

In other words, $\mathfrak{f}_\alpha \subseteq m'_{\alpha,F}(\alpha)\mathfrak{O}_K^*$. Hence,

$$\mathfrak{f}_\alpha = m'_{\alpha,F}(\alpha)\mathfrak{O}_K^*,$$

which is the first required equality. For the second one, we first note that since $\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]^*$, and $\mathfrak{O}_F[\alpha] \subseteq \mathfrak{O}_K^*$, then

$$\{\beta \in \mathfrak{O}_F[\alpha] : \beta\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]\} \subseteq \mathfrak{f}_\alpha.$$

Conversely, from the first proved equality, and the fact that

$$m'_{\alpha,F}(\alpha)\mathfrak{O}_K^* \subseteq m'_{\alpha,F}(\alpha)\mathfrak{O}_F[\alpha]^* = \mathfrak{O}_F[\alpha],$$

from Theorem 5.8, then for any $\beta \in \mathfrak{f}_\alpha = m'_{\alpha,F}(\alpha)\mathfrak{O}_K^*$ we get that $\beta \in \mathfrak{O}_F[\alpha]$ and $\beta\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]$. Hence, $\mathfrak{f}_\alpha \subseteq \{\beta \in \mathfrak{O}_F[\alpha] : \beta\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]\}$, so we have the full equality.

Lastly, $\mathfrak{f}_\alpha$ is the largest $\mathfrak{O}_K$-ideal contained in $\mathfrak{O}_F[\alpha]$ by the above and Remark 1.15 on page 31. □

The reader is now encouraged to solve Exercise 5.18 as an explicit example of the above.

The following links our previous notion of different to the above.

Theorem 5.9 — Generation by Differents of Elements

Let K/F be an extension of number fields. Then $\mathfrak{D}_{K/F}$ is the $\mathfrak{O}_K$-ideal generated by the $\delta_{K/F}(\alpha)$, where α runs over the elements of $\mathfrak{O}_K$.

Proof. By Lemma 5.6 on page 202, $\delta_{K/F}(\alpha) \in \mathcal{D}_{K/F}$ for all $\alpha \in \mathfrak{O}_K$. In fact, from that lemma we have:

$$\delta_{K/F}(\alpha)\mathfrak{O}_K^* = \mathfrak{f}_\alpha \mathcal{D}_{K/F}.$$

Now we show that it suffices to find an $\alpha \in \mathfrak{O}_K$ such that $\mathcal{P} \nmid \mathfrak{f}_\alpha$ for all prime $\mathfrak{O}_K$-ideals $\mathcal{P}$. If such an α exists, then the ideal $\sum_{\alpha \in \mathfrak{O}_K} \mathfrak{f}_\alpha$ generated by $\cup_{\alpha \in \mathfrak{O}_K} \mathfrak{f}_\alpha$ must equal $\mathfrak{O}_K$. Hence,

$$\mathcal{D}_{K/F} = \mathcal{D}_{K/F}\mathfrak{O}_K = \mathcal{D}_{K/F}\left(\sum_{\alpha \in \mathfrak{O}_K} \mathfrak{f}_\alpha\right) = \sum_{\alpha \in \mathfrak{O}_K} \mathcal{D}_{K/F}\delta_{K/F}(\alpha)\mathfrak{O}_K^* =$$

$$\sum_{\alpha \in \mathfrak{O}_K} \delta_{K/F}(\alpha)\mathfrak{O}_K^*(\mathfrak{O}_K^*)^{-1} = \sum_{\alpha \in \mathfrak{O}_K} \delta_{K/F}(\alpha)\mathfrak{O}_K,$$

which shows that $\mathcal{D}_{K/F}$ is generated by the $\delta_{K/F}(\alpha)$. Hence, it remains to show that such an α exists.

Let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal, and let $\mathfrak{p}$ be the prime $\mathfrak{O}_F$-ideal lying below it. Furthermore, suppose that $\mathfrak{p}\mathfrak{O}_K = \mathcal{P}^e\mathcal{I}$, where $e \in \mathbb{N}$ and $\mathcal{P} \nmid \mathcal{I}$.

Claim 5.6 There exists an $\alpha \in \mathcal{I}$, with $\alpha \notin \mathcal{P}$, such that its residue class, $\overline{\alpha}$, modulo $\mathcal{P}$ is a generator of the multiplicative group of nonzero elements of the field $\mathfrak{O}_K/\mathcal{P}$—see Exercise 4.25 on page 163.

Let $\beta \in \mathfrak{O}_K$ with $\beta \notin \mathcal{P}$. Then $\overline{\beta}$ is a generator of the multiplicative group of nonzero elements of the field $\mathfrak{O}_K/\mathcal{P}$. By Exercise 4.31 on page 164,

$$\beta^{N(\mathcal{P})} \equiv \beta \pmod{\mathcal{P}}.$$

If $\beta^{N(\mathcal{P})} \equiv \beta (\text{mod } \mathcal{P}^2)$, then let $\gamma \in \mathcal{P}$, with $\gamma \notin \mathcal{P}^2$. Then

$$\beta + \gamma \equiv \beta \pmod{\mathcal{P}} \text{ and } (\beta+\gamma)^{N(\mathcal{P})} \equiv \beta^{N(\mathcal{P})} \pmod{\mathcal{P}^2},$$

by the Binomial Theorem—see Corollary A.11 on page 341. Therefore,

$$(\beta+\gamma)^{N(\mathcal{P})} \equiv \beta + \gamma \pmod{\mathcal{P}} \text{ and } (\beta+\gamma)^{N(\mathcal{P})} \not\equiv \beta + \gamma \pmod{\mathcal{P}^2}.$$

Since $\mathcal{I}$ and $\mathcal{P}$ are relatively prime, then $\mathfrak{O}_K = \mathcal{P}^2 + \mathcal{I}$, so $\beta + \gamma = \beta_1 + \alpha$ where $\beta_1 \in \mathcal{P}^2$ and $\alpha \in \mathcal{I}$. Thus,

$$\alpha \equiv \beta + \gamma - \beta_1 \equiv \beta \pmod{\mathcal{P}},$$

so $\overline{\alpha}$ is a generator of the multiplicative group of nonzero elements of the field $\mathfrak{O}_K/\mathcal{P}$, and $\alpha \notin \mathcal{P}$. This completes Claim 5.6.

Claim 5.7 Let $n \in \mathbb{N}$ and suppose that S is a system of n representatives of $\mathfrak{O}_K$ modulo $\mathcal{P}$, with $1 \in S$ and let $\omega \in \mathcal{P}$, $\omega \notin \mathcal{P}^2$. Then

$$\mathcal{T} = \left\{ \sum_{j=0}^{n-1} a_j\omega^j : a_j \in S \text{ for } j = 0, 1, \ldots, n-1 \right\},$$

is a system of representatives of $\mathfrak{O}_K$ modulo $\mathcal{P}^n$.

We use induction on n. If $n = 1$, then $S = \mathcal{T}$, so we have the induction step. Assume, for the induction hypothesis that the result holds for $n-1$. Let $t_1, t_2 \in \mathcal{T}$ with $t_j = b_j + \omega s_j$ for $j = 1, 2$. if $t_1 - t_2 \in \mathcal{P}^n$, then $(b_1 - b_2) \in \mathcal{P}^n - (s_1 - s_2)\omega \subseteq \mathcal{P}$. Thus, $b_1 = b_2$ and $(s_1 - s_2)\omega \in \mathcal{P}^n$. Therefore, there exists an $\mathfrak{O}_K$-ideal J such that

$$\mathfrak{O}_K(s_1 - s_2)\omega = \mathcal{P}^n J.$$

Also, since $\mathcal{P}^2 \nmid (\omega) = \omega\mathfrak{O}_K$, there is an $\mathfrak{O}_K$-ideal I, not divisible by $\mathcal{P}$ such that

$$\mathfrak{O}_K\omega = \mathcal{P}I.$$

Thus,

$$\mathcal{P}^n J = \mathfrak{O}_K(s_1 - s_2)\omega = \mathfrak{O}_K(s_1 - s_2)\mathcal{P}I,$$

so

$$\mathcal{P}^{n-1} \mid \mathfrak{O}_K(s_1 - s_2).$$

Therefore, $s_1 - s_2 \in \mathcal{P}^{n-1}$. By induction hypothesis, $s_1 = s_2$, so $t_1 = t_2$. We have shown that for any $t_1, t_2 \in \mathcal{T}$, with $t_1 - t_2 \in \mathcal{P}^n$, we get $t_1 = t_2$. Hence, $\mathcal{T}$ has $N(\mathcal{P})^n$ different representatives of $\mathfrak{O}_K$ modulo $\mathcal{P}^n$. By Exercise 4.25 on page 163, $\mathcal{T}$ is a system of representatives of $\mathfrak{O}_K$ modulo $\mathcal{P}$. This is Claim 5.7.

Claim 5.8 *For any $n \in \mathbb{N}$ and any $\beta \in \mathfrak{O}_K$, there exists a unique $\gamma \in \mathfrak{O}_F[\alpha]$ such that*

$$\beta \equiv \gamma \pmod{\mathcal{P}^n}.$$

Let $\omega = \alpha^{N(\mathcal{P})} - \alpha$. Observe that by the same argument as used above on $\beta + \gamma$, we get that $\omega \notin \mathcal{P}^2$. Thus, by Claim 5.7, for any $\beta \in \mathfrak{O}_K$, there exists a unique $\sum_{j=0}^{n-1} a_j\omega^j \in \mathfrak{O}_F[\alpha]$ with $a_j \in S$ such that $\beta - \gamma \in \mathcal{P}^n$. This is Claim 5.8.

Finally, we now show that $\mathcal{P} \nmid \mathfrak{f}_\alpha$.

Let $\beta \in \mathfrak{O}_K m'_{\alpha,F}(\alpha) \cap \mathfrak{O}_F$. Then $\beta\mathfrak{O}_F = \mathfrak{p}^a\mathfrak{J}$, where a is a nonzero integer and the prime $\mathfrak{p}$ below $\mathcal{P}$ does not divide the $\mathfrak{O}_F$-ideal $\mathfrak{J}$. Consider

$$\beta^{h_F}\mathfrak{O}_F = (\sigma_1) \text{ and } \mathfrak{p}^{ah_F} = (\sigma_2).$$

Therefore, $\sigma_1 = \sigma_2\sigma_3$ where $\sigma_3 \in \mathfrak{J}^{h_F}$. Also, $\sigma_3 \notin \mathfrak{p}$ since $\mathfrak{p}^{ah_F+1} \nmid (\sigma_1)$. We now demonstrate that $\mathfrak{O}_K(\sigma_3\alpha^{ah_F}) \subseteq \mathfrak{O}_F[\alpha]$. By Claim 5.8, for any given $\rho \in \mathfrak{O}_K$, there exists a $\gamma \in \mathfrak{O}_F[\alpha]$ such that $\rho - \gamma \in \mathcal{P}^{eah_F}$. Since

$$\rho\sigma_3\alpha^{ah_F} = (\rho - \gamma)\sigma_3\alpha^{ah_F} + \gamma\sigma_3\alpha^{ah_F},$$

and $\gamma\sigma_3\alpha^{ah_F} \in \mathfrak{O}_F[\alpha]$, then it suffices to show that $(\rho - \gamma)\sigma_3\alpha^{ah_F} \in \mathfrak{O}_F[\alpha]$. Since $(\sigma_2) = \mathfrak{p}^{ah_F}$, then

$$\mathfrak{O}_K(\rho - \gamma)\sigma_3\alpha^{ah_F} = \frac{\mathfrak{O}_K(\rho - \gamma)\sigma_2\sigma_3\mathfrak{O}_K\alpha^{ah_F}}{\mathfrak{O}_K\mathfrak{p}^{ah_F}} \subseteq \frac{\mathfrak{O}_K\sigma_1\mathcal{P}^{eah_F}\mathfrak{O}_K\alpha^{ah_F}}{\mathcal{P}^{eah_F}\mathcal{J}^{ah_F}}$$

$$\subseteq \mathfrak{O}_K\beta^{h_F} \subseteq \mathfrak{O}_F[\alpha],$$

where the penultimate inclusion comes from the fact that $\alpha \in \mathcal{J}$, and the final inclusion arises from the fact that $m'_{\alpha,F}(\alpha)\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]$ by Exercise 5.12 on page 211. Having shown that the ideal $\mathfrak{O}_K(\sigma_3\alpha^{ah_F}) \subseteq \mathfrak{O}_F[\alpha]$, then it follows from Lemma 5.6 on page 202 that $\mathfrak{O}_K(\sigma_3\alpha^{ah_F}) \subseteq \mathfrak{f}_\alpha$. Since $\sigma_3 \notin \mathfrak{p}$, then $\sigma_3 \notin \mathcal{P}$. Thus, since $\alpha \notin \mathcal{P}$, we get by primality that $\sigma_3\alpha^{ah_F} \notin \mathcal{P}$. Hence, $\mathfrak{f}_\alpha \nsubseteq \mathcal{P}$, namely $\mathcal{P} \nmid \mathfrak{f}_\alpha$, which is the entire result. □

From the proof of Theorem 5.9 emerge two immediate consequences.

Corollary 5.5 If K/F is an extension of number fields, then for all prime $\mathfrak{O}_K$-ideals $\mathcal{P}$ there exists an $\alpha \in \mathfrak{O}_K$ such that $\mathcal{P} \nmid \mathfrak{f}_\alpha$.

Corollary 5.6 — Dedekind, 1881

Let K/F be an extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Suppose that $\mathcal{I}$ is an $\mathfrak{O}_K$-ideal not divisible by $\mathcal{P}$. Then there exists an $\alpha \in \mathcal{I}$ such that for all $\beta \in \mathfrak{O}_K$ and any $n \in \mathbb{N}$, there exists an element $\gamma \in \mathfrak{O}_F[\alpha]$ with

$$\beta \equiv \gamma \pmod{\mathcal{P}^n}.$$

Our next goal is to establish what may be considered as the main result in the theory of the different, namely the link between the different and ramification. We will prove that the primes that ramify in an extension K/F of number fields are precisely those primes that divide the different, and therefore that there are only finitely many of them. There are many methods in the literature for achieving such a task. One of them involves an idea put forth by Weil in 1943—see Biography 5.1 on page 211. He observed that the different is intimately linked to the notion of abstract differentiation in commutative rings.

Definition 5.10 — Derivations

Let R be a commutative ring with identity and let M be an R-module. A homomorphism $\mathfrak{d}$ from R into M is called a *derivation of R on M* provided that, for all α,β $\in R$,

$$\mathfrak{d}(\alpha\beta) = \alpha\mathfrak{d}(\beta) + \beta\mathfrak{d}(\alpha). \tag{5.13}$$

If T is a subring of R such that a derivation $\mathfrak{d}$ of R on M satisfies

$$\mathfrak{d}(\alpha) = 0 \text{ for all } \alpha \in T,$$

then $\mathfrak{d}$ is called a derivation of R on M that is *trivial* on T. In the case where M is a commutative ring, a derivation $\mathfrak{d}$ is deemed to be essential if there exists an element $\gamma \in \mathfrak{d}(R)$ such that γ is not a zero divisor.

Remark 5.2 Observe that since $\mathfrak{d}$ is a *homomorphism* of additive abelian groups, then in addition to (5.13), we have that

$$\mathfrak{d}(\alpha + \beta) = \mathfrak{d}(\alpha) + \mathfrak{d}(\beta),$$

for all α,β $\in R$. Also, note that (5.13) is the analogue of the standard *product formula* for derivatives in elementary calculus.

The reader may now solve Exercises 5.14–5.16 on page 212.

Theorem 5.10 — Differents and Derivations

Let K/F be an extension of number fields. Then $\mathcal{D}_{K/F}$ is the least common multiple of all $\mathfrak{O}_K$-ideals $\mathcal{I}$ for which there exists an essential derivation

$$\mathfrak{d} : \mathfrak{O}_K \mapsto \mathfrak{O}_K/\mathcal{I}$$

that is trivial on $\mathfrak{O}_F$.

Proof. We first show that it suffices to prove the result for $\mathcal{I} = \mathcal{P}^n$ where $n \in \mathbb{N}$ and $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal. Let $\mathcal{I} = \prod_{j=1}^n \mathcal{P}_j^{a_j}$, where the $\mathcal{P}_j$ are prime $\mathfrak{O}_K$-ideals, and $a_j \in \mathbb{N}$ for $j = 1, 2, \ldots, n$. Suppose that

$$\mathfrak{d} : \mathfrak{O}_K \mapsto \mathfrak{O}_K/\mathcal{I}$$

is an essential derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}_j^{a_j}$, which is trivial on $\mathfrak{O}_F$. Then

$$\mathfrak{d}_j : \mathfrak{O}_K \mapsto \mathfrak{O}_K/\mathcal{P}_j^{a_j}$$

defined for each $\beta \in \mathfrak{O}_K$ by

$$\mathfrak{d}_j(\beta) \equiv \mathfrak{d}(\beta) \pmod{\mathcal{P}_j^{a_j}}$$

is also an essential derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}_j^{a_j}$ that is trivial on $\mathfrak{O}_F$. Conversely, if $\mathfrak{d}_j$ is an essential derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}_j^{a_j}$ that is trivial on $\mathfrak{O}_F$, then the n-tuple $\mathfrak{d} = (\mathfrak{d}_1, \ldots, \mathfrak{d}_n)$ acting on

$$\mathfrak{O}_K/\mathcal{I} \cong \prod_{j=1}^n \mathfrak{O}_K/\mathcal{P}_j^{a_j},$$

via Theorem 1.21 on page 32, the Chinese Remainder Theorem, induces a derivation $\mathfrak{d}'$ of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{I}$ that is trivial on $\mathfrak{O}_F$. It remains to show that $\mathfrak{d}'$ is essential. Suppose that the n-tuple $(\beta_1, \ldots, \beta_n) \in \mathfrak{O}_K$ is such that $\mathfrak{d}_j(\beta_j)$ is not a zero divisor in $\mathfrak{O}_K/\mathcal{P}_j^{a_j}$. By Theorem 1.21, again, we may choose $\beta \in \mathfrak{O}_K$ such that

$$\beta \equiv \beta_j \pmod{\mathcal{P}_j^{a_j}}$$

for each $j = 1, 2, \ldots, n$. Therefore, $\mathfrak{d}'(\beta)$ is not a zero divisor in $\mathfrak{O}_K/\mathcal{I}$.

Our remaining task is to prove that an essential derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}^n$ exists if and only if $\mathcal{P}^n \mid \mathcal{D}_{K/F}$. If $\mathfrak{d}$ is such a derivation, then by Corollaries 5.5–5.6, we may select an $\alpha \in \mathfrak{O}_K$ such that $\mathcal{P} \nmid \mathfrak{f}_\alpha$, and for any $n \in \mathbb{N}$ and any $\beta \in \mathfrak{O}_K$ we have

$$\beta \equiv g(\alpha) \pmod{\mathcal{P}^{n+1}}$$

for some $g(\alpha) \in \mathfrak{O}_F[\alpha]$. For such a congruence, we get from Exercise 5.15 that

$$\mathfrak{d}(\beta) = \mathfrak{d}(g(\alpha)) = g'(\alpha)\mathfrak{d}(\alpha),$$

where the last equality follows from the very definition of a derivation, with g' being the derivative of g. If $\mathfrak{d}(\alpha)$ is a zero divisor, then $\mathfrak{d}(\beta)$ is a zero divisor for all $\beta \in \mathfrak{O}_K$, contradicting the choice of $\mathfrak{d}$. Thus, $\mathfrak{d}(\alpha)$ is not a zero divisor, so

$$0 = \mathfrak{d}(0) = \mathfrak{d}(m_{\alpha,F}(\alpha)) = m'_{\alpha,F}(\alpha)\mathfrak{d}(\alpha).$$

Therefore,

$$m'_{\alpha,F}(\alpha) \equiv 0 \pmod{\mathcal{P}^n}.$$

By Lemma 5.6 on page 202,

$$m'_{\alpha,F}(\alpha)\mathfrak{O}_K^* = \mathfrak{f}_\alpha \mathcal{D}_{K/F},$$

but $\mathcal{P} \nmid \mathfrak{f}_\alpha$, so $\mathcal{P}^n \mid \mathcal{D}_{K/F}$.

Conversely, assume that $\mathcal{P}^n \mid \mathcal{D}_{K/F}$, and select $\alpha \in \mathfrak{O}_K$ such that $\mathcal{P} \nmid \mathfrak{f}_\alpha$. Let $\beta \in \mathfrak{f}_\alpha$ with $\beta \notin \mathcal{P}$. By Lemma 5.6 again, every $\gamma \in \mathfrak{O}_K$ may be written as

$$\gamma = \frac{g(\alpha)}{\beta},$$

where $g(x) \in \mathfrak{O}_F[x]$. Since $\beta \in \mathfrak{f}_\alpha \subseteq \mathfrak{O}_F[\alpha]$, by Lemma 5.6 one more time, then $\beta = h(\alpha) \in \mathfrak{O}_F[\alpha]$. Since $\beta \notin \mathcal{P}$, then β has a multiplicative inverse $\sigma \in \mathfrak{O}_K$ modulo $\mathcal{P}$, namely

$$\beta\sigma \equiv 1 \pmod{\mathcal{P}^n}. \tag{5.14}$$

Define for each $\gamma = g(\alpha)/\beta \in \mathfrak{O}_K$,

$$\mathfrak{d}(\gamma) = (g'(\alpha)h(\alpha) - g(\alpha)h'(\alpha))\sigma^2 \pmod{\mathcal{P}^n}. \tag{5.15}$$

Claim 5.9 $\mathfrak{d}$ is an essential derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}^n$ which is trivial on $\mathfrak{O}_F$.

If $\gamma = g_j(\alpha)/\beta$ for $j = 1, 2$ are two expressions for $\gamma \in \mathfrak{O}_K$, then

$$g_1(\alpha) - g_2(\alpha) = 0,$$

so there exists a $k(x) \in \mathfrak{O}_F[x]$ such that

$$g_1(x) - g_2(x) = m_{\alpha,F}(x)k(x).$$

Therefore,

$$g_1'(\alpha) - g_2'(\alpha) = m_{\alpha,F}'(\alpha)k'(\alpha) \equiv 0 \pmod{\mathcal{P}^n},$$

where the congruence comes from Theorem 5.9 on page 203, since

$$\mathcal{P}^n \mid \mathcal{D}_{K/F} \mid m_{\alpha,F}'(\alpha)\mathfrak{O}_K.$$

This shows that (5.15) is well-defined.

If we consider the product

$$\frac{g(\alpha)}{\beta} = \gamma = \beta_1\beta_2 = \frac{g_1(\alpha)}{\beta}\frac{g_2(\alpha)}{\beta},$$

then $\beta_1 = \sigma g_1(\alpha)$ and $\beta_2 = \sigma g_2(\alpha)$. Therefore,

$$\begin{aligned}\beta_1\mathfrak{d}(\beta_2) + \beta_2\mathfrak{d}(\beta_1) &\equiv \sigma g_1(\alpha)\left[g_2'(\alpha)h(\alpha) - g_2(\alpha)h'(\alpha)\right]\sigma^2 \\ &+\sigma g_2(\alpha)\left[g_1'(\alpha)h(\alpha) - g_1(\alpha)h'(\alpha)\right]\sigma^2 \\ &\equiv \sigma^3\left(\left[g_1(\alpha)g_2'(\alpha) + g_1'(\alpha)g_2(\alpha)\right]h(\alpha) - 2g_1(\alpha)g_2(\alpha)h'(\alpha)\right) \pmod{\mathcal{P}^n}.\end{aligned} \tag{5.16}$$

Since

$$g_1(\alpha)g_2(\alpha) = \beta g(\alpha) = g(\alpha)h(\alpha),$$

then for some $\ell(x) \in \mathfrak{O}_F[x]$,

$$g_1(x)g_2(x) = g(x)h(x) + m_{\alpha,F}(x)\ell(x).$$

By differentiating the latter, evaluating at $x = \alpha$, and looking at it modulo $\mathcal{P}^n$, we achieve,

$$g_1(\alpha)g_2'(\alpha) + g_1'(\alpha)g_2(\alpha) \equiv g'(\alpha)h(\alpha) + g(\alpha)h'(\alpha) \pmod{\mathcal{P}^n}. \tag{5.17}$$

Hence, by comparing (5.16)–(5.17) and using (5.14), we get

$$\beta_1\mathfrak{d}(\beta_2) + \beta_2\mathfrak{d}(\beta_1) \equiv \sigma^2\left(g'(\alpha)h(\alpha) - g(\alpha)h'(\alpha)\right) \pmod{\mathcal{P}^n},$$

so

$$\beta_1\mathfrak{d}(\beta_2) + \beta_2\mathfrak{d}(\beta_1) = \mathfrak{d}(\beta_1\beta_2).$$

Thus, $\mathfrak{d}$ is a derivation, and it clearly is trivial on $\mathfrak{O}_F$. Since $\mathfrak{d}(\alpha)$ is the identity of $\mathfrak{O}_K/\mathcal{P}^n$, then $\mathfrak{d}$ is essential.

This completes the proof.[5.7] □

We are now in a position to establish the following main result.

[5.7] Observe that (5.15) is the analogue of the quotient rule in elementary calculus.

Theorem 5.11 — Fundamental Theorem of the Different

Let K/F be an extension of number fields, $\mathcal{P}$ a prime $\mathfrak{O}_K$-ideal with $\mathfrak{p}$ the prime $\mathfrak{O}_F$-ideal below it, and set $e = e_{K/F}(\mathcal{P})$. Then

$$\mathcal{P}^{e-1} \mid \mathcal{D}_{K/F}.$$

Furthermore, if $\gcd(e, N^{F/\mathbb{Q}}(\mathfrak{p})) = 1$, then

$$\mathcal{P}^e \nmid \mathcal{D}_{K/F}.$$

Proof. Let $\mathfrak{p}\mathfrak{O}_K = \mathcal{P}^e I$, where $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$, $\mathcal{P} \nmid I$, and $e = e_{K/F}(\mathcal{P})$. If $\beta \in \mathcal{P}I$, there must exist an $n \in \mathbb{N}$ sufficiently large such that

$$\beta^{p^n} \in \mathcal{P}^{p^n} I \subseteq \mathcal{P}\mathfrak{O}_K,$$

where $p = \mathfrak{p} \cap \mathbb{Z}$. By Exercise 5.8 on page 195, there exists a normal extension L of F containing K. Thus, if θ_j for $j = 1, 2, \ldots, d = |L : F|$ are all of the F-isomorphisms of L into $\mathbb{C}$, then for each such j, $\theta_j(\beta^{p^n}) \in \mathfrak{O}_L$. Hence,

$$T_{L/F}(\beta^{p^n}) \in \mathcal{P}\mathfrak{O}_L \cap \mathfrak{O}_F = \mathfrak{p}.$$

Thus, by the Binomial Theorem,

$$T_{L/F}(\beta^{p^n}) - T_{L/K}(\beta)^{p^n} \in \mathfrak{p}.$$

Hence, $T_{L/K}(\beta) \in \mathfrak{p}$, so

$$T_{L/K}(\mathcal{P}I) \subseteq \mathfrak{p}.$$

Therefore, by part 4 of Lemma 5.4 on page 197,

$$\mathcal{P}I \subseteq \mathfrak{p}\mathcal{D}_{K/F}^{-1}.$$

In other words,

$$\mathcal{P}I\mathcal{D}_{K/F} \subseteq \mathfrak{p} \subseteq \mathcal{P}\mathfrak{O}_K = \mathcal{P}^e I.$$

Hence, $\mathcal{D}_{K/F} \subseteq \mathcal{P}^{e-1}$, namely

$$\mathcal{P}^{e-1} \mid \mathcal{D}_{K/F},$$

as required for the first statement.

Now we establish the second statement. By Theorem 5.10, it suffices to prove that every derivation $\mathfrak{d}$ of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}^e$, which is trivial on $\mathfrak{O}_F$, satisfies that $\mathfrak{d}(\beta)$ is a zero divisor for all $\beta \in \mathfrak{O}_K$ such that $\mathfrak{d}(\beta) \neq 0$.

We break this into three cases.

Case 5.1 $\beta \in \mathcal{P} - \mathcal{P}^2$

Let $\alpha \in \mathfrak{p} - \mathfrak{p}^2$. Then there exist γ,$\sigma \in \mathfrak{O}_K - \mathcal{P}$ such that $\alpha = \beta^e\gamma/\sigma$, so

$$\sigma\alpha = \beta^e\gamma.$$

Therefore, since $\alpha \in \mathfrak{O}_F$, and $\mathfrak{d}(\beta^e) = 0$, then

$$0 = \mathfrak{d}(\beta^e\gamma) = \beta^e\mathfrak{d}(\gamma) + \gamma\mathfrak{d}(\beta^e) = \gamma\mathfrak{d}(\beta^e) = \gamma e\beta^{e-1}\mathfrak{d}(\beta),$$

where the last equality is from Exercise 5.15. Since $p \nmid e$, $\gamma \notin \mathcal{P}$, and $\beta^{e-1} \notin \mathcal{P}^e$, then $\mathfrak{d}(\beta)$ is a zero divisor. This completes case 5.1.

Case 5.2 $\beta \in \mathcal{P}^n$ *for* $n \geq 2$.

We may assume that $n < e$, since otherwise $\mathfrak{d}(\beta) = 0$. Also, we may assume that $\beta \notin \mathcal{P}^{n-1}$. Thus, there is a $\rho \in \mathcal{P} - \mathcal{P}^2$ and $\gamma, \sigma \in \mathfrak{O}_K - \mathcal{P}$ such that $\beta = \rho^n\gamma/\sigma$. Therefore, by Exercise 5.15,

$$\mathfrak{d}(\sigma\beta) = \mathfrak{d}(\rho^n\gamma) = \gamma\mathfrak{d}(\rho^n) + \rho^n\mathfrak{d}(\gamma) = \gamma n\rho^{n-1}\mathfrak{d}(\rho) + \rho^n\mathfrak{d}(\gamma),$$

and the right-hand side is an element of $\mathcal{P}^n/\mathcal{P}^e$, so the left-hand side is also such an element. However,

$$\mathfrak{d}(\sigma\beta) = \sigma\mathfrak{d}(\beta) + \beta\mathfrak{d}(\sigma),$$

and $\beta\mathfrak{d}(\sigma) \in \mathcal{P}^n/\mathcal{P}^e$, so $\sigma\mathfrak{d}(\beta) \in \mathcal{P}^n/\mathcal{P}^e$. Consequently, $(\sigma\mathfrak{d}(\beta))^{e-n} \in \mathcal{P}^e$, so since $\sigma \notin \mathcal{P}$, then $\mathfrak{d}(\beta)$ is a zero divisor in $\mathfrak{O}_K/\mathcal{P}^e$. This is Case 5.2.

Case 5.3 $\beta \notin \mathcal{P}$.

By Exercise 4.31 on page 164,

$$\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}},$$

so there exists an $\alpha \in \mathcal{P}$ such that

$$\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-1} = 1 + \alpha.$$

By Exercise 5.15,

$$\mathfrak{d}(\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-1}) = (N_{K/\mathbb{Q}}(\mathcal{P}) - 1)\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-2}\mathfrak{d}(\beta),$$

and we also have that

$$\mathfrak{d}(\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-1}) = \mathfrak{d}(1 + \alpha) = \mathfrak{d}(\alpha),$$

where $\mathfrak{d}(\alpha) \in \mathcal{P}$ is a zero divisor, since $\beta\alpha = \beta(\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-1}) = \beta^{N_{K/\mathbb{Q}}(\mathcal{P})} - \beta \in \mathcal{P}$. Given that $(N_{K/\mathbb{Q}}(\mathcal{P}) - 1)\beta^{N_{K/\mathbb{Q}}(\mathcal{P})-2} \notin \mathcal{P}$, then $\mathfrak{d}(\beta)$ is a zero divisor. This completes Case 5.3, and so the entire result. □

The following consequences of Theorem 5.11 are the promised links between the different and ramification.

Corollary 5.7 If $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal, then $\mathcal{P}$ ramifies in K/F if and only if $\mathcal{P} \mid \mathcal{D}_{K/F}$. Consequently, there are only finitely many ramified primes in K/F.

Proof. The first assertion is immediate from Theorem 5.11. That there are only finitely many follows from the first assertion via Exercise 2.52 on page 86. □

Corollary 5.8 A prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ ramifies in K if and only if $\mathfrak{p} \mid \Delta_{K/F}$.

Proof. If

$$\mathfrak{p} \mid \Delta_{K/F} = N^{K/F}(\mathcal{D}_{K/F}),$$

then $\mathcal{P}|\mathfrak{p}$ for some prime $\mathfrak{O}_K$-ideal dividing $\mathcal{D}_{K/F}$. By Corollary 5.7, $\mathcal{P}$ must ramify in K/F, whence, $\mathfrak{p}$ ramifies in K. Conversely, if $\mathfrak{p}$ ramifies in K, there exists a prime $\mathfrak{O}_K$ ideal $\mathcal{P}$ above $\mathfrak{p}$ which ramifies in K/F. By Corollary 5.7, $\mathcal{P} \mid \mathcal{D}_{K/F}$, so

$$\mathfrak{p} \mid \mathfrak{p}^{f_{K/F}(\mathcal{P})} = N^{K/F}(\mathcal{P}) \mid N^{K/F}(\mathcal{D}_{K/F}) = \Delta_{K/F},$$

which follows from Exercise 2.46 on page 86. □

The interpretation of Theorem 5.11 on the preceding page will be expanded in §5.3 when we introduce ramified and unramified field extensions.

Biography 5.1 André Weil, pronounced *vay*, (1906–1998) was born on May 6, 1906 in Paris, France. As he said in his autobiography, *The Apprenticeship of a Mathematician*, he was passionately addicted to mathematics by the age of ten. He was also interested in languages, as evidenced by his having read the *Bhagavad Gita* in its original Sanskrit at the age of sixteen. After graduating from the École Normal in Paris, he eventually made his way to Göttingen, where he studied under Hadamard. His doctoral thesis contained a proof of the Mordell-Weil Theorem, namely that the group of rational points on an elliptic curve over $\mathbb{Q}$ is a finitely generated abelian group. His first position was at Aligarh Muslim University, India (1930–1932), then the University of Strasbourg, France (1933–1940), where he became involved with the controversial *Bourbaki project*, which attempted to give a unified description of mathematics. The name *Nicholas Bourbaki* was that of a citizen of the imaginary state of Poldavia, which arose from a spoof lecture given in 1923. Weil tried to avoid the draft, which earned him six months in prison. It was during this imprisonment that he created the Riemann hypothesis—see Hypothesis B.1 on page 354. In order to be released from prison, he agreed to join the French army. Then he came to the United States to teach at Haverford College in Pennsylvania. He also held positions at Sao Paulo University, Brazil (1945–1947), the University of Chicago (1947–1958), and thereafter at the Institute for Advanced Study at Princeton. In 1947 at Chicago, he began a study, which eventually led him to a proof of the Riemann hypothesis for algebraic curves. He went on to formulate a series of conjectures that won him the Kyoto prize in 1994 from the Inamori Foundation of Kyoto, Japan. His conjectures provided the principles for modern algebraic geometry. His honours include an honorary membership in the London Mathematical Society in 1959, and election as a Fellow of the Royal Society of London in 1966. However, in his own official biography he lists his only honour as *Member, Poldevian Academy of Science and Letters.* He is also known for having said *In the future, as in the past, the great ideas must be the simplifying ideas*, as well as *God exists since mathematics is consistent, and the devil exists since we cannot prove it.* This is evidence of his being known for his poignant phrasing and whimsical individuality, as well as for the depth of his intellect. He died on August 6, 1998 in Princeton, and is survived by two daughters, and three grandchildren. His wife Eveline died in 1986.

Exercises

5.12. Let K/F be an extension of number fields, and let $\alpha \in \mathfrak{O}_K$ such that $K = F(\alpha)$. Prove that $m'_{\alpha,F}(\alpha)\mathfrak{O}_K \subseteq \mathfrak{O}_F[\alpha]$.

5.13. Let K/F be an extension of number fields, and let $\alpha \in \mathfrak{O}_K$ such that $K = F(\alpha)$. Prove that $(\mathfrak{O}_K^*)^{-1} = \mathfrak{O}_K m'_{\alpha,F}(\alpha)$ if and only if $\mathfrak{O}_K = \mathfrak{O}_F[\alpha]$. (*Hint: Use the Lagrange Interpolation Formula in Appendix A.*)

5.14. Let K/F be an extension of fields. Show that the set of all derivations of F in K form a vector space over K. For two given such derivations $\mathfrak{d}_1$, $\mathfrak{d}_2$, define the *bracket operation*,

$$[\mathfrak{d}_1, \mathfrak{d}_2] = \mathfrak{d}_2\mathfrak{d}_1 - \mathfrak{d}_1\mathfrak{d}_2.$$

Show that the bracket operation is a derivation of F into K. Furthermore, for any three such derivations $\mathfrak{d}_j$ for $j = 1, 2, 3$, establish the *Jacobi identity*:

$$[[\mathfrak{d}_1, \mathfrak{d}_2], \mathfrak{d}_3] + [[\mathfrak{d}_2, \mathfrak{d}_3], \mathfrak{d}_1] + [[\mathfrak{d}_3, \mathfrak{d}_1], \mathfrak{d}_2] = 0.$$

(*Hint: In the process of verification, establish and use the fact that the bracket operation is anticommutative, namely that* $[\mathfrak{d}_1, \mathfrak{d}_2] = -[\mathfrak{d}_2, \mathfrak{d}_1]$.) (The resulting vector space with the bracket operation forms a nonassociative algebra, called a *Lie Algebra*, over K, and the bracket operation is called a *Lie Product*, or *commutator product.*)

5.15. Let S be a commutative ring with identity and R a subring, and $\mathfrak{d}$ a derivation of R into S. Prove that for all $n \in \mathbb{N}$ and $\alpha \in R$,

$$\mathfrak{d}(\alpha^n) = n\alpha^{n-1}\mathfrak{d}(\alpha).$$

5.16. Let K/F be an extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Suppose that for a given $n \in \mathbb{N}$,

$$\mathfrak{d} : \mathfrak{O}_K \mapsto \frac{\mathfrak{O}_K}{\mathcal{P}^n}$$

is a derivation of $\mathfrak{O}_K$ into $\mathfrak{O}_K/\mathcal{P}^n$. Prove that $\mathfrak{d}(\alpha) = 0$ for all $\alpha \in \mathcal{P}^{n+1}$.

5.17. Let $F = \mathbb{Q}(\sqrt{10})$, and $I = (2, \sqrt{10})$. Find I^*, $\mathcal{D}_{F/\mathbb{Q}}(\mathcal{I})$, $\mathcal{D}_{F/\mathbb{Q}}$, $I^{*^{-1}}$ and$\Delta_{\ F/\mathbb{Q}}$.

5.18. With reference to Exercise 5.17, find $\mathfrak{f}_{\sqrt{10}}$.

Biography 5.2 Marius Sophus Lie (1842–1899) was born on December 17, 1842 in Nordfjordeid, Norway. Ludwig Sylow (1832–1918) was one of Lie's teachers at the University of Christiana (which became Oslo in 1925), from which he graduated in 1865. In 1869, Lie went to Berlin where he met Felix Klein (1849–1925). This began a collaborative effort that resulted in several joint publications. Among the consequences of this work is Klein's characterization of geometry involving properties invariant under group actions, which was established in 1872. As a result of the Franco-German war of 1870, both Lie and Klein left France. Lie planned to go to Italy, but was arrested as a German spy, with the unfortunate assumption being made that his mathematical notes were coded messages. Only after the intervention of Gaston Darboux (1842–1917), a leading French geometer at the time, did Lie get released. Lie then returned to Christiana, and obtained his doctorate there. He began an investigation of differential equations in an attempt to find an analogue of Galois theory. Ultimately, he was led to a structure that we now call a Lie algebra. He abandoned the study of partial differential equations in favour of his new structure. In 1900, Elie Cartan (1869–1951) published the classification of semisimple Lie algebras. However, Wilhelm Killing (1847–1923) had independently introduced Lie algebras with a different purpose since his interest was non-Euclidean geometry. Lie collaborated for about a decade with Friedrich Engel (1861–1941). Their joint publication in 1893, *Theorie der Tansformationgruppen* appeared in three volumes, and perhaps best represents Lie's major work on continuous groups of transformations. Engel was sent by Klein to study under Lie. Engel became Lie's assistant in 1892 when Lie succeeded Klein for his chair at Leipzig. In 1898, Lie returned to Kristiana, the intermediate name taken by Christiana before it became Oslo. There he took a chair that had been specially created for him. However, he died shortly thereafter on February 18, 1899.

5.3 Ramification

Everything is what it is, and not another thing.

Joseph Butler (1692–1752)
English bishop and theologian

In this section we look at the following concept in extensions of number fields employing the notions presented in §5.2

Definition 5.11 — Ramified and Unramified Extensions

If K/F is an extension of number fields such that there does not exist a prime $\mathfrak{O}_K$-ideal, which is ramified in K/F, then the extension is said to be *unramified.*[5.8] At the other end of the spectrum are those extensions for which there exists a prime $\mathfrak{O}_K$-ideal $\mathcal{P}$ with

$$e_{K/F}(\mathcal{P}) = |K : F|,$$

in which case the extension is called totally ramified, *fully ramified*, or *purely ramified* at $\mathcal{P}$. If $\mathcal{P}$ is a ramified prime $\mathfrak{O}_K$-ideal with

$$\mathcal{P} \cap \mathbb{Z} = (p), \text{ and } p \nmid e_{K/F}(\mathcal{P}),$$

then $\mathcal{P}$ is said to be *tamely ramified* in K/F. An extension K/F is said to be *tamely ramified*, provided that all ramified primes in K/F are tamely ramified. Thus, in particular, unramified extensions are tamely ramified. When p divides $e_{K/F}(\mathcal{P})$, then $\mathcal{P}$ is called wildly ramified, and the extension is called wildly ramified at $\mathcal{P}$.

Corollary 5.9 If $K/\mathbb{Q}$ is an unramified extension, then $K = \mathbb{Q}$.

Proof. By Remark 3.14 on page 116, if $K \neq \mathbb{Q}$, then $|\Delta_{K/\mathbb{Q}}| > 1$. Therefore, there must exist a ramified prime in $K/\mathbb{Q}$, by Corollary 5.8 on page 210. □

Remark 5.3 In view of Definition 5.11, the Fundamental Theorem of the Different, Theorem 5.11 on page 209, says that any tamely ramified prime $\mathfrak{O}_K$-ideal $\mathcal{P}$ in K/F satisfies the property that

$$\mathcal{P}^{e-1} \mid \mathfrak{D}_{K/F}, \text{ but } \mathcal{P}^e \nmid \mathfrak{D}_{K/F}, \text{ where } e = e_{K/F}(\mathcal{P}).$$

Hence, if K/F is normal, then $\mathfrak{p}^n \nmid \Delta_{K/F}$, where $\mathfrak{p} = \mathcal{P} \cap F$, and $n = |K : F|$—see Exercise 5.20 on page 219. Later, we will see that the converse is also true, namely, that a normal extension for which$\Delta_{\ K/F}$ is not divisible by the n^{th} power of a prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ must be tamely ramified at $\mathfrak{p}$—see Exercise 5.46 on page 253.

Now we look at ramification in composita of number fields—see Application A.1 on page 325 and the discussion surrounding it.

[5.8] This includes the so-called *infinite primes*, namely the embeddings of F into $\mathbb{C}$. This is the term used in class-field theory—see Theorem 5.21 on page 239. In an arbitrary extension K/F of number fields, a real embedding of F into $\mathbb{C}$ that extends to a complex embedding of K into $\mathbb{C}$ is said to *ramify*—see Exercise 2.11 on page 63. Thus, these infinite "primes" that ramify must be excluded as well. We explore and develop the notion of these infinite primes in Exercise 5.24 on page 220. The primes that are not infinite are called the *finite primes.*

Theorem 5.12 — Ramification in a Compositum of Number Fields
Let the number fields K_j for $j = 1, 2$ be extensions of the number field F, and let $L = K_1K_2$ be the compositum of K_1 and K_2 over F. Then a prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ divides$\Delta_{L/F}$ if and only if it divides$\Delta_{K_1/F}\Delta_{K_2/F}$.

Proof. By Lemma 5.5 on page 198, any prime divisor of$\Delta_{K_1/F}\Delta_{K_2/F}$ is a divisor of$\Delta_{L/F}$. Conversely, assume that the prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ divides$\Delta_{L/F}$, and $\mathfrak{p} \nmid \Delta_{K_1/F}$. Thus, there exists a prime $\mathfrak{O}_L$-ideal $\mathcal{P}$ such that $\mathcal{P} \mid \mathcal{D}_{L/F}$ and $\mathcal{P}$ lies over $\mathfrak{p}$. Since

$$\mathcal{D}_{L/F} = \mathcal{D}_{L/K_1}\mathcal{D}_{K_1/F},$$

by part 2 of Lemma 5.4 on page 197, then $\mathcal{P} \nmid \mathcal{D}_{K_1/F}\mathfrak{O}_{K_1}$. Thus, $\mathcal{P} \mid \mathcal{D}_{L/K_1}$. Select $\alpha \in \mathfrak{O}_{K_2}$ such that $K_2 = F(\alpha)$. Then, by Theorem 1.23 on page 38,

$$m_{\alpha,F}(x) = m_{\alpha,K_1}(x)f(x),$$

for some $f(x) \in K_1[x]$. Therefore,

$$m'_{\alpha,F}(\alpha) = m'_{\alpha,K_1}(\alpha)f(\alpha).$$

This implies that

$$m'_{\alpha,F}(\alpha) \in m'_{\alpha,K_1}(\alpha)\mathfrak{O}_K.$$

However, by Theorem 5.9 on page 203,

$$m'_{\alpha,K_1}(\alpha) \in \mathcal{D}_{L/K_1},$$

and since $\mathcal{P} \mid \mathcal{D}_{L/K_1}$, then

$$\mathcal{D}_{L/K_1} \subseteq \mathcal{P}.$$

Therefore, $m'_{\alpha,K_1}(\alpha) \in \mathcal{P}$, so $m'_{\alpha,F}(\alpha) \in \mathcal{P}$. Hence, by Theorem 5.9 again $\mathcal{D}_{K_2/F} \subseteq \mathcal{P}$, so $\mathcal{P} \mid \mathcal{D}_{K_2/F}$, as required. □

Corollary 5.10 If K_j/F is unramified for $j = 1, 2$, then K_1K_2/F is unramified.

Proof. This is immediate from Theorem 5.12, and Corollary 5.8 on page 210. □

Corollary 5.11 Let $F \subseteq K \subseteq L$ be a tower of number fields, where L is the smallest extension field of F containing K such that L is normal over F. Suppose that $\mathfrak{p}$ is a nonzero prime $\mathfrak{O}_F$-ideal. Then$\Delta_{L/F}$ and$\Delta_{K/F}$ have the same prime divisors, so $\mathfrak{p}$ is unramified in L/F if and only if $\mathfrak{p}$ is unramified in K/F.

Proof. Let θ_j for $j = 1, 2, \ldots, n$ be all of the embeddings of K into $\mathbb{C}$. Then

$$L = K^{\theta_1}K^{\theta_2}\cdots K^{\theta_n},$$

the compositum of all the embeddings. The result now follows from Theorem 5.12, and Lemma 5.5. □

Remark 5.4 The above results set the stage for later when we develop the so-called Hilbert class field, which is the maximal, unramified, normal extension of a given number field such that the Galois group is abelian. This Galois group will be shown to be isomorphic to the class group of the base field via the celebrated Frobenius automorphism. The Hilbert class field is called the maximal abelian unramified extension of the base field. There is much power yet to be developed.

We continue with further results on composita of number fields and their discriminants.

Theorem 5.13 — Discriminants and Degrees of Composita
Let K_j for $j = 1, 2$ be number fields with

$$\gcd(\Delta_{K_1}, \Delta_{K_2}) = 1,$$

and

$$|K_j : \mathbb{Q}| = n_j.$$

Then each of the following holds, where $L = K_1K_2$ is their compositum.

(a) $|L : \mathbb{Q}| = n_1n_2$.

(b) $\mathfrak{O}_L = \mathfrak{O}_{K_1}\mathfrak{O}_{K_2}$, and if $\{\alpha_1, \ldots, \alpha_{n_1}\}$ and $\{\beta_1, \ldots, \beta_{n_2}\}$ are integral bases of K_1 and K_2, respectively, then $\{\alpha_i\beta_j\}$ for $1 \le i \le n_1$, $1 \le j \le n_2$ is an integral basis for L.

(c) $\Delta_L = \Delta_{K_1}^{n_2}\Delta_{K_2}^{n_1}$.

Proof. (a) We have

$$|L : \mathbb{Q}| = |L : K_2| \cdot |K_2 : \mathbb{Q}| = |L : K_2|n_2.$$

If $|L : \mathbb{Q}| < n_1n_2$, then $|L : K_2| < n_1$. Let $K = \mathbb{Q}(\alpha)$. Then $m_{\alpha,K_2}(x) \mid m_{\alpha,\mathbb{Q}}(x)$. If F is the subfield of K_2 generated by the coefficients of $m_{\alpha,K_2}(x)$, then $F \ne \mathbb{Q}$. Since $F \subseteq K_2$, then $\Delta_F \mid \Delta_{K_2}$, by Theorem 3.15 on page 126. Since the coefficients of $m_{\alpha,K_2}(x)$ are elementary symmetric functions—see Definition A.16 on page 333—of the *roots* of $m_{\alpha,K_2}(x)$, then $m_{\alpha,K_2}(x) \in N_1[x]$, where N_1 is the smallest Galois extension of $\mathbb{Q}$ containing K_1. Therefore, $F \subseteq N_1$, so as above$\Delta_F \mid \Delta_{N_1}$. Let $p \mid \Delta_F$ be a prime. Then $p \mid \Delta_{N_1}$ and $p \mid \Delta_{K_2}$, so $p \mid \Delta_{K_1}$, by Corollary 5.11, contradicting the hypothesis that $\gcd(\Delta_1, \Delta_2) = 1$. This is (a).

(b) Since $\mathfrak{O}_{K_1}\mathfrak{O}_{K_2}$ is the smallest subring of $\mathfrak{O}_L$ containing both $\mathfrak{O}_{K_1}$ and $\mathfrak{O}_{K_2}$, then $\{\alpha_i\beta_j\}$ for $1 \le i \le n_1$, $1 \le j \le n_2$, is a $\mathbb{Z}$-basis for $\mathfrak{O}_{K_1}\mathfrak{O}_{K_2}$. Therefore,

$$\operatorname{disc}(\{\alpha_i\beta_j\}) = \det(\sigma_i\theta_j(\alpha_k\beta_\ell))^2, \tag{5.18}$$

where the σ_i are the $\mathbb{Q}$-isomorphisms of K_1 and the θ_j are the $\mathbb{Q}$-isomorphisms of K_2. The determinant in (5.18) is the Kronecker product

$$\det(\sigma_i(\alpha_k))^{2n_2} \times \det(\theta_j(\beta_\ell))^{2n_1} = \Delta_{K_1}^{n_2}\Delta_{K_2}^{n_1}$$

—see Definition A.21 on page 339. Thus, by the very definition of a field discriminant given in Definition 2.7 on page 77, $\{\alpha_i\beta_j\}$ is an integral basis for L.

(c) By Lemma 5.5 on page 198,

$$\Delta_{L/\mathbb{Q}} = \Delta_{K_1/\mathbb{Q}}^{|L:K_1|}N^{K_1/\mathbb{Q}}(\Delta_{L/K_1}) = \Delta_{K_1/\mathbb{Q}}^{n_2}N^{K_1/\mathbb{Q}}(\Delta_{L/K_1}),$$

and similarly

$$\Delta_{L/\mathbb{Q}} = \Delta_{K_2/\mathbb{Q}}^{n_1}N^{K_2/\mathbb{Q}}(\Delta_{L/K_2}).$$

Hence,$\Delta_{K_1}^{n_2}$ and$\Delta_{K_2}^{n_1}$ both divideΔ_L, and since $\gcd(\Delta_{K_1}, \Delta_{K_2}) = 1$, then

$$\Delta_{K_1}^{n_2}\Delta_{K_2}^{n_1} \mid \Delta_L.$$

Since $\operatorname{disc}(\{\alpha_i\beta_j\}) = \Delta_{K_1}^{n_2}\Delta_{K_2}^{n_1}$ by part (b), then$\Delta_L = \Delta_{K_1}^{n_2}\Delta_{K_2}^{n_1}$. □

The following application of Theorem 5.13 fulfills the promise made at the top of page 126.

Theorem 5.14 — Discriminants of Cyclotomic Fields
Let $n \in \mathbb{N}$, $n > 2$ and set $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. If $n = \prod_{j=1}^{r} p_j^{a_j}$ for distinct primes p_j and $a_j \in \mathbb{N}$, then

$$\Delta_K = \prod_{j=1}^{r} \Delta_{\mathbb{Q}(\zeta_{p_j^{a_j}})}^{\phi(n/p_j^{a_j})} = \frac{(-1)^{\phi(n)r/2} n^{\phi(n)}}{\prod_{j=1}^{r} p_j^{\phi(n)/(p_j-1)}}.$$

Proof. We use induction on r. Corollary 3.9 on page 125 establishes the induction step $r = 1$, so we assume the induction hypothesis, that the result holds for $r - 1$, where $r > 1$. Thus, by Corollary 3.9, and the induction hypothesis,

$$\gcd(\Delta_{\mathbb{Q}(\zeta_{n'})}, \Delta_{\mathbb{Q}(\zeta_{p_r^{a_r}})}) = 1,$$

where $n' = n/p_r^{a_r}$. Therefore, by part (b) of Theorem 5.13,

$$\Delta_K = \prod_{j=1}^{r} \Delta_{\mathbb{Q}(\zeta_{p_j^{a_j}})}^{\phi(n/p_j^{a_j})} = \Delta_{\mathbb{Q}(\zeta_{n'})}^{\phi(p_r^{a_r})} \Delta_{\mathbb{Q}(\zeta_{p_r^{a_r}})}^{\phi(n')}.$$

However, by the induction hypothesis,

$$\Delta_{\mathbb{Q}(\zeta_{n'})}^{\phi(p_r^{a_r})} = \frac{(-1)^{\phi(n')\phi(p_r^{a_r})(r-1)/2} (n')^{\phi(n')\phi(p_r^{a_r})}}{\prod_{j=1}^{r-1} p_j^{(\phi(n')/(p_j-1))\phi(p_r^{a_r})}} = \frac{(-1)^{\phi(n)(r-1)/2} (n')^{\phi(n)}}{\prod_{j=1}^{r-1} p_j^{\phi(n)/(p_j-1)}},$$

and by Corollary 3.9, (or the induction hypothesis),

$$\Delta_{\mathbb{Q}(\zeta_{p_r^{a_r}})}^{\phi(n')} = \frac{(-1)^{(\phi(p_r^{a_r})/2)\phi(n')} p_r^{a_r\phi(p_r^{a_r})\phi(n')}}{p_r^{(\phi(p_r^{a_r})/(p_r-1))\phi(n')}} = \frac{(-1)^{\phi(n)/2} p_r^{a_r\phi(n)}}{p_r^{\phi(n)/(p_r-1)}}.$$

Hence, by multiplying the last two expressions together, we get the final result. □

Corollary 5.12 A rational prime q is ramified in $\mathbb{Q}(\zeta_n)$ if and only if $q \mid n$.

Proof. This follows from Theorem 5.14 via Corollary 5.8 on page 210. □

We conclude this section with a result on prime decomposition, without ramification, in a cyclotomic extension.

Theorem 5.15 — Prime Factorization in Cyclotomic Extensions
Let K be a number field, and $n \in \mathbb{N}$. Set $L = K(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. Suppose that $\mathfrak{p}$ is a prime $\mathfrak{O}_K$-ideal with $n \notin \mathfrak{p}$, and

$$f_{K/\mathbb{Q}}(\mathfrak{p}) = e_{K/\mathbb{Q}}(\mathfrak{p}) = 1.$$

If $f \in \mathbb{N}$ is the smallest value such that $p^f \equiv 1 \pmod{n}$, where $(p) = \mathfrak{p} \cap \mathbb{Z}$, then

$$\mathfrak{p}\mathfrak{O}_L = \mathcal{P}_1 \cdots \mathcal{P}_g,$$

where the $\mathcal{P}_j$ are distinct prime $\mathfrak{O}_L$-ideals with $f_{L/K}(\mathcal{P}_j) = f$ for each $j = 1, 2, \ldots, n$ and

$$fg = |L : K|.$$

Proof. The extension L/K is normal since any K-isomorphism θ of L satisfies $\theta(L) = L$. Hence, we need only show that $f_{L/K}(\mathfrak{p}) = f$, since once this fact is proved, the remaining facts fall into place as an immediate consequence of Theorem 5.4 on page 189. To see that $\mathfrak{p}$ is unramified in L/K, use Corollaries 5.10 on page 214 and 5.12 on the preceding page.

Claim 5.10 *If $\mathfrak{f}_{\zeta_n}$ is the conductor of $\mathfrak{O}_K[\zeta_n]$ in $\mathfrak{O}_L$, then $\mathfrak{f}_{\zeta_n} \mid n\mathfrak{O}_L$.*

First, we have that

$$x^n - 1 = m_{\zeta_n,K}(x)g(x),$$

for some $g(x) \in \mathfrak{O}_K[x]$. Therefore, by taking derivatives and setting $x = \zeta_n$, we get

$$n\zeta_n^{n-1} = \delta_{L/K}(\zeta_n)g(\zeta_n).$$

Since $\zeta_n^{n-1} \in \mathfrak{U}_{\mathfrak{O}_L}$, then

$$\delta_{L/K}(\zeta_n)\mathfrak{O}_L \mid n\mathfrak{O}_L.$$

Thus, $\mathfrak{f}_{\zeta_n} \mid n\mathfrak{O}_L$, by Lemma 5.6 on page 202, which secures Claim 5.10.

By Claim 5.10, and by part (a) of Exercise 5.19 on page 219,

$$N^{L/K}(\mathfrak{f}_{\zeta_n}) \mid n^{|L:K|}\mathfrak{O}_K.$$

Therefore, since $n \notin \mathfrak{p}$, then $\mathfrak{p} \nmid N^{L/K}(\mathfrak{f}_{\zeta_n})$. This allows us to invoke Exercise 5.23 on page 219. Hence, for each $\gamma \in \mathfrak{O}_L$, there exists a polynomial $k(x) \in \mathfrak{O}_K[x]$ such that

$$\gamma \equiv k(\zeta_n) \pmod{\mathfrak{p}\mathfrak{O}_L}.$$

Thus, by the Binomial Theorem—see Corollary A.11 on page 341—

$$\gamma^{N(\mathfrak{p})^f} \equiv k(\zeta_n)^{N(\mathfrak{p})^f} \equiv k(\zeta_n^{N(\mathfrak{p})^f}) \equiv k(\zeta_n) \pmod{\mathfrak{p}\mathfrak{O}_L},$$

where we are using Definition 2.8 on page 83 for the norm exponents. Thus,

$$\gamma^{N(\mathfrak{p})^f} \equiv \gamma \pmod{\mathcal{P}_j},$$

for each $j = 1, 2, \ldots, g$. By Exercises 4.30–4.31 on pages 163–164, the exponent m given by,

$$(m) = N^{L/\mathbb{Q}}(\mathcal{P}_j) = N^{K/\mathbb{Q}}(\mathfrak{p})^{f_{L/K}(\mathfrak{p})}$$

is the smallest one such that

$$\gamma^m \equiv \gamma \pmod{\mathcal{P}_j},$$

for all $\gamma \in \mathfrak{O}_L$ and a given $j = 1, 2, \ldots, g$. Therefore, $f_{L/K}(\mathfrak{p}) \le f$. If

$$N^{L/\mathbb{Q}}(\mathcal{P}_j)^{f_{L/K}(\mathfrak{p})} \not\equiv 1 \pmod{n}, \tag{5.19}$$

then $\zeta_n^{f_{L/K}(\mathfrak{p})} \ne \zeta_n$ is a primitive n^{th} root of unity, and

$$\zeta_n^{f_{L/K}(\mathfrak{p})} - \zeta_n \in \mathcal{P}_j.$$

Hence, we have the basis discriminant containment:

$$\operatorname{disc}(\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)}\}) \in \mathcal{P}_j.$$

Thus,

$$\operatorname{disc}(\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)}\}) \in \mathcal{P}_j \cap \mathbb{Z} = (p),$$

where the prime p does not divide n. Since

$$\operatorname{disc}(\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)}\}) = \Delta_{\mathbb{Q}(\zeta_n)}$$

by Definition 2.7 on page 77, and Theorem 3.14 on page 123, then this contradicts Corollary 5.12 on page 216. Hence, the assumption (5.19) was incorrect, so

$$N(\mathcal{P}_j)^{f_{L/K}(\mathfrak{p})} \equiv 1 \pmod{n},$$

and $f \le f_{L/K}(\mathfrak{p})$, by the minimality of the choice of f. Hence, $f = f_{L/K}(\mathfrak{p})$. □

Corollary 5.13 Let $K = \mathbb{Q}(\zeta_n)$ for $n \in \mathbb{N}$ with $n > 2$. Suppose that p is a rational prime, with $n = p^a n'$, where a is a nonnegative integer, $p \nmid n'$, and f is the least natural number such that $p^f \equiv 1 (\text{mod } n')$, then

$$p\mathfrak{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_g,$$

where

$$e_{K/\mathbb{Q}}(p) = \phi(p^a) \ge 1,\ fg = \phi(n'),$$

and all $\mathcal{P}_j$ distinct prime $\mathfrak{O}_K$-ideals with

$$f_{K/\mathbb{Q}}(\mathcal{P}_j) = f = f_{K/\mathbb{Q}}(p).$$

Proof. If $n = n'$, namely when $a = 0$, then the result is an immediate consequence of Theorem 5.15 on page 216. If $a \in \mathbb{N}$, then let $F = \mathbb{Q}(\zeta_{n'})$. Therefore,

$$|F : \mathbb{Q}| = \phi(n'), \text{ and } |K : \mathbb{Q}| = \phi(n),$$

so

$$|K : F| = \phi(n)/\phi(n') = \phi(p^a) = |\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}|,$$

via Corollary 1.17 on page 41. By Theorem 5.15,

$$p\mathfrak{O}_F = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

for distinct prime $\mathfrak{O}_F$-ideals $\mathfrak{p}_j$, $j = 1, \ldots, g$, and $g = \phi(n')/f$. Moreover,

$$p\mathfrak{O}_K = (\mathcal{P}_1 \cdots \mathcal{P}_m)^e \tag{5.20}$$

for some $m, e \in \mathbb{N}$. However, by Theorem 5.4 on page 189,

$$mef_{K/\mathbb{Q}}(\mathcal{P}_j) = |K : \mathbb{Q}| = \phi(n).$$

Since p is not ramified in $F/\mathbb{Q}$, then $e \bigm| |K : F| = \phi(p^a)$. By Example 5.8 on page 190,

$$p = u(1 - \zeta_{p^a})^{\phi(p^a)},$$

where $u \in \mathfrak{U}_{\mathbb{Z}[\zeta_{p^a}]}$, so using (5.20), we get

$$p\mathfrak{O}_K = (1 - \zeta_{p^a})^{\phi(p^a)}\mathfrak{O}_K = (\mathcal{P}_1 \cdots \mathcal{P}_m)^e,$$

but $e \bigm| \phi(p^a)$, so $e = \phi(p^a)$ is forced. Since $m \ge g$, given that each $\mathfrak{p}_j$ could decompose further in K/F, it remains to show that $m \le g$. Since

$$m\phi(p^a)f_{K/\mathbb{Q}}(\mathcal{P}_j) = \phi(n) = \phi(p^a)\phi(n'),$$

then

$$mf_{K/\mathbb{Q}}(\mathcal{P}_j) = \phi(n'),$$

but we also have that

$$fg = \phi(n'), \text{ and } f_{K/\mathbb{Q}}(\mathcal{P}_j) = f_{K/F}(\mathcal{P}_j)f.$$

Hence, $mf_{K/F}(\mathcal{P}_j) = g$, so $g \geq m$, thereby completing the proof. □

In §5.4 we marry the Galois theory developed in §2.1 with the results developed thus far in this chapter to further develop the theory of decomposition of ideals in number fields.

Exercises

5.19. Let K/F be an extension of number fields, and let I, J be $\mathfrak{O}_K$-ideals. Establish each of the following.

(a) If $I \subseteq J$, then $N^{K/F}(I) \subseteq N^{K/F}(J)$.

(b) If I and $N^{K/F}(J)\mathfrak{O}_K$ are relatively prime, then $N^{K/F}(I)$ and $N^{K/F}(J)$ are relatively prime $\mathfrak{O}_F$-ideals.

(*Hint: Use Corollary 1.7 on page 27.*)

5.20. Let K/F be a normal extension of number fields, and let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal that is tamely ramified in K. Prove that

$$\mathfrak{p}^n \nmid \Delta_{K/F},$$

where $n = |K : F|$.

(*Hint: Use Theorem 5.5 on page 190, Theorem 5.11 on page 209, and part 3 of Lemma 5.4 on page 197.*)

5.21. Let K_j/F for $j = 1, 2$ be an extension of number fields, and let $L = K_1K_2$ be their compositum. Prove that

$$\mathcal{D}_{L/K_2} \mid \mathcal{D}_{K_1/F}\mathfrak{O}_L.$$

(*Hint: Use Theorem 5.9 on page 203.*)

5.22. Let K_j/F for $j = 1, 2$ be an extension of number fields, and let $L = K_1K_2$ be their compositum. Prove that

$$N^{K_2/F}(\Delta_{L/K_2}) \mid \Delta_{K_1/F}^{|L:K_1|},$$

and

$$N^{K_1/F}(\Delta_{L/K_1}) \mid \Delta_{K_2/F}^{|L:K_2|}.$$

(*Hint: Use Exercise 5.21 in conjunction with Exercise 5.6 on page 195.*)

5.23. Let L/K be an extension of number fields with $L = K(\alpha)$ for some $\alpha \in \mathfrak{O}_L$. Suppose that $\mathfrak{p}$ is a prime $\mathfrak{O}_K$-ideal such that

$$\mathfrak{p} \nmid N^{L/K}(\mathfrak{f}_\alpha).$$

Prove that for any $\gamma \in \mathfrak{O}_L$, there exists a $k(x) \in \mathfrak{O}_K[x]$ such that

$$\gamma \equiv k(\alpha) \pmod{\mathfrak{p}\mathfrak{O}_L}.$$

(*Hint: Use Theorem 1.21 on page 32.*)

In the next exercise, we develop the notion of an infinite prime first mentioned in Footnote 5.8 on page 213. To do so we make use of valuation theory a complete overview of which may be found in [54, Chapter 6].

First of all, an absolute value on a field F *is a function* $|\cdot| : F \mapsto \mathbb{R}$ *satisfying each of the following.*

(a) $|x| \geq 0$ for all $x \in F$ and $|x| = 0$ if and only if $x = 0$.

(b) $|x \cdot y| = |x| \cdot |y|$ for all $x, y \in F$.

(c) $|x + y| \leq |x| + |y|$ for all $x, y \in F$. (Triangle inequality)

If the triangle inequality can be replaced by the condition

$$|x + y| \leq \max\{|x|, |y|\} \textit{ for all } x, y \in F, \tag{5.21}$$

then the absolute value is said to be a non-Archimedean valuation, *and otherwise it is called an* Archimidean valuation.

Two valuations $|x|$ *and* $|x|_1$ *are said to be* equivalent *if* $|x| < 1$ *holds if and only if* $|x|_1 < 1$, *which is an equivalence relation—see Exercise 1.8 on page 6. An* equivalence class *of valuations on a field F is called a* prime *of* F, *denoted by* $\mathfrak{p}$, *with the valuation in* $\mathfrak{p}$ *denoted by* $|\cdot|_{\mathfrak{p}}$ *and its value at* x *denoted by* $|x|_{\mathfrak{p}}$. *An equivalence class of Archimedean valuations is called an* infinite prime *of* F *and an equivalence class of non-Archimedean valuations is called a* finite prime *of* F.

If $\mathfrak{p}$ *is an infinite prime of* F *and* $\theta : F \mapsto \mathbb{C}$ *is an embedding of* F *into* $\mathbb{C}$ *such that* $|\theta(x)|$ *is in* $\mathfrak{p}$ *and* θ *is a complex embedding, then* $\mathfrak{p}$ *is called a* complex prime, *and if* θ *is a real embedding, then it is called a* real prime*—see Exercise 2.11 on page 63 for the definitions of real and complex embeddings.*

If K/F *is an extension of number fields then extensions of* $\mathfrak{p}$ *to primes of* K *are described as follows. By Exercise 2.6 on page 63,* θ *extends to exactly* $g = |K : F|$ F*-isomorphisms* $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ *of* K, *which are infinite primes of* K *and that are the extensions of* $\mathfrak{p}$. *To be consistent with the finite case we write*

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g.$$

5.24. Let K/F be an extension of number fields and $\mathfrak{p}$ be an infinite prime of F with $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ the primes of K that extend $\mathfrak{p}$. Let the ramification number $e_i = e_{K/f}(\mathfrak{P}_i)$ equal 2 if $\mathfrak{p}$ is real and $\mathfrak{P}_i$ is complex and $e_i = 1$ otherwise. Set $f_i = F_{K/F}(\mathcal{P}_i) = 1$ in all cases. Prove that

$$\sum_{i=1}^{g} e_i f_i = |K : F|.$$

In the remaining exercises, we provide applications of the above-defined valuations.

5.25. If F is a field and α,$\beta \in F$ with $|\alpha| < |\beta|$ for a non-Archimedian valuation $|\cdot|$, prove that $|\alpha + \beta| = |\beta|$.

(*This says that, with respect to* $|\cdot|$, *every triangle is isosceles.*)

5.26. Suppose that F is a field with a non-Archimedean valuation $|\cdot|$. Prove that the valuation of F can be extended to the polynomial ring $F[x]$ by defining the absolute value of $f(x) = a_0 + a_1 x + \cdots a_n x^n$ to be $|f| = \max\{|a_0|, \ldots, |a_n|\}$.

5.4 Galois Theory and Decomposition

> *Trivial personalities decomposing in the eternity of print.*
>
> **Virginia Woolf (1882–1941)**
>
> English novelist

We begin with an illustration of a Galois extension as a motivator for an important concept.

Example 5.12 Let $K = \mathbb{Q}(\zeta_{35})$ and $F = \mathbb{Q}(\zeta_5)$. Then $K/\mathbb{Q}$ is a Galois extension, and $H = \langle\sigma\rangle$ given by

$$\sigma : \zeta_7 \mapsto \zeta_7^3 \text{ and } \sigma : \zeta_5 \mapsto \zeta_5$$

is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ with fixed field $\mathbb{Q}(\zeta_5)$. Notice that any rational prime $p \equiv 1 \pmod 5$ is completely split in $\mathbb{Q}(\zeta_5)$ by Corollary 5.13 on page 218.

Example 5.12 motivates the following.

Definition 5.12 — Decomposition Groups and Fields

Let K/F be a Galois extension of number fields with Galois group $\mathrm{Gal}(K/F)$, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then

$$\mathcal{D}_{\mathcal{P}}(K/F) = \{\sigma \in \mathrm{Gal}(K/F) : \mathcal{P}^\sigma = \mathcal{P}\}$$

is called *the decomposition group of* $\mathcal{P}$ *in* K/F. The fixed field of $\mathcal{D}_{\mathcal{P}}(K/F)$,

$$Z_{\mathcal{P}}(K/F) = \{\beta \in K : \beta^\sigma = \beta \text{ for all } \sigma \in \mathcal{D}_{\mathcal{P}}(K/F)\},$$

is called the *decomposition field of* $\mathcal{P}$ *in* K/F. When $\mathrm{Gal}(K/F)$ is abelian, then the decomposition group and the decomposition field depend only on $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$, so in this case, we denote them by

$$\mathcal{D}_{\mathfrak{p}}(K/F) \text{ and } Z_{\mathfrak{p}}(K/F),$$

and call them *the decomposition group of* $\mathfrak{p}$, and *the decomposition field of* $\mathfrak{p}$ in K/F. When $\mathrm{Gal}(K/F)$ is abelian, we say that K/F is an *abelian extension.*

We begin with a fundamental result on decomposition groups.

Lemma 5.7 — Conjugacy of Decomposition Groups

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then for all $\sigma \in \mathrm{Gal}(K/F)$,

$$\sigma^{-1}\mathcal{D}_{\mathcal{P}}(K/F)\sigma = \mathcal{D}_{\mathcal{P}^\sigma}(K/F).$$

Proof. Let $\tau \in \mathcal{D}_{\mathcal{P}}(K/F)$ and $\sigma \in \mathrm{Gal}(K/F)$. Then

$$(\mathcal{P}^\sigma)^{\sigma^{-1}\tau\sigma} = \mathcal{P}^{\tau\sigma} = \mathcal{P}^\sigma.$$

Therefore, $\sigma^{-1}\tau\sigma \in \mathcal{D}_{\mathcal{P}^\sigma}(K/F)$. Hence,

$$\sigma^{-1}\mathcal{D}_{\mathcal{P}}(K/F)\sigma \subseteq \mathcal{D}_{\mathcal{P}^\sigma}(K/F).$$

It remains to verify the reverse inclusion. If $\gamma \in \mathcal{D}_{\mathcal{P}^\sigma}(K/F)$, then

$$\mathcal{P}^{\sigma\gamma} = \mathcal{P}^{\sigma} \text{ which implies that } \mathcal{P}^{\sigma\gamma\sigma^{-1}} = \mathcal{P}.$$

Thus, $\sigma\gamma\sigma^{-1} \in \mathcal{D}_{\mathcal{P}}(K/F)$. In other words, $\gamma \in \sigma^{-1}\mathcal{D}_{\mathcal{P}}(K/F)\sigma$, so

$$\mathcal{D}_{\mathcal{P}^\sigma}(K/F) \subseteq \sigma^{-1}\mathcal{D}_{\mathcal{P}}(K/F)\sigma,$$

as required. □

Example 5.13 In Example 5.12 on the preceding page, the decomposition group of any rational prime $p \equiv 31 \pmod{35}$ in the abelian extension $\mathbb{Q}(\zeta_{35})/\mathbb{Q}$ is

$$\mathcal{D}_p(\mathbb{Q}(\zeta_{35})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\zeta_{35})/\mathbb{Q}(\zeta_5)),$$

and the decomposition field of p is

$$Z_p(\mathbb{Q}(\zeta_{35})/\mathbb{Q}) = \mathbb{Q}(\zeta_5).$$

Remark 5.5 Lemma 5.7 on the previous page shows that if K/F is a Galois extension of number fields, and $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal, then for any $\sigma \in \text{Gal}(K/F)$,

$$\sigma^{-1}\mathcal{D}_{\mathcal{P}}(K/F)\sigma = \mathcal{D}_{\mathcal{P}^\sigma}(K/F).$$

This is the group-theoretic analogue of the fact established for prime ideals, Corollary 5.1 on page 190, namely that the prime $\mathfrak{O}_K$-ideals are transitively permuted by the elements of $\text{Gal}(K/F)$. In other words, if $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal with

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j},$$

then the decomposition groups $\mathcal{D}_{\mathcal{P}_j}(K/F)$ for $1 \le j \le g$ are transitively permuted by the elements of $\text{Gal}(K/F)$. In the case where K is an abelian extension of F, then

$$\mathcal{D}_{\mathcal{P}_j}(K/F) = \mathcal{D}_{\mathcal{P}_k}(K/F) = \mathcal{D}_{\mathfrak{p}}(K/F),$$

for all natural numbers $j, k \le g$. In other words, in the abelian case, the decomposition groups are all the same, thereby justifying the penultimate remark made in Definition 5.12 on the previous page for the use of the notations $\mathcal{D}_{\mathfrak{p}}(K/F)$ and $Z_{\mathfrak{p}}(K/F)$.

The decomposition field is aptly named, as shown by the following.

Theorem 5.16 — Splitting in the Decomposition Field

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal with $\mathcal{P} \cap \mathfrak{O}_F = \mathfrak{p}$. Then for $Z = Z_{\mathcal{P}}(K/F)$,

$$|K : Z| = |\mathcal{D}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathfrak{p})f_{K/F}(\mathfrak{p}),$$

and if $\mathcal{P} \cap \mathfrak{O}_Z = \mathcal{P}_Z$, then

$$f_{Z/F}(\mathcal{P}_Z) = e_{Z/F}(\mathcal{P}_Z) = 1.$$

Proof. By Theorem 2.4 on page 60,

$$|\mathrm{Gal}(K/F) : \mathcal{D}_{\mathcal{P}}(K/F)| = |Z_{\mathcal{P}}(K/F) : F|.$$

By Lemma 5.7, each right coset $\mathcal{D}_{\mathcal{P}}(K/F)\sigma$ of $\mathcal{D}_{\mathcal{P}}(K/F)$ via $\sigma \in \mathrm{Gal}(K/F)$ sends $\mathcal{P}$ to $\mathcal{P}^{\sigma}$. In other words, if $\gamma \in \mathcal{D}_{\mathcal{P}}(K/F)\sigma$, then

$$\mathcal{P}^{\gamma} = \mathcal{P}^{\tau\sigma} = \mathcal{P}^{\sigma},$$

for all $\tau \in \mathcal{D}_{\mathcal{P}}(K/F)$. Therefore, $\mathcal{D}_{\mathcal{P}}(K/F)\sigma = \mathcal{D}_{\mathcal{P}}(K/F)\tau$ for $\sigma,\tau \in \mathrm{Gal}(K/F)$ implies that $\mathcal{D}_{\mathcal{P}}(K/F) = \mathcal{D}_{\mathcal{P}}(K/F)\tau\sigma^{-1}$, so $\mathcal{P} \to \mathcal{P}^{\tau\sigma^{-1}}$. In other words, $\mathcal{P}^{\sigma} = \mathcal{P}^{\tau}$. Therefore, we have established a one-to-one correspondence between the right coset $\mathcal{D}_{\mathcal{P}}(K/F)\sigma$ in $\mathrm{Gal}(K/F)$ and the primes $\mathcal{P}^{\sigma}$. By Corollary 5.1, these primes are transitively permuted by the $\sigma \in \mathrm{Gal}(K/F)$, so there must exist $g_{K/F}(\mathfrak{p})$ of them. Hence,

$$|Z_{\mathcal{P}}(K/F) : F| = g_{K/F}(\mathfrak{p}).$$

Thus, by Theorem 5.4 on page 189,

$$|\mathcal{D}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathfrak{p})f_{K/F}(\mathfrak{p}).$$

Now we verify the last statement in the theorem. Let $Z = Z_{\mathcal{P}}(K/F)$, and $\mathcal{P}_Z = \mathcal{P} \cap Z$. By Theorem 2.4, K/Z is a normal extension. Therefore,

$$\mathrm{Gal}(K/Z) = \mathcal{D}_{\mathcal{P}}(K/F),$$

so $\mathcal{P}^{\sigma} = \mathcal{P}$ for all $\sigma \in \mathrm{Gal}(K/F)$. By Theorem 5.4, $g_{K/Z}(\mathcal{P}_Z) = 1$, and

$$|K : Z| = e_{K/Z}(\mathcal{P}_Z)f_{K/Z}(\mathcal{P}_Z). \tag{5.22}$$

Also,

$$|K : F| = e_{K/F}(\mathfrak{p})f_{K/F}(\mathfrak{p})g_{K/F}(\mathfrak{p}), \tag{5.23}$$

and we have already shown that

$$|Z : F| = g_{K/F}(\mathfrak{p}). \tag{5.24}$$

Hence, putting (5.22)–(5.24) together, we get

$$e_{K/F}(\mathfrak{p})f_{K/F}(\mathfrak{p})g_{K/F}(\mathfrak{p}) = e_{K/Z}(\mathcal{P}_Z)f_{K/Z}(\mathcal{P}_Z)g_{K/F}(\mathfrak{p}),$$

so

$$e_{K/F}(\mathfrak{p})f_{K/F}(\mathfrak{p}) = e_{K/Z}(\mathcal{P}_Z)f_{K/Z}(\mathcal{P}_Z). \tag{5.25}$$

However, by Theorem 5.1 on page 184,

$$e_{K/F}(\mathfrak{p}) = e_{K/Z}(\mathcal{P}_Z)e_{Z/F}(\mathcal{P}_Z), \tag{5.26}$$

and

$$f_{K/F}(\mathfrak{p}) = f_{K/Z}(\mathcal{P}_Z)f_{Z/F}(\mathcal{P}_Z). \tag{5.27}$$

By comparing (5.25)–(5.27), we get

$$e_{Z/F}(\mathcal{P}_Z) = 1 = f_{Z/F}(\mathcal{P}_Z),$$

as required. □

Corollary 5.14 If K/F is a Galois extension of number fields, and $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal with $\mathcal{P} \cap \mathfrak{O}_F = \mathfrak{p}$, then

$$|Z_{\mathcal{P}}(K/F) : F| = g_{K/F}(\mathfrak{p}).$$

Furthermore, if $\mathcal{D}_{\mathcal{P}}(K/F)$ is a normal subgroup of $\mathrm{Gal}(K/F)$, then $\mathfrak{p}$ is completely split in $Z_{\mathcal{P}}(K/F)$.

Proof. From the proof of Theorem 5.16, we have the first statement. By Theorem 2.4, if $\mathcal{D}_{\mathcal{P}}(K/F)$ is normal in $\mathrm{Gal}(K/F)$, then Z/F is a normal extension where $Z = Z_{\mathcal{P}}(K/F)$, so by Theorem 5.16,

$$f_{Z/F}(\mathcal{P}_Z) = f_{Z/F}(\mathfrak{p}) = 1 = e_{Z/F}(\mathcal{P}_Z) = e_{Z/F}(\mathfrak{p}),$$

where $\mathcal{P}_Z = \mathcal{P} \cap Z$. Therefore,

$$g_{Z/F}(\mathfrak{p}) = |Z : F| = g_{K/F}(\mathfrak{p}),$$

namely $\mathfrak{p}$ is completely split in Z. □

Example 5.14 If we let $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, and $F = \mathbb{Q}$, then $\mathrm{Gal}(K/F) = S_3$, the symmetric group on three letters—see Definition A.1 on page 320. In Example 5.9 on page 191 we demonstrated that $p = 29$ splits into two primes

$$p\mathfrak{O}_K = \mathcal{P}_1\mathcal{P}_2$$

where $K = \mathbb{Q}(\sqrt[3]{2})$, with $f_{K/\mathbb{Q}}(\mathcal{P}_1) = 1 = e_{K/\mathbb{Q}}(\mathcal{P}_j)$ for $j = 1, 2$, and $f_{K/\mathbb{Q}}(\mathcal{P}_2) = 2$. Also, $f_{L/K}(\mathcal{Q}_1) = 2$, where $\mathcal{Q}_1$ is the prime $\mathfrak{O}_L$-ideal over $\mathcal{P}_1$. Thus,

$$Z_{\mathcal{Q}_1}(L/\mathbb{Q}) = K,$$

which is not normal over $\mathbb{Q}$, as demonstrated in Exercise 2.12 on page 63. Similarly, the decomposition fields for $\mathcal{Q}_2$ and $\mathcal{Q}_3$ are, respectively,

$$\mathbb{Q}(\zeta_3\sqrt[3]{2}) \text{ and } \mathbb{Q}(\zeta_3^2\sqrt[3]{2}).$$

In none of these (isomorphic) fields is 29 completely split, since

$$|Z_{\mathcal{Q}_1}(L/\mathbb{Q})| = 3 = g_{K/F}(29),$$

but $f_{K/\mathbb{Q}}(\mathcal{P}_j) \leq 2$ for $j = 1, 2$. This shows that the normality assumption in Corollary 5.14 is indeed necessary.

There exists another important subgroup of the Galois group from the perspective of decomposition. The reader unfamiliar with residue classes modulo an ideal should review Exercises 4.30–4.32 on pages 163–164 before proceeding.

Definition 5.13 — The Inertia Group and Inertia Field

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then

$$\mathcal{T}_{\mathcal{P}}(K/F) = \{\sigma \in \mathrm{Gal}(K/F) : \alpha^\sigma \equiv \alpha \pmod{\mathcal{P}} \text{ for all } \alpha \in \mathfrak{O}_K\}$$

is called the *inertia group* of $\mathcal{P}$ in K/F, and its fixed field,

$$T_{\mathcal{P}}(K/F) = \{\beta \in K : \beta^\sigma = \beta \text{ for all } \sigma \in \mathcal{T}_{\mathcal{P}}(K/F)\},$$

is called the *inertia field* of $\mathcal{P}$ in K/F.[5.9]

[5.9] The T is used for inertia subgroup since it comes from the German *Trägheitskörper*, and, similarly, Z for the decomposition field comes from *Zerlegungskörper*. These were the terms used by Hilbert in his *Zahlbericht*, where the theory was published for the first time. However, there is a certain consensus that Dedekind knew about the decomposition and inertia subfields, as shown by his papers, which were unpublished at the time that Hilbert wrote down his ramification theory.

Lemma 5.8 — Inertia and Conjugacy

Let K/F be a Galois extenion of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_F$-ideal. Then, for all $\sigma \in \text{Gal}(K/F)$,

$$\sigma^{-1}\mathcal{T}_{\mathcal{P}}(K/F)\sigma = \mathcal{T}_{\mathcal{P}^\sigma}(K/F).$$

Proof. If $\tau \in \mathcal{T}_{\mathcal{P}}(K/F)$ and $\sigma \in \text{Gal}(K/F)$, then for $\alpha \in K$,

$$\sigma\tau\sigma^{-1}(\alpha) - \alpha = \sigma\tau(\sigma^{-1}(\alpha)) - \sigma\sigma^{-1}(\alpha) = \sigma(\tau(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha)) \in \sigma(\mathcal{P}),$$

so $\sigma\mathcal{T}_{\mathcal{P}}(K/F)\sigma^{-1} \subseteq \mathcal{T}_{\sigma(\mathcal{P})}(K/F)$. By the same reasoning,

$$\sigma^{-1}\mathcal{T}_{\sigma(\mathcal{P})}(K/F)\sigma \subseteq \mathcal{T}_{\mathcal{P}}(K/F),$$

so we also have the reverse inclusion. □

The following gives a value to the order of the inertia group.

Theorem 5.17 — Index of the Inertia Group

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal with $\mathcal{P} \cap \mathfrak{O}_F = \mathfrak{p}$. Then $\mathcal{T}_{\mathcal{P}}(K/F)$ is a normal subgroup of $\mathcal{D}_{\mathcal{P}}(K/F)$, and

$$|\text{Gal}(K/F) : \mathcal{T}_{\mathcal{P}}(K/F)| = f_{K/F}(\mathfrak{p})g_{K/F}(\mathfrak{p}).$$

Also, for $T = T_{\mathcal{P}}(K/F)$, and $\mathcal{P}_T = \mathcal{P} \cap \mathfrak{O}_T$, we have that $f_{K/T}(\mathcal{P}) = 1$, $e_{T/F}(\mathcal{P}_T) = 1$, and $e_{K/T}(\mathcal{P}) = e_{K/F}(\mathfrak{p})$.

Proof. Let $\mathfrak{O}_K/\mathcal{P} = K_{\mathcal{P}}$ and $\mathfrak{O}_F/\mathfrak{p} = F_{\mathfrak{p}}$. Define a mapping

$$\psi : \mathcal{D}_{\mathcal{P}}(K/F) \mapsto \text{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}}),$$

by

$$\psi(\sigma) = \overline{\sigma},$$

where $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma\alpha}$, with $\overline{\alpha}$ being the residue class of α in $\mathfrak{O}_K/\mathcal{P}$. Thus, $\overline{\sigma} \in \text{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$, and ψ is a homomorphism. By the definition of $\mathcal{T}_{\mathcal{P}}(K/F)$, we get that $\ker(\psi) = \mathcal{T}_{\mathcal{P}}(K/F)$, so by Theorem A.5 on page 328,

$$\mathcal{D}_{\mathcal{P}}(K/F)/\mathcal{T}_{\mathcal{P}}(K/F) \cong \text{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}}),$$

and $\mathcal{T}_{\mathcal{P}}(K/F)$ is a normal subgroup of $\mathcal{D}_{\mathcal{P}}(K/F)$—see also Lemma 5.7 on page 221. Since Theorem 5.16 on page 222 gives us that $|\mathcal{D}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathcal{P})f_{K/F}(\mathcal{P})$, and by Definition 5.1 on page 182, $|K_{\mathcal{P}} : F_{\mathfrak{p}}| = f_{K/F}(\mathcal{P})$, then

$$|\mathcal{T}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathfrak{p}),$$

so

$$|\text{Gal}(K/F) : \mathcal{T}_{\mathcal{P}}(K/F)| = f_{K/F}(\mathfrak{p})g_{K/F}(\mathfrak{p}),$$

which is the first result. Next, we show that $f_{K/T}(\mathcal{P}) = 1$. Let $T_{\mathcal{P}_T} = \mathfrak{O}_T/\mathcal{P}_T$. By the definition of inertial degree, we need only show that

$$|K_{\mathcal{P}} : T_{\mathcal{P}_T}| = 1. \tag{5.28}$$

To show this, we demonstrate that if $\beta \in K_{\mathcal{P}}$, then

$$f(x) = (x - \beta)^e \in T_{\mathcal{P}_T}[x],$$

where $e = |\mathcal{T}_{\mathcal{P}}(K/F)| = |K : T_{\mathcal{P}}(K/F)|$. Once shown, then every element of $\mathrm{Gal}(K_{\mathcal{P}}/T_{\mathcal{P}_T})$ sends β to a root of $f(x)$, namely β itself, so $\mathrm{Gal}(K_{\mathcal{P}}/T_{\mathcal{P}_T})$ is trivial and (5.28) holds. Let $\alpha \in K_{\mathcal{P}}$. Then

$$g(x) = \prod_{\sigma \in \mathcal{T}_{\mathcal{P}}(K/F)} (x - \alpha^{\sigma}) \in \mathfrak{O}_T[x].$$

By reducing coefficients modulo $\mathcal{P}$, we get that $\overline{g}(x) \in K_{\mathcal{P}}[x]$, so by the definition of $T_{\mathcal{P}}(K/F)$, $\overline{g}(x) \in T_{\mathcal{P}_T}[x]$, and $\overline{\alpha^{\sigma}} = \overline{\alpha}$ so

$$g(x) = (x - \alpha)^e,$$

and we have verified (5.28) as required.

Now we show that $e_{T/F}(\mathcal{P}_T) = 1$. Since we have shown above that

$$|T : F| = |\mathrm{Gal}(K/F) : \mathcal{T}_{\mathcal{P}}(K/F)| = f_{K/F}(\mathfrak{p}) g_{K/F}(\mathfrak{p}),$$

then $e_{T/F}(\mathcal{P}_T) = 1$, and since $f_{K/T}(\mathcal{P}) = 1$, then $e_{K/F}(\mathcal{P}) = e_{K/F}(\mathfrak{p})$. □

Maintaining the notation and assumptions of Theorem 5.17, we have the following consequence.

Corollary 5.15 For any Galois extension K/F, we have

$$|\mathcal{T}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathfrak{p}),$$

and if $\mathcal{D}_{\mathcal{P}}(K/F)$ is a normal subgroup of $\mathrm{Gal}(K/F)$, then each of the $g_{K/F}(\mathfrak{p})$ prime $\mathfrak{O}_Z$-ideals is inert in T where $Z = Z_{\mathcal{P}}(K/F)$, and each prime $\mathcal{P}_T$-ideal is an e^{th} power in K.

Proof. From the proof of Theorem 5.17, $|\mathcal{T}_{\mathcal{P}}(K/F)| = e_{K/F}(\mathcal{P})$. By Corollary 5.14 on page 224, there exist $g = g_{K/F}(\mathcal{P})$ prime $Z = Z_{\mathcal{P}}(K/F)$-ideals above $\mathfrak{p}$. Hence, there exists exactly one prime $\mathfrak{O}_K$-ideal above each of the g prime $\mathfrak{O}_Z$-ideals. Thus, the inertial degrees of each of the g prime Z-ideals in T is the same. To prove that each prime $\mathfrak{O}_Z$-ideal is inert in T, it suffices to prove that each is unramified in T. However, from Theorem 5.17, $e_{T/F}(\mathcal{P}_T) = e_{Z/F}(\mathcal{P}_Z) = 1$. The result now follows from Theorem 5.4 on page 189. Hence, in consideration of the above results, $\mathcal{P}_T \mathfrak{O}_K = \mathcal{P}^e$, where $e = e_{K/F}(\mathfrak{p})$. □

In the following, an *intermediate field* in the extension K/F means an extension field of F contained in K.

Corollary 5.16 — Intermediate Fields as Decomposition and Inertia Fields
Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then

(a) If L is an intermediate field, then ZL is the decomposition field of $\mathcal{P}$ in K/L.

(b) If L is an intermediate field, then LT is the inertia field of $\mathcal{P}$ in K/L.

Proof. (a) Let $F_1 = \mathfrak{O}_{LZ}/\mathcal{P}_1$ where $\mathcal{P}_1 = \mathcal{P} \cap \mathfrak{O}_{LZ}$, $F_2 = \mathfrak{O}_L/\mathcal{P}_2$ where $\mathcal{P}_2 = \mathcal{P} \cap \mathfrak{O}_L$, $F_3 = \mathfrak{O}_Z/\mathcal{P}_3$ where $\mathcal{P}_3 = \mathcal{P} \cap \mathfrak{O}_Z$, and $F_4 = \mathfrak{O}_{L\cap Z}/\mathcal{P}_4$ where $\mathcal{P}_4 = \mathcal{P} \cap \mathfrak{O}_{L\cap Z}$. Then $\mathrm{Gal}(F_1/F_2)$ may be embedded into $\mathrm{Gal}(F_3/F_4)$ via restriction of automorphisms. However,

$$\mathrm{Gal}(F_3/F_4) = |F_3 : F_4| = f_{Z/L\cap Z}(\mathcal{P}_3) = 1,$$

by definition, so $f_{LZ/L}(\mathcal{P}_1) = 1$. Furthermore, $\mathcal{P}_L$ cannot split any further by Theorems 5.16–5.17. Hence, LZ is the decomposition field of $\mathcal{P}_L$ in K/L.

(b) This is proved in a similar fashion to that given part (a), by comparing the Galois groups of LT/L and $T/(L \cap T)$. □

Corollary 5.17 Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then each of the following hold.

(a) $Z_{\mathcal{P}}(K/F)$ is the smallest intermediate field L such that $\mathcal{P}$ is the only prime $\mathfrak{O}_K$-ideal lying over $\mathcal{P}_L = \mathcal{P} \cap \mathfrak{O}_L$.

(b) The field $Z_{\mathcal{P}}(K/F)$ is the largest intermediate field L such that

$$e_{L/F}(\mathcal{P}_L) = f_{L/F}(\mathcal{P}_L) = 1.$$

(c) The field $T_{\mathcal{P}}(K/F)$ is the largest intermediate field L such that

$$e_{L/F}(\mathcal{P}_L) = 1.$$

(d) The field $T_{\mathcal{P}}(K/F)$ is the smallest intermediate field L such that

$$e_{K/L}(\mathcal{P}) = |K : L|.$$

Proof. (a) Suppose that $\mathcal{P}$ is the only prime $\mathfrak{O}_K$-ideal lying over $\mathcal{P}_L$. Since $\mathrm{Gal}(K/L)$ transitively permutes the prime $\mathfrak{O}_K$-ideals above $\mathcal{P}_L$ by Corollary 5.1 on page 190, then $\mathrm{Gal}(K/L)$ is forced to be in $\mathcal{D}_{\mathcal{P}}(K/F)$. Thus, by Theorem 2.4 on page 60,

$$Z_{\mathcal{P}}(K/F) \subseteq L,$$

which establishes (a).
(b) If

$$e_{L/F}(\mathcal{P}_L) = f_{L/F}(\mathcal{P}_L) = 1,$$

then by Theorem 5.1 on page 184,

$$e_{K/F}(\mathcal{P}) = e_{K/L}(\mathcal{P})e_{L/F}(\mathcal{P}_L),$$

and

$$f_{K/F}(\mathcal{P}) = f_{K/L}(\mathcal{P})f_{L/F}(\mathcal{P}_L).$$

Therefore,

$$e_{K/F}(\mathcal{P}) = e_{K/L}(\mathcal{P}) \text{ and } f_{K/F}(\mathfrak{p}) = f_{K/L}(\mathcal{P}).$$

Thus, for $Z = Z_{\mathcal{P}}(K/F)$, by Theorem 5.16 on page 222,

$$e_{K/F}(\mathcal{P})f_{K/F}(\mathcal{P}) = |K : Z|.$$

Also,

$$|K : ZL| = e_{K/L}(\mathcal{P})f_{K/L}(\mathcal{P}),$$

since the decomposition field of $\mathcal{P}_L$ in K/L is ZL, by part (a) of Corollary 5.16. Thus, $Z = ZL$, so $L \subseteq Z$, which is (b).
(c) If $e_{L/F}(\mathcal{P}_L) = 1$, and $T = T_{\mathcal{P}}(K/F)$, then by part (b) of Corollary 5.16, LT is the inertia field of $\mathcal{P}$ in K/L. Thus,

$$e_{K/F}(\mathcal{P}) = |K : T| = |K : LT| = e_{K/L}(\mathcal{P}).$$

Hence, $T = LT$, so $L \subseteq T$, which verifies (c).
(d) If $\mathcal{P}_L$ is totally ramified in K, then by part (b) of Corollary 5.16,

$$e_{K/L}(\mathcal{P}) = |K : L| = |K : LT| = e_{K/L}(\mathcal{P}).$$

Therefore, $LT = L$ so $T \subseteq L$, which completes the entire result. □

Corollary 5.18 Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal with $\mathcal{P} \cap \mathfrak{O}_F = \mathfrak{p}$. Then if $\mathcal{D}_{\mathcal{P}}(K/F)$ is normal in $\mathrm{Gal}(K/F)$, $\mathfrak{p}$ is completely split in an intermediate field L if and only if $L \subseteq Z_{\mathcal{P}}(K/F)$.

Proof. If $\mathfrak{p}$ is completely split in L/K, then $e_{L/F}(\mathcal{P}_L) = f_{L/F}(\mathcal{P}_L) = 1$, where $\mathcal{P}_L = \mathcal{P} \cap \mathfrak{O}_L$. Therefore, by part (b) of Corollary 5.17, $L \subseteq Z_{\mathcal{P}}(K/F)$. Conversely, by Corollary 5.14 on page 224, $\mathfrak{p}$ is completely split in $Z_{\mathcal{P}}(K/F)$, so *a fortiori* it is completely split in L. □

Diagram 5.1 — Inertia, Ramification, and Decomposition

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Then the following illustrates the theory developed above. In what follows, $K_{\mathcal{P}} = \mathfrak{O}_K/\mathcal{P}$, $T = T_{\mathcal{P}}(K/F)$, $\mathcal{P}_T = \mathcal{P} \cap T$, $T_{\mathcal{P}_T} = \mathfrak{O}_T/\mathcal{P}_T$, $Z = Z_{\mathcal{P}}(K/F)$, $\mathcal{P}_Z = \mathcal{P} \cap Z$, $Z_{\mathcal{P}_Z} = \mathfrak{O}_Z/\mathcal{P}_Z$, $\mathfrak{p} = \mathcal{P} \cap F$, and $F_{\mathfrak{p}} = \mathfrak{O}_F/\mathfrak{p}$.

Primes	**Groups**	**Fields**	**Degrees**	**Residue Fields**
$\mathcal{P}$		K		$K_{\mathcal{P}}$
	$\mathcal{T}_{\mathcal{P}}(K/F)$	$\vert$	$\}\ e_{K/F}(\mathcal{P})$	$\vert$
$\mathcal{P}_T$	$\cap\vert$	T		$T_{\mathcal{P}_T}$
	$\mathcal{D}_{\mathcal{P}}(K/F)$	$\vert$	$\}\ f_{K/F}(\mathcal{P})$	$\vert$
$\mathcal{P}_Z$	$\cap\vert$	Z		$Z_{\mathcal{P}_Z}$
	$\mathrm{Gal}(K/F)$	$\vert$	$\}\ g_{K/F}(\mathcal{P})$	$\vert$
$\mathfrak{p}$		F		$F_{\mathfrak{p}}$

The above diagram is augmented by the following one that motivates an important concept.

Diagram 5.2 — Residue Class Fields and Their Global Counterparts

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal with $K_{\mathcal{P}} = \mathfrak{O}_K/\mathcal{P}$. Every element of $\mathrm{Gal}(K/F)$ restricts to an automorphism of $\mathfrak{O}_K$. Thus, if $\sigma \in \mathcal{D}_{\mathcal{P}}(K/F)$, there is an induced mapping $\psi : \mathfrak{O}_K \mapsto K_{\mathcal{P}}$ with $\ker(\psi) = \mathcal{P}$. Therefore, each $\sigma \in \mathcal{D}_{\mathcal{P}}(K/F)$ induces an automorphism $\overline{\sigma}$ of $K_{\mathcal{P}}$ in a fashion such that the following diagram commutes.[5.10]

$$\begin{tikzcd}
\mathfrak{O}_K \arrow[r, "\sigma"] \arrow[d, "\psi"] & \mathfrak{O}_K \arrow[d, "\psi"] \\
K_{\mathcal{P}} \arrow[r, "\overline{\sigma}"] & K_{\mathcal{P}}
\end{tikzcd}$$

Also $\overline{\sigma}$ fixes the finite field $\mathfrak{O}_F/\mathfrak{p} = F_{\mathfrak{p}}$ where $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$. Hence, $\overline{\sigma} \in \mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$, so this yields a mapping

$$\rho : \mathcal{D}_{\mathcal{P}}(K/F) \mapsto \mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}}),$$

which is a group homomorphism since products in $\mathcal{D}_{\mathcal{P}}(K/F)$ correspond to products in $\mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$. Also $\ker(\rho) = \mathcal{T}_{\mathcal{P}}(K/F)$, so $\mathcal{T}_{\mathcal{P}}(K/F)$ is a normal subgroup of $\mathcal{D}_{\mathcal{P}}(K/F)$—see Exercise 5.43 on page 253 for a generalization of this fact. This tells us that the quotient

[5.10] We remind the reader that a commutative diagram, in this case, means that we have the equality of composite maps $\psi\circ\sigma=\overline{\sigma}\circ\psi$.

group $\mathcal{D}_{\mathcal{P}}(K/F)/\mathcal{T}_{\mathcal{P}}(K/F)$ is embedded in $\mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$. A fundamental fact, which is buried in the proof of Theorem 5.17 on page 225, is that ρ is an epimorphism, so

$$\mathcal{D}_{\mathcal{P}}(K/F)/\mathcal{T}_{\mathcal{P}}(K/F) \cong \mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}}).$$

From Exercise 2.16 on page 64, the Galois group $\mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$ is cyclic of order $f_{K/F}(\mathcal{P})$. If $\mathcal{P}$ is unramified in K/F, then by the aforementioned proof,

$$\langle \overline{\sigma_{\mathcal{P}}} \rangle = \mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}}) \cong \mathcal{D}_{\mathcal{P}}(K/F),$$

and there is a unique $\sigma_{\mathcal{P}} \in \mathcal{D}_{\mathcal{P}}(K/F)$ such that $\sigma_{\mathcal{P}} \mapsto \overline{\sigma_{\mathcal{P}}}$. The generator of the decomposition group in this case is a very distinguished element, which is named as follows—see Biography 2.3 on page 80.

Definition 5.14 — The Frobenius Automorphism

If K/F is a Galois extension of number fields, and $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal unramified in K/F with $\mathcal{P} \cap \mathfrak{O}_F = \mathfrak{p}$, then $\mathcal{D}_{\mathcal{P}}(K/F)$ is cyclic and has generator:

$$\left(\frac{K/F}{\mathcal{P}}\right),$$

called *the Frobenius automorphism* of $\mathcal{P}$ in K/F, given by

$$\left(\frac{K/F}{\mathcal{P}}\right)(\alpha) \equiv \alpha^{N^{F/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathcal{P}}.$$

When $\mathrm{Gal}(K/F)$ is abelian, then the Frobenius automorphism depends only on $\mathfrak{p}$ and we write

$$\left(\frac{K/F}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N^{F/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{p}\mathfrak{O}_K},$$

where as usual $\mathfrak{p}\mathfrak{O}_K$ is the product of the prime $\mathfrak{O}_K$-ideals lying over $\mathfrak{p}$. In the abelian case, $\left(\frac{K/F}{\mathfrak{p}}\right)$ is also called the *Artin symbol*—see Remark 5.7 on page 239.

Definition 5.14 allows us to state one final consequence of Theorem 5.17.

Corollary 5.19 Let K/F be a Galois extension of number fields, with $\mathcal{P}$ a prime $\mathfrak{O}_K$-ideal. If $\mathcal{P}$ is unramified in K/F, then $\mathcal{D}_{\mathcal{P}}(K/F)$ is cyclic of order $f_{K/F}(\mathfrak{p})$ generated by the Frobenius automorphism of $\mathcal{P}$ in K/F. In particular, $\mathcal{P}$ is completely split in K if and only if $\left(\frac{K/F}{\mathcal{P}}\right) = 1$.

Application 5.1 —The Frobenius Automorphism on Cyclotomic Galois Groups

Let ζ_n for $n \in \mathbb{N}$ be a primitive n^{th} root of unity, and set $K = \mathbb{Q}(\zeta_n)$. We now apply the Frobenius automorphism to show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group of nonzero elements of $\mathbb{Z}/n\mathbb{Z}$.

Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is determined by its action on ζ_n, namely $\zeta_n^{\sigma} = \zeta_n^{n_\sigma}$, where $n_\sigma \in \mathbb{Z}$ is uniquely determined modulo n. Also, this action is independent of the choice of ζ_n since σ acting on any primitive n^{th} root of unity raises it to the power n_σ, given that all roots of unity are powers of ζ_n. Thus, if σ,τ $\in \mathrm{Gal}(K/\mathbb{Q})$, then

$$\zeta_n^{n_{\sigma\tau}} = \zeta_n^{\sigma\tau} = (\zeta_n^{n_\sigma})^{\tau} = \zeta_n^{n_\sigma n_\tau}.$$

Thus, $n_\sigma n_\tau \equiv n_{\sigma\tau} \pmod{n}$. In other words, the mapping defined by

$$\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mapsto n_\sigma \in \mathbb{Z}/n\mathbb{Z}^*,$$

is a homomorphism. Since each σ uniquely determines n_σ, then this map is a monomorphism. It remains to show that it is an epimorphism. Let $p \nmid n$ be a rational prime. Therefore, the Frobenius automorphism

$$\sigma_p = \left(\frac{K/\mathbb{Q}}{p}\right)$$

is well-defined since p is unramified in K. If $\mathcal{P}$ is any prime $\mathfrak{O}_K$-ideal over p, then this automorphism is given by

$$\alpha^{n_{\sigma_p}} \equiv \alpha^p \pmod{\mathcal{P}}. \tag{5.29}$$

From Exercise 1.54 on page 43 it follows that if $f(x) = x^n - 1$, then

$$\prod_k (\zeta_n^p - \zeta_n^k) = f'(\zeta_n^p),$$

where the product runs over all nonnegative $k \leq n-1$ with $p \nmid k$. Since $f'(\zeta_n^p) = n\zeta_n^{p(n-1)}$, then $\prod_k (\zeta_n^p - \zeta_n^k) \notin \mathcal{P}$. Hence, $\alpha^{n_{\sigma_p}} \equiv \alpha^p \pmod{\mathcal{P}}$ represents the residue class of p modulo n. In other words, the mapping $\sigma \mapsto n_\sigma$ is an isomorphism of $\mathrm{Gal}(K/F)$ onto $\mathbb{Z}/n\mathbb{Z}^*$.

We now illustrate how the Frobenius automorphism can be used to prove Gauss's quadratic reciprocity law.

Application 5.2 — The Quadratic Reciprocity Law via Frobenius

Let $K = \mathbb{Q}(\zeta_p)$ where $p > 2$ is prime and ζ_p is a primitive p^{th} root of unity. Set $p^* = (-1)^{(p-1)/2}p$. Then by Exercise 5.35 on page 232, $\mathbb{Q}(\sqrt{p^*}) = F$ is a quadratic subfield of K. In fact, it is the unique quadratic subfield of K, since $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order $p-1$, given that it is generated by σ where $\sigma(\zeta_p) = \zeta_p^g$ with g being a primitive root modulo p. By Application 5.1 on the preceding page, $\mathrm{Gal}(F/\mathbb{Q})$ corresponds to the subgroup $\mathbb{F}_p^*$ of nonzero elements of the field of p elements, $\mathbb{F}_p$. Hence, if $q \neq p$ is any odd prime, and

$$\left(\frac{K/\mathbb{Q}}{q}\right) = \sigma_q$$

is the Artin automorphism of q in $K/\mathbb{Q}$, then its restriction to F,

$$\sigma_q|_F = \left(\frac{K/\mathbb{Q}}{q}\right)\Bigg|_F = \left(\frac{F/\mathbb{Q}}{q}\right),$$

is the identity on F precisely when $\sigma_q : \zeta_p \mapsto \zeta_p^q$, where q is a square in $\mathbb{F}_p^*$. Otherwise, it is the nontrivial automorphism, with q being a nonsquare in $\mathbb{F}_p^*$. Thus, by considering the natural identifications:

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \frac{\mathrm{Gal}(K/\mathbb{Q})}{\mathrm{Gal}(K/F)} \cong \{\pm 1\},$$

we get

$$\left(\frac{F/\mathbb{Q}}{q}\right) = \left(\frac{q}{p}\right), \tag{5.30}$$

by the very definition of the Legendre symbol. From another perspective, since $F = \mathbb{Q}(\sqrt{p^*})$, then q splits in F if and only if

$$\left(\frac{F/\mathbb{Q}}{q}\right) = 1,$$

and q is inert exactly when

$$\left(\frac{F/\mathbb{Q}}{q}\right) = -1,$$

so for odd q, we get

$$\left(\frac{F/\mathbb{Q}}{q}\right) = \left(\frac{p^*}{q}\right). \tag{5.31}$$

By comparing (5.30)–(5.31), we get

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right).$$

However,

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$$

so

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

which is Gauss's Quadratic Reciprocity Law.

Application 5.2 also suggests how a rational prime splits in a cyclotomic field.

Application 5.3 — Frobenius and Splitting in Cyclotomic Fields

Suppose that $n \in \mathbb{N}$, $n > 1$, and without loss of generality $n \not\equiv 2 \pmod 4$, since $K = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ for n odd by Corollary 1.17 on page 41. Then by Application 5.1 on page 229,

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Thus,

$$\sigma_p = \left(\frac{K/\mathbb{Q}}{p}\right)$$

is defined for $p \nmid n$, and depends only on p since G is abelian. Thus, $\alpha^{\sigma_p} \equiv \alpha^p \pmod{p\mathfrak{O}_K}$, for all $\alpha \in \mathfrak{O}_K = \mathbb{Z}[\zeta_p]$, by Corollary 5.13 on page 218. Hence, p is completely split in K if and only if $p \equiv 1 \pmod n$, which is tantamount to saying that $\sigma_p = 1$, namely $\alpha \equiv \alpha^p \pmod{p\mathfrak{O}_K}$ for all $\alpha \in \mathfrak{O}_K$—see Exercises 4.31–4.32 on page 164.

Exercises

5.27. Let $\mathbb{F}_q$ the finite field of $q = p^f$ elements for some prime p. A map χ from $\mathbb{F}_q^*$ to the multiplicative group of roots of unity in $\mathbb{C}^*$ such that

$$\chi(ab) = \chi(a)\chi(b) \text{ for all } a, b \in \mathbb{F}_q^*$$

is called a (multiplicative) *character* on $\mathbb{F}_q^*$.[5.11] If $\chi(a) = 1$ for all $a \in \mathbb{F}_q^*$, then χ is called the *trivial character on* $\mathbb{F}_q^*$, denoted by ϵ. It is convenient to extend the domain of definition from $\mathbb{F}_q^*$ to $\mathbb{F}_q$ by setting $\chi(0) = 1$ if $\chi = \epsilon$, and $\chi(0) = 0$ if $\chi \neq \epsilon$. The *order* of χ is the least $m \in \mathbb{N}$ such that $\chi^m = \epsilon$. Establish each of the following.

[5.11] Notice that the Legendre symbol $(\frac{a}{p})$ is an example of a character on $\mathbb{F}_p$ by considering $(\frac{a}{p})$ as a coset of a modulo p—see Exercise 5.33.

(a) $\chi(1) = 1$.

(b) $\chi(a)^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$.

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ for all $a \in \mathbb{F}_q^*$, where $\overline{\chi(a)}$ is the complex conjugate of $\chi(a)$.

Exercises 5.28–5.32 will be with reference to characters as defined in Exercise 5.27.

5.28. Let χ be a character on $\mathbb{F}_q$. Prove that

$$\sum_{j=0}^{q-1} \chi(j) = \begin{cases} 0 & \text{if } \chi \neq \epsilon, \\ q & \text{if } \chi = \epsilon. \end{cases}$$

5.29. Prove that the characters on $\mathbb{F}_q^*$ form a multiplicative group, denoted by $\mathfrak{Ch}(\mathbb{F}_q^\times)$, via the definition of multiplication and inverses given by $\chi\lambda(a) = \chi(a)\lambda(a)$, and $\chi^{-1}(a) = (\chi(a))^{-1}$, for $a \in \mathbb{F}_q^*$ and characters χ and λ.

5.30. Prove that $\mathfrak{Ch}(\mathbb{F}_q^\times)$, given in Exercise 5.29, is cyclic of order $q - 1$ and that if $a \in \mathbb{F}_q^*$ with $a \neq 1$, there exists a character χ on $\mathbb{F}_q$ such that $\chi(a) \neq 1$.

Henceforth, if χ is a character on $\mathbb{F}_q^*$, then χ is said to be of order n, where $n \mid q - 1$, provided that n is the smallest such value for which $\chi^n = \epsilon$.

5.31. Suppose that $a \in \mathbb{F}_q^*$ with $a \neq 1$. Prove that

$$\sum_{\chi \in \mathfrak{Ch}(\mathbb{F}_q^\times)} \chi(a) = 0.$$

5.32. Suppose that $a \in \mathbb{F}_q^*$, and $n \in \mathbb{N}$ with $q \equiv 1 \pmod{n}$ such that $x^n = a$ has no solution for any $x \in \mathbb{F}_q$. Prove that there exists a character χ on $\mathbb{F}_q$ of order n such that $\chi(a) \neq 1$.

5.33. For an odd prime p, let $(\frac{x}{p})$ denote the Legendre symbol with $(\frac{0}{p}) = 0$ for convenience, and for $k \in \mathbb{Z}$, set

$$G(k) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta_p^{jk},$$

called a *quadratic Gauss sum.* Prove that

$$G(k) = \left(\frac{k}{p}\right) G(1).$$

✰ 5.34. With reference to Exercise 5.33, prove that $G^2(1) = (-1)^{\frac{p-1}{2}} p$.

5.35. Let $p > 2$ be a prime, and set $p^* = (-1)^{(p-1)/2} p$. Prove that[5.12] $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$.

5.36. Let $p \neq q$ be rational primes with p odd, and let d be a fixed divisor of $p - 1$. Prove that $q \equiv x^d \pmod{p}$ is solvable for some $x \in \mathbb{Z}$ if and only if q is completely split in the unique subfield of $\mathbb{Q}(\zeta_p)$ having degree d over $\mathbb{Q}$. (*Observe that Gauss's Quadratic Reciprocity Law follows from this, the case where $d = 2$—see also Application 5.2 on page 230.*)

[5.12] In Chapter 5, we will generalize this result considerably with a proof of the celebrated Kronecker-Weber Theorem (see Theorem 5.23 on page 244).

5.5 Kummer Extensions and Class-Field Theory

I don't like people who have never fallen or stumbled. Their virtue is lifeless and it isn't of much value. Life hasn't revealed its beauty to them.
From Part 2, Chapter 13, Section 12 of **Doctor Zhivago (1958)**
Boris Pasternak (1890–1960)
Russian novelist and poet

In this section, we commence with another type of extension distinct from the quadratic and cyclotomic extensions considered in §5.4, which will lead us into class-field theory that is an aspect of "higher algebraic number theory."

Definition 5.15 — Kummer Extensions

Let F be a number field containing a primitive n^{th} root of unity for a given fixed $n \in \mathbb{N}$, and set $f(x) = x^n - \alpha$ for a given $\alpha \in F$. Then $K = F(\sqrt[n]{\alpha})$ is called a *Kummer extension of* F, where $\sqrt[n]{\alpha}$ is a root of $f(x)$.

Lemma 5.9 — Kummer Extensions are Cyclic

If $K = F(\sqrt[n]{\alpha})$ is a Kummer extension of F, then K is a normal extension of F and $\mathrm{Gal}(K/F)$ is cyclic of order n.

Proof. Let $\varepsilon_j = \zeta_n^j$ for $j = 1, 2, \ldots, n$ be all of the n^{th} roots of unity in F, where ζ_n is a primitive nth root of unity. If σ is an F-isomorphism of K, then

$$\sigma : \sqrt[n]{\alpha} \mapsto \varepsilon_j \sqrt[n]{\alpha} \in F,$$

for some $j = 1, 2, \ldots, n$, which is another root of $x^n - \alpha$. Thus, K/F is a normal extension. If $\sigma_k, \sigma_\ell \in \mathrm{Gal}(K/F)$, are given by $\sigma_j(\sqrt[n]{\alpha}) = \varepsilon_j \sqrt[n]{\alpha}$ for $j = k, \ell$, then

$$\sigma_k\sigma_\ell(\sqrt[n]{\alpha}) = \sigma_k(\varepsilon_\ell \sqrt[n]{\alpha}) = \varepsilon_k\varepsilon_\ell \sqrt[n]{\alpha} = \varepsilon_\ell\varepsilon_k \sqrt[n]{\alpha} = \sigma_\ell\sigma_k(\sqrt[n]{\alpha}),$$

so $\mathrm{Gal}(K/F)$ is abelian. Select $\sigma \in \mathrm{Gal}(K/F)$, such that $\sigma : \sqrt[n]{\alpha} \mapsto \varepsilon_j \sqrt[n]{\alpha}$, where ε_j is a *primitive* nth root of unity. Then $\sigma^n = 1$ but $\sigma^m \neq 1$ for any natural number $m < n$, because $\varepsilon_j^m \neq 1$ for any such m, so σ generates $\mathrm{Gal}(K/F)$. In other words, $\mathrm{Gal}(K/F)$ is cyclic of order n. □

Theorem 5.18 — Decomposition in Kummer Extensions

Let K/F be a Kummer extension of degree n with $K = F(\beta)$ such that $\beta^n = \alpha \in \mathfrak{O}_F$. If $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal such that $n\alpha \notin \mathfrak{p}$ and g is the maximal divisor of n such that

$$x^g \equiv \alpha \pmod{\mathfrak{p}},$$

has a solution in $x \in \mathfrak{O}_F$, then

$$\mathfrak{p}\mathfrak{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_g,$$

for distinct prime $\mathfrak{O}_K$-ideals $\mathcal{P}_j$, $1 \le j \le g$, and

$$fg = |K : F|,$$

where f is the minimal exponent such that

$$\beta^f \equiv \alpha \pmod{\mathfrak{p}}.$$

Proof. Let $F_{\mathfrak{p}}$ denote the field $\mathfrak{O}_F/\mathfrak{p}$, and let $\overline{x}$ denote the image of x in $F_{\mathfrak{p}}$ under the natural map from $\mathfrak{O}_F$.

Claim 5.11 If $f \in \mathbb{N}$ is the smallest exponent such that

$$\overline{\beta}^f = \overline{\alpha} \in F_{\mathfrak{p}},$$

then $m(x) = x^f - \overline{\alpha}$ is irreducible over $F_{\mathfrak{p}}$.

Since $\overline{\beta}^n \in F_{\mathfrak{p}}$, then $n \geq f$. If $n = fq+r$ where $q \in \mathbb{N}$ and $0 \leq r < f$, then $\overline{\alpha}^r = \overline{\alpha}^{n-fq} \in F_{\mathfrak{p}}$, so $r = 0$, by the minimality of f. Thus, $f \mid n$. Since a primitive n-th root of unity, $\zeta_n \in F_{\mathfrak{p}}$, then $\zeta_n^{n/f} = \zeta_f \in F_{\mathfrak{p}}$. Also,

$$x^f - \overline{\alpha} = \prod_{j=0}^{f-1}(x - \overline{\beta}\zeta_f^j).$$

If $g(x)$ properly divides $(x^f - \overline{\alpha})$ for some $g(x) \in F_{\mathfrak{p}}[x]$, then $g(0) = \overline{\beta}^k\gamma \in F_{\mathfrak{p}}$, where $\gamma \in F_{\mathfrak{p}}$ and $k < f$. Hence, by the minimality of f, we must have that $k = f$, a contradiction. This establishes Claim 5.11.

Let $K_{\mathcal{P}}$ denote the field $\mathfrak{O}_K/\mathcal{P}$ where $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal over $\mathfrak{p}$. Since a root of $m(x)$ generates the field extension $K_{\mathcal{P}}/F_{\mathfrak{p}}$, then

$$f_{K/F}(\mathcal{P}) = f_{K/F}(\mathfrak{p}) = |K_{\mathcal{P}} : F_{\mathfrak{p}}| = f,$$

where the penultimate equality comes from Claim 5.1 in the Proof of Theorem 5.3 on page 187, and the last equality comes from the fact that

$$K_{\mathcal{P}} \cong \frac{F_{\mathfrak{p}}[x]}{(m(x))} \cong F_{\mathfrak{p}}(\beta),$$

which is a result of (A.3) on page 325. Hence,

$$|K_{\mathcal{P}} : F_{\mathfrak{p}}| = \deg_{F_{\mathfrak{p}}}(m) = f.$$

Since $n\alpha \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in K. Thus, by Theorem 5.4 on page 189,

$$g = |K : F|/f.$$

Since f is the minimal divisor of n such that

$$x^f \equiv \beta \pmod{\mathfrak{p}},$$

has a solution $x \in \mathfrak{O}_F$, then g is the maximal divisor of n such that

$$x^g \equiv \beta \pmod{\mathfrak{p}}$$

has a solution in $\mathfrak{O}_F$, so

$$\mathfrak{p}\mathfrak{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_g,$$

and this secures the proof. □

A special case of Theorem 5.18 is worth isolating, especially in view of the fact that this will be one of the stepping stones in concluding Kummer's proof of FLT for regular primes, which we will see in Theorem 5.22 on page 240.

Corollary 5.20 Suppose that p is a rational prime and F is a number field containing a primitive p^{th} root of unity. Then if α is not a p^{th} power of an element of $\mathfrak{O}_F$, $x^p - \alpha$ is irreducible over F and $\mathrm{Gal}(K/F)$ is cyclic of order p. In the latter case, one of the following two events occurs for any prime $\mathfrak{O}_F$-ideal $\mathfrak{q}$, where $p\alpha \notin \mathfrak{q}$.

(a) The congruence

$$x^p \equiv \alpha \pmod{\mathfrak{q}} \tag{5.32}$$

has a solution, in which case $g_{K/F}(\mathfrak{q}) = p$, and $f_{K/F}(\mathfrak{q}) = 1 = e_{K/F}(\mathfrak{q})$, namely $\mathfrak{q}$ is completely split in K.

(b) The congruence (5.32) has no solution, in which case $f_{K/F}(\mathfrak{q}) = p$, and $g_{K/F}(\mathfrak{q}) = 1 = e_{K/F}(\mathfrak{q})$, namely $\mathfrak{q}$ is inert in K.

We need the following result for the ensuing development.

Lemma 5.10 Let $K = F(\sqrt[p]{\alpha})$, where $\alpha \in \mathfrak{O}_F$ is not a p^{th} power in $\mathfrak{O}_F$, $\zeta_p \in F$, and p is a rational prime. Then any prime $\mathfrak{O}_F$-ideal $\mathfrak{q}$ satisfies exactly one of the properties

(a) $e_{K/F}(\mathfrak{q}) = 1 = f_{K/F}(\mathfrak{q})$ and $g_{K/F}(\mathfrak{q}) = p$, in which case $\mathfrak{q}$ is completely split in K.

(b) $g_{K/F}(\mathfrak{q}) = 1 = e_{K/F}(\mathfrak{q})$ and $f_{K/F}(\mathfrak{q}) = p$, in which case $\mathfrak{q}$ is inert in K.

(c) $f_{K/F}(\mathfrak{q}) = 1 = g_{K/F}(\mathfrak{q})$ and $e_{K/F}(\mathfrak{q}) = p$, in which case $\mathfrak{q}$ is totally ramified in K.

Proof. This is immediate from Theorem 5.4 on page 189 and Lemma 5.9 on page 233 . □

Remark 5.6 The case where $p\alpha \in \mathfrak{q}$ in Corollary 5.20 deserves to be settled as well since it has fundamental consequences for the aforementioned proof by Kummer. The following observation will assist the reader with the next result. If $\alpha \in \mathfrak{q}$, then $\alpha\mathfrak{O}_F = \mathfrak{q}^n I$, where $n \in \mathbb{N}$ and I is an $\mathfrak{O}_F$-ideal not divisible by $\mathfrak{q}$. In this case, we may assume without loss of generality that $p \nmid n$. To see this, assume $p \mid n$, let $\gamma \in \mathfrak{q}$ with $\gamma^2 \notin \mathfrak{q}$, and set $\alpha_1 = \alpha(\gamma^{-n/p})^p$. Then a root of $x^p - \alpha_1$ generates the same field extension K/F, since a root β_1 of the latter equation satisfies $\beta_1^p = \alpha_1 = \alpha(\gamma^{-n/p})^p$. Therefore, $\beta_1 \in F(\beta)$, where $\beta^p = \alpha$ and conversely $\beta \in F(\beta_1)$. Notice, as well, that once this translation is made, then the exact power of $\mathfrak{q}$ dividing α_1 is equal to $n - (n/p)p = 0$, so $\gcd(\alpha\mathfrak{O}_F, \mathfrak{q}) = 1$.

Theorem 5.19 — Kummer p-Extensions

Suppose that p is a rational prime and F is a number field containing a primitive p^{th} root of unity. Set $K = F(\beta)$ where $\beta^p = \alpha \in F$, and α is not the p^{th} power of an element of $\mathfrak{O}_F$. If $p\alpha \in \mathfrak{q}$, where $\mathfrak{q}$ is a prime $\mathfrak{O}_F$-ideal, then one of the following occurs.

(a) If $\alpha \in \mathfrak{q}$, then $\alpha\mathfrak{O}_F = \mathfrak{q}^n I$, where $n \in \mathbb{N}$, and I is an $\mathfrak{O}_F$-ideal with $\mathfrak{q} \nmid I$. If $p \nmid n$, then $\mathfrak{q}$ ramifies in K, namely $e_{K/F}(\mathfrak{q}) = p$, and $f_{K/F}(\mathfrak{q}) = 1 = g_{K/F}(\mathfrak{q})$.

(b) If $\alpha \notin \mathfrak{q}$, but $p \in \mathfrak{q}$, namely $\mathfrak{q} \cap \mathbb{Z} = (p)$, then $\mathfrak{O}_F(1 - \zeta_p) = \mathfrak{q}^n J$ where J is an $\mathfrak{O}_F$-ideal not divisible by $\mathfrak{q}$ and $n \in \mathbb{N}$, and one of the following occurs.

(i) The congruence

$$x^p \equiv \alpha \pmod{\mathfrak{q}^{np+1}} \tag{5.33}$$

has a solution $x \in \mathfrak{O}_F$, in which case $\mathfrak{q}$ is completely split in K. Conversely, if $\mathfrak{q}$ is completely split in K, then congruence (5.33) has such a solution.

(ii) The congruence (5.33) has no solution in $\mathfrak{O}_F$, but the congruence

$$x^p \equiv \alpha \pmod{\mathfrak{q}^{np}} \tag{5.34}$$

has a solution $x \in \mathfrak{O}_F$, in which case $\mathfrak{q}$ is inert in K.

(iii) The congruence (5.34) has no solution in $\mathfrak{O}_F$, in which case $\mathfrak{q}$ is totally ramified in K.

Proof. We begin with an observation, the proof of which is similar to the demonstration given in Remark 5.6 on the preceding page.

Claim 5.12 We may assume without loss of generality that

$$\mathfrak{q} \bigm| \alpha\mathfrak{O}_F, \text{ but } \mathfrak{q}^2 \nmid \alpha\mathfrak{O}_F.$$

Let $\gamma \in \mathfrak{q}$, and $\gamma \notin \mathfrak{q}^2$. Since $\gcd(p, n) = 1$, there exist $r, s \in \mathbb{Z}$ such that $rp + sn = 1$. Let $\alpha_1 = \alpha^s\gamma^{rp}$. Then a root of $x^p - \alpha_1$ generates the same field extension K/F. To see this, we observe that if

$$\beta_1^p = \alpha_1 = \alpha^s\gamma^{rp} = \beta^{ps}\gamma^{rp} = (\beta^s\gamma^r)^p,$$

then

$$\beta_1 = \beta^s\gamma^r\zeta_p^k \in F(\beta),$$

for some nonnegative integer k. Conversely,

$$\alpha_1^n = \alpha^{sn}\gamma^{nrp} = \alpha(\alpha^{sn-1})\gamma^{nrp} = \alpha(\alpha^{-rp})\gamma^{nrp} = \alpha(\alpha^{-1}\gamma^n)^{rp}.$$

Therefore,

$$\alpha = \alpha_1^n(\alpha\gamma^{-n})^{rp},$$

so $\alpha \in F(\beta_1)$, as above. Hence, $F(\beta) = F(\beta_1)$ as asserted.

From the choice of γ, the exact power of $\mathfrak{q}$ dividing $\alpha_1\mathfrak{O}_F = \alpha^s\mathfrak{O}_F\gamma^{rp}\mathfrak{O}_F$ is $\mathfrak{q}^{ns+rp} = \mathfrak{q}$. Hence, $\alpha\mathfrak{O}_F = \mathfrak{q}I$, where $\mathfrak{q} \nmid I$. This is Claim 5.12.

Let

$$\mathcal{Q} = \gcd(\mathfrak{q}\mathfrak{O}_K, \beta\mathfrak{O}_K).$$

Then

$$\mathcal{Q}^p = \gcd(\mathfrak{q}^p\mathfrak{O}_K, \alpha\mathfrak{O}_K) = \mathfrak{q}\mathfrak{O}_K.$$

By Theorem 5.4 on page 189, $\mathcal{Q}$ is a prime ideal so $\mathfrak{q}$ is totally ramified in K. This completes the proof of (a).

To establish part (i) of (b), we first assume that $\mathfrak{q}$ is completely split in K, so let

$$\mathfrak{q}\mathfrak{O}_K = \mathcal{Q}_1 \cdots \mathcal{Q}_p,$$

where the $\mathcal{Q}_j$ are distinct prime $\mathfrak{O}_K$-ideals. Thus, $f_{K/F}(\mathcal{Q}_j) = 1 = e_{K/F}(\mathcal{Q}_j)$ for $j = 1, 2, \ldots, p$. Therefore, $\mathcal{Q}_j^m \cap \mathfrak{O}_F \neq \mathfrak{q}^{m-1}$ for $m \in \mathbb{N}$, since if we have that $\mathcal{Q}_j^m \bigm| (\mathfrak{q}\mathfrak{O}_K)^{m-1} = \mathfrak{q}^{m-1}\mathfrak{O}_K$, then $e_{K/F}(\mathcal{Q}_j) > 1$, a contradiction.

Claim 5.13 $\mathcal{Q}_j^m \cap \mathfrak{O}_F = \mathfrak{q}^m$ for any $m \in \mathbb{N}$.

We use induction on m. If $m = 1$, then the result holds by Lemma 5.1 on page 182. Assume the induction hypothesis, that the result holds for $m - 1$. Then

$$\mathfrak{q}^m \subseteq \mathfrak{Q}_j^m \cap \mathfrak{O}_F \subseteq \mathfrak{Q}_j^{m-1} \cap \mathfrak{O}_F = \mathfrak{q}^{m-1},$$

with $\mathfrak{Q}_j^m \cap \mathfrak{O}_F \neq \mathfrak{q}^{m-1}$. Thus, $\mathfrak{Q}_j^m \cap \mathfrak{O}_F = \mathfrak{q}^m$, which is Claim 5.13.

By Claim 5.13, $\mathfrak{O}_F/\mathfrak{q}^{np+1}$ is a subring of $\mathfrak{O}_K/\mathfrak{Q}_j^{np+1}$. However, since $\mathfrak{q}$ is completely split in K, then $|\mathfrak{O}_K/\mathfrak{Q}_j : \mathfrak{O}_F/\mathfrak{q}| = f_{K/F}(\mathfrak{q}) = 1$, so $|\mathfrak{O}_F/\mathfrak{q}^{np+1}| = |\mathfrak{O}_K/\mathfrak{Q}_j^{np+1}|$, by Exercise 2.40 on page 82. Therefore, there exists a $\gamma \in \mathfrak{O}_F$ such that

$$\beta \equiv \gamma \pmod{\mathfrak{Q}_1^{np+1}},$$

namely

$$\mathfrak{Q}_1^{np+1} \mid (\gamma - \beta)\mathfrak{O}_K.$$

Thus,

$$N^{K/F}(\mathfrak{Q}_1)^{np+1} \mid N^{K/F}(\gamma - \beta)\mathfrak{O}_K.$$

However,

$$N_{K/F}(x - \beta) = x^p - \beta^p = x^p - \alpha,$$

so

$$\mathfrak{q}^{np+1} \mid (\gamma^p - \alpha),$$

which means that

$$x^p \equiv \alpha \pmod{\mathfrak{q}^{np+1}},$$

has a solution $x = \gamma \in \mathfrak{O}_F$.

Conversely, let (5.33) have a solution $x = \gamma \in \mathfrak{O}_F$. Select $u \in \mathfrak{q}^{-n}$ with $u \notin \mathfrak{q}^{-n+1}$, so that $\mathfrak{O}_F u\mathfrak{q}^n = I$ is an $\mathfrak{O}_F$-ideal. We have that $v = u(\gamma - \beta)$ is a root of $(x - u\gamma)^p + u^p\alpha$.

Claim 5.14 $(x - u\gamma)^p - u^p\alpha \in \mathfrak{O}_F[x]$.

Since $\mathfrak{q}^{n(p-1)} \mid \mathfrak{O}_F(1 - \zeta_p)^{p-1}$ by hypothesis, then for all $j \in \mathbb{N}$ such that $j \le p - 1$, we have $n(p-1) - nj \ge 0$, so

$$\binom{p}{j} u^j\gamma^j \in \mathfrak{O}_F.$$

Since

$$(x - u\gamma)^p + u^p\alpha = \sum_{j=0}^{p-1}(-1)^j\binom{p}{j}u^j\gamma^j x^{p-j} - u^p(\gamma^p - \alpha),$$

and $\gamma^p - \alpha \in \mathfrak{q}^{n+1}$, then $u^p(\gamma^p - \alpha) \in \mathfrak{q}$ since $u \in \mathfrak{q}^{-n}$. This completes Claim 5.14.

By Claim 5.14, $v \in \mathfrak{O}_K$, and so are the other roots, $u(\gamma - \zeta_p^{j-1}\beta)$ for $j = 0, 1, \ldots, p - 1$. Set

$$\mathfrak{Q}_j = \gcd(\mathfrak{q}\mathfrak{O}_K, u(\gamma - \zeta_p^{j-1}\beta)\mathfrak{O}_K).$$

Then $\mathfrak{Q}_j \neq \mathfrak{O}_K$ for $0 \le j \neq k \le p - 1$ since

$$\mathfrak{q} \mid N^{K/F}(v\mathfrak{O}_K) = u^p(\gamma^p - \alpha).$$

Also,

$$\mathfrak{q}\mathfrak{O}_K = \mathfrak{Q}_1 \cdots \mathfrak{Q}_p,$$

since every element of $\prod_{j=1}^p \mathfrak{Q}_j$ is a sum of elements of the form

$$\prod_{j=1}^{p}(\sigma_j + \tau_j u(\gamma - \zeta_p^{j-1}\beta)) = \sigma + \tau u^p(\gamma^p - \alpha) \in \mathfrak{q}\mathfrak{O}_K,$$

where $\sigma_j, \sigma \in \mathfrak{q}\mathfrak{O}_K$ and $\tau_j, \tau \in \mathfrak{O}_K$. Thus, $\mathfrak{Q}_j \cap \mathfrak{O}_F = \mathfrak{q}$ for each such j and each $\mathfrak{Q}_j$ is distinct by Theorem 5.4 on page 189. This completes the proof of part (i) of (b).

If (5.34) has a solution $x = \gamma \in \mathfrak{O}_F$, then as in the proof of part (i), $v = u(\gamma - \beta) \in \mathfrak{O}_K$ with minimal polynomial

$$m_{K/F}(v) = (x - u\gamma)^p - u^p\alpha,$$

and

$$\delta_{K/F}(v) = m'_{K/F}(v) = p(u\beta)^{p-1},$$

with $\gcd(\delta_{K/F}(v), \mathfrak{Q}) = 1$ for any prime $\mathfrak{O}_K$-ideal $\mathfrak{Q}$ dividing $\mathfrak{q}$. Thus, by Theorem 5.9 on page 203 and Corollary 5.7 on page 210, $\mathfrak{q}$ is unramified in K. By part (i), and Lemma 5.10 on page 235, $\mathfrak{q}$ must be inert in K. This secures part (ii).

For part (iii), assume that (5.34) on page 236 is unsolvable in $\mathfrak{O}_F$, and let ℓ be the largest exponent such that $x^p \equiv \alpha \pmod{\mathfrak{q}^\ell}$ is solvable in $\mathfrak{O}_F$. By Exercise 4.31 on page 164, we must have that $\ell \in \mathbb{N}$.

Claim 5.15 $p \nmid \ell$

Suppose that $\gamma \in \mathfrak{O}_F$ such that for some natural number $t \le n - 1$, we have a solution $\gamma \in \mathfrak{O}_F$ to the congruence

$$\gamma^p \equiv \alpha \pmod{\mathfrak{q}^{pt}}.$$

Suppose further that $\lambda \in \mathfrak{O}_F$ such that $\lambda^p \equiv 0 \pmod{\mathfrak{q}^t}$, but $\lambda^p \not\equiv 0 \pmod{\mathfrak{q}^{t+1}}$. Then for any $\omega \in \mathfrak{O}_F$,

$$(\gamma + \lambda\omega)^p \equiv \gamma^p + \lambda^p\omega^p \pmod{\mathfrak{q}^{tp+1}}.$$

However, since ω^p ranges over all residue classes modulo $\mathfrak{q}$, we may chose ω such that

$$\alpha \equiv (\gamma + \lambda\omega)^p \pmod{\mathfrak{q}^{tp+1}},$$

a contradiction to the hypothesis. However, since $\ell < np$, then $p \nmid \ell$. This completes Claim 5.15.

By Claim 5.15, we may select natural numbers $t, r \le n - 1$ such that $\ell = tp + r$. Let $u \in \mathfrak{q}^{-t}$ with $u \notin \mathfrak{q}^{-t+1}$, and set $v = u(\gamma - \beta)$, which is a root of $(x - u\gamma)^p - u^p\alpha$. By a similar argument to the above, $v \in \mathfrak{O}_K$ and $\mathfrak{q}^r$ is the exact power of $\mathfrak{q}$ dividing

$$N_{K/F}(v) = u^p(\gamma^p - \alpha).$$

Thus,

$$\gcd(\mathfrak{q}\mathfrak{O}_K, v\mathfrak{O}_K)$$

is an $\mathfrak{O}_K$-ideal distinct from $\mathfrak{O}_K$ and $\mathfrak{q}\mathfrak{O}_K$. Hence, $\mathfrak{q}\mathfrak{O}_K$ is not a prime $\mathfrak{O}_K$-ideal, and by part (i), $\mathfrak{q}\mathfrak{O}_K$ is not completely split in K. By Lemma 5.10, $\mathfrak{q}$ must be totally ramified in K. □

A direct consequence of Corollary 5.20 and Theorem 5.19 on page 235 is the following important unramified extensions result.

Theorem 5.20 — Unramified Kummer Extensions

Let F be a number field, $\alpha,\zeta_p \in F$ such that α is not a p^{th} power in F, p a rational prime such that $K = F(\sqrt[p]{\alpha})$, and $\gcd(\alpha\mathfrak{O}_F, p\mathfrak{O}_F) = 1$. Then $\mathcal{D}_{K/F} = \mathfrak{O}_F = (1)$ if and only if both of the following hold:[5.13]

(a) $\alpha\mathfrak{O}_F = I^p$ for some $\mathfrak{O}_F$-ideal I, and

(b) There exists a $\gamma \in \mathfrak{O}_F$ such that

$$\gamma^p \equiv \alpha \pmod{(1-\zeta_p)^p\mathfrak{O}_F}.$$

Remark 5.7 The cyclic unramified extensions described by Theorem 5.20 play an important role in Kummer's proof of Fermat's Last Theorem for regular primes in the second case. In fact, this is a beginning of an introduction to an aspect *class-field theory.* We will not develop the tools to discuss this area in depth, but we will describe some fundamental aspects, since they pertain to our completion of Kummer's aforementioned proof.

Recall from Definition 5.14 on page 229, when K/F is an unramified Galois extension of number fields, then the Frobenius automorphism $(\frac{K/F}{\mathcal{P}})$ is defined for any prime $\mathfrak{O}_K$-ideal $\mathcal{P}$. Thus, for any unramified Galois extension of number fields K/F, we may define the *Artin map*

$$\phi_{K/F} : I_{\Delta_K} \mapsto \mathrm{Gal}(K/F)$$

via

$$\phi_{K/F}(I) = \prod_{j=1}^{r} \left(\frac{K/F}{\mathcal{P}_j}\right)^{a_j},$$

where $I \in I_{\Delta_K}$ with $I = \prod_{j=1}^{r} \mathcal{P}_j^{a_j}$ for distinct $\mathfrak{O}_F$-ideals $\mathcal{P}_j$.[5.14] The Artin map may be shown to be an epimorphism, so

$$I_{\Delta_F}/\ker(\phi_{K/F}) \cong \mathrm{Gal}(K/F).$$

In fact, a fundamental result of class-field theory says more.

Theorem 5.21 — Fundamental Theorem of Class-Field Theory

If F is a number field and $K^{(1)}$ is the maximal unramified [5.15] abelian extension of F, called the *Hilbert Class Field*, then

$$\mathrm{Gal}(K^{(1)}/F) \cong \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$$

via

$$\phi_{K^{(1)}/F} : I_{\Delta_{K^{(1)}}} \mapsto \mathrm{Gal}(K^{(1)}/F).$$

Furthermore, since $K^{(1)}$ contains every abelian unramified extension of F, then for a tower $F \subseteq K \subseteq K^{(1)}$,

$$|K : F| \bigm| h_{\mathfrak{O}_F} = |K^{(1)} : F|.$$

[5.13] Note that there is no ramification at the infinite primes for odd primes p since F is totally complex in that case.

[5.14] The Artin map may be defined for more general extensions, which may be ramified, by excluding a set of ramified primes, a necessarily finite set by Corollary 5.7 on page 210. However, for our purposes herein, we need only look at the special case of unramified extensions. Also, note that from Theorem 5.20, if K/F is an *abelian* unramified extension, then the Artin map depends only on the *ideal class* of a given ideal I.

[5.15] In this context "unramified" also excludes those infinite primes that ramify (see Footnote 5.8 on page 213).

Proof. See [33]. □

An immediate and important consequence of this result from class-field theory is the following, which the reader should compare with Exercise 3.33 on page 121.

Corollary 5.21 A prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ splits completely in $K^{(1)}$ if and only if $\mathfrak{p}$ is a principal ideal.

Remark 5.8 Corollary 5.21 tells us that the Hilbert class field $K^{(1)}$ of F is characterized by the fact that the primes that split completely in $K^{(1)}$ are *precisely* the principal prime $\mathfrak{O}_F$-ideals. Note that in Theorem 5.21 on the preceding page, the association of the Galois group $\mathrm{Gal}(K^{(1)}/F)$ with $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ explains why $K^{(1)}$ is called a *class field.* Moreover, the theorem shows that there is a one-to-one correspondence between unramified abelian extensions K of F and subgroups H of the class group $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$. Furthermore, if the extension K/F corresponds to the subgroup $H \subseteq \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$, then the Artin map induces an isomorphism

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}/H \cong \mathrm{Gal}(K/F).$$

This last comment may be taken to be *class-field theory for unramified abelian extensions.* This illustrates the central theme of class-field theory, namely that the unramified extensions of a given number field F are classified in terms of the subgroups of the ideal class group $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$. In other words, the class of unramified extensions are classified in terms of data intrinsic to F.

In the special case established in Theorem 5.20 on the previous page, we see that $p \mid h_{\mathfrak{O}_F}$. This is enough to prove a crucial result that will allow us to complete Kummer's aforementioned proof. The reader is encouraged to solve Exercise 5.39 on page 243, which is related to the following lemma. Recall, as cited on page 151, that p is regular if $p \nmid h_{\mathfrak{O}_F}$ where $F = \mathbb{Q}(\zeta_p)$.

Lemma 5.11 — Kummer's Lemma

Let p be a regular prime, and let $F = \mathbb{Q}(\zeta_p)$. If $u \in \mathfrak{U}_{\mathfrak{O}_F}$ such that

$$u \equiv z \pmod{p\mathfrak{O}_F}$$

for some $z \in \mathbb{Z}$, then $u = v^p$ where $v \in \mathfrak{U}_{\mathfrak{O}_F}$.

Proof. Let $K = F(\sqrt[p]{u})$, where $\sqrt[p]{u}$ is a real root of $x^p - u$. If u is not the p^{th}-power of an element of $\mathfrak{U}_{\mathfrak{O}_F}$, then K/F is a nontrivial Kummer extension. Since

$$p\mathfrak{O}_F = (1 - \zeta_p)^{p-1}$$

by Example 5.8 on page 190, then by Exercise 4.32 on page 164 the hypothesis of Theorem 5.20 is satisfied, namely K/F is an unramified extension. Therefore, by Theorem 5.21, $p \mid h_{\mathfrak{O}_F}$, a contradiction to the regularity of p. □[5.16]

Theorem 5.22 — Kummer's Proof of FLT Case II for Regular Primes

If p is an odd regular prime, then (4.14) on page 149 has no solutions in rational integers x, y, z with $p \mid xyz$.

[5.16] Without the use of Theorem 5.21, the proof of Kummer's lemma is long, and relatively difficult by comparison since it involves Kummer's use of p-adic numbers. For instance, see [5, pp. 367–377]. By employing the elegant Theorem 5.21, even without proving it, we get an insight into the power of class-field theory, and it allows us to complete Kummer's proof of FLT for regular primes with less difficulty.

Proof. Clearly, we may assume without loss of generality that $\gcd(x, y, z) = 1$, so $p \mid z$ and $p \nmid xy$ may also be assumed without loss of generality. Set $z = p^k z_1$ with $k \in \mathbb{N}$, and $\gcd(z_1, p) = 1$. If $F = \mathbb{Q}(\zeta_p)$, then by Example 5.8

$$p\mathfrak{O}_F = (1 - \zeta_p)^{p-1} u,$$

where $u \in \mathfrak{U}_{\mathfrak{O}_F}$. Thus, (4.14) becomes

$$x^p + y^p + u^{pk}(1 - \zeta_p)^{pn} {z_1}^p = 0, \tag{5.35}$$

where $n = k(p-1) \in \mathbb{N}$. To prove the theorem, it will suffice (*a fortiori*) to prove that (5.35) cannot hold when $x, y, z_1 \in \mathfrak{O}_F$ with x, y, z_1 relatively prime to $1 - \zeta_p$.

We use proof by contradiction. Assume that (5.35) is solvable for some such $x, y, z_1 \in \mathfrak{O}_F$, and let $n \in \mathbb{N}$ be the smallest value for which it holds. Rewriting (5.35) as an ideal equation we get,

$$\prod_{j=0}^{p-1} (x + \zeta_p^j y) = \mathfrak{p}^{pn} J^p, \tag{5.36}$$

where $\mathfrak{p}$ is the prime $\mathfrak{O}_F$-ideal $(1 - \zeta_p)$, and J is an $\mathfrak{O}_F$-ideal. Although long, the proof amounts to essentially a descent argument where we contradict the minimality of n by showing that (5.36) holds for $n - 1$.

Since $n \in \mathbb{N}$, then for $j \geq 0$

$$\mathfrak{p} \mid (x + \zeta_p^j y).$$

However,

$$x + \zeta_p^j y = x + \zeta_p^k y - \zeta_p^k (1 - \zeta_p^{j-k}) y.$$

Therefore, since $\mathfrak{p} \mid (1 - \zeta_p^{j-k})$, then $\mathfrak{p} \mid (x + \zeta_p^j y)$ for *all* nonnegative $j \leq p - 1$. Also, we cannot have that

$$x + \zeta_p^k y \equiv x + \zeta_p^j y \pmod{\mathfrak{p}^2},$$

for $j \neq k$, since in that case we get

$$\zeta_p^k y (1 - \zeta_p^{j-k}) \equiv 0 \pmod{\mathfrak{p}^2},$$

which cannot hold since $\gcd(\zeta_p^k y, \mathfrak{p}) = 1$, given that $p \nmid y$, and by Exercise 3.37 on page 129, $1 - \zeta_p^{j-k}$ and $1 - \zeta_p$ are associates. Hence, $x + \zeta_p^j y$ are pairwise incongruent modulo $\mathfrak{p}^2$. Thus, $(z + \zeta_p^j y)(1 - \zeta_p)^{-1}$ are pairwise incongruent modulo $\mathfrak{p}$ for $0 \leq j \leq p - 1$. By Exercise 4.25 on page 163, these values provide a complete residue system modulo $\mathfrak{p}$. Therefore, for some nonnegative $j \leq p - 1$,

$$(x + \zeta_p^j y)(1 - \zeta_p)^{-1} \equiv 0 \pmod{\mathfrak{p}}.$$

Thus, for only this value j do we have

$$x + \zeta_p^j y \equiv 0 \pmod{\mathfrak{p}^2}.$$

Since we may replace y by $\zeta_p^k y$ for any nonnegative $k \leq p - 1$ in (5.35), we may assume at this stage, without loss of generality, that we have already chosen

$$x + y \equiv 0 \pmod{\mathfrak{p}^2} \text{ and } x + \zeta_p^j y \equiv 0 \pmod{\mathfrak{p}}, \text{ with } \mathfrak{p}^2 \nmid (x + \zeta_p^j y) \text{ for } 1 \leq j \leq p - 1,$$

so the left side of (5.36) is divisible by at least $\mathfrak{p}^{p-1}\mathfrak{p}^2 = \mathfrak{p}^{p+1}$. This implies that $n \geq 2$. Our assumption is that $\gcd(x, y, p) = 1$, so $\mathfrak{p} \nmid \gcd(x, y) = \mathfrak{g}$, the gcd of the two $\mathfrak{O}_F$-ideals (x) and (y). Therefore,

$$(x+\zeta_p^j y)=\mathfrak{p}\mathfrak{g}I_j,$$

where I_j is an $\mathfrak{O}_F$-ideal for $0 \le j \le p-1$, and

$$(x+y)=\mathfrak{p}^{p(n-1)+1}\mathfrak{g}I_0.$$

Claim 5.16 $\gcd(I_j, I_k)=1$ for $0 \le j \ne k \le p-1$.

Let $\mathfrak{q} \bigm| \gcd(I_j, I_k)$ for a prime $\mathfrak{O}_F$-ideal $\mathfrak{q}$ with $j \ne k$. Thus, if

$$\mathfrak{p}\mathfrak{g}\mathfrak{q} \bigm| \gcd(x+\zeta_p^j y, x+\zeta_p^k y),$$

then

$$\mathfrak{p}\mathfrak{g}\mathfrak{q} \bigm| \gcd(x(1-\zeta_p^{k-j}), \zeta_p^j y(1-\zeta_p^{k-j})).$$

Thus,

$$\mathfrak{g}\mathfrak{q} \bigm| \gcd(x,y),$$

contradicting the definition of $\mathfrak{g}$. This completes the proof of Claim 5.16.

By Claim 5.16, we may write (5.36) as

$$\mathfrak{g}^p\mathfrak{p}^{pn}\prod_{j=0}^{p-1} I_j = p^{pn}J^p,$$

where $I_j = J_j^p$ for some $\mathfrak{O}_F$-ideal $J_j \bigm| J$ with $0 \le j \le p-1$. Hence,

$$(x+y)=\mathfrak{p}^{p(n-1)+1}\mathfrak{g}J_0^p, \tag{5.37}$$

and

$$(x+\zeta_p^j y)=\mathfrak{p}\mathfrak{g}J_j^p \text{ for } 1 \le j \le p-1. \tag{5.38}$$

From (5.37), we get

$$(x+y)\mathfrak{p}^{-(p(n-1)+1)}J_0^{-p}=\mathfrak{g},$$

Substituting this into (5.38), we get

$$(x+\zeta_p^j y)\mathfrak{p}^{p(n-1)}=(x+y)(J_jJ_0^{-1})^p. \tag{5.39}$$

Since $\mathfrak{p}=(1-\zeta_p)$ is a principal prime $\mathfrak{O}_F$-ideal, then $(J_jJ_0^{-1})^p$ is principal. By invoking the regularity of $\mathfrak{p}$ and using Exercise 4.11 on page 147, we must have that $J_jJ_0^{-1}$ is principal. Therefore, for $1 \le j \le p-1$, we may set

$$J_jJ_0^{-1}=(\alpha_j/\beta_j),$$

where $\alpha_j, \beta_j \in \mathfrak{O}_F$. Since $\gcd(J_j,\mathfrak{p})=1=\gcd(J_0,\mathfrak{p})$, we may assume that $\gcd(\alpha_j,\mathfrak{p})=1=\gcd(\beta_j,\mathfrak{p})$. Thus, from (5.38)–(5.39),

$$(x+\zeta_p^j y)(1-\zeta_p)^{p(n-1)}=(x+y)(\alpha_j/\beta_j)^p u_j, \tag{5.40}$$

where $u_j \in \mathfrak{U}_{\mathfrak{O}_F}$. Since $(x+\zeta_p y)(1+\zeta_p)-(x+\zeta_p^2 y)=\zeta_p(x+y)$, we may multiply this by $(1-\zeta_p)^{p(n-1)}$ and use (5.40) with $j=1,2$ to get,

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^p u_1(1+\zeta_p)-(x+y)\left(\frac{\alpha_2}{\beta_2}\right)^p u_2=(x+y)\zeta_p(1-\zeta_p)^{p(n-1)}.$$

Multiplying through by $(\beta_1\beta_2)^p/[u_1(x+y)(1+\zeta_p)]$, we get,

$$(\alpha_1\beta_2)^p - \frac{u_2}{u_1(1+\zeta_p)}(\alpha_2\beta_1)^p = \frac{\zeta_p}{u_1(1+\zeta_p)}(1-\zeta_p)^{p(n-1)}(\beta_1\beta_2)^p.$$

By letting $\alpha = \alpha_1\beta_2 \in \mathfrak{O}_F$, $v = -u_2/[u_1(1+\zeta_p)] \in \mathfrak{U}_{\mathfrak{O}_F}$, $\beta = \alpha_2\beta_1 \in \mathfrak{O}_F$, $\gamma = \beta_1\beta_2$, and $v_1 = \zeta_p/[u_1(1+\zeta_p)] \in \mathfrak{U}_{\mathfrak{O}_F}$, we achieve,

$$\alpha^p + v\beta^p = v_1(1-\zeta_p)^{p(n-1)}\gamma^p. \tag{5.41}$$

We now proceed to show that this contradicts the minimality of n, which will complete the proof.

Above we showed that $n \geq 2$, so $p(n-1) \geq p$. Therefore,

$$\alpha^p + v\beta^p \equiv 0 \pmod{\mathfrak{p}^p}. \tag{5.42}$$

Since $\mathfrak{p} \nmid \beta$ by assumption, then β has a multiplicative inverse β_1 modulo $\mathfrak{p}^p$, namely $\beta\beta_1 \equiv 1 \pmod{\mathfrak{p}^p}$. Multiplying through (5.42) by β_1^p and rewriting, we get,

$$v \equiv (-\beta_1\alpha)^p \pmod{\mathfrak{p}^p}.$$

From Exercises 4.31–4.32 on page 164,

$$-\beta_1\alpha \equiv z \pmod{\mathfrak{p}},$$

where $z \in \mathbb{Z}$, so

$$(-\beta_1\alpha)^p \equiv z^p \pmod{\mathfrak{p}^p}.$$

In other words,

$$v \equiv z^p \pmod{\mathfrak{p}^p}.$$

By Lemma 5.11 on page 240, there exists a $w \in \mathfrak{U}_{\mathfrak{O}_F}$ such that $v = w^p$. Hence, via the above congruence, (5.41) becomes

$$\alpha^p + (w\beta)^p = v_1(1-\zeta_p)^{p(n-1)}\gamma^p,$$

which contradicts the minimality of n, and establishes the full result proved by Kummer.□

This concludes this section, and in conjunction with previous sections, establishes a number of powerful results that will allow us to establish the fundamental theorem of abelian extensions, the Kronecker-Weber Theorem in §5.6.

Exercises

5.37. Let K_j/F for $j = 1, 2$ be extensions of number fields, and let $\mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal. Prove that if $\mathfrak{p}$ is unramified in K_j for $j = 1, 2$, then $\mathfrak{p}$ is unramified in K_1K_2. In particular, show that if $\mathfrak{p}$ is completely split in K_j for $j = 1, 2$, then $\mathfrak{p}$ is completely split in K_1K_2.

5.38. Let $F/\mathbb{Q}$ be an abelian extension of number fields. In the next section, the Kronecker-Weber Theorem will verify that

$$F \subseteq \mathbb{Q}(\zeta_f) \text{ for some } f \in \mathbb{N}.$$

The smallest such f is called the *conductor* of F. Prove that if the conductor is odd and squarefree, then $F/\mathbb{Q}$ is tamely ramified.

5.39. Let $p > 2$ be prime $F = \mathbb{Q}(\zeta_p)$, and $\lambda = 1 - \zeta_p$. Prove that for any $\gamma \in \mathfrak{O}_F$, there exists a $z \in \mathbb{Z}$ such that

$$\gamma^p \equiv z \pmod{\lambda^p}.$$

Conclude that

$$\gamma^p \equiv z \pmod{p}.$$

5.6 The Kronecker-Weber Theorem

All the people we used to know.
They're an illusion to me now.
Some are mathematicians.
Some are carpenter's wives.

From **Tangled Up in Blue (1974)**
Bob Dylan (1941–)
American singer and songwriter

This section is devoted to a proof of the Fundamental Theorem of Abelian Extensions, also known as the following.[5.17]

Theorem 5.23 — The Kronecker–Weber Theorem
If F is a number field, which is an abelian extension of $\mathbb{Q}$, there exists a natural number n such that $F \subseteq \mathbb{Q}(\zeta_n)$. Moreover, n can be chosen in such a way that n andΔ_F have the same prime factors.

We establish Theorem 5.23 via a sequence of lemmas. We begin by showing that it suffices to restrict our attention to the case of prime-power degree.

Lemma 5.12 If Theorem 5.23 holds for abelian extensions of prime power degree over $\mathbb{Q}$, then it holds for any abelian extension of $\mathbb{Q}$.

Proof. First we show that every number field F abelian over $\mathbb{Q}$ is a compositum of abelian extensions of prime power degree over $\mathbb{Q}$. By Theorem A.1 on page 321,

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \prod_{j=1}^{r} G_j,$$

where G_j is an abelian group of order $|G_j| = p_j^{a_j}$ for distinct primes p_j, $a_j \in \mathbb{N}$, and

$$|F : \mathbb{Q}| = |\mathrm{Gal}(F/\mathbb{Q})| = \prod_{j=1}^{r} p_j^{a_j}.$$

Let F_i for $i = 1, 2, \ldots, r$ be the fixed field of $\prod_{j\neq i} G_j$, the product ranging over all $j \neq i$ for $1 \leq j \leq r$. Thus, $|F_i : \mathbb{Q}| = |\mathrm{Gal}(F/\mathbb{Q})/\prod_{j\neq i} G_j| = |G_i| = p_i^{a_i}$, by Theorem 2.4 on page 60. Therefore, by Exercise 3.36 on page 129, the compositum has degree

$$\left|\prod_{i=1}^{r} F_i : \mathbb{Q}\right| = \prod_{j=1}^{r} p_j^{a_j} = |F : \mathbb{Q}|.$$

Since $\prod_{i=1}^{r} F_i \subseteq F$, then $F = \prod_{i=1}^{r} F_i$.

[5.17] If we had developed the full force of class-field theory herein, then one could "easily" prove this fundamental theorem. For instance see [15, Theorem 8.8, p. 163]. However, even therein, where the main results of class-field theory are stated but not proved, it is admitted that "the general theorems of class-field theory are complicated to state." Thus, there is some price to pay in attaining the result no matter what the route happens to be since it is a relatively difficult theorem from any perspective.

Now assuming that Theorem 5.23 holds for all such F_i, then $F_i \subseteq \mathbb{Q}(\zeta_{n_i})$ for some $n_i \in \mathbb{N}$. Let $\ell = \operatorname{lcm}(n_1, n_2, \ldots, n_r)$. Then

$$F = \prod_{i=1}^{r} F_i \subseteq \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}, \ldots, \zeta_{n_r}) \subseteq \mathbb{Q}(\zeta_\ell),$$

and the result is proved in view of Theorem 5.13 on page 215. □

The next lemma is a Galois-theoretic result required for the subsequent lemma.

Lemma 5.13 Let K_j/F be Galois extensions of number fields for $j = 1, 2$. Then each of the following holds.

(a) K_1K_2/K_2 is a Galois extension and

$$\operatorname{Gal}(K_1K_2/K_2) \cong \operatorname{Gal}(K_1/K_1 \cap K_2).$$

(b) The extension $K_1K_2/K_1 \cap K_2$ is Galois, and we have the isomorphism of Galois groups, $\operatorname{Gal}(K_1K_2/K_1 \cap K_2) \cong \operatorname{Gal}(K_1/K_1 \cap K_2) \times \operatorname{Gal}(K_2/K_1 \cap K_2)$. In particular, if $K_1 \cap K_2 = F$, then

$$\operatorname{Gal}(K_1K_2/F) \cong \operatorname{Gal}(K_1/F) \times \operatorname{Gal}(K_2/F).$$

(c) If K_j/F for $j = 1, 2$ are abelian extensions of number fields, then K_1K_2/F is also abelian.

Proof. (a) By Exercise 2.6 on page 63 there exist $|K_1K_2 : K_2|$ embeddings of K_1K_2 into $\mathbb{C}$ that fix K_2 pointwise. If σ is such an extension, then

$$\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = \sigma(K_1)K_2 \subseteq K_1K_2.$$

Hence, K_1K_2/K_2 is Galois. Consider the mapping

$$\psi : \operatorname{Gal}(K_1K_2/K_2) \mapsto \operatorname{Gal}(K_1/K_1 \cap K_2),$$

given by $\sigma \mapsto \sigma|_{K_1}$, the restriction to K_1. By Exercise 2.6 this is an epimorphism. It remains to show that $\ker(\psi) = 1$. If $\psi(\sigma) = 1$, then σ fixes K_1 pointwise, but σ already fixes K_2 pointwise by definition, so σ fixes K_1K_2 pointwise. In other words, $\sigma = 1$, so $\ker(\psi) = 1$, and

$$\operatorname{Gal}(K_1K_2/K_2) \cong \operatorname{Gal}(K_1/K_1 \cap K_2).$$

(b) By the same reasoning as in the proof of part (a), $K_1K_2/K_1 \cap K_2$ is Galois. Also, by Theorem 2.4 on page 60, $K_j/K_1 \cap K_2$ is Galois for $j = 1, 2$. Consider the mapping

$$\rho : \operatorname{Gal}(K_1K_2/K_1 \cap K_2) \mapsto \operatorname{Gal}(K_1/K_1 \cap K_2) \times \operatorname{Gal}(K_2/K_1 \cap K_2)$$

given by

$$\rho : \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2}),$$

the restrictions to K_1 and K_2 respectively, which is an epimorphism by Exercise 2.6. We need to verify that $\ker(\rho) = 1$. If $\rho(\sigma) = (1, 1)$, then σ fixes both K_1 andK_2 pointwise, so $\sigma = 1$, as required.

(c) By part (b),

$$\mathrm{Gal}(K_1K_2/K_1 \cap K_2) \cong \mathrm{Gal}(K_1/K_1 \cap K_2) \times \mathrm{Gal}(K_2/K_1 \cap K_2) = G_1 \times G_2.$$

Since $G_j \subseteq \mathrm{Gal}(K_j/F)$ for $j = 1, 2$, both of which are abelian, then G_j is abelian for $j = 1, 2$, so $\mathrm{Gal}(K_1K_2/K_1 \cap K_2)$ is abelian. However, by Exercise 2.6, K_1K_2/F is Galois, and the F-automorphisms of $K_1 \cap K_2$ extend to $|K_1K_2 : K_1 \cap K_2|$ embeddings of K_1K_2 into $\mathbb{C}$, so $\mathrm{Gal}(K_1K_2/F)$ is abelian. □

Lemma 5.14 If $F/\mathbb{Q}$ is an abelian extension with $|F : \mathbb{Q}|$ andΔ_F both being powers of a prime p, then $F \subseteq \mathbb{Q}(\zeta_p^k)$ for some $k \in \mathbb{N}$.

Proof. We split the proof into the odd and even cases.

Case 5.4 $p > 2$

Let

$$K = \mathbb{Q}(\zeta_{p^{m+1}}), \text{ where } |F : \mathbb{Q}| = p^m.$$

By Application 5.1 on page 229, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order $\phi(p^{m+1})$. Let H be a subgroup of it of order $p - 1$, and let L be the fixed field of H.

Claim 5.17 $|FL : \mathbb{Q}|$ is a power of p.

Since $|H| = p - 1$, then $L/\mathbb{Q}$ is a cyclic extension withΔ_L a power of p given that$\Delta_L \mid \Delta_K$. Thus, FL is an abelian extension of $\mathbb{Q}$ by part (c) of Lemma 5.13 on the preceding page. Also,

$$|FL : \mathbb{Q}| = |FL : L| \cdot |L : \mathbb{Q}| = |F : F \cap L| \cdot |L : \mathbb{Q}|,$$

which is a power of p, where the last equality comes from part (a) of Lemma 5.13.

Claim 5.18 Δ_{FL} is a power of p.

Suppose that $q \mid \Delta_{FL}$. Then by Exercise 5.37 on page 243, either q is ramified in $L/\mathbb{Q}$ or q is ramified in $F/\mathbb{Q}$. Therefore, either $q \mid \Delta_L$ or $q \mid \Delta_F$. However,$\Delta_L \mid \Delta_{\mathbb{Q}(\zeta_{p^{m+1}})}$, which is a power of p, andΔ_F is a power of p by hypothesis, so $q = p$. This establishes Claim 5.18.

In view of Claims 5.17–5.18, we may invoke Exercise 5.41 on page 253 to get that $\mathrm{Gal}(FL/\mathbb{Q})$ is cyclic of prime power order. Since, by part (b) of Lemma 5.13,

$$\mathrm{Gal}(FL/L \cap F) \cong \mathrm{Gal}(F/L \cap F) \times \mathrm{Gal}(L/L \cap F),$$

then by Exercise 5.40, either $\mathrm{Gal}(F/L \cap F) = 1$ or $\mathrm{Gal}(L/L \cap F) = 1$. If the former occurs, then $F = L \cap F$, so $F \subseteq L$, and in the latter case, $L = L \cap F$, so $L \subseteq F$. However, $|F : \mathbb{Q}| = |L : \mathbb{Q}|$, so $F = L$, which implies that $F \subseteq \mathbb{Q}(\zeta_{p^{m+1}})$, thereby establishing Case 5.4.

Case 5.5 $p = 2$

Claim 5.19 For any $m \in \mathbb{N}$, there exists a totally real field K such that $|K : \mathbb{Q}| = 2^m$ with $\Delta_K = 2^n$, and $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$ for some $n \in \mathbb{N}$.

Let $L = \mathbb{Q}(\zeta_{2^{m+2}})$ and set $K = L \cap \mathbb{R}$. Since $m + 2 \geq 3$, then $\sqrt{-1} = i \in L$, so for $a \pm bi \in L$, we must have $2a, 2b \in K$. Therefore, $a, b \in K$ and $L = K(i)$. Hence, $|L : K| = 2$, so $|K : \mathbb{Q}| = 2^m$. If $q \mid \Delta_K$ for a prime q, then q ramifies in K, so q ramifies in L. Thus, $q \mid \Delta_K$, which is a power of 2, so $q = 2$. Thus,$\Delta_K = 2^n$ for some $n \in \mathbb{N}$. This completes Claim 5.19.

Claim 5.20 For a given $m \in \mathbb{N}$, the field K in Claim 5.19 is unique.

K is the maximal real subfield of $\mathbb{Q}(\zeta_{2^{m+2}})$. If $K_1 \neq K$ is another such field, then

$$|KK_1 : \mathbb{Q}| \geq 2^{m+2}.$$

Therefore, $KK_1 = \mathbb{Q}(\zeta_{2^{m+2}})$, contradicting the fact that KK_1 is real. This establishes Claim 5.20.

Since F and $\mathbb{Q}(i)$ are abelian extensions of $\mathbb{Q}$, then $F(i)$ is an abelian extension with degree a power of 2 over $\mathbb{Q}$, by part (c) of Lemma 5.13. Let

$$K = F(i) \cap \mathbb{R}.$$

Then K is a real extension of $\mathbb{Q}$,

$$|K : \mathbb{Q}| = 2^s$$

for some $s \in \mathbb{N}$, andΔ_K is also a power of 2. By Claims 5.19–5.20, $K \subseteq \mathbb{Q}(\zeta_{2^{s+2}})$. Since $F(i) = K(a+bi)$ for some $a, b \in \mathbb{R}$, then given that $a - bi \in F(i)$, we must have $a \in K$ and $bi \in F(i)$. Thus, $b^2 \in K$, so $a + bi$ is a root of

$$x^2 - 2ax + a^2 + b^2 \in K[x].$$

Hence, $|F(i) : F| = 2$. Therefore,

$$F \subseteq F(i) = K(i) \subseteq \mathbb{Q}(\zeta_{2^{s+2}}, i) \subseteq \mathbb{Q}(\zeta_r),$$

for some $r \in \mathbb{N}$, which establishes the full result. □

Before proceeding, we need the following important concepts, which are related to Definition 5.13 on page 224.

Definition 5.16 — Ramification Groups and Ramification Fields

Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. For each nonnegative integer j define:

$$\mathcal{V}_j = \{\sigma \in \mathcal{T}_{\mathcal{P}}(K/F) : \alpha^\sigma \equiv \alpha \pmod{\mathcal{P}^{j+1}} \text{ for all } \alpha \in \mathfrak{O}_K\},$$

called the j^{th} ramification group of $\mathcal{P}$ in K/F. The fixed field $V_{\mathcal{P}}^{(j)}(K/F)$ is called the j^{th} ramification field.[5.18] (Note that $\mathcal{T}_{\mathcal{P}}(K/F) = \mathcal{V}_0$ and $V_{\mathcal{P}}^{(0)}(K/F) = T_{\mathcal{P}}(K/F)$.)

We now establish some properties of the concepts in Definition 5.16 since they are needed in the sequel.

Lemma 5.15

(a) $\mathcal{V}_j$ is a normal subgroup of $\mathcal{T}_{\mathcal{P}}(K/F)$.

(b) $\mathcal{T}_{\mathcal{P}}(K/F) = \mathcal{V}_0 \supseteq \mathcal{V}_1 \supseteq \cdots$.

(c) There exists an $m \in \mathbb{N}$ such that $\mathcal{V}_m = 1$.

[5.18] The letter V is used for the ramification fields given that the derivation is from the German *Verzweigungskörper*—see Footnote 5.9 on page 224. The ramification groups were first defined by Hilbert in 1894—see Biography 3.4 on page 94.

(d) If $K_{\mathcal{P}}^*$ denotes the multiplicative group of nonzero elements of the field $K_{\mathcal{P}} = \mathfrak{O}_K/\mathcal{P}$, there exists a natural group isomorphism of $\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1$ into $K_{\mathcal{P}}^*$.

(e) $\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1$ is a cyclic group with order not divisible by p where $p = \mathcal{P} \cap \mathbb{Z}$.

(f) For $j \geq 0$, the groups $\mathcal{V}_{j-1}/\mathcal{V}_j$ are elementary abelian p-groups. In other words, they are finite dimensional vector spaces over $\mathbb{F}_p$.

(g) $\mathcal{V}_1$ is a p-group, and $T_{\mathcal{P}}^{(1)}(K/F)$ is the maximal tamely ramified extension at $\mathcal{P}$ contained in K.

(h) Suppose that $\mathcal{D}_{\mathcal{P}}(K/F)$ is abelian, and set $q = |F_{\mathfrak{p}}| = N^{F/\mathbb{Q}}(\mathfrak{p})$, where $F_{\mathfrak{p}} = \mathfrak{O}_F/\mathfrak{p}$. Then $\tau^{q-1} \in \mathcal{V}_1$ for all $\tau \in \mathcal{T}_{\mathcal{P}}(K/F)$ and

$$|\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1| \mid (q-1).$$

Proof. (a) If $\sigma \in \mathcal{T}_{\mathcal{P}}(K/F)$, then $\mathcal{P}^\sigma = \mathcal{P}$, so $(\mathcal{P}^{j+1})^\sigma = \mathcal{P}^{j+1}$. Thus, σ has the action

$$\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)},$$

where the $\overline{x}$ denotes the image of $x \in \mathfrak{O}_K$ in $\mathfrak{O}_K/\mathcal{P}^{j+1}$ under the natural mapping

$$\psi : \mathfrak{O}_K \mapsto \mathfrak{O}_K/\mathcal{P}^{j+1}.$$

Therefore, $\sigma \in \mathcal{V}_j$ if and only if σ is the identity mapping on $\mathfrak{O}_K/\mathcal{P}^{j+1}$. Since $\ker(\psi) = \mathcal{V}_j$, then by Theorem A.5 on page 328, $\mathcal{V}_j$ is a normal subgroup of $\mathcal{T}_{\mathcal{P}}(K/F)$.

(b) We have that $\mathcal{V}_{j+1} \subseteq \mathcal{V}_j$ for $j = 0, 1, \ldots$ since $\alpha^\sigma \equiv \alpha \,(\text{mod } \mathcal{P}^{j+2})$ implies that $\alpha^\sigma \equiv \alpha$ $(\text{mod } \mathcal{P}^{j+1})$.

(c) If $\sigma \in \cap_{j=0}^{\infty}\mathcal{V}_j$, then $\sigma(\alpha) - \alpha \in \cap_{j=0}^{\infty}\mathcal{P}^{j+1}$. Therefore, $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathfrak{O}_K$. Hence, $\cap_{j=0}^{\infty}\mathcal{V}_j = 1$. However, $\mathcal{T}_{\mathcal{P}}(K/F)$ is a finite group, so there must exist an $m \in \mathbb{N}$ such that $\mathcal{V}_m = 1$.

(d) Let $\mathfrak{O}_K/\mathcal{P} = K_{\mathcal{P}}$.

Claim 5.21 For a fixed $\gamma \in \mathcal{P} - \mathcal{P}^2$, and any $\sigma \in \mathcal{T}_{\mathcal{P}}(K/F)$, there exists $\alpha_\sigma \in \mathfrak{O}_K$ such that for

$$\gamma^\sigma \equiv \alpha_\sigma \gamma \pmod{\mathcal{P}^2},$$

where α_σ is uniquely determined modulo $\mathcal{P}$.

Let $\gamma\mathfrak{O}_K = \mathcal{P}I$, where $\mathcal{P} \nmid I$. Then by Theorem 1.21 on page 32, there exists a solution to the system of congruences

$$x \equiv \gamma^\sigma \pmod{\mathcal{P}^2},$$

$$x \equiv 0 \pmod{I}.$$

Let $\alpha_\sigma = x\gamma^{-1}$. Then α_σ is uniquely determined modulo $\mathcal{P}$ and

$$\alpha_\sigma\gamma = x \equiv \gamma^\sigma \pmod{\mathcal{P}^2}.$$

This completes the proof of Claim 5.21.

Claim 5.22 For any σ,τ $\in \mathcal{T}_{\mathcal{P}}(K/F)$, $\alpha_{\sigma\tau} \equiv \alpha_\sigma\alpha_\tau \,(\text{mod } \mathcal{P})$.

We have

$$\alpha_{\sigma\tau}\gamma \equiv \gamma^{\sigma\tau} \equiv (\gamma^{\sigma})^{\tau} \equiv (\alpha_{\sigma}\gamma)^{\tau} \equiv \alpha_{\sigma}^{\tau}\gamma^{\tau} \equiv \alpha_{\sigma}^{\tau}\alpha_{\tau}\gamma \pmod{\mathcal{P}^2}.$$

Since $\gamma \in \mathcal{P} - \mathcal{P}^2$, then by multiplying through the congruence

$$\alpha_{\sigma\tau}\gamma \equiv \alpha_{\sigma}^{\tau}\alpha_{\tau}\gamma \pmod{\mathcal{P}^2}$$

by γ^{-1} we get,

$$\alpha_{\sigma\tau} \equiv \alpha_{\sigma}^{\tau}\alpha_{\tau} \pmod{\mathcal{P}}.$$

However, $\alpha_{\sigma}^{\tau} \equiv \alpha_{\sigma} \,(\text{mod }\mathcal{P})$ for all $\tau \in \mathcal{T}_{\mathcal{P}}(K/F)$. This yields Claim 5.22.

Define a map:

$$\rho : \mathcal{T}_{\mathcal{P}}(K/F) \mapsto K_{\mathcal{P}}^{*},$$

by

$$\rho : \sigma \mapsto \alpha_{\sigma}.$$

By Claims 5.21–5.22, ρ is a well-defined homomorphism of groups. Since $\alpha_{\sigma} = 1$ if and only if $\gamma^{\sigma} \equiv \gamma \,(\text{mod }\mathcal{P}^2)$, by Claim 5.21, then $\alpha_{\sigma} = 1$ holds if and only if $\sigma \in \mathcal{V}_1$, so $\mathcal{V}_1 = \ker(\rho)$. This completes the proof of (d).

(e) If $e_1 = |\text{img}(\rho)|$, then $p \nmid e_1$ since

$$e_1 \;\Big|\; |K_{\mathcal{P}}^{*}| = p^e - 1$$

for some $e \in \mathbb{N}$. Also, since $\text{img}(\rho)$ is a subgroup of $K_{\mathcal{P}}^{*}$, then by Theorem A.8 on page 331, $\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1$ is a cyclic group, and by the above has order prime to p. This is (e).

(f) This part proceeds in much the same fashion as the solution to (d), except that we work on the *additive group* $K_{\mathcal{P}}^{+}$ of $K_{\mathcal{P}}$. Let $\gamma \in \mathcal{P} - \mathcal{P}^2$ be fixed. Then $\gamma^j \in \mathcal{P}^j - \mathcal{P}^{j+1}$ for any $j \in \mathbb{N}$.

Claim 5.23 For any $\sigma \in \mathcal{V}_{j-1}$, there exists $\alpha_{\sigma} \in \mathfrak{O}_K$ such that

$$\gamma^{\sigma} \equiv \gamma + \alpha_{\sigma}\gamma^{j} \pmod{\mathcal{P}^{j+1}}.$$

Set $\gamma\mathfrak{O}_K = \mathcal{P}^j I$ where $\mathcal{P} \nmid I$. By the Chinese Remainder Theorem for ideals cited above, there exists a solution to the congruences

$$x \equiv \gamma^{\sigma} \pmod{\mathcal{P}^{j+1}}, \text{ and } x \equiv 0 \pmod{I}.$$

Select $\alpha_{\sigma} = (x - \gamma)\gamma^{-j}$. Then

$$\alpha_{\sigma}\gamma^{j} \equiv x - \gamma \equiv \gamma^{\sigma} - \gamma \pmod{\mathcal{P}^{j+1}}.$$

Thus,

$$\gamma^{\sigma} \equiv \gamma + \alpha_{\sigma}\gamma^{j} \pmod{\mathcal{P}^{j+1}},$$

which is Claim 5.23.

Claim 5.24 For all $\sigma,\tau \in \mathcal{V}_{j-1}$, $\alpha_{\sigma\tau} \equiv \alpha_{\sigma} + \alpha_{\tau} \,(\text{mod }\mathcal{P})$.

We have that

$$\alpha_{\sigma\tau}\gamma^{j} \equiv \gamma^{\sigma\tau} - \gamma \equiv (\gamma^{\sigma})^{\tau} - \gamma \equiv (\gamma + \alpha_{\sigma}\gamma^{j})^{\tau} - \gamma \equiv \gamma^{\tau} + \alpha_{\sigma}^{\tau}\gamma^{j\tau} - \gamma$$

$$\equiv \gamma + \alpha_{\tau}\gamma^{j} + \alpha_{\sigma}^{\tau}(\gamma^{\tau})^{j} - \gamma \equiv \gamma^{j}(\alpha_{\tau} + \alpha_{\sigma}^{\tau}\gamma^{j(\tau-1)}) \pmod{\mathcal{P}^{j+1}}.$$

Thus, multiplying through by γ^{-j} we get

$$\alpha_{\sigma\tau} \equiv \alpha_\tau + \alpha_\sigma^\tau \gamma^{j(\tau-1)} \pmod{\mathcal{P}}.$$

Since $\alpha_\sigma^\tau \equiv \alpha_\sigma \pmod{\mathcal{P}}$ for all $\tau \in \mathcal{V}_{j-1} \subseteq \mathcal{V}_0$ and $\gamma^{j(\tau-1)} \equiv 1 \pmod{\mathcal{P}}$ given that $\gamma^{j\tau} \equiv \gamma^j$ (mod $\mathcal{P}$), then Claim 5.24 follows.

Define a map

$$\rho_1 a : \mathcal{V}_{j-1} \mapsto K_{\mathcal{P}}^+,$$

by

$$\sigma \mapsto \alpha_\sigma,$$

which is a well-defined additive group homomorphism independent of the choice of α by Claims 5.23–5.24, and $\ker(\rho_1) = \mathcal{V}_j$. Hence, $\mathcal{V}_{j-1}/\mathcal{V}_j$ is a direct sum of cyclic groups of order p, since $K_{\mathcal{P}}^+$ is such a sum, so $\mathcal{V}_{j-1}/\mathcal{V}_j$ is an elementary abelian p-group, thereby securing (f).

(g) By parts (b)–(c) above,

$$\mathcal{V}_0 \supseteq \mathcal{V}_1 \supseteq \cdots \supseteq \mathcal{V}_m = 1,$$

for some $m \in \mathbb{N}$. Also, $\mathcal{V}_0/\mathcal{V}_1$ is a cyclic group, and $\mathcal{V}_{j-1}/\mathcal{V}_j$ is an elementary abelian p-group by parts (e)–(f) just proved, so $\mathcal{V}_1$ is a p-group. Hence, $T_{\mathcal{P}}^{(1)}(K/F)$ is the maximal tamely ramified extension at $\mathcal{P}$ contained in K, which is (g).

(h) Let $\sigma \in \mathcal{D}_{\mathcal{P}}(K/F)$ be the element such that its image in $\mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$ is the Frobenius automorphism. Then for each $\tau \in \mathcal{T}_{\mathcal{P}}(K/F)$, we have from Claim 5.21 in the proof of part (d) that

$$\begin{aligned}\gamma^{\sigma^{-1}\tau\sigma} &\equiv (\gamma\alpha_{\sigma^{-1}})^{\tau\sigma} \equiv (\gamma^\tau \alpha_{\sigma^{-1}}^\tau)^\sigma \equiv (\alpha_\tau\gamma\alpha_{\sigma^{-1}}^\tau)^\sigma \\ &\equiv \alpha_\tau^\sigma \gamma^\sigma \alpha_{\sigma^{-1}}^{\tau\sigma} \equiv \alpha_\tau^\sigma\gamma^\sigma\alpha_{\sigma^{-1}}^\sigma \equiv \alpha_\tau^\sigma\alpha_\sigma\gamma\alpha_{\sigma^{-1}}^\sigma \pmod{\mathcal{P}^2}.\end{aligned}$$

We have shown that

$$\gamma^{\sigma^{-1}\tau\sigma} \equiv \alpha_\tau^\sigma \alpha_\sigma \alpha_{\sigma^{-1}}^\sigma \gamma \pmod{\mathcal{P}^2}. \tag{5.43}$$

Claim 5.25 $\alpha_\sigma\alpha_{\sigma^{-1}}^\sigma \equiv 1 \pmod{\mathcal{P}^2}$.

We have

$$\gamma^\sigma \equiv \alpha_\sigma\gamma \pmod{\mathcal{P}^2}, \tag{5.44}$$

and

$$\gamma^{\sigma^{-1}} \equiv \alpha_{\sigma^{-1}}\gamma \pmod{\mathcal{P}^2}. \tag{5.45}$$

Putting together (5.44)–(5.45), we get

$$(\alpha_{\sigma^{-1}})^\sigma\alpha_\sigma \equiv (\gamma^{\sigma^{-1}}\gamma^{-1})^\sigma\alpha_\sigma \equiv \gamma\gamma^{\sigma^{-1}}\alpha_\sigma \equiv (\gamma\alpha_\sigma)\gamma^{\sigma^{-1}} \equiv \gamma^\sigma\gamma^{\sigma^{-1}} \equiv 1 \pmod{\mathcal{P}^2},$$

as required to complete Claim 5.25.

By Claim 5.25 and (5.43) and the fact that σ is the element such that its image in $\mathrm{Gal}(K_{\mathcal{P}}/F_{\mathfrak{p}})$ is the Frobenius automorphism,

$$\gamma^{\sigma\tau\sigma^{-1}} \equiv \alpha_\tau^\sigma\gamma \equiv \alpha_\tau^q\gamma \pmod{\mathcal{P}^2}. \tag{5.46}$$

However, $\gamma^\tau \equiv \alpha_\tau\gamma \pmod{\mathcal{P}^2}$, $\gamma^{\tau^2} \equiv \alpha_\tau^2\gamma \pmod{\mathcal{P}^2}$, and so on. Thus, by induction

$$\gamma^{\tau^q} \equiv \alpha_\tau^q\gamma \pmod{\mathcal{P}^2}. \tag{5.47}$$

Combining (5.46)–(5.47), we get $\gamma^{\sigma\tau\sigma^{-1}} \equiv \gamma^{\tau^q} (\text{mod } \mathcal{P}^2)$. Thus, $\gamma^{\sigma\tau\sigma^{-1}\tau^{-q}} \equiv \gamma (\text{mod } \mathcal{P}^2)$. We have shown that $\sigma\tau\sigma^{-1}\tau^{-q} \in \mathcal{V}_1$. When $\mathcal{D}_{\mathcal{P}}(K/F)$ is abelian, then

$$(\sigma\tau\sigma^{-1}\tau^{-q})^{-1} = \tau^{q-1} \in \mathcal{V}_1,$$

for all $\tau \in \mathcal{T}_{\mathcal{P}}(K/F)$. Since $\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1$ is cyclic and $\tau^{q-1}\mathcal{V}_1 = \mathcal{V}_1$, then

$$|\mathcal{T}_{\mathcal{P}}(K/F)/\mathcal{V}_1| \,\big|\, (q-1),$$

which is (h) so we are done. □

Lemma 5.16 Let F be an abelian number field over $\mathbb{Q}$ with $|F:\mathbb{Q}| = n$. Then for every prime $p \,\big|\, \Delta_F$, with $p \nmid n$, there exists an abelian number field K over $\mathbb{Q}$ such that $|K:\mathbb{Q}| \,\big|\, n$, $F \subseteq K(\zeta_p)$, and $p \nmid \Delta_K$. Furthermore, any prime divisor ofΔ $_K$ is a prime divisor ofΔ $_F$.

Proof. We break this into two cases.

Case 5.6 $p \,\big|\, \Delta_F$, $p \nmid n$, and $\zeta_p \in F$.

Since $p \nmid n$, then by Theorem 5.4 on page 189, $p \nmid e_{F/\mathbb{Q}}(p)$. By part (g) of Lemma 5.15 on page 247, $|F : V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})|$ is a power of p, but $|F : V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})| \,\big|\, n$, so $F = V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})$, where $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal over p. By part (h) of Lemma 5.15, $|\mathcal{T}_{\mathfrak{p}}(F/\mathbb{Q})/\mathcal{V}_1| \,\big|\, (p-1)$, but since $F = V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})$, then $|\mathcal{T}_{\mathfrak{p}}(F/\mathbb{Q})| \,\big|\, (p-1)$. However, by Theorem 5.1 on page 184,

$$e_{F/\mathbb{Q}}(\mathfrak{p}) = e_{F/\mathbb{Q}(\zeta_p)}(\mathfrak{p}) e_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\mathfrak{p} \cap \mathbb{Z}[\zeta_p]).$$

Since $|\mathbb{Q}(\zeta_p) : Q| = p-1$, by Corollary 1.17 on page 41, then $e_{F/\mathbb{Q}(\zeta_p)}(\mathfrak{p}) = 1$.

Claim 5.26 $K = T_{\mathfrak{p}}(F/\mathbb{Q})$ satisfies the conditions of the lemma.

Since $\text{Gal}(F/\mathbb{Q})$ is abelian, then $K/\mathbb{Q}$ is an abelian extension with $|K:\mathbb{Q}| \,\big|\, n$. Also,

$$\mathcal{T}_{\mathfrak{p}}(K/\mathbb{Q}(\zeta_p)) = \mathcal{T}_{\mathfrak{p}}(F/\mathbb{Q}) \cap \text{Gal}(K/\mathbb{Q}(\zeta_p)).$$

By a similar argument to the above, the first ramification field of $\mathfrak{p}$ in $F/\mathbb{Q}(\zeta_p)$ is

$$V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q}(\zeta_p)) = F.$$

Therefore, $|F : K(\zeta_p)| = e_{\mathfrak{p}}(F/\mathbb{Q}(\zeta_p)) = 1$, so $F = K(\zeta_p)$. Since $K = T_{\mathfrak{p}}(K/\mathbb{Q})$, then $p \nmid \Delta_K$ by Corollary 5.8 on page 210. Furthermore, if $q \neq p$ is a prime with $q \,\big|\, \Delta_K$, then q ramifies in $K/\mathbb{Q}$, and so must ramify in $F/\mathbb{Q}$. Hence, $q \,\big|\, \Delta_F$, which completes Claim 5.26, and so Case 5.6.

Case 5.7 $p \,\big|\, \Delta_F$, $p \nmid n$, and $\zeta_p \notin F$.

Let $L = F \cap \mathbb{Q}(\zeta_p)$. Then by part (b) of Lemma 5.13 on page 245, $\text{Gal}(F(\zeta_p)/L) \cong \text{Gal}(F/L) \times \text{Gal}(\mathbb{Q}(\zeta_p)/L)$. Thus,

$$|F(\zeta_p) : L| \cdot |L : \mathbb{Q}| = |F(\zeta_p) : \mathbb{Q}| = |F : L| \cdot |\mathbb{Q}(\zeta_p) : L| \cdot |L : \mathbb{Q}|,$$

and this last value equals both

$$|F : L| \cdot |\mathbb{Q}(\zeta_p) : \mathbb{Q}| = |F : L| \cdot (p-1), \tag{5.48}$$

and

$$|F : \mathbb{Q}| \cdot |\mathbb{Q}(\zeta_p) : L| = n \cdot |\mathbb{Q}(\zeta_p) : L|. \tag{5.49}$$

From (5.48)–(5.49),

$$|F(\zeta_p):\mathbb{Q}| = |F:L|\cdot(p-1), \tag{5.50}$$

and

$$|F(\zeta_p):\mathbb{Q}| = n\cdot|\mathbb{Q}(\zeta_p):L|. \tag{5.51}$$

Thus, by multiplying (5.50)–(5.51), we get $|F(\zeta_p):\mathbb{Q}|^2 = |F:L|\cdot(p-1)\cdot n\cdot|\mathbb{Q}(\zeta_p):L|$. Therefore, since part (a) of Lemma 5.13 tells us that $|F(\zeta_p):F| = |\mathbb{Q}(\zeta_p):L|$, we have $|F(\zeta_p):\mathbb{Q}|\cdot|L:\mathbb{Q}|^2 = (p-1)\cdot n$. Hence,

$$|F(\zeta_p):\mathbb{Q}| \bigm| n\cdot(p-1). \tag{5.52}$$

Since p ramifies in F, then p ramifies in $F(\zeta_p)/\mathbb{Q}$. Therefore, $p \bigm| \Delta_{F(\zeta_p)}$. From (5.52), this yields that $p\nmid|F(\zeta_p):\mathbb{Q}|$. Let $\mathcal{P}$ be a prime $\mathfrak{O}_{F(\zeta_p)}$-ideal over p. Now we apply Case 5.6 to $F(\zeta_p)$. Let $K = T_{\mathcal{P}}(F(\zeta_p)/\mathbb{Q}) \subseteq F(\zeta_p)$. Then $|F(\zeta_p):K| = e_{\mathcal{P}}(F(\zeta_p)/\mathbb{Q}) = p-1$. Also,

$$|F(\zeta_p):\mathbb{Q}| = |F(\zeta_p):K|\cdot|K:\mathbb{Q}| = (p-1)\cdot|K:\mathbb{Q}|.$$

Thus, by (5.52), $|K:\mathbb{Q}| \bigm| n$. Since p is unramified in $K/\mathbb{Q}$, then $p\nmid\Delta_K$. Also, if $q\neq p$ is a prime such that $q \bigm| \Delta_K$, then q ramifies in $K/\mathbb{Q}$, so also in $F(\zeta_p)/\mathbb{Q}$. By Exercise 5.37 on page 243, q must be ramified in $F/\mathbb{Q}$ or in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Since $q\neq p$, then by Corollary 3.9 on page 125, q ramifies in $F/\mathbb{Q}$, so $q \bigm| \Delta_F$, and we have completed the entire proof. □

Lastly, we have the following concluding lemma.

Lemma 5.17 If Theorem 5.23 holds for abelian number fields whose degree and discriminant are a power of a given prime p, then it holds for arbitrary abelian extensions of degree a power of p.

Proof. Let $|F:\mathbb{Q}| = p^m$. If $q\neq p$ is a prime dividing$\Delta_{\ F}$, then by Lemma 5.16, there exists an abelian extension $K/\mathbb{Q}$ such that $F\subseteq K(\zeta_q)$, $|K:\mathbb{Q}| \bigm| |F:\mathbb{Q}|$, $q\nmid\Delta_K$, and if r is a prime dividing$\Delta_{\ K}$, then $r|\Delta_F$. Hence,$\Delta_{\ K}$ has *fewer* distinct prime divisors than Δ_F. Suppose that$\Delta_{\ K}$ is not a power of p. Then we repeat the above argument on K and get another field K_1 with$\Delta_{\ K_1}$ having fewer distinct prime factors than$\Delta_{\ K}$, while K_1 satisfies the properties of Lemma 5.16. Since there exist only finitely many such primes by Corollary 5.7 on page 210, we terminate this process after a finite number, $r+1$, of iterations. Therefore, for integers $s = 0,1,\ldots,r$, we have abelian extensions $K_s/\mathbb{Q}$ such that $|K_s:\mathbb{Q}|$ is a power of p, and $K_{s_j}\subseteq K_s(\zeta_{s_j})$, for some $s_j\in\mathbb{N}$, and $K_r\subseteq\mathbb{Q}(\zeta_r)$ for some $r\in\mathbb{N}$, with the last containment coming from Lemma 5.14 on page 246. Hence,

$$F\subseteq K(\zeta_{s_0}),\quad K\subseteq K_1(\zeta_{s_1}),\quad K_1\subseteq K_2(\zeta_{s_2}),\ldots,K_r\subseteq\mathbb{Q}(\zeta_{s_r}).$$

Therefore, $F\subseteq\mathbb{Q}(\zeta_{s_0},\zeta_{s_1},\ldots,\zeta_{s_r})\subseteq\mathbb{Q}(\zeta_n)$, where n is the lcm of the orders of the ζ_{s_j} for $j=0,1,\ldots,r$. □

Theorem 5.23 is now an immediate consequence of Lemmas 5.12–5.17. The proof of the Kronecker-Weber Theorem places us at the doorstep of class-field theory, at which we have already had a peek via Theorem 5.21 on page 239. The celebrated Kronecker-Weber Theorem was first stated by Kronecker in 1856, and first proved by H. Weber in 1886—see Biographies 4.9 on page 164 and 5.4 on page 254. Numerous proofs have been given since then. Among them are one given by Hilbert in 1896, one by F. Mertens in 1906, and another by Weber himself in 1907. A proof was given by the late Hans Zassenhaus in 1969. More recently a proof was given by Greenberg in 1974—see [23]–[24]. Although the proof of the latter is deemed to be "elementary," once all the facts cited therein are proved, the proof turns out to be longer than the once presented here and essentially the same sequence of lemmas is employed, so the reader is now provided with a relatively complete and straightforward introduction to the theorem.

Exercises

5.40. Let G be a cyclic group of order p^n where $n \in \mathbb{N}$ and p is prime. Prove that if $G \cong G_1 \times G_2$ where G_j are cyclic groups of order p^{m_j} for $j = 1, 2$, then either $m_1 = 0$ or $m_2 = 0$.

5.41. Prove that any number field F abelian over $\mathbb{Q}$ with *both* degree over $\mathbb{Q}$ and discriminant a power of an odd prime must be a cyclic extension of $\mathbb{Q}$.

5.42. Let G be a finite abelian p-group, where p is prime, and let $|G| = p^m$, for $m \in \mathbb{N}$. Establish the following two facts.

(a) For any subgroup H of G of order p^n with $n \in \mathbb{N}$, there exists a subgroup of G of order p^r for $n \le r \le m$ containing H.

(b) If G has only one subgroup of order p^{m-1}, then G is cyclic.

5.43. Let K/F be a Galois extension of number fields, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal. Prove that all ramification groups $\mathcal{V}_j$ for $j \ge 0$ are normal subgroups of $\mathcal{D}_{\mathcal{P}}(K/F)$.

(*Hint: See Lemma 5.15 on page 247.*)

5.44. Let K/F be a Galois extension of number fields, and let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n$ be the prime $\mathfrak{O}_K$-ideals ramified in K/F (possibly the empty set—see Remark 5.8 on page 240). Suppose that H is the subgroup of $\mathrm{Gal}(K/F)$ generated by the inertia groups $\mathcal{T}_{\mathcal{P}_j}(K/F)$ for $j = 1, 2, \ldots, n$, and let L be the fixed field of H. Prove that L is the maximal subfield of K that is unramified over F. In particular, conclude that if $F = \mathbb{Q}$, then $\mathrm{Gal}(K/F) = H$ is generated by the inertia groups. (*This result is called the* Monodromy Theorem *for algebraic number fields.*)

5.45. Suppose that K/F is a Galois extension of number fields with $\mathcal{P}$ a prime $\mathfrak{O}_K$-ideal. Let $\mathcal{V}_j$ for $j = 0, 1, 2, \ldots, m-1$ be all of the nontrivial ramification groups of K/F with different $\mathcal{D}_{K/F}$. Prove that if $\mathcal{P}^s \mid \mathcal{D}_{K/F}$, but $\mathcal{P}^{s+1} \nmid \mathcal{D}_{K/F}$, then

$$s = \sum_{j=0}^{m-1} (|\mathcal{V}_j| - 1).$$

(*This equation is called* Hilbert's formula.)

5.46. Let K/F be a Galois extension of number fields of degree n, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal with $e = e_{K/F}(\mathcal{P})$. Prove that $\mathcal{P}$ is tamely ramified in K/F if and only if $\mathcal{P}^e \nmid \mathcal{D}_{K/F}$. Conclude that $\mathcal{P}$ is tamely ramified in K/F if and only if $\mathfrak{p}^n \nmid \Delta_{K/F}$ where $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$. (Note that this establishes the promised converse of the result discussed in Remark 5.3 on page 213.)

5.47. Let K/F be an extension of number fields. Prove that $T_{K/F}(\mathfrak{O}_K) = \mathfrak{O}_F$ if and only if there is no prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ that divides $\mathcal{D}_{K/F}$.

5.48. Suppose that G is a multiplicative group of order n and R is a ring. Let $R[G]$ denote the additive abelian group

$$\sum_{g \in G} R = \underbrace{R + \cdots + R}_{n \text{ copies}}.$$

Thus, $R[G]$ consists of the formal sums $\sum_{j=1}^{n} r_{g_j} g_j$ for $r_{g_j} \in R$ and $g_j \in G$, with the sum ranging over all of the n elements g_j of G. Addition is defined by

$$\sum_{j=1}^{n} r_{g_j} g_j + \sum_{j=1}^{n} s_{h_j} g_j = \sum_{j=1}^{n} (r_{g_j} + s_{g_j}) g_j,$$

with possibly some zero coefficients to ensure that any two of these formal sums range over the same indices g_j for $j = 1, 2, \ldots, n$. Also, multiplication is defined by

$$\left(\sum_{i=1}^{m} r_{g_i} g_i\right)\left(\sum_{j=1}^{n} s_{h_j} h_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} (r_{g_i} s_{h_j})(g_i h_j).$$

Then with these operations $R[G]$ is called the *group ring of G over R*. Let K/F be a Galois extension of number fields with $G = \mathrm{Gal}(K/F)$ and $R = \mathfrak{O}_F$. Suppose further that $R[G] \cong \mathfrak{O}_K$. Prove that $T_{K/F}(\mathfrak{O}_K) = R$. In particular, when $F = \mathbb{Q}$, we think of $\mathfrak{O}_K$ and K as $\mathbb{Z}[G]$-modules by the action $(\sum_g r_g g)x = \sum_g r_g g(x)$ for $x \in K$. Use this to conclude that a Galois extension $K/\mathbb{Q}$ has a normal integral basis, namely a basis consisting of conjugates of a single integer, if and only if $\mathbb{Z}[G] \cong \mathfrak{O}_K$ as $\mathbb{Z}[G]$-modules—see Remark 2.3 on page 79.

5.49. Let K/F be a Galois extension of number fields such that $\mathfrak{O}_F[G] \cong \mathfrak{O}_K$ where $G = \mathrm{Gal}(K/F)$ (see Exercise 5.48). Prove that there does not exist any prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ such that $\mathfrak{p}^n \mid \Delta_{K/F}$ where $n = |G|$. Conclude that if $\mathfrak{O}_K \cong \mathfrak{O}_F[G]$ as an $\mathfrak{O}_F[G]$-module, then K/F is tamely ramified. (This result was first proved by A. Speiser in 1916.)

Biography 5.3 Andreas Speiser (1885–1970) was born on October 6, 1885. He studied at Göttingen from 1904 to 1909 as a student of Minkowski. His dissertation was on binary quadratic forms over general algebraic number fields. He wrote a book on group theory entitled *Die Theorie der Gruppen von endlicher Ordnung*, which was published in 1923. Several new editions came out, with the last one in 1980. He is also known for his editing of several collected works including, and especially, that of Euler. He died on December 10, 1970.

5.50. With reference to Exercises 5.48–5.49, prove that a quadratic extension K of $\mathbb{Q}$ with $\Delta_{K/\mathbb{Q}}$ even cannot have a normal integral basis.

Biography 5.4 Heinrich Martin Weber (1842–1913) was born on May 5, 1842 in Heidelberg, Germany. He was a student of Dedekind, and worked principally in algebra and number theory. His best-known work is his three-volume *Lehrbuch der Algebra*, which was published in 1895. This text became a standard, and influenced an entire generation of mathematicians to bring group theory into the twentieth century as a major branch of mathematics in its own right. Weber's proof of Theorem 5.23 on page 244 is known to have gaps (see the introduction to [27]). He died on May 17, 1913 in Strasbourg, Germany (now part of France).

5.7 An Application—Primality Testing

La dernièr chose qu'on trouve en faisant un ouvrage, est de savoir celle qu'il faut mettre la première.
The last thing one knows in constructing a work is what to put first.
From Section I, no. 19 of **Pensés (1670), ed. I. Brunschvieg (1909)**
Blaise Pascal (1623–1662)
French mathematician, physicist, and moralist

In this last section of chapter five, we look at an application of the contents to primality testing. By a *primality test*, we mean an algorithm that determines whether a given $n \in \mathbb{N}$ is prime. In this section, we look at a primality test described by Lenstra in [42]. This algorithm relies upon arithmetic in abelian extensions of $\mathbb{Q}$, and certain residue symbols. Hence, this may be viewed as an introduction to Chapter 6, as well as an application of the results of this chapter, including the Artin symbol and the Kronecker-Weber Theorem—see Definition 5.14 on page 229 and Theorem 5.23 on page 244.

The genesis of primality testing may be said to originate two hundred years before Christ with the *Sieve of Eratosthenes*—see [53, p. 32]. There is also the observation attributed to Fibonacci that a composite $n \in \mathbb{N}$ has a prime divisor less than $\sqrt{n}$. Another classical test given by *Wilson's Theorem* says that

$$n \in \mathbb{N} \text{ is prime if and only if } n \bigm| [(n-1)! + 1].$$

However, each of these three tests is highly inefficient. In other words, there is no known way to compute

$$(n-1)! + 1 \pmod{n},$$

for instance, in reasonable time for large values of n. Gauss computed large tables of primes, which provided enough data for him to conjecture the *Prime Number Theorem*—see Theorem A.28 on page 343. Gauss himself recognized the importance of factoring and primality testing, citing these being among the most important problems in arithmetic—see §4.4 for an overview of factoring. In the twentieth century, the pioneering work of D.H. Lehmer produced a school of thought in computational number theory that led to an array of very clever ideas for factoring and primality testing—see Biography 5.5 on page 259.

There are numerous primality tests both classical and recent. There is the *Elliptic curve test*, which the reader will find in [54], the *Lucas-Lehmer test*, *Pepin's test*, and *Pocklington's Theorem*, the details, for the latter three, which the reader will find in [53]. See also [71] for a detailed history of primality testing.

The test to be described in this section is based upon the following obvious result.

Theorem 5.24 Criterion for Primality
If $n \in \mathbb{N}$ with $n > 1$, then n is prime if and only if every divisor r of n is a power of n.

Of course, in practice, primality tests do not directly check that divisors of n are powers of n. However, this *is* done for *images* of r and n in certain groups G. Given a number $n \in \mathbb{N}$ to be tested, we proceed as follows. Set

$$\mathcal{S} = \{r \in \mathbb{N} : r \bigm| n\}.$$

There are three stages in primality testing algorithms based upon Theorem 5.24 on the previous page. They are described as follows.

Stage 1. This stage consists of finding a group G and a natural map σ from $\mathcal{S}$ to G with the property that $\sigma(r_1 r_2) = \sigma(r_1)\sigma(r_2)$ whenever $r_1, r_2 \in \mathcal{S}$. For instance, $G = (\mathbb{Z}/s\mathbb{Z})^*$ for some $s \in \mathbb{Z}$ such that $\gcd(s, n) = 1$ and $\sigma(r) = \overline{r}$, where $\overline{r}$ is the least positive residue of r modulo s, will suffice.

In the tests described below, G will always be $\mathrm{Gal}(K/\mathbb{Q})$ for some finite abelian extension K of $\mathbb{Q}$ such that $\gcd(\Delta_K, n) = 1$. By the Kronecker-Weber Theorem, there is an $s \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\zeta_s)$ with $\gcd(s, n) = 1$. Let $\theta \in \mathrm{Gal}(\mathbb{Q}(\zeta_s)/\mathbb{Q})$ defined by $\theta(\zeta_s) = \zeta_s^r$ for a given $r \in \mathcal{S}$. Then define $\sigma(r) = \theta|_K$. Observe that $\sigma(r_1 r_2) = \sigma(r_1)\sigma(r_2)$. Also, by Corollary 5.8 on page 210, r is unramified in K for any prime divisor r of n. Thus, if r is prime we may view $\sigma(r)$ as the Artin symbol $\left(\frac{K/\mathbb{Q}}{r}\right)$.

For any $r \in \mathcal{S}$, we define

$$K^{\sigma(r)} = \{\alpha \in K : \alpha^{\sigma(r)} = \alpha\},$$

and observe that if r is prime, then

$$K^{\sigma(r)} = Z_r(K/\mathbb{Q})$$

see Definition 5.12 on page 221.

Stage 2. This stage consists of showing that $\sigma(r)$ is a power of $\sigma(n)$ for any $r \bigm| n$, and we clearly may restrict our attention to prime divisors of n. In practice, this stage consists of putting n through a number of *pseudoprimality tests*—such as the Miller-Selfridge-Rabin test—[53, p. 119]— satisfying the properties:

(a) It is known that n passes the tests if n is prime.

(b) If n passes the tests, then we may conclude that $\sigma(r)$ is in the subgroup of G generated by $\sigma(n)$ for all divisors r of n.

In the tests described below, this stage will consist of looking for a ring homomorphism,

$$\psi : \mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z},$$

with $\psi(1) = 1$. To show that the finding of such a homomorphism will do the job described above for stage 2, we first show that when n is prime that such a homomorphism exists. Then we show that indeed its existence implies that $\sigma(r)$ is in the subgroup of G generated by $\sigma(n)$ for all divisors r of n.

Given that n is prime, $\sigma(n)$ is the Frobenius automorphism, or Artin symbol which generates the decomposition group of n in $K/\mathbb{Q}$. Therefore, by part (b) of Corollary 5.17 on page 227, the decomposition field of n in $K/\mathbb{Q}$,

$$K^{\sigma(n)} = Z_n(K/\mathbb{Q}),$$

is the largest subfield of K in which n splits completely. Therefore, there exists a prime $\mathfrak{O}_{K^{\sigma(n)}}$-ideal $\mathfrak{p}$ above n such that

$$\mathfrak{O}_{K^{\sigma(n)}}/\mathfrak{p} \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{F}_n$$

is the residue class field, so we have the existence of a ring homomorphism

$$\psi : \mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z}$$

—see Definition 5.1 on page 182 and Diagram 5.2 on page 228. However, if such a ψ exists, this does not ensure that n is prime. The methods for finding such a ψ *usually* detect a composite number, for example by finding an integer a such that $a^n \not\equiv a \pmod{n}$—see Exercise 4.31 on page 164. However, there exist composite integers such as $n = 561 = 3 \cdot 11 \cdot 17$ for which $a^n \equiv a \pmod{n}$ for all integers a—see Exercise 5.51 on page 260.

Suppose now that we have found such a ψ in stage 2 (and we assume that we can do so in computationally feasible time).[5.19] Let r be a prime divisor of n, and let

$$\rho : \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z}/r\mathbb{Z}$$

be the canonical map. Form $\rho \circ \psi : \mathfrak{O}_K \mapsto \mathbb{Z}/r\mathbb{Z}$, which is a ring homomorphism. Thus, the kernel of $\rho \circ \psi$ is an ideal $\mathcal{R}$ in $\mathfrak{O}_{K^{\sigma(n)}}$, and since

$$\mathfrak{O}_{K^{\sigma(n)}}/\mathcal{R} = \mathfrak{O}_{K^{\sigma(n)}}/\ker(\rho \circ \psi) = \operatorname{img}(\rho \circ \psi) = \mathbb{Z}/r\mathbb{Z},$$

then $\mathcal{R}$ is prime. Since $\mathcal{R}$ is of degree one, then

$$K^{\sigma(n)} \subseteq Z_r(K/\mathbb{Q}).$$

Thus, $K^{\sigma(n)}$ is fixed by $\sigma(n)$, and $Z_r(K/\mathbb{Q})$ is fixed by $\sigma(r)$. Thus, by Theorem 5.21 on page 239, $\langle \sigma(r) \rangle \subseteq \langle \sigma(n) \rangle$, as desired. Thus, we have shown that the existence of such a ψ guarantees that (b) above holds.

Stage 3. Use the information in Stages 1–2 to finish the primality test. In other words, the information will verify that n is prime or it will determine that it is composite.

The following is an application of the above primality test.

Example 5.15 Let $n \in \mathbb{N}$ be given, and let s be the largest divisor of $n-1$ for which we know a complete factorization. If $K = \mathbb{Q}(\zeta_s)$, then by Application 5.1 on page 229,

$$\operatorname{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/s\mathbb{Z})^*,$$

where $\sigma(r) \in \operatorname{Gal}(K/\mathbb{Q})$ corresponds to $\overline{r}$, with $\overline{r}$ denoting the residue class of r in $(\mathbb{Z}/s\mathbb{Z})^*$. Since $n \equiv 1 \pmod{s}$, then

$$K^{\sigma(n)} = K, \quad \mathfrak{O}_K = \mathbb{Z}[\zeta_s], \text{ and } m_{\zeta_s,\mathbb{Z}}(x) = \Phi_s(x).$$

If $a \in \mathbb{Z}$ such that

$$a^s \equiv 1 \pmod{n},$$

and

$$\gcd(a^{s/q} - 1, n) = 1$$

for all primes $q \bigm| s$, then the residue class of the s^{th} cyclotomic polynomial at a modulo n vanishes, namely

$$\overline{\Phi_s(a)} = 0$$

in $\mathbb{Z}/n\mathbb{Z}$. Given such a value a, we get a ring homomorphism $\psi : \mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z}$ by mapping ζ_s to a. Observe that $\zeta_s^s \mapsto a^s = 1$ in $\mathbb{Z}/n\mathbb{Z}$. Thus, by the discussion of stage 2 above, $\langle \sigma(r) \rangle \subseteq \langle \sigma(n) \rangle$. Therefore, $r \equiv 1 \pmod{s}$ for all $r \bigm| n$. Hence, if $s > \sqrt{n}$, it is certain that n is prime. This is known as *Pocklington's Theorem* see [53, Theorem 2.25, p. 123].

[5.19] The term *computationally feasible* or *computationally easy* means *in reasonable computational time.* On the other hand, problems that are *computationally infeasible*, or *computationally impossible* are those for which there (theoretically) exists a unique answer, but we cannot find it even if we devoted every scintilla of time and resources available. However, it should be stressed here that there is no *proved* example of a computationally infeasible problem.

A simple illustration of Example 5.15 on the previous page, is to test the fourth Fermat number

$$F_4 = 2^{16} + 1 = n$$

for primality. Let $s = 2^{16}$, $K = \mathbb{Q}(\zeta_s)$, and select $a = 3$. Then

$$a^s = 3^{2^{16}} \equiv 1 \pmod{n}, \text{ and } a^{s/2} = 3^{2^{15}} \not\equiv 1 \pmod{n}.$$

Hence, by Pocklington's Theorem, F_4 is prime.

The main application of Lenstra's primality test is described as follows.

Let $s \in \mathbb{N}$ such that $\gcd(s, n) = 1$, where the complete factorization of s is assumed to be known. Let t be the order of n modulo s. In other words, $t \in \mathbb{N}$ is the smallest value such that

$$n^t \equiv 1 \pmod{s}.$$

Thus, t is the order of n in $(\mathbb{Z}/s\mathbb{Z})^*$. For computational purposes, we assume that t is relatively *small.* Let $K = \mathbb{Q}(\zeta_s)$, so

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/s\mathbb{Z})^*$$

as above. By Corollary 5.13 on page 218,

$$|K : K^{\sigma(n)}| = t,$$

and

$$m_{\zeta_s, K^{\sigma(n)}}(x) = \prod_{j=0}^{t-1}(x - \zeta_s^{n^j}).$$

It follows from Example 1.22 on page 19 that $\mathfrak{O}_{K^{\sigma(n)}}$ is generated as a ring by the coefficients of $m_{\zeta_s, K^{\sigma(n)}}(x)$. Thus, to find a ring homomorphism

$$\psi : \mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z},$$

it suffices to find a ring extension R of $\mathbb{Z}/n\mathbb{Z}$ and a homomorphism

$$\hat{\psi} : \mathbb{Z}[\zeta_s] \mapsto R,$$

mapping the coefficients of $m_{\zeta_s, K^{\sigma(n)}}(x)$ inside $\mathbb{Z}/n\mathbb{Z}$. Suppose that we have such a ring. To find $\hat{\psi}$, it suffices to find

$$\hat{\psi}(\zeta_s) = a \in R$$

such that $a^s = 1$, $a^{s/q} - 1 \in R^*$ for all primes $q \mid s$, and

$$\prod_{j=0}^{t-1}(x - a^{n^j}) \in \frac{\mathbb{Z}}{n\mathbb{Z}}[x].$$

If such an element a has been found, there exists a ring homomorphism

$$\psi : \mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z},$$

so from Stage 2, it follows that every $r \mid n$ is congruent to a power of n modulo s.

If we assume that $s > \sqrt{n}$, then it suffices to try the least residues $\overline{n^j}$ modulo s for $j = 0, 1, 2, \ldots, t-1$ as possible divisors of n.[5.20]

To illustrate the above, we show that the following classical result is a special case of our test.

[5.20] In [42] it is concluded that the expected running time of the algorithm is less than $(\log n)^{c \log\log\log n}$, where c is some effectively computable constant.

Application 5.4 — Lucas–Lehmer Test for Mersenne Primes
Let $n = 2^m - 1$ with $m \in \mathbb{N}$, $m > 2$. Set $e_1 = 4$ and $e_{j+1} = e_j^2 - 2$ if $j \geq 1$. Then n is prime if and only if $e_{m-1} \equiv 0 \, (\text{mod } n)$.

To show that this test is a special case of our algorithm, we let $s = 2^{m+1}$ and $t = 2$. The interesting case occurs when m is odd (since the case for m even is easy). Define a ring

$$R = \frac{(\mathbb{Z}/n\mathbb{Z})[x]}{(x^2 - \sqrt{2}x - 1)},$$

where $\sqrt{2}$ means

$$2^{(m+1)/2} \pmod{n} \in \mathbb{Z}/n\mathbb{Z}.$$

Let $\hat{\psi} : \mathbb{Z}[\zeta_s] \mapsto R$, as above and set $\psi(x) = a$. Set $b = \sqrt{2} - a = -a^{-1}$, which is "the other" zero of $x^2 - \sqrt{2}x-.$ in R. By a simple induction argument

$$a^{2^j} + b^{2^j} \equiv e_j \pmod{n}, \tag{5.53}$$

for $j \in \mathbb{N}$. If n is prime, then R is a field in which a and b are conjugate, so $a^n = b$ by the theory of finite fields—see §2.1. Hence,

$$a^{2^m} = a^{n+1} = ba = -1,$$

so from (5.53), we get, $e_{m-1} \equiv a^{2^{m-1}} + b^{2^{m-1}} \equiv a^{2^{m-1}} + a^{-2^{m-1}} \equiv 0 \, (\text{mod } n)$. Conversely, if $e_{m-1} \equiv 0 \, (\text{mod } n)$, then $a^{2^m} \equiv -1 \, (\text{mod } n)$, so $a^s = a^{2^{m+1}} \equiv 1 \, (\text{mod } n)$. Thus, $a^{s/2} - 1 = -2 \in R^*$. From $a^n = a^{2^m - 1} \equiv -a^{-1} \equiv b \, (\text{mod } n)$, we get

$$(x - a)(x - a^n) \equiv (x - a)(x - b) \pmod{n},$$

and

$$(x - a)(x - b) = x^2 - \sqrt{2}x - 1 \in \frac{\mathbb{Z}}{n\mathbb{Z}}[x].$$

Hence, these conditions guarantee that there exists a ring homomorphism

$$\mathfrak{O}_{K^{\sigma(n)}} \mapsto \mathbb{Z}/n\mathbb{Z},$$

via Stage 1, and that every divisor of n is congruent to 1 or n modulo s. Hence, for $s > n$, we get that n is prime.

The test in this section can be used with that given in [1]. The reader is encouraged to solve Exercise 5.52 which opens the door to understanding the concepts used in [1], which also employs Artin symbols. Furthermore, the solution of Exercise 5.52 generalizes the notion of a quadratic Gauss sum given in Exercise 5.33 on page 232, and prepares the reader for Chapter 6 where we look at Reciprocity laws and residue symbols in general.

Biography 5.5 Derrick Henry Lehmer (1905–1991) was born on February 23, 1905 in Berkeley, California. He got his first degree from the University of California there in 1927. Then he achieved his Sc.M. from Brown University in 1929. Perhaps the best insight into his contributions may be seen in his collected works [36]. He was truly a pioneering giant in the world of computational number theory, and was widely respected in the mathematical community. He was also known for his valued sense of humour, as attested by John Selfridge in the forward to the aforementioned collected works, as well as by one of Lehmer's students, Ron Graham. In particular, Selfridge concludes with an apt description of Lehmer's contributions saying that he "has shown us this beauty with the sure hand of a master." He died on May 22, 1991.

Exercises

5.51. Prove that $x^{561} \equiv x \pmod{561}$ for all $x \in \mathbb{N}$.

(*The value* 561 *is the smallest* Carmichael number, *which is a composite integer* $n \in \mathbb{N}$ *such that* $a^{n-1} \equiv 1 \pmod{n}$ *for all* $a \in \mathbb{N}$ *such that* $\gcd(a, n) = 1$. *They are also known as* absolute pseudoprimes. *We have occasion to use this in text—see page 257.*)

5.52. Let $q = p^n$ where p is prime and $n \in \mathbb{N}$. If χ is a character on $\mathbb{F}_q^*$ and $\alpha \in \mathbb{F}_q^*$, then

$$G_\alpha(\chi) = \sum_{x=0}^{q-1} \chi(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x\alpha)},$$

is called the *Gauss sum on* $\mathbb{F}_q$ *belonging to the character* χ. (Recall that the trace of an element $T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \sum_{j=0}^{n-1} \alpha^{p^j}$, the sum of its conjugates over the base field, which is essentially the same as that given in Definitions 2.4 on page 65 and 5.2 on page 184 for number fields.)

Prove that for any $\alpha \in \mathbb{F}_q^*$ and any character χ on $\mathbb{F}_q^*$,

$$G_\alpha(\chi) = \chi(\alpha^{-1})G(\chi),$$

where $G(\chi) = G_1(\chi)$. Conclude in particular that

$$G_\alpha(\epsilon) = 0.$$

5.53. Prove that if $\alpha, x, y \in \mathbb{F}_q$, then

$$\frac{1}{q}\sum_{\alpha \in \mathbb{F}_q} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha(x-y))} = \delta_{x,y},$$

where $\delta_{x,y}$ is the Kronecker delta—see Theorem 5.7 on page 199 and Exercise 5.52.

5.54. Suppose that $\chi \neq \epsilon$ in Exercise 5.52. Establish the following generalization of Exercise 5.34 on page 232:

$$|G_\alpha(\chi)| = \sqrt{q}.$$

In particular, conclude that for any $\alpha \in \mathbb{F}_q^*$, we have

$$G_\alpha(\chi)G_\alpha(\chi^{-1}) = \chi(-1)q.$$

(*Hint: Use Exercise 5.53.*)

Chapter 6

Reciprocity Laws

> *Laws are like cobwebs, which catch small flies, but let wasps and hornets break through.*
> *from* **A critical essay upon the faculties of the mind (1709)**
> **Jonathan Swift (1667–1745)**
> *Anglo-Irish poet and satirist*

It may be said that the story of reciprocity laws is intimately linked with the history of algebraic number theory itself. Indeed, the historical evolution and generalization of the quadratic reciprocity law to residue symbols in algebraic number fields, essentially from Gauss to Artin, uses the techniques of algebraic number theory as an indispensable tool. Hence, understanding reciprocity laws is an integral part of algebraic number theory. Thus, we have left this topic to the concluding chapter, albeit we have already had a solid introduction via Definition 5.14 on page 229, Applications 5.1–5.3 on pages 229–231, and Exercise 5.36 on page 232, as well as the applications in §5.7. Furthermore, we motivated this chapter with the generalization of the quadratic Gauss sum given in Exercise 5.52. Since we have already dealt with the quadratic reciprocity law, as mentioned above, we begin with the next level up.

6.1 Cubic Reciprocity

Reciprocity laws arise from the following question. Given a fixed $n \in \mathbb{N}$, for which primes p, is there a solution $x \in \mathbb{Z}$ to the congruence

$$x^n \equiv a \pmod{p},$$

where $a \in \mathbb{Z}$ is known? More generally, we have the following.

Definition 6.1 — Power Residues

If $m, n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, then we say that a is an n^{th} *power residue modulo* m provided that

$$x^n \equiv a \pmod{m} \tag{6.1}$$

is solvable for some $x \in \mathbb{Z}$.

For instance, when $n = 2$, the residues are called *quadratic residues*, when $n = 3$ they are called *cubic residues*, when $n = 4$, they are called *quartic residues*, also called *biquadratic residues*, when $n = 5$ *quintic residues*, when $n = 6$, *sextic residues*, and so on.

When $n = 2$ and m is a prime, we get Gauss's Quadratic Reciprocity Law discussed in the preamble to this section on page 261. In this section, we study $n = 3$, called cubic reciprocity, predicted by Gauss. Eisenstein gave the first *published* proof of the Cubic Reciprocity Law in 1844—see Biography 3.10 on page 137. In this section, we will provide one of Eisenstein's proofs of this law.[6.1] First we need the following preliminary result, which is based upon ideal congruences introduced and explored in Exercises 4.25–4.32 on pages 163–164 with which the reader should be familiar at this juncture.

Remark 6.1 Note that by Corollaries 1.1 on page 13 and 1.6 on page 21, $\mathbb{Z}[\zeta_3]$ is a PID, equivalently a UFD by Theorem 1.18 on page 29. Thus, in what follows, the congruences modulo a prime element π of $\mathbb{Z}[\zeta_3]$ may be interpreted as congruences modulo the principal prime ideal (π).

Proposition 6.1 — Cubic Congruences

Suppose that $F = \mathbb{Q}(\zeta_3)$ and π is a prime element of $\mathfrak{O}_F$. If $\alpha \in \mathfrak{O}_F = \mathbb{Z}[\zeta_3]$ where $N_F(\pi) \neq 3$ and $\pi \nmid \alpha$, then there exists a unique nonnegative integer $n \leq 2$ such that

$$\alpha^{(N_F(\pi)-1)/3} \equiv \zeta_3^n \pmod{\pi}.$$

Proof. Since

$$\alpha^{N_F(\pi)-1} - 1 = \prod_{j=0}^{2}(\alpha^{(N_F(\pi)-1)/3} - \zeta_3^j), \tag{6.2}$$

then given $\pi \nmid \alpha$, we must have that π divides one of the factors on the right side of (6.2). If π divides two of these factors, then π divides the difference of them. The possible differences are $\pm(1-\zeta_3)$, $\pm(1-\zeta_3^2)$, and $\pm\zeta_3(1-\zeta_3)$, and by Exercises 2.24 on page 68 and 3.37 on page 129, the absolute value of the norms of any of these elements is 3. Therefore, by Exercise 2.46 on page 86, via Remark 6.1, $N_F(\pi) \bigm| 3$, a contradiction since $N_F(\pi) \neq 1, 3$. □

Proposition 6.1 provides the evidence that the following is well-defined.

Definition 6.2 — Cubic Residue Symbol

Suppose that $F = \mathbb{Q}(\zeta_3)$ and π is a prime element of $\mathfrak{O}_F$ with $N_F(\pi) \neq 3$. If $\alpha \in \mathfrak{O}_F$, then $(\frac{\alpha}{\pi})_3$ is defined by

$$\left(\frac{\alpha}{\pi}\right)_3 = 0 \text{ if } \pi \bigm| \alpha,$$

and

$$\left(\frac{\alpha}{\pi}\right)_3 = \zeta_3^n \text{ if } \pi \nmid \alpha,$$

where n is the unique integer determined by the congruence in Proposition 6.1.

If $\beta \in \mathfrak{O}_F$ is a nonzero, nonunit element, and

$$\beta = \prod_{j=1}^{m} \pi_j,$$

[6.1] Jacobi had already worked out the laws in 1836 and written them down in notes for lectures given at Königsberg in late 1836 and early 1837. In 1846, Jacobi even went so far as to write in a footnote of a paper, which was a republished version of an 1837 paper, that Eisenstein had gotten the proof from Jacobi's notes. Eisenstein responded in a paper published in *Crelle's Journal* in 1847 that he had neither seen Jacobi's lecture notes, nor was he aware of the proofs in them. See [12] for more historical details. Two proofs, essentially those of Eisenstein and Jacobi, can be found in [32].

where π_j are prime elements of $\mathfrak{O}_F$ with $N_F(\pi_j) \neq 3$ for $j = 1, 2, \ldots, m$, then $(\frac{\alpha}{\beta})_3$ is defined by

$$\left(\frac{\alpha}{\beta}\right)_3 = \prod_{j=1}^{m} \left(\frac{\alpha}{\pi_j}\right)_3 .$$

If $\beta \in \mathfrak{U}_{\mathfrak{O}_F}$, then set

$$\left(\frac{\alpha}{\beta}\right)_3 = 1,$$

for all nonzero $\alpha \in \mathfrak{O}_F$, and

$$\left(\frac{0}{\beta}\right)_3 = 0.$$

For the following, the reader is reminded of the introduction of Gauss sums and related characters in Exercises 5.27–5.34 on pages 231–232.

Remark 6.2 Suppose that $F = \mathbb{Q}(\zeta_3)$, $\alpha,\beta \in \mathfrak{O}_F$, π is a prime element of $\mathfrak{O}_F$, and $(\frac{\alpha}{\pi})_3$ is the cubic residue symbol. Then immediately from Definition 6.2,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 ,$$

and if $\alpha \equiv \beta \,(\text{mod } \pi)$, then

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 .$$

Therefore $(\frac{\alpha}{\pi})_3$ is a cubic character on the field $\mathbb{Z}[\zeta_3]/(\pi)$ of $N_F(\pi)$ elements, namely $\chi_\pi^{(3)}(\alpha) = (\frac{\alpha}{\pi})_3$ is a multiplicative character of order 3 on the finite field $\mathbb{F}_{N_F(\pi)}$.

By Exercise 6.2 on page 275, $(\frac{\alpha}{\pi})_3 = 1$ if and only if α is a cubic residue modulo π. By Exercise 6.5, every nonzero element of $\mathbb{Z}[\zeta_3]$ has six associates. Thus, to refine our development of the cubic reciprocity law, we need the following notion.

Definition 6.3 — Primary Cubic Integers

If $\pi \in \mathbb{Z}[\zeta_3]$, then we call π *primary* if $\pi \equiv \pm 1 \,(\text{mod } 3)$.[6.2] In particular, if π is a prime element, then it is called a *primary prime.*

Lemma 6.1 — Primary Property via Primary Factors

Let $F = \mathbb{Q}(\zeta_3)$ and let $\alpha \in \mathfrak{O}_F$ be a nonzero, nonunit element. Then α is primary if and only if there exists a decomposition in which all of its prime factors are primary.

Proof. Let $\alpha = \prod_{j=1}^{n} \pi_j$ where each π_j is a prime element of $\mathfrak{O}_F$ and $n \in \mathbb{N}$. If α is primary, then $3 \nmid N_F(\pi_j)$ for any $j = 1, \ldots, n$. By Exercise 6.6, we may write $\pi_j = u_j \rho_j$ where $u_j \in \mathfrak{U}_F$ and ρ_j is a primary prime in $\mathfrak{O}_F$. Thus, we may write

$$\prod_{j=1}^{n} u_j = \pm \zeta_3^m$$

[6.2] Some texts are more restrictive in their definition of *primary*, namely they define these elements to be those $\pi \equiv 2 \,(\text{mod } 3)$, instead of $\pi \equiv \pm 1 \,(\text{mod } 3)$ (see [32, Definition, p. 113] for instance). However, the theory is made simpler by the more general congruence.

for $m = 0, 1, 2$. Therefore, $\alpha = \pm\zeta_3^m \prod_{j=1}^n \rho_j$. Since $\alpha \equiv \pm 1 \pmod 3$ and for each j, $\rho_j \equiv \pm 1 \pmod 3$, then $\zeta_3^m \equiv \pm 1 \pmod 3$. However, $\zeta_3 \not\equiv -1 \pmod 3$ since $1 + \zeta_3$ is a unit by Exercise 4.20 on page 162. If $\zeta_3 \equiv 1 \pmod 3$, then $1 - \zeta_3 = 3\beta$ for some $\beta \in \mathfrak{O}_F$. Thus,

$$1 - \zeta_3 = 3\beta = (1 - \zeta_3)(1 - \zeta_3^2)\beta,$$

so $1 = (1 - \zeta_3^2)\beta$ forcing $(1 - \zeta_3^2)$ to be a unit contradicting the fact that $3 \bigm| (1 - \zeta_3^2)$. We have shown that $m \neq 1$. If $m = 2$, and $\zeta_3^2 \equiv 1 \pmod 3$, then by a similar argument to the above, we get that $1 - \zeta_3$ is a unit and this is a contradiction since 3 divides it. If $m = 2$ and $\zeta_3^2 \equiv -1 \pmod 3$, then this contradicts the fact that $1 + \zeta_3^2$ is a unit. Hence, $m \neq 2$. We have shown that $m = 0$. Therefore, $\alpha = \pm \prod_{j=1}^n \rho_j$, a product of primary primes. Conversely, if α is such a product, then the product is congruent to ± 1 modulo 3, so α is primary. □

We need one more concept and the results related to it before establishing the Cubic Reciprocity Law.

Definition 6.4 — Jacobi Sums

Let χ and λ be characters on $\mathbb{F}_q$ where $q = p^n$ for a prime p and $n \in \mathbb{N}$. Then

$$J_n(\chi, \lambda) = \sum_{x=0}^{q-1} \chi(x)\lambda(1 - x)$$

is called a *Jacobi sum*. If $n = 1$, we write $J_1 = J$ for convenience. The order m of the Jacobi sum $J_n(\chi, \lambda)$ is the least common multiple of the orders of χ and λ. Therefore, a Jacobi sum of order m is an integer in $\mathbb{Q}(\zeta_m)$.

Lemma 6.2 — Properties of Jacobi Sums

(a) Let χ and λ be characters on $\mathbb{F}_q$ where $q = p^n$ for a prime p and $n \in \mathbb{N}$. Then

$$J_n(\chi, \lambda) = \frac{G(\chi)G(\lambda)}{G(\chi\lambda)}.$$

(b) If $\chi = \chi^{(3)}$ is a cubic character on $\mathbb{F}_p$ where $p \equiv 1 \pmod 3$ is prime, and

$$J(\chi, \chi) = a + b\zeta_3,$$

then $3 \bigm| b$ and $a \equiv 2 \pmod 3$.

(c) For any prime p,

$$J(\epsilon, \chi) = 0,$$

where χ is any nontrivial character on $\mathbb{F}_p$, and

$$J(\epsilon, \epsilon) = p.$$

Proof. (a) We have that

$$G(\chi)G(\lambda) = \sum_{x \in \mathbb{F}_q} \chi(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} \sum_{y \in \mathbb{F}_q} \chi(y)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(y)}$$

$$= \sum_{x,y \in \mathbb{F}_q} \chi(x)\lambda(y)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x+y)} = \sum_{t \in \mathbb{F}_q} \Big(\sum_{x \in \mathbb{F}_q} \chi(x)\lambda(t - x) \Big) \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(t)}. \tag{6.3}$$

If $t = 0$, then

$$\sum_{x \in \mathbb{F}_q} \chi(x)\chi(t-x) = \sum_{x \in \mathbb{F}_q} \chi(x)\lambda(-x) = \lambda(-1) \sum_{x \in \mathbb{F}_q} \chi\lambda(x) = 0,$$

by Exercise 5.28 on page 232, since $\chi\lambda \neq \epsilon$. If $t \neq 0$, then by replacing x by tx_1 we get,

$$\sum_{x \in \mathbb{F}_q} \chi(x)\lambda(t-x) = \sum_{x_1 \in \mathbb{F}_q} \chi(tx_1)\lambda(t - tx_1)$$

$$= \sum_{x_1 \in \mathbb{F}_q} \chi\lambda(t)\chi(x_1)\lambda(1-x_1) = \chi\lambda(t) \sum_{x_1 \in \mathbb{F}_q} \chi(x_1)\lambda(1-x_1) = \chi\lambda(t) J_n(\chi,\lambda).$$

Hence, by substituting the above expression into (6.3), we get that,

$$G(\chi)G(\lambda) = \sum_{t \in \mathbb{F}_q} \chi\lambda(t) J_n(\chi,\lambda)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(t)} = J_n(\chi,\lambda)G(\chi\lambda),$$

which secures (a).

For part (b), we first need the following.

Claim 6.1 Suppose that χ is a character of order $n > 2$. Then

$$G(\chi)^n = \chi(-1)p \prod_{j=1}^{n-2} J(\chi,\chi^j).$$

In particular, for a cubic character $\chi = \chi^{(3)}$, we have

$$G(\chi)^3 = pJ(\chi,\chi).$$

By part (a), $G(\chi)^2 = J(\chi,\chi)G(\chi^2)$. Multiplying this by $G(\chi)$, we get

$$G(\chi)^3 = J(\chi,\chi)G(\chi^2)G(\chi) = J(\chi,\chi)J(\chi,\chi^2)G(\chi^3).$$

Continuing in this manner, we see that

$$G(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})G(\chi^{n-1}). \tag{6.4}$$

Since $\chi^{n-1} = \chi^{-1} = \overline{\chi}$ by Exercise 5.27 on page 231, then

$$G(\chi^{n-1})G(\chi) = G(\overline{\chi})G(\chi) = \chi(-1)p,$$

where the last equality follows from Exercise 5.54 on page 260. Therefore, $G(\chi^{n-1}) = \chi(-1)p/G(\chi)$, and substituting this into (6.4) yields Claim 6.1.

By Exercise 5.52,

$$G(\chi)^3 = \sum_{x=0}^{p-1} \chi^3(x)\zeta_3^{3x} = \sum_{x=1}^{p-1} \zeta_3^{3x} = -1,$$

where the last equality follows from Example 1.5 on page 2, and the penultimate equality comes from the facts that $\chi(0) = 0$ and $\chi^3(x) = 1$. Therefore, by Claim 6.1,

$$G(\chi)^3 = pJ(\chi,\chi) \equiv a + b\zeta_3 \equiv -1 \pmod 3. \tag{6.5}$$

By part (c) of Exercise 5.27 on page 231,

$$G(\overline{\chi})^3 = pJ(\overline{\chi}, \overline{\chi}) \equiv a + b\overline{\zeta_3} \equiv -1 \pmod 3. \tag{6.6}$$

Thus, subtracting (6.6) from (6.5) yields, $b(\zeta_3 - \overline{\zeta_3}) \equiv 0 \pmod 3$, namely

$$b\sqrt{-3} \equiv 0 \pmod 3,$$

which implies that $3b^2 \equiv 0 \pmod 9$, thereby forcing $3 \mid b$. Hence, from (6.5),

$$a + b\zeta_3 \equiv -1 \pmod 3,$$

so $a \equiv 2 \pmod 3$.

In particular, if χ is a cubic character, then

$$G(\chi) = \chi(-1)pJ(\chi,\chi) = pJ(\chi,\chi),$$

since $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = 1$. This secures part (b).

(c) The first assertion is immediate from Exercise 5.31 on page 232 and the second assertion is immediate from Definition 6.4. □

Lemma 6.3 — Cubic Jacobi Sums

Suppose that $F = \mathbb{Q}(\zeta_3)$, π is a primary prime element of $\mathfrak{O}_F$, and $N_F(\pi) = p \equiv 1 \pmod 3$. Then

$$J(\chi_\pi^{(3)}, \chi_\pi^{(3)}) = \begin{cases} -\pi & \text{if } \pi \equiv 1 \pmod 3, \\ \pi & \text{if } \pi \equiv -1 \pmod 3. \end{cases}$$

Proof. For the sake of simplicity of notation, we set $\chi_\pi^{(3)} = \chi$ for the balance of the proof. Let $J(\chi,\chi) = a + b\zeta_3$. By part (b) of Lemma 6.2 on page 264, $a \equiv 2 \pmod 3$ and $3 \mid b$. Also, by Exercise 5.54 on page 260 and Claim 6.1

$$N_F(J(\chi,\chi)) = N_F(G(\chi)^3/p) = N_F(\pi) = p.$$

Therefore, $J(\chi,\chi)\overline{J(\chi,\chi)} = p = \pi\overline{\pi}$, so $\pi \mid J(\chi,\chi)$ or $\pi \mid \overline{J(\chi,\chi)}$. We now show that the former holds. We have,

$$\begin{aligned} J(\chi,\chi) &= \sum_{x=0}^{p-1} \chi(x)\chi(1-x) \equiv \sum_{x=0}^{p-1} x^{(p-1)/3}(1-x)^{(p-1)/3} \\ &\equiv \sum_{x=0}^{p-1} x^{(p-1)/3} \sum_{j=0}^{(p-1)/3} \binom{(p-1)/3}{j} (-x)^j \\ &\equiv \sum_{j=0}^{(p-1)/3} \binom{(p-1)/3}{j} (-1)^j \sum_{x=0}^{p-1} x^{(p-1)/3+j} \pmod \pi, \end{aligned}$$

where the middle congruence comes from the Binomial Theorem. Also, we have that

$$(p-1)/3 + j < p - 1$$

for $j = 0, 1, \ldots, (p-1)/3$, so by Exercise 6.13 on page 277, $\sum_{x=0}^{p-1} x^{(p-1)/3+j} = 0$ in $\mathbb{F}_p$. Hence, $J(\chi,\chi) \equiv 0 \pmod \pi$. Since $\pi \mid J(\chi,\chi)$, which is itself a primary prime element of $\mathfrak{O}_F$ given that $J(\chi,\chi) \equiv a \equiv -1 \pmod 3$, then $J(\chi,\chi) = \pm\pi$, and the result follows. □

Theorem 6.1 — Cubic Reciprocity Law

Let α,β be relatively prime primary elements of $\mathfrak{O}_F$ where $F = \mathbb{Q}(\zeta_3)$. Then

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3 .$$

Proof. If $\alpha \in \mathfrak{U}_{\mathfrak{O}_F}$, then $\alpha = \pm 1$ since α is primary and $\pm\zeta_3^j \not\equiv \pm 1 \pmod 3$ for $j = 1, 2$. Thus, by definition,

$$\left(\frac{\alpha}{\beta}\right)_3 = 1 = \left(\frac{\beta}{\alpha}\right)_3 .$$

If α is not a unit, then by Remark 6.2 and Lemma 6.1 on page 263 it suffices to prove the result for the case where α,β are primary primes.

Case 6.1 α,β are rational primes, which are inert in F.

Since α and β are relatively prime, then by the last statement of Exercise 6.4 on page 275,

$$\left(\frac{\alpha}{\beta}\right)_3 = 1 = \left(\frac{\beta}{\alpha}\right)_3 .$$

This completes Case 6.1.

For a given prime element π of $\mathfrak{O}_F$, set $\chi_\pi(\gamma) = \chi_\pi^{(3)}(\gamma) = (\frac{\gamma}{\pi})_3$ in what follows.

Case 6.2 $\alpha = q \equiv 2 \pmod 3$ is inert and $\beta = \pi$ with $N_F(\pi) = p \equiv 1 \pmod 3$.

By Lemma 6.3 and Claim 6.1 on page 265,

$$G(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi) = \pm p\pi.$$

Therefore, $G(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3} \equiv \chi_q(p\pi) \equiv \chi_q(\pi) \pmod q$, where the last congruence follows from Remark 6.2 on page 263 since $p \equiv 1 \pmod 3$. Thus,

$$G(\chi_\pi)^{q^2} \equiv \chi_q(\pi) G(\chi_\pi) \pmod q. \tag{6.7}$$

However, by the Multinomial Theorem—see Theorem A.25 on page 341—

$$G(\chi_\pi)^{q^2} \equiv \sum_{x=0}^{p-1} \chi_\pi^{q^2}(x)\zeta_p^{q^2 x} \pmod q.$$

Also, since $q^2 \equiv 1 \pmod 3$ and $\chi_\pi(x)$ is a cube root of unity, then

$$\sum_{x=0}^{p-1} \chi_\pi^{q^2}(x)\zeta_p^{q^2 x} = \sum_{x=0}^{p-1} \chi_\pi(x)\zeta_p^{q^2 x} = G_{q^2}(\chi_\pi), \tag{6.8}$$

and by Exercise 5.52 on page 260,

$$G_{q^2}(\chi_\pi) = \overline{\chi}_\pi(q^2) G(\chi_\pi). \tag{6.9}$$

Combining (6.7)–(6.9), we get

$$\overline{\chi}_\pi(q^2) G(\chi_\pi) \equiv \chi_q(\pi) G(\chi_\pi) \pmod q.$$

However, by part (c) of Exercise 5.27 on page 231,

$$\overline{\chi}_\pi(q^2) = \overline{\left(\frac{q^2}{\pi}\right)_3} = \overline{\left(\frac{q}{\pi}\right)_3^2} = \overline{\left(\frac{q}{\pi}\right)_3^{-1}} = \overline{\overline{\left(\frac{q}{\pi}\right)_3}} = \left(\frac{q}{\pi}\right)_3 = \chi_\pi(q),$$

so

$$\chi_\pi(q)G(\chi_\pi) \equiv \chi_q(\pi)G(\chi_\pi) \pmod{q}.$$

Since $G(\chi_\pi)G(\overline{\chi}_\pi) = p$ from Exercise 5.54 on page 260, then multiplying the latter congruence by $G(\overline{\chi}_\pi)$, we get

$$\chi_\pi(q)p \equiv \chi_q(\pi)p \pmod{q},$$

so we may divide out the p and use the uniqueness given in Definition 6.2 to conclude that

$$\chi_\pi(q) = \chi_q(\pi),$$

which completes Case 6.2.

Case 6.3 Assume that $\alpha = \pi_1$ with $N_F(\pi_1) = p \equiv 1 \pmod 3$ and $\beta = \pi_2$ with $N_F(\pi_2) = q \equiv 1 \pmod 3$, and $p \neq q$.

Since $\overline{\pi}_1$ is primary, then as in Case 6.2

$$G(\chi_{\overline{\pi}_1})^{q-1} = (\pm p\overline{\pi}_1)^{(q-1)/3} \equiv \chi_{\pi_2}(p\overline{\pi}_1) \pmod{\pi_2}.$$

In other words,

$$G(\chi_{\overline{\pi}_1})^q \equiv \chi_{\pi_2}(p\overline{\pi}_1)G(\chi_{\overline{\pi}_1}) \pmod{\pi_2}. \tag{6.10}$$

However, as above, by the Multinomial Theorem and Exercise 5.52,

$$G(\chi_{\overline{\pi}_1})^q \equiv \sum_{x=0}^{p-1} \chi_{\overline{\pi}_1}^q(x)\zeta_p^{xq} = G_q(\chi_{\overline{\pi}_1}) = \overline{\chi}_{\overline{\pi}_1}(q)G(\chi_{\overline{\pi}_1}) \pmod{q}, \tag{6.11}$$

where $\overline{\chi}_{\overline{\pi}_1}(q) \neq 0$ since $p \neq q$. Comparing (6.10) and (6.11), and using part (c) of Exercise 5.27 we get,

$$\chi_{\pi_2}(p\overline{\pi}_1) = \overline{\chi}_{\overline{\pi}_1}(q) = \chi_{\overline{\pi}_1}(q)^{-1} = \chi_{\overline{\pi}_1}(q)^2 = \chi_{\overline{\pi}_1}(q^2).$$

We have shown that

$$\chi_{\pi_2}(p\overline{\pi}_1) = \chi_{\overline{\pi}_1}(q^2). \tag{6.12}$$

Now we repeat the above argument that led to (6.12), with the role of π_2 replacing that of $\overline{\pi}_1$, and π_1 replacing that of π_2. Then instead of (6.12), we get

$$\chi_{\pi_1}(q\pi_2) = \chi_{\pi_2}(p^2). \tag{6.13}$$

Also, by Exercise 6.4 on page 275, and part (c) of Exercise 5.27,

$$\chi_{\overline{\pi}_1}(q^2) = \overline{\chi}_{\pi_1}(q^2) = \chi_{\pi_1}(q). \tag{6.14}$$

Multiplying (6.12) by $\chi_{\pi_1}(\pi_2)$ we get,

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p\overline{\pi}_1) = \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi}_1}(q^2). \tag{6.15}$$

Also, by multiplying (6.14) by $\chi_{\pi_1}(\pi_2)$, the latter equals,

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_1}(q) = \chi_{\pi_1}(q\pi_2), \tag{6.16}$$

and by (6.13) ,

$$\chi_{\pi_2}(p^2) = \chi_{\pi_2}(p\pi_1\overline{\pi}_1) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p\overline{\pi}_1). \tag{6.17}$$

Hence, from (6.13)–(6.17),

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p\overline{\pi}_1) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p\overline{\pi}_1).$$

Dividing out by $\chi_{\pi_2}(p\overline{\pi}_1)$ yields,

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1),$$

which establishes Case 6.3.

We have proved the Cubic Reciprocity Law for all except the following (often overlooked) case.

Case 6.4 [6.3] *Assume that $\alpha = \pi \notin \mathbb{Z}$ is a primary prime and $\beta = \overline{\pi}$.*

By Remark 6.2 on page 263 and the cases already proved,

$$\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{\pi+\overline{\pi}}{\overline{\pi}}\right)_3 = \left(\frac{\overline{\pi}}{\pi+\overline{\pi}}\right)_3 = \left(\frac{-\overline{\pi}}{\pi+\overline{\pi}}\right)_3,$$

since -1 is a cubic residue, and since $-\overline{\pi} \equiv \pi \pmod{\pi+\overline{\pi}}$, then this in turn equals,

$$\left(\frac{\pi}{\pi+\overline{\pi}}\right)_3 = \left(\frac{\pi+\overline{\pi}}{\pi}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3,$$

and the proof is complete. □

Corollary 6.1 Let $p \equiv 1 \pmod 3$ be a prime with $p = \pi\overline{\pi}$ where $\pi = a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$. If $A, B \in \mathbb{Z}$ are such that

$$4p = A^2 + 27B^2,$$

then A is a cubic residue modulo p.

Proof. Since

$$\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3^{-1},$$

by Exercise 6.4, then necessarily

$$\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3 = 1, \tag{6.18}$$

by the cubic reciprocity law. Also, we have,

$$\pi + \overline{\pi} = a + b\zeta_3 + a + b\zeta_3^2 = 2a - b,$$

where the last equality comes from Example 1.5 on page 2.

Claim 6.2 For any prime $p \equiv 1 \pmod 3$, there are unique $A, B \in \mathbb{N}$ such that

$$4p = A^2 + 27B^2,$$

with $A \equiv \pm 1 \pmod 3$. *Here we say "unique" in the sense that, although $-A$ and $-B$ will also satisfy the equation, they are not natural numbers. Usually, one says that the A and B are unique "up to sign." Our choice of only the positive sign by selecting only* natural *numbers ensures uniqueness of sign.*

[6.3] The elegant proof of this case is due to Ron Evans, who suggested it in the writing of the first edition, as is the suggestion of Corollary 6.1, an application of cubic reciprocity based upon this case.

By the proof of part (b) of Lemma 6.2 on page 264,

$$J(\chi,\chi) = a + b\zeta_3$$

with

$$|J(\chi,\chi)|^2 = p$$

and

$$p = a^2 - ab + b^2.$$

Set $A = 2a - b \in \mathbb{N}$ and $B = |b|/3$. Then

$$4p = (2a-b)^2 + 3b^2 = A^2 + 27B^2.$$

Since $3 \bigm| b$ and $a \equiv 2 \pmod 3$ by part (b) of Lemma 6.2, then it follows that

$$A = |2a - b| \equiv \pm 1 \pmod 3.$$

Uniqueness of representation is shown by choosing A to be the smallest such value, from which it follows that there can be no other representation of this type. This is Claim 6.2.

By Claim 6.2,

$$4p = 4(a + b\zeta_3)(a - b\zeta_3^2) = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2 = A^2 + 27B^2.$$

Therefore, from (6.18) and the fact that $\pi + \overline{\pi} = A$, we get:

$$\left(\frac{A}{\pi}\right)_3 = 1 = \left(\frac{A}{\overline{\pi}}\right)_3.$$

That A is a cubic residue modulo p will follow from the next result.

Claim 6.3 For a given $\delta \in \mathbb{Z}[\zeta_3]$, $\delta \equiv \gamma^3 \pmod p$ for some $\gamma \in \mathbb{Z}[\zeta_3]$ if and only if $\delta \equiv \alpha^3 \pmod \pi$ and $\delta \equiv \beta^3 \pmod{\overline{\pi}}$ for some $\alpha,\beta \in \mathbb{Z}[\zeta_3]$. Furthermore, $\delta \equiv \gamma^3 \pmod p$ for some $\gamma \in \mathbb{Z}[\zeta_3]$ if and only if $\delta \equiv a^3 \pmod p$ for some $a \in \mathbb{Z}$.

By Theorem 1.21 on page 32, for any $\alpha,\beta \in \mathbb{Z}[\zeta_3]$, there exists a $\gamma \in \mathbb{Z}[\zeta_3]$ such that

$$\gamma \equiv \alpha \pmod \pi \text{ and } \gamma \equiv \beta \pmod{\overline{\pi}},$$

from which the first result clearly follows. For the other assertion, we note that

$$\mathfrak{O}_F/\pi = \mathbb{Z}[\zeta_3]/\pi \cong \mathbb{Z}/p\mathbb{Z},$$

since $N_F(\pi) = p$—see Definition 5.1 on page 182. Therefore, given $\gamma \in \mathfrak{O}_F$, there exists a rational integer a such that $\gamma \equiv a \pmod \pi$. Thus, if $\delta \equiv \gamma^3 \pmod p$, then we have that $\delta \equiv a^3 \pmod p$. The converse is trivial, with $a = \gamma$. □

Example 6.1 Let $p = 19$. Then $4 \cdot 19 = 7^2 + 27$. Thus, by Corollary 6.1, there exists an $x \in \mathbb{Z}$ such that $7 \equiv x^3 \pmod{19}$. In fact, $7 \equiv 4^3 \pmod{19}$.

Corollary 6.1 is an application of Case 6.4 in the proof of Theorem 6.1. We may exploit that case further to motivate another application of the Cubic Reciprocity Law.

Example 6.2 Let $\alpha = 2 + 3\sqrt{-3} = \pi$ and $\beta = 2 - 3\sqrt{-3} = \overline{\pi}$, both clearly primary elements of $\mathbb{Z}[\zeta_3] = \mathbb{Z}[(1+\sqrt{-3})/2] = \mathfrak{O}_F$, and $N_F(\pi) = N_F(\overline{\pi}) = 31 = p$. Also, to explicitly illustrate Case 6.4, we have,

$$\pi^{(N_F(\pi)-1)/3} = (2+3\sqrt{-3})^{10} \equiv 1 \equiv \zeta_3^0 \pmod{\overline{\pi}},$$

since

$$(2+3\sqrt{-3})^{10} = 24663337 - 8393412\sqrt{-3} = 1 + (2-3\sqrt{-3})(4027980 + 1845264\sqrt{-3}),$$

so $(2-3\sqrt{-3})^{10} \equiv 1 \equiv \zeta_3^0 \,(\text{mod } \pi)$ as well, since

$$(2-3\sqrt{-3})^{10} = 1 + (2+3\sqrt{-3})(4027980 - 1845264\sqrt{-3}).$$

Thus,

$$\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{2+3\sqrt{-3}}{2-3\sqrt{-3}}\right)_3 = 1 = \left(\frac{2-3\sqrt{-3}}{2+3\sqrt{-3}}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3.$$

Notice that

$$p = 31 = 2^2 + 27,$$

a case not covered by Corollary 6.1, in the sense that we cannot use it to determine if 2 is a cubic residue modulo p. The following result does tell us how to determine when 2 is a cubic residue modulo p in the general case.

By Exercise 6.2, we know that $\alpha \in \mathfrak{O}_F = Z[\zeta_3]$ is a cubic residue modulo a prime element $\pi \in \mathfrak{O}_F$ if and only if $(\frac{\alpha}{\pi})_3 = 1$. In particular, the cubic residuacity of 2 is of special importance from both a historical perspective and from the point of view of representation of rational primes as norms of cubic integers. In order to establish such results we need the following, which was proved by Gauss in 1801—see Biography 3.5 on page 95.

Theorem 6.2 — The Cubic Residuacity of 2

Let $p \equiv 1 \,(\text{mod } 3)$ be a prime and let $4p = a^2 + 3b^2$, where $a \equiv 1 \,(\text{mod } 3)$ and $b \equiv 0 \,(\text{mod } 3)$ are the unique natural numbers determined in Exercise 6.10 on page 276. Then

$$2 \equiv x^3 \pmod{p} \text{ for some } x \in \mathbb{Z} \text{ if and only if } 2 \mid a.$$

Proof. Since $p \equiv 1 \,(\text{mod } 3)$, then it follows from Remark 1.24 on page 52 that $p = \pi\pi'$ where π is a prime element of $\mathfrak{O}_F = \mathbb{Z}[\zeta_3]$ and π' is the algebraic conjugate of π. We may let $\pi = (a + b\sqrt{-3})/2$ since

$$N_F(\pi) = \pi\pi' = p = \frac{a^2 + 3b^2}{4}.$$

If $2 \equiv x^3 \,(\text{mod } p)$, then $2 \equiv x^3 \,(\text{mod } \pi)$, so

$$\frac{a + b\sqrt{-3}}{2} = \pi \equiv 1 \pmod{2},$$

by Exercise 6.3. This in turn holds if and only if

$$\frac{a+b}{2} \equiv 1 \pmod{2} \text{ and } b \equiv 0 \pmod{6}.$$

Together, these imply that $2 \mid a$.

Conversely, if $2 \mid a$, then necessarily $2 \mid b$, so we may write $a = 2a_1$ and $b = 2b_1$. Therefore,

$$\pi = \frac{a + b\sqrt{-3}}{2} = 1 + 2\left(\frac{a_1 - 1 + b_1\sqrt{-3}}{2}\right) \equiv 1 \pmod 2,$$

so by Exercise 6.3 and Claim 6.3 on page 270, $2 \equiv x^3 \,(\mathrm{mod}\ p)$ has a solution $x \in \mathbb{Z}$. □

Remark 6.3 The reader is cautioned that $(\frac{2}{p})_3 = 1$ does not necessarily imply that $2 \equiv x^3$ (mod p) has a solution $x \in \mathbb{Z}$. Exercise 6.4 tells us that in fact $(\frac{2}{p})_3 = 1$ for *any* prime $p > 3$. Consider the following example, which motivates the next result conjectured by Euler.

Example 6.3 Let $p = 7$, so $p = \pi\overline{\pi}$, in $\mathfrak{O}_F = \mathbb{Z}[\zeta_3]$, where $\pi = (5 + \sqrt{-3})/2$. Thus, one calculates that

$$\left(\frac{2}{\pi}\right)_3 \equiv 2^{(N_F(\pi)-1)/3} = 4 \equiv \zeta_3 \pmod{\pi},$$

since

$$4 = \frac{-1 + \sqrt{-3}}{2} - \left(\frac{5 + \sqrt{-3}}{2}\right)\left(\frac{-3 + \sqrt{-3}}{2}\right) = \zeta_3 - \pi\gamma,$$

where $\gamma = (-3 + \sqrt{-3})/2$. Similarly,

$$\left(\frac{2}{\overline{\pi}}\right)_3 \equiv \zeta_3^2 \pmod{\overline{\pi}}.$$

Therefore,

$$\left(\frac{2}{p}\right)_3 = \left(\frac{2}{\pi}\right)_3\left(\frac{2}{\overline{\pi}}\right)_3 = \zeta_3\zeta_3^2 = 1.$$

Yet, $2 \not\equiv x^3 \,(\mathrm{mod}\ p)$ for any $x \in \mathbb{Z}$, by Theorem 6.2, since $2 \nmid a = 1$ where $4 \cdot 7 = 1^2 + 3 \cdot 3^2$.

Theorem 6.3 – Prime Representation and Cubic Residuacity[6.4]

If p is a rational prime, then there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 27y^2$ if and only if $p \equiv 1$ (mod 3) and $2 \equiv z^3 \,(\mathrm{mod}\ p)$ for some $z \in \mathbb{Z}$.

Proof. If $p \equiv 1 \,(\mathrm{mod}\ 3)$ and $2 \equiv z^3 \,(\mathrm{mod}\ p)$ for some $z \in \mathbb{Z}$, then by Theorem 6.2 we have that $2 \mid a$, so $p = x^2 + 27y^2$, where $x = a/2$ and $y = b/6$. Conversely, if $p = x^2 + 27y^2$, then certainly $p \equiv 1 \,(\mathrm{mod}\ 3)$. Since $4p = (2x)^2 + 3(6y)^2$, then by Theorem 6.2, we have the result. □

In the next section, we will see Gauss's proof of another of Euler's conjectures, this time using *biquadratic reciprocity.*

Example 6.4 Returning to a consideration of Example 6.3, we see that 7 certainly cannot be represented in the form $x^2 + 27y^2$. What is hidden here is that in the non-maximal order $\mathbb{Z}[\sqrt{-27}]$—see Remark 3.5 on page 99—the ideal $\mathcal{P} = [7, 1 + \sqrt{-27}]$ is not principal. In fact, if $p \equiv 1 \,(\mathrm{mod}\ 3)$ is prime, then by Exercise 6.1, there is a rational integer b such that

[6.4] Euler conjectured this in *Tractatus de numerorum doctrina capita sedecim quae supersunt*, which he wrote during the years 1748–1750. However, the work was not completed and did not get published until 1849 (see [18]). Gauss was the first to prove the result as a consequence of his work on cubic residuacity including the result in Theorem 6.2.

$-27 \equiv b^2 \pmod{p}$. Thus, by Exercise 6.14, there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 27y^2$ if and only if the ideal $\mathcal{P} = [p, b + \sqrt{-27}]$ is principal in $\mathbb{Z}[\sqrt{-27}]$.[6.5] Therefore, $\mathcal{P} = [7, 1 + \sqrt{-27}]$ is not principal in $\mathbb{Z}[\sqrt{-27}]$. What Example 6.3 shows is that $p = 7$ is a product of prime elements $\pi\overline{\pi}$ in $\mathbb{Z}[\zeta_3]$ where $\pi, \overline{\pi} \notin \mathbb{Z}[\sqrt{-27}]$. Thus, Euler's criterion given in Theorem 6.3 says that primes $p \equiv 1 \pmod{3}$ are representable in the form $p = x^2 + 27y^2$ if and only if $\pi \in \mathbb{Z}[\sqrt{-27}]$. Thus, we have a surprisingly simple interpretation in terms of ideal theory.

Excluded from the Quadratic Reciprocity Law is the fact (given in (A.10) on page 342), that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

which is therefore called the *Supplement to the Quadratic Reciprocity Law.* We close this section with the cubic analogue of this fact.

Theorem 6.4 — Supplement to the Cubic Reciprocity Law
Let $\pi = -1 + 3m + 3n\zeta_3 \in \mathfrak{O}_F = \mathbb{Z}[\zeta_3]$ be a primary prime element.[6.6] Then

$$\left(\frac{1-\zeta_3}{\pi}\right)_3 = \zeta_3^{2m}.$$

Proof. Suppose first that $\pi = q \equiv -1 \pmod{3}$, so $q = -1 + 3m$. Since

$$(1-\zeta_3)^2 = -3\zeta_3, \tag{6.19}$$

then we need only show that $(\frac{-3\zeta_3}{\pi})_3 = \zeta_3^m$. By the last statement in Exercise 6.4,

$$\left(\frac{-3\zeta_3}{\pi}\right)_3 = \left(\frac{-3}{q}\right)_3 \left(\frac{\zeta_3}{q}\right)_3 = \left(\frac{\zeta_3}{q}\right)_3 = \zeta_3^{(N_F(q)-1)/3} = \zeta_3^{(q^2-1)/3} = \zeta_3^{3m^2-2m} = \zeta_3^m.$$

Now we let $a = 3m - 1$ and $b = 3n$ where $n \neq 0$, and $\gcd(a, b) = 1$, so $\pi = a + b\zeta_3$ with $p = \pi\overline{\pi}$. [6.7]

Claim 6.4

$$\left(\frac{\zeta_3}{\pi}\right)_3 = \zeta_3^{m+n}.$$

This follows from the fact that

$$\left(\frac{\zeta_3}{\pi}\right)_3 = \zeta_3^{(p-1)/3},$$

and $(p-1)/3 \equiv n - 2m \equiv m + n \pmod{3}$, since $p = N_F(\pi) = a^2 - 2ab + b^2$.

Claim 6.5

$$\left(\frac{a}{\pi}\right)_3 = \zeta_3^m.$$

[6.5] This phenomenon is studied in detail in [49]. Therein, such so-called *non-maximal orders* as $\mathbb{Z}[\sqrt{-27}]$ and their relationship with the maximal order or ring of integers such as $\mathbb{Z}[\zeta_3] = \mathbb{Z}[(1+\sqrt{-3})/2]$ is explored in depth. See also, [50, pp. 349–352] for an overview of the above from an elementary standpoint.

[6.6] There is no loss of generality in assuming that $\pi \equiv -1 \pmod{3}$ since one of $\pm\pi$ must satisfy the congruence. Also, by Example 1.5 on page 2, there is no need for a term involving ζ_3^2 in the given expression for π.

[6.7] The ideas used in the balance of the proof are due to K. S. Williams [72].

By the Cubic Reciprocity Law and the last statement in Exercise 6.4,

$$\left(\frac{a}{\pi}\right)_3 = \left(\frac{\pi}{a}\right)_3 = \left(\frac{a+b\zeta_3}{a}\right)_3 = \left(\frac{b\zeta_3}{a}\right)_3 = \left(\frac{b}{a}\right)_3\left(\frac{\zeta_3}{a}\right)_3 = \zeta_3^{(a^2-1)/3}.$$

However, since $(a^2-1)/3 \equiv m \pmod 3$, then we have Claim 6.5.

Claim 6.6

$$\left(\frac{a+b}{\pi}\right)_3 = \zeta_3^{2n}\left(\frac{1-\zeta_3}{\pi}\right)_3.$$

Since $(a+b)\zeta_3 \equiv -a(1-\zeta_3) \pmod{\pi}$, then

$$\left(\frac{a+b}{\pi}\right)_3 = \left(\frac{(a+b)\zeta_3\zeta_3^2}{\pi}\right)_3 = \left(\frac{-a(1-\zeta_3)\zeta_3^2}{\pi}\right)_3 = \left(\frac{a}{\pi}\right)_3\left(\frac{\zeta_3}{\pi}\right)_3^2\left(\frac{1-\zeta_3}{\pi}\right)_3,$$

so by Claims 6.4–6.5, this equals

$$\zeta_3^m\zeta_3^{2m+2n}\left(\frac{1-\zeta_3}{\pi}\right)_3 = \zeta_3^{2n}\left(\frac{1-\zeta_3}{\pi}\right)_3,$$

which establishes Claim 6.6.

Claim 6.7

$$\left(\frac{\pi}{a+b}\right)_3 = \zeta_3^{2(m+n)}.$$

Since $\pi \equiv -b(1-\zeta_3) \pmod{a+b}$, then

$$\left(\frac{\pi}{a+b}\right)_3 = \left(\frac{-b(1-\zeta_3)}{a+b}\right)_3 = \left(\frac{-b}{a+b}\right)_3\left(\frac{1-\zeta_3}{a+b}\right)_3 = \left(\frac{1-\zeta_3}{a+b}\right)_3,$$

where the last equality comes from the last statement in Exercise 6.4. However, by (6.19),

$$\left(\frac{1-\zeta_3}{a+b}\right)_3 = \left(\frac{(1-\zeta_3)^2}{a+b}\right)_3^2 = \left(\frac{-3\zeta_3}{a+b}\right)_3^2 = \left(\frac{-3}{a+b}\right)_3^2\left(\frac{\zeta_3}{a+b}\right)_3^2,$$

and by the last statement in Exercise 6.4 again, this equals

$$\left(\frac{\zeta_3}{a+b}\right)_3^2 = \zeta_3^{\frac{2}{3}((a+b)^2-1)} = \zeta_3^{m+n},$$

which completes the proof of Claim 6.7.

By Claims 6.6–6.7, and the Cubic Reciprocity Law,

$$\left(\frac{1-\zeta_3}{\pi}\right)_3 = \zeta_3^{-2n}\left(\frac{a+b}{\pi}\right)_3 = \zeta_3^{-2n}\left(\frac{\pi}{a+b}\right)_3 = \zeta_3^{-2n}\zeta_3^{2(m+n)} = \zeta_3^{2m},$$

which establishes the result. □

Exercises

6.1. Let $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$, $\alpha \in \mathfrak{O}_F$, π a prime element of $\mathfrak{O}_F$ with $N_F(\pi) = q$, and $g = \gcd(n, q-1)$. Prove that

$$x^n \equiv \alpha \pmod{\pi}$$

has a solution $x \in \mathfrak{O}_F$ if and only if

$$\alpha^{(q-1)/g} \equiv 1 \pmod{\pi}.$$

(*Hint: Use Theorem A.8 on page 331 and Theorem A.24 on page 340.*)

6.2. Suppose that $F = \mathbb{Q}(\zeta_3)$, $\alpha,\beta \in \mathfrak{O}_F$, π is a prime element of $\mathfrak{O}_F$, $(\frac{\alpha}{\pi})$ is the cubic residue symbol given in Definition 6.2 on page 262, and $N_F(\pi) \neq 3$. Prove that

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \text{ if and only if } \beta^3 \equiv \alpha \pmod{\pi},$$

for some $\beta \in \mathfrak{O}_F$.

(*Hint: Use Exercsie 6.1.*)

6.3. Let $F = \mathbb{Q}(\zeta_3)$ and π is a primary prime in $\mathfrak{O}_F$, with $\pi \notin \mathbb{Z}$. Prove that

$$\beta^3 \equiv 2 \pmod{\pi}$$

has a solution $\beta \in \mathfrak{O}_F$ if and only if

$$\pi \equiv 1 \pmod{2}.$$

(*Hint: Use Proposition 6.1 on page 262, Exercise 6.2, and the Cubic Reciprocity Law.*)

6.4. Suppose that $\alpha,\beta \in \mathbb{Z}[\zeta_3] = \mathfrak{O}_F$ where α is a prime element with $N_F(\alpha) \neq 3$ and $\alpha \nmid \beta$. Prove that

$$\overline{\chi^{(3)}}_{\alpha}(\beta) = \chi^{(3)}_{\overline{\alpha}}(\overline{\beta}).$$

Use this to deduce that for $r, s \in \mathbb{Z}$ with $\gcd(r, s) = 1$ and $3 \nmid s$,

$$\left(\frac{r}{s}\right)_3 = 1.$$

(*Hint: Use Exercise 6.2.*)

6.5. Prove that every nonzero element of $\mathbb{Z}[\zeta_3]$ has six associates.

6.6. Let $F = \mathbb{Q}(\zeta_3)$, and let $\alpha \in \mathfrak{O}_F$ be a nonzero element such that $3 \nmid N_F(\alpha)$. Prove that exactly two of the associates of α are primary, and that if β is a primary associate of α, then $-\beta$ is the other one.

6.7. Prove that

$$J(\chi,\chi^{-1}) = -\chi(-1),$$

for any nontrivial character χ on $\mathbb{F}_p$ where p is prime.

(*Hint: Use Exercise 5.28 on page 232.*)

Exercises 6.8–6.12 are designed as applications of Jacobi sums to certain Diophantine equations, especially over finite fields, not covered in the main text. For more information, see [3].

6.8. Let χ and λ be characters on $\mathbb{F}_p$ where p is prime and $\chi,\lambda\,,\chi\lambda \neq \epsilon$. Prove that

$$|J(\chi,\lambda)| = \sqrt{p}.$$

Use this fact to prove the following.

(a) If $p \equiv 1 \pmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

(b) If $p \equiv 1 \pmod 3$, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.

(*Hint: Use Exercises 5.30 on page 232, 5.54 on page 260, and part* (a) *of Lemma 6.2 on page 264*).

6.9. Suppose that

$$f(x_1, \ldots, x_n) = \alpha_0 + \sum_{j=1}^{n} \alpha_j x_j^{k_j},$$

where $\alpha_j \in \mathbb{F}_q$, $n, k_j \in \mathbb{N}$, and let $N_{f,q}$ be the number of solutions of

$$f(x_1, \ldots, x_n) = 0$$

in F_q, where $q = p^m$, $m \in \mathbb{N}$ for some rational prime p.[6.8] Prove that if

$$f(x) = x^n - \alpha$$

for $\alpha \in \mathbb{F}_p^\times$, $n \in \mathbb{N}$ and a prime $p \equiv 1 \pmod n$, then

$$N_{f,p} = \sum_{j=1}^{n} \chi^j(\alpha),$$

where χ is a character of order n on $\mathbb{F}_p$. In particular, use this fact to prove the following, where $(\frac{x}{p})$ is the Legendre symbol. If

$$f(x) = x^2 - a$$

and $p > 2$, then

$$N_{f,p} = 1 + \left(\frac{a}{p}\right).$$

(*Hint: Use Exercises 5.30 and 5.32 on page 232.*)

✰ 6.10. With reference to Exercise 6.9, suppose that $p \equiv 1 \pmod 3$ is prime and

$$f(x, y) = x^3 + y^3 - 1.$$

Prove the following result due to Gauss. There are $A, B \in \mathbb{Z}$ with $A \equiv 1 \pmod 3$ uniquely determined such that

$$4p = A^2 + 27B^2, \text{ and } N_{f,p} = p - 2 + A.$$

(*Hint: Use Exercise 6.7, parts* (b)–(c) *of Lemma 6.2, and the proof of Claim 6.2 on page 269.*)

[6.8] Equations of this form are called *diagonal equations.* For an in-depth analysis of such equations, see [3] and [43].

6.11. With the notation of Exercise 6.9 in place, prove that if

$$f(x,y) = x^2 + y^2 - 1$$

and $p > 2$, then

$$N_{f,p} = \begin{cases} p-1 & \text{if } p \equiv 1 \pmod 4, \\ p+1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

(*Hint: Use Exercises 6.7, 6.9, and see the solution to Exercise 5.33 on page 398.*)

6.12. Let $p \equiv 1 \pmod 3$ be prime and set

$$f(x,y) = x^3 + y^3 - 1.$$

Prove that, in the notation of Exercise 6.9,

$$|N_{f,p} - p + 2| \le 2\sqrt{p}.$$

6.13. Let $k \in \mathbb{N}$ and $p > 2$ prime. Prove that

$$\sum_{x \in \mathbb{F}_p} x^k = \begin{cases} 0 & \text{if } (p-1) \nmid k, \\ -1 & \text{if } (p-1) \mid k. \end{cases}$$

6.14. Let $p \equiv 1 \pmod 3$ be a rational prime, and (as shown in Example 6.4), let $b \in \mathbb{Z}$ such that $b^2 \equiv -27 \pmod p$. Prove that there exists $x, y \in \mathbb{Z}$ such that

$$p = x^2 + 27y^2$$

if and only if the ideal

$$\mathcal{P} = [p, b + \sqrt{-27}]$$

is principal in $\mathbb{Z}[\sqrt{-27}]$.

6.15. With reference to Exercise 6.14, prove that $\mathcal{P}^3 \sim 1$ in $\mathbb{Z}[\sqrt{-27}]$. *In fact, it can be shown that the class number of* $\mathbb{Z}[\sqrt{-27}]$ *is* 3 *see* [49, Footnote (1.5.9), pp. 25–26].

Biography 6.1 Carl Gustav Jacob Jacobi (1804–1851) was born in Potsdam in Prussia on December 10, 1804, to a wealthy German banking family. In August of 1825, Jacobi obtained his doctorate from the University of Berlin on a topic involving partial fractions. The next year he became a lecturer at the University of Königsberg and was appointed professor there in 1831. Jacobi's first major work was his application of (his first love) elliptic functions to number theory. Moreover, Jacobi and his good friend Dirichlet both generated their own brands of analytic number theory. As well, Jacobi was interested in the history of mathematics and was a prime mover in the publication of the collected works of Euler—a task, incredibly, not completed fully to this day. Outside of number theory, he made contributions to analysis, geometry, and mechanics. Although many of his colleagues felt that he might work himself to death, he died of smallpox on February 18, 1851.

6.2 The Biquadratic Reciprocity Law

> *The doors we open and close each day decide the lives we lead.*
>
> **Flora Whittemore—see [14]**
>
> American Homesteader

Gauss was the first to state the Biquadratic (or Quartic)[6.9] Reciprocity Law, but he never published a proof. However, in [19, pp. 101–171], he made serious use of complex numbers to discuss biquadratic residues.[6.10] Eisenstein was the first to publish a proof in 1844. Indeed, Eisenstein went on to publish five separate proofs of this law between 1844 and 1847. In order to present a proof in this section, we must develop a theory analogous to that developed for the cubic case. We begin with the following quartic version of Proposition 6.1 on page 262.

Proposition 6.2 — Quartic Congruences

Let $F = \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, and let π be a prime element of

$$\mathfrak{O}_F = \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}].$$

If

$$\alpha \in \mathfrak{O}_F,\ \pi \nmid \alpha \text{ and } N_F(\pi) \neq 2,$$

then there exists a unique nonnegative rational integer $n \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N_F(\pi)-1)/4} \equiv i^n \pmod{\pi}.$$

Proof. From Exercise 4.31 on page 164, it follows that since F is a PID,

$$\alpha^{N_F(\pi)-1} \equiv 1 \pmod{\pi},$$

and by Remark 1.24 on page 52,

$$N_F(\pi) \equiv 1 \pmod 4.$$

Thus, $\alpha^{(N_F(\pi)-1)/4}$ is a root of $x^4 \equiv 1 (\text{mod } \pi)$, as are ± 1 and $\pm i$. Hence, $\alpha^{(N_F(\pi)-1)/4}$ must be one of i^n for $0 \leq n \leq 3$ modulo π. □

Proposition 6.2 now allows us to formulate the following.

Definition 6.5 — Biquadratic/Quartic Residue Symbol

Let π be a prime element in $\mathfrak{O}_F = \mathbb{Z}[i]$ with $N_F(\pi) \neq 2$, and let $\alpha \in \mathfrak{O}_F$. If $\pi \nmid \alpha$, then we set

$$\left(\frac{\alpha}{\pi}\right)_4 = i^n,$$

where n is the unique integer given by Proposition 6.2. If $\pi \mid \alpha$, then we set

$$\left(\frac{\alpha}{\pi}\right)_4 = 0.$$

[6.9] We will use the terms *quartic* and *biquadratic* interchangeably.

[6.10] Indeed, Gauss was the first to use the term *complex number* and introduced the symbol i for $\sqrt{-1}$—see [11, p. 254].Thanks to Gopala Srinivasan for pointing out the latter reference.

If $\beta = \pi_1\pi_2\cdots\pi_m$, where each π_j $1 \le j \le m \in \mathbb{N}$ is a prime element of $\mathfrak{O}_F$ with $N_F(\pi_j) \neq 2$, then set

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4 \left(\frac{\alpha}{\pi_2}\right)_4 \cdots \left(\frac{\alpha}{\pi_m}\right)_4 .$$

If $\beta \in \mathfrak{U}_{\mathfrak{O}_F}$, then set

$$\left(\frac{\alpha}{\beta}\right)_4 = 1,$$

for every nonzero $\alpha \in \mathfrak{O}_F$, and set

$$\left(\frac{0}{\beta}\right)_4 = 0.$$

Now we establish some properties of the quartic residue symbol.

Proposition 6.3 — Properties of the Quartic Residue Symbol

Let $\alpha,\beta \in \mathfrak{O}_F = \mathbb{Z}[i]$, and let π be a prime element of $\mathfrak{O}_F$. Then each of the following holds.

(a) If α,β are both nonzero and $\gcd(\alpha,\beta) = 1$, then

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\overline{\alpha}}{\overline{\beta}}\right)_4 = 1,$$

where $\overline{x}$ is the algebraic conjugate of x.[6.11]

(b) If $\pi \nmid \alpha$, then

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \text{ if and only if } x^4 \equiv \alpha \pmod{\pi} \text{ has a solution } x \in \mathfrak{O}_F^*.$$

(c) $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4.$

(d) If $\alpha \equiv \beta \pmod{\pi}$, then $(\frac{\alpha}{\pi})_4 = \left(\frac{\beta}{\pi}\right)_4.$

Proof. (a) By Definition 6.5 and Proposition 6.2, it suffices to prove this for $\beta = \pi$, a prime element of $\mathfrak{O}_F$, so $\alpha^{(N_F(\pi)-1)/4} \equiv (\frac{\alpha}{\pi})_4 \pmod{\pi}$, which implies

$$\overline{\alpha}^{(N_F(\pi)-1)/4} \equiv \overline{\left(\frac{\alpha}{\pi}\right)_4} \pmod{\overline{\pi}}.$$

Also, by Definition 6.5,

$$\left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 = \overline{\alpha}^{(N_F(\overline{\pi})-1)/4} = \overline{\alpha}^{(N_F(\pi)-1)/4},$$

so

$$\left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 = \overline{\left(\frac{\alpha}{\pi}\right)_4},$$

and multiplying both sides by $\left(\frac{\alpha}{\pi}\right)_4$ yields part (a).

Part (b) follows from Exercise 6.1 on page 275, and parts (c) and (d) are immediate from Definition 6.5. □

[6.11] Note that in this case, $\overline{x} = x'$ is both the algebraic and complex conjugate of $x = a + bi$ for the special case of the Gaussian integers, since $x' = a - bi = \overline{x}$.

Remark 6.4 From Proposition 6.3, we see that $(\frac{\alpha}{\pi})_4$ is a quartic character on the field $\mathbb{Z}[i]/(\pi)$ of $N_F(\pi)$ elements, called a *quartic residue character*, and we write

$$\chi_\pi^{(4)}(\alpha) = \left(\frac{\alpha}{\pi}\right)_4 .$$

Now we introduce the quartic analogue of Definition 6.3 on page 263.

Definition 6.6 — Primary Gaussian Integers
If $\alpha = a + bi \in \mathbb{Z}[i]$, then α is said to be *primary* if

$$a \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2 \text{ and } a + b \equiv 1 \pmod 4.$$

Lemma 6.4 — A Formulation for Primary Gaussian Integers
$\alpha = a + bi \in \mathbb{Z}[i]$ is a primary if and only if $a + bi \equiv 1 (\text{mod } 2 + 2i)$.

Proof. If $a + b \equiv 1 (\text{mod } 4)$, where a is odd and b is even, then

$$a + bi = 1 + \left(\frac{-1+a+b}{4} + \left(\frac{1-a+b}{4}\right) i\right)(2+2i) \equiv 1 \pmod{2+2i}.$$

Conversely, if $a + bi \equiv 1 (\text{mod } 2 + 2i)$, then there exist $c, d \in \mathbb{Z}$ such that

$$a + bi = 1 + (c + di)(2 + 2i) = 1 + 2c - 2d + (2c + 2d)i.$$

Thus, by comparing coefficients,

$$a = 1 + 2c - 2d \equiv 1 \pmod 2,\ b = 2c + 2d \equiv 0 \pmod 2,$$

and

$$a + b = (1 + 2c - 2d) + (2c + 2d) = 1 + 4c \equiv 1 \pmod 4.$$

□

Remark 6.5 By Proposition 6.4, the only unit that is primary is 1. Also, by Exercise 6.19 on page 292, a Gaussian integer not equal to 1 is primary if and only if it can be factored into a product of primary Gaussian primes. Also, if α is primary, then $(1 + i) \nmid \alpha$. Any Gaussian integer not divisible by $1 + i$ is said to be *odd*. This is in keeping with the fact that if $(1 + i) \mid \alpha$, then $2 \mid N_F(\alpha)$. Given an odd Gaussian integer, exactly one of its four associates is primary. This is the quartic analogue of Exercise 6.6 on page 275.

We now establish some properties of primary integers.

Lemma 6.5 — Properties of Primary Integers
Let $\alpha = a + bi$ be a primary element of $\mathbb{Z}[i] = \mathfrak{O}_F$. Then

$$\left(\frac{i}{\alpha}\right)_4 = i^{(1-a)/2}.$$

Furthermore, if $\alpha = \pi$ with $N_F(\pi) = p \equiv 1 (\text{mod } 4)$ is a primary prime element of $\mathfrak{O}_F$, then

$$J(\chi_\pi^{(4)}, \chi_\pi^{(4)}) = (-1)^{(p+3)/4}\pi.$$

Proof. First, we show that to prove the first assertion it suffices to prove the result for $\alpha = \pi$, a primary prime. Let $\alpha = a + bi$ and $\beta = c + di$ be primary Gaussian integers. Then $b \equiv 1 - a \pmod 4$ and $d \equiv 1 - c \pmod 4$, which together imply that $(1-a)(1-c) \equiv bd \pmod 8$. It follows that $b + d \equiv 1 - ac + bd \pmod 8$. Thus, if

$$\left(\frac{i}{\alpha}\right)_4 = i^{(1-a)/2} \text{ and } \left(\frac{i}{\beta}\right)_4 = i^{(1-c)/2},$$

then

$$\left(\frac{i}{\alpha}\right)_4 \left(\frac{i}{\beta}\right)_4 = i^{(1-a)/2} i^{(1-c)/2} = i^{(b+d)/2} = i^{(1-ac+bd)/2} = \left(\frac{i}{\alpha\beta}\right)_4.$$

Hence, we may assume that $\alpha = \pi = a + bi$ is a primary prime element. Therefore,

$$\left(\frac{i}{a+bi}\right)_4 = i^{(N_F(\pi)-1)/4} = i^{(a^2+b^2-1)/4} = i^{(1-a)/2},$$

where the last equality comes from the fact that $a^2 + b^2 - 1 \equiv 2 - 2a \pmod{16}$, given that $b \equiv 1 - a \pmod 4$. This establishes the first assertion.[6.12]

To prove the second assertion, we set $\chi_\pi^{(4)} = \chi$ for simplicity. By Exercise 6.8 on page 276,

$$J(\chi,\chi)\overline{J(\chi,\chi)} = p = \pi\overline{\pi}.$$

By the same reasoning as in the proof of Lemma 6.3 on page 266, $J(\chi,\chi) \equiv 0 \pmod \pi$. However, by Exercise 6.8 again, $N_F(J(\chi,\chi)) = p$. Therefore, $J(\chi,\chi)$ is prime by Exercise 1.27 on page 19. Thus, there exists $u \in \mathfrak{U}_{\mathfrak{O}_F}$ such that

$$uJ(\chi,\chi) = \pi. \tag{6.20}$$

Claim 6.8

$$(-1)^{(p+3)/4} J(\chi,\chi)$$

is primary.

Since $\chi(x) = \chi(p - x)$ for $x = 2, 3, \ldots, (p-1)/2$, then by Definition 6.4 on page 264

$$J(\chi,\chi) = 2\sum_{x=2}^{(p-1)/2} \chi(x)\chi(1-x) + \chi\left(\frac{p+1}{2}\right)^2.$$

Since $\chi(x), \chi(1-x) \in \mathfrak{U}_{\mathfrak{O}_F}$, then

$$\chi(x) \equiv \chi(1-x) \equiv 1 \pmod{2+2i}.$$

Therefore,

$$J(\chi,\chi) \equiv 2\left(\frac{p-3}{2}\right) + \chi\left(\frac{p+1}{2}\right)^2 \pmod{2+2i}.$$

However, as well we have that

$$\chi\left(\frac{p+1}{2}\right)^2 = \chi(2^{-1})^2 = \chi(2)^{-2} = \chi(-i(1+i)^2)^2 = \chi(-i)^2 = \chi((-i)^2) = \chi(-1),$$

[6.12] We observe that this first assertion is often called *one* of the *supplementary laws* to the Biquadratic Reciprocity Law—see Theorems 6.7 and 6.8 below for the others.

and since $p \equiv 1 \pmod{2+2i}$, then

$$J(\chi,\chi) \equiv 2\left(\frac{p-3}{2}\right) + \chi(-1) \equiv -2+\chi(-1) \pmod{2+2i}.$$

Therefore,

$$-\chi(-1)J(\chi,\chi) \equiv 2\chi(-1) - 1 \equiv 1 \pmod{2+2i},$$

where the last congruence follows from the fact that $\chi(-1) = \pm 1$. By Lemma 6.4 on page 280, $-\chi(-1)J(\chi,\chi)$ is primary. Since π is primary, then the congruences in Definition 6.6 on page 280 imply that

$$\frac{a+1}{2} \equiv \frac{p+3}{4} \pmod 2.$$

Thus, since $-\chi(-1) = (-1)^{(a+1)/2}$, then $(-1)^{(p+3)/4}J(\chi,\chi)$ is primary. This is Claim 6.8. Now, by Claim 6.8 and Exercise 6.20 on page 292, $u = (-1)^{(p+3)/4}$, so the result follows by multiplying (6.20) on page 281 through by $(-1)^{(p+3)/4}$. □

At this juncture, we have developed sufficient machinery to establish the Quartic Reciprocity Law. The following proof is similar to the proofs given by Eisenstein and Jacobi using the theory of cyclotomy.[6.13]

Theorem 6.5 — The Biquadratic Reciprocity Law

Let $\alpha = a+bi, \beta = c+di \in \mathbb{Z}[i]$ such that $\gcd(\alpha,\beta) = 1$ with both α and β primary. Then

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4 (-1)^{bd/4}. \tag{6.21}$$

Proof. We break the proof into two cases.

Case 6.5 $\alpha \in \mathbb{Z}$.

In this case, (6.21) becomes

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4. \tag{6.22}$$

By the factorization property given in Definition 6.5 on page 278, we may assume without loss of generality that $\alpha = \pm p$, where p is an odd rational prime (since 2 is not primary), and β is a Gaussian prime. The case where $\beta \in \mathbb{Z}$ is covered by Exercise 6.16, so we assume that $\beta \notin \mathbb{Z}$ and $N_F(\beta) = p \equiv 1 \pmod 4$. For simplicity, we set $\chi_\pi^{(4)} = \chi$. First we assume that $\alpha = -q$ where $q \equiv 3 \pmod 4$ is a rational prime.

By Lemma 6.5 on page 280,

$$J(\chi,\chi) = \pm\pi.$$

Also, by Theorem A.25 on page 341, since $q \equiv -1 \pmod 4$,

$$J^q(\chi,\chi) \equiv J(\overline{\chi},\overline{\chi}) \pmod q. \tag{6.23}$$

[6.13] The term *cyclotomy* refers to the theory of cyclotomic numbers, which may be defined as follows. For a given odd prime power $p^n = q = kf+1$ where $f,k,n \in \mathbb{N}$ with $k \geq 2$, fix a primitive root g modulo q. Then given integers s and t, the *cyclotomic number* $(s,t)_k$ *of order* k is the number of ordered pairs of integers (a,b) with $g^{ak+s}+1 = g^{bk+t}$ for $0 \leq a,b \leq (q-1)/k$. Thus, we see that the theory of cyclotomy essentially involves consideration of equations of the form $ax^k + by^k = 1$. The theory of cyclotomy was originated by Gauss. Kummer first observed the connection between Jacobi sums and cyclotomic numbers. Later, interest in the theory was renewed by the work of Dickson, and authors of the modern day keep the flame burning. See [3] for an in-depth analysis of this theory and its consequences.

Therefore,

$$\pi^{q+1} = J^{q+1}(\chi,\chi) \equiv J(\overline{\chi},\overline{\chi})J(\chi,\chi) = |J(\chi,\chi)|^2 = p \pmod{q}, \tag{6.24}$$

where the last equality comes from Exercise 6.8 on page 276. Moreover, by Exercises 5.27 on page 231, 5.52 on page 260, 6.17 on page 292, (with $\beta = q$), and Theorem A.25 on page 341, (which allows us to bring the q inside the sum),

$$G^q(\chi) \equiv \overline{\chi}^q(q)G(\chi^q) = \chi(q)G(\overline{\chi}) \pmod{q}. \tag{6.25}$$

Multiplying (6.25) through by $G(\chi)$, and using Exercise 5.54, we get

$$G^{q+1}(\chi) \equiv G(\chi)\chi(q)G(\overline{\chi}) \equiv \chi(-1)p\chi(q) \pmod{q}.$$

Hence,

$$G^{q+1}(\chi) \equiv \chi(-q)p \pmod{q}. \tag{6.26}$$

From Exercise 6.21 in conjunction with (6.24) and (6.26), we get

$$\chi(-q)\pi^{q+1} \equiv \chi(-q)p \equiv G^{q+1}(\chi) = (G^2(\chi))^{(q+1)/2}$$
$$\equiv (\sqrt{p}J(\chi,\chi))^{(q+1)/2} \equiv (pJ^2(\chi,\chi))^{(q+1)/4} \pmod{q},$$

and since $J_p^2(\chi,\chi) = \pi^2$, by Lemma 6.5, then the last congruence becomes

$$(p\pi^2)^{(q+1)/4} \equiv (\pi^{q+3})^{(q+1)/4} \pmod{q},$$

where the last congruence follows from (6.24). Therefore, we have shown that

$$\left(\frac{-q}{\pi}\right)_4 = \chi(-q) \equiv \pi^{(q+3)(q+1)/4-(q+1)} = \pi^{(q^2-1)/4} \equiv \left(\frac{\pi}{-q}\right)_4 \pmod{q}.$$

Thus (6.22) holds for $\alpha = -q \equiv 1 \pmod{4}$.

Now we assume that $\alpha = q$ where $q \equiv 1 \pmod{4}$ is a rational prime. By Exercise 5.52 and Theorem A.25,

$$G^q(\chi) \equiv \overline{\chi}^q G(\chi^q) \equiv \overline{\chi}(q)G(\chi) \pmod{q}.$$

Multiplying through by $G^{-1}(\chi)$, we get,

$$G^{q-1}(\chi) \equiv \overline{\chi}(q) \pmod{q}.$$

Therefore, by Exercise 6.21,

$$\overline{\chi}(q) \equiv G^{q-1}(\chi) \equiv (G^4(\chi))^{(q-1)/4} \equiv (pJ_p^2(\chi,\chi))^{(q-1)/4} \pmod{q}.$$

However, by Lemma 6.5, $J^2(\chi,\chi) = \pi^2$. Thus, the last congruence becomes,

$$(p\pi^2)^{(q-1)/4} \equiv (\pi^3\overline{\pi})^{(q-1)/4} \pmod{q}.$$

Now let $q = \gamma\overline{\gamma}$ in $\mathbb{Z}[i]$. Then by Proposition 6.2 on page 278, the above congruence becomes

$$\left(\frac{\overline{\pi}}{\gamma}\right)_4 \left(\frac{\pi}{\gamma}\right)_4^3 \equiv \left(\frac{\overline{\pi}}{\gamma}\right)_4 \overline{\left(\frac{\pi}{\gamma}\right)_4} \pmod{q}.$$

Hence, in particular, we have shown that

$$\overline{\chi}(q) = \overline{\left(\frac{q}{\pi}\right)_4} \equiv \left(\frac{\overline{\pi}}{\gamma}\right)_4 \overline{\left(\frac{\pi}{\gamma}\right)_4} \pmod{\gamma}.$$

By taking complex conjugates, we get,

$$\left(\frac{q}{\pi}\right)_4 \equiv \left(\frac{\pi}{\overline{\gamma}}\right)_4 \left(\frac{\pi}{\gamma}\right)_4 \equiv \left(\frac{\pi}{q}\right)_4 \pmod{\overline{\gamma}},$$

which establishes (6.22) for $\alpha = q \equiv 1 \pmod 4$, thereby securing Case 6.5.

Case 6.6 $\alpha,\beta \in \mathbb{Z}[i]$ are arbitrary primary integers with $\gcd(\alpha,\beta) = 1$.

By Case 6.5 and the factorization property given in Definition 6.5, we may assume that $\gcd(a, b) = \gcd(c, d) = 1$.

Claim 6.9 If $a \in \mathbb{Z}$, $a \equiv 1 \pmod 4$ and $\beta \in \mathbb{Z}[i]$ is primary with $\gcd(\beta, a) = 1$, then

$$\left(\frac{\beta}{a}\right)_4 = \left(\frac{a}{\beta}\right)_4.$$

Given the factorization property in Definition 6.5, Claim 6.9 follows from Case 6.5 and Lemma 6.5.

Let

$$\sigma_n = (-1)^{(n-1)/2},$$

where $n \in \mathbb{Z}$ is odd. The reader may easily check that $\sigma_a a$, $\sigma_c c$, and $\sigma_a\sigma_c(ac + bd)$ are primary. In the sequel, we will use the facts that

$$\sigma_c = (-1)^{(c-1)/2} = (-1)^{d/2} = i^d, \tag{6.27}$$

and similarly,

$$\sigma_a = i^b. \tag{6.28}$$

Since $c\alpha \equiv ac + bd \pmod \beta$, then

$$\left(\frac{\sigma_c c}{\beta}\right)_4 \left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\sigma_c(ac + bd)}{\beta}\right)_4 = \left(\frac{\sigma_a}{\beta}\right)_4 \left(\frac{\sigma_a\sigma_c(ac + bd)}{\beta}\right)_4, \tag{6.29}$$

where the last equality follows from the fact that $(\frac{\sigma_a}{\beta})_4{}^2 = 1$. Also, by Claim 6.9,

$$\left(\frac{\sigma_c c}{\beta}\right)_4 = \left(\frac{\beta}{\sigma_c c}\right)_4 = \left(\frac{c + di}{\sigma_c c}\right)_4 = \left(\frac{di}{\sigma_c c}\right)_4 = \left(\frac{i}{\sigma_c c}\right)_4 = i^{(1-\sigma_c c)/2},$$

where the penultimate equality comes from Lemma 6.5 and Exercise 6.16 on page 292. Thus, from Case 6.5 and Claim 6.9, (6.29) becomes

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\sigma_a}{\beta}\right)_4 \left(\frac{\beta}{\sigma_a\sigma_c(ac + bd)}\right)_4 i^{(\sigma_c c-1)/2}. \tag{6.30}$$

By a similar argument to the above,

$$\left(\frac{\beta}{\alpha}\right)_4 = \left(\frac{\sigma_c}{\alpha}\right)_4 \left(\frac{\alpha}{\sigma_a\sigma_c(ac + bd)}\right)_4 i^{(\sigma_a a-1)/2}. \tag{6.31}$$

By taking complex conjugates in (6.31), we get

$$\overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{\sigma_c}{\alpha}\right)_4 \left(\frac{\overline{\alpha}}{\sigma_a\sigma_c(ac + bd)}\right)_4 i^{(1-\sigma_a a)/2},$$

since $(\frac{\sigma_c}{\alpha})_4 = \pm 1$ from (6.27). Now we multiply this last equation by (6.30) to get,

$$\left(\frac{\alpha}{\beta}\right)_4 \overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{\sigma_c}{\alpha}\right)_4 \left(\frac{\sigma_a}{\beta}\right)_4 \left(\frac{\beta\overline{\alpha}}{\sigma_a\sigma_c(ac + bd)}\right)_4 i^{(\sigma_c c-\sigma_a a)/2}. \tag{6.32}$$

Claim 6.10

$$\left(\frac{\sigma_c}{\alpha}\right)_4\left(\frac{\sigma_a}{\beta}\right)_4\left(\frac{\beta\overline{\alpha}}{\sigma_a\sigma_c(ac+bd)}\right)_4 = \left(\frac{i}{\sigma_a\sigma_c(ac+bd)}\right)_4.$$

First, we need to show that $\gcd(ad-bc, ac+bd) = 1$ in order to invoke Exercise 6.16. If a prime

$$p \bigm| \gcd(ad-bc, ac+bd),$$

then p is necessarily odd. Let $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$. Then since $\pi \bigm| p$,

$$\pi \bigm| \overline{\alpha}\beta = (ac+bd) + (ad-bc)i,$$

and

$$\pi \bigm| \alpha\overline{\beta} = (ac+bd) - (ad-bc)i.$$

Since $\gcd(\alpha,\beta\,) = 1 = \gcd(\overline{\alpha}, \overline{\beta})$, then

$$\pi \bigm| \alpha \text{ and } \pi \bigm| \overline{\alpha},$$

or

$$\pi \bigm| \beta \text{ and } \pi \bigm| \overline{\beta}.$$

Without loss of generality, we may assume that the former is the case. Hence,

$$\pi \bigm| \alpha\overline{\alpha} \text{ and } \pi \bigm| (\alpha+\overline{\alpha}) = 2a,$$

so $\pi \bigm| a$ and $\pi \bigm| b$, given that $p > 2$. Hence $p \bigm| \gcd(a,b) = 1$, a contradiction. Now we may invoke Exercise 6.16 to get

$$\left(\frac{\beta\overline{\alpha}}{\sigma_a\sigma_c(ac+bd)}\right)_4 = \left(\frac{ac+bd+(ad-bc)i}{\sigma_a\sigma_c(ac+bd)}\right)_4 = \left(\frac{(ad-bc)i}{\sigma_a\sigma_c(ac+bd)}\right)_4 = \left(\frac{i}{\sigma_a\sigma_c(ac+bd)}\right)_4.$$

Also, from Lemma 6.5 and (6.27)–(6.28), it follows that

$$\left(\frac{\sigma_c}{\alpha}\right)_4\left(\frac{\sigma_a}{\beta}\right)_4 = \left(\frac{i^d}{\alpha}\right)_4\left(\frac{i^b}{\beta}\right)_4 = \left(\frac{i}{\alpha}\right)_4^d\left(\frac{i}{\beta}\right)_4^b = i^{(1-a)d/2}i^{(1-c)b/2} = i^{bd/2}i^{bd/2} = 1,$$

since α and β are primary. This completes the proof of Claim 6.10.

By Claim 6.10, (6.32) becomes

$$\left(\frac{\alpha}{\beta}\right)_4\overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{i}{\sigma_a\sigma_c(ac+bd)}\right)_4 i^{(\sigma_c c-\sigma_a a)/2} = i^{(1-\sigma_a\sigma_c(ac+bd)+\sigma_c c-\sigma_a a)/2}.$$

However, by definition $\sigma_c c \equiv \sigma_a a \equiv 1 \pmod 4$, so the latter equals

$$i^{-\sigma_a\sigma_c bd/2} = (-1)^{-\sigma_a\sigma_c bd/4} = (-1)^{bd/4}.$$

This establishes (6.21) in general. □

An application of the Biquadratic Reciprocity Law is the following.

Theorem 6.6 — Quartic Reciprocity and Prime Representation

Suppose that $p \equiv 1 \pmod 4$ is a rational prime with $a \equiv (-1)^{(p-1)/4} \pmod 4$, where $p = a^2 + b^2$. Also, let $b/2 \equiv 1 \pmod 4$ if $p \equiv 5 \pmod 8$.[6.14] Then b is a quartic residue modulo p if $p \equiv 1 \pmod 8$, and $b/2$ is a quartic residue modulo p if $p \equiv 5 \pmod 8$.

[6.14] These choices of a and b are made without loss of generality since one of $\pm a$ and one of $\pm b/2$ must satisfy the congruences.

Proof. If $p \equiv 1 \pmod 8$, then $a + bi = \pi$ is primary since $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$. Therefore, by the Biquadratic Reciprocity Law, Proposition 6.3 and Exercise 6.16 on page 292,

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{ai}{\pi}\right)_4 = \left(\frac{a}{\pi}\right)_4 \left(\frac{i}{\pi}\right)_4 = \left(\frac{\pi}{a}\right)_4 \left(\frac{i}{\pi}\right)_4 = \left(\frac{a+bi}{a}\right)_4 i^{(1-a)/2}$$
$$= \left(\frac{bi}{a}\right)_4 i^{(1-a)/2} = \left(\frac{b}{a}\right)_4 \left(\frac{i}{a}\right)_4 i^{(1-a)/2} = \left(\frac{b}{a}\right)_4 i^{a-1} = 1.$$

Hence, by Exercise 6.22, b is a quartic residue modulo p.

If $p \equiv 5 \pmod 8$, then since $-a \equiv b/2 \equiv 1 \pmod 4$, both $\pi = a + bi$ and $b/2$ are primary. Therefore, by the Biquadratic Reciprocity Law, and Exercise 6.16,

$$\left(\frac{b/2}{\pi}\right)_4 = \left(\frac{\pi}{b/2}\right)_4 = \left(\frac{a}{b/2}\right)_4 = 1.$$

Thus, by Exercise 6.22, $b/2$ is a quartic residue modulo p. □

In Theorem 6.4 on page 273, we gave the Supplement to the Cubic Reciprocity Law. Now we look at the exceptional element $1 + i$ in the quartic case. The following result is due to Eisenstein, and the ideas in the proof are due to K. S. Williams [72].

Theorem 6.7 — Supplement to the Biquadratic Reciprocity Law

Let $\alpha = a + bi \in \mathbb{Z}[i]$ be primary. Then

$$\left(\frac{1+i}{\alpha}\right)_4 = i^{(a-b-1-b^2)/4}.$$

Proof. First we establish the result for the case $b = 0$.

Claim 6.11 If $\alpha = a \in \mathbb{Z}$, where $a \equiv 1 \pmod 4$, then

$$\left(\frac{1+i}{a}\right)_4 = i^{(a-1)/4}.$$

It suffices to prove the claim for $a = \pm p$ where p is a rational prime. To see this, assume that we have rational integers $a_1 \equiv a_2 \equiv 1 \pmod 4$. Then

$$(a_1 - 1)/4 + (a_2 - 1)/4 \equiv (a_1 a_2 - 1)/4 \pmod 4. \tag{6.33}$$

We first assume that $a = p \equiv 1 \pmod 4$ is a rational prime, so $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$. Then

$$\left(\frac{1+i}{p}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{1+i}{\overline{\pi}}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{i}{\overline{\pi}}\right)_4 \left(\frac{1-i}{\overline{\pi}}\right)_4, \tag{6.34}$$

where the last equality follows from the fact that $1 + i = i(1 - i)$. Thus, (6.34) becomes,

$$\left(\frac{i}{\overline{\pi}}\right)_4 \left(\frac{1+i}{\pi}\right)_4 \overline{\left(\frac{1+i}{\pi}\right)_4} = \left(\frac{i}{\overline{\pi}}\right)_4 = i^{(N_F(\overline{\pi})-1)/4} = i^{(p-1)/4}.$$

Now we may assume that $a = -p \equiv 1 \pmod 4$ where p is a rational prime. By the Binomial Theorem,

$$(1+i)^p = \sum_{j=0}^{p} \binom{p}{j} i^j \equiv 1 + i^p = 1 + i^3 = 1 - i \pmod p,$$

since $p \equiv 3 \pmod 4$ and $i^3 = -i$. Therefore,

$$(1+i)^{p-1} \equiv (1-i)(1+i)^{-1} \equiv (1-i)^2 2^{-1} = -2i2^{-1} \equiv -i \equiv i^{-1} \pmod p.$$

Hence,

$$\left(\frac{1+i}{-p}\right)_4 = (1+i)^{(p^2-1)/4} = ((1+i)^{p-1})^{(p+1)/4} \equiv i^{(-p-1)/4} \pmod p,$$

which establishes Claim 6.11.

By (6.33) and Claim 6.11, we may assume that $a+bi$ is primary with $\gcd(a,b)=1$. Set $a^* = (-1)^{b/2}a \equiv 1 \pmod 4$. Then by Exercise 6.16 on page 292, Lemma 6.5 on page 280 and part (d) of Proposition 6.3,

$$\left(\frac{1+i}{a+bi}\right)_4 = \left(\frac{i}{a^*}\right)_4^{-1}\left(\frac{bi}{a^*}\right)_4\left(\frac{1+i}{a+bi}\right)_4 = i^{(a^*-1)/2}\left(\frac{a+bi}{a^*}\right)_4\left(\frac{1+i}{a+bi}\right)_4.$$

However, since $a^* = a(-1)^{b/2} = ai^b$, then by the Biquadratic Reciprocity Law, the previous equation equals

$$i^{(a^*-1)/2}\left(\frac{a^*}{a+bi}\right)_4\left(\frac{1+i}{a+bi}\right)_4 = i^{(a^*-1)/2}\left(\frac{ai^b}{a+bi}\right)_4\left(\frac{1+i}{a+bi}\right)_4$$

$$= i^{(a^*-1)/2}\left(\frac{i}{a+bi}\right)_4^b\left(\frac{a+ai}{a+bi}\right)_4 = i^{(a^*-1)/2}i^{b(1-a)/2}\left(\frac{a+ai}{a+bi}\right)_4$$

and since $a+ai = a+bi+i(a-b)$, then by Lemma 6.5 this equals,

$$i^{(a^*-1+b(1-a))/2}\left(\frac{i(a-b)}{a+bi}\right)_4 = i^{(a^*-1+b(1-a))/2}i^{(1-a)/2}\left(\frac{(a-b)}{a+bi}\right)_4$$

$$i^{(a^*-a+b(1-a))/2}\left(\frac{(a-b)}{a+bi}\right)_4 = i^{3b^2/4}\left(\frac{(a-b)}{a+bi}\right)_4,$$

where the last equality follows from the fact that

$$(a^*-a)/2 + b(1-a)/2 \equiv b^2/4 + b^2/2 \equiv 3b^2/4 \pmod 4.$$

Since $a-b \equiv 1 \pmod 4$ is primary, then by the Biquadratic Reciprocity Law,

$$i^{3b^2/4}\left(\frac{(a-b)}{a+bi}\right)_4 = i^{3b^2/4}\left(\frac{(a+bi)}{a-b}\right)_4 = i^{-b^2/4}\left(\frac{(a-b+b+bi)}{a-b}\right)_4$$

$$= i^{-b^2/4}\left(\frac{(b+bi)}{a-b}\right)_4 = i^{-b^2/4}\left(\frac{(1+i)}{a-b}\right)_4,$$

where the last equality follows from Exercise 6.16 on page 292. From Claim 6.11, this equals

$$i^{-b^2/4}i^{(a-b-1)/4} = i^{(a-b-1-b^2)/4},$$

which completes the proof. □

An application of Theorem 6.7 on the preceding page is the following, which also is considered to be one of the supplementary laws for biquadratic reciprocity—see Lemma 6.5 on page 280.

Theorem 6.8 — The Quartic Nature of 2
If $\pi = a + bi \in \mathbb{Z}[i]$ is a primary prime, then

$$\left(\frac{2}{\pi}\right)_4 = i^{ab/2}.$$

Proof. Since $2 = i^3(1+i)^2$, then

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{i}{\pi}\right)_4^3 \left(\frac{1+i}{\pi}\right)_4^2,$$

so by Theorem 6.7 on page 286 and Lemma 6.5 on page 280,

$$\left(\frac{2}{\pi}\right)_4 = i^{3(1-a)/2} i^{(a-b-1-b^2)/2} = i^{(2-2a-b-b^2)/2}.$$

Since $a + b \equiv 1 \pmod 4$, then

$$2 - 2a - b - b^2 = 2(1-a) - b - b^2 \equiv 2b - b - b^2 = b(1-b) \equiv ab \pmod 4,$$

from which the result follows. □

The following consequence of Theorem 6.8 was conjectured by Euler and proved by Gauss as a consequence of his work on biquadratic reciprocity.

Corollary 6.2 Let $p \equiv 1 \pmod 4$ be a rational prime. Then there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 64y^2$ if and only if $2 \equiv z^4 \pmod p$ for some $z \in \mathbb{Z}$. In other words, if p splits in $\mathbb{Q}(i)$, then $p = x^2 + 64y^2$ for some $x, y \in \mathbb{Z}$ if and only if 2 is biquadratic residue modulo p.

Proof. Since $p \equiv 1 \pmod 4$, then $p = a^2 + b^2 = \pi\overline{\pi}$, where $\pi = a + bi \in \mathbb{Z}[i]$ is primary since we may choose a to be odd and b to be even. By Theorem 6.8, Exercise 6.22 on page 293, and part (b) of Proposition 6.3 on page 279, $2 \equiv x^4 \pmod p$ if and only if $8 \mid b$. In other words, $p = x^2 + 64y^2$ for some $x, y \in \mathbb{Z}$ if and only if 2 is a quartic residue modulo p. □

We continue with a result from the realm of *rational biquadratic reciprocity*. This refers to those quartic residue symbols which assume only values ± 1 —see Exercises 6.16–6.18 on page 292. In particular, if $p \equiv q \equiv 1 \pmod 4$ are primes such that p is a square modulo q, then by Exercise 6.17, $(\frac{q}{\pi})_4 = 1$ or -1 depending upon whether q is a quartic residue modulo p or not. Thus, $(\frac{q}{\pi})_4$ depends only upon p and q and not upon π.[6.15] This naturally leads us to ask for the relationship between $(\frac{q}{\pi})_4$ and $(\frac{p}{\rho})_4$ where $q = \rho\overline{\rho}$ in $\mathbb{Z}[i]$. In 1969, K. Burde [8] discovered the following elegant answer.

Theorem 6.9 — Burde's Rational Quartic Reciprocity Law
Let $p \equiv q \equiv 1 \pmod 4$ be rational primes with Legendre symbol $(\frac{p}{q}) = 1$, and set $p = \pi\overline{\pi}$, $q = \rho\overline{\rho}$ where $\pi = a + bi, \rho = c + di \in \mathbb{Z}[i]$, are primary.[6.16] Then

$$\left(\frac{q}{\pi}\right)_4 \left(\frac{p}{\rho}\right)_4 = \left(\frac{ac+bd}{q}\right) = (-1)^{(q-1)/4}\left(\frac{ad-bc}{q}\right) = \left(\frac{ac+bd}{p}\right).$$

[6.15] The reader is cautioned that, for the above reasons, it is common practice in the literature, to use the symbol $(\frac{p}{q})_4$ for $(\frac{p}{\rho})_4$. However, Exercise 6.16 tells us that $(\frac{p}{q})_4$=1, so when $(\frac{p}{q})_4$ is used as a *rational residue symbol*, it takes on a different meaning from that established in Definition 6.5, so a caveat has to be given to that effect—see [3, p. 252], for instance. For the sake of clarity, especially for the "browsing" reader, we break with convention and avoid such notation, which is unnecessary in view of Exercise 6.22.

[6.16] We lose no generality by assuming primary π and ρ here. See Claim 6.14.

Proof. First, we establish the following.

Claim 6.12 $\left(\frac{q}{\pi}\right)_4 = \left(\frac{\pi}{q}\right)_4$.

Using Proposition 6.3 on page 279 and the Biquadratic Reciprocity Law, we get

$$\left(\frac{q}{\pi}\right)_4 = \left(\frac{\rho\overline{\rho}}{\pi}\right)_4 = \left(\frac{\rho}{\pi}\right)_4 \left(\frac{\overline{\rho}}{\pi}\right)_4 = \left(\frac{\pi}{\rho}\right)_4 \left(\frac{\pi}{\overline{\rho}}\right)_4 = \left(\frac{\pi}{\rho\overline{\rho}}\right)_4 = \left(\frac{\pi}{q}\right)_4,$$

which secures Claim 6.12.

Claim 6.13 $\left(\frac{q}{\pi}\right)_4 \left(\frac{p}{\rho}\right)_4 \equiv \pi^{(q-1)/2} \pmod{\rho}$.

By Claim 6.12, and Proposition 6.3,

$$\left(\frac{q}{\pi}\right)_4 \left(\frac{p}{\rho}\right)_4 = \left(\frac{\pi}{q}\right)_4 \left(\frac{p}{\rho}\right)_4 = \left(\frac{\pi}{\rho}\right)_4 \left(\frac{\pi}{\overline{\rho}}\right)_4 \left(\frac{\pi}{\rho}\right)_4 \left(\frac{\overline{\pi}}{\rho}\right)_4 = \left(\frac{\pi}{\rho}\right)_4^2.$$

However, by Proposition 6.2 on page 278,

$$\left(\frac{\pi}{\rho}\right)_4^2 \equiv \left(\pi^{(N_F(\rho)-1)/4}\right)^2 \equiv \pi^{(q-1)/2} \pmod{\rho},$$

which yields Claim 6.13.

By the Quadratic Reciprocity Law,

$$c^{(q-1)/2} \equiv \left(\frac{c}{q}\right) = \left(\frac{|c|}{q}\right) = \left(\frac{q}{|c|}\right) = \left(\frac{c^2+d^2}{|c|}\right) = \left(\frac{d^2}{|c|}\right) = 1 \pmod{q}.$$

Thus, from Claim 6.13,

$$\left(\frac{q}{\pi}\right)_4 \left(\frac{p}{\rho}\right)_4 \equiv (ac+bci)^{(q-1)/2} = (ac+bd+b(c+di)i)^{(q-1)/2}$$

$$\equiv (ac+bd)^{(q-1)/2} \equiv \left(\frac{ac+bd}{q}\right) \pmod{\rho},$$

from which the first equality in the statement of the theorem follows, since the latter congruence also holds modulo $\overline{\rho}$ given that both sides of the congruence are ±1. To get the last two equalities, we need the following, which establishes that $\left(\frac{ad+bc}{q}\right)$ is independent of sign.

Claim 6.14 $\left(\frac{ad-bc}{q}\right) = \left(\frac{ad+bc}{q}\right)$.

Since $q = c^2 + d^2$, then

$$\left(\frac{ad-bc}{q}\right)\left(\frac{ad+bc}{q}\right) = \left(\frac{a^2d^2-b^2c^2}{q}\right) = \left(\frac{a^2d^2+b^2d^2-b^2d^2-b^2c^2}{q}\right)$$

$$= \left(\frac{d^2(a^2+b^2)-b^2(c^2+d^2)}{q}\right) = \left(\frac{d^2(a^2+b^2)}{q}\right) = \left(\frac{d^2p}{q}\right) = \left(\frac{p}{q}\right) = 1.$$

This completes the proof of Claim 6.14.

From Claim 6.14 we have,

$$\left(\frac{ac+bd}{q}\right)\left(\frac{ad-bc}{q}\right)=\left(\frac{ac+bd}{q}\right)\left(\frac{ad+bc}{q}\right)=\left(\frac{abq+cdp}{q}\right)=\left(\frac{cdp}{q}\right)$$
$$=\left(\frac{cd}{q}\right)=\left(\frac{2}{q}\right)\left(\frac{2cd}{q}\right)=\left(\frac{2}{q}\right)\left(\frac{(c+d)^2-q}{q}\right)=\left(\frac{2}{q}\right)$$
$$=(-1)^{(q^2-1)/8}=((-1)^{(q+1)/2})^{(q-1)/4}=(-1)^{(q-1)/4},$$

from which the penultimate equality of the theorem follows. The last equality in the statement of the theorem follows by symmetry. □

Given distinct primes $p\equiv q\equiv 1\,(\text{mod }4)$, such that p is a quartic residue modulo q, Burde's Theorem gives necessary and sufficient conditions for q to be a quartic residue modulo p. For instance, we have the following illustration.

Example 6.5 Let $p=29$ and $q=181$. Here we may take $a=5$, $b=2$, $c=9$ and $d=10$. Since $6^4\equiv 29\,(\text{mod }181)$, then $(\frac{29}{\rho})_4=1$, where $q=c^2+d^2=\rho\overline{\rho}$. Therefore, by Burde's Theorem with $p=a^2+b^2=\pi\overline{\pi}$,

$$\left(\frac{q}{\pi}\right)_4=\left(\frac{181}{\pi}\right)_4=\left(\frac{ac+bd}{q}\right)=\left(\frac{65}{181}\right)$$
$$=\left(\frac{5}{181}\right)\left(\frac{13}{181}\right)=\left(\frac{181}{5}\right)\left(\frac{181}{13}\right)=\left(\frac{181}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{2}{13}\right)=-1,$$

by (A.10) on page 342. Hence, 181 is not a fourth power modulo 29. However, $\left(\frac{181}{29}\right)=\left(\frac{7}{29}\right)=1$, so 181 is a quadratic residue modulo 29. This places 29 in category (b) of Exercise 6.18 on page 292.

As valuable as rational biquadratic reciprocity has shown to be, it has its limitations in the greater scope of applications of biquadratic reciprocity. For instance, if $n\geq 3$ is an odd integer and $p=4n+1$ is prime, then

$$N=2^{2n}+1=(2^n-2^{(n+1)/2}+1)(2^n+2^{(n+1)/2}+1)=AB,$$

is not prime. The Quadratic Reciprocity Law tells us that

$$2^{2n}+1=2^{(p-1)/2}+1\equiv\left(\frac{2}{p}\right)+1\equiv 0\pmod p,$$

since $p\equiv 5\,(\text{mod }8)$ by (A.10). Thus, $p\bigm| N$. The question naturally arises (and was posed by Brillhart in [6]): Which of A or B does p divide? To answer the question, we need to know A modulo p. Since $2^n=2^{(p-1)/4}$ and $(\frac{2}{p})=-1$, we need to determine which of $2^{(p-1)/4}\equiv i$ (mod π), or $2^{(p-1)/4}\equiv -i\,(\text{mod }\pi)$ holds, where $p=\pi\overline{\pi}$ with $\pi,\overline{\pi}\in\mathbb{Z}[i]$. In other words, we are in category (a) of Exercise 6.18. Rational quartic reciprocity does not help us here. Instead, we close this section with a demonstration of how the Biquadratic Reciprocity Laws and its supplements may be used to answer the above question. The following was first proved by Gosset [22] in 1910, but the following proof is due to Lemmermeyer [38].

Theorem 6.10 Quadratic Reciprocity and Factorization
Let $p = 4n + 1 = a^2 + 4b^2$ be a prime where $n \in \mathbb{N}$ is odd. Then

$$2^{2n} + 1 = AB,$$

where

$$A = 2^n - 2^{(n+1)/2} + 1, \quad B = 2^n + 2^{(n+1)/2} + 1,$$

$$b \equiv \pm 3 \pmod 8 \text{ if and only if } p \mid A \text{ and } B \equiv 2(1 + 2^n) \pmod p,$$

and

$$b \equiv \pm 1 \pmod 8 \text{ if and only if } p \mid B \text{ and } A \equiv 2(1 + 2^n) \pmod p.$$

Proof. First, set $\pi = a + 2bi$, where we may assume that $a \equiv 3 \pmod 4$ and $2b \equiv 2 \pmod 4$ without loss of generality since one of $\pm\pi$ must satisfy the congruences. As shown in the preamble to this theorem, $p \mid (2^{2n} + 1)$. Thus, by Theorem 6.8 on page 288,

$$2^{(p-1)/4} \equiv \left(\frac{2}{\pi}\right)_4 \equiv i^{ab} \equiv i^{-b} \pmod \pi. \tag{6.35}$$

Also, $2^{(p+3)/8} = ((1 + i)^2 i^{-1})^{(p+3)/8} = (1 + i)^{(p+3)/4} i^{-(p+3)/8}$, from which it follows that

$$2^{(p+3)/8}(1 + i)^{-1} = (1 + i)^{(p-1)/4} i^{-(p+3)/8} \equiv \left(\frac{1+i}{\pi}\right)_4 i^{-(p+3)/8}$$

$$\equiv i^{(a-2b-1-4b^2)/4} i^{-(p+3)/8} \equiv i^{(2a-4b-a^2-12b^2-5)/8} \pmod \pi,$$

where the penultimate congruence follows from Theorem 6.7 on page 286. A calculation shows that

$$\frac{2a - 4b - a^2 - 12b^2 - 5}{8} \equiv \frac{3 - b}{2} \pmod 4.$$

Thus, we have shown that

$$2^{(p+3)/8} \equiv (1 + i)i^{(3-b)/2} \pmod \pi. \tag{6.36}$$

We now use (6.35)–(6.36) in each of the following cases.
If $b \equiv 1 \pmod 8$, then

$$B = 2^{(p-1)/4} + 2^{(p+3)/8} + 1 \equiv i^{-b} + i^{(3-b)/2}(1 + i) + 1 \equiv i^3 + i + i^2 + 1 \equiv 0 \pmod \pi.$$

By taking complex conjugates, $i + i^3 + i^2 + 1 \equiv 0 \pmod{\overline{\pi}}$, so $B \equiv 0 \pmod p$.
If $b \equiv -1 \pmod 8$, then

$$B \equiv i^{-b} + i^{(3-b)/2} + i^{(5-b)/2} + 1 \equiv i + i^2 + i^3 + 1 \equiv 0 \pmod \pi,$$

so as in the previous case $p \mid B$.
If $b \equiv 3 \pmod 8$, then

$$A = 2^{(p-1)/4} - 2^{(p+3)/8}(1 + i) + 1 \equiv i^{-b} - i^{(3-b)/2}(1 + i) + 1 \equiv i - (1 + i) + 1 \equiv 0 \pmod \pi,$$

so as above, $p \mid A$.
If $b \equiv -3 \pmod 8$, then

$$A \equiv i^{-b} - i^{(3-b)/2}(1 + i) + 1 \equiv i^3 - i^3(1 + i) + 1 \equiv 0 \pmod \pi,$$

and as above $A \equiv 0 \pmod p$.
Since $A + B = 2 + 2^{n+1}$, then the remaining congruences follow. □

Exercises

6.16. Let $a, b \in \mathbb{Z}$ with b odd, a nonzero and $\gcd(a,b) = 1$. Prove that

$$\left(\frac{a}{b}\right)_4 = 1.$$

6.17. Let $a \in \mathbb{Z}$ be nonzero, and let $p \equiv 1 \pmod 4$ be a rational prime with $p = \pi\overline{\pi}$ where π is a prime element of $\mathbb{Z}[i]$. Prove that

$$\left(\frac{a}{\pi}\right)_4^2 = \left(\frac{a}{p}\right),$$

where the symbol on the right is the Legendre symbol. In particular, conclude that

$$\left(\frac{a}{\pi}\right)_4 = \pm 1 \text{ if and only if } \left(\frac{a}{p}\right) = 1.$$

6.18. With the same hypothesis as that of Exercise 6.17, prove that

$$\left(\frac{\mathbb{Z}[i]}{\pi\mathbb{Z}[i]}\right)^* \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*,$$

and that this multiplicative group is partitioned into three parts as follows:

(a) The biquadratic residues, namely those for which $(\frac{a}{\pi})_4 = 1$.

(b) The quadratic residues that are *not* biquadratic residues, namely those for which $(\frac{a}{\pi})_4 = -1$.

(c) The quadratic nonresidues, namely those for which $(\frac{a}{\pi})_4 = \pm i$.

The facts established in Exercises 6.16–6.18 are aspects of what is called rational biquadratic reciprocity*. See the preamble to Theorem 6.9.*

6.19. Prove that a Gaussian integer, which is not a unit, is primary if and only if it can be factored into a product of primary Gaussian primes.

6.20. Let $\alpha \in \mathbb{Z}[i] = \mathfrak{O}_F$ be a nonunit with $(1+i) \nmid \alpha$. Prove that there exists a unique unit $u \in \mathfrak{U}_{\mathfrak{O}_F}$ such that $u\alpha$ is primary. In particular, conclude (via Remark 6.5 on page 280) that if α is primary, then $u = 1$.

6.21. Let $\chi = \chi_\pi^{(4)} = (\frac{}{\pi})_4$ where $p \equiv 1 \pmod 4$ is a rational prime with $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$, and π primary. Prove that

$$G^2(\chi) = J(\chi,\chi)\sqrt{p} = (-1)^{(p+3)/4}\pi\sqrt{p}.$$

(*The fact that* $G^2(\chi) = (-1)^{(p+3)/4}\pi\sqrt{p}$ *has some historical interest. It implies that* $G(\chi) = \sigma\sqrt{(-1)^{(p+3)/4}\pi\sqrt{p}}$, *where* $\sigma = \pm 1$ *and the square root has positive real part. In 1979, Matthews* [45] *proved that*

$$\sigma = -\beta\left(\frac{2i}{\pi}\right)_4\left(\frac{2|b|}{a}\right),$$

where the symbol on the right is the Jacobi symbol and $\beta = \pm i$ *is defined by* $\beta \equiv (\frac{p-1}{2})!$ $\pmod{\pi}$.)

6.22. Suppose that $p \equiv 1 \pmod 4$ is a rational prime with $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$. Prove that a given $\delta \in \mathbb{Z}[i]$ is a quartic residue modulo p if and only if it is a quartic residue modulo both π and $\overline{\pi}$. Furthermore, prove that δ is a quartic residue modulo p if and only if $\delta \equiv z^4 \pmod p$ for some $z \in \mathbb{Z}$.

6.23. Let $p \equiv 3 \pmod 4$ be a rational prime, and $a \in \mathbb{Z}$ with $p \nmid a$. Prove that a is a biquadratic residue modulo p. Furthermore, establish that there exists an $x \in \mathbb{Z}$ such that $a \equiv x^4 \pmod p$ if and only if $\left(\frac{a}{p}\right) = 1$, where the latter is the Legendre symbol.

6.24. Let $p > 2$ be a rational prime. Prove that if

$$2 \equiv x^4 \pmod p \text{ for some } x \in \mathbb{Z}[i], \text{ then } p \equiv \pm 1 \pmod 8.$$

6.25. Let $p \equiv 1 \pmod 8$ be a rational prime, so $p = a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$—see Corollaries 4.1–4.2 on page 141. Also, let $p = \pi\overline{\pi}$ for $\pi, \overline{\pi} \in \mathbb{Z}[i]$. Prove that

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{a}{p}\right),$$

where the right-hand symbol is the Legendre symbol.

This fact that for a prime $p \equiv 1 \pmod 8$, the biquadratic character of 2 is determined by its decomposition $p = a^2 + 2b^2$, was first proved by Gauss.

6.26. Let $p = a^2 + b^2$ and $q = c^2 + d^2$ be distinct primes with $b \equiv d \equiv 0 \pmod 2$. Use Theorem 6.9 on page 288 to prove that

$$\left(\frac{ac+bd}{p}\right) = \left(\frac{ac+bd}{q}\right).$$

6.27. Let $p = a^2 + b^2 = 4m + 1$ be a rational prime where $\pi = a + bi \in \mathbb{Z}[i]$ is primary. Establish each of the following.

(a) If $\chi = \chi_\pi^{(4)}$, then $J(\chi,\chi^2) = \pi$.

(b) $2a \equiv (-1)^m \binom{2m}{m} \pmod p$.

The result in part (b) *was first proved by Gauss in 1828. A more involved result in this direction was found by Cauchy, namely if*

$$p = 20m + 1 = u^2 + 5v^2$$

is prime, then

$$\binom{10m}{m}\binom{10m}{3m} \equiv 4u^2 \pmod p.$$

Numerous results involving congruences and binomial coefficients have been found over the last century see [3, Chapter 9, pp. 268–293] *for details.*

6.3 The Stickelberger Relation

> *Personal relations are the important thing for ever and ever, and not this outer life of telegrams and anger.*
>
> *from Chapter 19 of* **Howard's End (1910)**
> **E.M. Forster**
> English Novelist

In §6.4, we will prove the Eisenstein Reciprocity Law, which generalizes the laws studied thus far in this chapter. However, in order to do so, we need to develop some notions surrounding the concept in the title, which is the primary object of study in this section—see Theorem 6.12 on page 302. First we need the following generalization of ideas developed in the preceding two sections.

Proposition 6.4 — Power Residue Congruences

Suppose that $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$ and $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal with $N(\mathfrak{p}) = q \equiv 1 \,(\text{mod } n)$. If $\alpha \in \mathfrak{O}_F$ and $\alpha \notin \mathfrak{p}$, then there exists a $j \in \mathbb{Z}$, unique modulo n, such that

$$\alpha^{(q-1)/n} \equiv \zeta_n^j \pmod{\mathfrak{p}}.$$

Proof. Since $|(\mathfrak{O}_F/\mathfrak{p})^*| = q - 1$, then $\alpha^{q-1} \equiv 1 \,(\text{mod } \mathfrak{p})$. Therefore, since $N(\mathfrak{p}) = q \equiv 1 \,(\text{mod } n)$, then $\alpha^{(q-1)/n}$ is a root of $x^n \equiv 1 \,(\text{mod } \mathfrak{p})$, as are the distinct values ζ_n^j for $j = 0, 1, \ldots, n-1$. Thus, $\alpha^{(q-1)/n}$ must be (uniquely) one of them by Exercise 4.29 on page 163. □

Definition 6.7 — Power Residue Symbol

Let $F = \mathbb{Q}(\zeta_n)$, where $n > 1$ is an integer, $\alpha \in \mathfrak{O}_F$, and $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal with $n \notin \mathfrak{p}$. Then the n^{th} power residue symbol is defined to be

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(N(\mathfrak{p})-1)/n} \equiv \zeta_n^j \pmod{\mathfrak{p}}, \text{ when } \alpha \notin \mathfrak{p},$$

where j is the unique integer given in Proposition 6.4, and

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 0, \text{ when } \alpha \in \mathfrak{p}.$$

If I is an $\mathfrak{O}_F$-ideal and

$$I = \prod_{j=1}^m \mathcal{P}_j$$

is the prime factorization of I given by Theorem 1.17 on page 28, where the $\mathcal{P}_j$ are not necessarily distinct, and $\gcd((n), I) = 1$, then

$$\left(\frac{\alpha}{I}\right)_n = \prod_{j=1}^m \left(\frac{\alpha}{\mathcal{P}_j}\right)_n,$$

and if $\gcd(\alpha,\beta) = 1$, then

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\alpha}{(\beta)}\right)_n.$$

Proposition 6.5 — Properties of the Power Residue Symbol

Suppose that $F = \mathbb{Q}(\zeta_n)$, $\alpha,\beta \in \mathfrak{O}_F$ and I, J are $\mathfrak{O}_F$-ideals relatively prime to n. Then

(a) $(\frac{\alpha\beta}{I})_n = (\frac{\alpha}{I})_n(\frac{\beta}{I})_n$.

(b) $(\frac{\alpha}{IJ})_n = (\frac{\alpha}{I})_n(\frac{\alpha}{J})_n$.

(c) If α is prime to I and $x^n \equiv \alpha \pmod{I}$ is solvable for some $x \in \mathfrak{O}_F$, then $(\frac{\alpha}{I})_n = 1$.

Proof. Part (c) follows from Exercise 6.1 on page 275, and parts (a)–(b) follow directly from Definition 6.7. □

Now we bring Galois theory into the picture.

Proposition 6.6 — Galois Action on Residue Symbols

Let $F = \mathbb{Q}(\zeta_n)$, and let I be an $\mathfrak{O}_F$-ideal with $\gcd(I, (n)) = 1$. If $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, then

$$\left(\frac{\alpha}{I}\right)_n^\sigma = \left(\frac{\alpha^\sigma}{I^\sigma}\right)_n .$$

Proof. Given property (b) of Proposition 6.5, it suffices to prove this for the case where $I = \mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal. By Definition 6.7 and the fact that $N(\mathfrak{p}) = N(\mathfrak{p}^\sigma)$,

$$\left(\frac{\alpha^\sigma}{\mathfrak{p}^\sigma}\right)_n \equiv (\alpha^\sigma)^{(N(\mathfrak{p}^\sigma)-1)/n} = (\alpha^\sigma)^{(N(\mathfrak{p})-1)/n} = (\alpha^{(N(\mathfrak{p})-1)/n})^\sigma \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n^\sigma \pmod{\mathfrak{p}},$$

which is the desired result. □

Now we bring Gauss sums into the picture. For a reminder of the definition of Gauss sums, see Exercise 5.52 on page 260.

Definition 6.8 — Power Residue Characters

Let $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$ and $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal such that $n \notin \mathfrak{p}$. Suppose further that $N(\mathfrak{p}) = q = p^f$, p is a rational prime and $f = f_{F/\mathbb{Q}}(\mathfrak{p})$, where $p^f \equiv 1 \pmod{n}$—see Corollary 5.13 on page 218. If $\psi(\alpha) = a$ is the image of α under the natural map $\psi : \mathfrak{O}_F \mapsto \mathfrak{O}_F/\mathfrak{p}$, then for $\psi(\alpha) = a \neq 0$, define a character $\chi_{\mathfrak{p}}^{(n)}$ on $\mathbb{F}_q = \mathfrak{O}_F/\mathfrak{p}$ by

$$\chi_{\mathfrak{p}}^{(n)}(a) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{-1} = \overline{\left(\frac{\alpha}{\mathfrak{p}}\right)_n} .$$

The reason for the choice of the inverse in Definition 6.8 will become evident in the proof of Theorem 6.11 on page 298. On the basis of Definition 6.8 and the definition of Gauss sums given in Exercise 5.52, we introduce the following link to Gauss sums.

Definition 6.9 — Gauss Sums and Power Residues

With the assumptions of Definition 6.8, we let $\chi = \chi_{\mathfrak{p}}^{(n)}$. Then we define

$$G(\mathfrak{p}) = G_1(\chi) = G(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)}, \tag{6.37}$$

and

$$\mathfrak{G}(\mathfrak{p}) = G(\mathfrak{p})^n, \tag{6.38}$$

The $\mathfrak{G}(\mathfrak{p})$ were studied by Jacobi in 1827 for the case where $q = p$.

Proposition 6.7 — Properties of Power Residue Gauss Sums

With the assumptions of Definition 6.8, each of the following holds.

(a) $G(\mathfrak{p}) \in \mathbb{Q}(\zeta_{np})$.

(b) $|G(\mathfrak{p})|^2 = q$.

(c) $\mathfrak{G}(\mathfrak{p}) \in \mathbb{Q}(\zeta_n)$.

Proof. By Equation (6.37) on page 295, and the fact that the values of $\chi_{\mathfrak{p}}^{(n)}$ are n^{th} roots of unity, with $p \nmid n$, then (a) follows—see Exercise 5.27 on page 231. Part (b) follows from Exercise 5.54 on page 260. Part (c) follows from Claim 6.1 on page 265 since the proof of that claim extends to $\mathbb{F}_q$. □

In order to establish the Stickelberger Relation, we need to understand the decomposition of primes above p in various cyclotomic extensions—see Biography 1.4 on page 54. The following development is toward that goal. We first remind the reader of the notion of the *order of an ideal modulo a prime ideal* introduced in Exercise 1.44 on page 34, denoted by $\operatorname{ord}_{\mathfrak{p}}(I)$.

Proposition 6.8 — Properties of $\mathbf{ord}_{\mathfrak{p}}(\mathbf{I})$

The integer $\operatorname{ord}_{\mathfrak{p}}(I)$ satisfies each of the following.

(a) If $\mathfrak{q}$ is a prime $\mathfrak{O}_F$-ideal, then $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{q}) = 0$ if $\mathfrak{p} \neq \mathfrak{q}$, and $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{q}) = 1$ if $\mathfrak{p} = \mathfrak{q}$.

(b) If I and J are $\mathfrak{O}_F$-ideals, then $\operatorname{ord}_{\mathfrak{p}}(IJ) = \operatorname{ord}_{\mathfrak{p}}(I) + \operatorname{ord}_{\mathfrak{p}}(J)$.

(c) Suppose that I is an $\mathfrak{O}_F$-ideal and

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})},$$

where the product is taken over all distinct prime $\mathfrak{O}_F$-ideals $\mathfrak{p}$, is the unique factorization given by Theorem 1.17 on page 28 with $a(\mathfrak{p}) \neq 0$ for only finitely many such integers. Then $a(\mathfrak{p})$ is that unique nonnegative integer given by

$$a(\mathfrak{p}) = \operatorname{ord}_{\mathfrak{p}}(I).$$

Proof. Since $\mathfrak{p} \nsubseteq \mathfrak{p}^2$ and since $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{q}) > 0$ if and only if $\mathfrak{q} \subseteq \mathfrak{p}$, then part (a) follows. Part (b) is part (a) of Exercise 1.44. Part (c) follows from Theorem 1.17 on page 28. □

Diagram 6.1

$$\begin{tikzcd}
\mathcal{P} \arrow[d, dash] & \subseteq & \mathfrak{O}_K \arrow[r] \arrow[d, dash] & \mathfrak{O}_K/\mathcal{P} \arrow[d, dash] \\
\mathfrak{P} \arrow[d, dash] & \subseteq & \mathfrak{O}_L \arrow[r] \arrow[d, dash] & \mathfrak{O}_L/\mathfrak{P} \arrow[d, dash] \\
\mathfrak{p} \arrow[d, dash] & \subseteq & \mathfrak{O}_F \arrow[r] \arrow[d, dash] & \mathfrak{O}_F/\mathfrak{p} \arrow[d, dash] \\
p & \subseteq & \mathbb{Z} \arrow[r] & \mathbb{Z}/p\mathbb{Z}
\end{tikzcd}$$

Diagram 6.1 will be a visual aid for the reader in the proof of the next result.

We now return to a consideration of the decomposition of p in cyclotomic fields discussed above. The following sets the stage for the Stickelberger Relation, since what is at the heart of this relation is prime ideal decomposition in cyclotomic fields, given that Gauss sums are in such fields. The reader should be familiar with the results surrounding Corollary 5.13 on page 218 before proceeding.

Let $n \in \mathbb{N}$, $F = \mathbb{Q}(\zeta_n)$, p a rational prime such that $p \nmid n$, and $\mathfrak{p}$ a prime $\mathfrak{O}_F$-ideal above p. Furthermore, let $K = \mathbb{Q}(\zeta_{p(q-1)})$, $L = \mathbb{Q}(\zeta_{q-1})$, where $q = p^f \equiv 1 \pmod{n}$, and $f = f_{F/\mathbb{Q}}(p)$. Also let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-ideal above $\mathfrak{p}$, and set $\mathcal{P} \cap L = \mathfrak{P}$.

Proposition 6.9 — Order of Ideals in Cyclotomic Fields

With notation as in the above preamble, each of the following holds.

(a) $\operatorname{ord}_{\mathcal{P}}(p\mathfrak{O}_K) = p - 1$.

(b) $\operatorname{ord}_{\mathcal{P}}(1 - \zeta_p) = 1$.

(c) $\operatorname{ord}_{\mathcal{P}}(\mathfrak{p}) = p - 1$.

(d) $\mathfrak{O}_F/\mathfrak{p} \cong \mathfrak{O}_L/\mathfrak{P}$.

Proof. Part (a) is an immediate consequence of Corollary 5.13. Also, from Example 5.8 on page 190, we see that

$$p\mathfrak{O}_F = p\mathfrak{O}_{\mathbb{Q}(\zeta_p)} = (1 - \zeta_p)^{p-1}\mathfrak{O}_{\mathbb{Q}(\zeta_p)} = (1 - \zeta_p)^{p-1}\mathfrak{O}_F,$$

so

$$p\mathfrak{O}_K = p\mathfrak{O}_{\mathbb{Q}(\zeta_p)}\mathfrak{O}_K = (1 - \zeta_p)^{p-1}\mathfrak{O}_K = \left(\prod_{j=1}^{g} \mathcal{P}_j\right)^{p-1},$$

where $\mathcal{P}_1 = \mathcal{P}$ say, and $g = g_{K/\mathbb{Q}}(p)$. Thus, $(1 - \zeta_p)\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j$, and (b) follows. Also, from Corollary 5.13,

$$\mathfrak{p}\prod_{j=2}^{g} \mathfrak{p}_j\mathfrak{O}_K = \left(\mathcal{P}\prod_{j=2}^{g} \mathcal{P}_j\right)^{p-1}.$$

Therefore, since $\gcd(\mathcal{P}, \mathcal{P}_j) = 1$ for $j > 1$,

$$\mathfrak{p}\mathfrak{O}_K = \mathcal{P}^{p-1},$$

from which (c) follows.

Lastly, we establish part (d). By Corollary 5.13,

$$f_{L/\mathbb{Q}}(p) = |\mathfrak{O}_L/\mathfrak{P} : \mathbb{Z}/(p)|$$

is the smallest natural number such that $p^{f_{L/\mathbb{Q}}(p)} \equiv 1 \pmod{q-1}$. However, $q = p^f$, so $p^f \equiv 1 \pmod{q-1}$, and $f = f_{L/\mathbb{Q}}(p)$, so by Theorem 5.1 on page 184,

$$f = f_{L/\mathbb{Q}}(p) = f_{L/F}(\mathfrak{p})f_{F/\mathbb{Q}}(p) = f_{L/F}(\mathfrak{p})f.$$

Thus,

$$1 = f_{L/F}(\mathfrak{p}) = |\mathfrak{O}_L/\mathfrak{P} : \mathfrak{O}_F/\mathfrak{p}|,$$

from which (d) follows via Definition 5.1 on page 182. □

Remark 6.6 Part (d) of Proposition 6.9 on the preceding page allows us to define a character for on $\mathbb{F}_q = \mathfrak{O}_L/\mathfrak{P} \cong \mathfrak{O}_F/\mathfrak{p}$, as a $(q-1)$-th power residue symbol, namely for $\gamma \in \mathfrak{O}_L$,

$$\chi_{\mathfrak{P}}^{(q-1)}(\psi(\gamma)) = \left(\frac{\gamma}{\mathfrak{P}}\right)_{q-1}$$

where ψ is the natural map $\psi : \mathfrak{O}_L \mapsto \mathbb{F}_q$. Thus, $\chi_{\mathfrak{P}}^{(q-1)}$ has order $q-1$, so it generates $\mathfrak{Ch}(\mathbb{F}_q^\times)$. This allows us to introduce another important Gauss sum.

Definition 6.10 — Gauss sums on $\mathbb{F}_q$

With the setup given in Diagram 6.1 on page 296, and $m \in \mathbb{N}$, set

$$G_m(\mathfrak{P}) = G((\chi_{\mathfrak{P}}^{(q-1)})^{-m}).$$

Remark 6.7 Notice that if $m = (q-1)/n$ in Definition 6.10, then $G_m(\mathfrak{P}) = G(\mathfrak{p})$ given in (6.37) on page 295, since for any $\alpha \in \mathfrak{O}_F$ we have,

$$\left(\frac{\alpha}{\mathfrak{P}}\right)_{q-1}^{(q-1)/n} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n .$$

The following result will give us the necessary machinery to prove the desired Stickelberger Relation.

Theorem 6.11 — Orders of Gauss Sums on $\mathbb{F}_q$

Given the setup in Diagram 6.1, and $m \in \mathbb{N}$ with $0 < m < q$,

$$\operatorname{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) = \sum_{j=0}^{f-1} a_j^{(m)}, \tag{6.39}$$

where the $a_j^{(m)}$ are defined by

$$m = \sum_{j=0}^{f-1} a_j^{(m)} p^j \tag{6.40}$$

which is the unique representation of m to base p with $0 \le a_j^{(m)} < p$.

Proof. If $q = 2$, then

$$G_1(\mathfrak{P}) = G_1(p) = G(1) = \pm\sqrt{\pm p}$$

by Exercise 5.34 on page 232. Therefore, $\operatorname{ord}_{\mathcal{P}}(G_1(\mathfrak{P})) = 1$. We may now assume that $q > 2$.

First, we note that it is a fact from elementary number theory that any integer has a unique representation as given in (6.40)—for instance see [53, Theorem 1.5, p. 8], known as the *Base Representation Theorem.* To establish (6.39), we first consider the case $m = 1$. Let $\lambda_p = 1 - \zeta_p$ and set $\chi = \chi_{\mathfrak{P}}^{(q-1)}$. Then

$$G_1(\mathfrak{P}) = \sum_{j=0}^{q-1} \chi^{-1}(j)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(j)} = \sum_{j=0}^{q-1} \chi^{-1}(j)(1-\lambda_p)^{T_{\mathbb{F}_q/\mathbb{F}_p}(j)}.$$

We may let $n_j \in \mathbb{N}$ such that

$$n_j \equiv T_{\mathbb{F}_q/\mathbb{F}_p}(\psi(\zeta_{q-1}^j)) \pmod p,$$

where ψ is given in Definition 6.8 on page 295, so since

$$\chi^{-1}(\psi(\zeta_{q-1}^j)) = \left(\frac{\zeta_{q-1}^j}{\mathfrak{P}}\right)_{q-1}^{-1} = \zeta_{q-1}^{-j},$$

then

$$G_1(\mathfrak{P}) = \sum_{j=0}^{q-2} \zeta_{q-1}^{-j}(1-\lambda_p)^{T_{\mathbb{F}_q/\mathbb{F}_p}(j)}.$$

Furthermore, since the Binomial Theorem tells us that

$$(1-\lambda_p)^{n_j} \equiv 1 - n_j\lambda_p \pmod{\mathcal{P}^2}$$

via Example 5.8 on page 190, given that $q > 2$, and since

$$n_j \equiv T_{\mathbb{F}_q/\mathbb{F}_p}(\psi(\zeta_{q-1}^j)) = \sum_{k=0}^{f-1} \zeta_{q-1}^{jp^k} \pmod p,$$

by the definition of relative trace in finite fields—see Exercise 5.52 on page 260—then it follows that

$$G_1(\mathfrak{P}) \equiv \sum_{j=0}^{q-2} \zeta_{q-1}^{-j}\left(1 - \lambda_p \sum_{k=0}^{f-1} \zeta_{q-1}^{jp^k}\right) \equiv -\lambda_p \sum_{k=0}^{f-1}\sum_{j=0}^{q-2} \zeta_{q-1}^{j(p^k-1)} \equiv -\lambda_p(q-1) \pmod{\mathcal{P}^2},$$

where the last two congruences follow from Exercise 6.28 on page 310, since

$$\sum_{j=0}^{q-2} \zeta_{q-1}^{j(p^k-1)} = \begin{cases} 0 & \text{for } k = 1, 2, \ldots, f-1, \\ q-1 & \text{if } k = 0. \end{cases}$$

Thus, since $q = p^f \equiv 0 \pmod{\mathcal{P}^2}$, then

$$G_1(\mathfrak{P}) \equiv \lambda_p \pmod{\mathcal{P}^2}.$$

Since $\lambda_p \in \mathcal{P} - \mathcal{P}^2$ by part (b) of Proposition 6.9 on page 297, then $\operatorname{ord}_{\mathcal{P}}(G_1(\mathfrak{P})) = 1$, which completes the proof for $m = 1$.

Claim 6.15 If $1 \le m, n, m+n < q-1$, then

$$\operatorname{ord}_{\mathcal{P}}(G_{m+n}(\mathfrak{P})) \le \operatorname{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) + \operatorname{ord}_{\mathcal{P}}(G_n(\mathfrak{P})).$$

By part (a) of Lemma 6.2 on page 264,

$$G_m(\mathfrak{P})G_n(\mathfrak{P}) = J_q(\chi^{-m}, \chi^{-n})G_{m+n}(\mathfrak{P}). \tag{6.41}$$

Thus, by part (b) of Proposition 6.8 on page 296

$$\operatorname{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) + \operatorname{ord}_{\mathcal{P}}(G_n(\mathfrak{P}))$$

$$= \operatorname{ord}_{\mathcal{P}}(J_q(\chi^{-m}, \chi^{-n})) + \operatorname{ord}_{\mathcal{P}}(G_{m+n}(\mathfrak{P})) \ge \operatorname{ord}_{\mathcal{P}}((G_{m+n}(\mathfrak{P})),$$

and Claim 6.15 follows.

Claim 6.16 $\mathrm{ord}_{\mathcal{P}}(G_{m+n}(\mathfrak{P})) \equiv \mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) + \mathrm{ord}_{\mathcal{P}}(G_n(\mathfrak{P})) \pmod{p-1}$.

By Corollary 5.13 on page 218,

$$\mathfrak{P}\mathfrak{O}_K = \mathcal{P}^{p-1},$$

and by Exercise 5.27 on page 231,

$$J_q(\chi^{-m}, \chi^{-n}) \in L,$$

so

$$(p-1) \bigm| \mathrm{ord}_{\mathcal{P}}(J_q(\chi^{-m}, \chi^{-n})),$$

from which we get Claim 6.16, via (6.41).

Claim 6.17 For $m \in \mathbb{N}$, $\mathrm{ord}_{\mathcal{P}}(G_{pm}(\mathfrak{P})) = \mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P}))$.

Since

$$G_{pm}(\mathfrak{P}) = \sum_{j=0}^{q-1} \chi(j)^{-pm} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(j)} = \sum_{j=0}^{q-1} \chi(j^p)^{-m} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(j^p)} = G_m(\mathfrak{P}),$$

since $j \mapsto j^p$ is an automorphism of $\mathbb{F}_q$, and $T_{\mathbb{F}_q/\mathbb{F}_p}(j) = T_{\mathbb{F}_q/\mathbb{F}_p}(j^p)$. Claim 6.17 follows.

Claim 6.18 If $1 \le m < q$, then

$$\mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) \le \sum_{j=0}^{f-1} a_j^{(m)}.$$

By Claims 6.15, 6.16 and the already proved fact that $\mathrm{ord}_{\mathcal{P}}(G_1(\mathfrak{P})) = 1$, we get

$$\mathrm{ord}_{\mathcal{P}}(G_a(\mathfrak{P})) = a$$

for $1 \le a < p$. Thus, using Claims 6.15 and 6.17,

$$\mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) \le \sum_{j=0}^{f-1} \mathrm{ord}_{\mathcal{P}}(G_{a_j^{(m)}p^j}(\mathfrak{P})) = \sum_{j=0}^{f-1} \mathrm{ord}_{\mathcal{P}}(G_{a_j^{(m)}}(\mathfrak{P})) = \sum_{j=0}^{f-1} a_j^{(m)},$$

which is Claim 6.18.

Claim 6.19 $\sum_{m=1}^{q-2} \mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) = \frac{f(p-1)(q-2)}{2}$.

By Exercise 5.54 on page 260,

$$G_m(\mathfrak{P})G_{q-1-m}(\mathfrak{P}) = \chi(-1)^m q = \chi(-1)^m p^f, \tag{6.42}$$

since

$$G_{q-1-m}(\mathfrak{P}) = G((\chi_{\mathfrak{P}}^{(q-1)})^m). \tag{6.43}$$

By taking $\mathrm{ord}_{\mathcal{P}}$ of both sides of (6.42), and using part (c) of Proposition 6.9 on page 297, we get,

$$\mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) + \mathrm{ord}_{\mathcal{P}}(G_{q-1-m}(\mathfrak{P})) = f(p-1).$$

Thus,

$$\sum_{m=1}^{q-2} \mathrm{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) + \sum_{m=1}^{q-2} \mathrm{ord}_{\mathcal{P}}(G_{q-1-m}(\mathfrak{P})) = f(p-1)(q-2).$$

However, by (6.43),

$$\sum_{m=1}^{q-2} \operatorname{ord}_{\mathcal{P}}(G_m(\mathfrak{P})) = \sum_{m=1}^{q-2} \operatorname{ord}_{\mathcal{P}}(G_{q-1-m}(\mathfrak{P})),$$

so Claim 6.19 follows.

Claim 6.20 $\sum_{m=1}^{q-2}\sum_{j=0}^{f-1} a_j^{(m)} = \frac{f(p-1)(q-2)}{2}$.

Since $q-1=\sum_{j=0}^{f-1}(p-1)p^j$ by Theorem B.4 on page 347, then by (6.40) on page 298,

$$q-1-m = \sum_{j=0}^{f-1}\left(p-1-a_j^{(m)}\right)p^j.$$

This shows that $a_j^{(q-1-m)} = p-1-a_j^{(m)}$ for $j=0,1,\ldots,f-1$. Therefore,

$$\sum_{j=0}^{f-1} a_j^{(m)} + \sum_{j=0}^{f-1} a_j^{(q-1-m)} = f(p-1).$$

Thus,

$$\sum_{m=1}^{q-2}\left(\sum_{j=0}^{f-1} a_j^{(m)} + \sum_{j=0}^{f-1} a_j^{(q-1-m)}\right) = f(p-1)(q-2).$$

However, an easy check shows that

$$\sum_{m=1}^{q-2}\sum_{j=0}^{f-1} a_j^{(m)} = \sum_{m=1}^{q-2}\sum_{j=0}^{f-1} a_j^{(q-1-m)},$$

so Claim 6.20 is established.

The main result now follows from Claims 6.18–6.20. □

Corollary 6.3 $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{G}(\mathfrak{p})) = \frac{n}{p-1}\sum_{j=0}^{f-1} a_j^{((q-1)/n)}$.

Proof. By part (c) of Proposition 6.9,

$$(p-1)\operatorname{ord}_{\mathfrak{p}}(\mathfrak{G}(\mathfrak{p})) = \operatorname{ord}_{\mathcal{P}}(\mathfrak{G}(\mathfrak{p})), \tag{6.44}$$

but by Theorem 6.11, and the fact, from Remark 6.7 on page 298, that $G_{(q-1)/n}(\mathfrak{P}) = G(\mathfrak{p})$,

$$n\sum_{j=0}^{f-1} a_j^{((q-1)/n)} = n\cdot \operatorname{ord}_{\mathcal{P}}(G_{(q-1)/n}(\mathfrak{P})) = \operatorname{ord}_{\mathcal{P}}(G_{(q-1)/n}(\mathfrak{P})^n) = \operatorname{ord}_{\mathcal{P}}(\mathfrak{G}(\mathfrak{p})),$$

so from (6.44) we get the result. □

We are now in a position to state and prove the following, first proved by Stickelberger in 1890. The special case where n is a prime and $p\equiv 1 \pmod{n}$ was first proved by Kummer in 1847.

Theorem 6.12 — The Stickelberger Relation
Suppose that $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$, $n > 1$, and $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal with $n \notin \mathfrak{p}$. Then in $\mathfrak{O}_F$ we have the ideal decomposition,

$$(\mathfrak{G}(\mathfrak{p})) = \mathfrak{p}^{\sum_t t\sigma_t^{-1}},$$

where the sum runs over all natural numbers $t < n$ with $\gcd(t, n) = 1$, and $\sigma_t \in G = \mathrm{Gal}(F/\mathbb{Q})$ is given by $\sigma_t : \zeta_n \mapsto \zeta_n^t$.

Proof. By part (b) of Proposition 6.7 on page 296,

$$|\mathfrak{G}(\mathfrak{p})|^2 = q = p^f,$$

so the only prime $\mathfrak{O}_F$-ideals dividing $\mathfrak{G}(\mathfrak{p})$ are those dividing p. Let $\mathfrak{p}_1$ be a prime $\mathfrak{O}_F$-ideal above p. Then, by Corollary 5.1 on page 190, there exists a

$$\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

such that

$$\mathfrak{p}_1^{\sigma_t} = \mathfrak{p}.$$

Thus, for natural numbers $t < n$, relatively prime to n, we define

$$\mathfrak{p}_t = \mathfrak{p}^{\sigma_t^{-1}}. \tag{6.45}$$

Claim 6.21 $\mathrm{ord}_{\mathfrak{p}_t}(\mathfrak{G}(\mathfrak{p})) = \frac{n}{p-1} \sum_{j=0}^{f-1} a_j^{(t(q-1)/n)}$.

From (6.45), we have,

$$\mathrm{ord}_{\mathfrak{p}_t}(\mathfrak{G}(\mathfrak{p})) = \mathrm{ord}_{\mathfrak{p}^{\sigma_t^{-1}}}(\mathfrak{G}(\mathfrak{p})) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{G}(\mathfrak{p})^{\sigma_t}). \tag{6.46}$$

Let $z \in \mathbb{Z}$ such that $z \equiv t \pmod n$ and $z \equiv 1 \pmod p$. Then

$$G(\mathfrak{p})^{\sigma_z} = \left(\sum_{x=0}^{q-1} \chi_{\mathfrak{p}}^{(n)}(x) \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} \right)^{\sigma_z} = \sum_{x=0}^{q-1} \chi_{\mathfrak{p}}^{(n)}(x)^t \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)},$$

since $\zeta_p^{\sigma_z} = \zeta_p$ by the choice of z. Therefore,

$$\mathfrak{G}(\mathfrak{p})^{\sigma_t} = \left(\sum_{x=0}^{q-1} \left(\chi_{\mathfrak{p}}^{(n)}(x)\right)^t \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} \right)^n = \left(G_{t(q-1)/n}(\mathfrak{P})\right)^n,$$

where the last equality follows from the fact that

$$\left(\chi_{\mathfrak{p}}^{(n)}\right)^t = \left(\chi_{\mathfrak{P}}^{(q-1)}\right)^{-t(q-1)/n},$$

via Definition 6.10 on page 298. Thus, by Theorem 6.11,

$$n \sum_{j=0}^{f-1} a_j^{(t(q-1)/n)} = n \cdot \mathrm{ord}_{\mathcal{P}}(G_{t(q-1)/n}(\mathfrak{P})) = \mathrm{ord}_{\mathcal{P}}(G_{t(q-1)/n}(\mathfrak{P})^n) =$$

$$= \mathrm{ord}_{\mathcal{P}}(\mathfrak{G}(\mathfrak{p})^{\sigma_t}) = (p-1)\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{G}(\mathfrak{p})^{\sigma_t}) = (p-1)\,\mathrm{ord}_{\mathfrak{p}_t}(\mathfrak{G}(\mathfrak{p})),$$

where the penultimate equality follows from part (c) of Proposition 6.9 on page 297, and the last equality comes from (6.46). We have established Claim 6.21.

Given $t \in \mathbb{N}$, $t < n$ and $\gcd(t, n) = 1$, we let t_i be defined by

$$t \equiv t_i p^j \pmod{n},$$

for some unique pair (i, j) with $0 \leq j < f$ and $1 \leq i \leq g$, where g is the number of cosets of $\mathfrak{U}_{\mathbb{Z}/n\mathbb{Z}}/\langle\psi(p)\rangle$. Thus, $t_1, t_2, \ldots, t_g$ are the rational integer representatives of those cosets. Claim 6.21 tells us that

$$(\mathfrak{G}(\mathfrak{p})) = \mathfrak{p}^r,$$

where

$$r = \frac{n}{p-1} \sum_{i=1}^{g} \left(\sum_{j=0}^{f-1} a_j^{(t_i(q-1)/n)} \right) \sigma_{t_i}^{-1}.$$

Claim 6.22 If $\{x\} = x - \lfloor x \rfloor$, called the *fractional part* of the real number x, and $\lfloor x \rfloor$ is the floor function, then

$$r = n \sum_{i=1}^{g} \left(\sum_{j=0}^{f-1} \left\{ \frac{p^j t_i}{n} \right\} \right) \sigma_{t_i}^{-1}.$$

For simplicity set

$$m = \sum_{j=0}^{f-1} a_j^{(s)},$$

with $s = (t_i(q-1)/n)$.

For $i \geq 0$, we let $\overline{f - i + j}$ denote the residue class modulo f of the integer $f - i + j$. Then

$$p^i m \equiv \sum_{j=0}^{f-1} p^j a_{\overline{(f-i+j)}}^{(s)} \pmod{q-1}.$$

Since

$$\sum_{j=0}^{f-1} p^j a_{\overline{(f-i+j)}}^{(s)} < q - 1$$

for all such i, then

$$\left\{ \frac{p^i m}{q-1} \right\} = \frac{1}{q-1} \sum_{j=0}^{f-1} p^j a_{\overline{(f-i+j)}}^{(s)},$$

for all such i. It follows that

$$\sum_{i=0}^{f-1} \left\{ \frac{p^i m}{q-1} \right\} = \frac{1}{q-1} \left(\sum_{i=0}^{f-1} p^i \right) \left(\sum_{j=0}^{f-1} a_j^{(s)} \right)$$

and by Theorem B.4 on page 347, this equals

$$\frac{1}{q-1} \left(\frac{1-p^f}{1-p} \right) \sum_{j=0}^{f-1} a_j^{(s)} = \frac{1}{p-1} \sum_{j=0}^{f-1} a_j^{(s)},$$

which yields Claim 6.22.
However, $\mathfrak{p}^{\sigma_p} = \mathfrak{p}$, by Corollary 5.13 on page 218. In other words,

$$\langle \sigma_p \rangle = \mathcal{D}_p(F/\mathbb{Q})$$

—see Application 5.3 on page 231. Therefore, r may be replaced by

$$n \sum_{i=1}^{g} \left(\sum_{j=0}^{f-1} \left\{ \frac{p^j t_i}{n} \right\} \right) \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} = n \sum_{t=1}^{n-1} \left\{ \frac{t}{n} \right\} \sigma_t^{-1} = \sum_t t \sigma_t^{-1}, \tag{6.47}$$

where the last sum runs over all natural numbers $t < n$ and relatively prime to n, and the last equality follows from the fact that

$$n \left\{ \frac{t}{n} \right\} \equiv t \pmod{n}.$$

We have shown that

$$(\mathfrak{G}(\mathfrak{p})) = \mathfrak{p}^{\sum_t t \sigma_t^{-1}},$$

where the sum runs over all natural numbers $t < n$ relatively prime to n, which is the Stickelberger Relation. □

The proof of the Stickelberger Relation provides us with a distinguished element that we will be able to use in §6.4.

Definition 6.11 — The Stickelberger Element and Ideal
With notation as in Theorem 6.12,

$$\theta = \sum_t \left\{ \frac{t}{m} \right\} \sigma_t^{-1}$$

is called the *Stickelberger Element.* The *Stickelberger Ideal* is

$$I(F) = \mathbb{Z}[G] \cap \theta \mathbb{Z}[G],$$

which are the $\mathbb{Z}[G]$-multiples of θ that have coefficients in $\mathbb{Z}$.

Remark 6.8 In view of Definition 6.11, Equation (6.47) in the proof of the Stickelberger Relation tells us that

$$(\mathfrak{G}(\mathfrak{p})) = \mathfrak{p}^{n\theta}.$$

Also observe that

$$\theta \in \mathbb{Q}[G],$$

where

$$G = \mathrm{Gal}(F/\mathbb{Q}).$$

See Exercise 5.48 on page 253 for the general definition of a group ring.

The following three examples illustrate Theorem 6.12 for small values of n.

Example 6.6 If $n = 2$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, and $\mathfrak{p} = (p)$ where $p > 2$ is a rational prime such that

$$G(\mathfrak{p})^2 = (-1)^{(p-1)/2}p.$$

This is the trivial case with

$$G = \mathrm{Gal}(F/\mathbb{Q}) = 1.$$

The Stickelberger Relation does not precisely say this, but we know that this holds by Exercise 5.34 on page 232.

Example 6.7 Suppose that $n = 3$, $f = 1$, and $p \equiv 1 \pmod 3$. Then $\mathfrak{p} = (\pi)$, where π is a primary element of $\mathfrak{O}_F$. Thus, by Claim 6.1 on page 265 and Exercise 6.8 on page 276,

$$G(\mathfrak{p})^3 = p\overline{\pi} = \pi\overline{\pi}^2 = \pi^{1+2\sigma_p},$$

where

$$\langle \sigma_p \rangle = \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}).$$

Example 6.8 Let $n = 4$, $f = 1$, and $p \equiv 1 \pmod 4$. Then $\mathfrak{p} = (\pi)$, where π is a primary element of $\mathfrak{O}_F = \mathbb{Z}[i]$. By Exercise 6.21 on page 292,

$$G^4(\mathfrak{p}) = p\overline{\pi}^2 = \pi\overline{\pi}^3 = \pi^{1+3\sigma_p},$$

where

$$\langle \sigma_p \rangle = \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}).$$

The following application of the Stickelberger Relation appears as Theorem 145 in Hilbert's *Zahlbericht*, and was known to Kummer. The following is also a motivator for another result of Stickelberger, which we will establish at the conclusion of this section.

Theorem 6.13 — Stickelberger and Class Groups of Quadratic Fields
Let $F = \mathbb{Q}(\sqrt{-\ell})$ where $\ell \equiv 3 \pmod 4$ is prime and $\ell > 3$. Then

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{(N-R)/\ell} = 1,$$

where

$$N = \sum_n n$$

is the sum over all natural numbers $n < \ell$ such that $(\frac{-\ell}{n}) = -1$, and

$$R = \sum_r r$$

is the sum over all natural numbers $r < \ell$ such that $(\frac{-\ell}{r}) = 1$, where $(\frac{*}{*})$ is the Kronecker symbol.

Proof. Let $K = \mathbb{Q}(\zeta_\ell)$. Since inert primes are always principal and since the ramified prime $\mathfrak{q}$ in F is principal since $\mathfrak{q} = (\sqrt{-\ell})$, then it suffices to look at primes $p = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$ is a prime $\mathfrak{O}_F$-ideal with $\mathfrak{p} \neq \mathfrak{p}'$. Thus, by Theorem 1.17, it suffices to prove that $(N - R)/\ell$ *annihilates*[6.17] the class $\langle \mathfrak{p} \rangle$, where

$$(N - R)/\ell \in \mathbb{Z}$$

[6.17] This means that the exponent sends the class group to the trivial group.

by Exercise 6.31 on page 310. Let Z denote the decomposition subfield of p in $K/\mathbb{Q}$, and let $\mathcal{P}$ be a prime $\mathfrak{O}_K$-prime over $\mathfrak{p}$. From the proof of the Stickelberger Relation, we know that $\mathfrak{G}(\mathcal{P})$ is a power of $G(\mathcal{P})$ and so all conjugates of $\mathfrak{G}(\mathcal{P})$ are in Z. Therefore, the ideal generated by $\mathfrak{G}(\mathcal{P})$ is in Z, but this does not necessarily mean that $\mathfrak{G}(\mathcal{P}) \in Z$. We must prove this. Set

$$\chi = \chi_{\mathcal{P}}^{(\ell)}, \text{ and } q = p^f \text{ where } f = f_{K/\mathbb{Q}}(p).$$

If we let $\hat{\sigma}_p$ be an element of $\operatorname{Gal}(\mathbb{Q}(\zeta_{p\ell})/\mathbb{Q})$ such that $\hat{\sigma}_p|_K = \sigma_p$, then

$$G(\mathcal{P})^{\hat{\sigma}_p} = G(\chi)^{\hat{\sigma}_p} = \sum_{x\in\mathbb{F}_q} \chi(x)^{\sigma_p} \left(\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)}\right)^{\hat{\sigma}_p} = \sum_{x\in\mathbb{F}_q} \chi(x^{\sigma_p}) \left(\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x^{\sigma_p})}\right)^{\hat{\sigma}_p}. \tag{6.48}$$

Since

$$\chi(x) = \left(\frac{x^{\sigma_p}}{\mathcal{P}}\right)_\ell^{-1} = \chi(x^{\sigma_p}),$$

given that $\sigma_p \in \mathcal{D}_{\mathcal{P}}(K/\mathbb{Q})$, and

$$T_{\mathbb{F}_q/\mathbb{F}_p}(x) = T_{\mathbb{F}_q/\mathbb{F}_p}(x^{\sigma_p}),[6.18]$$

then (6.48) becomes

$$G(\mathcal{P})^{\hat{\sigma}_p} = \sum_{x\in\mathbb{F}_q} \chi(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(xa(p))}, \tag{6.49}$$

since x^{σ_p} ranges over $\mathbb{F}_q$ as x does, and $a(p)$ is defined by

$$\zeta_p^{\sigma_p} = \zeta_p^{a(p)}$$

for some $a(p) \in (\mathbb{Z}/p\mathbb{Z})^*$. In turn, (6.49) is equal to

$$\sum_{x\in\mathbb{F}_q} \chi^{-1}(a(p))\chi(x)^{\sigma_p}\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} = \chi^{-1}(a(p))G(\chi).$$

We have shown that

$$G(\mathcal{P})^{\hat{\sigma}_p} = \chi^{-1}(a(p))G(\chi).$$

Therefore, since $G(\mathcal{P})^\ell = \mathfrak{G}(\mathcal{P}) \in K$, then

$$\mathfrak{G}(\mathcal{P})^{\sigma_p} = \left(G(\mathcal{P})^\ell\right)^{\sigma_p} = (\chi^{-1}(a(p))^\ell G^\ell(\mathcal{P}) = G^\ell(\mathcal{P}) = \mathfrak{G}(\mathcal{P}).$$

Hence, $\mathfrak{G}(\mathcal{P}) \in Z$.

For convenience sake, we may now let $\mathcal{P}$ denote both the prime $\mathfrak{O}_K$-ideal above $\mathfrak{p}$ and the prime $\mathfrak{O}_Z$-ideal above $\mathfrak{p}$, since there is no splitting between Z and K. Diagram 6.2 below illustrates the scenario in the balance of the proof. By the Stickelberger Relation,

$$\left(G(\mathcal{P})^\ell\right) = (\mathfrak{G}(\mathcal{P})) = \mathcal{P}^{\sum_{t=1}^{\ell-1} t\sigma_t^{-1}}.$$

Thus, by taking norms, we get

$$(\beta) = \left(N_{Z/F}\left(\mathfrak{G}(\mathcal{P})\right)\right) = \left(N_{Z/F}\left(\mathcal{P}\right)\right)^{\sum_{t=1}^{\ell-1} t\sigma_t^{-1}}$$

[6.18] Recall from Exercise 2.16 on page 64 and Definition 5.1 on page 182 that σ_p may be regarded as an element of $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ via the natural map $\operatorname{Gal}(K/\mathbb{Q}) \mapsto \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ since $\mathbb{F}_q = \mathfrak{O}_K/\mathcal{P}$ and $\mathbb{F}_p = \mathfrak{O}_Z/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$, where $\mathfrak{P} = \mathcal{P} \cap Z$.

$$= \mathfrak{p}^{\sum_{t=1}^{\ell-1} t\sigma_t^{-1}} = \mathfrak{p}^{\sum_r r}\mathfrak{p}'^{\sum_n n} = \mathfrak{p}^R\mathfrak{p}'^N = \mathfrak{p}^{R-N},$$

since $\mathfrak{p}^{\sigma_n} = \mathfrak{p}'$ for each n such that $(\frac{-\ell}{n}) = -1$.[6.19] Now let $\gamma = \sqrt[\ell]{\beta}$. Then we have the ideal equation in $M = F(\zeta_p)$ given by,

$$(\gamma) = \left(N_{L/M}\left(G(\mathcal{P})\right)\right) = \mathfrak{p}^{(R-N)/\ell},$$

where $L = Z(\zeta_p)$.

Diagram 6.2

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_{p\ell}) \arrow[dl, dash] \arrow[dr, dash] & \\
 & L = Z(\zeta_p) \arrow[dl, dash] \arrow[dr, dash] & & K = \mathbb{Q}(\zeta_\ell) \arrow[dl, dash] \\
M = F(\zeta_p) \arrow[dr, dash] & & Z = Z_p(K/\mathbb{Q}) \arrow[dl, dash] & \\
 & F = \mathbb{Q}(\sqrt{-\ell}) & &
\end{tikzcd}$$

It remains to show that $\gamma \in F$. Let $R = F(\sqrt[\ell]{\beta})$. Since M/F is totally ramified at p and $R \subseteq M$, then it suffices to show that R/F is unramified, since then $R = F$. Given that we chose p to be unramified in K, then $K(\sqrt[\ell]{\beta})/K$ is totally ramified at p by Theorem 5.1 on page 184. However, since (β) is the ℓ^{th} power of an ideal in K, then $K(\sqrt[\ell]{\beta})/K$ can only ramify at prime $\mathfrak{O}_K$-ideals over ℓ by Theorem 5.19 on page 235. This forces $K(\sqrt[\ell]{\beta}) = K$ so $R = F$. Observe that $\mathfrak{p}^{(R-N)/\ell} \sim 1$ implies that

$$\mathfrak{p}^{(N-R)/\ell} \sim 1,$$

so the result is secured.[6.20] □

Example 6.9 Let $\ell = 23$ and $F = \mathbb{Q}(\sqrt{-23})$. Then

$$N = 5 + 7 + 10 + 11 + 14 + 15 + 17 + 19 + 20 + 21 + 22 = 161,$$

and

$$R = 1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 13 + 16 + 18 = 92,$$

so

$$\frac{N-R}{\ell} = 3.$$

In fact, $h_F = 3$.

Remark 6.9 Dirichlet actually proved that, for $\ell \equiv 3 \pmod 4$ a prime, $\ell \neq 3$,

$$h_{\mathbb{Q}(\sqrt{-\ell})} = \frac{1}{\ell}(N-R), \tag{6.50}$$

the proof of which involves analytic number theory. Furthermore, we will see as a special case of Exercise 6.31 on page 310 that $(N-R)/\ell$ is indeed an integer, but the proof that

$$(N-R)/\ell \in \mathbb{N}$$

also involves analytic number theory. Moreover, there is a link between the class numbers of $\mathbb{Q}(\sqrt{\ell})$ and $\mathbb{Q}(\sqrt{-\ell})$ and continued fraction expansions of $\sqrt{\ell}$ see [30] and [73], as well as [49, pp. 158–162] for related results.

[6.19] It is instructive to compare this with Applications 5.1–5.3 on pages 229–231.

[6.20] Jacobi discovered that $4p^{(N-R)/\ell} = x^2 + \ell y^2$, for some $x, y \in \mathbb{Z}$. On the basis of this result, he conjectured that $h_F = (N-R)/\ell$.

Example 6.10 One can use (6.50) on page 307 to find class number one complex quadratic fields by setting $\ell = N - R$, from which one calculates that for

$$\Delta_F = -\ell \in \{-7, -11, -19, -43, -67, -163\}$$

we have $h_F = 1$.

Remark 6.10 Theorem 6.13 on page 305 says that the class group of $F = \mathbb{Q}(\sqrt{-\ell})$, for $\ell \equiv 3 \pmod 4$ a prime, is annihilated by

$$-\frac{1}{\ell}\sum_{x=1}^{\ell-1} x\left(\frac{x}{\ell}\right) = \frac{1}{\ell}\left(\sum_n n - \sum_r r\right) = \frac{1}{\ell}(N-R),$$

where the residue symbol is the Lengendre symbol. In other words,

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{-\frac{1}{\ell}\sum_{x=1}^{\ell-1} x\left(\frac{x}{\ell}\right)} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{(N-R)/\ell} = 1.$$

There is a more general result about annihilation of class groups as follows.

Theorem 6.14 — Stickelberger on Annihilation of Class Groups
Let $F = \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$, and let θ be the Stickelberger element. If $\alpha \in \mathbb{Z}[G]$, where $G = \mathrm{Gal}(F/\mathbb{Q})$, such that $\alpha\theta \in \mathbb{Z}[G]$, then $\alpha\theta$ annihilates $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$.

Proof. Let p be a rational prime, with $\mathfrak{p}$ a prime $\mathfrak{O}_F$-ideal above $p \nmid n$. Then by the Stickelberger Relation,

$$(G(\mathfrak{p})^n) = (\mathfrak{G}(\mathfrak{p})) = \mathfrak{p}^{n\theta}.$$

Thus, if $\alpha \in \mathbb{Z}[G]$ such that $\alpha\theta \in \mathbb{Z}[G]$, then

$$\left(\mathfrak{p}^{\theta\alpha}\right)^n = \left(\mathfrak{p}^{n\theta}\right)^\alpha = (G(\mathfrak{p})^n)^\alpha = (G(\mathfrak{p})^\alpha)^n.$$

Let $\gamma = G(\mathfrak{p})^{n\alpha}$, and set $L = F(\sqrt[n]{\gamma})$, so L is a Kummer extension. Since

$$\alpha\theta \in \mathbb{Z}[G] \cong \mathfrak{O}_F$$

by Exercise 5.48 on page 253, then $(G(\mathfrak{p})^\alpha) = \mathfrak{p}^{\theta\alpha}$ is an $\mathfrak{O}_F$-ideal, so (γ) is the n^{th} power of an $\mathfrak{O}_F$-ideal. We now show that $G(\mathfrak{p})^\alpha \in F$. It follows from Theorem 5.19 on page 235 (by looking at successive prime degree, q, extensions of F in L for $q \mid n$), that L/F is unramified for any prime $\mathfrak{O}_F$-ideal above rational primes *not* dividing n. Since

$$F \subseteq L \subseteq \mathbb{Q}(\zeta_{np}),$$

by part (a) of Proposition 6.7 on page 296, then L/F must be ramified at primes above p by Theorem 5.4 on page 189. However, by Corollary 5.13 on page 218, the only ramified primes in L/F are those above $p \nmid n$, a contradiction unless $L = F$. Hence,

$$G(\mathfrak{p})^\alpha \in F.$$

We have shown that $\mathfrak{p}^{\theta\alpha}$ is a principal ideal *in* $\mathfrak{O}_F$. By Theorem 1.17 on page 28, we have shown that every ideal prime to (n) is principal in $\mathfrak{O}_F$. However, by Exercise 1.38 on page 33, every class of $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ contains an ideal prime to (n), so the proof is complete. □

In Theorem 6.13 on page 305, we were not dealing with a cyclotomic extension. However, there is a consequence of Theorem 6.14 that does deal with the more general case. In the following, we use the Kronecker-Weber Theorem presented on page 244. In particular, the reader is reminded that the *conductor* of an abelian extension K of $\mathbb{Q}$ is the smallest natural number n such that $K \subseteq \mathbb{Q}(\zeta_n)$.

Corollary 6.4 Suppose that $K/\mathbb{Q}$ is an abelian extension with conductor n, and $G = \mathrm{Gal}(K/\mathbb{Q})$. If θ is the Stickelberger Element and $\alpha \in \mathbb{Z}[G]$ such that $\alpha\theta \in \mathbb{Z}[G]$, then $\mathbf{C}_{\mathfrak{O}_\mathbf{K}}^{\alpha\theta} = 1$, where the σ_t in Theorem 6.12 on page 302 denote both the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \mathrm{Gal}(F/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$, namely we understand σ_t to mean $\sigma_t|_K$ when considering $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Let $p \nmid n$ be a rational prime, and let $\mathcal{P}$ be a prime $\mathfrak{O}_F$-ideal over p with $\mathcal{P} \cap \mathfrak{O}_K = \mathfrak{p}$. Let $\alpha \in \mathbb{Z}[G]$ such that $\alpha\theta \in \mathbb{Z}[G]$. Extend the elements of G so that $\alpha\theta$ may be regarded as an element of $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})]$. From Theorem 6.14, we have $(\mathfrak{p}\mathfrak{O}_K)^{\alpha\theta} = (G(\mathcal{P})^\alpha)$. Let $\sigma \in \mathrm{Gal}(F/K)$, which permute the prime $\mathfrak{O}_F$-ideals over $\mathfrak{p}$ by Corollary 5.1 on page 190. Let $\tau \in \mathrm{Gal}(F(\zeta_p)/\mathbb{Q}(\zeta_p))$ such that $\tau|_F = \sigma$, so $\zeta_p^\tau = \zeta_p$ (recalling that $p \nmid n$), and $\mathfrak{p}^\tau = \mathfrak{p}$. Then $G(\mathcal{P})^\tau = G(\mathcal{P}^\sigma)$, by Definition 6.9 on page 295. Hence, $G(\mathcal{P})^{\alpha\sigma} = G(\mathcal{P})^\alpha$, so $G(\mathcal{P})^\alpha \in K$. We have shown that $\mathfrak{p}^{\alpha\theta} = (G(\mathcal{P})^\alpha)$, so as in the proof of Theorem 6.14, $\mathbf{C}_{\mathfrak{O}_\mathbf{K}}$ is annihilated by $\alpha\theta$. □

The following illustrates the power of Theorem 6.14 by completely generalizing Theorem 6.13 with ease. The proof of the following is due to Lemmermeyer [38].

Corollary 6.5 Let$\Delta_F < 0$ be the discriminant of a complex quadratic field with$\Delta_F \notin \{-3, -4, -8\}$. Then

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{(N-R)/|\Delta_F|} = 1,$$

where N is the sum of all natural numbers $n < |\Delta_F|$ such that $(\frac{\Delta_F}{n}) = -1$, and R is the sum over all natural numbers $r < |\Delta_F|$ such that $(\frac{\Delta_F}{r}) = 1$, where $(\frac{*}{*})$ is the Kronecker symbol.

Proof. In this case, the Stickelberger Element is

$$\theta = \frac{R + \sigma N}{|\Delta_F|},$$

where

$$\langle\sigma\rangle = \mathrm{Gal}(F/\mathbb{Q}) = G.$$

Also, by Exercise 6.31 on the following page, $\theta \in \mathbb{Z}[G]$. Thus, by Theorem 6.14,

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{\theta} = 1,$$

but $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{1+\sigma} = 1$, so

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{|R-N|/|\Delta_F|} = 1 = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{(N-R)/|\Delta_F|},$$

as required. □

Example 6.11 Let$\Delta_F = -52$. Then

$$N = 3 + 5 + 21 + 23 + 27 + 33 + 35 + 37 + 41 + 43 + 45 + 51 = 364,$$

and

$$R = 1 + 7 + 9 + 11 + 15 + 17 + 19 + 25 + 29 + 31 + 47 + 49 = 260$$

so

$$\mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{(N-R)/|\Delta_F|} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}^{2} = 1.$$

In fact, $h_F = 2$ for $F = \mathbb{Q}(\sqrt{-13})$.

Theorem 6.14 was proved for $K = \mathbb{Q}(\zeta_p)$, where p is a prime, by Kummer in 1847. It was proved in general by Stickelberger in 1879.

Remark 6.11 For the reader interested in exploring the consequences of this theory at a higher level, we give the following data. Analogues of Theorem 6.14 for totally real fields have been found by B. Oriat [57] and A. Wiles [70]. There is also the important work of Thaine [68], where cyclotomic units are used to define an analogue of the Stickelberger element for real abelian fields. This allowed him to prove a result on the annihilation of class groups of real abelian number fields. Subsequently Kolyvagin invented tools for constructing relations in ideal class groups, extending Thaine's methods. These methods have had deep and far-reaching consequences. Among them is the use of these tools to give an elementary proof of the Main Conjecture of Iwasawa theory—see [69] for details on the results surrounding Kolyvagin's work.

Exercises

6.28. Let $n \in \mathbb{N}$, $n > 1$, and ζ_n a primitive n^{th} root of unity in a field F. Prove that $\sum_{j=0}^{n-1} \zeta_n^j = 0$ in F.

6.29. Let $\mathbb{F}_q$ where $q = p^r$ and p is prime. A Gauss or Jacobi sum over $\mathbb{F}_q$ is called *pure* if, when raised to a natural number exponent, it becomes real. Prove that quadratic Gauss sums are pure, but Gauss sums belonging to characters of order $k > 2$ are never pure when $q = p$.

This result was first proved by Stickelberger in 1890. Pure Gauss sums are a useful tool in many areas including the determination of when -1 *is the power of a given prime modulo a natural number. For instance, see* [3].

(*Hint: Use Exercise 5.34 on page 232, Exercise 5.52 on page 260 part (a) of Proposition 6.7 on page 296, and part* (a) *of Proposition 6.7 on page 296.*)

6.30. Let $\ell \geq 3$ be a prime with $\ell \equiv 3 \,(\text{mod } 4)$, $F = \mathbb{Q}(\sqrt{-\ell})$ and $\mathfrak{p}$ a prime $\mathfrak{O}_F$-ideal above the rational prime $p \equiv 1 \,(\text{mod } \ell)$. Suppose further that $p = \mathfrak{p}\mathfrak{p}'$ in $\mathfrak{O}_F$, and $K = \mathbb{Q}(\zeta_\ell)$, with $\mathcal{P}$ is a prime $\mathfrak{O}_K$-ideal over $\mathfrak{p}$. Prove that $\mathfrak{p}\mathfrak{O}_K = \prod_r \mathcal{P}^{\sigma_r}$, where the product runs over all natural numbers $r < \ell$ that are squares modulo ℓ, and $\sigma_r(\zeta_\ell) = \zeta_\ell^r$.

(*Hint: Use Application 5.2 on page 230.*)

6.31. With N, R and $\ell > 3$ given in Corollary 6.5, prove that

$$N \equiv R \equiv 0 \pmod{|\Delta_F|}.$$

6.4 The Eisenstein Reciprocity Law

> *The end crowns the work.*
>
> **Early sixteenth century proverb**

The object of this section is to establish the Eisenstein Reciprocity Law—see Theorem 6.15 on page 313 and Biography 3.10 on page 137. First, we need to extend the definition of $\mathfrak{G}(\mathfrak{p})$, given in (6.38) on page 295, from prime ideals to arbitrary ideals as follows.

Definition 6.12 — Power Residue Gauss Sums Extended

Let $F = \mathbb{Q}(\zeta_n)$ and I be an $\mathfrak{O}_F$-ideal with $I = \prod_{j=1}^{r} \mathfrak{p}_j$, a product of not necessarily distinct prime $\mathfrak{O}_F$-ideals. Then

$$\mathfrak{G}(I) = \prod_{j=1}^{r} \mathfrak{G}(\mathfrak{p}_j).$$

A sequence of lemmas is required to prepare for the proof of the Eisenstein Reciprocity law.

Lemma 6.6 — More Properties of Power Residue Gauss Sums

Suppose that $F = \mathbb{Q}(\zeta_n)$, I, J are $\mathfrak{O}_F$-ideals, and $\alpha \in \mathfrak{O}_F$ with $\gcd(IJ, n) = 1 = \gcd(\alpha, n)$. Also let $\tau = \sum_t t\sigma_t^{-1}$, where the sum runs over all natural numbers $t < n$ with $\gcd(t, n) = 1$. Then each of the following holds.

(a) $\mathfrak{G}(I)\mathfrak{G}(J) = \mathfrak{G}(IJ)$.

(b) $|\mathfrak{G}(I)|^2 = (N(I))^n$.

(c) $(\mathfrak{G}(I)) = (I^\tau)$.

Proof. Part (a) is immediate from Definition 6.12. By part (a), it suffices to prove parts (b)–(c) for $I = \mathfrak{p}$, a prime $\mathfrak{O}_F$-ideal. By part (b) of Proposition 6.7 on page 296,

$$|\mathfrak{G}(\mathfrak{p})|^2 = p^n = (N(\mathfrak{p}))^n,$$

which yields part (b). Part (c) is Theorem 6.12 on page 302. □

We now need to explore the action of τ, defined in Lemma 6.6, on power residue Gauss sums over principal ideals.

Lemma 6.7 — Galois Action on Power Residue Gauss Sums

Let $F = \mathbb{Q}(\zeta_n)$, $n \in \mathbb{N}$, I an $\mathfrak{O}_F$-ideal such that $\gcd(n, I) = 1$, $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, and $\tau = \sum_t t\sigma_t^{-1}$, where the sum runs over all natural numbers $t < n$ with $\gcd(t, n) = 1$. Then

(a) $\mathfrak{G}(I)^\sigma = \mathfrak{G}(I^\sigma)$.

(b) If $\alpha \in \mathfrak{O}_F$, then $|\alpha^\tau|^2 = |N_F(\alpha)|^n$.

(c) If $\alpha \in \mathfrak{O}_F$ such that $\gcd(\alpha, n) = 1$, then $\mathfrak{G}((\alpha)) = \pm\zeta_n^j \alpha^\tau$ for some $j \in \mathbb{Z}$.

Proof. By part (a) of Lemma 6.6 on the preceding page we may let $I = \mathfrak{p}$ be a prime $\mathfrak{O}_F$-ideal. If $\alpha \in \mathfrak{O}_F$, then

$$G(\mathfrak{p}) = \sum_{x=0}^{q-1} \left(\frac{\alpha}{\mathfrak{p}}\right)^{-1} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} = \sum \chi_{\mathfrak{p}}^{(n)}(\psi(\alpha))\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\psi(\alpha))},$$

where the sum runs over all coset representatives $\psi(\alpha) \in \mathfrak{O}_F/\mathfrak{p} = \mathbb{F}_q$ (with ψ being given as in Definition 6.8 on page 295). Let

$$\hat{\sigma} \in \mathcal{D}_p(\mathbb{Q}(\zeta_{pn})/\mathbb{Q}),$$

where $\hat{\sigma}|_F = \sigma$. Then by Proposition 6.6 on page 295,

$$G(\mathfrak{p})^{\hat{\sigma}} = \sum \chi_{\mathfrak{p}}^{(n)}(\psi(\alpha^\sigma))\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\psi(\alpha^\sigma))} = G(\mathfrak{p}^\sigma).$$

Thus, by raising each side to the n^{th} power we get $\mathfrak{G}(\mathfrak{p})^\sigma = \mathfrak{G}(\mathfrak{p}^\sigma)$, from which part (a) follows.

For part (b), let σ_{-1} be complex conjugation, namely $\sigma_{-1} : \zeta_n \mapsto \zeta_n^{-1}$. Therefore,

$$|\alpha^\tau|^2 = \alpha^\tau \alpha^{\tau\sigma_{-1}} = \alpha^{\tau(1+\sigma_{-1})}. \tag{6.51}$$

Since

$$\sigma_{-1}\tau = \sigma_{-1}\sum_t t\sigma_t^{-1} = \sum_t t\sigma_t^{-1} = \sum_t (n-t)\sigma_{n-t}^{-1},$$

then

$$(1+\sigma_{-1})\tau = \sum_t t\sigma_t^{-1} + \sum_t (n-t)\sigma_{n-t}^{-1} = n\sum_t \sigma_{n-t}^{-1} = n\sum_t \sigma_t^{-1}.$$

However,

$$N_F(\alpha) = \prod_t \alpha^{\sigma_t^{-1}} = \alpha^{\sum_t \sigma_t^{-1}}.$$

Therefore, from (6.51),

$$|N_F(\alpha)|^n = |\alpha|^{n\sum_t \sigma_t^{-1}} = |\alpha|^{\tau(1+\sigma_{-1})} = |\alpha^\tau|^2,$$

which secures (b).

Since

$$(\mathfrak{G}((\alpha))) = (\alpha)^\tau = (\alpha^\tau),$$

by part (c) of Lemma 6.6, then as ideal generators, $\mathfrak{G}(\mathfrak{p})$ and α^τ differ by a unit. In other words,

$$\mathfrak{G}((\alpha)) = u\alpha^\tau,$$

for some $u \in \mathfrak{U}_{\mathfrak{O}_F}$. Since

$$|\mathfrak{G}((\alpha))|^2 = (N_F(\alpha))^n$$

by part (b) of Lemma 6.6, and

$$|\alpha^\tau|^2 = |N_F(\alpha)|^n$$

by part (b) of this proposition, then

$$N((\alpha)) = |N_F(\alpha)|,$$

by Corollary 2.8 on page 85. Hence,

$$|u| = \frac{|\mathfrak{G}((\alpha))|}{|\alpha^\tau|} = 1.$$

Similarly, it may be shown that $|u^\sigma| = 1$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Therefore, by Corollary 3.10 on page 128, $\alpha \in \mathcal{R}_F$. In other words, $u = \pm\zeta_n^j$ for some $j \in \mathbb{Z}$. □

We need one more notion in order to state the Eisenstein Reciprocity Law.

Definition 6.13 — Primary Cyclotomic Integers
Let $r > 2$ be a prime, $F = \mathbb{Q}(\zeta_r)$, and $\alpha \in \mathfrak{O}_F$. Then α is called primary if $\gcd(\alpha, r) = 1$ and

$$\alpha \equiv z \pmod{(1-\zeta_r)^2}$$

for some $z \in \mathbb{Z}$.

Remark 6.12 We do not need the notion of *semi-primary* here, which is what Hilbert called these α. He needed a stronger notion of primary in order to prove Kummer's Reciprocity Law (see [38]). Hilbert called an element α primary if it is semi-primary, or what we have defined here as primary, together with the additional property that $\alpha\overline{\alpha}$ is congruent to a rational integer modulo $(1-\zeta_r)^{r-1}$.

Theorem 6.15 Eisenstein's Reciprocity Law
Let r be an odd prime, $F = \mathbb{Q}(\zeta_r)$, $a \in \mathbb{Z}$ and $\alpha \in \mathfrak{O}_F$ be a primary element such that $\gcd(r, a) = 1 = \gcd(\alpha, a)$. Then

$$\left(\frac{\alpha}{a}\right)_r = \left(\frac{a}{\alpha}\right)_r.$$

Proof. By Proposition 6.5 on page 295, it suffices to prove this result for $a = p_1$ a prime. Let $\mathfrak{p}_1$ be a prime $\mathfrak{O}_F$-ideal above p_1 with $N(\mathfrak{p}_1) = p_1^{f_1} = q_1$. Then by hypothesis, $\gcd(\mathfrak{p}_1, r) = 1$.

Claim 6.23 $\left(\frac{\mathfrak{G}((\alpha))}{\mathfrak{p}_1}\right)_r = \left(\frac{N(\mathfrak{p}_1)}{\alpha}\right)_r$.

By part (a) of Lemma 6.6, it suffices to prove the claim for $(\alpha) = \mathfrak{p}$, a prime $\mathfrak{O}_F$-ideal with $N(\mathfrak{p}) = p^f = q$. Thus, in $\mathfrak{O}_F$ we have the following congruences:

$$G(\mathfrak{p})^{q_1} \equiv \sum_{x=0}^{q-1} \left(\chi_{\mathfrak{p}}^{(r)}(x)\right)^{q_1} \left(\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)}\right)^{q_1} \equiv \sum_{x=0}^{q-1} \chi_{\mathfrak{p}}^{(r)}(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(q_1 x)} \pmod{p_1},$$

since $q_1 \equiv 1 \pmod{r}$ by Corollary 5.13 on page 218. Therefore, the above is in turn congruent to

$$\sum_{x=0}^{q-1} \chi_{\mathfrak{p}}^{(r)}(q_1^{-1}x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} \equiv \left(\frac{q_1}{\mathfrak{p}}\right)_r \sum_{x=0}^{q-1} \chi_{\mathfrak{p}}^{(r)}(x)\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(x)} \equiv \left(\frac{q_1}{\mathfrak{p}}\right)_r G(\mathfrak{p}) \pmod{p_1}.$$

Also, in $\mathfrak{O}_F$, we have the following congruence:

$$G(\mathfrak{p})^{q_1-1} = \mathfrak{G}(\mathfrak{p})^{(q_1-1)/r} \equiv \left(\frac{\mathfrak{G}(\mathfrak{p})}{\mathfrak{p}_1}\right)_r \pmod{\mathfrak{p}_1}.$$

Hence,

$$\left(\frac{\mathfrak{G}(\mathfrak{p})}{\mathfrak{p}_1}\right)_r \equiv \left(\frac{q_1}{\mathfrak{p}}\right)_r = \left(\frac{N(\mathfrak{p}_1)}{\mathfrak{p}}\right)_r \pmod{\mathfrak{p}_1}.$$

Since $r \notin \mathfrak{p}_1$, then we must in fact have equality in the last congruence, which establishes Claim 6.23.

Claim 6.24 Let $\mathfrak{G}(\alpha) = \pm\zeta_r^j \alpha^\tau$, where τ is given in Lemma 6.7 on page 311. Then

$$\left(\frac{\pm\zeta_r^j}{\mathfrak{p}_1}\right)_r \left(\frac{\alpha}{N(\mathfrak{p}_1)}\right)_r = \left(\frac{N(\mathfrak{p}_1)}{\alpha}\right)_r .$$

By Claim 6.23 and part (c) of Lemma 6.7,

$$\left(\frac{N(\mathfrak{p}_1)}{\alpha}\right)_r = \left(\frac{\mathfrak{G}((\alpha))}{\mathfrak{p}_1}\right)_r = \left(\frac{\pm\zeta_r^j}{\mathfrak{p}_1}\right)_r \left(\frac{\alpha^\tau}{\mathfrak{p}_1}\right)_r , \tag{6.52}$$

and since

$$\left(\frac{\alpha^{t\sigma_t^{-1}}}{\mathfrak{p}_1}\right)_r = \left(\frac{\alpha^{\sigma_t^{-1}}}{\mathfrak{p}_1}\right)_r^t = \left(\frac{\alpha^{\sigma_t^{-1}}}{\mathfrak{p}_1}\right)_r^{\sigma_t} = \left(\frac{\alpha}{\mathfrak{p}_1^{\sigma_t}}\right)_r ,$$

by Proposition 6.6 on page 295, then

$$\left(\frac{\alpha^\tau}{\mathfrak{p}_1}\right)_r = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{\mathfrak{p}_1}\right)_r = \prod_t \left(\frac{\alpha}{\mathfrak{p}_1^{\sigma_t}}\right)_r = \left(\frac{\alpha}{N(\mathfrak{p}_1)}\right)_r ,$$

where the last equality comes from Theorem 5.5 on page 190. From (6.52), Claim 6.24 now follows.

Claim 6.25 $\left(\frac{\alpha}{N(\mathfrak{p}_1)}\right)_r = \left(\frac{N(\mathfrak{p}_1)}{\alpha}\right)_r .$

By Claim 6.24 we need only show that $\left(\frac{\pm\zeta_r^j}{\mathfrak{p}_1}\right)_r = 1$. However, α is primary, so by Exercise 6.33 on page 317, $\pm\zeta_r^j = \pm 1$. Thus,

$$\left(\frac{\pm\zeta_r^j}{\mathfrak{p}_1}\right)_r = \left(\frac{\pm 1}{\mathfrak{p}_1}\right)_r = (\pm 1)^{(N(\mathfrak{p}_1)-1)/r} = 1,$$

since r is odd and $N(\mathfrak{p}_1) - 1 = p_1^{f_1} - 1$ is even. This completes the proof of Claim 6.25.

By Proposition 6.5 on page 295, Claim 6.25 says that

$$\left(\frac{\alpha}{p_1}\right)_r^f = \left(\frac{\alpha}{p_1^f}\right)_r = \left(\frac{\alpha}{N(\mathfrak{p}_1)}\right)_r = \left(\frac{N(\mathfrak{p}_1)}{\alpha}\right)_r = \left(\frac{p_1}{\alpha}\right)_r^{f_1} .$$

However, since $p_1^{f_1} \equiv 1 \pmod r$, then $f_1 \mid (r-1)$, so $\gcd(f_1, r) = 1$. Therefore,

$$\left(\frac{\alpha}{p_1}\right)_r = \left(\frac{p_1}{\alpha}\right)_r ,$$

which completes the proof of the Eisenstein Reciprocity Law. □

One of the more pleasing applications of the Eisenstein Reciprocity Law is the following result proved in 1912. This was an important development in the long search for a proof of FLT. From this result will follow another important such result proved by Wieferich.

Theorem 6.16 — Furtwängler's Theorem

Let $x, y, z \in \mathbb{Z}$ be pairwise relatively prime, and let $p > 2$ be a prime such that

$$x^p + y^p + z^p = 0. \tag{6.53}$$

If $p \nmid yz$ and q is a prime divisor of y, then

$$q^{p-1} \equiv 1 \pmod{p^2}.$$

Proof. We remind the reader that, as we saw in the proof of Theorem 4.4 on page 152, $(x + \zeta_p^j y)$ is a p^{th} power in $\mathfrak{O}_F$ for any $j \geq 0$, where $F = \mathbb{Q}(\zeta_p)$. Let

$$u = (x+y)^{p-2}y,\ \alpha = (x+y)^{p-2}(x+\zeta_p y), \text{ and } \lambda = 1-\zeta_p.$$

Then since $x+\zeta_p y = x+y-y\lambda$, and by Exercise 4.19 on page 162, $(x+y)^{p-1} \equiv 1 \pmod{\lambda^2}$,

$$\zeta_p^{-u}\alpha = (1-\lambda)^{-u}\alpha \equiv (1-\lambda)^{-u}((x+y)^{p-1} - y\lambda(x+y)^{p-2}) \equiv (1+u\lambda)(1-u\lambda) \equiv 1 \pmod{\lambda^2}.$$

This shows that $\zeta_p^{-u}\alpha$ is primary. Thus, by the Eisenstein Reciprocity Law,

$$\left(\frac{q}{\zeta_p^{-u}\alpha}\right)_p = \left(\frac{\zeta_p^{-u}\alpha}{q}\right)_p = \left(\frac{\zeta_p}{q}\right)_p^{-u}\left(\frac{\alpha}{q}\right)_p.$$

Since $(\zeta_p^{-u}\alpha) = (\alpha)$ is a p^{th} power, then

$$1 = \left(\frac{q}{\zeta_p^{-u}\alpha}\right)_p = \left(\frac{\zeta_p}{q}\right)_p^{-u}\left(\frac{\alpha}{q}\right)_p. \tag{6.54}$$

However, $q \mid y$ and $\alpha \equiv (x+y)^{p-1} \pmod{q}$, so

$$\left(\frac{\alpha}{q}\right)_p = \left(\frac{(x+y)^{p-1}}{q}\right)_p = \left(\frac{q}{(x+y)^{p-1}}\right)_p = 1,$$

since $(x+y)$ is a p^{th} power. Thus, by (6.54),

$$\left(\frac{\zeta_p}{q}\right)_p^{u} = 1. \tag{6.55}$$

Claim 6.26 If $g = g_{F/\mathbb{Q}}(q)$ and $f = f_{F/\mathbb{Q}}(q)$, then

$$\left(\frac{\zeta_p}{q}\right)_p = \zeta_p^{g(q^f-1)/p}.$$

Let $q\mathfrak{O}_F = \prod_{j=1}^{g} \mathfrak{q}_j$. Then

$$\left(\frac{\zeta_p}{q}\right)_p = \prod_{j=1}^{g}\left(\frac{\zeta_p}{\mathfrak{q}_j}\right)_p = \prod_{j=1}^{g}\zeta_p^{(q^f-1)/p} = \zeta_p^{\sum_{j=1}^{g}(q^f-1)/p} = \zeta_p^{g(q^f-1)/p},$$

by Definition 6.7 on page 294. Therefore, by (6.55),

$$ug\frac{q^f-1}{p} \equiv 0 \pmod{p}. \tag{6.56}$$

Since $g \mid (p-1)$ by Theorem 5.4, then $p \nmid g$ and since $u = (x+y)^{p-2}y$, then $p \nmid u$. Therefore, by (6.56), $(q^f-1)/p \equiv 0 \pmod{p}$. In other words,

$$q^f \equiv 1 \pmod{p^2}.$$

Since $f \mid (p-1)$, then we have Furtwängler's result. □

A simple consequence of Theorem 6.16 is the following, proved in 1909.

Corollary 6.6 — Wieferich's Theorem
If $x^p + y^p + z^p = 0$ has a solution for nonzero $x, y, z \in \mathbb{Z}$ with $p \nmid xyz$, then

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{6.57}$$

Proof. Clearly one of x, y, z is even, so we may assume without loss of generality that $2 \mid y$. By Furtwängler's Theorem with $q = 2$, the result follows. □

Remark 6.13 Primes p satisfying (6.57) are called *Wieferich primes.* The first two such primes are $p = 1093$ and $p = 3511$. More generally, if we replace 2 with any $b \in \mathbb{N}$ with $b > 2$ and require that they satisfy (6.57), then these are also treated as Wieferich primes. It is unknown if there are infinitely many such primes for a given base b. It is not even known if there are infinitely many such that (6.57) fails to hold for a given base b. Examples of bases $b > 2$ for which (6.57) holds are $(b, p) = (5, 53471161), (7, 491531), (11, 71)$.

There have been many generalizations of the Eisenstein Reciprocity Law given by Artin, Hasse, Hilbert, and Takagi (see [38] for an overview). Some are beyond the scope of the theory presented in this book. For instance, for a statement of a general reciprocity law using local class field theory see [15, pp. 167–168]. For the Artin Reciprocity Law given in terms of idèles (introduced by Chevalley in order to give an approach different from the classical one that allows global class field theory to be deduced from the local one), see Tate's article in [10, Chapter VII, pp. 162–203]. One may also consult Hasse's article in [10, Chapter XI, pp. 266–279]. In fact, we conclude this section with the statement of a general reciprocity law that is within the purview of the theory provided herein.

Theorem 6.17 — The Artin–Hasse Reciprocity Law
Let $F = \mathbb{Q}(\zeta_r)$ where $r > 2$ is prime and $\alpha,\beta \in \mathfrak{O}_F$ such that $\gcd(\alpha,\beta) = 1$, $\alpha \equiv 1 \pmod{r}$, and $\beta \equiv 1 \pmod{\lambda}$, where $\lambda = 1 - \zeta_r$. Then

$$\left(\frac{\alpha}{\beta}\right)_r \left(\frac{\beta}{\alpha}\right)_r^{-1} = \zeta_r^{T_{F/\mathbb{Q}}\left(\frac{\alpha-1}{r}\cdot\frac{\beta-1}{\lambda}\right)}.$$

Proof. See [38]. □

To illustrate the power of Theorem 6.17, we show how to easily achieve the Eisenstein Reciprocity Law from it, as a closing feature of this last section of the main text. The proof in the following was communicated to this author by Franz Lemmermeyer in the writing of the first edition.

Example 6.12 Since

$$\left(\frac{a}{\alpha}\right)_r = \left(\left(\frac{a}{\alpha}\right)_r^{-1}\right)_r^{-1} = \left(\frac{a^{r-1}}{\alpha}\right)^{r-1} = \left(\frac{a^{r-1}}{\alpha^{r-1}}\right)_r,$$

then it suffices to show that

$$\left(\frac{a^{r-1}}{\alpha^{r-1}}\right)_r = \left(\frac{\alpha^{r-1}}{a^{r-1}}\right)_r.$$

To this end, let $b = a^{r-1} \equiv 1 \pmod{r}$ and $\beta = \alpha^{r-1} \equiv 1 \pmod{\lambda}$. Thus, Theorem 6.17 applies since

$$T_{F/\mathbb{Q}}\left(\frac{b-1}{r}\cdot\frac{\beta-1}{\lambda}\right) = \frac{b-1}{r}T_{F/\mathbb{Q}}\left(\frac{\beta-1}{\lambda}\right) \equiv 0 \pmod{r},$$

given that $r \mid (\beta - 1)/\lambda$ when α is primary. Hence

$$\left(\frac{b}{\beta}\right)_r = \left(\frac{\beta}{b}\right)_r .$$

The Theorem 6.17 is one of the simpler formulations found by Artin and Hasse in a search, between 1923 and 1926, for what Hilbert called "The most general reciprocity law." The quest continues into the realm of *non-abelian* class field theory, spearheaded by the work of Langlands and Shimura, and carried on by numerous others.

Exercises

6.32. Let $r > 2$ be a prime, $F = \mathbb{Q}(\zeta_r)$, and I an $\mathfrak{O}_F$-ideal such that $\gcd(r, I) = 1$. Prove that

$$\mathfrak{G}(I) \equiv \pm 1 \pmod{r}.$$

6.33. Let $r > 2$ be prime, $F = \mathbb{Q}(\zeta_r)$, and $\alpha \in \mathfrak{O}_F$ a primary element. Prove that $\mathfrak{G}(\alpha) = \pm\alpha^\tau$, where τ is given in Lemma 6.7 on page 311.

✰ 6.34. Suppose that $a \in \mathbb{Z}$, and ℓ is a rational prime such that $\ell \nmid a$. Prove that

$$x^\ell \equiv a \pmod{p}$$

is solvable for all but finitely many primes p if and only if

$$a = b^\ell$$

for some $b \in \mathbb{Z}$.

In a course in elementary number theory, one quickly learns the fact that an integer a, which is a square modulo all primes ℓ, must be the square of a rational integer. This is usually given as an application of the Jacobi symbol. This exercise is intended to substantially generalize that fact as an application of the Eisenstein Reciprocity Law.

Biography 6.2 Phillipp Furtwängler (1869–1940) was born on April 21, 1869 near Hildesheim, Germany. By the age of fourteen, he had lost both of his parents. He went to school in Hildesheim, then went to Göttingen in 1889. At this time Hilbert had not yet arrived at Göttingen, but Fricke and Klein were there. Furtwängler completed his dissertation on ternary cubic forms in 1896. He then held numerous positions. The first was as an assistant at the Geodesic Institute in Potsdam from 1897 to 1903. In 1903, he married Ella Buchwald, but she died shortly after the birth of their daughter. Then he was at the Agricultural Academy in Bonn from 1903 to 1907, after which he taught at the Technical University in Aachen, then returned to Bonn. His activities during those years included a proof of the reciprocity law for prime powers, and establishment of the existence of Hilbert class fields. In 1912, he succeeded Mertens at the University of Vienna. While at Vienna, his research activities included the problem of capitulation in Hilbert class fields, and a proof of Hilbert's principal ideal theorem in 1930. He also worked in Diophantine approximation, the geometry of numbers, and FLT. In 1929, he married Emilie Schön at a time when he was already quite ill, and had to retire in 1938. He died on May 19, 1940 in Wien. There are streets in Germany named Furtwängler after Phillipp's distant relative, Wilhelm Furtwängler, the famous conductor and composer.

Appendix A

Abstract Algebra

It's hard to beat a person who never gives up.

Babe Ruth (George Herman Roth) (1895–1948)
American baseball player

The purpose of this appendix is to give a review of the background material required for understanding the concepts in the text as a finger-tip reference to the basic concepts in abstract algebra. We do this via a discussion of the fundamental concepts, without proofs, so the reader may be reminded of the salient background information without having to go to another source. However, if proofs are required, the reader may consult such standard texts as [29].

First, we will consider the following set of axioms, and discuss certain sets $\mathcal{S}$, together with binary operations of *addition*, denoted by $+$, and *multiplication*, denoted by juxtaposition or by $\cdot$ the multiplication sign. We will determine which sets satisfy certain of these axioms, and thereby introduce the various concepts in a basic course in abstract algebra

✦ Basic Axioms

A.1. For all $\alpha,\beta \in \mathcal{S}$, $\alpha + \beta \in \mathcal{S}$. (Additive closure)

A.2. For all $\alpha,\beta \in \mathcal{S}$, $\alpha\beta \in \mathcal{S}$. (Multiplicative closure)

A.3. For all $\alpha,\beta \in \mathcal{S}$, $\alpha + \beta = \beta + \alpha$. (Additive commutativity)

A.4. For all $\alpha,\beta,\gamma \in \mathcal{S}$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$. (Additive associativity)

A.5. There is a unique $z \in \mathcal{S}$ with $z + \alpha = \alpha + z = \alpha$. (Additive identity)

(When no confusion can arise, we use the symbol 0 here for the additive identity z, since it mimics the ordinary zero of the integers.)

A.6. To each $\alpha \in \mathcal{S}$, there is an $\alpha^* \in \mathcal{S}$ such that $\alpha + \alpha^* = \alpha^* + \alpha = z$. (Additive inverse)

A.7. For all $\alpha,\beta \in \mathcal{S}$, $\alpha\beta = \beta\alpha$. (Multiplicative commutativity)

A.8. For all $\alpha,\beta,\gamma \in \mathcal{S}$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. (Multiplicative associativity)

A.9. There exists a unique $1_{\mathcal{S}} \in \mathcal{S}$ such that for each $\alpha \in \mathcal{S}$, $1_{\mathcal{S}}\alpha = \alpha 1_{\mathcal{S}} = \alpha$. (Multiplicative identity)

(Here, as with the additive identity above, we can use the symbol 1 in place of the multiplicative identity $1_{\mathcal{S}}$, when no confusion will arise from so doing, since $1_{\mathcal{S}}$ mimics the function of this multiplicative identity of the integers.)

A.10. For all $\alpha,\beta,\gamma \in \mathcal{S}$, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. (Distributivity)

A.11. For all $\alpha,\beta \in \mathcal{S}$, if $\alpha\beta = z$, then $\alpha = z$ or $\beta = z$. (No zero divisors)

A.12. For any $\alpha \in \mathcal{S}$, with $\alpha \neq z$ there exists an element denoted by α^{-1} such that $\alpha\alpha^{-1} = 1_{\mathcal{S}} = \alpha^{-1}\alpha$. (Multiplicative inverse)

✦ Groups

An additive group is a set satisfying A.1 and A.4–A.6. Similarly, a multiplicative group is a set satisfying axioms A.2, A.8–A.9, and A.12.

In the text—see the proof of Theorem 2.10 on page 77, for instance—we will have need of a special multiplicative group as follows.

Definition A.1 — The Symmetric Group

The *symmetric group on n letters*, denoted by S_n, is the set of all bijections of $\{1, 2, \ldots, n\}$. Multiplication is given by composition of functions, which is associative. The identity map is the identity of S_n, and there are unique inverses since bijections are one-to-one and onto (see the section on *Mappings—Morphisms* starting on page 326). The elements of S_n are called *permutations*, and the cardinality of S_n is $n! = n(n-1)(n-2)\cdots 2\cdot 1$. A *transposition* is an element $\sigma \in S_n$ such that σ interchanges two elements of $\{1, 2, \ldots, n\}$, while leaving all of the others fixed.

A basic fact concerning permutation groups is that all permutations are expressible as a product of transpositions. This leads to a finer classification of the elements of S_n.

Definition A.2 — Even and Odd Permutations

If $\sigma \in S_n$ and σ is the product of an odd number of transpositions, then σ is called an odd permutation. If σ is the product of an even number of transpositions, then σ is called an *even permutation.* The set of all even permutations forms a subgroup of S_n, denoted by A_n, called the *alternating group on n symbols*, and $|A_n| = n!/2$. The *sign of a permutation* σ, denoted by $\text{sgn}(\sigma)$, is 1 or -1 according as σ is even or odd. The sgn is a well-defined map since it can be shown that a permutation cannot be both odd and even.

Definition A.3 — Abelian Groups

Any set which satisfies A.1, and A.3–A.6 is an *additive abelian group*, and if it satisfies A.2, A.7–A.9, and A.12, then it is a *multiplicative abelian group.* If G is a multiplicative abelian group, then G is *cyclic* whenever the group generated by some $g \in G$, coincides with G. The element g is the *generator* of G, denoted by

$$G = \langle g \rangle.$$

If $g^n = 1_G$ for some $n \in \mathbb{N}$, then the smallest such n is the *order* of the *finite cyclic group* G, denoted by $n = |G|$. If no such n exists, then G is said to be an *infinite cyclic group.* A group P is called an *elementary abelian* p-group for a prime $p \in \mathbb{Z}$ if every element $x \in P$ satisfies $x^p = 1$. If P is the maximum elementary abelian p-subgroup of a group G, and $|P| = p^r$, then r is called the *p-rank of* G. This means that

$$P \cong \underbrace{C_p \times \cdots \times C_p}_{r \quad factors},$$

where C_p is a cyclic group of order p, and G does not contain a subgroup of this type with more than r factors.[A.1]

[A.1] Note that this definition of rank is valid only for abelian groups. In general, one may define the rank as the number of factors of the maximal p-elementary abelian “factor” group. For instance, the quaternion group has 2-rank 2, and its maximal elementary abelian subgroup is $\mathbb{Z}/2\mathbb{Z}$.

The following basic result is useful in the main text—see the proof of Lemma 5.12 on page 244, for instance.

Remark A.1 In the following, a *direct product* of groups is formed by the component-wise multiplication of elements.

Theorem A.1 — Fundamental Theorem of Finite Abelian Groups

If G is a finite abelian group, then any two decompositions of G into a direct product of cyclic groups of prime power order contain the same number of multiplicands of each order.

✦ Cosets of Groups

Let G, H be arbitrary groups with $H \subseteq G$. Then H is a *subgroup of* G. Suppose that $g \in G$ is fixed, and set

$$gH = \{gh : h \in H\}.$$

Then gH is a *left coset of* H *in* G *determined by* g. A *right coset* is similarly defined. If G is abelian, then left and right cosets are equal, and we refer merely to a coset of H in G.

Let $g_1, g_2 \in G$ be fixed. Either

$$g_1 H \cap g_2 H = \varnothing$$

or

$$g_1 H = g_2 H.$$

Furthermore, the group G is partitioned into disjoint left cosets of H. The number of distinct left cosets of H in G is denoted $|G : H|$, called the *index of* H *in* G. (In particular, $|G|$ is the order of G.) Moreover, it is an easy task to verify the following fact.

Proposition A.1 — Group Criterion

If G is a group, then the nonempty set $H \subseteq G$ is a subgroup of G if and only if $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$.

Given the above discussion, we may conclude that G is partitioned into a disjoint union of $|G : H|$ subsets, each containing $|H|$ elements. Thus, by counting the number of elements in G, we get the following.

Theorem A.2 — Lagrange's Theorem

If G is a group and H is a subgroup of G, then

$$|G| = |G : H| \cdot |H|.$$

Corollary A.7 If G is a finite group and $|G| = n$, then $|g| \bigm| |G|$, and $g^n = 1$ for all $g \in G$.

Theorem A.3 A finite abelian group of order $n \in \mathbb{N}$ has subgroups of all orders dividing n.

Given the above setup, we may now define another group.

Definition A.4 — The Quotient Group and Normal Subgroups

Let G be an abelian group, and H a subgroup of it. The *quotient group*

$$\overline{G} = G/H = \{\overline{g_1}, \ldots, \overline{g_n}\} = \{g_1H, \ldots, g_nH\}$$

of G by H is the group with multiplication defined by

$$\overline{g_jg_k} = g_jg_kH = g_jHg_kH = g_\ell H = \overline{g_\ell},$$

for some $\ell = 1, 2, \ldots, n$, having identity $1_{\overline{G}} = H = \overline{1_G}$, and inverses $\overline{g_j}^{-1} = g_j^{-1}H$. The mapping

$$\psi : G \mapsto \overline{G}, \text{ given by } \psi : g \mapsto \overline{g}$$

is called the *canonical map*, or *natural map.*

If G is not an abelian group, then in order to form the quotient group one needs the following concept. A subgroup H of G is called *normal* provided that $gH = Hg$ for all $g \in G$. In other words, the left and right cosets of H in G agree, or that H is always conjugated to itself, namely $g^{-1}Hg = H$ for all $g \in G$. When H is normal in G, we may form the quotient group $\overline{G}$ as the set of all products of cosets. Since left and right cosets agree, then the product of any two cosets is again a coset of H in G, so $\overline{G}$ is a group with this multiplication.

✦ Rings and Fields

Definition A.5 — Rings, and Fields

(1) A *ring* is a set together with two binary operations called addition and multiplication, denoted by + and ×, satisfying the following:

   (a) R is an abelian group under addition.

   (b) Multiplication is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in \mathbb{R}$.

   (c) The distributive law holds in R, namely for all $a, b, c \in R$ multiplication is distributive over addition, namely

$$a \times (b + c) = (a \times b) + (a \times c)$$

   and

$$(a + b) \times c = (a \times c) + (b \times c).$$

(2) If (1) holds, and multiplication is commutative, then R is called a *commutative ring.*

(3) If (1) holds, and there is an element $1 \in R$ such that

$$1 \times a = a \times 1 = a \text{ for all } a \in R,$$

then R is called a *ring with identity.*

(4) A ring with identity $1 \neq 0$ is called a *division ring* or *skew field* if every nonzero element of R has a multiplicative inverse.

(5) A commutative division ring is called a *field.*

Definition A.6 — Subrings

A *subring* of a ring R is a subgroup of R that is closed under multiplication.

Remark A.2 Definition A.6 says that, in practice, to show that a *subset* of a ring R is a *subring* it suffices to show that it is *nonempty* and *closed under subtraction and multiplication.*

✦ Modules

Suppose that M is an additive abelian group, and that R is a ring, which satisfy each of the following axioms:

A.13. For each $r \in R$, $m \in M$, $rm \in M$.

A.14. For each $r \in R$ and $m, n \in M$, $r(m+n) = (rm) + (rn)$.

A.15. For each $r, s \in R$ and $m \in M$, $(r+s)m = (rm) + (sm)$.

A.16. For each $r, s \in R$ and $m \in M$, $r(sm) = (rs)m$.

A.17. If R has identity 1_R, then for each $m \in M$, $1_R m = m$.

Then M is a *left module* over R. If R is a commutative ring with identity, then M is both a right and a left R-module called a *two-sided, unitary module* or for our purposes, simply an *R-module.* For example, being a $\mathbb{Z}$-module is equivalent to being an additive abelian group. If R is a division ring, then M is called a *vector space*, and multiplication from R is called *scalar multiplication*, with the elements of M called *vectors.*[A.2]

A *submodule* of an R-module M is a subset N of M such that

A.18. N is a subgroup of the additive group of M, and

A.19. For all $r \in R$, and $n \in N$, $rn \in N$.

It follows that a subset N of M is an R-submodule of M if and only if

A.20. $0 \in N$,

A.21. For all $m, n \in N$, $m - n \in N$, and

A.22. For all $r \in R$, and $n \in N$, $rn \in N$.

For instance, if G is an additive abelian group, then for any $n \in \mathbb{Z}$,

$$ng = \pm(\underbrace{g + g + \cdots + g}_{|n| \text{ copies}}).$$

Therefore, abelian groups are $\mathbb{Z}$-modules and the submodules are just the subgroups thereof.

Let $m \in M$ be fixed, and let N be a submodule of M. Define

$$m + N = \{m + n : n \in N\},$$

the coset of N in M determined by m.

[A.2] There is a more general definition of vector space (and of a module), which we do not need in this text. For the more general setup, and details pertaining to it, the reader may consult [29, p. 169 ff].

A.23. For any $m_1, m_2 \in N$, $m_1 + N = m_2 + N$ if and only if $mm_1 + N = mm_2 + N$ for any $m \in M$.

A.24. Define

$$M/N = \{m + N : m \in M\}.$$

Then M/N is an R-module, called *the quotient module of* M by N. If M/N is finite, we denote its order by

$$|M/N| = |M : N|,$$

the *index of* N *in* M.

If $\mathcal{S} = \{M_j : j = 1, 2, \ldots, n\}$ is a set of R-modules, then let M be the set of n-tuples

$$(m_1, m_2, \ldots, m_n) \text{ with } m_j \in M_j \text{ for } j = 1, 2, \ldots n,$$

with the *zero element* of M being the n-tuple, $(0, 0, \ldots, 0)$. Define addition in M by

$$(m_1, m_2, \ldots, m_n) + (m'_1, m'_2, \ldots, m'_n) = (m_1 + m'_1, m_2 + m'_2, \ldots, m_n + m'_n),$$

for all $m_j, m'_j \in M_j$ with $j = 1, 2, \ldots, n$, and multiplication from R on an n-tuple from M by

$$r(m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n) \text{ for all } r \in R.$$

This defines an R-module structure on M called the *direct sum* of the modules M_j, $j = 1, 2, \ldots, n$, denoted by

$$\oplus_{j=1}^{n} M_j = M_1 \oplus \cdots \oplus M_n. \tag{A.1}$$

Definition A.7 — Bases, Dependence, and Finite Generation

If $\mathcal{S}$ is a subset of an R-module M, then the intersection of all submodules of M containing $\mathcal{S}$ is called the *submodule generated by* $\mathcal{S}$, or *spanned by* $\mathcal{S}$. If there is a finite set $\mathcal{S}$, and $\mathcal{S}$ generates M, then M is said to be *finitely generated.* If $\mathcal{S} = \varnothing$, then $\mathcal{S}$ generates the zero module. If $\mathcal{S} = \{m\}$, a singleton set, then the submodule generated by $\mathcal{S}$ is said to be the *cyclic submodule generated by* m.

A subset $\mathcal{S}$ of an R-module M is said to be *linearly independent* provided that for distinct $s_1, s_2, \ldots, s_n \in \mathcal{S}$, and $r_j \in R$ for $j = 1, 2, \ldots, n$,

$$\sum_{j=1}^{n} r_j s_j = 0 \text{ implies that } r_j = 0 \text{ for } j = 1, 2, \ldots, n.$$

If $\mathcal{S}$ is not linearly independent, then it is called *linearly dependent.* A linearly independent subset of an R-module that spans M is called a *basis* for M.

An important concept that we will need throughout the text is the following notion—see Theorem 2.9 on page 75, for instance.

Definition A.8 — Free Modules and Free Abelian Groups

If R is a commutative ring with identity, and M is an R-module, then M is called a *free R-module* if M has a nonempty basis.

Remark A.3 The situation of most interest to us in the text is that of a free $\mathbb{Z}$-module, which is just a $\mathbb{Z}$-module with a basis, and this is the same thing as a *free abelian group.* It can be shown that any two such bases for a free abelian group G have the same cardinality. Therefore, this cardinality is an invariant of G, called the *rank of* G. If the number of elements in a basis is finite then the free abelian group is said to be of *finite rank.* Furthermore, it can be shown that all subgroups of a free abelian group G are also free abelian with rank at most that of G.

Vector spaces (over division rings, remember) are special.

Theorem A.4 — Vector Spaces and Dimension

If V is a vector space, and $\mathcal{S}$ is a subset that spans V, then $\mathcal{S}$ contains a basis of V. Furthermore, any two bases of V have the same cardinality. This is called the *invariant dimension property.*

The cardinality of a basis for a vector space V over a division ring D is called *the dimension of* V *over* D, denoted by $|V : D|$. A submodule of a vector space is called a *subspace.*

Application A.1 — Field Extensions

If $D \subseteq V$, where D and V are fields in Theorem A.4, then V is called an *extension field* of D and $|V : D|$ is called the *degree* of the field extension. It follows that if $F_1 \subseteq F_2 \subseteq F_3 \subseteq \mathbb{C}$ with F_j fields for $j = 1, 2, 3$, then

$$|F_3 : F_1| = |F_3 : F_2| \cdot |F_2 : F_1|. \tag{A.2}$$

If $\mathcal{S}$ is a subset of a field F, then we call the *subfield generated by* $\mathcal{S}$ the intersection of all fields containing F and containing $\mathcal{S}$. If E is an extension field of F and $\mathcal{S} \subseteq E$, then the *subfield generated by* F *and* $\mathcal{S}$ is defined as the subfield generated by $F \cup \mathcal{S}$. If $\mathcal{S} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for some $n \in \mathbb{N}$, then the field generated by $\mathcal{S}$ and F is denoted by

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

called a *finitely generated extension of* F. In the case where $n = 1$, E is called a *simple extension of* F.

When $K, F \subseteq \mathbb{C}$ are fields, then the *compositum* of K and F, also called the *composite*, is the smallest subfield of $\mathbb{C}$ containing both K and F. This consists of all finite sums $\sum \alpha_j \beta_j$ where $\alpha_j \in K$ and $\beta_j \in F$. In particular, for the simple extensions defined above, we have that whenever $\alpha \in C$ is algebraic over F, then

$$F[\alpha] = F(\alpha) \cong F[x]/(f(x)), \tag{A.3}$$

where the generator of the ideal, given by $f(x)$, is an irreducible monic polynomial uniquely characterized by the conditions: (1) $f(\alpha) = 0$, and (2) if $g(x) \in F[x]$ with $g(\alpha) = 0$, then $f(x) \bigm| g(x)$. See Example 1.22 on page 19, for instance, as an application of this result.

In the above, we defined free R-modules. We may now present another characterization of those free R-modules of finite rank. An R-module M of rank $n \in \mathbb{N}$ is free provided that it is isomorphic to a direct sum of n copies of the R-module R. In particular, every free $\mathbb{Z}$-module M of rank n is of the form

$$M \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ copies}}, \tag{A.4}$$

and this is called a *free abelian group of rank n.* Thus, every subgroup of a free abelian group of rank n is a free abelian group of rank at most n.

✦ Mappings — Morphisms

Let S and T be sets. Then a function (or mapping)

$$f : S \mapsto T$$

is called an *injection* (or one-to-one) provided that

$$a = b \text{ whenever } f(a) = f(b) \text{ for any } a, b \in S.$$

It is called *surjective* (or onto) provided that $f(S) = T$, namely

$$T = \{f(s) : s \in S\},$$

or in other words, for each $t \in T$, there exists an $s \in S$ such that $f(s) = t$. A function f is called *bijective* (or a *bijection*) if it is both an injection and a surjection.

Suppose that G and H are two groups where $\cdot$ denotes the operation in G, and $\otimes$ denotes the operation in H. If

$$f : G \mapsto H$$

is a function such that

$$f(g_1 \cdot g_2) = f(g_1) \otimes f(g_2),$$

then f is called a *homomorphism of groups* (or group homomorphism). When there is no danger of confusion, we express $\otimes$ and $\cdot$ simply by juxtaposition, and write

$$f(g_1 g_2) = f(g_1)f(g_2),$$

for convenience. We will maintain this convention in the sequel, namely that we will not distinguish between the operations in the objects under consideration.

Definition A.9 — Auto, Endo, Iso, and Mono-Morphisms

If $f : G \mapsto H$ is injective as a map of sets, then f is called a *monomorphism of groups* (or *group monomorphism*), and f is called an *epimorphism of groups* (or *group epimorphism*) provided that f is surjective as a map of sets. If f is bijective as a map of sets, we call it an *isomorphism of groups* (or *group isomorphism*). When the context is clear, and no confusion can arise, we drop the reference to groups and call f simply a *monomorphism*, *epimorphism* or *isomorphism.* A homomorphism

$$f : G \mapsto G$$

is called an *endomorphism* of G, and if f is an isomorphism, then it is called an *automorphism* of G. A *field automorphism* is an isomorphism of F satisfying the *two* properties that $f(\alpha\beta) = f(\alpha)f(\beta)$ and $f(\alpha + \beta) = f(\alpha) + f(\beta)$ for all α,β $\in F$.

The *kernel* of $f : G \mapsto H$ is given by

$$\ker(f) = \{g \in G : f(g) = 0\}.$$

Also, the *image* of G under f is given by

$$\text{img}(f) = \{h \in H : f(g) = h \text{ for some } g \in G\}.$$

If S is a subset of H, then

$$f^{-1}(S) = \{g \in G : f(g) \in S\}$$

is called the *inverse image of S.*

Remark A.4 The set of all automorphisms of a group G forms a group itself under composition of functions, denoted by $\mathrm{Aut}(G)$—see Lemma 2.1 on page 55 for an application to field extensions. For instance, the group of automorphisms of a finite field $\mathbb{F}_{p^n}$ is a cyclic group of order n.

Definition A.10 — Homomorphism and Embeddings of Rings

Let R and S be rings. Then a function $f : R \mapsto S$ is a *homomorphism of rings* provided that for all $a, b \in R$

$$f(a+b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b).$$

The homomorphism f is called a *monomorphism of rings* (or *embedding of R into S*, or *an injection of rings*, or *a one-to-one homomorphism of rings*), if f is injective as a map of sets. Also, f is called an *epimorphism of rings* if f is surjective as a map of sets. If f is a bijection as a map of sets, then f is called an *isomorphism of rings.* When f is an isomorphism of rings, we say that R and S are isomorphic, and write

$$R \cong S.$$

As above, we abbreviate to say simply *homomorphism*, *monomorphism*, *epimorphism*, or *isomorphism*, when the context is clear. Also, the *kernel* and *image* inherit the group structure from a map of additive abelian groups. If ϕ is an isomorphism of the ring R, and S is a subring of R, then the isomorphism given by

$$s \mapsto \phi(s) \text{ for all } s \in S$$

is called the *restriction isomorphism* of ϕ to S, denoted by

$$\phi|_S. \tag{A.5}$$

Definition A.11 — Cosets and Quotient Rings

If R is a commutative ring with identity and I is an R-ideal, then a *coset* of I in R is a set, for a given $r \in R$, of the form $r + I = \{r + \alpha : \alpha \in I\}$. The set

$$R/I = \{r + I : r \in R\}$$

becomes a ring under addition and multiplication of cosets given by

$$(r+I)(s+I) = rs + I \text{ and } (r+I) + (s+I) = (r+s) + I \text{ for } r, s \in R$$

which is independent of the choices of r, s. Then R/I is called the *quotient ring* or the *factor ring* of R by I. It is also referenced as the *residue classes of R modulo I.*
A mapping

$$f : R \mapsto R/I,$$

which takes elements of R to their coset representatives in R/I, is called the *natural map* of R to R/I, and this is easily seen to be an epimorphism. In this case, the cardinality of R/I is denoted by $|R : I|$.

If M and N are modules over a ring R, then a function

$$f : M \mapsto N$$

is an *R-module homomorphism* provided that for all $m_1, m_2 \in M$ and $r \in R$

$$f(m_1 + m_2) = f(m_1) + f(m_2) \text{ and } f(rm_1) = rf(m_1).$$

If R is a division ring, then an R-module homorphism is called a *linear transformation.*

Since an R-module homomorphism is necessarily a homomorphism of additive abelian groups, then the same terminology is carried over to f as an *R-module monomorphism, epimorphism*, or *isomorphism*, provided that f is injective, surjective, or bijective (respectively), as a map of sets. Hence, the *kernel* (respectively image), of f is its kernel (respectively image), as a homomorphism of abelian groups.

If R is a commutative ring with identity, then an *R-algebra* is a ring A such that

A.25. A is an R-module, and

A.26. $r(ab) = (ra)b = a(rb)$ for all $r \in R$ and $a, b \in A$.

Any R-algebra that is (as a ring) a division ring, is called a *division algebra.* An algebra over a field K is called a *finite dimensional algebra* over K. A homomorphism (respectively momomorphism, epimorphism, or isomorphism), of R-algebras

$$f : A \mapsto B$$

is a ring homomorphism (respectively momomorphism, epimorphism, or isomorphism), that is also an R-module homomorphism, (respectively momomorphism, epimorphism, or isomorphism). Also, as in the ring case, the notion of *kernel* and *image* of f are inherited from the group structure.

Fundamental results concerning isomorphisms will be needed in the text. The following is a fundamental result on isomorphisms of which (A.3) on page 325 is an application.

Theorem A.5 — Fundamental Isomorphism Theorem for Rings[A.3]

If R and S are commutative rings with identity, and

$$\phi : R \mapsto S$$

is a homomorphism of rings, then

$$R/\ker(\phi) \cong \operatorname{img}(\phi).$$

✦ Rings of Quotients

In this section, we look at a generalization of the construction of the rational number field.

Definition A.12 — Multiplicative Sets

A nonempty subset S of a ring R is called *multiplicative* provided that

$$r, s \in S \text{ implies that } rs \in S.$$

The classical motivation for the following is to think of the set S of nonzero rational integers. This is a multiplicative subset of $\mathbb{Z}$. One may construct $\mathbb{Q}$ from the relation on the set $\mathbb{Z} \times S$ given by

$$(a, b) \sim (c, d) \text{ if and only if } ad - bc = 0,$$

[A.3] This holds for more general rings, but our principal object of study in this text is the ring of integers of a number field, so we look only at this case for convenience. See [29] for the more general case.

which is an equivalence relation (namely a binary relation R that is reflexive (aRa), symmetric (aRb implies bRa), and transitive (aRb and bRc imply aRc)).

Then $\mathbb{Q}$ is the set of equivalence classes, denoted by

$$\{(a,b)\} = a/b$$

with addition and multiplication defined in the usual way. These well-defined operations make $\mathbb{Q}$ into a field, and the mapping $z \mapsto z/1$ embeds $\mathbb{Z}$ in $\mathbb{Q}$. We now generalize this setup.

Theorem A.6 — Ring of Quotients[A.4]

Let S be a multiplicative subset of an integral domain R. Then the relation on $R \times S$ defined by

$$(a,b) \sim (c,d) \text{ if and only if } ad - bc = 0$$

is an equivalence relation. Denote the set of equivalence classes arising from this equivalence relation by $S^{-1}R$. If $0 \notin S$, then $S^{-1}R$ is an integral domain, called the *quotient ring of* R or *ring of fractions* or *ring of quotients* of R by S. If S is the set of all nonzero elements of R, then $S^{-1}R$ is a field called the *quotient field* of R. In the latter case, the map

$$\psi : R \mapsto S^{-1}R \text{ given by } r \mapsto rs/s \text{ for any } s \in S$$

is a monomorphism that embeds R in its quotient field. Thus, $\psi(s)$ is a unit in $S^{-1}R$ for each $s \in S$.

✦ Polynomials and Polynomial Rings

If R is a ring, then a polynomial $f(x)$ in an indeterminant x with coefficients in R is an infinite formal sum

$$f(x) = \sum_{j=0}^{\infty} a_j x^j = a_0 + a_1 x + \cdots + a_n x^n + \cdots ,$$

where the *coefficients* a_j are in R for $j \geq 0$ and $a_j = 0$ for all but a finite number of those values of j. If $a_n \neq 0$, and $a_j = 0$ for $j > n$, then a_n is called the *leading coefficient* of $f(x)$. If the leading coefficient $a_n = 1$, then $f(x)$ is said to be *monic*. The set of all such polynomials is denoted by $R[x]$.

We may add two polynomials from $R[x]$, $f(x) = \sum_{j=0}^{\infty} a_j x^j$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$, by

$$f(x) + g(x) = \sum_{j=0}^{\infty} (a_j + b_j) x^j \in R[x],$$

and multiply them by

$$f(x)g(x) = \sum_{j=0}^{\infty} c_j x^j,$$

where

$$c_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

[A.4] This setup applies to any commutative ring, but our main concern in this text is rings of integers, which are integral domains, so we specialize to that case here.

Also, $f(x) = g(x)$ if and only if $a_j = b_j$ for all $j = 0, 1, \ldots$. Under the above operations $R[x]$ is a ring, called the *polynomial ring over R in the indeterminant x*. Furthermore, if R is commutative, then so is $R[x]$, and if R has identity 1_R, then 1_R is the identity for $R[x]$. Notice that with these conventions, we may write $f(x) = \sum_{j=0}^{n} a_j x^j$ where a_n is the leading coefficient since we have tacitly agreed to "ignore" zero terms.

Note that we could dispense with the indeterminant altogether and write

$$f = (a_0, a_1, \ldots, a_n, \ldots).$$

Then the above operations would be on these sequences of elements. Note that $f(x)$ is not a function and the $+$ in its representation does not represent addition. This is made clear by the sequential notation. Thus, the abbreviated notation that we have adopted, $f(x) = \sum_{j=0}^{\infty} a_j x^j$, is called the *sigma notation*, rather than the summation notation.

If $\alpha \in R$, we write $f(\alpha)$ to represent the element $\sum_{j=0}^{n} a_j \alpha^j \in R$, called the *substitution* of α for x. When $f(\alpha) = 0$, then α is called a *root* of $f(x)$. The substitution gives rise to a mapping $\overline{f} : R \mapsto R$ given by $\overline{f} : \alpha \mapsto f(\alpha)$, which is determined by $f(x)$. Thus, $\overline{f}$ is called a *polynomial function* over R.

Example A.1 Let $R = \mathbb{Z}/p\mathbb{Z}$ where p is prime. If $f(x) = x^p$ and $g(x) = x$, then these two polynomials of $R[x]$ are distinct. However, $\overline{f}(\alpha) = \alpha^p$ and $\overline{g}(\alpha) = \alpha$. However, by Fermat's Little Theorem, $\alpha^p = \alpha$ in R. Hence, distinct polynomials can give rise to the same polynomial function. (For a detailed discussion of related polynomial congruences and the theory behind them, see [50, pp. 105–117]).

Definition A.13 — Degrees and Division of Polynomials

If $f(x) \in R[x]$, with $f(x) = \sum_{j=0}^{d} a_j x^j$, and $a_d \neq 0$, then d is called the *degree of $f(x)$ over R*, denoted by $\deg_R(f)$. If no such d exists, we write $\deg_R(f) = -\infty$, in which case $f(x)$ is the zero polynomial in $R[x]$—see Example A.2 on the next page. We say that a *polynomial $g(x) \in R[x]$ divides $f(x) \in R[x]$*, if there exists an $h(x) \in R[x]$ such that $f(x) = g(x)h(x)$. We also say that $g(x)$ is a *factor* of $f(x)$. If F is a field of characteristic zero, then

$$\deg_{\mathbb{Q}}(f) = \deg_F(f)$$

for any $f(x) \in \mathbb{Q}[x]$. In this case, we write $\deg(f)$ for $\deg_F(f)$, without loss of generality, and call this *the degree of $f(x)$*.

✦ Polynomial Congruences

Theorem A.7 — Lagrange's Theorem

Suppose that f is an integral polynomial of degree $d \geq 1$, and p is a rational prime. Then $f(x) \equiv 0 \pmod{p}$ has at most d incongruent solutions.

If c is the greatest common divisor of the coefficients of $f(x) \in \mathbb{Z}[x]$, then c is called the *content of f*. If $c = 1$, then f is called *primitive*.[A.5]

[A.5] The content of a polynomial f is also defined more generally when $f(x) \in D[x]$, where D is a UFD—see Definition 1.8 on page 7. The content is not uniquely defined since common divisors are not unique given the existence of units. However, any two contents are necessarily associates in D—see Definition 1.5 on page 4. In $\mathbb{Z}$, this does not present a problem since the only units are ± 1, so the gcd (which is positive), must be unique. If D is a general UFD, then a polynomial is primitive if the content is a unit in D.

Definition A.14 — Irreducible Polynomials over Rings

A polynomial $f(x) \in R[x]$ is called *irreducible* (over R), if $f(x)$ is not a unit in R and any factorization $f(x) = g(x)h(x)$, with $g(x), h(x) \in R[x]$ satisfies the property that one of $g(x)$ or $h(x)$ is in R, called a *constant polynomial.* In other words, $f(x)$ cannot be the product of two nonconstant polynomials.

For the following application we remind the reader that a finite field, denoted by $\mathbb{F}_q$ with $q \in \mathbb{N}$ elements must satisfy the property that q is a prime power. Such fields are also called *Galois fields.* If $q = p^m$ for a prime p and $m \in \mathbb{N}$, then $\mathbb{F}_p$ is called the *prime subfield* of F_q. In general, a prime subfield is a field having no proper subfields, so $\mathbb{Q}$ is the prime subfield of any field of characteristic 0, and F_p is the prime subfield of any field of characteristic p.

Theorem A.8 — Multiplicative Subgroups of Fields

If F is a field and F^* is a finite subgroup of the multiplicative group of nonzero elements on F, then F^* is cyclic. In particular, if $F = \mathbb{F}_{p^n}$ is a finite field, then $\mathbb{F}^*$ is a finite cyclic group.

In general, it is important to make the distinction between degrees of a polynomial over various rings, since the base ring under consideration may alter the makeup of the polynomial.

Example A.2 The polynomial

$$f(x) = 2x^2 + 2x + 2$$

is of degree two over $\mathbb{Q}$. However, over $\mathbb{F}_2$, the finite field of two elements, $\deg_{\mathbb{F}_2} = -\infty$, since f is the zero polynomial in $\mathbb{F}_2[x]$.

Some facts concerning irreducible polynomials will be needed in the text as follows—see Exercise 2.15 on page 64, for instance.

Theorem A.9 — Irreducible Polynomials over Finite Fields

The product of all monic irreducible polynomials over a finite field F_q whose degrees divide a given $n \in \mathbb{N}$ is equal to $x^{q^n} - x$.

Based upon Theorem A.9, the next result may be used as an algorithm for irreducibility over prime fields and thereby generate irreducible polynomials. First, we need a definition.

Definition A.15 — The GCD of Polynomials

If $f_i(x) \in F[x]$ for $i = 1, 2$, where F is a field, then the *greatest common divisor of* $f_1(x)$ *and* $f_2(x)$ is a unique monic polynomial $g(x) \in F[x]$ satisfying both:

(a) For $i = 1, 2$, $g(x)|f_i(x)$.

(b) If there is a $g_1(x) \in F[x]$ such that $g_1(x)|f_i(x)$ for $i = 1, 2$, then $g_1(x)|g(x)$.

If $g = 1$, we say that $f_1(x)$ and $f_2(x)$ are *relatively prime*, denoted by

$$\gcd(f_1(x), f_2(x)) = 1.$$

Corollary A.8 The following are equivalent.

(a) A polynomial f is irreducible over F_p where p is prime and $\deg_{\mathbb{F}_p}(f) = n$.

(b) For all natural numbers $i \le \lfloor n/2 \rfloor$, $\gcd(f(x), x^{p^i} - x) = 1$.

There is a general result concerning irreducible polynomials over any field.

Theorem A.10 — Irreducible Polynomials over Arbitrary Fields
Let F be a field and $f(x) \in F[x]$. Denote by $(f(x))$ the principal ideal in $F[x]$ generated by $f(x)$. Then the following are equivalent.

(a) f is irreducible over F.

(b) $F[x]/(f(x))$ is a field.

Our main concern in this text is with subfields of $\mathbb{C}$. In particular, what is the relationship between $\deg_{\mathbb{Q}}(f)$, and $\deg_{\mathbb{Z}}(f)$? This is answered by an important result of Gauss, which relates degrees, and irreducibility of polynomials in $\mathbb{Q}$ and $\mathbb{Z}$.

Lemma A.1 — Gauss's Lemma[A.6]
If $f(x) \in \mathbb{Z}[x]$, and

$$f(x) = g(x)h(x) \text{ for } g(x), h(x) \in \mathbb{Q}[x],$$

then

$$f(x) = G(x)H(x) \text{ for some } G(x), H(x) \in \mathbb{Z}[x].$$

Furthermore, $\deg_{\mathbb{Q}}(g) = \deg_{\mathbb{Z}}(G)$, and $\deg_{\mathbb{Q}}(h) = \deg_{\mathbb{Z}}(H)$.

Lemma A.1 tells us that any polynomial which is irreducible in $\mathbb{Z}[x]$ is also irreducible in $\mathbb{Q}[x]$, or contrapositively, if $f(x)$ is reducible in $\mathbb{Q}[x]$, then it is already reducible in $\mathbb{Z}[x]$. Given this fact, it is useful to have an irreducibility test over $\mathbb{Q}$.

Theorem A.11 — Schönemann/Eisenstein Criterion[A.7]
Let $f(x) \in \mathbb{Z}[x]$ with $f(x) = \sum_{j=0}^{d} a_j x^j$. If there exists a prime $p \in \mathbb{Z}$ such that both

(a) $a_j \equiv 0 \pmod{p}$ for $j = 0, 1, \ldots, d-1$ with $a_d \not\equiv 0 \pmod{p}$, and

(b) $a_0 \not\equiv 0 \pmod{p^2}$

hold, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Now that we have the notion of irreducibility for polynomials, we may state a unique factorization result for polynomials over fields.

[A.6] Another lemma, also known as Gauss's Lemma, says that the product of primitive polynomials in $\mathbb{Z}[x]$ is primitive in $\mathbb{Z}[x]$.

[A.7] Although this is known as Eisenstein's criterion in the literature, it was actually *first* discovered by T. Schönemann in [64]. He actually claimed priority over Eisenstein in [65]. The consensus is that Schönemann's paper was overlooked because he put the criterion at the end of the paper without any applications or even a hint as to its importance, whereas Eisenstein put his at the front of the paper and demonstrated the applicability to such things as the irreducibility of the cyclotomic polynomials.

Theorem A.12 — Unique Factorization for Polynomials

If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials $p(x)$, each of which is unique up to order and units (nonzero constant polynomials) in F.

The Euclidean Algorithm applies to polynomials in a way that allows us to talk about common divisors of polynomials in a fashion similar to that for integers.

There is also a Euclidean result for polynomials over a field.

Theorem A.13 — Euclidean Algorithm for Polynomials

If $f(x), g(x) \in F[x]$, where F is a field, and $g(x) \neq 0$, there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x),$$

where either $0 \leq \deg(r) < \deg(g)$, or $r(x) = 0$, the zero polynomial with $\deg(r) = -\infty$.

Thus, $F[x]$ is a Euclidean domain with respect to the valuation $v(f) = 2^{\deg(f)}$, with $\deg(0) = -\infty$, namely $2^{\deg(0)} = 0$.

Finally, if $f(x)$ and $g(x)$ are relatively prime, there exist $s(x), t(x) \in F[x]$ such that

$$1 = s(x)f(x) + t(x)g(x).$$

An important concept that we will need, for instance, in the proof of Theorem 3.17 on page 127, is the following.

Definition A.16 — Symmetric Functions

Let R be a commutative ring with identity, and $f(x) \in R[x_1, x_2, \ldots, x_n]$, the polynomial ring in n indeterminates x_j for $j = 1, 2, \ldots, n$. Then f is called *symmetric* if for each $\sigma \in S_n$, the symmetric group on n letters,

$$f^\sigma(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}),$$

denoted by simply $f^\sigma = f$. In particular, if

$$s_j(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$$

is defined to be the sum of all possible distinct products of j distinct x_i, then s_j is a symmetric function called an *elementary symmetric polynomial.* Thus,

$$\begin{aligned}
s_1(x_1, x_2, \ldots, x_n) &= \sum_{j=1}^{n} x_j; \\
s_2(x_1, x_2, \ldots, x_n) &= \sum_{1 \leq i < j \leq n} x_i x_j; \\
s_3(x_1, x_2, \ldots, x_n) &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k; \\
&\vdots \\
s_k(x_1, x_2, \ldots, x_n) &= \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}; \\
&\vdots \\
s_n(x_1, x_2, \ldots, x_n) &= \prod_{j=1}^{n} x_j.
\end{aligned}$$

Theorem A.14 — Newton

Let R be a commutative ring with identity. Then every symmetric polynomial in

$$R[x_1, x_2, \ldots, x_n]$$

is expressible as a polynomial in

$$R[s_1, s_2, \ldots, s_n].$$

Corollary A.9 Let R be a commutative ring with identity and $f(x) \in R[x]$ be a polynomial of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ in R. If $g(x_1, x_2, \ldots, x_d)$ is a symmetric polynomial over R, then

$$g(\alpha_1, \alpha_2, \ldots, \alpha_d) \in R.$$

Definition A.17 — Splitting Fields for Polynomials

If $f(x) \in F[x]$ where $F \subseteq \mathbb{C}$ is a field and α_j for $1 \le j \le d$ are all of the roots of $f(x)$ in $\mathbb{C}$, then there exists a smallest extension field E of F such that

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) \in E[x]$$

called the *splitting field* of f over F. Moreover, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_d)$.

Theorem A.15 — Extensions of Isomorphisms

Let K_1 and K_2 be extension fields of F which has characteristic zero or is finite. Suppose that $f_j(x) \in K_j[x]$ with splitting field E_j for $j = 1, 2$. If ϕ is an isomorphism of K_1 and K_2 with $\phi(f_1(x)) = f_2(x)$, then ϕ can be extended to an isomorphism of E_1 to E_2.

Corollary A.10 If F is a field of characteristic zero or is finite with $f(x) \in F[x]$, then there exists a splitting field of $f(x)$ which is unique up to F-isomorphism. In particular, any two algebraic closures are F-isomorphic—see Definition 1.31 on page 37.

Related to the above are the following fundamental facts. See Exercise 2.6 on page 63 for comparison and usage of notions surrounding these concepts.

Theorem A.16 — The Number of Extensions of Isomorphims

If K is an extension field of F of finite degree $|K : F| = n$, where F has characteristic zero or is finite, and if L is an algebraically closed field containing F, then there are n F-isomorphisms of K into L.

Theorem A.17 — The Primitive Element Theorem

If K is an extension field of F which has characteristic zero or is finite, then there exists $\alpha \in K$ such that $K = F(\alpha)$.

Theorem A.18 — The Fundamental Theorem of Algebra

If $f(x) \in \mathbb{C}[x]$ and $\deg(f) = d \in \mathbb{N}$, then $f(x)$ factors into a product of d factors in $\mathbb{C}[x]$.

✦ Basic Matrix Theory

If $m, n \in \mathbb{N}$, then an $m \times n$ matrix (read "m by n matrix") is a rectangular array of entries with m rows and n columns. We will assume that the entries come from a commutative ring with identity R. If A is such a matrix, and $a_{i,j}$ denotes the entry in the i^{th} row and j^{th} column, then

$$A = (a_{i,j}) = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots a_{2,n} \\ \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots a_{m,n} \end{pmatrix}.$$

Two $m \times n$ matrices $A = (a_{i,j})$, and $B = (b_{i,j})$ are equal if and only if $a_{i,j} = b_{i,j}$ for all i and j. The matrix $(a_{j,i})$ is called the *transpose* of A, denoted by

$$A^t = (a_{j,i}).$$

Addition of two $m \times n$ matrices A and B is done in the natural way,

$$A + B = (a_{i,j}) + (b_{i,j}) = (a_{i,j} + b_{i,j}),$$

and if $r \in R$, then $rA = r(a_{i,j}) = (ra_{i,j})$, called *scalar multiplication.* A *scalar* is a quantity that has magnitude, but not direction. This term comes from the vector space context, which we develop below. The case where the term scalar is used most often in practice is when $R = \mathbb{R}$.

Under the above definition of addition and scalar multiplication, the set of all $m \times n$ matrices with entries from R, a commutative ring with identity, form an R-module, denoted by $\mathcal{M}_{m\times n}(R)$. If R is a division ring, then $\mathcal{M}_{m\times n}(R)$ is a vector space over R.

If $A = (a_{i,j})$ is an $m \times n$ matrix and $B = (b_{i,j})$ is an $n \times r$ matrix, then the *product* of A and B is defined as

$$AB = (a_{i,j})(b_{i,j}) = \left(\sum_{k=1}^{n} a_{i,k} b_{k,j}\right), \text{ with } 1 \le i \le m, \text{ and } 1 \le j \le r.$$

When multiplication is defined, then it is associative, and distributive over addition. If $m = n$, then $\mathcal{M}_{n\times n}(R)$ is a ring, with identity given by the $n \times n$ matrix:

$$I_n = \begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & 1_R & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1_R \end{pmatrix},$$

called *the $n \times n$ identity matrix*, where 1_R is the identity of R.

Another important aspect of matrices that we will need throughout the text is motivated by the following. We maintain the assumption that R is a commutative ring with identity. Let $(a, b), (c, d) \in \mathcal{M}_{1\times 2}(R)$. It is a straightforward exercise for the reader to verify that (a, b) and (c, d) are linearly independent vectors in $\mathcal{M}_{1\times 2}(R)$ if and only if $ad - bc \neq 0$—see Definition A.7 on page 324. If we set up these row vectors into a single 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then $ad - bc$ is called the *determinant* of A, denoted by $\det(A)$. More generally, we may define the determinant of any $n \times n$ matrix in $\mathcal{M}_{n\times n}(R)$ for any $n \in \mathbb{N}$. The determinant of any $r \in \mathcal{M}_{1\times 1}(R)$ is just $\det(r) = r$. Thus, we have the definitions for $n = 1, 2$, and we may now give the general definition inductively. The definition of the determinant of a 3×3 matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

is defined in terms of the above definition of the determinant of a 2×2 matrix, namely $\det(A)$ is given by

$$a_{1,1} \det \begin{pmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{pmatrix} - a_{1,2} \det \begin{pmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{pmatrix} + a_{1,3} \det \begin{pmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{pmatrix}.$$

Therefore, we may inductively define the determinant of any $n \times n$ matrix in this fashion. Assume that we have defined the determinant of an $n \times n$ matrix. Then we define the determinant of an $(n+1) \times (n+1)$ matrix $A = (a_{i,j})$ as follows. First, we let $A_{i,j}$ denote the $n \times n$ matrix obtained from A by deleting the i^{th} row and j^{th} column. Then we define the *minor* of $A_{i,j}$ at position (i, j) to be $\det(A_{i,j})$. The *cofactor* of $A_{i,j}$ is defined to be

$$\text{cof }(A_{i,j}) = (-1)^{i+j} \det(A_{i,j}).$$

We may now define the determinant of A by

$$\det(A) = a_{i,1}\text{cof }(A_{i,1}) + a_{i,2}\text{cof }(A_{i,2}) + \cdots + a_{i,n+1}\text{cof }(A_{i,n+1}). \tag{A.6}$$

This is called the *expansion of a determinant by cofactors* along the i^{th} row of A. Similarly, we may expand along a column of A.

$$\det(A) = a_{1,j}\, \mathit{cof}(A_{1,j}) + a_{2,j}\, \mathit{cof}(A_{2,j}) + \cdots + a_{n+1,j}\, \mathit{cof}(A_{n+1,j}),$$

called the *cofactor expansion along the j^{th} column of A*. Hence, a determinant may be viewed as a function that assigns a real number to an $n \times n$ matrix, and the above gives a method for finding that number. Other useful properties of determinants that we will have occasion to use in the text are given in the following.

Theorem A.19 — Properties of Determinants

Let R be a commutative ring with identity and let $A = (a_{i,j})$, $B = (b_{i,j}) \in \mathcal{M}_{n\times n}(R)$. Then each of the following hold.

(a) $\det(A) = \det(a_{i,j}) = \det(a_{j,i}) = \det(A^t)$.

(b) $\det(AB) = \det(A)\det(B)$.

(c) If matrix A is achieved from matrix B by interchanging two rows (or two columns), then $\det(A) = -\det(B)$.

(d) If $\mathcal{S}_n$ is the symmetric group on n letters, then

$$\det(A) = \sum_{\sigma\in\mathcal{S}_n} (\text{sgn}(\sigma)) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)},$$

where $\text{sgn}(\sigma)$ is the sign of σ given in Definition A.2 on page 320.

If $A \in \mathcal{M}_{n\times n}(R)$, then A is said to be *invertible*, or *nonsingular* if there is a unique matrix denoted by

$$A^{-1} \in M_{n\times n}(R)$$

such that

$$AA^{-1} = I_n = A^{-1}A.$$

Theorem A.20 — Properties of Invertible Matrices

Let R be a commutative ring with identity, $n \in \mathbb{N}$, and A invertible in $\mathcal{M}_{n\times n}(R)$. Then each of the following holds.

(a) $(A^{-1})^{-1} = A$.

(b) $(A^t)^{-1} = (A^{-1})^t$, where "t" denotes transpose.

(c) $\det(A)$ is a unit in R.

There is a special class of invertible matrices, which we will have occasion to use in the development of the basics in this text—for instance see Exercise 1.59 on page 54.

Definition A.18 — General Linear Group and Unimodular Matrices

If R is a field, or $R = \mathbb{Z}$, then the totality of $n \times n$ nonsingular matrices with entries from R forms a group under matrix multiplication, called the *general linear group*, denoted by $GL_n(R)$. In the case where $R = \mathbb{Z}$, Theorem A.20 tells us that $\det(A) = \pm 1$ for any $A \in GL_n(\mathbb{Z})$. The matrices in $GL_n(\mathbb{Z})$ are called *unimodular*.

Another important fact is contained in the sequel, a result which follows from cofactor expansions—see Biography B.2 on page 351 for some ironies of attribution in this regard.

Theorem A.21 — Cramer's Rule

Let $A = (a_{i,j})$ be the *coefficient matrix* of the following system of n linear equations in n unknowns:

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \cdots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \cdots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{n,1}x_1 & + & a_{n,2}x_2 & + & \cdots & + & a_{n,n}x_n & = & b_n, \end{array}$$

over a field F. If $\det(A) \neq 0$, then the system has a solution given by:

$$x_j = \frac{1}{\det(A)}\left(\sum_{i=1}^{n}(-1)^{i+j}b_i \det(A_{i,j})\right), \quad (1 \le j \le n).$$

We may also determine the inverse of a nonsingular matrix via a notion related to the development of Cramer's Rule.

Definition A.19 — Adjoint
Let R be a commutative ring with identity. If $A = (a_{i,j}) \in \mathcal{M}_{n\times n}(R)$, then the matrix

$$A^a = (b_{i,j})$$

given by

$$b_{i,j} = (-1)^{i+j}\det(A_{j,i})$$

is called the *adjoint of A*.

Some properties of adjoints related to inverses are as follows.

Theorem A.22 — Properties of Adjoints
If R is a commutative ring with identity and $A \in \mathcal{M}_{n\times n}(R)$, then each of the following holds.

(a) $AA^a = \det(A)I_n = A^aA$.

(b) A is invertible in $\mathcal{M}_{n\times n}(R)$ if and only if $\det(A)$ is a unit in R, in which case

$$A^{-1} = \frac{A^a}{\det(A)}.$$

Note that when R is a field in Theorem A.22, then $\det(A)$ is a unit if and only if $\det(A) \neq 0$.

The following facts will also prove to be useful in the text—see the proof of Theorem 2.2 on page 58, for instance.

Theorem A.23 — Systems of Linear Homogeneous Equations
A system of m linear equations in n unknowns x_i over a field F

$$a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1$$

$$\vdots$$

$$a_{m,1}x_1 + a_{m,2}x_2 + \cdots a_{m,n}x_n = b_m$$

has a (simultaneous*)* solution if and only if the matrix equation $AX = B$ has a solution X, where $A = (a_{i,j}) \in \mathcal{M}_{m\times n}(F)$, $X = (x_i) \in \mathcal{M}_{n\times 1}(F)$, and $B = (b_j) \in \mathcal{M}_{m\times 1}(F)$. The system $AX = B$ is called a *homogeneous system of linear equations* if $B = (0) \in \mathcal{M}_{m\times 1}(F)$ is the zero vector. If $m < n$, then $AX = 0$ has a *nontrivial solution*, that is to say, one for which not all $x_i = 0$. In this case, there are elements $c_i \in F$ not all zero such that $\sum_{i=1}^n a_{i,j}c_i = 0$.

We introduced linear transformations on page 328. We now define an associated matrix.

Definition A.20 — Matrix of a Transformation
Suppose that $\psi : V \mapsto V$ is a linear transformation of a vector space V over a field F. If $\{v_1, \ldots, v_n\}$ is a basis for V over F, then the *matrix of* ψ is given by $(\alpha_{i,j})$, where $\alpha_{i,j} \in F$ are uniquely determined by

$$\psi(v_i) = \sum_{j=1}^{n} \alpha_{i,j}v_j \quad (1 \le i \le n).$$

The determinant of the linear transformation is denoted by $\det(\psi) = \det(\alpha_{i,j})$.

Lastly, for this section on matrices, we define the following, which we will need as a tool in the main text—see the proof of Theorem 5.13 on page 215, for instance.

Definition A.21 Kronecker Products

If $A = (\alpha_{i,j}) \in \mathcal{M}_{r\times r}(F)$ and $B = (\beta_{k,\ell}) \in \mathcal{M}_{s\times s}(F)$ for a field F, then the *Kronecker product* of A and B, denoted by $A \times B$, is obtained by taking the matrix $B = (\beta_{k,\ell})$ and replacing each entry $\beta_{k,\ell}$ by the $r \times r$ matrix $\beta_{k,\ell}(\alpha_{i,j})$.

Now we have a smattering of concepts that we will require and we put them under their own headings.

✦ The Arithmetic-Geometric Mean Inequality

We will have need of the following classical result in the text. See [28, Theorem 5.2, p. 544] for a proof. If $n \in \mathbb{N}$ and $x_j \in \mathbb{R}^+$ for $j = 1, 2, \ldots, n$, then

$$(x_1 \cdot x_2 \cdots x_n)^{1/n} = \left(\prod_{j=1}^{n} x_j\right)^{1/n} \le \frac{1}{n}\sum_{j=1}^{n} x_j = \frac{1}{n}(x_1 + x_2 + \cdots + x_n).$$

✦ Stirling's Formula

$$\frac{n^n}{n!} = \frac{e^{-\frac{\alpha}{12n}+n}}{\sqrt{2\pi n}}, \tag{A.7}$$

for some α in the interval $(0, 1)$. This is a version that will be suitable for our purposes in this text—see the proof of Corollary 3.7 on page 116, for instance.
Another important fact is from the theory of sets.

✦ Zorn's Lemma

Suppose that S is a linearly ordered[A.8] family of sets that is closed with respect to taking unions. In other words, for any number of $\mathcal{S}_j \in S$ (possibly infinitely many), $\cup_j \mathcal{S}_j \in S$. Then S has a maximal element. Zorn's Lemma is equivalent to the Axiom of Choice (see [50, p. 367], for instance).

Biography A.1 Max Zorn (1906–1993) was born on June 6, 1906 in Germany. He received his doctorate from Hamburg in 1930 under the direction of Artin (see Biography 1.2 on page 24). He was then appointed to Halle in 1933. However, he left Germany because of the Nazis. He worked at Yale from 1934 to 1936. It was during this period that he produced what we now call Zorn's lemma. He then spent ten years in California, after which he moved to Indiana, where he became a Professor. Perhaps his most famous student was Israel Nathan Herstein (1923–1988). Zorn did work, not only in set theory, but also in topology and algebra. One of his other classical results was the proof that the Cayley numbers are unique in the sense that they form the only alternative, quadratic, real nonassociative algebra without zero divisors. He died on March 9, 1993.

[A.8] Recall that a *linear order* is a binary relation R on a set S such that the following three conditions are satisfied.

(1) aRb, or bRa for all $a,b \in S$, with a distinct from b,

(2) aRa for *no* $a \in S$, and

(3) if aRb, and bRc, then aRc.

Biography A.2 James Stirling (1692–1770), was born in May 1692 in Garden (near Stirling), Scotland, and educated at Glasgow. In 1717, he published his first work *Linae Terti Ordinis Neutonianae*, extending Newton's theory of plane curves by classifying cubic curves. He was elected to the Royal Society in London in 1726, and in 1730, he published, as Example 2 of Proposition 28, in the *Methodus differentialis*, the approximation $n!\approx\sqrt{2\pi n}(\frac{n}{e})^n$, in the same year as Abraham de Moivre (1657–1705) published his *Miscellanea analytica.* There is a certain consensus among mathematical historians that de Moivre knew a version of formula (A.7) earlier than Stirling. De Moivre used many such formulas in his research in probability theory. For instance, de Moivre was ostensibly the first to work with the probability formula $\int_0^\infty e^{-x^2}dx=\sqrt{\pi}/2$, which appeared in 1733 in a privately printed paper entitled *Approximatio ad summam terminorum binomii* $(a+b)^n$ *in seriem expansi.* In 1735, Stirling returned to Scotland, and became manager of the Scotch Mining Company at Leadhills. In 1746, he was elected to the Royal Society of Berlin. In that same year Colin Maclaurin (1698–1746) died, and Stirling was offered his chair at Edinburgh, but he declined. He is also known for numbers called Stirling numbers, which have to do with permutations of lists of numbers. Stirling died on December 5, 1770 in Edinburgh.

We also remind the reader of the following elementary, albeit important facts.

✦ Dirichlet's Box Principle

If more than $n \in \mathbb{N}$ objects are placed in n boxes, then at least one of the boxes contains more than one element.

This is also called the *Pigeonhole Principle* based upon the application of $n+1$ pigeons flying into n holes.

✦ The Well-Ordering Principle

Every non-empty subset of $\mathbb{N}$ contains a least element.
It can be shown that the Well-Ordering principle is logically equivalent to following—see [53, Exercise 1.3, p. 11].

✦ The Principle of Mathematical Induction

Suppose that $\mathcal{S} \subseteq \mathbb{N}$ and both (a) and (b) below hold.

(a) $1 \in \mathcal{S}$, and

(b) If $n > 1$ and $n-1 \in \mathcal{S}$, then $n \in \mathcal{S}$.

Then $\mathcal{S} = \mathbb{N}$.

The following will be useful in text—see the solution of Exercise 6.1 on page 401 for instance.

Theorem A.24 Solutions of Linear Congruences

For $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$,

$$ax \equiv b \pmod{n} \tag{A.8}$$

has a solution $x \in \mathbb{Z}$ if and only if $g = \gcd(a,n) \bigm| b$. Furthermore, if such a solution exists, then there are exactly g incongruent solutions modulo n and exactly one of these is in the least residue system modulo n/g, this being the unique solution to (A.8).

The following result was first proved by Leibniz and has a familiar consequence as a special case, which is used throughout the text—see the proof of the cubic reciprocity law in Theorem 6.1 on page 267, and the proof of the biquadratic reciprocity law in Theorem 6.5 on page 282, for instance.

✦ The Multinomial Theorem

Theorem A.25 Let R be a commutative ring with identity, and let $m, n \in \mathbb{N}$ with $m > 1$. If $a_1, a_2, \ldots, a_m \in R$, then

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{(j_1, j_2, \ldots, j_m)} \frac{n! a_1^{j_1} a_2^{j_2} \cdots a_m^{j_m}}{j_1! j_2! \cdots j_m!},$$

where the sum ranges over all m-tuples $(j_1, j_2, \ldots, j_m)$ of nonnegative integers j_i with $j_1 + j_2 + \cdots + j_m = n$.

Corollary A.11 — The Binomial Theorem

Let R be a commutative ring with identity, $a, b \in R$, and $n \in \mathbb{N}$. Then

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j},$$

where

$$\binom{n}{j} = \frac{n!}{(n-j)!j!} \in \mathbb{Z}$$

is the binomial coefficient.

Biography A.3 Gottfried Wilhelm von Leibniz (1646–1716), was born on July 1, 1646 in Leipzig, Saxony (now Germany). By the age of twelve, he had taught himself Latin and Greek in order to be able to read the books of his father, who was a philosophy professor at Leipzig. Leibniz studied law at Leipzig from 1661 to 1666 and ultimately received a doctorate in law from the University of Altdorf in 1667. He pursued a career in law at the courts of Mainz from 1667 to 1672. Then he went to Paris from 1672 to 1676, during which time he studied mathematics and physics under Christian Huygens (1629–1695). In 1676, he left for Hannover, Hanover (now Germany), where he remained for the balance of his life. Leibniz began looking for a uniform and useful notation for the calculus in 1673. In 1684, he published the details of the differential calculus, the year before Newton published his famed *Principia*. The bitter dispute between Newton and Leibniz concerning priority over the discovery of the calculus is detailed in [50, pp. 234–235]. In 1700, Leibniz founded the Berlin Academy and was its first president. Then he became increasingly reclusive until his death in Hannover on November 14, 1716.

The following will be of use in the text—see the proof of Theorem 5.8 on page 201, for instance.

✦ The Lagrange Interpolation Formula

Theorem A.26 Let F be a field, and let a_j for $j = 0, 1, 2, \ldots, n$ be distinct elements of F. If c_j for $j = 0, 1, 2, \ldots, n$ are any elements of F, then

$$f(x) = \sum_{j=0}^{n} \frac{(x - a_0) \cdots (x - a_{j-1})(x - a_{j+1}) \cdots (x - a_n)}{(a_j - a_0) \cdots (a_j - a_{j-1})(a_j - a_{j+1}) \cdots (a_j - a_n)} c_j$$

is the unique polynomial in $F[x]$ such that $f(a_j) = c_j$ for all $j = 0, 1, \ldots, n$.

For ease of reference and convenience, the reader is reminded of the following definitions.

✦ Some Elementary Number Theory

We remind the reader of the Definition of Euer's totient for convenience.

Definition A.22 — Euler's Totient

For any $n \in \mathbb{N}$ the *Euler totient*, also known as *Euler's ϕ-function*, $\phi(n)$ is defined to be the number of $m \in \mathbb{N}$ such that $m < n$ and $\gcd(m, n) = 1$.

Definition A.23 — The Legendre Symbol

If $c \in \mathbb{Z}$ and $p > 2$ is prime such that $p \nmid c$, then the Legendre symbol is given by:

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if } c \text{ is a quadratic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

Note that the above implies

$$\left(\frac{c}{p}\right) \equiv c^{(p-1)/2} \pmod{p}. \tag{A.9}$$

Also, we have for the $c = 2$ case that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{A.10}$$

As well,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases} \tag{A.11}$$

Definition A.24 — The Jacobi Symbol

Let $n \in \mathbb{N}$, $n > 1$ be odd, and $c \in \mathbb{Z}$ with $\gcd(c, n) = 1$. Suppose that $n = \prod_{j=1}^{k} p_j$ where the p_j are (not necessarily distinct) primes. Then the *Jacobi symbol* is

$$\left(\frac{c}{n}\right) = \prod_{j=1}^{k} \left(\frac{c}{p_j}\right),$$

where the right-hand symbols are Legendre symbols.

Definition A.25 — The Kronecker Symbol

Suppose that $n \in \mathbb{N}$ and$\Delta\ _F$ is the discriminant of a quadratic number field—see Defintion 1.33 on page 46. The *Kronecker symbol* $\left(\frac{\Delta_F}{n}\right)$ is given by

$$\left(\frac{\Delta_F}{n}\right) = 0$$

if $\gcd(\Delta_F, n) > 1$, and

$$\left(\frac{\Delta_F}{2}\right) = \begin{cases} 1 & \text{if} \quad {}_F\Delta \equiv 1 \pmod 8, \\ -1 & \text{if} \quad \Delta_F \equiv 5 \pmod 8). \end{cases}$$

$$\left(\frac{\Delta_F}{p}\right) \text{ is the Legendre symbol for any prime } p > 2.$$

$$\left(\frac{\Delta_F}{n}\right) \text{ is the Jacobi symbol if } n \text{ is odd and } \gcd(n, \Delta_F) = 1.$$

If $n = 2^a m$ where m is odd, then

$$\left(\frac{\Delta_F}{n}\right) = \left(\frac{\Delta_F}{2}\right)^a \left(\frac{\Delta_F}{m}\right),$$

where $\left(\frac{\Delta_F}{m}\right)$ is the Jacobi symbol.

Also, of value in the text is the following result on representation of natural numbers—see [53, Corollary 6.1, p. 245], for instance.

Theorem A.27 A natural number n can be represented as the sum of two integer squares if and only if every prime factor of the form $p \equiv -1 \pmod 4$ appears to an even power in the canonical prime factorization of n.

We conclude this appendix with a statement of the following celebrated result. Gauss first studied the number of primes less than x, denoted by $\pi(x)$. He observed that as x increases $\pi(x)$ behaves akin to $x/\log_e(x)$. Therefore, he conjectured in 1793, at the age of sixteen, that the following holds.

Theorem A.28 — The Prime Number Theorem

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log_e(x)} = 1,$$

denoted by

$$\pi(x) \sim x/\log_e(x).^{\text{A.9}}$$

[A.9] In general, if f and g are functions of a real variable x, then $f(x) \sim g(x)$ means $\lim_{x\to\infty} f(x)/g(x) = 1$. Such functions are said to be *asymptotic*.

Although Riemann had given an outline of a proof for Theorem A.28, the necessary tools had not yet been developed. This outline was one of the major motivations for the development of complex analysis from 1851 until the first proofs were given in 1896 independently by Hadamard, and Poussin.

There are better approximations to $\pi(x)$ such as the *logarithmic integral*

$$li(x) = \int_2^x dt/\log_e(t),$$

which Gauss also conjectured, after postulating the validity of Theorem A.28.

Biography A.4 Charles Jean Gustave Nicholas De La Vallée Poussin (1866–1962) was born in Louvain, Belgium on August 14, 1866. In 1891, he became an assistant at the University of Louvain, where he worked with Louis Claude Gilbert, one of his former teachers. Gilbert died at the age of twenty-six, and Poussin was elected to his chair in 1893. He held that chair for the next fifty years. He is perhaps best known for his proof of the Prime Number Theorem in 1896, and his important, fundamental textbook *Cours d'analyse*, which saw several editions. However, the text contained no complex function theory. Poussin did turn to the theory of complex variables after 1925. He wrote *Le potential logarithmique*, which was published after the war in 1949. He died on March 2, 1962 in Louvain.

Biography A.5 Jacques Salomon Hadamard (1865–1963) was born in Versailles, France on December 8, 1865. He studied at the École Normale Supérieure, where Emile Picard was one of his teachers. He obtained his doctorate in 1892 on the topic of functions defined by Taylor series. Hadamard was elected to a chair at Paris where he discovered his proof of the prime number theorem. This proof was only part of his work in complex analysis. He is credited with approximately three-hundred publications including contributions to the theory of integral functions and singularities of functions represented by Taylor series, as well as a generalization of Green's functions. Hadamard was also deeply involved with politics. A relation of his, Alfred Dreyfus, who was a French army officer, was tried for treason. This began a controversy that lasted over a decade, and became known as the *Dreyfus Affair*, which scarred the history of the French Third Republic. Hadamard actively participated in clearing Dreyfus's name. This occurred on July 22, 1906, when Dreyfus was exonorated and decorated with the Legion of Honour—see [52, p. 77] for an overview of the Dreyfus scandal and the surrounding issues. Hadamard lost two of his sons in World War I after which his politics moved to the left, partly in response to the rise of Nazi power. After France fell in 1940, Hadamard left for the United States, but returned to Paris in 1944. After World War II, he became an active peace campaigner. He died just before his ninety-eighth birthday on October 17, 1963 in Paris.

Appendix B

Sequences and Series

> *Simplicity is the ultimate sophistication.*
>
> **Leonardo da Vinci (1452–1519)**
> Florentine painter, sculptor, architect, engineer, inventor

We look at the important fundamental notions behind sequences and series as they will be needed in the main text. The proofs for most of what follows may be found in any standard first- or second- year calculus text.

Definition B.1 — Sequences

A sequence is a function whose domain is $\mathbb{N}$, with images denoted by a_n, called the n^{th} *term of the sequence.* The entire sequence is denoted by $\{a_n\}_{n=1}^{\infty}$, or simply $\{a_n\}$, called an infinite sequence or simply a *sequence.* If $\{a_n\}$ is a sequence, and $L \in \mathbb{R}$ such that

$$\lim_{n\to\infty} a_n = L,$$

then the sequence is said to *converge*, whereas sequences that have no such limit are said to *diverge.* If the terms of the sequence are nondecreasing, $a_n \le a_{n+1}$ for all $n \in \mathbb{N}$, or nonincreasing, $a_n \ge a_{n+1}$ for all $n \in \mathbb{N}$, then $\{a_n\}$ is said to be *monotonic.* A sequence $\{a_n\}$ is called *bounded above* if there exists an $M \in \mathbb{R}$ such that $a_n \le M$ for all $n \in \mathbb{N}$. The value M is called an *upper bound* for the sequence. A sequence $\{a_n\}$ is called *bounded below* if there is an $B \in \mathbb{R}$ such that $B \le a_n$ for all $n \in \mathbb{N}$, and B is called a *lower bound* for the sequence. A sequence $\{a_n\}$ is called *bounded* if it is bounded above and bounded below.

Some fundamental facts concerning sequences are contained in the following.

Theorem B.1 — Properties of Sequences

Let $\{a_n\}$ and $\{b_n\}$ be sequences. Then

(a) If $\{a_n\}$ is bounded and monotonic, then it converges.

(b) If $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = L \in \mathbb{R}$, and $\{c_n\}$ is a sequence such that there exists an $N \in \mathbb{N}$ with $a_n \le c_n \le b_n$ for all $n > N$, then $\lim_{n\to\infty} c_n = L$.

(c) If $\lim_{n\to\infty} |a_n| = 0$, then $\lim_{n\to\infty} a_n = 0$.

Definition B.2 — Infinite Series[B.1]

If $\{a_j\}$ is an infinite sequence, then

$$\sum_{j=1}^{\infty} a_j$$

[B.1] One may trace infinite series back to Archimedes (287–212 B.C.). He established a result on the quadrature of the parabola, thereby essentially proving that the series $\sum_{j=1}^{\infty} 4^{-j}$ converges.

is called an *infinite series.* The sum

$$S_n = \sum_{j=1}^{n} a_j$$

is called the n^{th} *partial sum* of the series. The series is said to *converge* if the sequence $\{S_n\}$ converges, and it is said to *diverge* if the sequence diverges. If the series converges, then $\lim_{n\to\infty} S_n = S \in \mathbb{R}$ is called the *sum* of the series, denoted by

$$S = \sum_{j=1}^{\infty} a_j.$$

An infinite series of the form

$$\sum_{j=0}^{\infty} ar^n \quad (a, r \in \mathbb{R}, a, r \neq 0)$$

is called a *geometric series with ratio r*.

Theorem B.2 — Properties of Infinite Series

Let $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ be infinite series. Then each of the following hold.

(a) If $\sum_{j=1}^{\infty} a_j$ converges, then the sequence $\{a_j\}_{j=1}^{\infty}$ converges to 0.

(b) If $c \in \mathbb{R}$ is constant, then $\sum_{j=1}^{\infty} ca_j = c\sum_{j=1}^{\infty} a_j$.

(c) If $\sum_{j=1}^{\infty} a_j = S_1 \in \mathbb{R}$, and $\sum_{j=1}^{\infty} b_j = S_2 \in \mathbb{R}$, then $\sum_{j=1}^{\infty}(a_j + b_j) = S_1 + S_2$.

Remark B.1 If an infinite series is convergent, then one may remove or insert any finite number of terms without affecting its convergence. Also, one may group the terms of the series in brackets, without altering the order of the terms, and the resulting series converges to the same sum. However, the converse of the last statement is false. In other words, one cannot *remove* brackets and have a series that necessarily converges. For instance, the infinite series $(1 - 1) + (1 - 1) + \cdots$ is convergent, but the series obtained by removing the brackets is not. Hence, brackets may be inserted without affecting convergence, but may not be removed—see Remark B.2 on page 349.

We now look at some well-known tests for convergence.

Theorem B.3 — Integral Test for Convergence

If f is a positive, continuous, decreasing function of a real variable $x \geq 1$ and $a_j = f(j)$, then

$$\sum_{j=1}^{\infty} a_j \text{ and } \int_1^{\infty} f(x)dx$$

either both converge or both diverge.

Theorem B.4 — Convergence of Geometric Series
The geometric series

$$\sum_{j=0}^{\infty} ar^j$$

diverges if $|r| \geq 1$. If $0 < |r| < 1$, the series converges to the sum

$$\sum_{j=0}^{\infty} ar^j = \frac{a}{1-r}.$$

Also, for any $r \neq 1$, the n^{th} partial sum of the geometric series is given by

$$S_n = \sum_{j=0}^{n} ar^j = \frac{a(1-r^{n+1})}{1-r}.$$

Theorem B.5 — Direct Comparison Test
Suppose that $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ are infinite series such that $0 \leq a_j \leq b_j$ for all $j \in \mathbb{N}$. Then

$$\sum_{j=1}^{\infty} a_j \text{ converges if } \sum_{j=1}^{\infty} b_j \text{ converges.}$$

Note that the contrapositive is:

$$\sum_{j=1}^{\infty} b_j \text{ diverges if } \sum_{j=1}^{\infty} a_j \text{ diverges.}$$

Definition B.3 — Harmonic Series and p-Series
A series of the form

$$\sum_{j=1}^{\infty} \frac{1}{j^p} = \frac{1}{1^p} + \frac{1}{2^p} + \cdots + \frac{1}{j^p} + \cdots$$

is called a p-series, where $p \in \mathbb{R}^+$ is constant. If $p = 1$, then

$$\sum_{j=1}^{\infty} \frac{1}{j} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{j} + \cdots$$

is called a harmonic series.

Theorem B.6 — Convergence of p-Series
The series $\sum_{j=1}^{\infty} \frac{1}{j^p}$ converges for $p > 1$ and diverges for $0 < p \leq 1$.

Theorem B.7 — Limit Comparison Test
Let $a_j > 0$, $b_j > 0$ and

$$\lim_{n \to \infty} \left(\frac{a_j}{b_j} \right) = L \in \mathbb{R}^+.$$

Then $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ both converge, or they both diverge.

Definition B.4 — Alternating Series

An infinite series of the form

$$\sum_{j=1}^{\infty}(-1)^j a_j \text{ or } \sum_{j=1}^{\infty}(-1)^{j+1}a_j,$$

with $a_j > 0$, is called an *alternating series.*

Biography B.1 The fact that the harmonic series diverges was first discovered by Nicolae Oresme in the fourteenth century. His birth year is unknown with any degree of certainty by historians, but most set it at 1323. There is also some disagreement as to where he was born, but most data supports that it was somewhere near Caen, France, if not in Caen itself. He was a Parisian scholar, who studied theology, and became bursar at the University of Paris. Later he became canon, then dean of Rouen. In 1370, he was appointed chaplain to King Charles V, advising the King on spiritual as well as financial matters. Oresme was also the among the first, even before Descarte, to use a coordinate system for graphing, incorporating such ideas as velocity-time graphs. He suggested a three-dimensional generalization of the concept in his work *Tractatus de Figuratione Potentarium et Mensurarum.* The work contained implicit suggestions of a four-dimensional geometry, but analytic geometry was not yet developed to take him further. In his *Algorismus Proportionum*, Oresme developed the idea of fractional powers. He suggested that irrational exponents such as, in modern notation, $x^{\sqrt{2}}$ are possible. This was undoubtedly the first appearance of the notion of a higher transcendental function. However, he did not have enough development of either notation or terminology to take the notion very far. Oresme's ingenious idea for proving the divergence of the harmonic series was to group successive terms in the series placing the first term in the first group, the next two terms in the second group, the next four in the third group, continuing so that the n^{th} group has 2^{n-1} terms. He then deduced that since there are infinitely many groups with each group having a sum of at least 1/2, then adding together enough terms, one can achieve a number larger than any given number. Oresme ultimately became the Bishop of Lisieux, France and died there on July 11, 1382.

Theorem B.8 — Alternating Series Test

The alternating series

$$\sum_{j=1}^{\infty}(-1)^j a_j \text{ and } \sum_{j=1}^{\infty}(-1)^{j+1}a_j, \text{ with } a_j > 0 \text{ for all } j \in \mathbb{N}$$

converge if both $\lim_{j\to\infty} a_j = 0$ and $a_1 > a_2 > a_3 > \cdots$.

Theorem B.9 — Absolute and Conditional Convergence

If the series

$$\sum_{j=1}^{\infty}|a_j|$$

converges, then $\sum_{j=1}^{\infty} a_j$ converges and we call $\sum_{j=1}^{\infty} a_j$ is *absolutely convergent.* On the other hand, if $\sum_{j=1}^{\infty} a_j$ converges, but $\sum_{j=1}^{\infty} |a_j|$ diverges, we say that $\sum_{j=1}^{\infty} a_j$ is *conditionally convergent.*

Remark B.2 If an infinite series is absolutely convergent, then its terms can be rearranged in any order without changing the sum of the series. On the other hand, if a series is conditionally convergent, then the series can be rearranged to give a *different sum.*

Theorem B.10 — Ratio Test
If $\sum_{j=1}^{\infty} a_j$ is an infinite series, with $a_j \neq 0$ for all $j \in \mathbb{N}$, then each of the following holds.

(a) $\sum_{j=1}^{\infty} a_j$ is absolutely convergent if

$$\lim_{j\to\infty} \left| \frac{a_{j+1}}{a_j} \right| < 1.$$

(b) $\sum_{j=1}^{\infty} a_j$ diverges if

$$\lim_{j\to\infty} \left| \frac{a_{j+1}}{a_j} \right| > 1 \text{ or } \lim_{j\to\infty} \left| \frac{a_{j+1}}{a_j} \right| = \infty.$$

Theorem B.11 — Root Test
Let $\sum_{j=1}^{\infty} a_j$ be an infinite series. Then each of the following holds.

(a) If $\lim_{j\to\infty} \sqrt[n]{|a_j|} < 1$, then $\sum_{j=1}^{\infty} a_j$ is absolutely convergent.

(b) If $\lim_{j\to\infty} \sqrt[n]{|a_j|} > 1$ or $\lim_{j\to\infty} \sqrt[n]{|a_j|} = \infty$, then $\sum_{j=1}^{\infty} a_j$ diverges.

The simplest and most important of the infinite series are the following, with which we will be most concerned in the main text.

✦ **Power Series**

Definition B.5 — Power Series
If x is a real variable, then

$$\sum_{j=0}^{\infty} a_j (x-c)^j$$

is called a *power series* centered at $c \in \mathbb{R}$.

Theorem B.12 — Convergence of Power Series
If $\sum_{j=0}^{\infty} a_j (x-c)^j$ is a power series, then exactly one of the following holds.

(a) The series is absolutely convergent for all $x \in \mathbb{R}$.

(b) The series converges only for $x = c$.

(c) There exists an $R \in \mathbb{R}$ such that the series is absolutely convergent for $|x - c| < R$, and diverges for $|x - c| > R$.

The value R is called the *radius of convergence* of the series. Thus, in part (a), $R = \infty$ and in part (b), $R = 0$. In part (c), the real interval $(c - R, c + R)$ is called the *interval of convergence* of the series.

Theorem B.13 — Abel's Theorem

If the radius of convergence of the power series $\sum_{j=0}^{\infty} a_j x^j$ is R and

$$\sum_{j=0}^{\infty} a_j R^j$$

is convergent, then

$$\lim_{x \to R} \left(\sum_{j=0}^{\infty} a_j x^j \right) = \sum_{j=0}^{\infty} a_j R^j.$$

Corollary B.12 If $R = 1$ and $\sum_{j=0}^{\infty} a_j$ is convergent, then

$$\lim_{x \to 1} \left(\sum_{j=0}^{\infty} a_j x^j \right) = \sum_{j=0}^{\infty} a_j.$$

Application B.1 — Hyperbolic Tangent

Consider the infinite series $1 - t^2 + t^4 - t^6 + \cdots$ the sum of which for $|t| < 1$ is $(1 + t^2)^{-1}$. Integrating termwise for $-1 < x < 1$, we get

$$\arctan(x) = \int_0^x \frac{dt}{1 + t^2} = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots$$

which implies that

$$\lim_{x \to 1} \arctan(x) = \tan^{-1}(1) = \frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \cdots$$

which is the formula for π discovered by Gregory—see Biography B.2 on the facing page.

Of particular importance is the following.

Theorem B.14 — Taylor and Maclaurin Polynomials and Series

If a function f of a real variable x has derivatives $f^{(j)}$ for $j = 1, 2, \ldots n$ at c, then

$$P_n(x) = \sum_{j=0}^{n} \frac{f^{(j)}(c)}{j!}(x - c)^j$$

is called the n^{th} *Taylor polynomial for f at c*. If $c = 0$, then it is called the n^{th} *Maclaurin polynomial for f*.

If f has derivatives of all orders at c, then the series

$$\sum_{j=0}^{\infty} \frac{f^{(j)}(c)}{j!}(x - c)^j$$

is called the *Taylor series for f at c*. If $c = 0$, then the series is called the *Maclaurin series for f*.

Biography B.2 Colin Maclaurin (1698–1746) is known today almost exclusively for the series that bears his name, namely $f(x) = \sum_{j=0}^{\infty} f^{(j)}(0)x^j/j!$, where $f^{(j)}$ is the j^{th} derivative of the function f—see Theorem B.14. This series appeared in his *Treatise of Fluxions* in 1742. However, it is a special case of the more general Taylor series published by the secretary of the Royal Society, Brook Taylor (1685–1731) in his *Methodus Incrementorum* of 1715. However, this series was known long before by the Scotsman James Gregory (1638–1675), although Taylor was not aware of this. Furthermore, the series appeared in *Methodus differentialis* by Stirling more than a decade before Maclaurin's publication—see Biography A.2 on page 340. There is also evidence that this series was known to Indian mathematicians such as Kelallur Nilakantha Somayaji (1444–1544). It is somewhat ironic that Maclaurin is known for the above series, when he had deep results of his own in geometry. Maclaurin is considered by many historians to be the most outstanding of the generation of British mathematicians after Newton. He was born in Argyllshire, Scotland, and was educated at Glasgow. He was Professor at Marischal College, Aberdeen from 1717 to 1725, then at the University of Edinburgh from 1725 until 1745. In 1740, he shared a prize from the Académie des Sciences, with Euler and Daniel Bernoulli, for a study of tides—see Biography 4.7 on page 161. The irony of attribution is compounded by the fact that a discovery made by Maclaurin in 1729 is credited to Gabriel Cramer (1704–1752)—see Theorem A.21 on page 337. Maclaurin was also actively involved in the defense of Edinburgh during the Jacobite rebellion of 1745, and fled the city for York when it fell to "Bonnie Prince Charlie." The war in the trenches had taken its toll on him however. He died the next year on June 14, 1746 in Edinburgh. Maclaurin's *Treatise of Algebra* was published posthumously in 1748.

Definition B.6 — Remainder of a Taylor Polynomial

If f is a function of a real variable x and $P_n(x)$ is the n^{th} Taylor polynomial for f at c, then

$$R_n(x) = f(x) - P_n(x)$$

is called the n^{th} remainder of $f(x)$.

Lagrange's form of the remainder of a Taylor polynomial is given in the following—see Biography 3.3 on page 93.

Theorem B.15 — Taylor's Theorem

If f is a function such that $f^{(j)}$ exists for $j = 1, 2, \ldots, n+1$ in an interval I containing c, then for all $x \in I$, there exists a z between x and c such that

$$f(x) = \sum_{j=0}^{n} \frac{f^{(j)}(c)}{j!}(x-c)^j + R_n(x),$$

where

$$R_n(x) = \frac{f^{(n+1)}(z)}{(n+1)!}(x-c)^{n+1}.$$

Theorem B.16 — Convergence of a Taylor Series
Let f be a function having derivatives of all orders in an open interval I centered at c. Then

$$f(x) = \sum_{j=0}^{\infty} \frac{f^{(j)}(c)}{j!}(x-c)^j$$

if and only if there exists a z between x and c such that

$$\lim_{n\to\infty} R_n(x) = \lim_{n\to\infty} \frac{f^{(n+1)}(z)}{(n+1)!}(x-c)^{n+1} = 0,$$

for all $x \in I$.

The following formulas will be very useful throughout the main text.

✦ — **Power Series for some Elementary Functions**
In what follows, the interval for x given for each series is the interval of convergence.

B.1. $\frac{1}{x} = \sum_{j=0}^{\infty}(-1)^j(x-1)^j = 1-(x-1)+(x-1)^2 - \cdots$ with $x \in (0,2)$.

B.2. $\log(1+x) = \sum_{j=1}^{\infty} \frac{(-1)^{j-1}(x)^j}{j} = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$ with $x \in (-1,1]$.

B.3. $e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$ with $x \in \mathbb{R}$.

B.4. $\sin(x) = \sum_{j=0}^{\infty} \frac{(-1)^j x^{2j+1}}{(2j+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots$ with $x \in \mathbb{R}$.

B.5. $\cos(x) = \sum_{j=0}^{\infty} \frac{(-1)^j x^{2j}}{(2j)!} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots$ with $x \in \mathbb{R}$.

B.6. $e^{\sin(x)} = 1 + x + \frac{x^2}{2!} - \frac{3x^4}{4!} - \frac{8x^5}{5!} - \frac{3x^6}{6!} + \frac{56x^7}{7!} + \cdots$ with $x \in \mathbb{R}$.

The following notion brings series into the realm of the complex numbers $\mathbb{C}$ and allows us to introduce important fundamental results to be used in the main text. For instance, we presented the connection with Bernoulli numbers in Theorem 4.5 on page 156.

Definition B.7 — Dirichlet Series—The Riemann Zeta Function
Dirichlet series is an infinite series of the form

$$\sum_{j=1}^{\infty} a_j e^{-s\lambda_j},$$

where $a_j, s \in \mathbb{C}$, $\lambda_j \in \mathbb{R}$, and the sequence $\{\lambda_j\}$ tends monotonically to infinity. In particular, if $\lambda_j = \log(j)$, and $a_j = 1$ for all $j \in \mathbb{N}$, then

$$\zeta(s) = \sum_{j=1}^{\infty} j^{-s}$$

is called the *Riemann zeta function*—see page 155.

Biography B.3 Georg Friedrich Bernhard Riemann (1826–1866) was born on September 17, 1826 in Breselenz, Hanover (now Germany). He was the son of a Lutheran pastor, and his family was relatively poor. Moreover, he was physically frail, but what he lacked in physical strength, he more than made up in intellectual acuity. Furthermore, his lack of financial wealth did not prevent him from getting a strong education. In 1846, he studied under Jacobi, Dirichlet, and Eisenstein at Berlin, went to Göttingen in 1849 to study under Gauss, and achieved his Ph.D. in 1851. In 1854, he became *Privatdozent* at the University of Göttingen. His *Habilitationschrift* or *inaugural dissertation* was given on his thesis entitled *Über die Hypothesen welche der Geometrie zu Grunde liegen* or *On the hypotheses which lie at the foundation of geometry.* This presented such a deep general perception of geometry that its results ultimately made way for Einstein's theory of general relativity, since Riemann proposed the general study of curved metric spaces, rather than geometry on a sphere. His ultimate contributions to theoretical physics were deep, and long-lasting. In 1859, after the death of Dirichlet, Riemann was appointed to fill his chair at Göttingen. Riemann's name is attached to a host of mathematical objects and theorems including the Riemann integral, the Riemann surface, Riemannian geometry, the Riemann mapping theorem, Riemann manifolds, and the still unresolved Riemann hypothesis—see Hypothesis B.1 on the following page—to mention a few. Riemann married at the age of thirty-six in 1862. The following month he became ill with pleurisy, which ultimately turned into pulmonary tuberculosis. He travelled to Italy several times to enjoy the milder climate and recover. On his final trip, he went to a villa at Selasca, Lake Maggiore in Italy. He died with his wife by his side on July 20, 1866.

The Riemann zeta function converges for $\Re(s) > 1$. If $\Re(s) > 1$, then the following is called *Euler's identity*

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

where the product runs over all primes p. Although we shall not explicitly need the following facts in the text, we state them here for the reader with knowledge of complex analysis. The function $\zeta(s)$ is a holomorphic function in the half plane $\Re(s) > 1$, and can be continued analytically to a meromorphic function on the whole plane. Its unique singularity is the point $s = 1$ at which it has a simple pole with residue 1. Riemann proved the above in 1859.

There is also a classical connection of the zeta function with the following concept.

Definition B.8 — Gamma Functions

The *gamma function* is given by

$$\Gamma(s) = s^{-1}e^{-\gamma s}\prod_{j=1}^{\infty}\left(1 + \frac{s}{j}\right)^{-1} e^{s/j},$$

where

$$\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n)\right)$$

is called *Euler's constant.* For $\Re(s) > 0$, we may write

$$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}dx.$$

The following application will be useful in text. The Gamma function is used to verify the following—see [54, Exercise 10.13, p. 345], for instance.

Application B.2 —Infinite Product Expansion for Sine

$$\sin(x) = x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right),$$

The following relationship between the zeta function and the gamma function is called *the functional equation of the zeta function*, proved by Riemann in 1859.

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s).$$

As a result of the functional equation, it is known that all the nontrivial zeros of $\zeta(s)$ (namely those for which $s \neq -2, -4, -6 \ldots$) must lie in the *critical strip* $0 < \Re(s) < 1$, and that they are located symmetrically about the *critical line* $\Re(s) = 1/2$. However, heretofore nobody has been able to prove Riemann's contention:

Hypothesis B.1 — The Riemann Hypothesis

$\zeta(s) \neq 0$ for any s with $\Re(s) > 1/2$.

Proofs of the above results may be found in [54, Theorem 5.15, p. 225] and the discussion surrounding it therein.

Some of the history behind the zeta function is worthy of note. In 1731, Euler had done calculations that allowed him to conclude that $\zeta(2) \sim 1.644934$, and later got stronger approximations. By 1734, Euler had proved that

$$\zeta(2) = \pi^2/6.$$

He had communicated with Daniel Bernoulli on his early successes in 1734. Daniel found Euler's discoveries to be "remarkable." In 1737, after the successful calculation of $\zeta(2)$ under his belt, Euler published *Variae Observationes circa series infinitas*, which contained the now-famous *Euler product*:

$$\zeta(s) = \frac{2^s \cdot 3^s \cdot 5^s \cdot 7^s \cdot 11^s \cdots}{(2^s-1)(3^s-1)(5^s-1)(7^s-1)(11^s-1)\cdots}.$$

Also contained in that paper, he established (in modern notation) that as $x \to \infty$, then

$$\sum_{p \leq x} \frac{1}{p} = \log\log(x) + C + \mathrm{O}\left(\frac{1}{\log(x)}\right),$$

where C is a constant.[B.2] By 1740 Euler had determined $\zeta(2n)$ for any $n \in \mathbb{N}$—see Theorem 4.5 on page 156. However, for odd integers n, $\zeta(n)$ remains a mystery. In attempts to solve the problem, Euler was led to the following result, which he published in a paper called *Exercitationes Analyticae* in 1772,

$$1 + \frac{1}{3^3} + \frac{1}{5^3} + \cdots = \frac{\pi^2}{4}\log(2) + 2\int_0^{\pi/2} x \log(\sin(x))dx.$$

What is all the more amazing is that Euler was blind by this time and all the calculations were done mentally. For further details on the life of Leonard Euler—see Biography 4.4 on page 148.

[B.2] We remind the reader that the *big* O notation is defined by $f(x) = \mathrm{O}(g(x))$, for positive real-valued functions f and g, provided there exists an $r \in \mathbb{R}$ such that $f(x) < rg(x)$.

Appendix C

The Greek Alphabet

Timeo Danaos et dona ferentes: I fear the Greeks though bearing gifts.
Virgil (Publius Vergilius Maro) (70–19 B.C.)
Roman poet

Capital	Lower-case	English transliteration	Pronunciation
A	α	a	alpha
B	β	b	beta
Γ	γ	g	gamma
Δ	δ	d	delta
E	ϵ	e	epsilon
Z	ζ	z	zeta
H	η	ē	eta
Θ	θ	th	theta
I	ι	i	iota
K	κ	k	kappa
Λ	λ	l	lambda
M	μ	m	mu as in *mew*
N	ν	n	nu as in *new*
Ξ	ξ	x	xi as in *ksee*
O	o	o	omicron
Π	π	p	pi as in *pie*
P	ρ	r	rho as in *row*
Σ	σ	s	sigma
T	τ	t	tau as in *towel*
Υ	υ	y	upsilon
Φ	ϕ	ph	phi as in *fee*
X	χ	ch	chi as in *cheye*
Ψ	ψ	ps	psi as in psee
Ω[C.1]	ω	õ	omega

The ē denotes a *long* e as in *see*, as opposed to the *short* e as in *bed.* The symbol õ is used here to mean an o as in *boring*, somewhat longer than the o in omicron, but not as long as the long o in *too.* The *pronunciations* given here are those used by English-speaking people. The Greeks have (sometimes) different pronunciations for the letters. For instance, the Greeks pronunciation of α is the same as given above, but the Greek pronunciation of β is *vita.* Thus, the difference between the conventional ones, given in the column above, may vary from the *real* ones used by the Greeks themselves.

[C.1] "I am the Alpha and the Omega, the first and the last, the beginning and the end." (Revelation 22:VII) of the Holy Bible.

Appendix D

Latin Phrases

> *amicus certus in re incerta cernitur: a true friend is certain when certainty is uncertain—i.e., a friend in need is a friend indeed.*
>
> **Latin proverb spoken by Ennius (239–169 B.C.)**
> Roman writer

Latin Phrase	English equivalent
abeunt studia in mores	practices, zealously pursued, pass into habits
ab uno disce omnes	from one, learn to know all
ad arbitrium	at will (arbitrarily)
ad extremum	to the extreme (at last)
ad hoc	to this (for a particular purpose)
ad infinitum	without limit (to infinity)
ad libitum (ad lib)	improvise
aere perennius	more lasting than bronze
a fortiori	from the stronger (argument) meaning: with greater reason — used in drawing a conclusion that is deemed to be even more certain than another
alea jacta est	the die is cast
a maximis ad minima	from the greatest to the least
animis opibusque parati	prepared in mind and resources
arrectis auribus	with pricked-up ears (attentively)
aurea mediocritas	the golden mean
bonis avibus	under good auspices
cadit quaestio	the question drops, meaning the argument fails
cetera desunt	the rest is missing
cogito ergo sum	I think, therefore I am (exist)
divide et impera	divide and rule
docendo discimus	we learn by teaching
ecce signum	behold the sign (look at the proof)
e contrario	on the contrary
exempli gratia (e.g.)	for example
e pluribus unum	one out of many
et sic de similibus	and so of like things
excelsior	still higher
exceptis excipiendis	with the necessary exceptions
ex necessitate rei	from the necessity of the case
ex nihilo nihil fit	from nothing comes nothing
ex vi termini	from the force of the term
facile princeps	easily first
finem respice	consider the end

Latin Phrase	English equivalent
finis coronat opus	the end crowns the work
hoc opus	this is the hard work
id est (i.e.)	that is
in aeternum	forever
in dubio	in doubt (undetermined)
in vino veritas	there is truth in wine
in vivo	in a living thing, or in the body of a work
janius clausis	behind closed doors
lapsus calami	slip of the pen
lapsus linguae	slip of the tongue
littera scripta manet	the written letter abides
locus in quo	place in which
magna est veritas et praevalebit	truth is mighty and will prevail
mirabile visu	wonderful to behold
multum in parvo	much in little
mutatis mutandis	with necessary changes made
ne quid nimis	nothing in excess
non sequitur	a conclusion that does not logically follow from the premises
nosce te ipsum	know thyself
nugae	trifles
obscurum per obscurius	(explaining) the obscure by the more obscure
onus probandi	burden of proof
si vis pacem para bellum	if you wish peace, prepare for war
sic	so, thus[D.1]
sine qua non	an indispensable condition
status quo	state in which (the existing state)
suo loco	in its proper place
tempus fugit	time flies
uno animo	with one mind (unanimously)
vincit omnia veritas	truth conquers all things

[D.-1] In the current vernacular, this is used to mean “You scratch my back and I’ll scratch yours.”

[D.0] This refers to a method of proof, which assumes the contrary of a hypothesis to be proved, and deduces an absurd consequence.

[D.1] This is used to mean *intentionally so written. Sic* is used after a quote, calling attention to it, in order to indicate that it really does reproduce the original, or in the current vernacular, “Yes, they *really* did say that.”

Bibliography

[1] L.M. Adleman, C. Pomerance, and R.S. Rumely, *On distinguishing prime numbers from composite numbers*, Annals of Math. **117** (1983), 173–206. (*Cited on page 259.*)

[2] D. Atkins, M. Graff, A.K. Lenstra, and P.C. Leyland, *The magic words are SQUEAMISH OSSIFRAGE* in **Advances in Cryptology** — ASIACRYPT '94, Springer-Verlag, Berlin, LNCS **917**, (1995), 263–277. (*Cited on page 169.*)

[3] B.C. Berndt, R.J. Evans, and K.S. Williams, **Gauss and Jacobi Sums**, C.M.S. Series **21**, Wiley, New York, Toronto (1998). (*Cited on pages 275–276, 282, 288, 293, 310.*)

[4] M. Bhargava, *Higher composition laws and applications* in International Congress of Mathematicians. Vol. II, 271–294, Eur. Math. Soc., Zrich, (2006). (*Cited on page 98.*)

[5] Z.I. Borevich and I.R. Shafarevich, **Number Theory**, Academic Press, New York, London (1966). (*Cited on page 240.*)

[6] J. Brillhart, *Concerning the numbers* $2^{2p}+1$, p *a prime*, Math. Comp. **16** (1962), 424–430. (*Cited on page 290.*)

[7] J.P. Buhler, H.W. Lenstra Jr., and C. Pomerance, *Factoring integers with the number field sieve*, in **The Development of the Number Field Sieve**, A.K. Lenstra and H. W. Lenstra Jr. (Eds.), Lecture Notes in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York **1554** (1993), 50–94. (*Cited on page 174.*)

[8] K. Burde, *Ein rationales biquadratisches Reciprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175–184. (*Cited on page 288.*)

[9] O.A. Cámpoli, *A principal ideal domain that is not a Euclidean domain*; Amer. Math. Monthly **95** (1988), 868–871. (*Cited on page 14.*)

[10] J.W.S. Cassels and A. Fröhlich, **Algebraic Number Theory**, Academic Press, London and New York (1967). (*Cited on page 316.*)

[11] G. Chrystal, **Algebra**, **Vol. I**, AMS Chelsea (1964). (*Cited on page 278.*)

[12] M.J. Collison, *The origins of the cubic and biquadratic reciprocity laws*, Arch. Hist. Exact Sci. **17** (1977), 63–69. (*Cited on page 262.*)

[13] D. Coppersmith, A. Odlyzko, and R. Schroeppel, *Discrete logarithms in* $GF(p)$, Algorithmica **I** (1986), 1–15. (*Cited on page 174.*)

[14] Ellen Carney, **A Biography of Flora Whittemore**, Maverick Publications (1990). (*Cited on page 278.*)

[15] D.A. Cox, **Primes of the Form $\mathbf{x^2 + ny^2}$**, Wiley, New York, (1989). (*Cited on pages 90, 244, 316.*)

[16] J.A. Davies, D.B. Holdridge, and G.L. Simmons, *Status report on factoring* (*at Sandia National Labs*) in **Advances in Cryptology** — EUROCRYPT '84, Springer-Verlag, Berlin, LNCS **209**, (1985), 183–215. (*Cited on page 169.*)

[17] R. Evans, *Pure Gauss sums over finite fields*, Mathematika **28** (1981), 239–248. (*Cited on page 405.*)

[18] L. Euler,**Opera Omnia**, Series prima, Vols. I–V, Teubener, Leipzig and Berlin, 1911–1944. (*Cited on page 272.*)

[19] C.F. Gauss, **Werke**, Volume II, Königlichen Gesellschaft der Wissenschaften, Göttingen (1876). (*Cited on page 278.*)

[20] C.F. Gauss, **Disquisitiones Arithmeticae** (English edition), Springer-Verlag, Berlin, Heidelberg, New York (1985). (*Cited on pages 40, 95.*)

[21] J. Gerver, *Factoring large numbers with a quadratic sieve*, Math. Comp. **41** (1983), 287–294. (*Cited on page 169.*)

[22] T. Gosset, *On the quartic residuacity of* $1 + i$, Mess. Math. **40** (1910), 165–169. (*Cited on page 290.*)

[23] M.J. Greenberg, *An elementary proof of the Kronecker-Weber theorem*, Amer. Math. Monthly, **81** (1974), 601–607. (*Cited on page 252.*)

[24] M.J. Greenberg, *Correction to "An elementary proof of the Kronecker-Weber theorem,"* Amer. Math. Monthly, **82** (1975), 803. (*Cited on page 252.*)

[25] J. Greene, *Principal ideal domains are almost Euclidean*, Amer. Math. Monthly **104** (1997), 154–156. (*Cited on pages 14, 34.*)

[26] R. Harris, **Lustrum**, Hutchinson, London (2009). (*Cited on page 65.*)

[27] David Hilbert, **The Theory of Algebraic Number Fields** (English translation–Translated by I. Adamson), Springer-Verlag, Berlin, Heidelberg, New York (1998). (*Cited on page 254.*)

[28] L.K. Hua, **Introduction to Number Theory**, Springer-Verlag, Berlin, Heidelberg, New York (1982). (*Cited on page 339.*)

[29] T.W. Hungerford, **Algebra**, Springer, New York (1974). (*Cited on page 62, 319, 323, 328.*)

[30] F. Hirzebruch, *Hilbert modular surfaces*, L'Enseignment Math. **19** (1973), 183–281. (*Cited on page 307.*)

[31] P. Indyk and S. Szarek, *A simple construction of almost-Euclidean subspaces of* ℓ_1^N *via tensor products*, Preprint 2009. See *http://arxiv.org/pdf/1001.0041.* (*Cited on page 14.*)

[32] K. Ireland and M. Rosen, **A Classical Introduction to Algebraic Number Theory**, Second Edition, Springer-Verlag, Berlin, Heidelberg, New York (1990). (*Cited on page 262.*)

[33] G.J. Janusz, **Algebraic Number Fields**, AMS Graduate Studies in Math. **7** (1996). (*Cited on page 240.*)

[34] M. Kraitchik, **Mathematical Recreations**, Dover, New York (1953). (*Cited on page 173.*)

[35] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Annalen **56** (1903), 671–676. (*Cited on page 91.*)

[36] D.H. Lehmer, **Selected Papers of D.H. Lehmer**, Volumes I–III, (D. McCarthy (Ed.)), The Charles Babbage Research Centre, St. Pierre, Canada (1981). (*Cited on page 259.*)

[37] D.H. Lehmer and R.E. Powers, *On factoring large numbers*, Bull. Amer. Math. Soc. **37** (1931), 770–776. (*Cited on page 167.*)

[38] F. Lemmermeyer, **Reciprocity Laws: Their Evolution from Euler to Artin**, Springer, Berlin, Heidelberg (2009). (*Cited on pages 290, 309, 313, 316, 406.*)

[39] A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse, and J.M. Pollard, *The number field sieve*, in **The Development of the Number Field Sieve**, A.K. Lenstra, and H. W. Lenstra Jr. (Eds.), Lecture Notes in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York **1554** (1993), 11–42. (*Cited on pages 174–175, 177.*)

[40] A.K. Lenstra and M.S. Manasse, *Factoring by electronic mail* in **Advances in Cryptology** — EUROCRYPT '89, Springer-Verlag, Berlin, LNCS **434**, (1990), 355–371. (*Cited on page 169.*)

[41] A.K. Lenstra, H.W. Lenstra, M.S. Manasse, and J.M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349. (*Cited on pages 174, 177, 179–180.*)

[42] H.W. Lenstra Jr., *Primality testing with Artin Symbols*, in **Number Theory Related to Fermat's Last Theorem**, Neil Koblitz, (ed.), **Progress in Math. 26**, Birkhäuser, Boston, Basel, Stuttgart (1982), 341–347. (*Cited on pages 255, 258.*)

[43] R. Lidl and H. Niederreiter, **Finite Fields**, Addison Wesley, Reading, Mass., (1983) (Second edition, Cambridge University Press, 1997). (*Cited on page 276.*)

[44] R. MacKenzie and J. Scheuneman, *A number field without a relative integral basis*, Amer. Math. Monthly **78** (1971), 882–883. (*Cited on page 79.*)

[45] C.R. Matthews, *Gauss sums and elliptic functions. I: The Kummer sum*, Invent. Math. **52** (1979), 163–185; *II: The Quartic sum* **54** (1979), 23–52. (*Cited on page 292.*)

[46] R.A. Mollin, *An elementary proof of the Rabinowitch-Mollin-Williams criterion for real quadratic fields*, J. Math. Sci. **7** (1996), 17–27. (*Cited on page 143.*)

[47] R.A. Mollin, **Number Theory and Applications**, Proceedings of the NATO Advanced Study Institute, Banff Centre, Canada, 27 April–5 May 1988, Kluwer Academic Publishers, Dordrecht (1989). (*Cited on page xiii.*)

[48] R.A. Mollin, **Number Theory**, Proceedings of the First Conference of the Canadian Number Theory Association, Banff Centre, Canada, April 17–27, 1988, Walter de Gruyter, Berlin (1990). (*Cited on page xiii.*)

[49] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, London, Tokyo (1995). (*Cited on pages 48, 53, 99, 136, 138, 273, 277, 307.*)

[50] R.A. Mollin, **Fundamental Number Theory with Applications**, *First Edition*, CRC, Boca Raton, London, New York (1998). (*Cited on pages 48, 273, 330, 339, 341.*)

[51] R.A. Mollin, **An Introduction to Cryptography**, Second Edition, CRC, Taylor & Francis Group, Boca Raton, London, New York (2007). (*Cited on pages 165–166.*)

[52] R.A. Mollin, **Codes: The Guide to Secrecy from Ancient to Modern Times**, CRC, Taylor & Francis Group, Boca Raton, London, New York (2008). (*Cited on page 180, 344.*)

[53] R.A. Mollin, **Fundamental Number Theory with Applications**, *Second Edition*, CRC, Taylor & Francis Group, Boca Raton, London, New York (2008). (*Cited on pages 4, 8, 87, 92, 120–121, 138, 156, 158, 174, 180, 255–257, 298, 343, 398.*)

[54] R.A. Mollin, **Advanced Number Theory with Applications**, CRC, Taylor & Francis Group, Boca Raton, London, New York (2009). (*Cited on pages ix, 12–13, 15, 20, 35, 87, 121, 139, 149, 157, 169, 174, 213, 220, 255, 340, 354.*)

[55] L.J. Mordell, *Reminiscences of an octogenarian mathematician*, Amer. Math. Monthly **78** (1971), 952–961. (*Cited on page 144.*)

[56] L.J. Mordell, **Diophantine Equations**, Academic Press, London and New york (1969). (*Cited on page 148.*)

[57] B. Oriat, *Annulation de groupes de classes réelles*, Nagoya Math. J. **81** (1981), 45–56. (*Cited on page 310.*)

[58] J.M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349. (*Cited on page 170.*)

[59] C. Pomerance, *The quadratic sieve factoring algorithm* in **Advances in Cryptology** — EUROCRYPT '84, Springer-Verlag, Berlin, LNCS **209**, (1985), 169–182. (*Cited on page 167.*)

[60] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfactoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. **142** (1913), 153–164. (*Cited on pages 143–144.*)

[61] T.-S. Rhai, *A characterization of polynomial domains over a field*, Amer. Math. Monthly **69** (1962). 984–986. (*Cited on page 11.*)

[62] L.T. Rigatelli, **Evariste Galois**, Birkhäuser Verlag, Basel, Boston,Berlin, English translation (1996). (*Cited on page 64.*)

[63] W.L. Schaff, **Mathematics Our Great Heritage**, Harper and Brothers, New York (1948). (*Cited on pages 70, 83.*)

[64] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. **32** (1846), 93–105. (*Cited on page 332.*)

[65] T. Schönemann, *Notiz*, J. Reine Angew. Math. **40** (1850), 188. (*Cited on page 332.*)

[66] C.L. Siegel, *Zu zwei Bemerkungen Kummers*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. **II** (1964), 51–57. (*Cited on page 154.*)

[67] D. Teets and K. Whitehead, *The discovery of Ceres: How Gauss became famous*, Math. Magazine **72** (1999), pp. 83–91. (*Cited on page 95.*)

[68] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. **128** (1988), 1–18. (*Cited on page 310.*)

[69] L.C. Washington, **Introduction to Cyclotomic Fields**, Graduate Texts in Math. **83**, Second edition, Springer-Verlag, Berlin, Heidelberg, New York (1997). (*Cited on page 310.*)

[70] A. Wiles, *On a conjecture of Brumer*, Ann. of Math. **131** (1990), 555–565. (*Cited on page 310.*)

[71] H.C. Williams, **Édouard Lucas and Primality Testing**, Wiley, New York, Toronto (1998). (*Cited on pages 162, 255.*)

[72] K.S. Williams, *On Eisenstein's supplement to the law of cubic reciprocity*, Bull. Calcutta Math. Soc. **69** (1977), 311–314. (*Cited on pages 273, 286.*)

[73] D. Zagier, *A Kronecker limit formula for real quadratic fields*, Math. Ann. **213** (1975), 153–184. (*Cited on page 307.*)

Solutions to Odd-Numbered Exercises

Section 1.1

1.1 Since $\mathbb{Z}[(1+\sqrt{n})/2] \subseteq \mathbb{Q}(\sqrt{n})$, then if it is a ring, it is an integral domain. Thus, by Remark A.2 on page 323 it suffices to show that it is closed under subtraction and multiplication. Closure under subtraction is easy to see, since

$$\left(a+b\frac{1+\sqrt{n}}{2}\right)-\left(c+d\frac{1+\sqrt{n}}{2}\right)=\left(a-c+(b-d)\frac{1+\sqrt{n}}{2}\right).$$

Also, since $n \equiv 1 \pmod 4$ and

$$\left(a+b\frac{1+\sqrt{n}}{2}\right)\left(c+d\frac{1+\sqrt{n}}{2}\right)=\left(ac+bd\frac{n-1}{4}\right)+(ad+bc+bd)\,\frac{1+\sqrt{n}}{2},$$

there is closure under multiplication. For $\mathbb{Z}[\sqrt{n}]$ there is no need to restrict to $n \equiv 1 \pmod 4$ since we are dealing only with elements of the form $a+b\sqrt{n}$ with $a,b \in \mathbb{Z}$. Hence, the above argument works in the same fashion to show it is an integral domain as well.

1.3 If $\alpha \in \mathfrak{U}_{\mathbb{Z}[\omega_n]}$, there exist $\alpha,\beta \in \mathbb{Z}[\omega_n]=D$ such that $\alpha\beta=1$. So $N(\alpha\beta)=N(1)=1$. But since $N(\alpha\beta)=N(\alpha)N(\beta)$ by Exercise 1.2, then $N(\alpha)=\pm 1$. Conversely, if $N(\alpha)=\pm 1$, then $\alpha=a+b\sqrt{n}$ where $2a, 2b \in \mathbb{Z}$, and hence $a^2-b^2n=\pm 1$. Thus, $\beta=a-b\sqrt{n}\in D$ and $\alpha\beta=\pm 1$, so $\alpha \in \mathfrak{U}_D$.

1.5 If $\alpha=\beta_1\beta_2$ for $\beta_j \in \mathbb{Z}[\sqrt{n}]$, then $\beta_j=a_j+b_j\sqrt{n}$ with $a_j,b_j\in\mathbb{Z}$, $j=1,2$. Since

$$\beta_1\beta_2=a_1a_2+b_1b_2n+(a_1b_2+b_1a_2)\sqrt{n},$$

then

$$p=\left|(a_1a_2+b_1b_2n)^2-(a_1b_2+b_1a_2)^2n\right|=\left|(a_1^2-b_1^2n)(a_2^2-b_2^2n)\right|,$$

so

$$\left|a_j^2-b_j^2n\right|=1 \text{ for one of } j=1,2.$$

In other words, one of β_j for $j=1,2$ is a unit in $\mathbb{Z}[\sqrt{n}]$, by Exercise 1.3, so α is irreducible in $\mathbb{Z}[\sqrt{n}]$.

The converse fails. For instance $2=2+0\sqrt{10}=a+b\sqrt{10}$ is irreducible in $\mathbb{Z}[\sqrt{10}]$, but $a^2-b^2n=4$ in this case.

1.7 Let $\mathfrak{U}_D$ denote the set of units in an integral domain D. Then by $\pm 1_D \in \mathfrak{U}_D$. Also, given $\alpha,\beta \in \mathfrak{U}_D$, there exist $\alpha_1,\beta_1 \in D$ such that

$$\alpha\alpha_1=1_D \tag{S1}$$

and $\beta\beta_1=1_D$, so $\alpha\beta(\alpha_1\beta_1)=1_D$, namely $\alpha\beta\in\mathfrak{U}_D$, proving that $\mathfrak{U}_D$ is closed under multiplication. Furthermore, $\mathfrak{U}_D$ inherits the properties of associativity and commutativity from the integral domain D. Moreover, if $\alpha\in\mathfrak{U}_D$, then by (S1), $\alpha_1\in\mathfrak{U}_D$ is a multiplicative inverse of α. Hence $\mathfrak{U}_D$ is a multiplicative abelian group.

1.9 If α is irreducible and a nonunit $\beta \mid \alpha$, there is a $\gamma \in D$ such that $\alpha = \beta\gamma$. However, since α is irreducible, γ must be a unit, so $\alpha \sim \beta$. Conversely, if the only divisors of α are associates and units, any factorization $\alpha = \beta\gamma$ must be trivial. Thus, α is irreducible.

1.11 It is false. If $\alpha = 4 + \sqrt{10}$ and $\beta = 4 - \sqrt{10}$, then $N(\alpha) = N(\beta) = 6$. However, if $4+\sqrt{10} = (a+b\sqrt{10})(4-\sqrt{10})$, then $4 = 4a - 10b$ and $1 = 4b - a$. However, plugging $a = 4b - 1$ into $4 = 4a - 10b$, we get that $6b = 8$, a contradiction. Hence, $\alpha \not\sim \beta$.

1.13 Let $\alpha = 6 = 2 \cdot 3 = (6+\sqrt{30})(6-\sqrt{30})$, where $2, 3, (6 \pm \sqrt{30})$ are irreducible, but not associates of one another.

1.15 Since $u = a + bi$ is a unit if and only if $N(u) = \pm 1$ by Exercise 1.3, then $a^2 + b^2 = 1$. Hence, $(a, b) \in \{(0, \pm 1), (\pm 1, 0)\}$ implying that the units in the Gaussian integers are given by

$$\mathfrak{U}_{\mathbb{Z}[i]} = \{\pm 1, \pm i\}.$$

1.17 If γ and δ are gcds of α and β, then by (b) of the definition $\gamma \mid \delta$ and $\delta \mid \gamma$, so by Definition 1.5 on page 4, $\gamma \sim \delta$.

The ring $D = 2\mathbb{Z}$ has $2 \in D$, but 2 has no divisors in D. Hence, $2, 4 \in D$ have no greatest common divisor.

Section 1.2

1.19 Let α,β $\in D$ be nonzero elements and set

$$\mathcal{S} = \{\gamma \in D : \gamma = \sigma\alpha + \delta\beta, \text{ for some } \sigma,\delta \in D\}.$$

Since $1_D\alpha + 0 \in \mathcal{S}$ and $0 + 1_D\beta \in \mathcal{S}$, then $\mathcal{S}$ consists of more than just the zero element. If f is the Euclidean function on D, we may choose an element $\gamma_0 = \sigma_0\alpha + \delta_0\beta \in \mathcal{S}$ with $f(\gamma_0)$ as a minimum. Now let $\gamma = \sigma\alpha + \delta\beta \in \mathcal{S}$ be arbitrary. By condition (b) of Euclidean domains in Definition 1.9, there are $q, r \in D$ such that

$$\gamma = q\gamma_0 + r, \text{ with either } r = 0, \text{ or } f(r) < f(\gamma_0).$$

Since

$$r = \gamma - q\gamma_0 = \sigma\alpha + \delta\beta - q(\sigma_0\alpha + \delta_0\beta) = (\sigma - q\sigma_0)\alpha + (\delta - q\delta_0)\beta \in \mathcal{S},$$

then if $r \neq 0$, condition (b) of Euclidean domains tells us that

$$f(r) = f((\sigma - q\sigma_0)\alpha + (\delta - q\delta_0)\beta) < f(\gamma_0),$$

a contradiction to the minimality of $f(\gamma_0)$. Thus, $r = 0$, and so $\gamma = q\gamma_0$. In other words, $\gamma_0|\gamma$ for all $\gamma \in \mathcal{S}$. In particular $\gamma_0|\alpha$ and $\gamma_0|\beta$. Hence, γ_0 is a common divisor of α and β as required.

1.21 Since $1_D \mid \alpha$ for all nonzero $\alpha \in D$, then by Exercise 1.20, $\phi(1_D) \leq \phi(\alpha)$.

1.23 It is false. First we show that 3 is prime in $D = \mathbb{Z}[i]$. Since D is a UFD by Corollary 1.1 on page 13, then being prime is tantamount to being irreducible by Theorem 1.2 on page 7. So if $3 = (a+bi)(c+di)$, and $c+di$ is not a unit, then since $N(a+bi) = a^2+b^2$ and $N(3) = 9$ (with the impossibility of 3 being a sum of two squares of *nonzero* integers—see Theorem A.27 on page 343) one of c or d equals 3 and $a + bi$ is a unit, namely 3 is prime in D. This provides the counterexample since 3 is prime but its norm is 9.

1.25 We assume that D is almost Euclidean and prove that every irreducible element in D is prime. Suppose that

$$\mathcal{S} = \left\{ \sum_{\beta_j \in D} \beta_j \alpha_j \in D : \alpha_j \in D \text{ is irreducible but not prime} \right\}.$$

In other words, $\mathcal{S}$ consists of all finite linear combinations of elements in D which are irreducible but not prime. If $\mathcal{S} \neq \varnothing$, there is an element $\alpha \in \mathcal{S}$ such that $\phi(\alpha)$ has least positive value by the Well-Ordering Principle — see page 340. By property (c) of an almost Euclidean function, if $\beta \in \mathcal{S}$ which is irreducible but not prime, and α does not divide β, there exist $x, y \in D$ such that $0 < \phi(\alpha x + \beta y) < \phi(\alpha)$. However, $\alpha x + \beta y \in \mathcal{S}$ by definition, contradicting the minimality of $\phi(\alpha)$. Hence, $\alpha \bigm| \beta$ for all irreducibles $\beta \in \mathcal{S}$ that are not prime. Hence, $\alpha \sim \beta$ for all irreducibles β that are not prime.

Since α is not prime then by definition there exist $\beta_1, \beta_2 \in D$ such that $\alpha \bigm| \beta_1\beta_2$ and α does not divide β_j for $j = 1, 2$. However, there exists a β_3 such that $\beta_1\beta_2 = \beta_3\alpha$, and by the definition of $\mathcal{S}$, $\beta_1\beta_2 \in \mathcal{S}$. Let δ be an irreducible such that $\delta \bigm| \beta_1$ or $\delta \bigm| \beta_2$. Without loss of generality suppose $\delta \bigm| \beta_1$. Then if δ is not prime, from the above $\delta \sim \alpha$, so there is a unit δ_1 with $\alpha = \delta\delta_1$ and a $\delta_2 \in D$ with $\beta_1 = \delta\delta_2$. Hence, $\beta_1 = \delta_1^{-1}\alpha\delta_2$, forcing $\alpha \bigm| \beta_1$, a contradiction. We have shown that any irreducible, that divides β_1 or β_2, must be prime. If $\delta \bigm| \alpha$, then since α is irreducible, $\alpha = \delta u$ for a unit $u \in D$. But again, assuming $\delta \bigm| \beta_1$ we deduce that $\alpha \bigm| \beta_1$ as above. Hence, $\delta \bigm| \beta_3$. Given that β_1 and β_2 must be factorizable into a product of irreducibles, using the same argument as in the proof of Theorem 1.6 on page 13, we have shown that all irreducibles that divide $\beta_1\beta_2$ must divide β_3, which implies that α is a unit, a contradiction. Hence $\mathcal{S} = \varnothing$, which completes the task.

Section 1.3

1.27 Suppose that $N(\alpha) = a^2 + b^2 = p$ is prime. If $\alpha = \beta\gamma$ for $\beta,\gamma \in \mathbb{Z}[i]$, then $N_F(\beta), N_F(\gamma) \in \mathbb{Z}$, so they both divide p. Hence, one of them, say $N_F(\beta) = 1$. This means that β is a unit in $Z[i]$. Thus, any divisor of α is a unit or associate. Therefore, α is irreducible, and hence a prime in $\mathbb{Z}[i]$ by Corollary 1.1 on page 13.

Since $N(\alpha) = N(a + bi) = N(a - bi) = (a + bi)(a - bi) = p$, then p is not a prime in $\mathbb{Z}[i]$ since it is divisible by both $a + bi$ and $a - bi$, neither of which is a unit or an associate of p. Indeed, both $a + bi$ and $a - bi$ are primes in $\mathbb{Z}[i]$ by Exercise 1.22 on page 14. Also, $p \equiv 1 \pmod 4$ or $p = 2$ since a prime is a sum of two squares if and only if $p \not\equiv 3 \pmod 4$ by Theorem A.27 on page 343.

1.29 Since $0 \in R_j$ for all $j \in \mathcal{J}$, then $0 \in \cap_{j \in \mathcal{J}} R_j$, so $\cap_{j \in \mathcal{J}} R_j \neq \varnothing$. For any $a, b \in \cap_{j \in \mathcal{J}} R_j$, $a, b \in R_j$ for all $j \in \mathcal{J}$, so $a + b, ab \in R_j$ for all such j. Hence, $a + b, ab \in \cap_{j \in \mathcal{J}} R_j$. Thus, the latter is a ring in R. To see that $\cup_{j \in \mathcal{J}} R_j$ is a subring, we first note that it is nonempty since $0 \in \cup_{j \in \mathcal{J}} R_j$, as 0 is in every R_j. If $a, b \in \cup_{j \in \mathcal{J}} R_j$, then there are $k,\ell \in \mathscr{J}$ such that $a \in R_k$, $b \in R_\ell$. If $k \leq \ell$, then $R_k \subseteq R_\ell$, so $a + b \in R_\ell$, and we have additive closure since $a + b \in \cup_{j \in \mathcal{J}} R_j$. Lastly, since each R_j is closed under multiplication, so is $\cup_{j \in \mathcal{J}} R_j$ and we have the result.

Section 1.4

1.31 It is valid. Here is a proof. Let N and M/N be Noetherian R-modules. If

$$M_1 \subseteq M_2 \subseteq \cdots \tag{S2}$$

is an ascending chain of R-submodules of M, for each $j \in \mathbb{N}$ let

$$M_j + N = \{m + N : m \in M_j\}.$$

Then $M_j + N$ is an R-submodule of M/N and $M_j + N \subseteq M_{j+1} + N$. Hence,

$$M_1 + N \subseteq M_2 + N \subseteq \cdots \tag{S3}$$

is an ascending chain of submodules of M/N. Since M/N is a Noetherian R-module, then (S3) terminates so there exists an $n \in \mathbb{N}$ such that $M_j + N \subseteq M_n + N$ for all $j \geq n$. Since $M_j \cap N$ is clearly a submodule of N and $M_j \cap N \subseteq M_{j+1} \cap N$, then

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \tag{S4}$$

is an ascending chain of submodules of N. Since N is a Noetherian R-module, then (S4) terminates. Hence, there exists an $m \in \mathbb{N}$ such that $M_j \cap N = M_m \cap N$ for all $j \geq m$. If we set $N = \max\{m, n\}$, then for any $j \geq N$,

$$M_j + N = M_{j+1} + N \text{ and } M_j \cap N = M_{j+1} \cap N.$$

We want to show that (S2) terminates. Suppose it does not. Then there exists an $j_0 \in \mathbb{N}$ such that M_{j_0} is properly contained in M_{j_0+1} for some $j_0 \geq N$. In this case we may select an element $m_{j_0+1} \in M_{j_0+1}$ with $m_{j_0+1} \notin M_{j_0}$. However, $m_{j_0+1} \in M_{j_0+1} + N = M_{j_0} + N$, so there exists an $m_{j_0} \in M_{j_0}$ and $n \in N$ such that $m_{j_0+1} = m_{j_0} + n$. By rewriting, $m_{j_0+1} - m_{j_0} = n \in N$. Moreover, $M_{j_0} \subseteq M_{j_0+1}$ so $m_{j_0+1} - m_{j_0} \in M_{j_0+1}$, which implies $m_{j_0+1} - m_{j_0} \in M_{j_0+1} \cap N \subseteq M_{j_0}$, a contradiction. We have shown that (S2) terminates, so M is Noetherian as an R-module.

1.33 Let

$$I_1 \subseteq I_2 \subseteq \cdots \tag{S5}$$

be an ascending chain of D_2-ideals. Since D_1 is a Noetherian domain and D_2 is a finitely generated D_1 module, then by Exercise 1.32, D_2 is a Noetherian D_1-module. Since I_j for any $j \in \mathbb{N}$ is a D_1-submodule of D_2 then (S5) must terminate, so D_2 is Noetherian.

1.35 If R does not satisfy the DCC, there exists an infinite nonterminating descending sequence of ideals $\{I_j\}$, so there can exist no minimal element in this set. Conversely, if R satisfies the DCC, then any nonempty collection $\mathcal{S}$ of ideals has an element I. If I is not minimal, it contains an element I_1. If I_1 is not minimal, it contains an ideal I_2, and so on. Eventually, due to the DCC, the process terminates, so the set contains a minimal element.

Section 1.5

1.37 Since $J+H$ is an ideal, then given $\alpha \in I, \beta \in J, \gamma \in H$, we have $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma \in IJ+IH$ and $\alpha(\beta+\gamma) \in I(J+H)$.

1.39 Since an invertible fractional R-ideal I satisfies $II^{-1} = R$, there exist $a_i \in I^{-1}$ and $b_i \in I$ such that $1_R = \sum_{i=1}^n a_i b_i$. Thus, if $\alpha \in I$, then $\alpha = \sum_{i=1}^n (\alpha a_i) b_i$. Also, $\alpha a_i \in I$ for $i = 1, 2, \ldots, n$ and since $a_i \in I^{-1} = \{\beta \in F : \beta I \subseteq R\}$, then I is finitely generated as an R-module by the b_i, for $i = 1, 2, \ldots, n$.

1.41 Suppose that $I = Rb_1 + Rb_2 + \cdots + Rb_n$ where $b_j = c_j/a_j \in F$, for $a_j, c_j \in R$, with $a_j \neq 0$ for $j = 1, 2, \ldots, n$. Let $\alpha = \prod_{j=1}^n a_j$. Then $\alpha \neq 0$ and

$$\alpha I = Rc_1 \prod_{j=2}^{n} a_j + \cdots + Rc_n \prod_{j=1}^{n-1} a_j \subseteq R,$$

which makes I a fractional R-ideal.

1.43 That (i) implies (ii) is Theorem 1.17 on page 28 and Theorem 1.16 on page 27. That (ii) implies (iii) is clear. That (iii) implies (iv) follows from Remark 1.13 on page 26 and Theorem 1.16 on page 27. That (iv) is equivalent to (v) is Exercise 1.42. We now show that (iv) implies (i) to complete the logical circle. By Exercise 1.39, part (A) of Definition 1.23 on page 25 is satisfied. If $\alpha \in F$, the quotient field of D, then by Exercise 1.40, $R[\alpha]$ is a finitely generated R-module. Thus, by Exercise 1.41, $R[\alpha]$ is a fractional R ideal. Accordingly, since $R[\alpha]R[\alpha] = R[\alpha]$, then

$$R[\alpha] = RR[\alpha] = (R[\alpha])^{-1}(R[\alpha])R[\alpha] = (R[\alpha])^{-1}(R[\alpha][\alpha]) = (R[\alpha])^{-1}R[\alpha] = R,$$

so $\alpha \in R$, which shows that R is integrally closed in F. This is part (C) of Definition 1.23. It remains to show that every nonzero prime D-ideal is maximal. Since we have part (A) of Definition 1.23, then by Remark 1.12 on page 26, a prime ideal $\mathcal{P}$ is contained in a maximal D-ideal $\mathcal{M}$. Thus, by (iv) $\mathcal{M}$ is invertible. Hence, $M^{-1}\mathcal{P} = I$ is a fractional R-ideal and

$$M^{-1}\mathcal{P} \subseteq M^{-1}M = R,$$

so $M^{-1}\mathcal{P}$ is an integral R-ideal. Moreover, since

$$M(M^{-1}\mathcal{P}) = R\mathcal{P} = \mathcal{P},$$

and $\mathcal{P}$ is prime, then by Theorem 1.7 on page 16, either $M \subseteq \mathcal{P}$ or $M^{-1}\mathcal{P} \subseteq \mathcal{P}$. If $M^{-1}\mathcal{P} \subseteq \mathcal{P}$, then

$$R \subseteq M^{-1} = M^{-1}R = M^{-1}\mathcal{P}\mathcal{P}^{-1} \subseteq \mathcal{P}\mathcal{P}^{-1} \subseteq R,$$

which shows that $M^{-1} = R$. However, $R = MM^{-1} = MR = M$, contradicting that M is maximal. Hence, $M \subseteq \mathcal{P}$, which means that $M = \mathcal{P}$, which is maximal.

1.45 If $I = (0)$ or $I = R = (1)$, then one element suffices, so assume that $(0) \subset I \subset R$ and let $\alpha \in I$ such that $\alpha \neq 0, 1$. Then $(\alpha) \subseteq I$ and $I \mid (\alpha)$ by Corollary 1.7 on page 27. Thus, there exists an R-ideal J such that $(\alpha) = IJ$.

Let $\mathcal{S}$ be the set of distinct prime R-ideals $\mathcal{P}_j$ for $j = 1, 2, \ldots, n$ such that either $\mathrm{ord}_{\mathcal{P}}(I) \neq 0$ or $\mathrm{ord}_{\mathcal{P}}(IJ) \neq 0$, or possibly both. Since $I \neq R$, then $\mathcal{S} \neq \varnothing$.

By part (c) of Exercise 1.44, there exists a $\beta \in F$, the quotient field of R such that $\operatorname{ord}_{\mathcal{P}}((\beta)) = \operatorname{ord}_{\mathcal{P}}(I)$ for all prime R-ideals $\mathcal{P}$ dividing I. Therefore, for all prime R-ideals $\mathcal{P} \mid I$,

$$\operatorname{ord}_{\mathcal{P}}(I) = \min(\operatorname{ord}_{\mathcal{P}}(I), \operatorname{ord}_{\mathcal{P}}((\alpha))) = \min(\operatorname{ord}_{\mathcal{P}}((\beta)), \operatorname{ord}_{\mathcal{P}}((\alpha))) = \operatorname{ord}_{\mathcal{P}}((\alpha) + (\beta)),$$

by part (b) of Exercise 1.44. Hence,

$$I = (\alpha) + (\beta) = (\alpha, \beta),$$

as required.

1.47 Let D be an almost Euclidean domain and let ϕ be an almost Euclidean function of D. Let I be any nonzero ideal of D and let

$$\mathcal{S} = \{\phi(\alpha) : \alpha \in I\}$$

and let $\phi(m)$ for $m \in I$ be a minimal positive value in $\mathcal{S}$. By part (c) of the definition of an almost Euclidean function in Exercise 1.25, given $\gamma \in I$ and any $x, y \in D$ we cannot have $0 < \phi(\gamma x + my) < \phi(m)$, by the minimality of $\phi(m)$, so we must have $\gamma = mq$ for some $q \in D$. Hence, $I = (m)$ since γ was arbitrary. This shows that D is a PID. By Theorem 1.12 on page 21, D is Noetherian.

1.49 No, since property 3 of Definition 1.24 on page 26 fails to hold given that there exists no integer r such that $r\mathcal{I} \subseteq \mathbb{Z}$.

Section 1.6

1.51 Taking the hint, it suffices to prove the result for $n = 2$, since we may extrapolate by induction from this case.

Consider $m_{\alpha,\mathbb{Q}}(x) = \prod_{j=1}^{d_\alpha}(x - \alpha_j)$, where the α_j are all of the conjugates of $\alpha_1 = \alpha$ over $\mathbb{Q}$, and let $m_{\beta,\mathbb{Q}}(x) = \prod_{j=1}^{d_\beta}(x - \beta_j)$, where the β_j are all of the conjugates of $\beta_1 = \beta$ over $\mathbb{Q}$. Also, $\alpha_j \neq \alpha_k$ for any $j \neq k$, and $\beta_i \neq \beta_\ell$ for any $i \neq \ell$, by Corollary 1.14 on page 38. Select a $q \in \mathbb{Q}$ such that $q \neq (\alpha - \alpha_k)/(\beta_j - \beta)$ for any $k = 1, 2, \ldots, d_\alpha$ and any $j = 1, 2, \ldots, d_\beta$, and let

$$\gamma = \alpha + q\beta, \tag{S6}$$

with

$$f(x) = m_{\alpha,\mathbb{Q}}(\gamma - qx) \in \mathbb{Q}(\gamma)[x].$$

Since

$$f(\beta) = m_{\alpha,\mathbb{Q}}(\gamma - q\beta) = m_{\alpha,\mathbb{Q}}(\alpha) = 0,$$

and

$$m_{\beta,\mathbb{Q}}(\beta) = 0,$$

then β is a common root of $f(x)$ and $m_{\beta,\mathbb{Q}}(x)$. We now show that this is the only common root. If there exists a $\sigma \in \mathbb{C}$, with $\sigma \neq \beta$, such that $f(\sigma) = 0 = m_{\beta,\mathbb{Q}}(\sigma) = 0$, then $\sigma = \beta_j$ for some $j > 1$. Since

$$0 = m_{\alpha,\mathbb{Q}}(\alpha) = m_{\alpha,\mathbb{Q}}(\gamma - q\beta_j) = f(\beta_j),$$

then there is a $k \in \{1, 2, \ldots, d_\beta\}$ such that $\gamma - q\beta_j = \alpha_k$. Thus, by (S6),

$$\alpha_k + q\beta_j = \gamma = \alpha + q\beta,$$

so

$$q = \frac{\alpha - \alpha_k}{\beta_j - \beta},$$

contradicting the choice of q. We have shown that β is the only common root of $f(x)$ and $m_{\beta,\mathbb{Q}}(x)$. Therefore, by Theorem 1.23 on page 38, $m_{\beta,\mathbb{Q}(\gamma)}(x) \bigm| f(x)$ and $m_{\beta,\mathbb{Q}(\gamma)}(x) \bigm| m_{\beta,\mathbb{Q}}(x)$. However, since $f(x)$ and $m_{\beta,\mathbb{Q}}(x)$ have only one root in common, then

$$\deg(m_{\beta,\mathbb{Q}(\gamma)}(x)) = 1.$$

Thus, $m_{\beta,\mathbb{Q}(\gamma)}(x) = x + \delta$ for some $\delta \in \mathbb{Q}(\gamma)$. Since $m_{\beta,\mathbb{Q}(\gamma)}(\beta) = 0 = \beta + \delta$, then $\beta = -\delta \in \mathbb{Q}(\gamma)$, so $\alpha = \gamma - q\beta \in \mathbb{Q}(\gamma)$. This shows that $\mathbb{Q}(\alpha,\beta) \subseteq \mathbb{Q}(\gamma)$. However, since $\gamma = \alpha + q\beta \in \mathbb{Q}(\alpha,\beta)$, $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha,\beta)$. We have completed the proof that $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\gamma)$, as required.

1.53 Clearly, $\mathbb{Q}(\frac{\sqrt{2}}{2}(1+i)) \subseteq \mathbb{Q}(i, \sqrt{2})$. To see that equality holds, we observe that

$$\left(\frac{1+i}{\sqrt{2}}\right)^2 = i = \zeta_4,$$

so

$$\left(\frac{1+i}{\sqrt{2}}\right)$$

is a primitive eighth root of unity, and so is any odd power thereof. Since

$$|\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}| = 4 = \left|\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right) : \mathbb{Q}\right|,$$

then we must have

$$Q(i, \sqrt{2}) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right).$$

Section 1.7

1.55 Let M be a $\mathbb{Z}$-module. If $r \in \mathbb{Z}$, and $m \in M$, then

$$r \cdot m = \underbrace{m + \cdots m}_{r},$$

so the properties of an additive abelian group are inherited from this action. Conversely, if M is an additive abelian group, then the addition within the group gives the $\mathbb{Z}$-module action as above.

1.57 We only prove this for $\sigma = 1$, since the other case is similar.

Suppose that I is an ideal. Therefore, $a\sqrt{D} \in I$, so $c|a$ by the minimality of c. We have

$$\sqrt{D}(b + c\sqrt{D}) = b\sqrt{D} + cD \in I,$$

so $c|b$. Moreover, since

$$\left(\frac{b}{c} - \sqrt{D}\right)(b + c\sqrt{D}) = \frac{b^2 - c^2D}{c} \in I,$$

then

$$a|(b^2 - c^2D)/c.$$

In other words,

$$ac|(b^2 - c^2D).$$

Conversely, assume that I satisfies the conditions. To verify that I is an ideal, we need to show that $a\sqrt{D} \in I$ and $(b + \sqrt{D})\sqrt{D} \in I$. This is a consequence of the following identities, the details of which we leave to the reader for verification:

$$a\sqrt{D} = -(b/c)a + (a/c)(b + c\sqrt{D}),$$

and

$$b\sqrt{D} + cD = -(b^2 - c^2D)/c + b(b + c\sqrt{D})/c,$$

so I is an ideal.

1.59 If $[\alpha,\beta] = [\gamma,\delta]$, there are integers $x, x_0, y, y_0, z, z_0, w, w_0$ such that

$$\alpha = x\gamma + y\delta, \beta \quad = w\gamma + z\delta,$$

and

$$\gamma = x_0\alpha + y_0\beta, \delta \quad = w_0\alpha + z_0\beta.$$

These two sets of equations translate into two matrix equations as follows.

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = X\begin{pmatrix}\gamma\\ \delta\end{pmatrix},$$

where

$$X = \begin{pmatrix} x & y\\ w & z\end{pmatrix},$$

and

$$\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = X_0\begin{pmatrix}\alpha\\ \beta\end{pmatrix},$$

where

$$X_0 = \begin{pmatrix} x_0 & y_0\\ w_0 & z_0\end{pmatrix}.$$

Hence,

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = XX_0\begin{pmatrix}\alpha\\ \beta\end{pmatrix}.$$

Therefore, $XX_0 = I_2$ and hence the determinants of X and X_0 are ± 1, so the result follows.

Conversely, assume that the matrix equation holds as given in the exercise. Then clearly

$$[\alpha,\beta] \subseteq [\gamma,\delta].$$

Since the determinant of X is ± 1, we can multiply both sides of the matrix equation by the inverse of X to get that γ and δ are linear combinations of α and β. Thus,

$$[\gamma,\delta] \subseteq [\alpha,\beta].$$

The result is now proved.

1.61 Let

$$J_i = (a_i, (b_i + \sqrt{\Delta})/2) \text{ for } i = 1, 2$$

be $\mathfrak{O}_F$-ideals such that $J_1 J_2 \subseteq \mathcal{P}$. Then by the multiplication formulas given on page 48, $J_1 J_2 = (a_3, (b_3 + \sqrt{\Delta})/2)$ where $a_3 = a_1 a_2 / g \equiv 0 (\text{mod } p)$ with $g = \gcd(a_1, a_2, (b_1 + b_2)/2))$. If $p \nmid a_2$ (which means that $J_2 \not\subseteq \mathcal{P}$), then $p \mid a_1$, since p cannot divide g, given that it does not divide a_2. Thus, to show that $J_1 \subseteq \mathcal{P}$, it remains to show that $b_1 = 2pn + b$ for some $n \in \mathbb{Z}$, by Exercise 1.60. Now, by Exercise 1.57,

$$b_1^2 \equiv \Delta \pmod{4a_1} \text{ and } b^2 \equiv \Delta \pmod{4p},$$

so $b_1^2 \equiv b^2 (\text{mod } 4p)$. Since p is prime, then $b_1 \equiv \pm b (\text{mod } 2p)$. If

$$b_1 \equiv -b \pmod{2p}, \text{ then } J_1 \subseteq \mathcal{P}' = (p, (-b + \sqrt{\Delta})/2),$$

so if $(-b + \sqrt{\Delta})/2 \in \mathcal{P}$, then $J_1 \subseteq \mathcal{P}$ so we are done by Theorem 1.7 on page 16. If $(-b + \sqrt{\Delta})/2 \notin \mathcal{P}$, then $\mathcal{P} \cap \mathcal{P}' = (p)$, so $a_3 = 1$, and this forces $p \mid 1$, a contradiction. The remaining case is $b_1 \equiv b (\text{mod } 2p)$, so $b_1 = 2pn + b$ for some $n \in \mathbb{Z}$, as required.

Section 2.1

2.1 Suppose that θ is an embedding of F in $\mathbb{C}$ with $\theta(\alpha) = \beta$. Since

$$0 = m_{\alpha,\mathbb{Q}}(\alpha) = \sum_{j=0}^{d-1} q_j \alpha^j \text{ with } q_j \in \mathbb{Q},$$

then

$$0 = \theta(0) = \theta\left(\sum_{j=0}^{d-1} q_j \alpha^j\right) = \sum_{j=0}^{d-1} q_j \theta(\alpha)^j = \sum_{j=0}^{d-1} q_j \beta^j.$$

Thus, $\beta = \alpha_j$ for some $j = 1, 2, \ldots, d$. Thus, there are at most d embeddings of F in $\mathbb{C}$. Now we show that if θ_j is defined by $\theta_j(f(\alpha)) = f(\alpha_j)$ for $j = 1, 2, \ldots, d$, with $f(x) \in F[x]$, then θ_j is indeed an embedding of F in $\mathbb{C}$. To do this, we first show that θ_j is well-defined. If $f(\alpha) = g(\alpha)$ for $f(x), g(x) \in F[x]$, then $f(x) - g(x) = h(x) m_{\alpha,\mathbb{Q}}(x)$ for some $h(x) \in F[x]$, so $f(\alpha_j) - g(\alpha_j) = h(\alpha_j) m_{\alpha,\mathbb{Q}}(\alpha_j) = 0$. Hence, $\theta_j(f(\alpha)) = f(\alpha_j) = g(\alpha_j) = \theta_j(g(\alpha))$, so θ_j is well-defined, and the conjugates of α are the α_j, which in turn are precisely the roots of $m_{\alpha,\mathbb{Q}}(x)$. Lastly, we demonstrate how the one-to-one property follows. Suppose that $\theta_j(f(\alpha)) = \theta_j(g(\alpha))$. Then $f(\alpha_j) = g(\alpha_j)$, so as in the above, $f(x) - g(x) = h(x) m_{\alpha_j,\mathbb{Q}}(x)$. Thus, $f(\alpha) - g(\alpha) = h(\alpha) m_{\alpha_j,\mathbb{Q}}(\alpha) = 0$ since $\theta(\alpha) = \alpha_j$.

2.3 By Theorem 1.23 on page 38, $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, so by Exercise 2.2, $f_{\alpha F}(x) \in \mathbb{Z}[x]$. We have shown that the F-conjugates of α are roots of a monic polynomial with coefficients in $\mathbb{Z}$, namely they are algebraic integers by Definition 1.28 on page 35.

2.5 If all the F-conjugates are distinct, then $f_{\alpha,F}(x)$ is a product of distinct linear factors. Thus, by Exercise 2.2, we have $t = 1$ and $m_{\alpha,\mathbb{Q}}(x) = f_{\alpha,F}(x)$. Therefore,

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg(m_{\alpha,\mathbb{Q}}(x)) = \deg(f_{\alpha,F}(x)) = d = |F : \mathbb{Q}|.$$

However, since $\alpha \in F$, $\mathbb{Q}(\alpha) \subseteq F$, so $F = \mathbb{Q}(\alpha)$.

Conversely assume that $F = \mathbb{Q}(\alpha)$. Then

$$\deg(m_{\alpha,\mathbb{Q}}(x)) = |F : \mathbb{Q}| = d.$$

By Exercise 2.2, this implies that $t = 1$ and $m_{\alpha,\mathbb{Q}}(x) = f_{\alpha,F}(x)$. Hence, the F-conjugates of α are distinct.

2.7 Since the minimal polynomial of α over $\mathbb{Q}$ is of the form

$$m_\alpha(x) = x^2 + bx + c \in \mathbb{Z}[x],$$

then $\alpha^2 + b\alpha + c = 0$. Therefore, by the quadratic formula,

$$\alpha = (-b \pm \sqrt{b^2 - 4ac})/2.$$

Since we may remove all square factors from $b^2 - 4c = s^2 d$, and since $\alpha \in \mathbb{Q}(\sqrt{d})$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$.

2.9 Since $\sqrt{n_1} + \sqrt{n_2} \in \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2})$, we need only show that $\sqrt{n_1}$, and $\sqrt{n_2}$ are in $\mathbb{Q}(\sqrt{n_1} + \sqrt{n_2})$. Since

$$(\sqrt{n_1} + \sqrt{n_2})^2 = n_1 + n_2 + 2\sqrt{n_1}\sqrt{n_2},$$

then $\sqrt{n_1}\sqrt{n_2} \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2})$. Also, since

$$n_1 - 2\sqrt{n_1}\sqrt{n_2} + n_2 = (\sqrt{n_1} - \sqrt{n_2})^2 \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2}),$$

then

$$(\sqrt{n_1} + \sqrt{n_2})(\sqrt{n_1} - \sqrt{n_2})^2 = (n_1 - n_2)(\sqrt{n_1} - \sqrt{n_2}) \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2}).$$

Therefore, $\sqrt{n_1} - \sqrt{n_2} \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2})$. Hence,

$$\sqrt{n_1} = \frac{1}{2}(\sqrt{n_1} - \sqrt{n_2} + \sqrt{n_1} + \sqrt{n_2}) \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2}),$$

and similarly, $\sqrt{n_2} \in \mathbb{Q}(\sqrt{n_1} + \sqrt{n_2})$.

It remains to determine the Galois group. Let $\sigma_j : \sqrt{n_j} \mapsto -\sqrt{n_j}$ for $j = 1, 2$ with $\sigma_1(\sqrt{n_2}) = \sqrt{n_2}$ and $\sigma_2(\sqrt{n_1}) = \sqrt{n_1}$. These are distinct $\mathbb{Q}$-automorphisms of K, of order 2, and since $|K : \mathbb{Q}| = 4$, $\text{Gal}(K/\mathbb{Q}) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$, the *Klein four-group*, namely is the direct product of two distinct cyclic groups of order 2—see Remark A.1 on page 321.

2.11 This is immediate from Exercise 2.1 since the complex embeddings come in conjugate pairs.

2.13 By Fermat's Little Theorem, we get that $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$ for all α,$\beta \in F$. Since $1_F \mapsto 1_F$, then σ fixes $\mathbb{F}_p$.

2.15 Since F^* has order $p^n - 1$, every nonzero $\alpha \in F$ satisfies $\alpha^{p^n-1} = 1_F$. Therefore, every nonzero $\alpha \in F$ is a root of $x^{p^n-1} - 1_F$, so also a root of $f(x) = x(x^{p^n-1} - 1_F) = x^{p^n} - x \in \mathbb{F}_p[x]$. Since $f(0) = 0$, then $f(x)$ has p^n distinct roots. In other words, $f(x)$ splits over F. It remains to establish uniqueness. If K is a splitting field for $f(x)$ over $\mathbb{F}_p$, then $f'(x) = -1$ and $\gcd(f(x), f'(x)) = 1$. Therefore, by part (b) of Exercise 2.14, $f(x)$ has p^n distinct roots in F. Let $\sigma : F \mapsto F$ be given by Exercise 2.13. Thus, $\alpha \in F$ is a root of $f(x)$ if and only if $\phi(\alpha) = \alpha$. Hence, the subfield of F having all roots of $f(x)$ in F must in fact *be* F, so uniqueness is proved.

Section 2.2

2.17 From the properties of embeddings, we get

$$T_F(\alpha+\beta)=\sum_{j=1}^{d}\theta_j(\alpha+\beta)=\sum_{j=1}^{d}(\theta_j(\alpha)+\theta_j(\beta))=\sum_{j=1}^{d}\theta_j(\alpha)+\sum_{j=1}^{d}\theta_j(\beta)=T_F(\alpha)+T_F(\beta).$$

Also,

$$N_F(\alpha\beta)=\prod_{j=1}^{d}\theta_j(\alpha\beta)=\prod_{j=1}^{d}(\theta_j(\alpha)\theta_j(\beta))=\prod_{j=1}^{d}\theta_j(\alpha)\prod_{j=1}^{d}\theta_j(\beta)=N_F(\alpha)N_F(\beta).$$

For $q\in\mathbb{Q}$,

$$T_F(q\alpha)=\sum_{j=1}^{d}\theta_j(q\alpha)=\sum_{j=1}^{d}q\theta_j(\alpha)=q\sum_{j=1}^{d}\theta_j(\alpha)=qT_F(\alpha),$$

and

$$N_F(q\alpha)=\prod_{j=1}^{d}\theta_j(q\alpha)=\prod_{j=1}^{d}q\theta_j(\alpha)=q^d\prod_{j=1}^{d}\theta_j(\alpha)=q^dN_F(\alpha).$$

2.19 Since the embeddings of F in $\mathbb{C}$ are

$$\theta_1:\sqrt{7}\mapsto\sqrt{7},\text{ and }\theta_2:\sqrt{7}\mapsto-\sqrt{7},$$

then

$$T_F(\alpha)=\alpha+\alpha'=\left(\frac{1+\sqrt{7}}{2}\right)+\left(\frac{1-\sqrt{7}}{2}\right)=1,$$

and

$$N_F(\alpha)=\alpha\cdot\alpha'=(1-7)/4=-3/2.$$

Therefore, by Theorem 2.5 on page 66,

$$m_\alpha(x)=x^2-T_F(\alpha)x+N_F(\alpha)=x^2-x-3/2.$$

2.21 Suppose that $\alpha=(a+b\sqrt{p})/c\in F$ with $a,b,c\in\mathbb{Z}$, $\gcd(a,b,c)=1$, and $N_F(\alpha)=2$. (The gcd condition may be assumed without loss of generality since we may otherwise divide out the common factor.) Then

$$c^2N_F(\alpha)=a^2-b^2p=2c^2.$$

If c is even, then a and b are both odd by the gcd condition. Thus,

$$1\equiv a^2\equiv b^2p\equiv p \pmod 8,$$

a contradiction. Therefore, c is odd, so b and c must both be odd. Hence,

$$2\equiv 2c^2\equiv a^2 \pmod p.$$

However, this is false since 2 is a quadratic residue modulo a prime $p>2$ if and only if $p\equiv\pm1\ (\text{mod } 8)$—see (A.10) on page 342.

2.23 Let $\alpha = \sqrt{2}+\sqrt{3}$. Then

$$m_\alpha(x) = x^4 - 10x^2 + 1.$$

Note that if $F = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, then $T_F(\alpha) = 0$, and $N_F(\alpha) = 1$. Thus, we are aided by Theorem 2.5.

2.25 We have

$$T_F(1-\zeta_p^j) = \sum_{j=1}^{p-1}(1-\zeta_p^j) = \sum_{j=1}^{p-1} 1 - \sum_{j=1}^{p-1}\zeta_p^j.$$

However, by Example 1.5, $\sum_{j=1}^{p-1}\zeta_p^j = -1$. Therefore,

$$T_F(1-\zeta_p^j) = \sum_{j=1}^{p-1} 1 - (-1) = p - 1 - (-1) = p,$$

as required.

2.27 $\zeta_3 = \frac{1}{4}\left(\mathfrak{g}+\zeta_3\right) + \frac{1}{4}\left(\mathfrak{g}+\zeta_3\right)^3 - \frac{1}{2}$.

2.29 To prove the hint, we invoke Exercise 1.54 on page 43 and Theorem 1.25 on page 40 to get

$$\frac{x^p-1}{x-1} = \prod_{j=1}^{p-1}(x-\zeta_p^j) = m_{\zeta_p}(x),$$

then by differentiating the left and right-hand sides we get,

$$\frac{px^p - px^{p-1} - x^p + 1}{(x-1)^2} = \sum_{1\le k\le p-1} \prod_{\substack{j=1\\ j\ne k}}^{p-1} (x-\zeta_p^j).$$

Therefore, if we substitute $x = \zeta_p^i$ into the left-hand side, we get

$$\frac{p - p\zeta_p^{i(p-1)}}{(\zeta_p^i-1)^2} = \frac{p\zeta_p^{p-i}(\zeta_p^i-1)}{(\zeta_p^i-1)^2} = \frac{p\zeta_p^{p-i}}{\zeta_p^i-1},$$

and for the right-hand side, the substitution yields,

$$\prod_{\substack{j=1\\ j\ne i}}^{p-1} (\zeta_p^i - \zeta_p^j).$$

We have shown that:

$$\frac{p\zeta_p^{p-i}}{\zeta_p^i-1} = \prod_{\substack{j=1\\ j\ne i}}^{p-1} (\zeta_p^i - \zeta_p^j). \tag{S7}$$

However, since $m_{\zeta_p}(0) = 1$, then

$$\prod_{j=1}^{p-1}\zeta_p^j = 1,$$

and since $m_{\zeta_p}(1) = p$, then

$$\prod_{j=1}^{p-1}(1-\zeta_p^j) = p = \prod_{j=1}^{p-1}(\zeta_p^j - 1).$$

Therefore, by (S7),

$$\prod_{j=1}^{p-1}\prod_{\substack{j=1\\ j\neq i}}^{p-1}(\zeta_p^i - \zeta_p^j) = \prod_{j=1}^{p-1}\frac{p\zeta_p^{p-j}}{\zeta_p^j - 1} = p^{p-1}\frac{\prod_{j=1}^{p-1}\zeta_p^{p-j}}{\prod_{j=1}^{p-1}(\zeta_p^j - 1)} = p^{p-1}/p = p^{p-2}.$$

This last equation has $(p-1)(p-2)$ factors, half of which have $i < j$, so

$$\prod_{1\le i<j\le p-1}(\zeta_p^i - \zeta_p^j) = (-1)^{(p-1)(p-2)/2}\prod_{1\le i<j\le p-1}(\zeta_p^i - \zeta_p^j)^2,$$

which, since $p > 2$, is equal to

$$(-1)^{(p-1)/2}\prod_{1\le i<j\le p-1}(\zeta_p^i - \zeta_p^j)^2,$$

as required.

2.31 By Exercise 2.29,

$$\operatorname{disc}(m_{\alpha,\mathbb{Q}}) = \prod_{1\le i<j\le d}(\alpha_i - \alpha_j)^2.$$

Also,

$$m'_{\alpha,\mathbb{Q}}(x) = \sum_{j=1}^{d}\prod_{\substack{i=1\\ i\neq j}}^{d}(x - \alpha_i).$$

Therefore,

$$m'_{\alpha,\mathbb{Q}}(\alpha_j) = \prod_{\substack{i=1\\ i\neq j}}^{d}(\alpha_j - \alpha_i),$$

so

$$N_F(m'_{\alpha,\mathbb{Q}}(\alpha_j)) = \prod_{j=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_j) = \prod_{1\le i<j\le d}(\alpha_j - \alpha_i)\prod_{1\le j<i\le d}(\alpha_j - \alpha_i),$$

and since there are $d(d-1)/2$ pairs (i,j) with $1 \le i < j \le d$, then the above equals

$$(-1)^{d(d-1)/2}\prod_{1\le i<j\le d}(\alpha_j - \alpha_i)^2 = (-1)^{d(d-1)/2}\operatorname{disc}(m_{\alpha,\mathbb{Q}}).$$

This completes the proof.

Section 2.3

2.33 We use induction on d. If $d = 2$, then

$$\det(\alpha_j^{i-1}) = \begin{vmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{vmatrix} = \alpha_2 - \alpha_1.$$

This is the induction step. Now assume that the result holds for all such $n \times n$ matrices with $n < d$. If $\operatorname{cof}(A_{i,j})$ denotes the *cofactor* of the matrix $A = (\alpha_j^{i-1})$, then by (A.6),

$$\det(\alpha_j^{i-1}) = \sum_{j=1}^{d} \alpha_j^{i-1} \operatorname{cof}(A_{i,j}).$$

By induction hypothesis, the result holds for each $A_{i,j}$, so the entire result holds.

2.35 Let $F = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$. Then α has minimal polynomial $m_{\alpha,\mathbb{Q}}(x) = x^2 - 2$, so via Exercise 2.31,

$$\operatorname{disc}(m_{\alpha,\mathbb{Q}}) = (-1)^{d(d-1)/2} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)) = (-1)^{2(2-1)/2}(2\sqrt{2})(-2\sqrt{2}) = 8.$$

2.37 We have $n = |F : \mathbb{Q}| = 8$, and $d = |\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$. Also from Exercise 2.36, $T_{\mathbb{Q}(\alpha)}(\alpha) = 0$, and $N_{\mathbb{Q}(\alpha)}(\alpha) = -5$. Therefore, by Theorem 2.5,

$$T_F(\alpha) = \frac{8}{4} T_{\mathbb{Q}(\alpha)}(\alpha) = 0,$$

and

$$N_F(\alpha) = (N_{\mathbb{Q}(\alpha)}(\alpha))^{8/4} = (-5)^2 = 25.$$

2.39 Since $\mathfrak{O}_F = \mathbb{Z}[\alpha]$, then $\mathcal{B} = \{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis for F, where $|F : \mathbb{Q}| = d$. By Exercise 2.38, $\operatorname{disc}(\mathcal{B}) = \operatorname{disc}(m_{\alpha,\mathbb{Q}})$. Hence,$\Delta_F = \operatorname{disc}(m_{\alpha,\mathbb{Q}})$.

2.41 Suppose that $M = N \oplus N_1$. If $r \in R$, then

$$Mr \cap N = (N \oplus N_1)r \cap N = (Nr \oplus N_1 r) \cap N = (Nr \cap N) \oplus (N_1 r \cap N) = Nr \cap N = Nr.$$

2.43 By Theorem 1.24 on page 39, a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$. Let

$$m_{\alpha,\mathbb{Q}}(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0,$$

be the minimal polynomial of α over $\mathbb{Q}$. Since $\alpha\alpha^i = \sum_{k=1}^{d} b_{i,k}\alpha^k = b_{i,i+1}\alpha^{i+1} = \alpha^{i+1}$, then the matrix $B = (b_{i,j})$ is given by[S1]

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots - & c_{d-1} \end{pmatrix}.$$

[S1] In linear algebra B is called the *matrix of the transformation* $\alpha \mapsto \alpha \cdot \alpha^i$. Also, the *trace* of α is given by $\sum_{j=1}^{d} b_{j,j}$, and the norm of α is given by $\det(B)$. These are alternative definitions of the norm and trace that we are now showing to be equivalent to the ones we gave in Definition 2.4 for the more general number field F (see Theorem 2.5 for the relevant connections).

By Exercise 2.42, we may form a basis $\{\beta_1, \ldots, \beta_n\}$ for F over $\mathbb{Q}$, where $\beta_j = \alpha^j$ for $j = 0, 1, \ldots, d-1$. Also, by Theorem 2.5 on page 66, $d|n$, and since $\alpha\beta_i = \sum_{j=1}^n a_{i,j}\beta_j$, then the matrix $A = (a_{i,j})$ must have determinant

$$\det(A) = \det \begin{pmatrix} B & & & \\ & B & & \\ & & \ddots & \\ & & & B \end{pmatrix},$$

where there are n/d blocks of B on the main diagonal. Since

$$|\det(B)| = |c_0|, \text{ and } |\det(A)| = |\det(B)|^{n/d},$$

then

$$|\det(A)| = |c_0|^{n/d}.$$

However, by Theorem 2.5,

$$|c_0| = |N_{\mathbb{Q}(\alpha)}(\alpha)|, \text{ and } (N_{\mathbb{Q}(\alpha)}(\alpha))^{n/d} = N_F(\alpha),$$

so

$$|\det(A)| = |N_F(\alpha)|,$$

as required. (The reader should compare this with Exercise 2.2 on page 62.)

Section 2.4

2.45 Suppose that

$$I = \prod_{j=1}^r \mathcal{P}_j^{a_j}$$

for distinct prime $\mathfrak{O}_F$-ideals $\mathcal{P}_j$. Then since

$$N(I) = \prod_{j=1}^r N(\mathcal{P}_j)^{a_j}$$

is prime, we must have $r = 1 = a_1$, so I is prime.

2.47 Since there are nonzero $\alpha,\beta \in \mathfrak{O}_F$ and integral $\mathfrak{O}_F$-ideals I, J such that

$$\mathcal{I} = \frac{1}{\alpha} I \text{ and } \mathcal{J} = \frac{1}{\beta} J,$$

then

$$\mathcal{I}\mathcal{J} = \frac{1}{\alpha\beta} IJ.$$

Therefore, by Definition 2.8 on page 83,

$$N(\mathcal{I}\mathcal{J}) = \frac{N(IJ)}{N((\alpha\beta))},$$

so by Definition 1.15 on page 16,

$$N(\mathcal{I}\mathcal{J}) = \frac{N(IJ)}{N((\alpha)(\beta))},$$

and by Exercise 2.46,

$$N(\mathfrak{I}\mathfrak{J}) = \frac{N(IJ)}{N((\alpha))N((\beta))}.$$

Hence,

$$N(\mathfrak{I}\mathfrak{J}) = \frac{N(I)}{N((\alpha))}\frac{N(J)}{N((\beta))} = N(\mathfrak{I})N(\mathfrak{J}).$$

2.49 Let $N(\mathcal{P}) = \prod_{j=1}^{r} p_j^{m_j}$. By Exercise 2.48, $\mathcal{P} \mid (N(\mathcal{P}))$. Therefore, $\mathcal{P}$ divides one of the principal ideals (p_j). If $\mathcal{P} \mid (p_k)$ for some $k \neq j$, then by the Euclidean algorithm, there exist $u, v \in \mathbb{Z}$ such that $up_j + vp_k = 1$. Since $up_j, vp_k \in \mathcal{P}$, then $1 \in \mathcal{P}$, a contradiction. Hence, $N(\mathcal{P}) = p_1^{m_1} = p^m$ a prime power. Thus, $N(\mathcal{P}) \mid N(p) = p^n = p^{|F:\mathbb{Q}|}$, so $N(\mathcal{P}) = p^m$ for some $m \leq n$.

2.51 All ideals in $\mathbb{Z}[\sqrt{10}]$ of norm 6 have the form $[6, a + b\sqrt{10}]$ where

$$a^2 - 10b^2 \equiv 0 \pmod 6$$

by Exercise 1.57 on page 53. Thus, $[6, 2 + \sqrt{10}]$ and $[6, 2 - \sqrt{10}]$ are two of them. By Exercise 1.59 on page 54, this is all of them.

2.53 This is a direct consequence of Exercises 2.48 and 2.52.

Section 3.1

3.1 Clearly, since$f(x, y) = g(X, Y)$ for

$$X = px + qy \tag{S8}$$

and

$$Y = rx + sy, \tag{S9}$$

then equivalent forms represent the same integers by definition. Since $ps - qr = \pm 1$ and from (S8)–(S9), $x = \pm(sX - qY)$ and $y = \pm(rX - pY)$, so $\gcd(x, y) = 1$ if and only if $\gcd(X, Y) = 1$.

3.3 Suppose that $f(x, y) = g(X, Y)$ where $X = px + qy$, $Y = rx + sy$, and $ps - qr = 1$. If we set $x = X$ and $Y = y$, namely $p = s = 1$ and $q = r = 0$, then $f(x, y) = g(x, y)$ and we have the reflexive property. Also, since

$$g(X_1, Y_1) = f(x, y),$$

where $X_1 = sx - qy$ and $Y_1 = py - rx$, then we have the symmetry property.

Lastly, for transitivity, assume that

$$g(X, Y) = h(PX + QY, RX + SY),$$

where $PS - QR = 1$. Then since

$$PX + QY = P(px + qy) + Q(rx + sy) = (Pp + Qr)x + (Pq + Qs)y = P_1x + Q_1y$$

and

$$RX + SY = R(px + qy) + S(rx + sy) = (Rp + Sr)x + (Rq + Ss)y = R_1x + S_1y$$

we have

$$P_1S_1 - Q_1R_1 = (Pp + Qr)(Rq + Ss) - (Pq + Qs)(Rp + Sr) =$$

$$PRpq + QRrq + PpSs + QrSs - PqRp - PqSr - QsRp - QsSr =$$

$$QR(rq - sp) + PS(ps - qr) = -QR + PS = 1,$$

so

$$f(x, y) = h(P_1x + Q_1y, R_1x + S_1y),$$

with $P_1S_1 - Q_1R_1 = 1$, which is the transitive property.

3.5 If $f \sim g$, $f = (a, b, c)$, $g = (a_1, b_1, c_1)$ with f primitive, then

$$ax^2 + bxy + cy^2 = a_1(px + qy)^2 + b_1(px + qy)(rx + sy) + c_1(rx + sy)^2 =$$

$$(a_1p^2 + b_1pr + c_1r^2)x^2 + (2pqa_1 + (ps + rq)b_1 + 2rsc_1)xy + (q^2a_1 + qsb_1 + c_1s^2)y^2,$$

so if $\gcd(a_1, b_1, c_1) = g$, then $g \bigm| \gcd(a, b, c) = 1$, and the result is secured.

3.7 Applying the substitution $x = pX + qY$ and $y = rX + sY$ to the form

$$f(x, y) = ax^2 + bxy + cy^2,$$

we get the form $AX^2 + BXY + CY^2$, where

$$A = ap^2 + bpr + cr^2,$$

$$B = 2apq + b(ps + qr) + 2crs,$$

$$C = aq^2 + bqs + cs^2.$$

A straightforward calculation shows that

$$B^2 - 4AC = (b^2 - 4ac)(ps - qr)^2,$$

which yields the result.

3.9 If the primitive form $f(x, y)$ properly represents $n \in \mathbb{Z}$, then

$$f(x, y) = nx^2 + bxy + cy^2$$

may be assumed by Exercise 3.2. Therefore, $D = b^2 - 4nc$. Thus, D is a quadratic residue modulo n. If n is even, then $D \equiv b^2 \pmod{8}$ where b is necessarily odd, so $D \equiv 1 \pmod{8}$. Conversely, if $D \equiv b^2 \pmod{|n|}$, where n is odd, we may assume that D and b have the same parity by replacing b by $b + n$, if necessary. Therefore, since $D \equiv 0, 1 \pmod{4}$, then $D \equiv b^2 \pmod{4|n|}$, which implies that there exists an integer m such that $D = b^2 - 4mn$. Hence, $nx^2 + bxy + my^2$ properly represents n and has discriminant D. Lastly, since $\gcd(D, n) = 1$, then $\gcd(n, b, m) = 1$, so $nx^2+bxy+my^2$ is primitive. If n is even and $D \equiv b^2 \pmod{4|n|}$, then there exists an integer m such that $D = b^2 - 4mn$ and we proceed as above.

3.11 Let $f(x, y) = ax^2+bxy+cy^2$ be a reduced form of discriminant $D < 0$. Thus, $b^2 \le a^2$ and $a \le c$. Therefore,

$$-D = 4ac - b^2 \ge 4a^2 - a^2 = 3a^2,$$

whence,

$$a \le \sqrt{(-D)/3}.$$

For D fixed, $|b| \le a$. This together with the latter inequality imply that there are only finitely many choices for a and b. However, since $b^2 - 4ac = D$, then there are only finitely many choices for c. We have shown that there are only finitely many reduced forms of discriminant D. By Theorem 3.1 on page 90, the number of equivalence classes of such forms is finite, which is the required result.

3.13 Since a reduced form has coefficients satisfying $b^2 \le a^2 \le ac$ and $b^2 - 4ac = D$, then

$$D = b^2 - 4ac \le -3ac,$$

so $ac \le -D/3$. When $D = -4n$, this means that

$$ac \le 4n/3. \tag{S10}$$

We use (S10) to test for values up to the bound to prove the result.

When $n = 1$, this means that $ac \le 4/3$ so $a = c = 1$ is forced and $b = 0$. Hence, the only reduced form of discriminant -4 is $x^2 + y^2$. If $n = 2$, then $ac \le 8/3$, so $c = 2$ and $a = 1$ is forced given that ac must be even since $b^2 - 4ac = -8$. Therefore, $b = 0$, and the only reduced form of discriminant -8 is $x^2 + 2y^2$. If $n = 3$, then $ac \le 4$. Again, since ac must be even, $c \ge a$, and $\gcd(a, b, c) = 1$, then $c = 3$, $a = 1$, and $b = 0$ is forced. Thus $x^2 + 3y^2$ is the only primitive reduced form of discriminant -12. (There is one *imprimitive form*, namely $2x^2 + 2xy + 2y^2$, which we do not count.) If $n = 4$, then $ac \le 16/3 < 6$. With the caveats as above, we must have $c = 4$, $a = 1$, $b = 0$, so $x^2 + 4y^2$ is the only primitive reduced form of discriminant -16. (There is one *imprimitive form*, namely $2x^2 + 2y^2$, which we do not count.)

Lastly, if $n = 7$, then $ac \le 28/3 < 9$, and $(b/2)^2 + 7 = ac$, so the only possibility is $c = 7$, $a = 1$, and $b = 0$, so $x^2 + 7y^2$ is the only primitive reduced form of discriminant -28. (There is one *imprimitive form*, namely $2x^2 + 2xy + 4y^2$, which we do not count.)

Section 3.2

3.15 If $\alpha \sim -\alpha$, then there exist $p, q, r, s \in \mathbb{Z}$ such that $ps - qr = 1$ and in the case where $\Delta_F \equiv 0 \pmod 4$,

$$x^2 - \frac{\Delta_F}{4} y^2 = -(px + qy)^2 + \frac{\Delta_F}{4}(rx + sy)^2.$$

By comparing the coefficients of x^2, we get

$$p^2 - \frac{\Delta_F}{4} r^2 = -1,$$

so $p + r\sqrt{\Delta_F/4}$ is a unit of norm -1 in $\mathfrak{O}_F = \mathbb{Z}[\sqrt{\Delta_F/4}]$.

WhenΔ $_F \equiv 1 \pmod 4$, then

$$x^2 + xy + \frac{1 - \Delta_F}{4} y^2 = -(px + qy)^2 - (px + qy)(rx + sy) - \frac{1 - \Delta_F}{4}(rx + sy)^2.$$

By comparing the coefficients of x^2 we get that

$$(2p + r)^2 - \Delta_F r^2 = -4,$$

so

$$p + \frac{1+\sqrt{\Delta_F}}{2} r$$

is a unit of norm -1 in $\mathfrak{O}_F = \mathbb{Z}[(1+\sqrt{\Delta_F})/2]$.

3.17 Since we have that

$$\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} = \frac{I_{\Delta_F}}{P^+_{\Delta_F}} \cong \frac{I_{\Delta_F}}{P_{\Delta_F}} \cdot \frac{P_{\Delta_F}}{P^+_{\Delta_F}},$$

then, when F is real, by Exercise 3.15, $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$ if and only if $\mathfrak{O}_F$ has a unit of norm -1. When F is complex, then $P_{\Delta_F} = P^+_{\Delta_F}$ since all norms are positive, so $\mathbf{C}^+_{\mathfrak{O}_\mathbf{F}} = \mathbf{C}_{\mathfrak{O}_\mathbf{F}}$. This proves the assertion.

3.19 Using the hint, we see that when $b^2 - 4ac = \Delta_F \equiv 0 \pmod 4$, then b is even so

$$acx^2 + bxy + y^2 = (bx/2 + y)^2 - \frac{\Delta_F}{4}x^2$$

since comparing the coefficients of x^2, we get $b^2/4 - \Delta_F/4 = ac$, comparing the coefficients of xy we get $b = b/2 \cdot 2$, and the coefficients of y^2 are both 1. When $\Delta_F \equiv 1 \pmod 4$, then b is odd so

$$acx^2 + bxy + y^2 = \left(-\frac{b+1}{2}x - y\right)^2 + \left(-\frac{b+1}{2}x - y\right)x + \frac{1-\Delta_F}{4}x^2,$$

since comparing the coefficients of x^2 we get

$$\left(\frac{b+1}{2}\right)^2 - \frac{b+1}{2} + \frac{1-\Delta_F}{4} = \frac{b^2+2b+1-2b-2+1-b^2+4ac}{4} = ac,$$

and comparing the coefficients of xy we get

$$2 \cdot \frac{b+1}{2} - 1 = b,$$

and the coefficients of y^2 are both 1.

3.21 Set $\alpha = 1 + u$ if $u \neq -1$, and $\alpha = \sqrt{\Delta_F}$ if $u = -1$. If $u \neq -1$, then

$$(1+u')u = u + uu' = u + N_F(u) = u + 1.$$

Therefore,

$$\frac{\alpha}{\alpha'} = \frac{u+1}{u'+1} = u.$$

If $u = -1$, then

$$\frac{\alpha}{\alpha'} = \frac{\sqrt{\Delta_F}}{-\sqrt{\Delta_F}} = -1 = u,$$

as required.

Section 3.3

3.23 This is proved in the same fashion as the solution of Exercise 2.43 presented on page 378.

3.25 Let $S \subseteq \mathbb{R}^n$ be the set of points defined by the inequalities

$$|F_1(x_1, \ldots, x_n)| < c_1 + \epsilon,$$

and

$$|F_j(x_1, \ldots, x_n)| < c_j \quad (j = 2, \ldots, n),$$

where $0 < \epsilon < 1$. Then S is convex, bounded, and symmetric. Hence,

$$V(S) > \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_n}^{c_n} \frac{1}{|\det(r_{i,j})|} dx_n = 2^n \prod_{k=1}^{n} c_k \frac{1}{|\det(r_{i,j})|} > 2^n D(L).$$

Then Minkowski's Theorem 3.9 yields the result.

3.27 Let L be the set of all points $P \in \mathbb{R}^n$ that satisfy the first system of equations in the exercise for $j = 1, \ldots, k$. Therefore, the implication given in the second display of the exercise guarantees that L is an additive subgroup of $\mathbb{R}^n$. Also, by that implication, if

$$F_j(x) \equiv F_j(y) \pmod{m_j},$$

then x and y are in the same coset of $\mathbb{Z}^n$ modulo L. Hence, the number of such cosets is at most $\prod_{j=1}^{k} m_j$. Thus, L is a free abelian group of finite index in $\mathbb{Z}^n$. Therefore, L has rank n, by Exercise 3.24, so L is a lattice. Also, by Exercise 3.23, $D(L) \leq \prod_{j=1}^{k} m_j$. Hence, $V(S) > 2^n D(L)$. Now, we apply Exercise 3.25 to get the result.

3.29 F is clearly a $\mathbb{Q}$-algebra. Also, if α,β $\in F$, then

$$\Theta_F(\alpha + \beta) = (\theta_1(\alpha + \beta), \ldots, \theta_{r_1+r_2}(\alpha + \beta)) =$$

$$(\theta_1(\alpha) + \theta_1(\beta), \ldots, \theta_{r_1+r_2}(\alpha) + \theta_{r_1+r_2}(\beta)) =$$

$$(\theta_1(\alpha), \ldots, \theta_{r_1+r_2}(\alpha)) + (\theta_1(\beta), \ldots, \theta_{r_1+r_2}(\beta)) = \Theta_F(\alpha) + \Theta_F(\beta),$$

and

$$\Theta_F(\alpha\beta) = (\theta_1(\alpha\beta), \ldots, \theta_{r_1+r_2}(\alpha\beta)) =$$

$$(\theta_1(\alpha)\theta_1(\beta), \ldots, \theta_{r_1+r_2}(\alpha)\theta_{r_1+r_2}(\beta)) =$$

$$(\theta_1(\alpha), \ldots, \theta_{r_1+r_2}(\alpha))(\theta_1(\beta), \ldots, \theta_{r_1+r_2}(\beta)) = \Theta_F(\alpha)\Theta_F(\beta),$$

soΘ_F is a ring homomorphism. If $q \in \mathbb{Q}$, then since $\theta_j(q) = q$ for all j, then $\Theta_F(q\alpha) = q\Theta_F(\alpha)$ for all $q \in \mathbb{Q}$ and $\alpha \in F$. Hence,Θ_F is a $\mathbb{Q}$-algebra homomorphism. Finally, since θ_j is a monomorphism for each j, then it follows thatΘ_F is a $\mathbb{Q}$-algebra monomorphism.

3.31 By Exercise 3.18, $I^{h_F} = (\beta)$ for some $\beta \in \mathfrak{O}_F$. Let $\alpha = \beta^{1/h_F} \in \mathbb{A}$. Since $\mathfrak{O}_{F(\alpha)} = \mathbb{A} \cap F(\alpha)$, then $\alpha \in \mathfrak{O}_{F(\alpha)}$. Also,

$$\left(\mathfrak{O}_{F(\alpha)} I\right)^{h_F} = \mathfrak{O}_{F(\alpha)} I^{h_F} = \mathfrak{O}_{F(\alpha)}(\beta) = \mathfrak{O}_{F(\alpha)}(\alpha)^{h_F} = \left(\mathfrak{O}_{F(\alpha)}(\alpha)\right)^{h_F}.$$

By Theorem 1.17,

$$\mathfrak{O}_{F(\alpha)} I = \mathfrak{O}_{F(\alpha)}(\alpha).$$

3.33 By Exercise 1.45 on page 34, there are $\delta, \mu \in \mathfrak{O}_F$, such that $I = (\delta, \mu)$. Substituting this into the given ideal equation we get,

$$\mathfrak{O}_K(\gamma) = \mathfrak{O}_K(\delta, \mu).$$

Therefore,

$$\gamma = \lambda\delta + \nu\mu$$

for some λ,$\nu \in \mathfrak{O}_K$. By Exercise 3.31, $\delta, \mu \in \mathfrak{O}_{F(\alpha)}(\alpha)$. Thus, there are η,$\zeta \in \mathfrak{O}_{F(\alpha)}$ such that

$$\delta = \eta\alpha, \text{ and } \mu = \zeta\alpha.$$

Hence,

$$\gamma = \lambda\eta\alpha + \nu\zeta\alpha = \alpha(\lambda\eta + \nu\zeta),$$

so $\alpha \bigm| \gamma$ in $\mathbb{A}$. A similar argument shows that $\gamma \bigm| \alpha$. Hence, α and γ are associates in $\mathbb{A}$, so there exists a unit $u \in \mathbb{A}$ such that $\gamma = u\alpha$, as required.

Section 3.4

3.35 For j ranging over the values $1 \le j \le p^a$ with $\gcd(p, j) = 1$, we get

$$\prod_j (x - \zeta_{p^a}^j) = \frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = \sum_{k=0}^{p-1} x^{kp^{a-1}}.$$

Then set $x = 1$.

3.37 By Exercise 3.35,

$$N_F\left(\frac{1 - \zeta_n^j}{1 - \zeta_n}\right) = \frac{N_F(1 - \zeta_n^j)}{N_F(1 - \zeta_n)} = \frac{p}{p} = 1.$$

Also, by Definition 1.32 on page 40 and Exercise 3.35,$\Phi_{\ n}(1) = p$.

3.39 Let $n = \prod_{j=1}^k p_j^{a_j}$ be the canonical prime factorization n. For the balance of the solution, all sums and products range over $j \in \mathbb{N}$ such that $j < p_j^{a_j}$ and $p \nmid j$. A simple induction shows that

$$S = \sum j = \frac{p_j^{2a_j - 1}(p_j - 1)}{2} \equiv 0 \pmod{p_j^{a_j}},$$

since $n > 2$. Therefore, by Theorem 2.5 on page 66,

$$N_F(\zeta_{p_j^{a_j}}) = \left(N_{\mathbb{Q}(\zeta_{p_j^{a_j}})}\left(\zeta_{p_j^{a_j}}\right)\right)^{\phi(n)/\phi(\zeta_{p_j^{a_j}})} = \left(\prod \zeta_{p_j^{a_j}}^j\right)^{\phi(n)/\phi(\zeta_{p_j^{a_j}})} = \zeta_{p_j^{a_j}}^{S\phi(n)/\phi(\zeta_{p_j^{a_j}})} = 1.$$

Thus,

$$N_F(\zeta_n) = N_F\left(\prod_{j=1}^k \zeta_{p_j^{a_j}}\right) = \prod_{j=1}^k \left(N_F\left(\zeta_{p_j^{a_j}}\right)\right) = 1.$$

Section 3.5

3.41 From the additive property of the logarithm, $\mathcal{L}_F(\alpha\beta) = \mathcal{L}_F(\alpha) + \mathcal{L}_F(\beta)$. Hence, $\mathcal{L}_F$ is a group homomorphism.

3.43 If T and U are both even, then $\varepsilon_{\Delta_F} \in \mathbb{Z}[\sqrt{\Delta_F}]$, so since

$$\mathbb{Z}[\sqrt{\Delta_F}] \subseteq \mathfrak{O}_F = \mathbb{Z}[(1+\sqrt{\Delta_F})/2],$$

then $G = \langle \varepsilon_{\Delta_F} \rangle$ if and only if T and U are even.

3.45 Let $I \in \mathbf{C}_{\mathfrak{O}_F,2}$. Then $I^2 \sim 1$ and $I \sim I'$ by the preamble to this exercise. Thus, by Definition 3.7 on page 100, there is an $\alpha \in F$ such that $I = \alpha I'$. Taking norms we have $N(I) = N(I')$, so $N_F(\alpha) = \pm 1$. When$\Delta_F < 0$, then $N_F(\alpha) = 1$. When$\Delta_F > 0$ and $N_F(\alpha) = -1$, we may multiply α by ε_F to get $N_F(\varepsilon_F\alpha) = 1$. Hence, without loss of generality, we may assume that $N_F(\alpha) = 1$. Therefore, by Exercise 3.21, there is a $\beta \in \mathfrak{O}_F$ such that $\alpha = \beta'/\beta$. Therefore, $J = \beta I$ is an ambiguous ideal in $\mathbf{I}$ since

$$J' = \beta' I' = \beta\alpha I' = \beta I = J.$$

3.47 Suppose that $I = (N(I), (b - \sqrt{\Delta_F})/2)$. If

$$I = I' = (N(I), (b - \sqrt{\Delta_F})/2),$$

then

$$(b + \sqrt{\Delta_F})/2 - (b - \sqrt{\Delta_F})/2 = \sqrt{\Delta_F} \in I.$$

Thus, $I \bigm| (\sqrt{\Delta_F})$, so by Exercise 2.46 on page 86, $N(I) \bigm| \Delta_F$.

Conversely, if $N(I) \bigm| \Delta_F$, then by Exercise 1.57 on page 53, $N(I) \bigm| b$ sinceΔ_F is not divisible by the square of any odd prime. Therefore, $-b \equiv 0 (\text{mod } N(I))$, so by Exercise 1.60 on page 54, $I = I'$.

3.49 Suppose that $(\beta) = (\beta')$, where β may be assumed to be primitive. Then there is a unit $u \in \mathfrak{U}_{\mathfrak{O}_F}$ such that $u = \beta/\beta'$. We may assume, without loss of generality, that there are no nontrivial rational integer factors in β. Thus, $u = \pm\varepsilon^n_{\Delta_F}$ for some nonnegative $n \in \mathbb{Z}$. If $u = \varepsilon^n_{\Delta_F}$, then set $\rho = \beta/\alpha^n$. Therefore,

$$\rho' = \beta'/(\alpha')^n = \beta'\beta/((\alpha')^n\beta) = \beta'\beta/(\alpha^n\beta') = \beta/\alpha^n = \rho,$$

where the third equality follows from the fact that

$$\varepsilon^n_{\Delta_F} = (\alpha/\alpha')^n = \beta/\beta' \text{ implies } (\alpha')^n\beta = \alpha^n\beta'.$$

Hence, $\rho = z \in \mathbb{Z}$, so $\beta = \alpha^n z$, but there are no nontrivial rational integer factors in β, so $|z| = 1$. Hence, $\beta = \pm\alpha^n$. However, by Exercise 3.47, $N_F(\beta) = N_F(\alpha^n)$ dividesΔ_F. If $n > 1$, then $|N_F(\alpha)|^n = 4$ is the only possibility, namely $n = 2$ and $N_F(\alpha) = \pm 2$, since the only possible square dividingΔ_F is 4. Thus, $\alpha = x + y\sqrt{D_F}$ for some $x, y \in \mathbb{Z}$ with $x^2 - y^2 D = \pm 2$. Therefore,

$$\begin{aligned} \beta = \pm(x^2 + y^2 D_F + 2xy\sqrt{D_F}) &= \pm(\pm 2 + 2y^2 D_F + 2xy\sqrt{D_F}) \\ &= \pm 2(\pm 1 + y^2 D_F + xy\sqrt{D_F}), \end{aligned}$$

so 2 is a nontrivial rational integer factor of β, a contradiction. Hence, $n = 0$, or $n = 1$. If $n = 1$, then $(\beta) = (\alpha)$, and if $n = 0$, then $(\beta) = (1) = \mathfrak{O}_F$.

If $\beta = -\varepsilon^n_{\Delta_F}\beta'$, then set $\rho = \beta/(\alpha^n\sqrt{D_F})$. Again we get that $\rho = \rho'$ as above. Hence, $\pm\alpha^n\sqrt{D_F} = \beta$, and $N_F(\beta) \bigm| \Delta_F$, so again $n = 0, 1$. Thus, either $(\beta) = (\sqrt{D_F})$ or $(\beta) = (\alpha\sqrt{D_F})$.

3.51 By Exercise 1.57 on page 53, we may set

$$I = (N(I), (b + \sqrt{\Delta_F})/2),$$

so $I' = (N(I), (-b + \sqrt{\Delta_F})/2)$. Then by the multiplication formulas on page 48,

$$II' = (N(I)),$$

with $a_1 = a_2 = N(I) = g$, and $a_3 = 1$.

3.53 By Exercise 3.52, $N_F(\varepsilon_{\Delta_F}) = -1$, where $\varepsilon_{\Delta_F} = (r + s\sqrt{p})/2$ for rational integers $r \equiv s \pmod 2$. By taking

$$x + y\sqrt{p} = \left(\frac{r + s\sqrt{p}}{2}\right)^3,$$

we get that $x^2 - py^2$ equals

$$N_F(x + y\sqrt{p}) = N_F\left(\left(\frac{r + s\sqrt{p}}{2}\right)^3\right) = \left(N_F\left(\frac{r + s\sqrt{p}}{2}\right)\right)^3 = (-1)^3 = -1,$$

where $x, y \in \mathbb{Z}$ is verified by a simple check.

3.55 Assume that I is reduced and let $I = [a,\alpha]$, where $a = N(I)$ and $\alpha = (b + \sqrt{\Delta_F})/2$. Set

$$\beta_0 = \lfloor -\alpha'/a \rfloor a + \alpha \in I.$$

Then, since $\lfloor -\alpha'/a \rfloor > -\alpha'/a - 1$,

$$|\beta_0'| = -\lfloor -\alpha'/a \rfloor a - \alpha' < a.$$

If $\beta_0 < 0$, then $|\beta_0| = -\beta_0 > a$, by the definition of reduction. Therefore,

$$-\lfloor -\alpha'/a \rfloor a - \alpha = -\beta_0 = -\lfloor -\alpha'/a \rfloor a - \alpha > a > |\beta_0'| = -\lfloor -\alpha'/a \rfloor a - \alpha'.$$

Hence,

$$(b - \sqrt{\Delta_F})/2 = \alpha' > \alpha = (b + \sqrt{\Delta_F})/2,$$

namely $-\sqrt{\Delta_F} > \sqrt{\Delta_F}$, a contradiction. Hence, $\beta_0 > 0$. Therefore, there exists a least element $\beta \in I$ such that $|\beta'| < a$ and $\beta > 0$ (possibly $\beta = \beta_0$). Since I is reduced, then $\beta > a$. Also, since $0 < \beta - a < \beta$, then $|\beta' - a| > a$, by the minimality of β. If $\beta' > 0$, then $a - \beta' = |\beta' - a| > a$, so $\beta' < 0$, a contradiction. Hence,

$$-a = -N(I) < \beta' < 0.$$

Since $\beta \in I$, we may let,

$$\beta = am + \alpha n \text{ for some } m, n \in \mathbb{Z}.$$

If $|n| > 1$, then let $m = s + nt$ for $t \in \mathbb{Z}$ and $|s| \le |n|/2$. Set

$$\gamma = |\beta - sa|/n = |\alpha + at| \in I.$$

Therefore,

$$|\gamma'| = |(\beta' - as)/n| \le |\beta'/n| + |as/n| < a/2 + a/2 = a.$$

However,

$$\gamma = |\gamma| \le |\beta/n| + |as/n| < \beta /2 + \beta/2 = \beta,$$

contradicting the minimality of β. Hence, $|n| = \pm 1$. Therefore, by Exercise 1.60 on page 54, $I = [a,\beta]$.

Conversely, suppose that $I = [a,\alpha]$ such that $\alpha > a$, and $-a < \alpha' < 0$. If I is not reduced, there is a $\gamma \in I$ such that $|\gamma| < a$ and $|\gamma'| < a$. Since $\gamma = ma + n\alpha$ for some $m, n \in \mathbb{Z}$, then

$$|ma + n\alpha| < a, \tag{S11}$$

and

$$|ma + n\alpha'| < a. \tag{S12}$$

If $mn > 0$, then (S11) is contradicted. If $mn < 0$, then (S12) is contradicted. Thus, $mn = 0$. If $m = 0$, and $n \neq 0$, then (S11) implies that $|\alpha| < a$, a contradiction. If $n = 0$, and $m \neq 0$, then (S12) yields a contradiction. Therefore, $m = n = 0$, and I is reduced.

3.57 First, assume that F is real. If I is reduced, then by Exercise 3.55, there is a $\beta \in I$ such that $\beta > N(I)$, $-N(I) < \beta' < 0$, and $I = (N(I), \beta)$. Therefore,

$$N(I) < \beta - \beta' = \omega_{\Delta_F} - \omega'_{\Delta_F} = \sqrt{\Delta_F}.$$

If F is complex, and $I = (N(I), \alpha)$, then

$$4N_F(\alpha) - T_F(\alpha)^2 = -\Delta_F.$$

If I is reduced, then $|\alpha| \geq N(I)$, and since $|T_F(\alpha)| \leq N(I)$, then

$$-\Delta_F = 4N_F(\alpha) - T_F(\alpha)^2 \geq 4N_F(\alpha) - N(I)^2 =$$

$$4|\alpha|^2 - N(I)^2 \geq 4N(I)^2 - N(I)^2 = 3N(I)^2.$$

3.59 If I is not reduced, so that $4 \mid \Delta_F$ and $\sqrt{\Delta_F}/2 \in I$, then set $\beta = \sqrt{\Delta_F}/2$. Otherwise, set $\beta = \sqrt{\Delta_F}$. By Exercises 3.56 and 3.58, $N(I) > \beta$, or I is already reduced. Since $\beta \in I$, there exists an $\mathfrak{O}_F$-ideal J such that $IJ = (\beta)$, by Corollary 1.7 on page 27. Since $\beta' = -\beta$, then $|N_F(\beta)| = \beta^2$ and $N(J) < \beta$. Since $I = I'$, then $J = J'$. Hence, J is reduced. Since $IJ \sim 1$, then $I^2 J \sim I$. However, $I^2 \sim 1$ by Exercise 3.47 and Exercise 3.20 on page 107. Therefore, $I \sim J$.

3.61 Let $I = (N(I), b + \omega_{\Delta_F})$, and set $J = (n, b + \omega_{\Delta_F})$. Since

$$N(I) \mid N_F(b + \omega_{\Delta_F}), \text{ and } n \mid N(I),$$

then J is an $\mathfrak{O}_F$-ideal. If n is even, and and$\Delta\ _F \equiv 0 \pmod 4$, then $(2) \mid I$, contradicting the primitivity of I. Therefore, since

$$4N_F(b + \omega_{\Delta_F}) = (2b + \omega_{\Delta_F} + \omega'_{\Delta_F})^2 - \Delta_F,$$

then $\gcd(n, 2b + \omega_{\Delta_F} + \omega'_{\Delta_F}) = 1$. Thus, by the multiplication formulas given on page 48,

$$J^2 = (n^2, b + \omega_{\Delta_F}) = I.$$

Section 4.1

4.1 We have that $(-3/p) = (-1/p)(3/p) = 1$ if and only if $(-1/p) = (3/p) = -1$ or $(-1/p) = (3/p) = 1$. Thus, from the hint, $(-3/p) = 1$ if and only if either $p \equiv -1 \pmod 4$ and $p \equiv \pm 5 \pmod{12}$, or else $p \equiv 1 \pmod 4$ and $p \equiv \pm 1 \pmod{12}$. In other words, $(-3/p) = 1$ if and only if either $p \equiv -5 \pmod{12}$ or $p \equiv 1 \pmod{12}$, and this holds if and only if $p \equiv 1 \pmod 3$.

4.3 Since $(-11/p) = (-1/p)(11/p) = 1$ if and only if $(-1/p) = (11/p) = -1$ or $(-1/p) = (11/p) = 1$, then $(-11/p) = 1$ if and only if either $p \equiv -1 \pmod 4$ and $p \equiv 1, 3, 4, 5, 9 \pmod{11}$, or else $p \equiv 1 \pmod 4$ and $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. In other words, $(-11/p) = 1$ if and only if either $p \equiv 3, 15, 23, 27, 31 \pmod{44}$ or $p \equiv 1, 5, 9, 21, 25 \pmod{44}$, and this holds if and only if

$$p \equiv 1, 3, 5, 9, 15, 21, 23, 25, 27, 31 \pmod{44}.$$

By Corollaries 1.1–1.2 on page 13, Theorem 1.28 on page 45, and Theorem 3.6 on page 103, we have that $h_{-11} = h_{\mathbb{Z}[(1+\sqrt{-11})/2]} = 1$. Thus, by Theorem 4.1, if $(\Delta_F/p) = (-11/p) = 1$, then $p = a^2 + ab + 3b^2$ for some integers a, b. Also $11 = (-1)^2 - 1 \cdot 2 + 3 \cdot 2^2$. Conversely, by Exercise 3.9, if $p \neq 11$ and $p = a^2 + ab + 3b^2$, then $(-11/p) = 1$.

4.5 Given that $(-43/p) = (-1/p)(43/p) = 1$ if and only if $(-1/p) = (43/p) = -1$ or $(-1/p) = (43/p) = 1$, then $(-43/p) = 1$ if and only if either $p \equiv -1 \pmod 4$ and

$$p \equiv 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23,$$
$$24, 25, 31, 35, 36, 38, 40, 41 \pmod{43}, \tag{S13}$$

or else $p \equiv 1 \pmod 4$ and (S13) holds. This implies that $(-43/p) = 1$ if and only if either

$$p \equiv 11, 15, 23, 31, 35, 47, 59, 67, 79, 83, 87, 95, 99,$$
$$103, 107, 111, 127, 135, 139, 143, 167 \pmod{172}, \tag{S14}$$

or

$$p \equiv 1, 9, 13, 17, 21, 25, 41, 49, 53, 57, 81, 97, 101, 109,$$
$$117, 121, 133, 145, 153, 165, 169 \pmod{172}, \tag{S15}$$

Lastly, (S14)–(S15) hold if and only if

$$p \equiv 1, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81,$$
$$83, 87, 95, 97, 99, 101, 103, 107, 109, 111, 117, 121, 127, 133,$$
$$135, 139, 143, 145, 153, 165, 167, 169 \pmod{172}.$$

Now, as in the solution of Exercise 4.3, we have that $h_{-43} = h_{\mathbb{Z}[(1+\sqrt{-43})/2]} = 1$. Thus, by Theorem 4.1, if $(\Delta_F/p) = (-43/p) = 1$, then $p = a^2 + ab + 11b^2$ for some integers a, b. Also $43 = (-1)^2 - 1 \cdot 2 + 11 \cdot 2^2$. Conversely, by Exercise 3.9, if $p \neq 43$ and $p = a^2 + ab + 11b^2$, then $(-43/p) = 1$.

4.7 The following are all the prime values for class number one negative discriminants via Rabinowitsch.

$-\Delta_F$	$x^2+x+(1-\Delta_F)/4$	for $x=0,1,\ldots,\lfloor\lvert\Delta_F\rvert/4-1\rfloor$
3	x^2+x+1	–
7	x^2+x+2	2.
11	x^2+x+3	3, 5.
19	x^2+x+5	5, 7, 11, 17.
43	x^2+x+11	11, 13, 17, 23, 31, 41, 53, 67, 83, 101.
67	x^2+x+17	17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227, 257.
163	x^2+x+41	41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

4.9 First we note that, using the notation in the proof of Theorem 3.5,

$$\tau : J = (2, 1+\sqrt{-5}) \mapsto (2,2,3),$$

and

$$\tau : I = (1, \sqrt{-5}) \mapsto (1,0,5)$$

where $J \not\sim 1$ in $\mathbf{C}_{\mathfrak{O}_\mathbf{F}}$. The latter holds since $(1,0,5)$ and $(2,2,3)$ are reduced forms so if they were properly equivalent, then they would be identical by Claim 3.1 on page 90. Also, we note that $J^2=(2)$.

For part (a), If $p \equiv 1,9 \pmod{20}$, then $(-5/p)=1$ so by Theorem 1.30 on page 49 and Remark 1.24 on page 52 $(p)=\mathcal{P}\mathcal{P}'$, where $\mathcal{P}=(p,(b+\sqrt{-20})/2)$ and $\mathcal{P}'=(p,(-b+\sqrt{-20})/2)$. Now, if $\mathcal{P}$ is principal, then $\mathcal{P}=(a+b\sqrt{-5})$ for some integers a,b. Thus,

$$(p)=\mathcal{P}\mathcal{P}'=(a+b\sqrt{-5})(a-b\sqrt{-5})=(a^2+5b^2),$$

so since $N(\mathcal{P})=p$, then $p=a^2+5b^2$, as required. If $\mathcal{P}$ is not principal, then $\mathcal{P}\sim J$, so $\mathcal{P}J \sim J^2 \sim 1$. Hence, there are integers x,y so that $\mathcal{P}J=(x+y\sqrt{-5})$, so

$$N(\mathcal{P}J)=N(\mathcal{P})N(J)=2p=x^2+5y^2.$$

Thus, both x and y are odd, so $2p \equiv 6 \pmod 8$, whence, $p \equiv 3 \pmod 4$, a contradiction. We have established one direction for part (a). Conversely, if $p=a^2+5b^2$, then $(p/5)=(a^2/5)=1$, so $p\equiv 1,4 \pmod 5$. Also, since one of a,b must be even, then $p\equiv 1 \pmod 4$. Hence, $p \equiv 1,9 \pmod{20}$, as required.

For part (b), first assume that $p\equiv 3,7 \pmod{20}$. Then $(-5/p)=1$ since $(-1/p)=-1=(5/p)$. As above $(p)=\mathcal{P}\mathcal{P}'$. If $\mathcal{P}$ is principal, then as above $p=a^2+5b^2$, which means that $p\equiv 1 \pmod 4$, a contradiction. Thus, as above $2p=x^2+5y^2$ for some integers x,y. Thus, x and y must have the same parity, so we may select an integer z such that $x=y+2z$. Therefore,

$$2p=(y+2z)^2+5y^2=4z^2+4yz+6y^2,$$

and dividing through by 2, we get

$$p=2z^2+2yz+3z^2.$$

We have established one direction for part (b). Conversely, assume that there are integers a, b with $p = 2a^2 + 2ab + 3b^2$. Then

$$2p = x^2 + 5y^2,$$

where $x = 2a + b$ and $y = b$. Thus, as above, $p \equiv 3 \pmod 4$. Also, $(-5/p) = 1$ by Exercise 3.9. Therefore, $1 = (-5/p) = (-1/p)(5/p) = -(5/p)$, so $(5/p) = (5/p) = -1$. Thus, $p \equiv 2, 3 \pmod 5$, whence $p \equiv 3, 7 \pmod{20}$, which secures part (b) .

Section 4.2

4.11 Since $I^{h_{\mathfrak{O}_F}} \sim 1$, $I^n \sim 1$, and $\gcd(h_{\mathfrak{O}_F}, n) = 1$, then there exist integers x, y such that $nx + h_{\mathfrak{O}_F} y = 1$. Therefore,

$$I = I^{nx+h_{\mathfrak{O}_F}y} = (I^n)^x (I^y)^{h_{\mathfrak{O}_F}} \sim 1,$$

as we sought to prove.

4.13 In Theorem 4.2, let $k = -13 = -1 - 3u^2$ with $u = 2$, for which $x = p^m = 4u^2 + 1 = 17$ with $m = 1$ and $y = \pm 2(3 + 8 \cdot 2^2) = \pm 70$. Thus, $p = 2^2 + 13$, and $70^2 = 17^3 - 13$. Thus, $(x, y) = (17, \pm 70)$.

4.15 As per the hint, a solution (x, y) to (4.2) implies that

$$y + \sqrt{k} = w(u + v\sqrt{k})^3 \tag{S16}$$

for a unit $w \in \mathfrak{O}_F$ and some $u, v \in \mathbb{Z}$. Then $w = \pm\varepsilon_k^z$ for some $z \in \mathbb{Z}$. Since we may write $z = 3z_1 + r$ where $r \in \{0, \pm 1, \pm 2\}$, then we may absorb $(\pm\varepsilon_k^{z_1})^3$ into the cube $(u + v\sqrt{k})^3$, so we may assume, without loss of generality, that $w = \varepsilon_k^r$, where $r \in \{0, \pm 1, \pm 2\}$. Given the definition of ε and the fact that $(T + U\sqrt{k})^{-1} = T - U\sqrt{k}$, then we may assume $w \in \{\varepsilon_k^j : j = 0, 1, -1\}$ if ε_k has norm 1 and

$$w \in \{\varepsilon_k^j : j = 0, 2, -2\}$$

if ε_k has norm -1. In either case, $w \in \{\varepsilon^j : j = 0, 1, -1\}$.

Case S.7 $w = 1$

From (S16),

$$y + \sqrt{k} = (u^3 + 3uv^2k) + (3u^2v + v^3k)\sqrt{k},$$

so by comparing coefficients of $\sqrt{k}$, we have that

$$1 = 3u^2v + v^3k = v(3u^2 + v^2k), \tag{S17}$$

so $v = \pm 1$. Hence, multiplying (S17) by v yields

$$\pm 1 = v = 3u^2v^2 + v^4k \geq k > 1,$$

a contradiction.

Case S.8 $w \in \{T \pm U\sqrt{k}\}$

From (S16) we have

$$y+\sqrt{k}=(T\pm U\sqrt{k})(u+v\sqrt{k})^3=(T\pm U\sqrt{k})\left((u^3+3uv^2k)+(3u^2v+v^3k)\sqrt{k}\right)$$

$$=(T(u^3+3uv^2k)\pm(Uk(3u^2+v^3k))+(T(3u^2v+v^3k)\pm U(u^3+3uv^2k))\sqrt{k}.$$

Therefore, by comparing coefficients of $\sqrt{k}$ again yields

$$1=T(3u^2v+v^3k)\pm U(u^3+3uv^2k). \tag{S18}$$

Since $k\equiv 4 \pmod 9$ and $U\equiv 0 \pmod 9$, then $1=T^2-kU^2$ implies that

$$T\equiv\pm 1 \pmod{81}.$$

Hence, by (S18),

$$1\equiv\alpha(3u^2+4v^2)v \pmod 9, \tag{S19}$$

where $\alpha\equiv\pm 1 \pmod 9$.

From (S19), $\alpha v\equiv\pm 1 \pmod 9$, so

$$3u^2+4\equiv\alpha v\equiv\pm 1 \pmod 9.$$

Thus,

$$3u^2\equiv 4,6 \pmod 9,$$

which are impossible. This completes all cases.

Section 4.3

4.17 According to the hint, if $\sum_{j=1}^{\infty}(1/j)=d\in\mathbb{R}$. Then there is an $N\in\mathbb{N}$ such that $N\le d<N+1$. Also, note that

$$\sum_{j=1}^{\infty}\frac{1}{j}=1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\cdots>1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\cdots$$

so each block has a sum bigger than 1/2. Let $M\in\mathbb{N}$ be chosen such that the number of blocks larger than 1/2 satisfies $M\ge 2N$. Then

$$d=\sum_{j=1}^{\infty}\frac{1}{j}>1+\frac{2M}{2}\ge N+1,$$

a contradiction.

4.19 By Exercise 3.37 on page 129, $1-\zeta_p$ and $1-\zeta_p^j$ are associates for all $j=1,2,\ldots,p-1$. By Exercise 2.24 on page 68, we have the ideal equation

$$\prod_{j=1}^{p-1}(1-\zeta_p^j)=(p).$$

However, given the comment on associates,

$$(1-\zeta_p^j)=(1-\zeta_p)=(\lambda),$$

so

$$(\lambda)^{p-1}=(p),$$

as required.

4.21 If $k \equiv 1 \pmod{p}$, then congruence (4.23) on page 153 becomes

$$x(\zeta_p^{-1} - \zeta_p) \equiv 0 \pmod{(p)}.$$

In the same fashion as in the elimination of the case $k \equiv 0 \pmod{p}$, we get that $p \mid x$, contradicting the hypothesis.

4.23 First, we show that

$$f(x) = \frac{x}{e^x - 1} + \frac{x}{2}$$

is an even function, namely that $f(x) = f(-x)$. We have

$$2f(-x) = -x\left(\frac{e^{-x}+1}{e^{-x}-1}\right) = -x\left(\frac{1+e^x}{1-e^x}\right) = x\left(\frac{e^x+1}{e^x-1}\right) = 2f(x).$$

Therefore, by Definition 4.1,

$$\frac{x}{e^x-1} + \frac{x}{2} = 1 + \sum_{n=2}^{\infty} \frac{B_n}{n!} x^n = 1 + \sum_{n=2}^{\infty} \frac{B_n}{n!} (-x)^n,$$

so

$$\sum_{n=2}^{\infty} \frac{B_n}{n!} \left[x^n - (-x)^n\right] = 0.$$

Therefore, the even terms subtract out and we are left with:

$$2\sum_{m=1}^{\infty} \frac{B_{2m+1}}{(2m+1)!} x^{2m+1} = 0,$$

which implies that each coefficient $B_{2m+1} = 0$, as required.

4.25 This is immediate from Definition 2.8 on page 83 and Definition A.11 on page 327, since the different cosets of I in $\mathfrak{O}_F$ form the different residue classes modulo I.

4.27 This will follow from Exercise 2.47 on page 86 once we establish the result for any prime power. The integers in $\mathfrak{O}_F$ that are *not* relatively prime to $\mathcal{P}^a$ are those divisible by $\mathcal{P}$. There are $N(\mathcal{P}^{a-1}) = (N(\mathcal{P}))^{a-1}$ of these that are incongruent modulo $\mathcal{P}^a$. Thus,

$$\boldsymbol{\Phi}(\mathcal{P}^a) = N(\mathcal{P})^a - N(\mathcal{P})^{a-1} = N(\mathcal{P}^a)\left(1 - \frac{1}{N(\mathcal{P})}\right).$$

4.29 Since f is the product of d linear factors in its algebraic closure, then it has exactly d roots there.

4.31 This follows from Exercises 4.28 and 4.30. Since the residue classes modulo I, relatively prime to I, form a group of order $\boldsymbol{\Phi}(I)$, then

$$\alpha^{\boldsymbol{\Phi}(I)} \equiv 1 \pmod{I},$$

for any $\alpha \in \mathfrak{O}_F$ relatively prime to I. In particular, if $I = \mathcal{P}$, a prime $\mathfrak{O}_F$-ideal, then $\boldsymbol{\Phi}(\mathcal{P}) = N(\mathcal{P}) - 1$, so

$$\alpha^{N(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}}.$$

Section 4.4

4.33 Let $F = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{-2}$. Since $|\Delta_F|$ is minimal over all discriminants of bases for F over $\mathbb{Q}$, then by Theorem 2.7 on page 71,

$$\operatorname{disc}\{1, \alpha, \alpha^2\} = D^2 \Delta_F,$$

where $D = |\mathfrak{O}_F : \mathbb{Z}[\alpha]|$. Also, we compute

$$\operatorname{disc}\{1, \alpha, \alpha^2\} = -108 = -2^2 \cdot 3^3.$$

Since

$$|\mathfrak{O}_F : \mathbb{Z}| = |\mathfrak{O}_F : \mathbb{Z}[\alpha]| \cdot |\mathbb{Z}[\alpha] : \mathbb{Z}| = 3,$$

then D must be odd. If $D > 1$ then $3 \mid D$. Since $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha + 2] = \mathbb{Z}[a]$, where $a = \alpha + 2$, we choose to work with the latter at this stage. Since $3 \mid D$, there must exist a $\beta \in \mathbb{Z}[a]$ such that

$$\beta = \frac{b_0 + b_1 a + b_2 a^2}{3},$$

where 3 does not divide all of the integers b_j for $j = 0, 1, 2$. Suppose that $3 \mid b_0$ but $3 \nmid b_1$. Then $\beta - b_0/3 = (b_1 a + b_2 a^2)/3 \in \mathfrak{O}_F$. Also, $\gamma = b_1 a^2/3 = (\beta - b_0/3)a - a^3 b_2/3 \in \mathfrak{O}_F$ since $a/3$ is an algebraic integer given that it is a root of

$$(3x - 2)^3 + 2 = 27x^3 - 54x^2 + 36x - 6.$$

Therefore,

$$3^3 N_F(\gamma) = N_F(3\gamma) = N_F(b_1 a^2) = b_1^3 N_F(a)^2 = -4b_1^3,$$

so $3 \mid b_1$, a contradiction. The other cases such as $3 \mid b_1$ but $3 \nmid b_0$ are handled similarly. Thus, $D = 1$, $\operatorname{disc}\{1, \alpha, \alpha^2\} = \Delta_F$, and $\mathbb{Z}[\alpha] = \mathfrak{O}_F$.

4.35 Since, for a primitive cube root of unity ζ_3, we have

$$N_F(\beta) = (a + b\alpha + c\alpha^2)(a + b\zeta_3\alpha + c\zeta_3^2\alpha^2)(a + b\zeta_3^2\alpha + c\zeta_3^4\alpha^2),$$

then using the fact that $\sum_{j=0}^{2} \zeta_3^j = 0$ we get

$$N_F(\beta) = (a + b\alpha + c\alpha^2)((a^2 + 2bc) - (ab + 2c^2)\alpha + (b^2 - ac)\alpha^2),$$

so, by simplifying,

$$N_F(\beta) = a^3 - 2b^3 + 4c^3 + 6abc.$$

4.37 Since $(5^7 - 1) \mid (5^{77} - 1)$ and $4 \mid (5^7 - 1)$, then $(5^7 - 1)/4 = 19531 \mid (5^{77} - 1)$.

4.39 Since $3(3^{239} - 1) = 3^{240} - 3 = x^3 - 3$, where $x = 3^{80}$, and $N_F(a + b\sqrt[3]{3}) = a^3 + 3b^3$, for $F = \mathbb{Q}(\sqrt[3]{3})$, then $N_F(x - \sqrt[3]{3}) = x^3 - 3$. An initial run shows that

$$\gcd(3^{240} - 3, a^3 + 3b^3) = 479,$$

for $a = 14$, and $b = 185$, so $479 | (3^{239} - 1)$.

4.41 $n = 12358397 = 3361 \cdot 3677$.

4.43 $n = 74299271 = 7789 \cdot 9539$.

Section 4.5

4.45 Here $r = 2$, $s = -3$, and $t = 153$, for $n = 2^{153} + 3$. Thus, from (4.52), $k = 77$, $m = 2^{77}$, and $c = -6$. We select d as in (4.51), to get $d = 2$. Thus,

$$f(x) = x^2 + 6 \text{ with } \alpha = \sqrt{6},$$

and $F = \mathbb{Q}(\sqrt{6})$ having ring of integers $\mathbb{Z}[\sqrt{6}]$ a UFD. A smoothness bound need not be chosen large since an initial run produces

$$\gcd(a + b \cdot 2^{77}, n) = 5 \text{ for } a = 3, b = 1,$$

and

$$\gcd(a + b \cdot 2^{77}, n) = 11 \text{ for } a = 15, b = 1,$$

so 5 and 11 are factors. In fact

$$2^{153} + 3 =$$

$$5 \cdot 11 \cdot 600696432006490087537 \cdot 345598297796034189382757.$$

Section 5.1

5.1 That $\mathfrak{I} \subseteq \mathfrak{I}\mathfrak{O}_K \cap F$ is clear. We now establish the reverse inclusion. By Remark 1.13 on page 26, there exists a $\beta \in \mathbb{A}$ such that $\beta\mathfrak{I} \subseteq \mathfrak{O}_F$. Thus, by Exercise 3.31, there exists an $\alpha \in \mathbb{A}$ such that

$$\alpha\mathfrak{O}_K = \beta\mathfrak{I}\mathfrak{O}_K.$$

Also, by Exercise 3.32,

$$\beta\mathfrak{I}\mathfrak{O}_K \cap F = \alpha\mathfrak{O}_K \cap F \subseteq \mathfrak{O}_F(\alpha) \cap F = \beta\mathfrak{I},$$

so $\beta\mathfrak{I}\mathfrak{O}_K \cap F \subseteq \beta\mathfrak{I}$, from which we get $\mathfrak{I}\mathfrak{O}_K \cap F \subseteq \mathfrak{I}$. Hence, $\mathfrak{I}\mathfrak{O}_K \cap F = \mathfrak{I}$ as required. The last statement in the exercise follows from the above result since

$$\mathfrak{I} = \mathfrak{I}\mathfrak{O}_K \cap F = \mathfrak{J}\mathfrak{O}_K \cap F = \mathfrak{J}.$$

5.3 Suppose that $\mathfrak{I} = \prod_{j=1}^n \mathcal{P}_j^{a_j}$ and $\mathfrak{J} = \prod_{j=1}^n \mathcal{Q}_j^{b_j}$, where the $\mathcal{P}_j$ and $\mathcal{Q}_j$ are distinct prime $\mathfrak{O}_K$-ideals, with $a_j, b_j \in \mathbb{Z}$, and set $f_{K/F}(\mathcal{P}_j) = f_j$, $f_{K/F}(\mathcal{Q}_j) = h_j$. Suppose further that $\mathcal{P}_j = \mathcal{Q}_j$ for $j = 1, 2, \ldots, m \leq n$, where possibly $m = 0$, meaning that $\mathfrak{I}$ and $\mathfrak{J}$ do not agree on any of the prime factors. Then if $\mathfrak{p}_j = \mathcal{P}_j \cap \mathfrak{O}_F$ and $\mathfrak{q}_j = \mathcal{Q}_j \cap \mathfrak{O}_F$, then

$$N^{K/F}(\mathfrak{I})N^{K/F}(\mathfrak{J}) = \prod_{j=1}^{n} \mathfrak{p}_j^{a_j f_j} \prod_{j=1}^{n} \mathfrak{q}_j^{b_j h_j} = \prod_{j=1}^{m} \mathfrak{p}_j^{(a_j+b_j)f_j} \prod_{j=m+1}^{n} \mathfrak{p}_j^{a_j f_j} \mathfrak{q}_j^{b_j h_j} = N^{K/F}(\mathfrak{I}\mathfrak{J}).$$

5.5 By Exercise 1.38, there exists an ideal H such that $HJ = (\alpha)$ for some $\alpha \in R$. Therefore, $JH \not\subseteq \alpha I$, for if $\alpha \in \alpha I$, then $\alpha = \alpha\sigma$ for some $\sigma \in I$, so by the cancellation law, $\sigma = 1 \in I$, contradicting that $I \neq R$. If we choose and fix a $\beta \in H$ such that $\beta J \not\subseteq \alpha I$, we may set $\gamma = \beta/\alpha \in F$. This forces $\gamma J = (\beta/\alpha)J \not\subseteq I$. Also, since $\beta \in H$ and $HJ = (\alpha)$, then for any $\delta \in J$, $\beta\delta = \alpha r$ for some $r \in R$. Hence, $\gamma J \subseteq R$.

5.7 It suffices to prove this for a prime $\mathfrak{O}_F$-ideal $I = \mathfrak{p}$ by Exercise 5.3. Suppose that

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathcal{P}_j^{e_j}, \text{ where } e_j = e_{K/F}(\mathcal{P}_j) \text{ and } g = g_{K/F}(\mathfrak{p}).$$

Then

$$N^{K/F}(\mathfrak{p}) = \prod_{j=1}^{g} N^{K/F}(\mathcal{P}_j)^{e_j} = \prod_{j=1}^{g} \mathfrak{p}^{e_j f_j} = \mathfrak{p}^{\sum_{j=1}^{g} e_j f_j} = \mathfrak{p}^n,$$

by Theorem 5.3 where $f_j = f_{K/F}(\mathcal{P}_j)$.

5.9 Set $f(x) = \sum_{j=0}^{d} a_j x^j$ with $a_d \neq 0$. Then, if $a_0 = 0$, $f(p) \equiv 0 \pmod{p}$ for all primes p, so we assume that $a_0 \neq 0$. If $p_1, p_2, \dots p_k$ are all of the primes that divide $f(x)$, and if $c = a_0 \prod_{i=1}^{k} p_i$, then $f(cy) = a_0 g(y)$ where

$$g(y) = \sum_{j=0}^{d} a_j \left(\prod_{i=1}^{k} p_i \right)^{j} a_0^{j-1} y^j \equiv 1 \pmod{p_i}$$

for all $i = 1, 2, \dots, k$. Thus, $p_i \nmid g(y)$ for all such i. Therefore, $|g(y)| = 1$ for all nonzero $y \in \mathbb{Z}$. By Lagrange's Theorem A.7, the congruences

$$g(y) \equiv 1 \pmod{p} \text{ and } g(y) \equiv -1 \pmod{p}$$

each have at most d solutions each for any prime p, so there must exist a $y \in \mathbb{Z}$ such that a $p | g(y)$ for some prime $p \neq p_i$ for any $1 \leq i \leq k$, a contradiction.

5.11 We use Theorem 1.30 to conclude the following facts. If $p \equiv 1 \pmod{4}$, then p splits in $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_{2^n})$. If $p \equiv 3 \pmod{8}$, then p splits in $\mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_{2^n})$, and if $p \equiv 7 \pmod{8}$, then p is split in $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_{2^n})$. Since $p = 2$ ramifies, we are done.

Section 5.2

5.13 If $\mathfrak{O}_K = \mathfrak{O}_F[\alpha]$, then $\mathfrak{O}_K^* = \mathfrak{O}_K / m'_{\alpha,F}(\alpha)$, by Theorem 5.8, so

$$(\mathfrak{O}_K^*)^{-1} = \mathfrak{O}_K^{-1} m'_{\alpha,F}(\alpha) = \mathfrak{O}_K m'_{\alpha,F}(\alpha).$$

Conversely, if $\mathfrak{O}_K^* = \mathfrak{O}_K / m'_{\alpha,F}(\alpha)$, we need only show that any $\beta \in \mathfrak{O}_K$ is in $\mathfrak{O}_F[\alpha]$. However, by the Lagrange Interpolation Formula, there is a polynomial $f(x) \in F[x]$ such that $f(\alpha) = \beta$. Hence, $\beta \in F[\alpha]$. Therefore, $\beta \in F[\alpha] \cap \mathfrak{O}_K = \mathfrak{O}_F[\alpha]$.

5.15 We use induction on n. If $n = 1$, then the result is clear. The induction hypothesis is that the result holds for $n - 1$. Since

$$\mathfrak{d}(\alpha^n) = \alpha \mathfrak{d}(\alpha^{n-1}) + \alpha^{n-1} \mathfrak{d}(\alpha),$$

then

$$\mathfrak{d}(\alpha^{n-1}) = (n-1)\alpha^{n-2} \mathfrak{d}(\alpha),$$

by the induction hypothesis, so

$$\mathfrak{d}(\alpha^n) = (n-1)\alpha^{n-1} \mathfrak{d}(\alpha) + \alpha^{n-1} \mathfrak{d}(\alpha) = n\alpha^{n-1} \mathfrak{d}(\alpha).$$

5.17 By employing Theorem 5.7, it is straightforward to verify that $I^* = (\frac{1}{4}, \frac{\sqrt{10}}{20})$. Thus, $I^{*-1} = (20, 4\sqrt{10})$. By part 1 of Lemma 5.4,

$$I^{*-1} = (20, 4\sqrt{10}) = 2\sqrt{10}I = \mathcal{D}_{F/\mathbb{Q}}(I) = I\mathcal{D}_{F/\mathbb{Q}},$$

so $\mathcal{D}_{F/\mathbb{Q}} = (2\sqrt{10})$. Thus,$\Delta_{F/\mathbb{Q}} = (40) = (\Delta_F)$. Note that $N_F(2\sqrt{10}) = -40$, but as ideals, $(-40) = (40)$, where$\Delta_F = 40$ is also given by Application 2.1 on page 77.

Section 5.3

5.19 (a) Since $N^{K/F}(I), N^{K/F}(J)$ are $\mathfrak{O}_F$-ideals, then the result follows from Corollary 1.7.

(b) If the desired norms are not relatively prime, there is a prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ dividing both. Thus, $\mathfrak{p}\mathfrak{O}_K \mid N^{K/F}(J)\mathfrak{O}_K$, so $\mathfrak{p}\mathfrak{O}_K$ is relatively prime to I. Therefore, no prime above $\mathfrak{p}$ occurs in the factorization of I. In particular, $\mathfrak{p}$ does not divide $N^{K/F}(I)$, a contradiction.

5.21 This proceeds much the same as in the proof of Theorem 5.12 on page 214. Let $\alpha \in \mathfrak{O}_{K_1}$. Therefore, $m_{\alpha,K_2}(x) \mid m_{\alpha,F}(x)$, so there exists a monic $f(x) \in \mathfrak{O}_{K_2}[x]$ such that

$$m_{\alpha,F}(x) = m_{\alpha,K_2}(x)f(x).$$

Thus,

$$m'_{\alpha,F}(\alpha) = m'_{\alpha,K_2}(\alpha)f(\alpha),$$

so $m'_{\alpha,F}(x) \in \mathcal{D}_{L/K_2}$. Therefore, by Theorem 5.9, $\mathcal{D}_{K_1/F} \subseteq \mathcal{D}_{L/K_2}$, namely

$$\mathcal{D}_{L/K_2} \mid \mathcal{D}_{K_1/F}\mathfrak{O}_L.$$

5.23 Suppose that $\mathfrak{p}\mathfrak{O}_L = \prod_{j=1}^{g} \mathcal{P}_j^{e_j}$ for distinct prime $\mathfrak{O}_L$-ideals $\mathcal{P}_j$. Since we have that $\mathfrak{p} \nmid N^{L/K}(\mathfrak{f}_\alpha)$, then $\mathcal{P}_j \nmid \mathfrak{f}_\alpha$ for all such j. By the Chinese Remainder Theorem for ideals, there exists a $\beta \in \mathfrak{O}_K[\alpha]$ such that

$$\beta \equiv 0 \pmod{\mathfrak{f}_\alpha} \text{ and } \beta \equiv 1 \pmod{\mathcal{P}_j} \text{ for all } j = 1, 2, \ldots g.$$

We may let $\beta = g(\alpha)$ for some polynomial $g(x) \in \mathfrak{O}_K[x]$. Then, for any $\gamma \in \mathfrak{O}_L$, we may write $\gamma = h(\alpha)/g(\alpha)$ for some $h(x) \in \mathfrak{O}_K[x]$. Since $\gcd(\beta\mathfrak{O}_L, \mathfrak{p}\mathfrak{O}_L) = 1$, there exists an $n \in \mathbb{N}$ such that

$$g(\alpha)^n \equiv 1 \pmod{\mathfrak{p}\mathfrak{O}_L}.$$

Therefore,

$$\gamma \equiv g(\alpha)^{n-1}h(\alpha) \pmod{\mathfrak{p}\mathfrak{O}_L}.$$

By setting $k(\alpha) = g(\alpha)^{n-1}h(\alpha)$, we get the result.

5.25 Clearly we have

$$|\alpha + \beta| \le \max\{|\alpha|, |\beta|\} = |\beta|.$$

Also, since $\beta = (\alpha + \beta) - \alpha$, then

$$|\beta| \le \max\{|\alpha + \beta|, |-\alpha|\},$$

and since $|\alpha| = |-\alpha|$, the latter implies that $|\beta| \le |\alpha + \beta|$, so

$$|\alpha + \beta| = |\beta|.$$

Section 5.4

5.27 (a) Since $\chi(1) \neq 0$ and $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, then $\chi(1) = 1$.

(b) Since $a^q = a$ for all $a \in \mathbb{F}_q$, then $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$. Thus,

$$1 = \chi(1) = \chi(a^{q-1}) = \chi(a)^{q-1}.$$

(c) Since

$$1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a),$$

then $\chi(a^{-1}) = \chi(a)^{-1}$. By part (b), $|\chi(a)| = 1$, so $\overline{\chi(a)} = \chi(a)^{-1}$.

5.29 We have

$$\chi\lambda(ab) = \chi(ab)\lambda(ab) = \chi(a)\chi(b)\lambda(a)\lambda(b) = \chi(a)\lambda(a)\chi(b)\lambda(b) = \chi\lambda(a)\chi\lambda(b),$$

so $\chi\lambda$ is a character. Also,

$$\chi^{-1}(ab) = (\chi(ab))^{-1} = (\chi(a)\chi(b))^{-1} = \chi^{-1}(a)\chi^{-1}(b),$$

so χ^{-1} is a character. That $\mathfrak{Ch}(\mathbb{F}_q^\times)$ is a group now follows from Proposition A.1 on page 321.

5.31 Let $S = \sum_{\chi \in \mathfrak{Ch}(\mathbb{F}_q^\times)} \chi(a)$. Since $a \neq 1$, then by Exercise 5.30, there exists a $\lambda \in \mathfrak{Ch}(\mathbb{F}_q^\times)$ such that $\lambda(a) \neq 1$. Thus,

$$\lambda(a)S = \sum_{\chi \in \mathfrak{Ch}(\mathbb{F}_q^\times)} \lambda(a)\chi(a) = \sum_{\chi \in \mathfrak{Ch}(\mathbb{F}_q^\times)} \lambda\chi(a) = S,$$

so $(\lambda(a) - 1)S = 0$, which implies that $S = 0$ since $\lambda(a) - 1 \neq 0$.

5.33 If $p|k$, then $\zeta_p^{jk} = 1$ for all j, so

$$G(k) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0 = \left(\frac{k}{p}\right) G(1).$$

—see [53, Exercise 4.5, p. 187], as well as Exercises 5.27 and 5.31.

If $p \nmid k$, then

$$\left(\frac{k}{p}\right) G(k) = \sum_{j=0}^{p-1} \left(\frac{jk}{p}\right) \zeta_p^{jk} = \sum_{\ell=0}^{p-1} \left(\frac{\ell}{p}\right) \zeta_p^{\ell} = G(1),$$

where the penultimate equality comes from the fact that ℓ goes over all residues modulo p as jk does. Hence,

$$G(k) = \left(\frac{k}{p}\right) G(1).$$

5.35 This is immediate from Exercises 5.33–5.34.

Section 5.5

5.37 If $\mathfrak{p}$ is unramified in K_j for $j = 1, 2$ and $\mathcal{P}$ is any prime $\mathfrak{O}_K$-ideal over $\mathfrak{p}$, we need only show that $e_{K_1K_2/F}(\mathcal{P}) = 1$. By Exercise 5.8 on page 195, there exists a normal extension field L of F containing K_1K_2. Let $\mathcal{Q}$ be a prime $\mathfrak{O}_L$-ideal above $\mathcal{P}$. Then $\mathcal{T}_{\mathcal{Q}}(L/F)$ is the is the inertia group of $\mathcal{Q}$ with inertia field $T_{\mathcal{Q}}(L/F)$. By part (c) of Corollary 5.17 on page 227, $K_j \subseteq T_{\mathcal{Q}}(L/F)$ for $j = 1, 2$. Since K_1K_2 is the smallest field containing both K_1 and K_2, then $K_1K_2 \subseteq T_{\mathcal{Q}}(L/F)$, so $\mathcal{Q} \cap K_1K_2 = \mathcal{P}$ is unramified over F.

To prove the last assertion, use the above argument with $\mathcal{D}_{\mathcal{Q}}(L/F)$ taking the role of $\mathcal{T}_{\mathcal{Q}}(L/F)$.

5.39 Since $N_{F/\mathbb{Q}}(\lambda) = p$, by Exercise 2.24 on page 68, there exists an $a \in \mathbb{Z}$ such that

$$\gamma \equiv a \pmod{\lambda}$$

by Exercise 4.32 on page 164. Hence,

$$\gamma^p \equiv a^p \pmod{\lambda^p},$$

so by taking $z = a^p$, we are done. Since $p = \lambda^{p-1}u$ for some $u \in \mathcal{U}_F$, then

$$\gamma^p \equiv z \pmod{p}$$

as well.

Section 5.6

5.41 First we show that there exists exactly one prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$ above p, which is totally ramified in F. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two prime $\mathfrak{O}_F$-ideals above p. From Lemma 5.7 on page 221, we know that

$$\mathcal{D}_{\mathfrak{p}_1}(F/\mathbb{Q}) = \mathcal{D}_{\mathfrak{p}_2}(F/\mathbb{Q}) = \mathcal{D}_p(F/\mathbb{Q}),$$

—see also Remark 5.5 on page 222. By Theorem 5.4 on page 189, p is unramified in $T_p(F/\mathbb{Q}) = T$, so $p \nmid \Delta_T$ by Corollary 5.8 on page 210. By Theorem 3.15 on page 126, $\Delta_T \bigm| \Delta_F$, which is a power of p. Hence, $q \nmid \Delta_T$ for any $q \neq p$. Therefore,$\Delta\ _T = 1$ and $T = \mathbb{Q}$ by Corollary 5.9 on page 213. Also, since $Z = Z_p(F/\mathbb{Q}) \subseteq T$, then $Z = \mathbb{Q}$, so p is fully ramified in F.

Since $\mathcal{T}_p(F/\mathbb{Q})/\mathcal{V}_1$ is cyclic by part (e) of lemma 5.15 on page 247 and since $\mathcal{V}_1 = 1$, by the above, then $\mathcal{T}_p(F/\mathbb{Q}) = \mathrm{Gal}(F/\mathbb{Q})$ is cyclic.

5.43 Let $\tau \in \mathcal{D}_{\mathcal{P}}(K/F)$ and $\sigma \in \mathcal{V}_j$. Then for $\alpha \in \mathfrak{O}_K$, we have

$$\alpha^{\tau\sigma\tau^{-1}} \equiv ((\alpha^\tau)^\sigma)^{\tau^{-1}} \equiv (\alpha^\tau)^{\tau^{-1}} \equiv \alpha \pmod{\mathcal{P}^{j+1}},$$

by the definition of the $\mathcal{V}_j$. Hence, $\tau\sigma\tau^{-1} \in \mathcal{V}_j$, which is therefore normal in $\mathcal{D}_{\mathcal{P}}(K/F)$.

5.45 It suffices to prove the result for K/F totally ramified at $\mathcal{P}$, since the $\mathcal{V}_j$ for $\mathcal{P}$ in K/F is the same as the $\mathcal{V}_j$ for $\mathcal{P}$ in K/T where $T = T_{\mathcal{P}}(K/F)$. Thus, we assume that $F = T$, so $|K : F| = e_{K/F}(\mathcal{P}) = e$.

Let $\alpha \in \mathcal{P} - \mathcal{P}^2$, then from Claim 5.7 on page 204, it follows that

$$\{1, \alpha\,, \alpha^2, \ldots, \alpha^{e-1}\}$$

is an integral basis for $K_{\mathcal{P}}/F_{\mathfrak{p}}$, where $K_{\mathcal{P}} = \mathfrak{O}_K/\mathcal{P}$ and $F_{\mathfrak{p}} = \mathfrak{O}_F/\mathfrak{p}$ with $\mathfrak{p} = \mathcal{P} \cap \mathfrak{O}_F$. Since

$$|K_{\mathcal{P}} : F_{\mathfrak{p}}| = e = |K : F|,$$

then $\mathfrak{O}_K = \mathfrak{O}_F[\alpha]$. Hence, from Theorem 5.8 on page 200 and Lemma 5.6 on page 202, we have that

$$\delta_{K/F}(\alpha)\mathfrak{O}_K = \mathcal{D}_{K/F}.$$

Thus, $\mathcal{P}^s \mid \delta_{K/F}(\alpha)$, but $\mathcal{P}^{s+1} \nmid \delta_{K/F}(\alpha)$.

Let $\sigma \in \mathcal{V}_j - \mathcal{V}_{j+1}$. Thus, $\alpha - \alpha^\sigma \in \mathcal{P}^{j+1} - \mathcal{P}^{j+2}$, by the definition of the $\mathcal{V}_j$. Therefore, s is the exact power of $\mathcal{P}$ dividing $(\alpha - \alpha^\sigma)\mathfrak{O}_K$. Since

$$m_{\alpha,F}(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \alpha^\sigma),$$

then

$$m'_{\alpha,F}(x) = \prod_{\sigma \neq 1} (x - \alpha^\sigma),$$

so

$$\delta_{K/F}(\alpha) = \prod_{\sigma \neq 1} (\alpha - \alpha^\sigma).$$

If we let

$$\mathfrak{O}_K(\alpha - \alpha^\sigma) = \mathfrak{O}_K \mathcal{P}^{s(\sigma)},$$

then

$$s = \sum_{\sigma \neq 1} s(\sigma) = \sum_{j=0}^{m-1} \sum_{\substack{\sigma \in \mathcal{V}_j \\ \sigma \notin \mathcal{V}_{j+1}}} s(\sigma) = \sum_{j=0}^{m-1} (|\mathcal{V}_j| - |\mathcal{V}_{j+1}|)(j+1) =$$

$$(|\mathcal{V}_0| - |\mathcal{V}_1|) + 2(|\mathcal{V}_1| - |\mathcal{V}_2|) + 3(|\mathcal{V}_2| - |\mathcal{V}_3|) + \cdots + m(|\mathcal{V}_{m-1}| - 1) =$$

$$|\mathcal{V}_0| + |\mathcal{V}_1| + |\mathcal{V}_2| + \cdots + |\mathcal{V}_{m-1}| - m = \sum_{j=0}^{m-1} (|\mathcal{V}_j| - 1),$$

which is Hilbert's formula.

5.47 By part 4 of Lemma 5.4 on page 197, with $\mathcal{J} = \mathfrak{O}_K$, we get that $T_{K/F}(\mathfrak{O}_K)$ is the least common multiple of the $\mathfrak{O}_F$-ideals dividing $\mathcal{D}_{K/F}$. In other words, the biggest $\mathfrak{O}_F$-ideal dividing $\mathcal{D}_{K/F}$ is $T_{K/F}(\mathfrak{O}_K)\mathfrak{O}_K$. So, if $T_{K/F}(\mathfrak{O}_K) = \mathfrak{O}_F$ and $\mathfrak{p} \mid \mathcal{D}_{K/F}$ for some prime $\mathfrak{O}_F$-ideal $\mathfrak{p}$, then $\mathcal{D}_{K/F} \subseteq \mathfrak{p}$. However, from part 4 of the aforementioned lemma again,

$$\mathfrak{O}_F = T_{K/F}(\mathfrak{O}_K) \subseteq \mathcal{D}_{K/F},$$

a contradiction to the primality of $\mathfrak{p}$. Conversely, if $T_{K/F}$ is not onto, then given that it is the lcm of the $\mathfrak{O}_F$-ideals dividing $\mathcal{D}_{K/F}$, there exists a prime $\mathfrak{O}_F$-ideal dividing $\mathcal{D}_{K/F}$.

5.49 By Exercise 5.47, $\mathfrak{p} \nmid \mathfrak{D}_{K/F}$ for any prime $\mathfrak{O}_F$-ideal. By part 3 of Lemma 5.4,

$$\Delta_{K/F}\mathfrak{O}_K = N^{K/F}(\mathfrak{D}_{K/F})\mathfrak{O}_K = \mathfrak{D}^n_{K/F}\mathfrak{O}_K.$$

Thus, if $\mathfrak{p}^n \mid \Delta_{K/F}$, then $\mathfrak{p} \mid \mathfrak{D}_{K/F}$, a contradiction. Therefore, if $\mathfrak{O}_K \cong \mathfrak{O}_F[G]$ as an $\mathfrak{O}_F[G]$-module, then K/F is tamely ramified by Exercise 5.46.

Section 5.7

5.51 Let $a \in \mathbb{N}$ such that $\gcd(561, a) = 1$. Thus, since $561 = 3 \cdot 11 \cdot 17$, then

$$a^2 \equiv 1 \pmod 3, \quad a^{10} \equiv 1 \pmod{11}, \text{ and } a^{16} \equiv 1 \pmod{17}.$$

Thus,

$$a^{560} \equiv (a^2)^{280} \equiv 1 \pmod 3, a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11},$$

and

$$a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}.$$

Hence,

$$a^{561} \equiv a \pmod{561},$$

for all $a \in \mathbb{N}$. Finally, since $j^{561} \equiv j \,(\text{mod } 561)$ for $j = 3, 11, 17$, then the result is secured.

5.53 If $x = y$, then

$$\frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha(x-y))} = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} 1 = 1.$$

If $x \neq y$, then $\beta = \alpha(x-y)$ ranges over $\mathbb{F}_q$ as α does. Therefore,

$$\frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha(x-y))} = \frac{1}{q}\sum_{\beta\in\mathbb{F}_q} \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(\beta)} = \frac{1}{q}G_1(\epsilon) = 0,$$

where the last equality comes from Exercise 5.52.

Section 6.1

6.1 Let γ be a generator of $\mathbb{F}_q^*$ (via the hint, see Theorem A.8) and set $x = \gamma^a$ and $\alpha = \gamma^b$. Then $x^n = \alpha$ if and only if $\gamma^a = \gamma^{bn}$, and this is equivalent to saying that

$$a \equiv bn \pmod{q-1}.$$

Via the hint, by Theorem A.24 on page 340, the latter holds if and only if $a = gt$ for some $t \in \mathbb{Z}$. Hence, $x^n \equiv \alpha \,(\text{mod } \mathfrak{p})$ has a solution $x \in \mathfrak{O}_F$ if and only if

$$\alpha^{(q-1)/g} \equiv (\gamma^a)^{(q-1)/g} \equiv (\gamma^{gt})^{(q-1)/g} \equiv \gamma^{(q-1)t} \equiv 1 \pmod{\mathfrak{p}}.$$

6.3 By Proposition 6.1,

$$\pi = \pi^{(N_F(2)-1)/3} \equiv \left(\frac{\pi}{2}\right)_3 \pmod 2, \tag{S20}$$

Also, by Exercise 6.2,

$$\left(\frac{2}{\pi}\right)_3 = 1 \text{ if and only if } \beta^3 \equiv 2 \pmod{\pi},$$

Therefore,

$$\beta^3 \equiv 2 \pmod{\pi} \text{ if and only if } \left(\frac{\pi}{2}\right)_3 = 1,$$

by the Cubic Reciprocity Law. Thus, by Congruence (S20), this is equivalent to

$$\pi \equiv 1 \pmod{2}.$$

6.5 If $\alpha = a + b\zeta_3$, then the associates are: $\alpha = a + b\zeta_3$, $\zeta_3\alpha = -b + (a-b)\zeta_3$, $\zeta_3^2\alpha = (b-a) - a\zeta_3$, $-\alpha = -a - b\zeta_3$, $-\zeta_3\alpha = b + (b-a)\zeta_3$, and $-\zeta_3^2\alpha = (a-b) + a\zeta_3$.

6.7

$$J(\chi,\chi^{-1}) = \sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_q}} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1\\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right).$$

If we set $a/(1-a) = c$ and $c \neq 1$, then $a = c/(1+c)$. Hence,

$$J(\chi,\chi^{-1}) = \sum_{c\neq -1} \chi(c),$$

and by Exercise 5.28, this equals $-\chi(-1)$.

6.9 By Exercise 5.30, there exists a character of order n on $\mathbb{F}_p$. Clearly, there are at most n distinct characters of order dividing n. Thus, χ^j for $1 \leq j \leq n$ are *all* of the characters of order dividing n. If $\alpha \in \mathbb{F}_p^*$ and $f(x) = 0$ is not solvable in $\mathbb{F}_p$, then by Exercise 5.32 there exists a character χ of order n with $\chi(\alpha) \neq 1$. Thus, if we set $S = \sum_{j=1}^n \chi^j(\alpha)$, then trivially $S\chi(\alpha) = S$, so $S(\chi(\alpha) - 1) = 0$. Since $\chi(\alpha) \neq 1$, then $S = 0 = N_{f,p}$. If $\alpha \in \mathbb{F}_p^*$ and $f(x) = 0$ is solvable in $\mathbb{F}_p$, then there exists a $\beta \in \mathbb{F}_p$ such that $\beta^n = \alpha$. Therefore,

$$\chi(\alpha) = \chi(\beta^n) = \chi(\beta)^n = 1,$$

since $\chi^n = \epsilon$. This implies that

$$\sum_{j=1}^n \chi(\alpha) = n = N_{f,p}.$$

Lastly, if $\alpha = 0$, then

$$\sum_{j=1}^n \chi(\alpha) = \epsilon(0) = 1 = N_{f,p}.$$

This proves the first assertion. In particular, if $p > 2 = n$, let $\chi_p(a) = (\frac{a}{p})$. Then

$$N_{f,p} = \epsilon(a) + \chi_p(a) = 1 + \left(\frac{a}{p}\right).$$

6.11 Let $g(x) = x^2 - a$ and $h(x) = x^2 - b$. Then

$$N_{f,p} = \sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_p}} N_{g,p}N_{h,p},$$

so by the last part of Exercise 6.9, this equals

$$p+\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)+\sum_{b=0}^{p-1}\left(\frac{b}{p}\right)+\sum_{\substack{a+b=1\\a,b\in\mathbb{F}_p}}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

A fact from elementary number theory is that the first two sums are equal to zero (see the solution to Exercise 5.33), so we have only to evaluate the last sum. For this we employ Exercise 6.7.

$$J(\chi,\chi^{-1})=-\chi(-1)=-\left(\frac{-1}{p}\right)=-(-1)^{(p-1)/2},$$

from which the result follows.

6.13 If $(p-1)\mid k$, then since $x^{p-1}\equiv 1\,(\text{mod } p)$, by Fermat's Little Theorem, we have that the sum is equal to $p-1\equiv -1\,(\text{mod } p)$. Now assume that $(p-1)\nmid k$, and let $\alpha\in\mathbb{F}_p^*$ be a generator—see Theorem A.8 on page 331. Then

$$\sum_{x=1}^{p-1}x^k=\sum_{j=0}^{p-2}\alpha^{jk}=\sum_{j=0}^{p-2}(\alpha^k)^j=\frac{1-\alpha^{k(p-1)}}{1-\alpha^k},$$

where the last equality follows from Theorem B.4 on page 347. By Fermat's Little Theorem, the numerator vanishes, but since $(p-1)\nmid k$, then the denominator does not.

6.15 This follows since $\mathcal{P}^3=(10+3\sqrt{-27})$, and $7^3=10^2+27\cdot 3^2$.

Section 6.2

6.17 By Proposition 6.2 on page 278,

$$\left(\frac{a}{\pi}\right)_4^2=\left(\frac{a^2}{\pi}\right)_4\equiv a^{(N_F(\pi)-1)/2}\quad(\text{mod } \pi).$$

By taking complex conjugates, we get the same congruence modulo $\overline{\pi}$. Thus,

$$\left(\frac{a}{\pi}\right)_4^2\equiv a^{(N_F(\pi)-1)/2}\equiv a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\quad(\text{mod } p).$$

Therefore,

$$\left(\frac{a}{\pi}\right)_4^2=\left(\frac{a}{p}\right).$$

6.19 The proof is essentially the same as that given in the solution of Lemma 6.1 on page 263.

6.21 By part (a) of Lemma 6.2 on page 264,

$$G^2(\chi)=G(\chi^2)J(\chi,\chi).$$

However, by Exercise 5.54 on page 260, and the fact that $\chi^2=\chi^{-2}=\overline{\chi}^2$, we have

$$G(\chi^2)=\sqrt{p},$$

and by Lemma 6.5 on page 280,

$$J(\chi,\chi)=(-1)^{(p+3)/4}\pi.$$

6.23 Since p is a prime in $\mathbb{Z}[i]$, then $\left(\frac{a}{p}\right)_4 = 1$ by Exercise 6.16, so by part (b) of Proposition 6.3 on page 279, a is a quartic residue modulo p. Furthermore, if

$$a \equiv z^2 \pmod{p}$$

for some $z \in \mathbb{Z}$, then certainly $(\frac{a}{p}) = 1$. Conversely, if $(\frac{a}{p}) = 1$, then $a \equiv z^2 \pmod{p}$ for some $z \in \mathbb{Z}$. By the part just proved, a is a quartic residue modulo p, so

$$a \equiv \alpha^4 \pmod{p}$$

for some $\alpha = a + bi \in \mathbb{Z}[i]$, as well. Thus, $\alpha^2 \equiv \pm z \pmod{p}$. Hence, for some $c, d \in \mathbb{Z}$, we have

$$a^2 - b^2 + 2abi = \pm z + (c + di)p,$$

so by equating coefficients,

$$a^2 - b^2 \pm z + pc = 0, \text{ and } 2ab = pd.$$

Therefore, since p is odd, then either $p \mid a$ or $p \mid b$. If $p \mid a$, then

$$b^2 \equiv \pm z \pmod{p},$$

so

$$a \equiv \alpha^4 \equiv z^2 \equiv b^4 \pmod{p}.$$

Similarly, if $p \mid b$, then

$$a \equiv \alpha^4 \equiv a^4 \pmod{p}.$$

6.25 By Exercise 6.17, $(\frac{-1}{\pi})_4 = \pm 1$, so by Exercise 6.18 we must have $(\frac{-1}{\pi})_4 = 1$, since $(\frac{2}{p}) = 1$ from (A.10) on page 342. Therefore,

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{-2b^2}{\pi}\right)_4,$$

and by Exercise 6.17 and Proposition 6.3, this equals

$$\left(\frac{-p + a^2}{\pi}\right)_4 = \left(\frac{a^2}{\pi}\right)_4 = \left(\frac{a}{\pi}\right)_4^2 = \left(\frac{a}{p}\right),$$

as required.

6.27 By part (a) of Lemma 6.2 on page 264,

$$J(\chi,\chi)^2 = \frac{G(\chi)^4}{G(\chi^2)^2}.$$

However, since χ^2 is a quadratic character, then $G(\chi^2) = \pm\sqrt{p}$, and by Claim 6.1 on page 265

$$G(\chi)^4 = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2).$$

Thus,

$$J(\chi,\chi)^2 = \chi(-1)J(\chi,\chi)J(\chi,\chi^2),$$

so dividing through by $J(\chi,\chi)$ then multiplying through by $\chi(-1)$ we get,

$$J(\chi,\chi^2) = \chi(-1)J(\chi,\chi),$$

which is part (a), by Lemma 6.5 on page 280. For part (b), we use part (a) in the following.

$$J(\chi^3,\chi^2) = J(\chi^3(\chi^3)^2) = \chi^3(-1)J(\chi^3,\chi^3) = \chi(-1)\overline{J(\chi,\chi)} = \overline{\pi},$$

where the last equality comes from Lemma 6.5. Therefore, $\chi(\alpha) \equiv \alpha^{(p-1)/4} \equiv \alpha^m \pmod{\pi}$ implies

$$-J(\chi^3,\chi^2) \equiv \sum_{j=1}^{p-1} j^{3m}(1-j)^{2m} \pmod{\pi},$$

and by the Binomial Theorem this is congruent to

$$\sum_{j=1}^{p-1} j^{3m} \sum_{k=0}^{m} (-1)^k \binom{2m}{k} j^{2m-k} \equiv \sum_{k=0}^{m} (-1)^k \binom{2m}{k} \sum_{j=1}^{p-1} j^{5m-k} \pmod{\pi}.$$

However, by Exercise 6.13 on page 277, $\sum_{j=1}^{p-1} j^{5m-k} \equiv 0 \pmod{p}$ for any $k < m$, since in that case, $5m-k < p-1$. Also, if $k = m$, then $\sum_{j=1}^{p-1} j^{5m-k} = -1$. Hence,

$$J(\chi^3,\chi^2) \equiv (-1)^m \binom{2m}{m} \pmod{\pi}.$$

Therefore,

$$2a = \pi + \overline{\pi} \equiv \overline{\pi} = J(\chi^3,\chi^2) \equiv (-1)^m \binom{2m}{m} \pmod{\pi}.$$

By taking complex conjugates, we also get

$$2a \equiv (-1)^m \binom{2m}{m} \pmod{\overline{\pi}}.$$

Thus,

$$2a \equiv (-1)^m \binom{2m}{m} \pmod{p},$$

which is part (b).

Section 6.3

6.29 By Exercise 5.34, quadratic Gauss sums are pure. However, suppose that χ has order $k > 2$, $q = p$ and g is a primitive root modulo p such that $g \equiv 1 \pmod{4k^2}$. Let $\sigma_g \in \mathrm{Gal}(\mathbb{Q}(\zeta_{4k^2p})/\mathbb{Q})$ be defined by $\sigma_g(\zeta_{4k^2p}) = (\zeta_{4k^2p})^g$. Since $G(\chi) \in \mathbb{Q}(\zeta_{kp})$, by part (a) of Proposition 6.7, then by Exercise 5.52,

$$\left(G(\chi)^k\right)^{\sigma_g} = G(\chi)^k,$$

so since $\sigma_g|_{\mathbb{Q}(\zeta_{kp})} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{pk})/\mathbb{Q}(\zeta_k))$ for $g = 1, 2, \ldots, p-1$, then $G(\chi)^k \in \mathbb{Q}(\zeta_k)$. Thus, if $r = G(\chi)/\sqrt{p}$ is a root of unity, then $r^{4k^2} = 1$ since $r^{2k} \in \mathbb{Q}(\zeta_k)$. Thus, $r^{\sigma_g} = r$. However,

$$r = r^{\sigma_g} = \frac{G(\chi)^{\sigma_g}}{\sqrt{p}^{\sigma_g}} = \frac{\overline{\chi}(g)G(\chi)}{\pm\sqrt{p}} = \pm\overline{\chi}(g)r.$$

Therefore, $\chi(g) = \pm 1$, contradicting that χ has order $k > 2$.

This solution is due to R. Evans [17].

6.31 If $|\Delta_F| = \ell > 3$ a prime, then choose $r \in \mathbb{Z}$ such that $r \not\equiv 1 (\bmod\ \ell)$ and $(\frac{\ell}{r}) = 1$. Then $rR \equiv R (\bmod\ \ell)$. Thus, $\ell \mid R(r-1)$, which forces $\ell \mid R$. But $R + N = \sum_{j=1}^{\ell-1} j \equiv 0$ $(\bmod\ \ell)$, so $\ell \mid N$. Now let$\Delta_F = d_0 d_1$, where d_0 is a discriminant, with $|d_0|$ an odd prime, or one of 4 or 8, and $d_1 \in \mathbb{Z}$ with $|d_1| \neq \pm 1$. Let

$$f : R \mapsto (\mathbb{Z}/|d_0|\mathbb{Z})^*,$$

be the natural map $r \mapsto \overline{r}$. Then f is onto since if $(\frac{d_1}{r}) = -1$, then $\left(\frac{\Delta_F/d_1}{r}\right) = -1$, given that $\left(\frac{\Delta_F}{r}\right) = 1$, so all elements of $(\mathbb{Z}/|d_0|\mathbb{Z})^*$ are covered. Hence,

$$|\ker(f)| = \phi(|d_1|)/2.$$

Therefore, among the $\phi(|\Delta_F|)/2$ elements in R, exactly $\phi(|d_1|)/2$ reduce, modulo $|d_0|$, to a given element in $(\mathbb{Z}/|d_0|\mathbb{Z})^*$. Hence, if $|d_0|$ is an odd prime, then

$$R \equiv \frac{1}{2}\phi(d_1) \sum_{a=1}^{|d_0|-1} a \equiv 0 \pmod{|d_0|}.$$

If $d_0 = -4$, then $R \equiv \phi(d_1)(1+3)/2 \equiv 0 (\bmod\ |d_0|)$, and if $d_0 = \pm 8$, then $R \equiv \phi(d_1)(1+3+5+7)/2 \equiv 0 (\bmod\ |d_0|)$. Since $d_0 \mid R$ for all odd primes and for 4 or 8, when they occur, then $|\Delta_F| \mid R$. Similarly, $|\Delta_F| \mid N$.

The above solution is due to Lemmermeyer [38].

Section 6.4

6.33 By Example 5.8 on page 190,

$$(1 - \zeta_r)^{r-1} = (r)$$

in $\mathfrak{O}_F$, so

$$(1 - \zeta_r)^{\sigma} = (1 - \zeta_r)$$

for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Thus,

$$(1 - \zeta_r)^{\tau} \subseteq (1 - \zeta_r).$$

By Exercise 6.32, $\mathfrak{G}(\alpha) = \pm\zeta_r^j \alpha^{\tau} \equiv \pm 1 (\bmod\ r)$. Since α is primary, then

$$\alpha \equiv z \pmod{(1 - \zeta_r)^2},$$

for some $z \in \mathbb{Z}$, so

$$\alpha^{\tau} \equiv z^{\tau} \equiv z^{\sum_{j=1}^{r-1} j} = z^{r(r-1)/2} \equiv (\pm 1)^r \equiv \pm 1 \pmod{(1 - \zeta_r)^2},$$

where the equality comes from Theorem B.4 on page 347. Therefore,

$$\pm 1 \equiv \pm\zeta_r^j \alpha^{\tau} \equiv \pm\zeta_r^j \pmod{(1 - \zeta_r)^2},$$

so

$$\zeta_r \equiv \pm 1 \pmod{(1 - \zeta_r)^2}. \qquad \text{(S21)}$$

Therefore, since $\zeta_r = 1 - (1 - \zeta_r)$ and $j > 1$ by (S21), then by the Binomial Theorem,

$$\pm 1 \equiv \zeta_r^j \equiv 1 - j(1 - \zeta_r) \pmod{(1 - \zeta_r)^2}.$$

If the plus sign holds, then $(1 - \zeta_r) \mid 2$, so $r \mid 2$ by Exercise 2.46 on page 86, a contradiction since $r > 2$. Thus,

$$1 - j(1 - \zeta_r) \equiv 1 \pmod{(1 - \zeta_r)^2},$$

which implies that $(1 - \zeta_r) \mid j$, from which we get that $r \mid j$ by Exercise 2.46 again. This means that $\zeta_r^j = 1$, so we have the result.