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

Ser

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

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

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

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

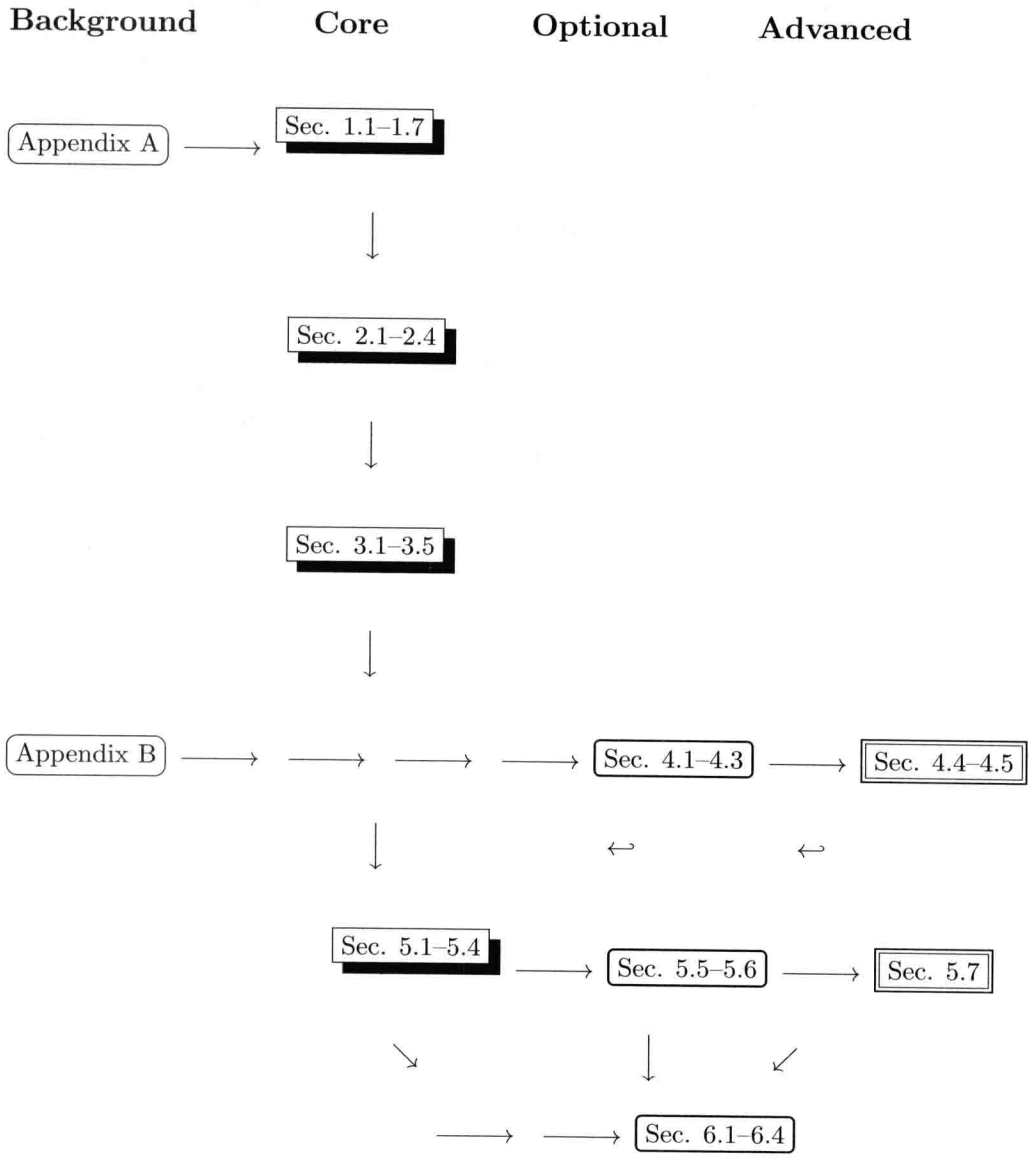
A glance at the Table of Contents will reveal that there is a wealth of material beyond a basic course in algebraic number theory. This section is intended for the instructor, by giving several routes from a course in the basics of algebraic number theory to a more advanced course with numerous applications, 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



Contents

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 $\alpha, \beta \in D$ 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 $\alpha, \beta \in D$ 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*.