ABSTRACT

BATSON, SCOTT CHRISTOPHER. On the Relationship Between Two Embeddings of Ideals into Geometric Space and the Shortest Vector Problem in Principal Ideal Lattices. (Under the direction of Ernest L. Stitzinger.)

An ideal lattice is the geometric embedding of an ideal in the algebraic integer ring of some number field. Many recent developments in lattice-based cryptography are centered around the use of ideal lattices. The shortest vector problem (SVP) is the most important hard lattice problem. Few algorithms that find a short vector in ideal lattices exploit their additional algebraic structure, and whether or not the SVP can be solved algebraically in ideal lattices remains unknown. We study the relationship between the canonical and coefficient embeddings of ideals in algebraic integer rings of cyclotomic number fields. We examine the algebraic structure of principal ideal lattices under the coefficient embedding by considering them as principal ideals of a cyclotomic quotient ring. Finally, empirical evidence is provided to exhibit a relationship between the algebraic structure of a principal ideal in this quotient ring and the geometric structure of its corresponding ideal lattice. These results demonstrate progress towards solving the SVP in ideal lattices algebraically.

On the Relationship Between Two Embeddings of Ideals into Geometric Space and the Shortest Vector Problem in Principal Ideal Lattices

by
Scott Christopher Batson

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2015

APPROVED BY:

Thomas J. Lada	Kailash C. Misra
Mohan S. Putcha	Ernest L. Stitzinger Chair of Advisory Committee

DEDICATION

To my family.

BIOGRAPHY

Scott is the son of Chris Batson and Cindy Fortune. He grew up in the mountains of North Carolina and graduated from West Henderson High School. Scott received a Millennium Scholars Award from Troy University in Troy, Alabama where he majored in Mathematics Education and graduated Summa Cum Laude. He also met and married his wife, Suzanne, in Troy. After teaching a high school pre-engineering curriculum, Scott entered graduate school at North Carolina State University where he studied under the advisement of Dr. Ernest Stitzinger. For two years he taught classes and carried out the responsibilities of being a Graduate Teaching Assistant. He was then awarded a Science, Mathematics, and Research for Transformation (SMART) Scholarship, funded by the Department of Defense, to support his graduate studies and research. Scott has received a Master of Science degree in Applied Mathematics from North Carolina State University, and will graduate in May of 2015 with a Ph.D. in Mathematics.

ACKNOWLEDGEMENTS

First and foremost I would like to thank God for blessing me beyond measure. I know that He is responsible for all of the opportunities that I have been afforded and successes that I have experienced. It is also by His grace that I am saved through faith in Jesus Christ. He has made all things possible.

I am forever grateful to my advisor, Dr. Ernie Stitzinger, for his kindness, enthusiasm, and guidance throughout this endeavor. The impact of your advising and mentoring will reach far beyond my graduate student career. I have learned so much from you and your example. Thank you for taking me as a student, overseeing my research on this topic, and imparting some your wisdom through our many conversations. Thank you for always leading me in the right direction.

I have had many exceptional teachers in my life, and they all deserve to be acknowledged. I would especially like to thank my professors at Troy University for inspiring me to seek a Ph.D. in Mathematics. I want to thank my professors at North Carolina State University, particularly the members of my advisory committee, for everything they taught me. I am fortunate to have such an influential group of committee members. The department's support staff has also been instrumental in the completion of this dissertation. I greatly appreciate the helpful conversations with both Dr. Chris Peikert and Dr. Lenny Fukshansky as well.

The SMART Scholarship Program has given me a tremendous opportunity, and I would not have been able to carry out this research without their funding and support. I am grateful to SPAWAR for sponsoring me through the SMART Program, and to all of the SPAWAR employees that I have worked with thus far for giving me opportunities to

contribute. I am especially grateful to the individuals who have been willing to mentor me along the way.

Words cannot express how thankful I am to my entire family for their continued love, encouragement, and support. I am blessed to have had so many special people make an impact on my life. This dissertation is dedicated to each one of you, and to the memory of those who were not able to be here for this achievement.

I would certainly not be who I am today, personally or professionally, without my mom and dad. Thank you for providing me with a Christian home. Thank you for raising me to believe that I can accomplish anything. Thank you for teaching me to work hard and always do my best. Thank you for the sacrifices that you made to create opportunities for me. Thank you for loving me enough to encourage the pursuit of my dreams. Thank you for being an example to follow, and for always being there. Thank you for everything. I am very proud, honored, and blessed to be your son.

Finally, I could not have completed this journey without my wonderful wife, Suzanne. You are my rock. Through all of the hard times, and good times, you were exactly what I needed. I am very thankful that I was able to share this experience with you. You inspire me to be a better person every day. Thank you for the uncountable sacrifices that you made in helping to make this dream a reality. Thank you for your love, patience, understanding, encouragement, and support through everything. I love you so much.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

Lattices have been a useful tool for mathematicians since their first noted appearance in the number-theoretic work of LaGrange and Gauss, and have subsequently found numerous applications across mathematics. During the 1890s, the study of lattices was greatly advanced in a mathematical theory initiated by Minkowski called the geometry of numbers. Computational aspects of lattices were not widely studied until the early 1980s. Applications of lattices to cryptanalysis, among other things, were realized during this time. Lattice reduction techniques have been used in factoring univariate polynomials over the integers, factoring bivariate polynomials over the rational numbers, diophantine approximation, and linear programming [120]. The cryptographic applications of lattices, however, are the underlying motivation behind our work.

The use of lattices in the cryptanalysis of various cryptographic schemes, including NTRU, RSA, factoring-based cryptosystems, and discrete-log cryptosystems with groups of unity can be seen in [25, 30, 53, 71, 84, 88, 107, 110, 111]. It was not discovered until the mid-1990s that lattices could also be used in the construction of cryptographic primitives [1], which has developed into a very active area of research. The conjectured hardness of the shortest vector problem (SVP) is the basis for many of the lattice-based schemes, and is the core of many algorithmic applications of lattices [86]. Information regarding the hardness of the SVP may be found in [2, 56, 60, 77, 79, 83, 107]. Intuitively, one may envision a public-key cryptosystem where the public key is a lattice represented by very long basis vectors, and the secret key is given by short lattice vectors. Early public-key lattice cryptosystems include the Ajtai-Dwork scheme [3], GGH [45], and the ring-based NTRU [48] scheme.

Lattice-based cryptography has emerged as a strong candidate for post-quantum cryptography [49, 68, 84, 95, 100] because there are currently no known quantum algorithms for solving lattice problems that perform significantly better than the best known classical algorithms [84], although one may see [64] for a lattice reduction method that utilizes a quantum search. Readers are referred to [17] and [46] for a short introduction to post-quantum cryptography and quantum computing, respectively. Current developments in lattice-based cryptography, for instance [65, 66, 68, 69, 81, 92, 115], somewhat center around the use of lattices with a special algebraic structure called *ideal lattices*.

The algebraic structure of ideal lattices allows for faster computation and more efficient storage of cryptographic primitives [95]. One application of ideal lattices is realized in the first fully homomorphic public-key encryption scheme, proposed by Gentry in [43]. In a fully homomorphic scheme, one can manipulate encrypted data without the decryption key, which allows for computing on encrypted data. There are a number of potential applications for fully homomorphic encryption, including secure cloud computing. A fully homomorphic scheme would allow a user to store data on an untrusted server in encrypted form while still allowing the server to process, and respond to, user data queries [43].

Ideal lattices are now widely deployed in lattice-based cryptographic constructions, but an open question is whether or not they offer the same security as regular lattices [95]. The security of the most efficient lattice-based schemes currently hinges on assuming that lattice problems are not easier to solve in ideal lattices. The most important hard lattice problem is the SVP, so we consider this problem in ideal lattices. There are essentially four different types of lattice reduction algorithms used to find a short lattice vector: the celebrated LLL algorithm [63] along with its many generalizations and variants, including [58, 59, 97, 104, 106, 108, 109]; enumeration techniques [31, 34, 41, 54, 96, 98]; sieving algorithms [4, 5, 8, 18, 47, 90]; and Voronoi-cell based methods [85]. The LLL algorithm is the most widely known and studied algorithm used for lattice reduction. These existing algorithms generally operate in a geometric fashion and do not utilize the additional algebraic structure to find short vectors in ideal lattices.

The focus of our research is to exploit the algebraic structure of ideal lattices in solving the SVP. This goal could be achieved in one of two ways; either we exploit certain properties of an ideal lattice to improve upon an existing algorithm (as in [103]), or we solve the SVP in ideal lattices algebraically. It currently remains unknown whether or not the SVP can be solved algebraically in ideal lattices. By working with ideal lattices as algebraic objects, we move towards this result.

1.1 Our Approach and Related Work

The approach taken in this work is to study ideal lattices by viewing them as ideals in integral polynomial quotient rings. We are particularly interested in the information that can be obtained on the geometric structure of the ideal lattice by analyzing the algebraic structure of the corresponding ideal and quotient ring. We also restrict our focus to *principal* ideal lattices to narrow the scope of this research. In light of more recent works, such as [69] and [93], working with ideal lattices in this regard may seem a little naïve. We feel that our approach is justified by choosing to only work with rings of cyclotomic integers, and through a careful examination of the relationship that exists between the coefficient embedding and canonical embedding of ideals in these rings. The initial thought behind approaching ideal lattices this way is that the algebraic structure of ideal lattices corresponding to ideals and/or quotient rings with a certain structure may lead to a particular family of ideal lattices in which the SVP is easier to solve. We have also found that this approach may be aimed at solving the SVP algebraically in ideal lattices, and is conducive to discovering and documenting the algebraic properties which may be exploited in an algorithm that finds short vectors of ideal lattices. For more on the idea of exploiting special families of lattices, see [93].

This work is related to [68, 69, 93] because of the number-theoretic approach to ideal lattices taken in the third chapter. The investigation into the relationship between the canonical and coefficient embeddings of ideals, and some analysis regarding how classical lattice quantities and number-theoretic quantities are related, also contribute to the similarity. There is a short discussion on the relationship between the coefficient and canonical embedding found in [68] and [69], but our third chapter is devoted to providing a much more detailed analysis. These aforementioned works were some of the first to bridge a gap between the algebraic number theory and computer science literature pertaining to ideal lattices, and the hope is that our work will further connect these two areas. The fourth chapter of this dissertation is related to works like [95] and [103] because of our goal to exploit the algebraic structure of ideal lattices in finding short vectors, as well as the steps we take towards solving the SVP algebraically in (principal) ideal lattices.

Additional works related to our investigation into the properties of ideal lattices include those by Bayer-Fluckiger [11] and Lyubashevsky [65].

Since a focus of this work concerns computational aspects of the geometry of numbers, one may find [24] to be a helpful resource. More recent introductions to lattices include those found in [65, 77, 82, 83, 118]. Additional information on the LLL lattice reduction algorithm and its applications can be found in [21, 47, 89, 120]. For more on lattice-based cryptography and ideal lattices see [49, 82], theses [65, 118], surveys [33, 60, 84, 88, 101], and the extensive bibliographies contained within. The discussion that follows is a brief overview of existing works that are relevant to the knowledge and development of ideal lattices, or that take advantage of a special lattice structure to find short vectors.

Cyclic lattices, considered initially by Micciancio in [80] and then later in [66] and [92], are defined as lattices closed under a rotation operation acting on its vectors. That is, all cyclic rotations of a lattice vector are elements of the lattice. In [38] the authors remark that cyclic lattices are precisely the full-rank sub-lattices of $\mathbb{Z}^n$ that remain invariant under the action of the n-cycle permutation $(1 \ \ldots \ n)$ acting on its vectors. The authors of [38] then question the potential algebraic structure of a lattice invariant under the action of other permutations acting on its vectors, which remains open. Micciancio [81] notes the similarity of cyclic lattices to those used by NTRU in [48]. It was later realized that there is a correspondence between cyclic lattices and ideals in the quotient ring $\mathbb{Z}[x]/(x^n - 1)$, where the rotation operation acting on the vectors is equivalent to multiplying an element of the ideal by $x \mod x^n - 1$.

This idea was generalized in [66] and [81], and ideal lattices were defined as those which can be equivalently characterized as ideals of a ring $\mathbb{Z}[x]/(f(x))$ for some $f(x) \in \mathbb{Z}[x]$. In general, only monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$ are used to construct these rings in practice. Preferred $f(x)$ to use in this construction of ideal lattices include cyclotomic polynomials, which are always monic and irreducible, and power-of-two cyclotomic polynomials in particular. For more on ideal lattices in this regard, see [65] and [118]. Identifying whether or not a given lattice is an ideal lattice was considered in [32], which also included a statistical analysis for several dimensions showing that randomly generated lattices are practically never ideal.

Algorithmic results that consider a lattice with special structure include [44, 50, 117], but [72] was the first work concerning the improvement of algorithms working to solve lattice problems in an ideal lattice. The authors showed that the solution of certain lattice problems in cyclic lattices of dimension n could be sped up by a factor of n. It was remarked in [86] that sieve algorithms could also be slightly optimized to take advantage of lattices with a circular structure, such as the NTRU lattice [48] and cyclic lattices [81]. In this case all "rotations" of a vector could be used when reducing a point against the list, meaning each lattice vector in the compiled list represents n points. The idea of using "rotations" of sampled vectors to improve sieve algorithms on cyclic lattices was generalized in [103]. Here it is noted that a "rotation" corresponds to multiplication by x in the quotient ring, which is still an element of the ideal, so all rotations of lattice vectors can be used in the sieving process. To the author's knowledge, this is the first SVP or lattice reduction algorithm that utilizes the special algebraic structure of any ideal lattice.

As an analogue to the SVP Challenge [42], Plantard and Schneider [95] introduced the Ideal Lattice Challenge, offering a standard way of generating ideal lattices to allow for testing algorithms that find short vectors. Ideal lattices are generated using cyclotomic polynomials to construct a quotient ring from which a corresponding ideal is produced. Another goal of [95] is to assess whether or not the structure of the polynomial used to construct the quotient ring changes the hardness of the underlying lattice problems.

The focus of our work, and many of the works referenced above, is on rings of the form $\mathbb{Z}[x]/(\Phi_m(x))$ for a cyclotomic polynomial $\Phi_m(x)$. While the majority of literature available on the cryptographic applications of ideal lattices maintains this quotient ring characterization, the number-theoretic perspective of viewing these rings as rings of algebraic integers in cyclotomic number fields is natural; it lends itself to a different geometric approach that avoids any dependence on the form of $\Phi_m(x)$, which can be quite irregular [69]. Defining the norm of an element in accordance with its canonical embedding into $\mathbb{C}^n$ gives a nice way of analyzing norm expansion since all multiplication and addition are done coordinate-wise [68, 69, 93]. The authors of [68, 69, 93] develop cryptographic tools around ideal lattices using novel applications of some classical algebraic number theory notions.

Algebraic number theory is a well-studied branch of mathematics that is rich in results. There have been very thorough investigations of algebraic number theory from a computational point of view [26, 62, 112]. Ideal lattices arise naturally in algebraic number theory, and this view of ideal lattices makes them easy to work with while offering strong results [69]. Bayer-Fluckiger considered ideal lattices from an algebraic number theory perspective in several papers that she authored, or co-authored, beginning in the 1990s, several years prior to the appearance of cyclic lattices in the computer science literature. A nice exposition on ideal lattices from this number theory viewpoint is found in [11]. Additional works that view ideal lattices as they arise in algebraic number theory include those found in [6, 22, 36, 37, 38].

1.2 Summary of Results

The goals of the research performed for this dissertation were to study the relationship between the canonical and coefficient embeddings, investigate the algebraic structure of principal ideals in cyclotomic quotient rings, and then exploit this algebraic structure to find short vectors in principal ideal lattices. It would be of particular interest to solve the SVP in ideal lattices algebraically rather than to exploit certain algebraic properties in more geometrically focused algorithms. While the relationship between the coefficient and canonical embeddings has been considered in previous works [68, 69], Chapter 3 is devoted to describing this relationship more explicitly. These two embeddings are related by a fixed linear transformation that depends only on the cyclotomic number field. The matrix of this transformation is studied, and results on the equivalence of the SVP in ideal lattices under the two embeddings are provided. We also relate the number of independent shortest vectors in these two embeddings of an ideal.

Our investigation into the algebraic structure of principal ideals in cyclotomic quotient rings leads to an interesting connection between a generator of the ideal and a shortest vector of its corresponding ideal lattice. In particular, a shortest vector of every one- and two-dimensional principal ideal lattice will always correspond to an associate of the ideal's generator. Experimental results suggest that a short vector of principal ideal lattices, as output by the LLL algorithm on a special lattice basis, will most likely correspond to an associate of the ideal's generator in higher dimensions as well. Since all associates of a principal ideal's generator will generate the same ideal, this evidence suggests that the "shortest generator" of a principal ideal will probabilistically correspond to a solution of the SVP in its associated principal ideal lattice. This observation marks a first step towards solving the SVP algebraically in principal ideal lattices.

1.3 Organization

The remainder of this dissertation is organized as follows:

- Chapter 2 defines our notation and covers the necessary background on rings, ideals, and cyclotomic polynomials; cyclotomic number fields and their embeddings; the "powerful" basis; lattices; and ideal lattices. A brief discussion on the choice to work exclusively with cyclotomic number fields is also included.

- Chapter 3 contains an analysis of the relationship between the canonical and coefficient embeddings. We also study the equivalence of the SVP in any two geometric embeddings of an ideal.

- Chapter 4 connects the algebraic structure of principal ideals in cyclotomic quotient rings $\mathbb{Z}[x]/(\Phi_m(x))$ and the geometric structure of their corresponding ideal lattices. Empirical evidence is provided to demonstrate a strong correlation between a generator of the ideal and a shortest vector of the corresponding ideal lattice, as output by the LLL algorithm. All computations were performed in Maple$^{\text{TM}}$ [70]. Maple$^{\text{TM}}$ is a trademark of Waterloo Maple Inc.

- Chapter 5 offers concluding remarks on the significance of our results, and outlines some future work to be done in this area.

Chapter 2

Preliminaries

This chapter contains the relevant mathematical and lattice background, as well as some fundamental results that will be needed in the development of ideal lattices. We only review the necessary background for the work presented in this dissertation, which involves cyclotomic polynomials and cyclotomic number fields. A knowledge and understanding of abstract algebra and linear algebra up to the graduate level will be assumed. More background in these areas may be found in references such as [7, 51, 52, 76]. Our algebraic number theory setting is largely adapted from [69], but one may also refer to [26, 62, 87] for additional information and proofs. Throughout the chapter we will define the notation to be used in this dissertation, although this notation is fairly standard across the literature.

2.1 Algebra Background

We use G to denote a group and R to denote a ring. In this work all rings R will be commutative rings with unity. There is only one binary operation $(+)$ defined on a group, while there are two binary operations $(\cdot, +)$ defined on a ring. Given a commutative ring R, a non-empty subset $I \subseteq R$ is called an *ideal*, written $I \triangleleft R$, provided the following two conditions are met:

1. $a \pm b \in I$ for all $a, b \in I$; and

2. $r \cdot a = ra \in I$ for all $a \in I$ and $r \in R$.

The ideal $Ra = aR = \{x \in R \ : \ x = ra \text{ for some } r \in R\}$ is called the *principal ideal* generated by the element $a \in R$, written $(a) \triangleleft R$. An ideal of R is *maximal* if it is not equal to R and not contained in any other ideal. The ring R is *Noetherian* if every ideal is finitely generated. For an ideal $I \triangleleft R$, the set of *cosets* of I in R is denoted by $R/I = \{a + I \ : \ a \in R\}$. This set R/I is a commutative ring, called a *quotient ring.* A non-zero ring R is an *integral domain* if for all $a, b \in R$ whose product $ab = 0$, then either $a = 0$ or $b = 0$. An ideal $I \triangleleft R$ is *prime* if the quotient ring R/I is an integral domain.

Assume that the ring R is an integral domain. An element $u \in R$ is a *unit* if u has a multiplicative inverse in R. For $a, b \in R$ we say that a *divides* b if $b = aq$ for some $q \in R$, and a is a *proper divisor* of b if neither a nor q are units. Two elements $a, b \in R$ are *associates*, written $a \sim b$, if $b = ua$ for some unit $u \in R$. An element is *irreducible* if it is not a unit and has no proper divisors. The element $p \in R$ is *prime* if p is not a unit and when p divides the product ab, written $p|ab$, then either p divides a or p divides b. Two elements are said to be *relatively prime* if they have no common factors except units, in which case 1 is a greatest common divisor. A *Dedekind domain* is an integral domain R such that every ideal is finitely generated, every non-zero prime ideal is maximal, and R is integrally closed in the set $\{a/b \ : \ a, b \in R, b \neq 0\}$.

Let $a, b \in R$ and suppose that $a \neq 0$. If there exists a size function ν on R such that $b = aq + r$ for some $q, r \in R$, and either $r = 0$ or $\nu(r) < \nu(a)$, then R is called a *Euclidean* *domain* (ED). A *principal ideal domain* (PID) is an integral domain in which every ideal is principal. An integral domain R where factoring terminates and each element $a \in R$ may be expressed uniquely (up to multiplication by units) as the product of irreducible elements is called a *unique factorization domain* (UFD). These domains are related in the following manner.

Theorem 2.1.1. *A Euclidean domain is a principal ideal domain, and a principal ideal domain is a unique factorization domain.*

Let $\zeta_m = e^{2\pi i/m}$ be the primitive mth root of unity for some positive integer m. The mth *cyclotomic polynomial* is defined as

$$\Phi_m(x) = \prod_{(k,m)=1, k<m} (x - \zeta_m^k) = \frac{x^m - 1}{\prod_{d|m, d\neq m} \Phi_d(x)},$$

where the product is taken over all integers $k < m$ that are relatively prime to m. The polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ is the monic, irreducible (minimal) polynomial of ζ_m, hence there is an isomorphism $\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathbb{Z}[\zeta_m]$. Euler's Phi function φ assigns to each positive integer m the number $\varphi(m)$ of integers i such that $1 \leq i \leq m$ and i is relatively prime to m. This number $\varphi(m)$ is also the degree of the mth cyclotomic polynomial $\Phi_m(x)$.

Fact 2.1.2 ([69], Fact 2.11)**.** *For any m, we have $x^m - 1 = \prod_{d|m} \Phi_d(x)$, where d runs over all the positive divisors of m. In particular, $\Phi_p(x) = 1 + x + \cdots + x^{p-2} + x^{p-1}$ for any prime p.*

Definition 2.1.3. *For an integer m, define $\hat{m} = m/2$ if m is divisible by 2 and $\hat{m} = m$ otherwise. The radical of m, denoted rad(m), is defined as the product of all prime numbers that divide m.*

Fact 2.1.4 ([69], Fact 2.12)**.** *For any m, we have $\Phi_m(x) = \Phi_{rad(m)}(x^{m/rad(m)})$. In particular, if m is a power of a prime p, then $\Phi_m(x) = \Phi_p(x^{m/p})$.*

Throughout this dissertation we will be primarily concerned with principal ideals $I = (g(x))$ of the cyclotomic quotient ring $\mathbb{Z}[x]/(\Phi_m(x))$, denoted $(g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$. The choice of $\Phi_m(x)$ in constructing this quotient ring determines the action of multiplication within the ring. When denoting elements of a polynomial quotient ring, we somewhat abuse proper notation. The quotient ring $\mathbb{Z}[x]/(f(x))$ is constructed by essentially imposing the relation that $f(x) = 0$ in $\mathbb{Z}[x]$. If $r(x) \in \mathbb{Z}[x]$, then the elements in $\mathbb{Z}[x]$ that also map to the image of $r(x)$ in $\mathbb{Z}[x]/(f(x))$ are precisely the elements in the coset $r(x) + (f(x))$, which have the form $r(x) + q(x) \cdot f(x)$ for some $q(x) \in \mathbb{Z}[x]$. In this work, the element $r(x) \in \mathbb{Z}[x]/(f(x))$ is taken to be the unique polynomial $r(x) \in \mathbb{Z}[x]$ of degree less than $f(x)$ that represents the coset $r(x) + (f(x))$.

2.2 Algebraic Number Theory Background

A complex number $\alpha \in \mathbb{C}$ is an *algebraic number* of degree n if it is a root of some $f(x) \in \mathbb{Z}[x]$ of degree n and no polynomials of degree less than n. If, in addition, this polynomial $f(x) \in \mathbb{Z}[x]$ is monic then $\alpha \in \mathbb{C}$ is an *algebraic integer* of degree n. An *algebraic number field* K is formed by adjoining an algebraic number to the field of rational numbers $\mathbb{Q}$. The algebraic integers O_K of a number field K form a ring.

2.2.1 Cyclotomic Number Fields

By adjoining ζ_m to $\mathbb{Q}$ we form the mth *cyclotomic number field* of degree $\varphi(m) = n$, written $K_m = \mathbb{Q}(\zeta_m)$. The algebraic integers O_{K_m} in a cyclotomic number field K_m, also referred to as the ring of cyclotomic integers, form a commutative ring with unity. The cyclotomic field $K_m = \mathbb{Q}(\zeta_m)$ may be viewed as a vector space of dimension $\varphi(m) = n$ over $\mathbb{Q}$ with the basis $B = \{1, \zeta_m, \ldots, \zeta_m^{n-1}\}$, called the *power basis.* The power basis B is a $\mathbb{Q}$-basis for the cyclotomic field K_m and a $\mathbb{Z}$-basis for its ring of algebraic integers O_{K_m}, which implies $O_{K_m} \cong \mathbb{Z}[\zeta_m]$. Define a subspace $H \subseteq \mathbb{C}^n$ for some $n \geq 2$ as

$$H = \left\{ x \in \mathbb{C}^n \ : \ x_i = \overline{x}_{n-i+1} \text{ for all } i = 1, \ldots, n \right\}.$$

Let H be endowed with the norms induced by $\mathbb{C}^n$. The space H and $\mathbb{R}^n$ are isomorphic inner product spaces. The unitary basis matrix A of this isomorphism maps elements of H to elements of $\mathbb{R}^n$.

$$A = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & & & & & 1 \\ & \ddots & & & \iddots & \\ & & 1 & 1 & & \\ & & i & -i & & \\ & \iddots & & & \ddots & \\ i & & & & & -i \end{pmatrix}$$

The matrix A is an $n \times n$ matrix where the only non-zero elements are found on the diagonals. One may easily verify that this is a unitary matrix, and that it defines an isomorphism $H \cong \mathbb{R}^n$.

An *embedding* of a cyclotomic number field $K_m = \mathbb{Q}(\zeta_m)$ into $\mathbb{C}$ is a ring homomorphism $\sigma_i : K_m \to \mathbb{C}$ that fixes every element of $\mathbb{Q}$. The cyclotomic field K_m has exactly $\varphi(m) = n$ embeddings $\{\sigma_i\}_{i=1}^n$ that occur in conjugate pairs. They will be ordered according to $\sigma_i = \overline{\sigma_{n-i+1}}$. These embeddings are defined entirely by their action on the powers of ζ_m. Throughout this work it is common to assume that σ_1 is the identity map. We use the embeddings of a cyclotomic number field to define the canonical embedding. The *canonical embedding* $\sigma : K_m \to H \subset \mathbb{C}^{\varphi(m)}$ of an element $a \in K_m$ is the n-dimensional vector given by

$$\sigma(a) = (\sigma_i(a))_{i=1}^{n} = (\sigma_1(a), \ldots, \sigma_n(a))$$

where $\sigma_1(a) = \overline{\sigma_n(a)}$, $\sigma_2(a) = \overline{\sigma_{n-1}(a)}$ and so on. Let $B_0 = \{b_0, \ldots, b_{n-1}\}$ be a $\mathbb{Z}$-basis for the ring of cyclotomic integers O_{K_m}. The *field discriminant* $\mathcal{D}_{K_m}$ of a cyclotomic number field K_m is defined as the squared determinant $\mathcal{D}_{K_m} = \det([\sigma(O_{K_m})])^2$, where $[\sigma(O_{K_m})]$ is the $n \times n$ matrix

$$\begin{aligned}
[\sigma(O_{K_m})] &= \begin{pmatrix} \sigma(b_0) & \ldots & \sigma(b_{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} \sigma_1(b_0) & \ldots & \sigma_1(b_{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(b_0) & \ldots & \sigma_n(b_{n-1}) \end{pmatrix}
\end{aligned}$$

having the canonical embedding of $b_{i-1} \in B_0$ as its ith column. For cyclotomic fields with index m, the following formula may be used to compute the field discriminant.

$$\mathcal{D}_{K_m} = (-1)^{\varphi(m)/2} \cdot \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}$$

The product in the denominator is over all primes $p < m$ that divide m. This quantity $\mathcal{D}_{K_m}$ is a measure of the geometric sparsity of the cyclotomic integers $\sigma(B) \subset H$ under the canonical embedding [69].

$$\sigma(B) = \begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_m) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(1) & \sigma_n(\zeta_m) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \mathbb{Z}^n \subset H$$

Fact 2.2.1. *Let K be an algebraic number field with $O_K = \mathbb{Z}[\alpha]$ for some $\alpha \in O_K$. Then $\mathcal{D}_K$ is equal to the discriminant of the minimal polynomial of α over $\mathbb{Q}$.*

This fact from algebraic number theory yields the following implication: the field discriminant $\mathcal{D}_{K_m}$ is equal to the the discriminant of the mth cyclotomic polynomial $\Phi_m(x)$. This consequence is noted only to remark that the above formula for computing $\mathcal{D}_{K_m}$ may also be used to compute the polynomial discriminant of $\Phi_m(x)$.

2.2.2 The Powerful Basis

Another $\mathbb{Q}$-basis for K_m and $\mathbb{Z}$-basis for O_{K_m} is the *powerful basis*, which is presented nicely by the authors in [69]. Defining the powerful basis requires a tensorial decomposition of cyclotomic fields using the following proposition from algebraic number theory.

Proposition 2.2.2 ([69], Proposition 2.13)**.** *Let m have prime-power factorization $m = \prod_\ell m_\ell$, i.e. the m_ℓ are powers of distinct primes. Then $K_m = \mathbb{Q}(\zeta_m)$ is isomorphic to the tensor product $\bigotimes_\ell K_{m_\ell}$ of the fields $K_{m_\ell} = \mathbb{Q}(\zeta_{m_\ell})$, via the correspondence $\prod_\ell a_\ell \leftrightarrow (\otimes_\ell a_\ell)$, where on the left we implicitly embed each $a_\ell \in K_{m_\ell}$ into K_m.*

If F and K are two field extensions of $\mathbb{Q}$, then addition and multiplication in $F \otimes K$ are defined as follows: First, note that F, K are modules over $\mathbb{Q}$ [51]. The tensor product

$F \otimes K$ of these two fields is the set of all $\mathbb{Q}$-linear combinations of tensors $a \otimes b$ where $a \in F$ and $b \in K$. The tensor operation $\otimes$ by definition is then $\mathbb{Q}$-bilinear and satisfies the following relations for all $r \in \mathbb{Q}$, all $a_1, a_2 \in F$, and all $b_1, b_2 \in K$.

$$(a_1 + a_2) \otimes b_1 = a_1 \otimes b_1 + a_2 \otimes b_1$$
$$a_1 \otimes (b_1 + b_2) = a_1 \otimes b_1 + a_1 \otimes b_2$$
$$a_1 r \otimes b_1 = a_1 \otimes r b_1$$
$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$$

Let $L = (\ell_{ij})$ be an $m \times n$ matrix and $R = (r_{ij})$ a $p \times q$ matrix. The *Kronecker (tensor) product* of L and R is the $mp \times nq$ block matrix

$$L \otimes R = \begin{pmatrix} \ell_{11}R & \dots & \ell_{1n}R \\ \vdots & \ddots & \vdots \\ \ell_{m1}R & \dots & \ell_{mn}R \end{pmatrix}.$$

Similarly, the Kronecker product of two vectors $v = (v_0 \ \dots \ v_{n_1})$ and $w = (w_0 \ \dots \ w_{n_2})$ is defined as the vector of dimension $n_1 \cdot n_2$ given by

$$v \otimes w = \begin{pmatrix} v_0 \cdot w & \dots & v_{n_1} \cdot w \end{pmatrix}.$$

The *powerful basis* of $K_m = \mathbb{Q}(\zeta_m)$, denoted in this work by $B\prime$, is defined as follows by the authors of [69]. The authors of [69] remark that this basis coincides with the "canonical basis" of O_{K_m} appearing in [20].

Definition 2.2.3. *For a prime power m, define $B\prime$ to be the power basis $B = \{\zeta_m^i\}_{i=0}^{\varphi(m)-1}$, treated as a $\varphi(m)$-dimensional vector over O_{K_m}. For m having a prime-power factoriza-*

tion given by $m = \prod_\ell m_\ell$, define the powerful basis $B' = \bigotimes_\ell B'_\ell$, the tensor product of the power(ful) bases B'_ℓ of each $K_{m_\ell} = \mathbb{Q}(\zeta_{m_\ell})$.

The tensor product $B' = \bigotimes_\ell B'_\ell$ is a vector of dimension $\prod_\ell \varphi(m_\ell)$. Specifying an entry in B' requires one index $j_\ell \in \{0, \dots, \varphi(m_\ell) - 1\}$ for each prime-power factor of m to form a tuple (j_ℓ). The specified entry is then $B'_{(j_\ell)} = \prod_\ell \zeta_{m_\ell}^{j_\ell}$. As described in [69], this vector may be "flattened" to a vector of dimension $\varphi(m)$ by using the relation $\zeta_{m_\ell} = \zeta_m^{m/m_\ell} \in K_m$. Specifically, the tuple (j_ℓ) of indices from each prime-power factor of m maps to $j = \sum_\ell (m/m_\ell) j_\ell \mod m$ and then $B' = \{\zeta_m^j\}$. Our convention is to arrange the elements of B' so that the exponent $j \in \{0, \dots, \varphi(m) - 1\}$ of ζ_m is ordered from least to greatest.

Example 2.2.4. *Consider the cyclotomic index $m = 12$. The power basis of $K_{12} = \mathbb{Q}(\zeta_{12})$ is given by $B = \{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$. To construct the powerful basis, observe that the cyclotomic field $K_{12} \cong K_4 \otimes K_3$ by the tensorial decomposition. K_4 has power(ful) basis $B'_4 = \{\zeta_4^0, \zeta_4\}$ and K_3 has power(ful) basis $B'_3 = \{\zeta_3^0, \zeta_3\}$. By treating B'_4 and B'_3 as vectors, their Kronecker (tensor) product is given by*

$$B'_{12} = B'_4 \otimes B'_3 = \begin{pmatrix} (\zeta_4^0 \cdot \zeta_3^0) & (\zeta_4^0 \cdot \zeta_3^1) & (\zeta_4^1 \cdot \zeta_3^0) & (\zeta_4^1 \cdot \zeta_3) \end{pmatrix}.$$

Using the relation $\zeta_{m_\ell} = \zeta_m^{m/m_\ell}$ yields

$$B'_{12} = B'_4 \otimes B'_3 = \begin{pmatrix} (\zeta_{12}^0 \cdot \zeta_{12}^0) & (\zeta_{12}^0 \cdot \zeta_{12}^4) & (\zeta_{12}^3 \cdot \zeta_{12}^0) & (\zeta_{12}^3 \cdot \zeta_{12}^4) \end{pmatrix}.$$

Hence the powerful basis of $K_{12} = \mathbb{Q}(\zeta_{12})$ is given by $B' = \{1, \zeta_{12}^3, \zeta_{12}^4, \zeta_{12}^7\}$.

Referring to specific power or powerful bases may be useful throughout this dissertation. In this event, the cyclotomic index m will be used to denote the power basis

B_m and the powerful basis $B\prime_m$ of the mth cyclotomic number field. See [69] for a more detailed discussion on the powerful basis and results pertaining to its algebraic and geometric properties. The powerful basis exhibits some geometrical advantages over the power basis, but both bases will be used in this work as it becomes convenient.

2.3 Lattice Background

A *lattice* is a discrete additive subgroup of some specified geometric space. The primary focus in this dissertation will be on lattices in $\mathbb{R}^n$, although lattices in the space $H \subset \mathbb{C}^n$ will arise as well. We will be concerned exclusively with full-rank lattices. Given a set of n linearly independent vectors $\{b_1, \ldots, b_n\} \subset \mathbb{R}^n$, the *lattice* (or $\mathbb{Z}$-module) generated by these vectors is the set of all integer linear combinations

$$\mathcal{L} = \left\{ \sum_{1 \le i \le n} \alpha_i b_i \ : \ \alpha_i \in \mathbb{Z} \right\}.$$

A *basis* of this n-dimensional lattice consists of n linearly independent vectors whose integer span generates the same set $\mathcal{L}$. It is often convenient to represent the lattice with a basis matrix $B = (b_{ij})$ having the vectors $b_1, \ldots, b_n$ as columns. This is to be interpreted as

$$\mathcal{L} = \mathcal{L}(B) = (B)\mathbb{Z}^n = \begin{pmatrix} b_1 & \ldots & b_n \end{pmatrix} \mathbb{Z}^n.$$

Intuitively the lattice $\mathcal{L}$ is an arrangement of points in $\mathbb{R}^n$. We associate with each of these points a vector originating from the origin. It is natural to ask which vector of a given lattice is the shortest. This is the well-known, NP-hard shortest vector problem (SVP).

Definition 2.3.1 (Shortest Vector Problem, SVP)**.** *Given a basis matrix $B \in \mathbb{R}^{n\times n}$ and a p-norm $\|\cdot\|_p$, find a non-zero lattice vector Bx such that $Bx = \min \|By\|_p$ for any $y \in \mathbb{Z}^n \setminus \{0\}$.*

The sole norm used in this study of the SVP will be the Euclidean norm (2-norm). Observe that there is not a unique solution to the SVP. For instance, if $v \in \mathcal{L}$ solves the SVP, then so does $-v \in \mathcal{L}$. Accordingly, we are interested in *a* shortest vector instead of *the* shortest vector. Approximation versions of this problem are also widely considered in the literature. The *approximate shortest vector problem*, denoted appr-SVP, is solved by finding a non-zero lattice vector whose norm is within some approximation factor to that of a shortest vector.

Given an n-dimensional non-trivial lattice $\mathcal{L}$ define its ith *successive minima* $\lambda_i(\mathcal{L})$ (for $i = 1, \ldots, n$) as the smallest radius such that the ball $B(0, \lambda_i)$ centered at the origin contains i linearly independent lattice vectors. When the lattice is clear from context we write λ_i rather than $\lambda_i(\mathcal{L})$. As with the SVP, successive minima can be defined with respect to any norm, but we again choose to work strictly with the Euclidean norm. Note that $0 < \lambda_1 \leq \cdots \leq \lambda_n$, and the value of λ_1 is the length of a solution to the SVP (with respect to the same norm). A lattice is called *well-rounded* (WR) if $\lambda_1 = \lambda_2 = \cdots = \lambda_n$. This characterization implies that all WR lattices have a basis consisting of shortest vectors.

The *fundamental parallelepiped*, or *fundamental domain*, is another important concept in the study of lattices. Given a lattice $\mathcal{L}$ with basis $\{b_1, \ldots, b_n\}$, the fundamental domain of $\mathcal{L}$ is defined as the region

$$\mathcal{F}(b_1, \ldots, b_n) = \{t_1 b_1 + \cdots + t_n b_n \ : \ 0 \leq t_i < 1 \text{ for all } i\}.$$

Lemma 2.3.2 ([120], Lemma 16.2)**.** *Let $L \subseteq M \subseteq \mathbb{R}^n$ be lattices generated by vectors $\ell_1, \ldots, \ell_n$ and $m_1, \ldots, m_n$ respectively. Then* $\det(m_{ij})_{1 \leq i,j \leq n}$ *divides* $\det(\ell_{ij})_{1 \leq i,j \leq n}$.

Proof.

For $1 \leq i, j \leq n$ there exists some $a_{ij} \in \mathbb{Z}$ such that $\ell_{ij} = \sum_{1 \leq j \leq n} a_{ij} m_j$. Hence $|\det(\ell_{ij})| = |\det(a_{ij})| \cdot |\det(m_{ij})|$ and the claim follows.

□

In particular, if $L = M$ is taken to be the same lattice, then this result implies that any two bases for a lattice are related by an integer matrix with determinant ±1. Thus the absolute value of the determinant of a basis matrix is invariant under the choice of basis for the lattice and remains constant. Geometrically this quantity corresponds to the volume of the fundamental parallelepiped. For a lattice $\mathcal{L}$ with basis matrix B, define the *norm*, or *determinant*, of the lattice $\mathcal{L}$ to be $|\mathcal{L}(B)| = |\det(B)| = vol(\mathcal{F}(B))$.

Since the volume of the fundamental parallelepiped does not depend on the choice of basis, pushing the orthogonality of basis vectors creates shorter vectors. This notion governs the geometric procedures appearing in many lattice reduction algorithms, which are designed to produce very short vectors. Given a basis for the lattice $\mathcal{L}$, the goal of lattice reduction is to return a basis consisting of short, reasonably orthogonal vectors. Lattice reduction algorithms are the most common approach to the SVP. Perhaps the most significant, and certainly the most noted, lattice reduction algorithm is the LLL algorithm [63]. We use this algorithm for the experiments described in Chapter 4, however its functionality is not essential to understanding the work presented in this dissertation. We turn the reader to our bibliography for references that provide a detailed analysis of the LLL and its applications, e.g. [21, 89, 120].

2.4 Ideal Lattices

Let $\theta : K_m \to \mathbb{R}^n$ be an additive homomorphism where $\varphi(m) = n$. This homomorphism will embed any ideal $I \lhd O_{K_m}$ in the ring of cyclotomic integers geometrically into $\mathbb{R}^n$ as a lattice $\theta(I)$, called an *ideal lattice*. The map θ is called a *geometric embedding* of I. When the geometric embedding is clear from context, the ideal I will be synonymous with this lattice. Commonly computed lattice quantities (determinant, successive minima, etc.) may then be affiliated with the ideal I. If this ideal I is a principal ideal, then we call the lattice $\theta(I)$ a *principal ideal lattice*. It is of great importance to note that general lattices have the algebraic structure of a group, but ideal lattices possess the structure of a ring. This dissertation is aimed at exploiting that additional algebraic structure when solving the SVP in (principal) ideal lattices.

2.4.1 The Canonical and Coefficient Embeddings

Our primary interests are situated around two particular geometric embeddings. The first embedding of interest is the canonical embedding σ. Given an ideal $I \lhd O_{K_m}$ in the ring of cyclotomic integers with $\mathbb{Z}$-basis $B_0 = \{b_0, \ldots, b_{n-1}\}$, a $\mathbb{Z}$-basis for the ideal lattice $\sigma(I) \subset H$ under the canonical embedding will be $\sigma(B_0) = \{\sigma(b_0), \ldots, \sigma(b_{n-1})\}$. The map $\sigma : K_m \to H$ may be viewed as a map $\sigma : K_m \to \mathbb{R}^n$ by using the matrix A as a transformation $A : H \to \mathbb{R}^n$. Henceforth we will assume that σ maps into $\mathbb{R}^n$ unless noted otherwise.

Example 2.4.1. *The Canonical Embedding of* $(3 + 2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$.

Consider the power basis $B = \{1, \zeta_6\}$ *of* $\mathbb{Z}[\zeta_6]$*. Let* I *denote the ideal* $(3 + 2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$*. There are two (complex) embeddings* $\sigma_1(\zeta_6) = \zeta_6$ *and* $\sigma_2(\zeta_6) = \overline{\sigma_1(\zeta_6)} = \overline{\zeta_6}$ *associated with this field extension. The canonical embedding* σ *of an element* $a \in \mathbb{Q}(\zeta_6)$ *is therefore* *given by* $\sigma(a) = (\sigma_1(a), \sigma_2(a))$*. Since* $B = \{(3+2\zeta_6),\ (-2+5\zeta_6)\}$ *is an integral basis of* $(3+2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$*, it follows that* $\sigma(B) = \{\sigma(3+2\zeta_6), \sigma(-2+5\zeta_6)\}$ *is an integral basis of* $\sigma(I) \subset H$*.*

$$\begin{aligned}\sigma(3+2\zeta_6) &= (\sigma_1(3+2\zeta_6), \sigma_2(3+2\zeta_6)) \\ &= (4+i\sqrt{3}, 4-i\sqrt{3})\end{aligned}$$

$$\begin{aligned}\sigma(-2+5\zeta_6) &= (\sigma_1(-2+5\zeta_6), \sigma_2(-2+5\zeta_6)) \\ &= (\frac{1+i(5\sqrt{3})}{2}, \frac{1-i(5\sqrt{3})}{2})\end{aligned}$$

Thus the lattice $\sigma(I) \subset H$ *is given by*

$$\sigma(I) = \begin{pmatrix} 4+i\sqrt{3} & \frac{1+i(5\sqrt{3})}{2} \\ 4-i\sqrt{3} & \frac{1-i(5\sqrt{3})}{2} \end{pmatrix} \mathbb{Z}^2.$$

By applying the matrix A*, this ideal lattice will be viewed as an ideal lattice* $\mathcal{L} \subset \mathbb{R}^2$*.*

$$\begin{aligned}[\sigma(I)]_B = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \cdot \begin{pmatrix} 4+i\sqrt{3} & \frac{1+i(5\sqrt{3})}{2} \\ 4-i\sqrt{3} & \frac{1-i(5\sqrt{3})}{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 8 & 1 \\ -2\sqrt{3} & -5\sqrt{3} \end{pmatrix} \\ \Rightarrow \mathcal{L} = [\sigma(I)]_B \mathbb{Z}^2 = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 8 & 1 \\ -2\sqrt{3} & -5\sqrt{3} \end{pmatrix} \mathbb{Z}^2\end{aligned}$$

Figure 2.1 depicts the two-dimensional principal ideal lattice corresponding to the principal ideal $(3+2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$ *under the canonical embedding.*

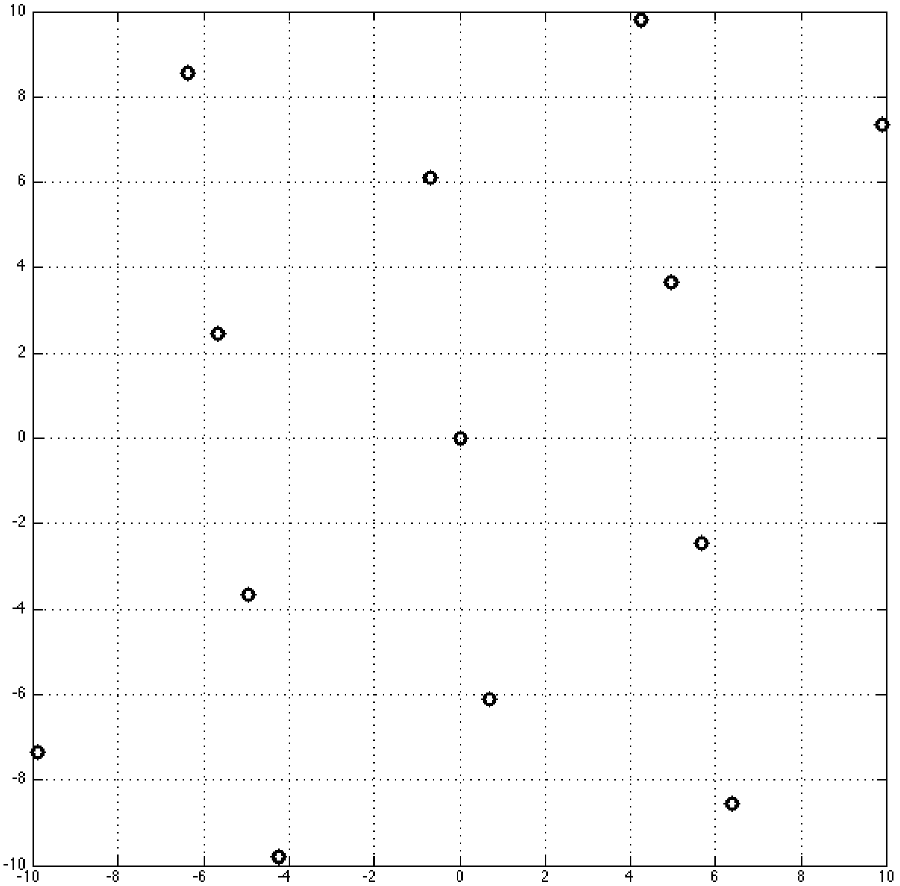

Figure 2.1: Canonical Embedding of $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$

Observe that there are six possible solutions to the SVP in this example. This lattice is WR, so it admits a basis of minimal vectors. Also note the geometric sparsity of lattice points. The spacing of points in ideal lattices under the canonical embedding seems to be more even than in ideal lattices under the second embedding of interest.

Fix a basis $B_0 = \{b_0, \ldots, b_{n-1}\}$ that is an ordered $\mathbb{Q}$-basis for K_m and $\mathbb{Z}$-basis for O_{K_m} where $\varphi(m) = n$, such as the power basis B or powerful basis $B\prime$. The *coefficient embedding* $c : K_m \to \mathbb{R}^n$ of an element $a \in K_m$ is given by its coordinate vector relative to the basis B_0, written $[a]_{B_0}$. The image of an ideal $I \triangleleft O_{K_m}$ under c is the ideal lattice

$c(I) \subset \mathbb{R}^n$. There is a clear correspondence between vectors of the lattice and elements of the ideal given by

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \end{pmatrix} \in c(I) \leftrightarrow \alpha_0 b_0 + \alpha_1 b_1 + \cdots + \alpha_{n-1} b_{n-1} \in I$$

where $\alpha_i \in \mathbb{Z}$.

Example 2.4.2. *The Coefficient Embedding of* $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$.
Consider the power basis $B = \{1, \zeta_6\}$ *of* $\mathbb{Z}[\zeta_6]$. *First, find an integral basis for the principal ideal* $(3+2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$, *which will correspond to a basis of the principal ideal lattice. Since* $\varphi(6) = 2$, *this will be a two-dimensional lattice. Clearly* $3+2\zeta_6 \in I$, *and by the definition of ideal this implies that* $\zeta_6 \cdot (3 + 2\zeta_6) \in I$. *Recall that*

$$\zeta_6 = e^{2\pi i/6} = \frac{1+\sqrt{-3}}{2} \quad \Rightarrow \quad \zeta_6^2 = e^{4\pi i/6} = \frac{-1+\sqrt{-3}}{2}.$$

We must now express $\zeta_6 \cdot (3 + 2\zeta_6)$ *in terms of the basis* $\{1, \zeta_6\}$ *for* $\mathbb{Z}[\zeta_6]$. *Observe*

$$\begin{aligned} \zeta_6 \cdot (3 + 2\zeta_6) &= 3\zeta_6 + 2\zeta_6^2 \\ &= 3\zeta_6 + 2(-1 + \zeta_6) \text{ \textit{relative to the basis} } \{1, \zeta_6\} \text{ \textit{of} } \mathbb{Z}[\zeta_6] \\ &= -2 + 5\zeta_6. \end{aligned}$$

The elements $3 + 2\zeta_6 \in I$ *and* $-2 + 5\zeta_6 \in I$ *form an integral basis for the ideal. These polynomials in* ζ_6 *will correspond to vectors that constitute a basis for the associated* *principal ideal lattice under the coefficient embedding.*

$$\begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}-2\\5\end{pmatrix} \in \mathcal{L} \quad \Rightarrow \quad \mathcal{L} = \begin{pmatrix}3 & -2\\2 & 5\end{pmatrix}\mathbb{Z}^2$$

Figure 2.2 depicts the two-dimensional principal ideal lattice corresponding to the principal ideal $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$ *under the coefficient embedding.*

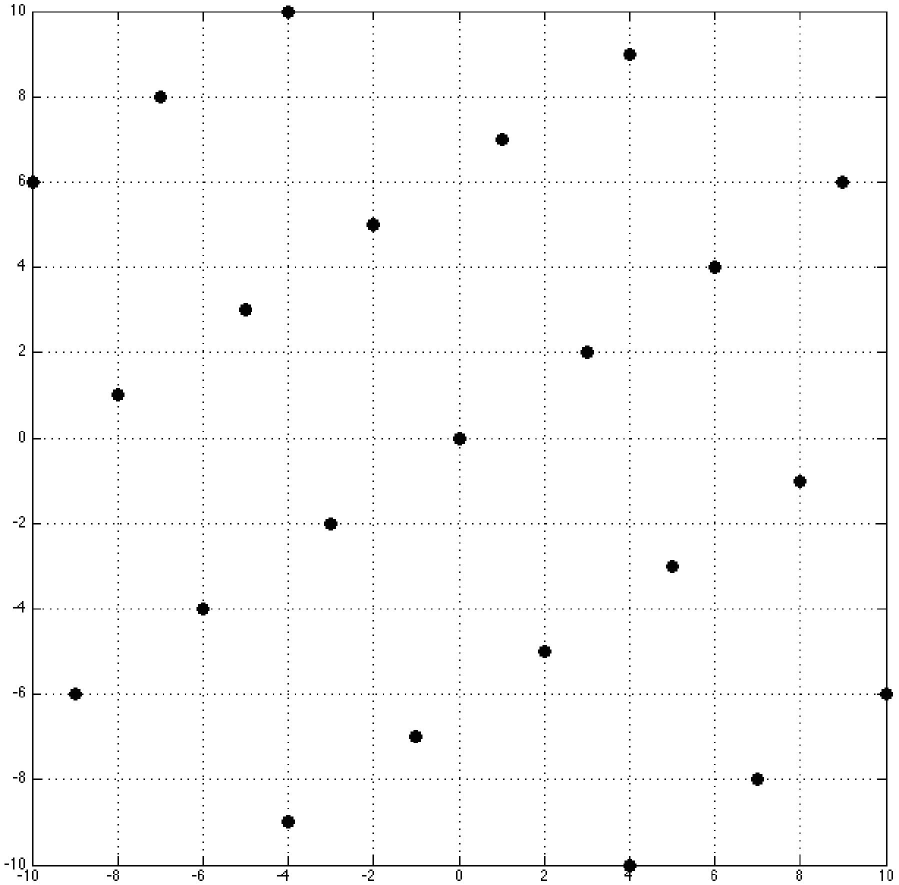

Figure 2.2: Coefficient Embedding of $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$

Note some differences between the canonical and coefficient embeddings of $(3+2\zeta_6) \triangleleft O_{K_6}$ presented in Examples 2.4.1 and 2.4.2. First, the ideal lattice $c(I)$ does not have as many shortest vectors as $\sigma(I)$. There are only two possible solutions to the SVP, which are linearly dependent. The ideal lattice $c(I)$ is not WR because there is no lattice basis of minimal vectors. Finally, the lattice points in $c(I)$ are not as sparse as the points of $\sigma(I)$.

2.4.2 Ideal Lattices and Quotient Rings

Recall the isomorphism $\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathbb{Z}[\zeta_m] \cong O_{K_m}$ via the mapping $x \leftrightarrow \zeta_m$, and consider the power basis $B = \{1, \zeta_m, \ldots, \zeta_m^{n-1}\}$ of K_m. The coefficient embedding of an ideal $I \triangleleft \mathbb{Z}[\zeta_m]$ relative to B is equivalent to the coefficient embedding of the corresponding ideal $I \triangleleft \mathbb{Z}[x]/(\Phi_m(x))$ relative to the power basis $B = \{1, x, \ldots, x^{n-1}\}$ of $\mathbb{Z}[x]/(\Phi_m(x))$. This equivalent characterization will allow us to investigate the algebraic structure of ideal lattices from a quotient ring perspective.

Example 2.4.3. *The Coefficient Embedding of* $(3+2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$.
Use the power basis $B = \{1, x\}$ *of* $\mathbb{Z}[x]/(\Phi_6(x))$. *Find an integral basis for the principal ideal* $(3+2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$, *which will correspond to a basis of the principal ideal lattice* $\mathcal{L}$. *Since* $\varphi(6) = 2$, *this will be a two-dimensional lattice. Clearly* $3+2x \in I$, *and by the definition of ideal this implies that* $x \cdot (3+2x) \mod x^2 - x + 1 \in I$. *We must now compute* $x \cdot (3+2x) \mod x^2 - x + 1$. *Observe*

$$\begin{aligned} x \cdot (3+2x) \mod x^2 - x + 1 &= 3x + 2x^2 \mod \Phi_6(x) \\ &= 3x + 2(x-1) \mod \Phi_6(x) \\ &= -2 + 5x \mod x^2 - x + 1. \end{aligned}$$

Now that we have a basis for the ideal, one may show that these polynomials will correspond to vectors that constitute a basis for the associated principal ideal lattice under the coefficient embedding.

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 5 \end{pmatrix} \in \mathcal{L} \text{ and } \mathcal{L} = \begin{pmatrix} 3 & -2 \\ 2 & 5 \end{pmatrix} \mathbb{Z}^2$$

Figure 2.3 depicts the two-dimensional principal ideal lattice corresponding to the principal ideal $(3 + 2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$ under the coefficient embedding.

By looking at the ideal lattices constructed in Examples 2.4.2 and 2.4.3, one may quickly infer that the coefficient embedding relative to the power basis is indeed equivalent to a quotient ring perspective of ideal lattices. The quotient ring characterization of an ideal lattice is a lattice $\mathcal{L}$ where every vector $v \in \mathcal{L}$ corresponds to a polynomial $v(x) \in I$ for some ideal $I \triangleleft \mathbb{Z}[x]/(\Phi_m(x))$. This correspondence is given by

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \end{pmatrix} \in \mathcal{L} \leftrightarrow \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \in I.$$

Clearly this defines an isomorphism between an ideal of $\mathbb{Z}[x]/(\Phi_m(x))$ and a lattice. We identify that lattice with its corresponding ideal and quotient ring, and often write $\mathcal{L} \cong I \triangleleft \mathbb{Z}[x]/(\Phi_m(x))$.

Proposition 2.4.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n. If $v(x) \in \mathbb{Z}[x]/(f(x))$ is any non-zero element relatively prime to $f(x)$, then the vectors corresponding to $v(x), x \cdot v(x), \dots, x^{n-1} \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ in $\mathbb{R}^n$ are linearly independent.*

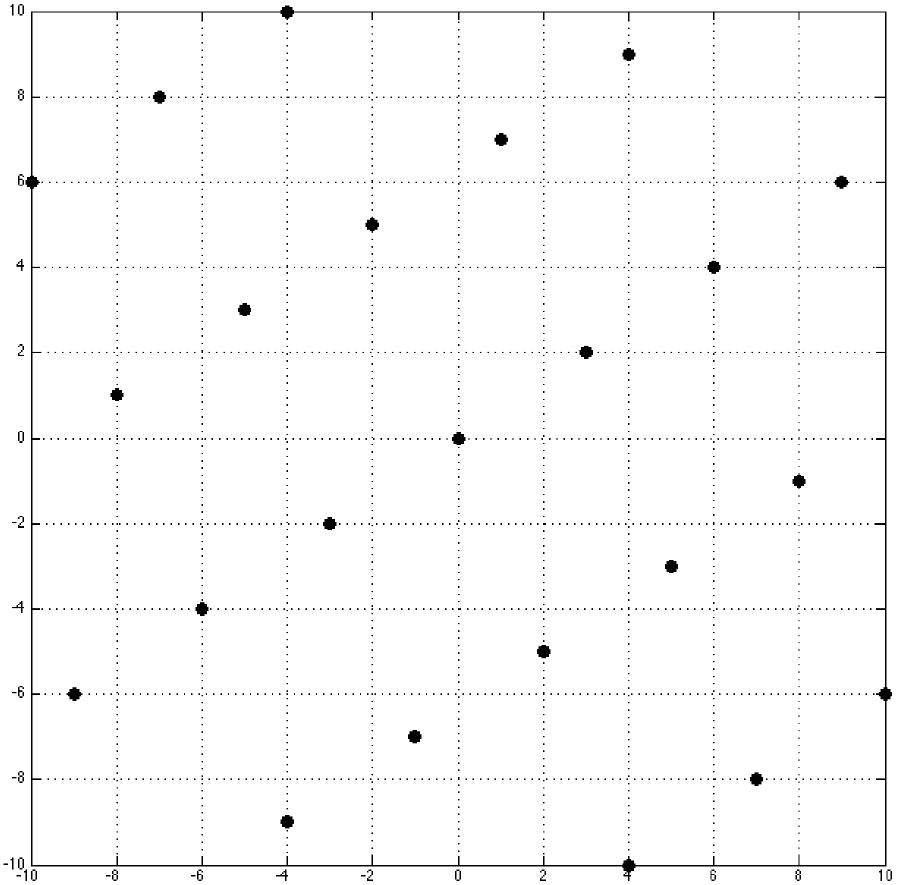

Figure 2.3: Coefficient Embedding of $(3+2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$

Proof.

Suppose that there is a linear combination of the vectors corresponding to $v(x), x \cdot v(x), \ldots, x^{n-1} \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ equal to zero.

$$\sum_{i=0}^{n-1} \alpha_i \cdot x^i \cdot v(x) = 0 \mod f(x)$$

Then $v(x) \cdot (\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}) = 0 \mod f(x)$. Equivalently, the polynomial $f(x)$ divides this product $f(x) | v(x) \cdot (\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1})$. Note that $\mathbb{Z}[x]$ is a unique factorization domain. Since $f(x)$ is relatively prime to $v(x)$ by assumption, $f(x)$ and $v(x)$ have no common divisors. Thus $f(x)|(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1})$. However, $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1})$ has degree strictly less than $f(x)$, which is a contradiction unless $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1})$ is 0. Hence $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}) = 0$ and the vectors corresponding to $v(x), x \cdot v(x), \ldots, x^{n-1} \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ are linearly independent.

□

Corollary 2.4.5 ([65], Lemma 2.12)**.** *Let $\mathcal{L}$ be a lattice corresponding to a non-zero ideal in the ring $\mathbb{Z}[x]/(f(x))$ where $f(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial of degree n. Then $\mathcal{L}$ is a full-rank lattice of dimension n.*

Proof.

At least one generator of the ideal is non-zero since the ideal is not trivial, say $v(x) \in \mathbb{Z}[x]/(f(x))$. Since $f(x) \in \mathbb{Z}[x]$ is monic and irreducible by assumption, $v(x)$ and $f(x)$ are relatively prime. Hence the elements $v(x), x \cdot v(x), \ldots, x^{n-1} \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ are both in the ideal and linearly independent by Proposition 2.4.4. Thus, $\mathcal{L}$ is n-dimensional and hence full-rank.

□

Corollary 2.4.6. *Let $\mathcal{L}$ be a lattice corresponding to a non-zero principal ideal $I = (g(x))$ in the ring $\mathbb{Z}[x]/(f(x))$ where $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree n and $g(x) \in \mathbb{Z}[x]/(f(x))$. If $g(x)$ and $f(x)$ are relatively prime, then $\mathcal{L}$ is a full-rank lattice of dimension n.*

Proof.

Since $g(x) \in \mathbb{Z}[x]/(f(x))$ is non-zero and relatively prime to $f(x)$ by assumption, the vectors corresponding to $g(x), x \cdot g(x), \ldots, x^{n-1} \cdot g(x) \in \mathbb{Z}[x]/(f(x))$ are in the ideal

$I = (g(x))$ and linearly independent by Proposition 2.4.4, which implies that $\mathcal{L}$ is n-dimensional and hence full-rank.

□

Corollary 2.4.7. *Let $m = 2^k$ be a power-of-two cyclotomic index and $I \lhd \mathbb{Z}[x]/(\Phi_m(x))$ be a non-trivial ideal. If $\mathcal{L} \cong I \lhd \mathbb{Z}[x]/(\Phi_m(x))$ is an ideal lattice, then $\mathcal{L}$ is well-rounded.*

Proof.
Since $m = 2^k$ is a power of two, the cyclotomic polynomial has the form $\Phi_m(x) = x^{2^{k-1}}+1$. Let $0 \neq g(x) \in I$ be the polynomial in the ideal that corresponds to a shortest vector of $\mathcal{L}$. Then $g(x), x\cdot g(x), \ldots, x^{n-1}\cdot g(x) \in I$ are all linearly independent and their corresponding vectors have the same norm as the vector that corresponds to $g(x) \in I$. Thus $\mathcal{L}$ has n linearly independent shortest vectors, and is WR by definition.

□

In particular, these general results hold if $f(x)$ is taken to be the cyclotomic polynomial $\Phi_m(x)$. The vectors in Proposition 2.4.4 will be used to construct a particular lattice basis for the principal ideal lattices studied in this work. Consider a principal ideal $(g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$ generated by the polynomial $g(x) \in \mathbb{Z}[x]/(\Phi_m(x))$. The *rotation basis matrix* of $g(x)$ for the corresponding principal ideal lattice is given by

$$G = \begin{pmatrix} g(x) & x \cdot g(x) & \ldots & x^{n-1} \cdot g(x) \end{pmatrix},$$

where the ith column of G is the coefficient vector that corresponds to $x^{i-1} \cdot g(x)$ mod $\Phi_m(x)$. When constructing a rotation matrix, we always assume the polynomials $x^i \cdot g(x)$ are reduced mod the appropriate polynomial. This rotation matrix defines the ideal lattice $\mathcal{L} \cong (g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$.

For any monic, irreducible $f(x) \in \mathbb{Z}[x]$ in general, observe that the vectors corresponding to $x^i \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ for $i = 1, \ldots, n-1$ will most likely not have the same norm as $v(x) \in \mathbb{Z}[x]/(f(x))$. The form of $f(x)$ determines how multiplication by x in the ring $\mathbb{Z}[x]/(f(x))$ may expand the coefficients of polynomials, and thus the norm of their corresponding vectors. Bounding the norm of vectors corresponding to $v(x), x \cdot v(x) \in \mathbb{Z}[x]/(f(x))$ through an expansion factor was considered in [65]. The authors concluded that suitable choices of $f(x)$ include $f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ where n is prime, and $f(x) = x^n + 1$ where n is a power of two. By Facts 2.1.2 and 2.1.4 these two polynomials are cyclotomic polynomials of prime cyclotomic index and power-of-two cyclotomic index, respectively.

At this point we would like to address the choice to work exclusively with cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$ in this dissertation. For an algebraic number field K in general, any additive homomorphism $\theta : K \to \mathbb{R}^n$ (or $\mathbb{C}^n$) will embed ideals of O_K as an ideal lattice. Ideal lattices have been defined in the literature as both a geometric embedding of an ideal in O_K, and also as a lattice whose vectors correspond to elements of an ideal in the ring $\mathbb{Z}[x]/(f(x))$ for some monic, irreducible $f(x) \in \mathbb{Z}[x]$. The algebraic number theory definition of an ideal lattice is accepted to be the more mathematically correct notion. However, we desire to investigate ideal lattices algebraically, and geometrically, using the quotient ring perspective. The following fact provides a connection between algebra and algebraic number theory.

Lemma 2.4.8. *If $f(x) \in \mathbb{Z}[x]$ is the (monic) minimal polynomial of $\theta \in \mathbb{C}$, then $\mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}[\theta]$.*

Proof.

If $f(x)$ is degree n, any $\alpha \in \mathbb{Z}[\theta]$ may be expressed an integer linear combination of

$\{1, \theta, \ldots, \theta^{n-1}\}$. Define an isomorphism $\eta : \mathbb{Z}[x]/(f(x)) \to \mathbb{Z}[\theta]$ where $p(x) \mapsto p(\theta)$.

□

To have any equivalence between the algebraic number theory and quotient ring definitions of ideal lattices would require the ring of algebraic integers O_K of a number field K to be expressed as $\mathbb{Z}[\theta]$ for some $\theta \in O_K$. Number fields satisfying this condition are called *monogenic number fields*. Not all number fields are monogenic, but quadratic and cyclotomic fields are. Hence, $\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathbb{Z}[\zeta_m] \cong O_{K_m}$ for cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$.

Chapter 3

The Relationship Between the Canonical and Coefficient Embeddings

In this chapter, the relationship between the canonical and coefficient embeddings of an ideal will be explored. It will be shown that these embeddings are related by a fixed linear transformation that depends only on the cyclotomic number field, and the matrix T of this transformation will be defined explicitly. The structure of this matrix will be studied and conditions for when the SVP is equivalent in any two embeddings of an ideal will be provided. In particular, we will use the 2-norm condition number $\kappa_2(T)$ of the matrix T to show that the SVP will be equivalent up to this “distortion” factor. It will also be shown that the coefficient embedding of an ideal will have no more independent shortest vectors than the canonical embedding of the ideal.

Developing the relationship that exists between the canonical and coefficient embeddings provides a template that may be used to understand the relationship between any two geometric embeddings. For instance, from the work presented here, one may infer that any two geometric embeddings of an ideal will be related by a fixed linear transformation that depends only on the number field K, which is true by definition, or that the SVP in these two embeddings will be equivalent up to a factor corresponding to the distortion between the embeddings (i.e. the 2-norm condition number of the matrix of the transformation relating them). These inferences are observations that the authors of [68] made while discussing their choice to work with the canonical embedding. While a very strong case is made in [68, 69, 93] that the canonical embedding is the best notion to use in working with ideal lattices, it is more natural from an abstract algebra standpoint to consider the coefficient embedding, which is the approach taken in the next chapter.

A discussion about how the algebraic number theory perspective of ideal lattices encompasses an equivalent of the quotient ring viewpoint may be found in Chapter 2. From a number-theoretic point of view it is more natural to consider the canonical embedding of an element as opposed to its coefficient embedding. Hence, to justify working with ideal lattices as ideals of polynomial quotient rings, the relationship between the canonical and coefficient embeddings of an ideal in $\mathbb{Z}[\zeta_m]$ must be well developed and understood.

3.1 The Transformation Relating the Canonical and Coefficient Embeddings

Denote the change of basis matrix from B to $B\prime$ by $[I]_B^{B\prime}$. For an ideal $J \triangleleft O_{K_m}$, let $[c(J)]_B$ and $[\sigma(J)]_B$ denote the matrix of the ideal lattice in $\mathbb{R}^n$ under the coefficient and canonical embeddings relative to integral basis B of $O_{K_m} \cong \mathbb{Z}[\zeta_m]$, respectively.

Theorem 3.1.1. *Let $J \lhd O_{K_m}$ be any ideal in the ring of cyclotomic integers, and let B and B' denote the power and powerful bases of O_{K_m}, respectively. The canonical and coefficient embeddings of J, relative to B, are related by a fixed linear transformation T given by the matrix $T = [\sigma(O_{K_m})]_B$. Moreover, the following matrix relations hold.*

1. $[I]_B^{B'} \cdot [c(J)]_B = [c(J)]_{B'}$

2. $[c(J)]_B = [I]_{B'}^{B} \cdot [c(J)]_{B'}$

3. $[\sigma(O_{K_m})]_B \cdot [I]_{B'}^{B} = [\sigma(O_{K_m})]_{B'}$

4. $[\sigma(O_{K_m})]_B = [\sigma(O_{K_m})]_{B'} \cdot [I]_B^{B'}$

5. $[\sigma(O_{K_m})]_B \cdot [c(J)]_B = [\sigma(O_{K_m})]_B \cdot [I]_{B'}^{B} \cdot [c(J)]_{B'} = [\sigma(J)]_B$

6. $[\sigma(O_{K_m})]_{B'} \cdot [c(J)]_{B'} = [\sigma(O_{K_m})]_{B'} \cdot [I]_B^{B'} \cdot [c(J)]_B = [\sigma(J)]_{B'}$

Proof.

(1) and (2) are true by the definition of a change of basis matrix. A proof of (5) will be given because the proof of (6) is similar. It will only be shown that $[\sigma(O_{K_m})]_B \cdot [c(J)]_B = [\sigma(J)]_B$ because $[\sigma(O_{K_m})]_B \cdot [c(J)]_B = [\sigma(O_{K_m})]_B \cdot [I]_{B'}^{B} \cdot [c(J)]_{B'}$ follows from (1).

Take $K_m = \mathbb{Q}(\zeta_m) \Rightarrow O_{K_m} \cong \mathbb{Z}[\zeta_m]$ and let $\varphi(m) = n$. The power basis of O_{K_m} is $B = \{1, \zeta_m, \ldots, \zeta_m^{n-1}\}$. Suppose that J is any (not necessarily proper) ideal of O_{K_m} having $\mathbb{Z}$-basis $\{b_1, \ldots, b_\ell\}$ where $b_j \in O_{K_m}$ for all $j \in \{1, \ldots, \ell\}$. We want to show

$[\sigma(O_{K_m})]_B \cdot [c(J)]_B = [\sigma(J)]_B$. By construction,

$$[\sigma(O_{K_m})] = A \cdot \begin{pmatrix} \sigma(1) & \dots & \sigma(\zeta_m^{n-1}) \end{pmatrix} = A \cdot \begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix},$$

$$[c(J)]_B = \begin{pmatrix} [b_1]_B & \dots & [b_\ell]_B \end{pmatrix},$$

$$\text{and } [\sigma(J)]_B = A \cdot \begin{pmatrix} \sigma(b_1) & \dots & \sigma(b_\ell) \end{pmatrix} = A \cdot \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_\ell) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \dots & \sigma_n(b_\ell) \end{pmatrix},$$

where $A = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & & & & & 1 \\ & \ddots & & & \iddots & \\ & & 1 & 1 & & \\ & & i & -i & & \\ & \iddots & & & \ddots & \\ i & & & & & -i \end{pmatrix}$ is an $n \times n$ unitary matrix. Hence it must be shown that

$$A \cdot \begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \cdot \begin{pmatrix} [b_1]_B & \dots & [b_\ell]_B \end{pmatrix} = A \cdot \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_\ell) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \dots & \sigma_n(b_\ell) \end{pmatrix}.$$

It will suffice to show that

$$\begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \cdot \begin{pmatrix} [b_1]_B & \dots & [b_\ell]_B \end{pmatrix} = \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_\ell) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \dots & \sigma_n(b_\ell) \end{pmatrix}$$

or even

$$\begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \cdot \begin{pmatrix} [b_i]_B \end{pmatrix} = \begin{pmatrix} \sigma_1(b_i) \\ \vdots \\ \sigma_n(b_i) \end{pmatrix} = \begin{pmatrix} [\sigma(b_i)]_B \end{pmatrix}$$

for an arbitrary $i \in \{1, \dots, \ell\}$. Suppose that $b_i = \alpha_1 \cdot 1 + \cdots + \alpha_n \cdot \zeta_m^{n-1}$, meaning that the coordinates of b_i relative to the power basis B are

$$\begin{pmatrix} [b_i]_B \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Observe

$$\begin{aligned}
\begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \cdot \begin{pmatrix} [b_i]_B \end{pmatrix} &= \begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\zeta_m^{n-1}) \\ \vdots & & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\zeta_m^{n-1}) \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \\
&= \begin{pmatrix} \alpha_1\sigma_1(1) + \cdots + \alpha_n\sigma_1(\zeta_m^{n-1}) \\ \vdots \\ \alpha_1\sigma_n(1) + \cdots + \alpha_n\sigma_n(\zeta_m^{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} \sigma_1(\alpha_1 \cdot 1 + \cdots + \alpha_n \cdot \zeta_m^{n-1}) \\ \vdots \\ \sigma_n(\alpha_1 \cdot 1 + \cdots + \alpha_n \cdot \zeta_m^{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} \sigma_1(b_i) \\ \vdots \\ \sigma_n(b_i) \end{pmatrix}.
\end{aligned}$$

This relation will hold for all $i \in \{1, \dots, \ell\}$, so the claim that $[\sigma(O_{K_m})]_B \cdot [c(J)]_B = [\sigma(J)]_B$ has been shown. Claim (6) may be shown similarly by using the powerful basis $B\prime = \{\zeta_m^{k_0}, \dots, \zeta_m^{k_{n-1}}\}$ and showing $[\sigma(O_K)]_{B\prime} \cdot [c(J)]_{B\prime} = [\sigma(J)]_{B\prime}$. Since $[I]_{B\prime}^{B} = ([I]_{B}^{B\prime})^{-1}$, only (3) must be shown to prove both (3) and (4). To prove (3) we will use (5) and take $J = O_{K_m}$ and the specified $\mathbb{Z}$-basis for J to be the powerful basis of O_{K_m}. Note that in this case we have $[c(J)]_B = [I]_{B\prime}^{B}$ because the ith column of $[c(J)]_B$ is given by $[\zeta_m^{k_i}]_B$, which is also defined to be the ith column of $[I]_{B\prime}^{B}$. Furthermore, the ith column of $[\sigma(J)]_B$ is given by $\sigma(\zeta_m^{k_i})$, which coincides with how $[\sigma(O_{K_m})]_{B\prime}$ was constructed. Thus, by substituting into (5), we have

$$[\sigma(O_{K_m})]_B \cdot [I]_{B\prime}^{B} = [\sigma(O_{K_m})]_{B\prime}$$

as required to prove (3). Since (3) ⇒ (4) this concludes the proof of Theorem 3.1.1.

□

Denote the matrix of the transformation that relates the canonical and coefficient embeddings of an ideal in $O_{K_m} \cong \mathbb{Z}[\zeta_m]$, relative to integral basis B of O_{K_m}, by $[T_m]_B$.

Corollary 3.1.2. *If $J \lhd O_{K_m}$ is a proper ideal, then $[\sigma(J)]_B = [\sigma(J)]_{B\prime}$.*

Proof.
If $J = O_{K_m}$ and $\varphi(m) = n$, then either $[c(J)]_B$ or $[c(J)]_{B\prime}$ will be the $n \times n$ identity matrix depending on if the power or powerful basis is used, respectively. Without loss of generality, if $[c(J)]_B = I_n$ is the $n \times n$ identity matrix, then $[c(J)]_B = [I]_{B\prime}^{B} \cdot [c(J)]_{B\prime} = I_n$. However, if J is a proper ideal, then neither $[c(J)]_B$ nor $[c(J)]_{B\prime}$ will be the identity matrix. Using Theorem 3.1.1 one may show

$$\begin{aligned} &[T_m]_B \cdot [c(J)]_B = [T_m]_B \cdot [I]_{B\prime}^{B} \cdot [c(J)]_{B\prime} = [\sigma(J)]_B \text{ by (5) in Theorem 3.1.1; and} \\ &[T_m]_B [c(J)]_B = [T_m]_{B\prime} \cdot [c(J)]_{B\prime} \text{ by (3) in Theorem 3.1.1} \\ &\Rightarrow [\sigma(J)]_B = [\sigma(J)]_{B\prime} \end{aligned}$$

□

In general, any additive homomorphism from the ring of algebraic integers to $\mathbb{R}^n$ (or $\mathbb{C}^n$) will give a geometric embedding of an ideal defined entirely by its action on a basis of the ring. Any two such embeddings of the same ideal will be related by some fixed linear transformation, so we can partially understand any embedding through by examining the transformation that relates it to another [91]. The following example is a continuation of Examples 2.4.1 and 2.4.2. It shows how the coefficient and canonical embeddings of the ideal $(3+2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$ are related, and demonstrates the action of $[T_6]_B$ on the basis $\{(3+2\zeta_6), (-2+5\zeta_6)\}$ of this ideal.

Example 3.1.3. *The Relationship Between the Canonical and Coefficient Embeddings of the Ideal* $(3+2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$*.*

As in Examples 2.4.1 and 2.4.2, we will use the power basis $B_6 = \{1, \zeta_6\}$ *for the ring* $\mathbb{Z}[\zeta_6]$*. In Example 2.4.1 it was shown that an integral basis for the principal ideal lattice* $\sigma(I) \subset \mathbb{R}^2$ *is given by*

$$\left\{ b_1 = \begin{pmatrix} \frac{8}{\sqrt{2}} \\ \frac{-2\sqrt{3}}{\sqrt{2}} \end{pmatrix}, b_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-5\sqrt{3}}{\sqrt{2}} \end{pmatrix} \right\}.$$

The ideal lattice $\sigma(I)$ *may be represented by the matrix* $[\sigma(I)]_B = \begin{pmatrix} b_1 & b_2 \end{pmatrix}$ *having vectors* b_1 *and* b_2 *as columns. Figure 3.1 displays the basis vectors* b_1 *and* b_2 *in the plot of the ideal lattice* $\sigma(I)$*.*

Recall from Example 2.4.2 that $\{v_1, v_2\}$ *is an integral basis for the principal ideal lattice* $c(I)$*, where*

$$v_1 = \begin{pmatrix} 3 \\ 2 \end{pmatrix} \text{ and } v_2 = \begin{pmatrix} -2 \\ 5 \end{pmatrix}.$$

This principal ideal lattice $c(I)$ *may be represented by the matrix* $[c(I)]_B = \begin{pmatrix} v_1 & v_2 \end{pmatrix}$ *having vectors* v_1 *and* v_2 *as columns. Figure 3.2 displays the basis vectors* v_1 *and* v_2

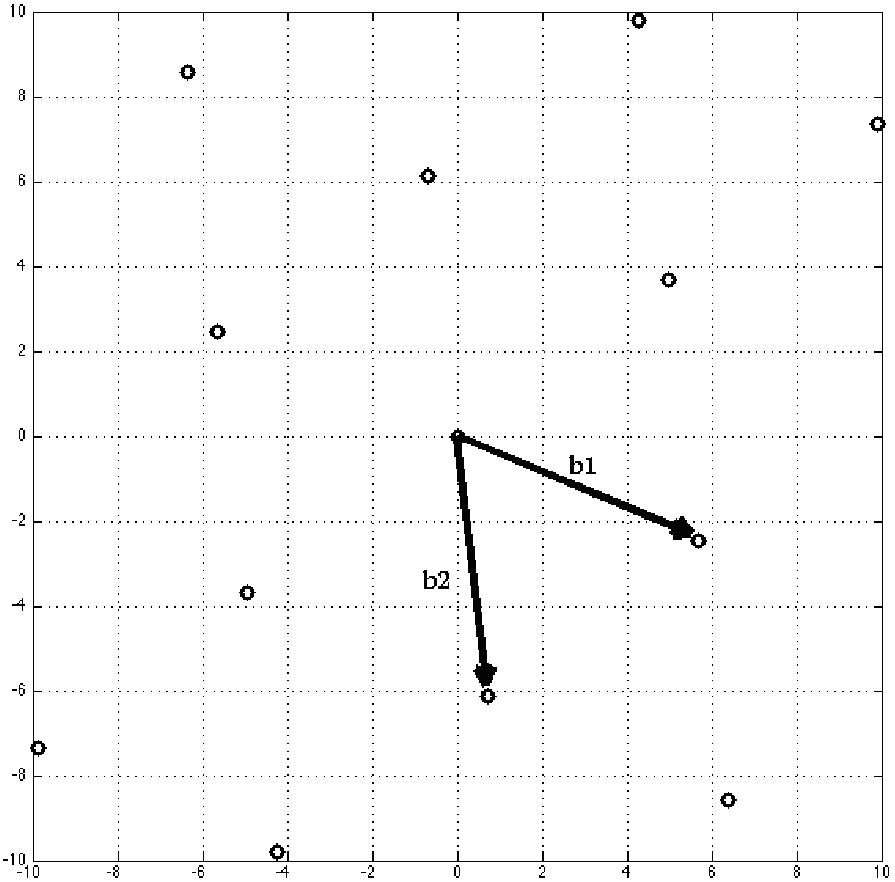

Figure 3.1: A Basis for the Canonical Embedding of $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$

in the plot of the ideal lattice $c(I)$. Theorem 3.1.1 states that the matrix $[T_6]_B = A \cdot \begin{pmatrix} \sigma(1) & \sigma(\zeta_6) \end{pmatrix}$ *will relate these two embeddings of* $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$*. The matrix* $[T_6]_B$ *is*

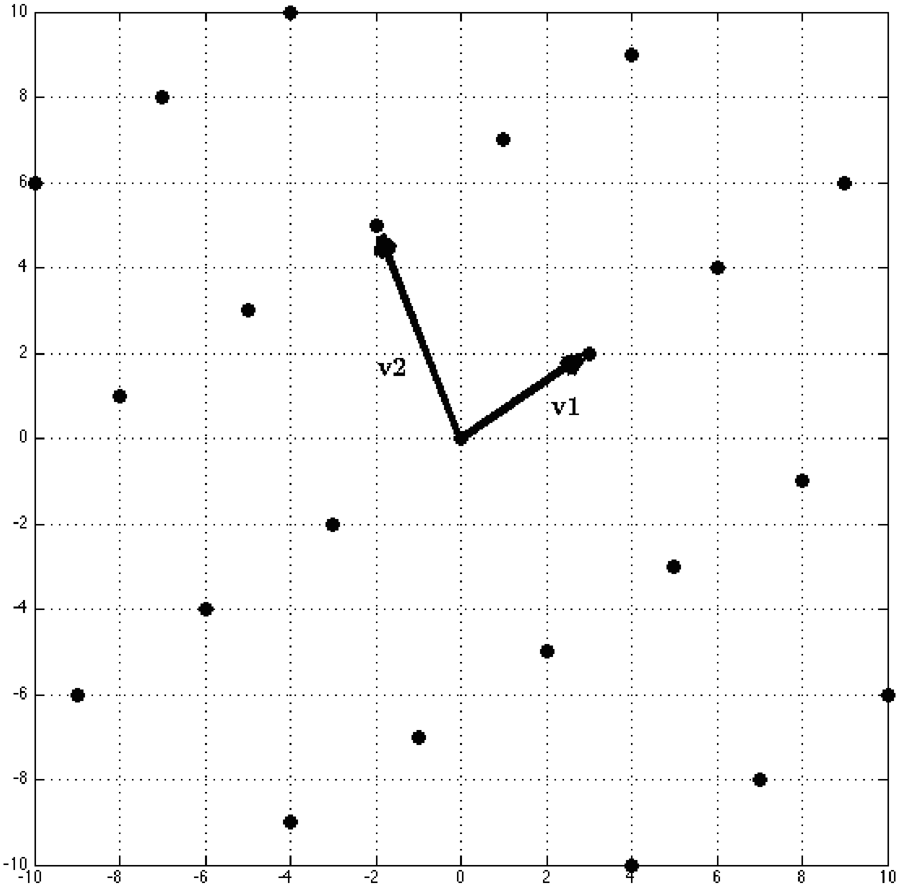

Figure 3.2: A Basis for the Coefficient Embedding of $(3 + 2\zeta_6) \lhd \mathbb{Z}[\zeta_6]$

given by

$$
\begin{aligned}
[T_6]_B &= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_6) \\ \sigma_2(1) & \sigma_2(\zeta_6) \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta_6 \\ 1 & \overline{\zeta_6} \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1+\sqrt{-3}}{2} \\ 1 & \frac{1-\sqrt{-3}}{2} \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 2 & 1 \\ 0 & -\sqrt{3} \end{pmatrix}.
\end{aligned}
$$

One may easily verify that $[T_6]_B \cdot [c(I)]_B = [\sigma(I)]_B$. In the process of verifying this relation, observe that the vector $v_1 \in c(I)$ maps to the vector $b_1 \in \sigma(I)$ under $[T_6]_B$. Also, the vector $v_2 \in c(I)$ maps to the vector $b_2 \in \sigma(I)$. The corresponding vectors $v_1 \in c(I)$ and $b_1 \in \sigma(I)$ are depicted in Figure 3.3, where the principal ideal lattices $c(I)$ and $\sigma(I)$ have been plotted together. The solid arrow corresponds to $v_1 \in c(I)$, and the dashed arrow corresponds to $b_1 \in \sigma(I)$.

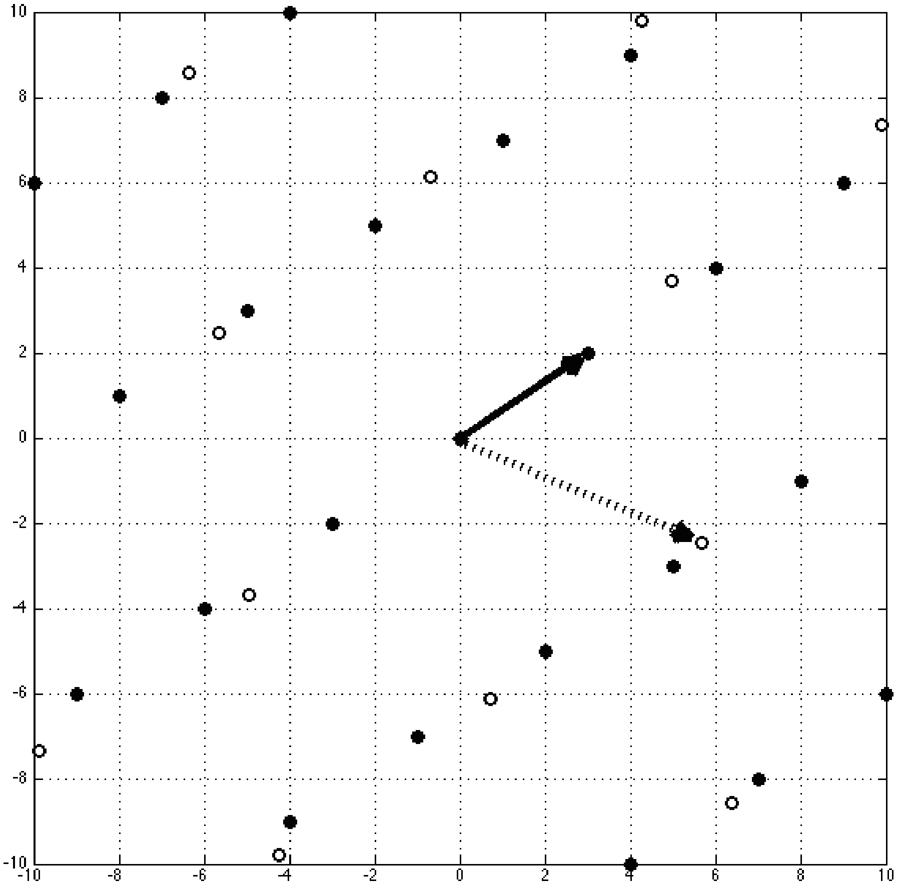

Figure 3.3: Corresponding Vectors in Two Embeddings of $(3 + 2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$

3.1.1 Singular Values of this Transformation

For an integer m, recall that $\hat{m} = m/2$ if m is divisible by 2, and $\hat{m} = m$ otherwise. Also, $rad(m)$ is defined as the product of all prime numbers that divide m. The following Lemma may be found, along with its proof, in [69].

Lemma 3.1.4 ([69], Lemma 4.3). *The largest singular value of $\sigma(B\prime) \subset H$ is $s_1(B\prime) = \sqrt{\hat{m}}$, and the smallest singular value is $s_n(B\prime) = \sqrt{m/rad(m)}$.*

The matrix $\sigma(B\prime)$ is the matrix of the canonical embedding of the ring of cyclotomic integers O_{K_m} in $\mathbb{C}^{\varphi(m)}$ relative to the powerful basis. We would like to translate these results to the matrix $[T_m]_{B\prime} = [\sigma(O_{K_m})]_{B\prime}$, which relates the canonical and coefficient embeddings in $\mathbb{R}^{\varphi(m)}$. The following proposition will imply that $[T_m]_{B\prime}$ has the same singular values as the matrix $\sigma(B\prime)$ from Lemma 3.1.4.

Proposition 3.1.5. *Two matrices $M, N \in \mathbb{C}^{m\times n}$ have the same singular values if and only if there exist unitary matrices $P \in \mathbb{C}^{m\times m}$ and $Q \in \mathbb{C}^{n\times n}$ such that $M = PNQ$.*

Proof.
Without loss of generality, suppose that $n \leq m$. This means that $M, N \in \mathbb{C}^{m\times n}$ will have n singular values.
($\Rightarrow$) Suppose that M, N have the same singular values. Define the matrix

$$\Sigma = \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_n \end{pmatrix}$$

to be the $n \times n$ diagonal matrix with the singular values $s_1 \geq \cdots \geq s_n$ on its diagonal.

Let M and N have singular value decompositions (SVD) given by

$$M = U_M \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot V_M$$

$$N = U_N \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot V_N$$

where $U_M, U_N \in \mathbb{C}^{m \times m}$ and $V_M, V_N \in \mathbb{C}^{n \times n}$ are all unitary, and the matrix $\left(\begin{smallmatrix} \Sigma \\ 0 \end{smallmatrix}\right)$ is $m \times n$. Let $P = (U_M \cdot U_N^*)$ and $Q = (V_N^* \cdot V_M)$. Note that both P and Q are unitary. Denote the $m \times m$ identity matrix by I_m and the $n \times n$ identity matrix by I_n. Then

$$\begin{aligned} M = U_M \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot V_M &= U_M \cdot I_m \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot I_n \cdot V_M \\ &= U_M \cdot (U_N^* \cdot U_N) \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot (V_N \cdot V_N^*) \cdot V_M \\ &= (U_M \cdot U_N^*) \cdot U_N \cdot \begin{pmatrix} \Sigma \\ \\ 0 \end{pmatrix} \cdot V_N \cdot (V_N^* \cdot V_M) \\ &= PNQ. \end{aligned}$$

($\Leftarrow$) Suppose that there exist unitary matrices $P \in \mathbb{C}^{m \times m}$ and $Q \in \mathbb{C}^{n \times n}$ such that

$M = PNQ$. Define the diagonal matrices

$$\Sigma_M = \begin{pmatrix} s_1(M) & & \\ & \ddots & \\ & & s_n(M) \end{pmatrix}$$
$$\Sigma_N = \begin{pmatrix} s_1(N) & & \\ & \ddots & \\ & & s_n(N) \end{pmatrix}$$

where the diagonal entries of Σ_M and Σ_N are the singular values of M and N, respectively. Let M, N have SVDs given by

$$M = U_M \begin{pmatrix} \Sigma_M \\ 0 \end{pmatrix} V_M$$

$$N = U_N \begin{pmatrix} \Sigma_N \\ 0 \end{pmatrix} V_N$$

where $U_M, U_N \in \mathbb{C}^{m \times m}$ and $V_M, V_N \in \mathbb{C}^{n \times n}$ are all unitary, and both $\left(\begin{smallmatrix} \Sigma_M \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \Sigma_N \\ 0 \end{smallmatrix}\right)$

are $m \times n$. Then, because $M = PNQ$,

$$\begin{aligned} U_M \cdot \begin{pmatrix} \Sigma_M \\ 0 \end{pmatrix} \cdot V_M &= P \cdot U_N \cdot \begin{pmatrix} \Sigma_N \\ 0 \end{pmatrix} \cdot V_N \cdot Q \\ \Rightarrow \begin{pmatrix} \Sigma_M \\ 0 \end{pmatrix} &= U_M^* \cdot P \cdot U_N \cdot \begin{pmatrix} \Sigma_N \\ 0 \end{pmatrix} \cdot V_N \cdot Q \cdot V_M^* \end{aligned}$$

Define the matrices $G = (U_M^* \cdot P \cdot U_N)$ and $H = (V_N \cdot Q \cdot V_M^*)$, which are both unitary. Then

$$\begin{aligned} \begin{pmatrix} \Sigma_M \\ 0 \end{pmatrix} \cdot \begin{pmatrix} \Sigma_M & 0 \end{pmatrix} &= (G \cdot \begin{pmatrix} \Sigma_N \\ 0 \end{pmatrix} \cdot H) \cdot (H^* \cdot \begin{pmatrix} \Sigma_N & 0 \end{pmatrix} \cdot G^*) \\ \Rightarrow \begin{pmatrix} \Sigma_M^2 \end{pmatrix} &= G \cdot \begin{pmatrix} \Sigma_N^2 \end{pmatrix} \cdot G^* \end{aligned}$$

when multiplying both sides by the transpose. Note that this factorization is an SVD of $\left(\Sigma_M^2 \right)$ because G is a unitary matrix. Since the singular values of a matrix are unique, and because $\left(\Sigma_M^2 \right)$ is a non-negative diagonal matrix, its diagonal entries are equal to the diagonal entries of $\left(\Sigma_N^2 \right)$, which is another non-negative diagonal matrix. Hence $\Sigma^2 = \Sigma_M^2 = \Sigma_N^2$ is a positive diagonal matrices with the ith diagonal entry given by $\Sigma_{i,i} = s_i(M)^2 = s_i(N)^2$, where $s_i(M)$ and $s_i(N)$ are the ith singular values of M and N respectively. Since all singular values by definition are non-negative, it follows that $s_i(M) = s_i(N)$ for all $i = 1, \dots, n$. Thus M and N have the same singular values as required.

$\square$

Observe that $[T_m]_{B\prime} = [\sigma(O_{K_m})]_{B\prime}] = A \cdot \sigma(B\prime) \cdot I_n$ where A is the unitary basis matrix used to map ideal lattices in $\mathbb{C}^n$ to ideal lattices in $\mathbb{R}^n$, and I_n is the $n \times n$ identity matrix. Both A and I_n are unitary matrices, so the result in Lemma 3.1.4 may be applied to provide the singular values of $[T_m]_{B\prime}$.

Theorem 3.1.6. *The largest and smallest singular values of the matrix $[T_m]_{B\prime}$ are given by $s_1([T_m]_{B\prime}) = \sqrt{\hat{m}}$ and $s_n([T_m]_{B\prime}) = \sqrt{m/rad(m)}$, respectively.*

This theorem defines the singular values of the matrix that relates the canonical and coefficient embeddings relative to the powerful basis $B\prime$, not the power basis B. The matrices $[T_m]_{B\prime}$ and $[T_m]_B$ are not equal unless m is a prime-power. Consequently, they do not necessarily have the same singular values.

3.2 On the Equivalence of the SVP in Ideal Lattices Under Two Embeddings

We now use the singular values of the matrix $[T_m]_{B\prime}$ to study the equivalence of the SVP under the canonical and coefficient embeddings of an ideal. Some results will be extended to any two geometric embeddings of an ideal in O_{K_m}. This section relies heavily on the work presented in section 3.1.1, meaning that most results will be centered around the powerful basis. First, a basic result is given to show how the length of a matrix-vector product can be bounded using the singular values of the matrix and the length of the vector. Given a matrix $T \in \mathbb{C}^{n \times n}$ we use $s_1(T)$ and $s_n(T)$ to denote the largest and smallest singular values of T, respectively.

Lemma 3.2.1. *For any matrix $T \in \mathbb{C}^{n\times n}$ and $x \in \mathbb{C}^n$,*

$$s_n(T) \cdot \|x\|_2 \leq \|Tx\|_2 \leq s_1(T) \cdot \|x\|_2.$$

Proof.

First, suppose that $x \in \mathbb{C}^n$ is the zero vector. Then clearly

$$s_n(T) \cdot \|x\|_2 \leq \|Tx\|_2 \leq s_1(T) \cdot \|x\|_2 \Rightarrow s_n(T) \cdot 0 \leq 0 \leq s_1(T) \cdot 0$$

and the bounds hold. If $x \neq 0$, then the following is true.

$$s_n(T) = \min_{z\neq 0} \frac{\|Tz\|_2}{\|z\|_2} \leq \frac{\|Tx\|_2}{\|x\|_2} \leq \max_{z\neq 0} \frac{\|Tz\|_2}{\|z\|_2} = s_1(T)$$
$$\Rightarrow s_n(T) \cdot \|x\|_2 \leq \|Tx\|_2 \leq s_1(T) \cdot \|x\|_2$$

□

Note that $s_n([T_m]_{B'}) = \sqrt{m/rad(m)} \geq 1$, meaning that the matrix $[T_m]_{B'}$ cannot shrink any vectors that it maps from the coefficient embedding to the canonical embedding. This hints at an explanation of why lattice points in $\sigma(I)$ are generally more sparse than in $c(I)$ for an ideal $I \lhd O_{K_m}$, which was observed through Examples 2.4.1 and 2.4.2. Let $\kappa_2([T_m]_{B'})$ denote the 2-norm condition number of the matrix $[T_m]_{B'}$, defined as the ratio of its largest singular value to its smallest singular value. Since the largest and smallest singular values of a matrix give insight as to how much a matrix can stretch or shrink a vector, respectively, the 2-norm condition number serves as a "distortion" factor of $[T_m]_{B'}$. For certain cyclotomic indices m the matrix $[T_m]_{B'}$ behaves nicely.

Proposition 3.2.2. $\kappa_2([T_m]_{B'}) = 1$ *if and only if* $m = 2^k$ *for some integer* $k \geq 0$.

Proof.

Observe that $\kappa_2([T_m]_{B\prime}) = \sqrt{\hat{m} \cdot rad(m)/m} = \sqrt{\hat{m} \cdot rad(m)/m} = 1 \Leftrightarrow \hat{m} \cdot rad(m)/m = 1$. Suppose that m is not divisible by 2. Then $\hat{m} \cdot rad(m)/m = rad(m) = 1 \Leftrightarrow m = 1$. Now suppose that m is divisible by 2. Then $\hat{m} \cdot rad(m)/m = m \cdot rad(m)/2m = rad(m)/2 = 1 \Leftrightarrow rad(m) = 2 \Leftrightarrow m = 2^k$ for some $k \in \mathbb{Z}_{\geq 0}$. Hence $\kappa_2([T_m]_{B\prime}) = 1 \Leftrightarrow m = 1$ or $m = 2^k$ for some $k \in \mathbb{Z}_{\geq 1}$.

□

Corollary 3.2.3. *If $m = 2^k$ for some positive integer k and $I \lhd O_{K_m}$ is an ideal in the ring of cyclotomic integers, then the SVP in $\sigma(I)$ is equivalent to the SVP in $c(I)$.*

Proof.

By Proposition 3.2.2 it's clear that $s_1([T_m]_B) = s_n([T_m]_B)$ because $\kappa_2([T_m]_B) = 1$. Apply Lemma 3.2.1 to see that the matrix $[T_m]_B$ will stretch all lattice vectors equally. Since the matrix of the transformation that relates these two embeddings of an ideal stretches each vector equally, it's clear that a solution to the SVP in one embedding will map to a solution of the SVP in the other embedding under $[T_m]_B$.

□

Note that the power and powerful bases are the same in the case $m = 2^k$ because the cyclotomic index is a prime-power. While the matrix $[T_m]_B$ for $m = 2^k$ will stretch all vectors by the same factor, it is not an isometry since the length of a vector is not preserved. In fact, $[T_m]_B$ will map each vector in $c(I)$ to a vector in $\sigma(I)$ whose length is $s_1([T_{2^k}]_B) = s_n([T_{2^k}]_B) = \sqrt{\hat{m}} = 2^{k-1}$ times greater. The only cyclotomic indices for which it is possible that the matrix $[T_m]_{B\prime}$ will not stretch a vector are characterized in the following lemma.

Lemma 3.2.4. *The smallest singular value $s_n([T_m]_{B'})$ of the matrix $[T_m]_{B'}$ is equal to 1 if and only if the cyclotomic index $m = \prod_i^\ell p_i$ is the product of distinct primes.*

Proof.

$s_n([T_m]_{B'}) = \sqrt{m/rad(m)} = 1 \Leftrightarrow m = rad(m) \Leftrightarrow m = \prod_i^\ell p_i$ is the product of distinct primes.

□

All 2-norm condition numbers of $[T_m]_{B'}$ will be of the form $\kappa_2([T_m]_{B'}) = \sqrt{r} \geq 1$ for some odd positive integer $r \geq 1$. This number is minimal when m is a power-of-two, but the second smallest 2-norm condition number is $\kappa([T_m]_{B'}) = \sqrt{3}$, which occurs if and only if $m = 2^k \cdot 3^\ell$ for integers $k \geq 0$ and $\ell \geq 1$, according to the following proposition.

Proposition 3.2.5. $\kappa_2([T_m]_{B'}) = \sqrt{p}$ *for some prime p if and only if $m = 2^k \cdot p^\ell$ for some integers $k \geq 0$ and $\ell \geq 1$.*

Proof.

Either the cyclotomic index m is divisible by 2 or not, so first suppose that m is not divisible by 2. Then

$$\kappa_2([T_m]_{B'}) = \sqrt{\frac{\hat{m} \cdot rad(m)}{m}} = \sqrt{\frac{m \cdot rad(m)}{m}} = \sqrt{rad(m)} = \sqrt{p} \Leftrightarrow rad(m) = p$$

which happens $\Leftrightarrow m = p^\ell = 2^0 \cdot p^\ell$, for some $\ell \in \mathbb{Z}_{\geq 1}$ by definition of $rad(m)$. If m is divisible by 2, then

$$\kappa_2([T_m]_{B'}) = \sqrt{\frac{\hat{m} \cdot rad(m)}{m}} = \sqrt{\frac{m \cdot rad(m)}{2m}} = \sqrt{\frac{rad(m)}{2}} = \sqrt{p} \Leftrightarrow rad(m) = 2p.$$

This happens if and only if $m = 2^k \cdot p^\ell$, for some integers $k \geq 1$ and $\ell \geq 1$ by the definition of $rad(m)$. □

The following theorem provides a condition under which the SVP is equivalent in two geometric embeddings of an ideal. This condition characterizes the circumstances under which a shortest vector in one embedding will map to a shortest vector in another embedding.

Theorem 3.2.6. *Let $I \lhd O_K$ be a non-zero ideal in the ring of algebraic integers with integral basis B_0. For any two geometric embeddings γ, δ of I denote by T the matrix of the transformation that relates these embeddings, i.e. $[T]_{B_0} \cdot [\gamma(I)]_{B_0} = [\delta(I)]_{B_0}$. If $v \in \gamma(I)$ is a shortest vector and $\kappa_2(T) \cdot \|v\|_2 \leq \|w\|_2$ for all $0 \neq w \in \gamma(I)$ with $\|w\|_2 > \|v\|_2$, then T will map at least one shortest vector of $\gamma(I)$ to a shortest vector of $\delta(I)$.*

Proof.
Let $s_n = s_n(T)$ and $s_1 = s_1(T)$ be the smallest and largest singular values of the matrix T that relates the two embeddings, respectively. By Lemma 3.2.1,

$$s_n \cdot \|x\|_2 \leq \|T \cdot x\|_2 \leq s_1 \cdot \|x\|_2 \text{ for any } x \in \gamma(I).$$

Let $v \in \gamma(I)$ be a shortest vector. Using the definition of singular values, if $\|Tv\|_2 \leq s_1 \cdot \|v\|_2 \leq s_n \cdot \|w\|_2 \leq \|Tw\|_2$ for all $0 \neq w \in \gamma(I)$ with $\|w\|_2 > \|v\|_2$, then $Tv = \min \|Tz\|_2 \in \delta(I)$ is a shortest vector where the minimum is taken over all shortest vectors $z \in \gamma(I)$. Hence there is at least one shortest vector of $\gamma(I)$ that will map to a shortest vector of $\delta(I)$ under T. This relation is equivalent to $\frac{s_1}{s_n} \cdot \|v\|_2 \leq \|w\|_2$ for all $0 \neq w \in \gamma(I)$ with $\|w\|_2 > \|v\|_2$. Thus, some shortest vector of $\gamma(I)$ will map to a shortest vector in $\delta(I)$ if $\kappa_2(T) \cdot \|v\|_2 \leq \|w\|_2$.

□

Corollary 3.2.7. *Let T be the matrix of the transformation that relates two geometric embeddings γ and δ. If $\kappa_2(T) = 1$, then the SVP is equivalent in the two embeddings.*

Proof.

Clearly the condition in Theorem 3.2.6 will always hold if $\kappa_2(T) = 1$.

□

Theorem 3.2.6 applies to an ideal in the ring of algebraic integers of any number field, not just cyclotomic fields. This theorem provides a condition for which solving the SVP in one embedding of an ideal will lead to a solution of the SVP in another embedding of the ideal. Even if this condition holds for one solution to the SVP, it is possible that not every solution of the SVP in one embedding would correspond to a solution of the SVP in the other. For instance, one shortest vector may change in length by a factor of $s_n(T)$ while another changes in length by a factor of $s_1(T)$. This theorem only guarantees that there is at least one shortest vector in the first embedding that maps to a shortest vector in the second embedding if the conditions are met. Smaller $\kappa_2(T)$ values imply a smaller difference between how far shortest vectors could stretch, or shrink, as they are being mapped from one embedding to another by the matrix T. If T stretches all shortest vectors in one embedding equally, then every solution to the SVP in that embedding will map to a shortest vector in the second embedding.

In particular, Theorem 3.2.6 may be applied to the canonical and coefficient embeddings. One may also see how Corollary 3.2.7 may be used to imply Corollary 3.2.3. It is also of interest to know if either the canonical or coefficient embedding of an ideal will have more independent shortest vectors than the other. Perhaps more shortest vectors in a particular embedding of an ideal suggests that the SVP is easier to solve in that embedding than in a different embedding with fewer shortest vectors.

To answer the question about the number of independent shortest vectors, first consider another geometric embedding $\tau : K \to \mathbb{R}^n$ where K is a number field of signature $n = r_1 + 2r_2$. That is, K has r_1 real embeddings $\rho_1, \dots, \rho_{r_1}$ and $2r_2$ complex embeddings $\sigma_1, \dots, \sigma_{r_2}, \overline{\sigma_1}, \dots, \overline{\sigma_{r_2}}$. Define the geometric embedding $\tau : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ as

$$\tau = (\rho_1, \dots, \rho_{r_1}, \mathcal{R}(\sigma_1), \mathcal{I}(\sigma_1), \dots, \mathcal{R}(\sigma_{r_2}), \mathcal{I}(\sigma_{r_2}))$$

where $\mathcal{R}(\sigma_i)$ and $\mathcal{I}(\sigma_i)$ are the real and imaginary parts of σ_i, respectively. Consider how τ is related to the canonical embedding σ. In general, a number field K will have r_1 real embeddings $\rho_1, \dots, \rho_{r_1}$ and $2r_2$ complex embeddings $\sigma_1, \dots, \sigma_{r_2}, \overline{\sigma_1}, \dots, \overline{\sigma_{r_2}}$. We may define the canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ as $\sigma = (\rho_1, \dots, \rho_{r_1}, \sigma_1, \dots, \sigma_{r_2}, \overline{\sigma_{r_2}}, \dots, \overline{\sigma_1})$. However, if K is a cyclotomic field, note that both τ and σ are defined entirely by complex embeddings, which equates to the definition of the canonical embedding given in the second chapter.

Let $K_m = \mathbb{Q}(\zeta_m)$ be the mth cyclotomic number field with $\varphi(m) = n$. Define the $n \times n$ matrix W as

$$W = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & -1 \\ \vdots & \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 0 & 1 & -1 & \dots & 0 & 0 \\ 1 & -1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

where the ith row of W is given by

$$W_i = \begin{cases} \begin{pmatrix} 0 & 0 & \dots & 1_{2i-1} & 1_{2i} & \dots & 0 & 0 \end{pmatrix} \text{ if } i \leq \frac{n}{2} \\ \begin{pmatrix} 0 & 0 & \dots & 1_{2(n-i)+1} & -1_{2(n-i)+2} & \dots & 0 & 0 \end{pmatrix} \text{ if } i > \frac{n}{2} \end{cases}$$

and the index denotes the column position of the 1 (or -1).

Lemma 3.2.8. *For an ideal $I \triangleleft O_{K_m}$, the embeddings $\tau(I)$ and $\sigma(I)$ are related by the transformation represented by W.*

Proof.

Let I be an ideal of O_K with basis $B = \{b_1, \dots, b_n\}$. Define a matrix $R = [\tau(I)]_B$ where the jth column is $\tau(b_j)$ given by

$$R_j = \begin{pmatrix} \mathcal{R}(\sigma_1(b_j)) \\ \mathcal{I}(\sigma_1(b_j)) \\ \vdots \\ \mathcal{R}(\sigma_{r_2}(b_j)) \\ \mathcal{I}(\sigma_{r_2}(b_j))) \end{pmatrix}$$

Define a matrix $S = [\sigma(I)]_B$ with ij-entry equal to

$$S_{ij} = \begin{cases} \sigma_i(b_j), i \leq \frac{n}{2} \\ \overline{\sigma_{n-i+1}(b_j)}, i > n/2 \text{ (complex conjugate)} \end{cases} .$$

One may easily show that the product of the ith row of T and jth column of R equal the ij-entry of S, which proves the claim. □

Lemma 3.2.9. *If $\|\tau(a)\|_2^2 = r$, then $\|\sigma(a)\|_2^2 = 2r$ for all $a \in K_m$.*

Proof.

Suppose that $\|\tau(a)\|_2^2 = |\mathcal{R}(\sigma_1(a))|^2 + |\mathcal{I}(\sigma_1(a))|^2 + \cdots + |\mathcal{R}(\sigma_{r_2}(a))|^2 + |\mathcal{I}(\sigma_{r_2}(a))|^2 = r$. Then

$$\begin{aligned}\|\sigma(a)\|_2^2 &= |\sigma_1(a)|^2 + \cdots + |\sigma_{r_2}(a)|^2 + |\overline{\sigma_{r_2}(a)}|^2 + \cdots + |\overline{\sigma_1(a)}|^2 \\ &= 2[|\mathcal{R}(\sigma_1(a))|^2 + |\mathcal{I}(\sigma_1(a))|^2 + \cdots + |\mathcal{R}(\sigma_{r_2}(a))|^2 + |\mathcal{I}(\sigma_{r_2}(a))|^2] \\ &= 2r\end{aligned}$$

□

Lemma 3.2.10. *Let $A \in \mathbb{C}^{n\times n}$. All singular values of A are the same if and only if A is a multiple of a unitary matrix.*

Proof.

Let A have SVD given by $A = U \cdot \Sigma \cdot V^*$ where $U, V^* \in \mathbb{C}^{n\times n}$ are unitary and Σ is $n \times n$ diagonal matrix with the same singular values of A on its diagonal.

$$\Sigma = \begin{pmatrix} s & 0 & \dots & 0 \\ 0 & s & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & s \end{pmatrix}$$

Let I_n be the $n \times n$ identity matrix. Then $A = U\Sigma V^* \Leftrightarrow AA^* = U\Sigma^2U^* = s^2 \cdot UI_nU^* = s^2 \cdot I_n$ and $A^*A = V\Sigma^2V^* = s^2 \cdot VI_nV^* = s^2 \cdot I_n \Leftrightarrow AA^* = A^*A = s^2 \cdot I_n$ and the claim is proved.

□

Proposition 3.2.11. *W is a multiple of a unitary matrix.*

Proof.

By Lemma 3.2.10, all singular values of W are the same if and only if W is a multiple of a unitary matrix. Singular values of a matrix satisfy $s_1 \geq \cdots \geq s_n \geq 0$, so one must only check the extreme singular values s_1 and s_n. Apply Lemma 3.2.9 to show

$$s_n(W) = \min_{\|x\|_2=1} \|Wx\|_2 = \min_{\|x\|_2=1} \sqrt{2} \cdot \|x\|_2 = \sqrt{2}; \text{ and}$$
$$s_1(W) = \max_{\|x\|_2=1} \|Wx\|_2 = \max_{\|x\|_2=1} \sqrt{2} \cdot \|x\|_2 = \sqrt{2}.$$

□

Proposition 3.2.12. *Let $I \lhd O_{K_m}$ be an ideal in the ring of cyclotomic integers. The geometric embeddings $\tau(I)$ and $\sigma(I)$ are isomorphic.*

Proof.

Let $a \in I$. The isomorphism between these embeddings is seen by the mapping

$$\tau(a) = \begin{pmatrix} \mathcal{R}(\sigma_1(a)) \\ \mathcal{I}(\sigma_1(a)) \\ \vdots \\ \mathcal{R}(\sigma_{r_2}(a)) \\ \mathcal{I}(\sigma_{r_2}(a))) \end{pmatrix} \leftrightarrow \begin{pmatrix} \mathcal{R}(\sigma_1(a)) + \mathcal{I}(\sigma_1(a)) \\ \mathcal{R}(\sigma_2(a)) + \mathcal{I}(\sigma_2(a)) \\ \vdots \\ \mathcal{R}(\sigma_{r_2}(a)) + \mathcal{I}(\sigma_{r_2}(a)) \\ \mathcal{R}(\sigma_{r_2}(a)) - \mathcal{I}(\sigma_{r_2}(a)) \\ \vdots \\ \mathcal{R}(\sigma_2(a)) - \mathcal{I}(\sigma_2(a)) \\ \mathcal{R}(\sigma_1(a)) - \mathcal{I}(\sigma_1(a)) \end{pmatrix} = \sigma(a).$$

□

Corollary 3.2.13. *Let $I \lhd O_{K_m}$ be an ideal in the ring of cyclotomic integers. Then the SVP in $\tau(I)$ is equivalent to the SVP in $\sigma(I)$.*

Proof.

By Proposition 3.2.12, the two embeddings are isomorphic. To see the equivalence of SVP, note that W is a multiple of a unitary matrix $\Rightarrow \kappa_2(W) = 1$. Now apply Corollary 3.2.7.

□

Now that the equivalence of the embedding τ and the canonical embedding σ has been shown, a result pertaining to the number of independent shortest vectors in an ideal lattice $\tau(I)$ from [37] will be amended to reflect this relationship. A relation between the number of independent shortest vectors in the canonical embedding of an ideal $\sigma(I)$ and the coefficient embedding of an ideal $c(I)$ will follow.

Theorem 3.2.14. *Let $I \lhd O_K$ be a non-zero ideal in the ring of algebraic integers of some number field K of degree ≥ 2. Then $\sigma(I)$ is WR if and only if $\tau(I)$ is WR if and only if K is a cyclotomic number field.*

Proof.

By Theorem 1.2 of [37], $\tau(I)$ is WR if and only if K is a cyclotomic number field. The rest follows from Proposition 3.2.12.

□

Thus, for any ideal $I \lhd O_{K_m}$ where $\varphi(m) \geq 2$, the ideal lattices $\tau(I)$ and $\sigma(I)$ are well-rounded and have a basis consisting of shortest vectors. So, there will be exactly $\varphi(m)$ independent shortest vectors in both of these ideal lattices when the cyclotomic index m is strictly greater than 2.

Theorem 3.2.15. *Let $I \lhd O_{K_m}$ be an ideal in the ring of cyclotomic integers. Then the ideal lattice $c(I)$ will have no more independent shortest vectors than the ideal lattice $\sigma(I)$.*

Proof.

Let $I \lhd O_{K_m}$ be an integral ideal. If $m \leq 2$, then clearly a one-dimensional ideal lattice will only have one independent shortest vector, and the statement is true. Let $m > 2$. By Theorem 3.2.14, the ideal lattice $\sigma(I)$ will always have $\varphi(m) = n$ independent shortest vectors, and the ideal lattice $c(I)$ can never have more than n independent shortest vectors.

□

3.3 More on the Power and Powerful Bases

Sections 3.1 and 3.2 contain several results whose proofs make strong use of the powerful basis $B\prime$. To work with the notion of ideal lattices as ideals of a polynomial quotient ring, one might be more interested in considering the power basis B, which translates very naturally to the quotient ring perspective. Recall that the powerful basis is the power basis for prime-power cyclotomic indices $m = p^k$ by definition. Proposition 3.3.1 yields a corollary that provides more than just the prime-power cyclotomic indices for which the powerful basis may be viewed a power basis.

Proposition 3.3.1. *Let m be an odd integer. Then the powerful basis of K_m is the same as the powerful basis of K_{2m}.*

Proof.

First, note that since m is odd it has prime-power factorization given by $m = \prod_{i=1}^{\ell} m_i$

where each $m_i = p_i^{k_i}$ for some (odd) prime p_i and positive integer $k_i \geq 1$. By definition the powerful basis of K_m is is defined as $B\prime_m = \otimes_i B\prime_{m_i}$, the tensor product of the power(ful) bases of each K_{m_i}. Multiplying m by 2 yields the prime-power factorization $2m = 2 \cdot \prod_{i=1}^{\ell} m_i$. Since the power(ful) basis of K_2 is $B\prime_2 = \{1\}$, the powerful basis of K_{2m} will be given by the following.

$$\begin{aligned} B\prime_{2m} &= B\prime_2 \otimes B\prime_m = B\prime_2 \otimes B\prime_{m_1} \otimes B\prime_{m_2} \otimes \cdots \otimes B\prime_{m_\ell} \\ &= \{1\} \otimes B\prime_{m_1} \otimes B\prime_{m_2} \otimes \cdots \otimes B\prime_{m_\ell} \\ &= B\prime_{m_1} \otimes B\prime_{m_2} \otimes \cdots \otimes B\prime_{m_\ell} \\ &= B\prime_m \end{aligned}$$

□

This is a particularly nice property of the powerful basis. One implication of this result is that if $K_m = \mathbb{Q}(\zeta_m)$ and m is an odd integer, then $K_m = K_{2m} = \mathbb{Q}(\zeta_{2m})$. Rather than considering two different power bases for the same field generated by a different power of ζ_m, the powerful basis is constructed so that it is *the* powerful basis of this cyclotomic field extension. It is desirable to construct only one basis for each cyclotomic field, and the powerful basis, unlike the power basis, satisfies this condition.

Corollary 3.3.2. *Let $m = p^k$ for any prime p and some integer $k \geq 1$. Then the powerful basis of K_{2m} is a power basis.*

Proof.

If $m = 2^k$ is a power of two, then by definition the powerful basis of K_{2m} is the power basis $B\prime = B = \{1, \zeta_{2^{k+1}}, \zeta_{2^{k+1}}^2, \dots\}$. If $m = p^k$ is odd, then by Proposition 3.3.1 the power(ful) basis $B\prime = B$ of K_m is the powerful basis of K_{2m}. □

Instead of viewing the powerful basis as a power basis for only prime-power cyclotomic indices $m = p^k$, we are also now able to view the powerful basis for cyclotomic indices $2m = 2 \cdot p^k$ as a power basis. Since the power basis is what will be used to work with ideal lattices in a polynomial quotient ring setting, it is logical to address the density of cyclotomic indices for which the powerful basis may be viewed as a power basis.

For the range $[1, k]$ of cyclotomic indices, let $\mathit{count}(1, k)$ return the number of prime-power indices within the range. Let $\mathit{count}2(1, k)$ return the number of indices $i \in [1, k]$ for which either $i = p^k$ for a prime p or $i = 2 \cdot p^k$ for an odd prime p. Then $\mathit{count}(1, k)$ would reflect the number of cyclotomic indices in the range whose power basis is the powerful basis, and $\mathit{count}2(1, k)$ would reflect the total number of powerful bases in the range that may be viewed as a power basis. Table 3.1 shows these computed quantities for the specified ranges, as well as the computed proportion of indices within each range captured by $\mathit{count}(1, k)$ and $\mathit{count}2(1, k)$, respectively. The Maple$^{\text{TM}}$ code used in these calculations may be found in Appendix B.

For cyclotomic indices $m = 140$ and $m = 142$, exactly half of the cyclotomic fields with indices in the range $[1, m]$ have a powerful basis that may be viewed as a power basis. For $m > 142$, fewer than half of the indices in the range $[1, m]$ will have a powerful basis that one may view as a power basis. Lattices large enough for use in practice may be found in rings of cyclotomic integers with index $m \leq 142$; the largest dimension of a lattice arising from a cyclotomic field with index $m \leq 142$ is $\max_{i \in [1,142]} \varphi(i) = 138$.

Table 3.1: Density of Power Bases

Cyclotomic Index Range	count(1,k)	Percentage	count2(1,k)	Percentage
[1, 50]	24	48.0%	34	68.0%
[1, 100]	36	36.0%	54	54.0%
[1, 150]	49	32.7%	73	48.7%
[1, 200]	61	30.5%	90	45.0%
[1, 250]	69	27.6%	105	42.0%
[1, 300]	80	26.7%	121	40.3%
[1, 350]	89	25.4%	136	38.9%
[1, 400]	98	24.5%	151	37.8%
[1, 450]	107	23.8%	162	36.0%
[1, 500]	115	23.0%	176	35.2%
[1, 550]	123	22.4%	189	34.4%
[1, 600]	131	21.8%	202	33.7%
[1, 650]	141	21.7%	216	33.2%
[1, 700]	148	21.1%	228	32.6%
[1, 750]	156	20.8%	241	32.1%
[1, 800]	163	20.4%	252	31.5%
[1, 850]	171	20.1%	264	31.1%
[1, 900]	179	19.9%	277	30.8%
[1, 950]	186	19.6%	288	30.3%
[1, 1000]	194	19.4%	300	30.0%

Chapter 4

On The Algebraic Structure of Principal Ideal Lattices

The purpose of this chapter is to study the relationship between the algebraic structure of ideals in cyclotomic quotient rings $\mathbb{Z}[x]/(\Phi_m(x))$, and the geometric structure of their corresponding ideal lattices. We begin this chapter by examining the algebraic structure of (principal) ideals in cyclotomic quotient rings. A logical first step towards solving the SVP in ideal lattices algebraically is to compile a list of the algebraic properties that might be exploited. We will provide results showing that a solution to the SVP in all one- and two-dimensional principal ideal lattices will always correspond to an associate of the ideal's generator. We will then describe two experiments and present empirical evidence to exhibit a similar correspondence in higher dimensions. Our results suggest that a solution to the "shortest generator problem" in principal ideals of $\mathbb{Z}[x]/(\Phi_m(x))$ corresponds to a probabilistic solution of the SVP in their companion principal ideal lattices.

4.1 The Algebraic Structure of $\mathbb{Z}[x]/(\Phi_m(x))$

Rings of cyclotomic integers have been long-studied in algebraic number theory. Translating established results on the structure of cyclotomic integers $O_{K_m} \cong \mathbb{Z}[\zeta_m]$ from the algebraic number theory literature into results on the structure of the quotient ring $\mathbb{Z}[x]/(\Phi_m(x))$ will be straightforward because of the isomorphism $\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathbb{Z}[\zeta_m]$. The following results are taken from a survey on Euclidean number fields [113]. After these results are stated, we will study their implications with regards to the structure of $\mathbb{Z}[x]/(\Phi_m(x))$.

Theorem 4.1.1 ([113], Theorem 2.22)**.** *Let $K_m = \mathbb{Q}(\zeta_m)$. If the field discriminant $\mathcal{D}_{K_m} \leq 500$, then $O_{K_m} \cong \mathbb{Z}[\zeta_m]$ is a PID if and only if O_{K_m} is Euclidean.*

Theorem 4.1.2 ([113], Theorem 5.1)**.** *$\mathbb{Z}[\zeta_m]$ is a PID if and only if $m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$.*

The author of [113] remarks that the algebraic integers corresponding to cyclotomic indices $m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 20, 24$ are known to be norm-Euclidean, meaning that O_{K_m} is a Euclidean domain with respect to the absolute value of a norm N. Recall that for any odd positive integer m the fields $K_m = \mathbb{Q}(\zeta_m)$ and $K_{2m} = \mathbb{Q}(\zeta_{2m})$ are equivalent. Hence there are more cyclotomic indices than the ones listed in Theorem 4.1.2 such that $\mathbb{Z}[\zeta_m]$ is a principal ideal domain, although they represent the same cyclotomic field extensions.

Theorem 4.1.3 ([113], Theorem 5.14)**.** *If $m \neq 16, 24$ is a positive integer with $\varphi(m) \leq 10$, then $\mathbb{Z}[\zeta_m]$ is norm-Euclidean.*

Any algebraic number theory text will affirm that the rings $\mathbb{Z}[\zeta_m]$ are Dedekind domains. The equivalence between $\mathbb{Z}[x]/(\Phi_m(x))$ and $\mathbb{Z}[\zeta_m]$ then implies that $\mathbb{Z}[x]/(\Phi_m(x))$

is a Noetherian ring, and the non-zero prime ideals in $\mathbb{Z}[x]/(\Phi_m(x))$ are maximal. In particular, every non-trivial ideal may be represented as a product of prime, i.e. maximal, ideals. If $\mathbb{Z}[x]/(\Phi_m(x))$ is a principal ideal domain, then this product is unique up to reordering. The following Proposition is a corollary to Theorems 4.1.1, 4.1.2 and 4.1.3.

Proposition 4.1.4. *$\mathbb{Z}[x]/(\Phi_m(x))$ is a Euclidean domain if $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 22, 24, 26, 27, 30, 38, 54.$*

Proof.

By Theorem 4.1.1 and Theorem 4.1.2, the following cyclotomic indices satisfy $\mathcal{D}_K \leq 500$ and $\mathbb{Z}[\zeta_m]$ is a principal ideal domain:

$$m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 18, 19, 22, 27, 38, 54.$$

Thus the rings $\mathbb{Z}[\zeta_m]$ having an index listed above are Euclidean. The cyclotomic indices $m \neq 16, 24$ with $\varphi(m) \leq 10$ are

$$m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 18, 20, 22, 30.$$

By Theorem 4.1.3, the rings $\mathbb{Z}[\zeta_m]$ corresponding to these cyclotomic indices are norm-Euclidean and hence Euclidean. Also, the remark in [113] that cyclotomic integers corresponding to indices

$$m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 20, 24$$

are known to be norm-Euclidean implies that these rings are also Euclidean.

By taking the union of these sets of indices, and knowing that $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ if m is an odd positive integer, the ring $\mathbb{Z}[\zeta_m]$ is Euclidean if

$$m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 22, 24, 26, 27, 30, 38, 54.$$

This statement holds for $\mathbb{Z}[x]/(\Phi_m(x))$ because of the isomorphism $\mathbb{Z}[\zeta_m] \cong \mathbb{Z}[x]/(\Phi_m(x))$.

□

Theorem 2.1.1 implies that the rings $\mathbb{Z}[x]/(\Phi_m(x))$ with index listed in Proposition 4.1.4 are also principal ideal domains, and hence unique factorization domains. The maximum value of $\varphi(m)$ for any index m listed in Proposition 4.1.4 is 18, meaning that ideal lattices arising from these rings will not be near large enough for use in any cryptographic applications. Consequently, exploiting their algebraic structure by using a Euclidean-type algorithm to solve the SVP in ideal lattices is not of practical interest, but remains of theoretical interest. The following Proposition is another corollary to the theorems taken from [113].

Proposition 4.1.5. *$\mathbb{Z}[x]/(\Phi_m(x))$ is a PID if* $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 40, 42, 44, 45, 48, 50, 54, 60, 66, 70, 84, 90.$

Proof.

Follows directly from Theorems 2.1.1, 4.1.1, 4.1.2 and 4.1.3.

□

Corollary 4.1.6. *Let m be a cyclotomic index listed in Proposition 4.1.5. Then any ideal lattice corresponding to an ideal in $\mathbb{Z}[x]/(\Phi_m(x))$ is a principal ideal lattice.*

Proof.

This result is a consequence of Proposition 4.1.5 and the coefficient embedding.

□

The rings $\mathbb{Z}[x]/(\Phi_m(x))$ which are Euclidean domains and/or principal ideal domains have now been identified through a translation of algebraic number theory results. These are basic properties to verify when studying the algebraic structure of any ring. While ideal lattices arising from certain cyclotomic quotient rings must necessarily be principal ideal lattices (see Proposition 4.1.5 and Corollary 4.1.6), it is the ability to choose an ideal for use in many cryptographic applications that provides sufficient justification for studying principal ideals in $\mathbb{Z}[x]/(\Phi_m(x))$. If the SVP in principal ideal lattices is studied in depth, then one may be interested in choosing to work with principal ideal lattices in an applied setting.

4.1.1 The Algebraic Structure of Ideals in $\mathbb{Z}[x]/(\Phi_m(x))$

Much is known about the representation of ideals in rings of algebraic integers. This may be seen in many algebraic number theory texts, e.g. [26]. The definition of an ideal in a ring R given in the second chapter is equivalent to the number theory definition of an *integral* ideal in a ring of algebraic integers. From a number theoretic perspective, we choose to work exclusively with integral ideals of $\mathbb{Z}[\zeta_m]$ because of their equivalence to ideals in $\mathbb{Z}[x]/(\Phi_m(x))$. We will assume that any ideal of $\mathbb{Z}[\zeta_m]$ is an integral ideal. The following Proposition provides some insight into how the ideals of $\mathbb{Z}[\zeta_m]$ may be represented.

Proposition 4.1.7 ([26], Proposition 4.7.7)**.** *Let I be an ideal of $\mathbb{Z}[\zeta_m]$. For any non-zero element $\alpha \in I$ there exists an element $\beta \in I$ such that $I = \alpha\mathbb{Z}[\zeta_m] + \beta\mathbb{Z}[\zeta_m]$.*

That is, any (integral) ideal of $\mathbb{Z}[\zeta_m]$ may be represented by at most two elements. Hence any ideal of $\mathbb{Z}[x]/(\Phi_m(x))$ is generated by no more than two elements. The author of [26] remarks that the ideals of $\mathbb{Z}[\zeta_m]$ behave exactly as the numbers in $\mathbb{Z}$, which is a particularly nice structure. The remainder of this section will be focused on the structure of principal ideals in $\mathbb{Z}[x]/(\Phi_m(x))$. The following results will be useful in proving Theorem 4.1.10, which will be used to show that two principal ideals of the ring $\mathbb{Z}[x]/(\Phi_m(x))$ are equivalent if and only if the generators are associates.

Lemma 4.1.8. *Let R be an integral domain. For any unit $u \in R$, $(u) = uR = R$.*

Proof.

Clearly $(u) = uR \subseteq R$, so we will show that $R \subseteq uR$ for any unit $u \in R$. Suppose that $r_0 \in R$. Then $r_0 \in R \Rightarrow 1 \cdot r_0 = u \cdot u^{-1} \cdot r_0 \in R$ since u is a unit. Hence $r_0 = u \cdot r_1$ for $r_1 = u^{-1} \cdot r_0$. Since $r_1 \in R$ it follows that $r_0 \in uR \Rightarrow R \subseteq uR$.

□

Lemma 4.1.9. *A subring of a field which contains 1 is an integral domain.*

Proof.

Let R be a subring of the field F, and let $1 \in R$. It must be shows that R has no zero divisors. Let $a, b \in R$ with $a \cdot b = 0 \in R$. Then, because $0, a, b$ are also elements of F, this implies that either $a = 0$ or $b = 0$.

□

Theorem 4.1.10. *If $f(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial of degree n, then the ring $R = \mathbb{Z}[x]/(f(x))$ is an integral domain. Furthermore, for any $a, b \in R$, the principal ideals $(a) \triangleleft R$ and $(b) \triangleleft R$ are equal if and only if a and b are associates, written $a \sim b$.*

Proof.

Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n, and let $R = \mathbb{Z}[x]/(f(x))$. Note that R is a subring of the field $F = \mathbb{Q}(x)/(f(x))$, and $1 \in R$. Then, by Lemma 4.1.9, R is an integral domain. We will now show that $(a) = (b) \Leftrightarrow a \sim b$.

$(\Rightarrow)$ $(a) = (b) \Rightarrow a \in (b) \Rightarrow a = ub$ for some $u \in R$. Similarly, $b \in (a) \Rightarrow b = va$ for some $v \in R$. With substitution, $a = ub = uva \Rightarrow uv = vu = 1$ since R is an integral domain. Hence $u, v \in R$ are units, and $a \sim b$.

$(\Leftarrow)$ $a \sim b \Rightarrow a = ub$ for some unit $u \in R$ by definition. Hence $(a) = aR = ubR = buR = bR = (b)$ since $uR = R$ by Lemma 4.1.8.

□

Corollary 4.1.11. *Let $0 \neq f(x), g(x) \in \mathbb{Z}[x]/(\Phi_m(x))$. Then the principal ideals generated by $f(x)$ and $g(x)$ in $\mathbb{Z}[x]/(\Phi_m(x))$ are equal if and only if $f(x) \sim g(x)$.*

Proof.

A consequence of Theorem 4.1.10.

□

This result will be helpful in analyzing the relationship between the algebraic structure of a principal ideal and the geometric structure of the associated principal ideal lattice. It is particularly useful in the two experiments that are presented in the following section.

4.2 The SVP in Principal Ideal Lattices

This section begins with proof of a relationship between the generator of a principal ideal and a solution to the shortest vector problem in the associated principal ideal lattice. In particular, it will be shown that *some* generator will solve the SVP in all one- and two-dimensional principal ideal lattices under both the coefficient and canonical embeddings.

Theorem 4.2.1. *Let $g(x) \in \mathbb{Z}[x]/(\Phi_m(x))$ and $\mathcal{L} \cong (g(x)) \triangleleft \mathbb{Z}[x]/(\Phi_m(x))$ be a principal ideal lattice for any $m = 1, 2, 3, 4, 6$. Then an associate of $g(x)$ will correspond to a solution of the SVP in $\mathcal{L}$.*

Proof.

If $m = 1, 2$, then the ring $\mathbb{Z}[x]/(\Phi_m(x))$ is isomorphic to the integers $\mathbb{Z}$. Let $0 \neq g \in \mathbb{Z}$. For a principal ideal $(g) \triangleleft \mathbb{Z}$, $\|g\|_2 \leq |a| \cdot \|g\|_2 = \|a \cdot g\|_2$ for any non-zero $a \in \mathbb{Z}$, and so the claim holds. The claim will now be shown for $m = 3$ which implies the claim for $m = 6$ since $\mathbb{Z}[x]/(\Phi_3(x)) \cong \mathbb{Z}[x]/(\Phi_6(x))$. A similar analysis will yield the result for $m = 4$. Let $g(x) = (g_0 + g_1 x)$ for some $g_0, g_1 \in \mathbb{Z}$ and consider the principal ideal $(g(x)) \triangleleft \mathbb{Z}[x]/(x^2 + x + 1)$. Any non-zero element $h(x) \in (g(x))$ may be expressed as

$$h(x) \mod x^2 + x + 1 = (f_0 + f_1 x) \cdot (g_0 + g_1 x) \mod x^2 + x + 1$$

for some $f_0, f_1 \in \mathbb{Z}$, at least one of which is non-zero. Hence

$$\begin{aligned} h(x) \mod x^2 + x + 1 &= f_0 g_0 + f_0 g_1 x + f_1 g_0 x + f_1 g_1 x^2 \mod x^2 + x + 1 \\ &= f_0 g_0 + (f_0 g_1 + f_1 g_0) x + f_1 g_1 (-x - 1) \\ &= (f_0 g_0 - f_1 g_1) + (f_0 g_1 + f_1 g_0 - f_1 g_1) x. \end{aligned}$$

Observe that

$$\begin{aligned}\|g(x)\|_2^2 &= \left\| \begin{pmatrix} g_0 \\ g_1 \end{pmatrix} \right\|_2^2 \\ &= g_0^2 + g_1^2\end{aligned}$$

and also

$$\begin{aligned}\|h(x)\|_2^2 &= \left\| \begin{pmatrix} f_0g_0 - f_1g_1 \\ f_0g_1 + f_1g_0 - f_1g_1 \end{pmatrix} \right\|_2^2 \\ &= (f_0g_0 - f_1g_1)^2 + (f_0g_1 + f_1g_0 - f_1g_1)^2 \\ &= f_0^2g_0^2 - 2f_0f_1g_0g_1 + f_1^2g_1^2 + f_1^2g_0^2 + (-2f_1^2 + 2f_0f_1)g_0g_1 + (f_0 - f_1)^2g_1^2 \\ &= (f_0^2 + f_1^2)g_0^2 - (2f_1^2)g_0g_1 + [(f_0 - f_1)^2 + f_1^2]g_1^2.\end{aligned}$$

Since $(f_0^2+f_1^2) \geq 1$ and $[(f_0-f_1)^2+f_1^2] \geq 1$ because both f_0 and f_1 cannot be 0, it follows that $\|g(x)\|_2^2 \leq \|h(x)\|_2^2$ unless the product of the coefficients of the generator is positive $g_0 \cdot g_1 > 0$. Hence, unless the product $g_0 \cdot g_1 > 0$, the generator itself will correspond to a solution of the SVP in the principal ideal lattice. Suppose that $g_0 \cdot g_1 > 0$, and note that this requires both g_0 and g_1 to be non-zero. Without loss of generality, assume that $g_1 \geq g_0$, which implies that $|g_0 \cdot g_1| \geq |g_0^2|$. Note that $x^2 \in \mathbb{Z}[x]/(\Phi_3(x))$ is a unit because $x^2 \cdot x = 1 \in \mathbb{Z}[x]/(\Phi_3(x))$, and so $(g(x) \cdot x^2)$ will generate the same principal ideal as $g(x)$

by Corollary 4.1.11. Observe

$$\begin{aligned}(g_0 + g_1x) \cdot x^2 \mod x^2 + x + 1 &= (g_0 + g_1x) \cdot (-x - 1) \mod x^2 + x + 1 \\ &= -g_0x - g_0 - g_1x^2 - g_1x \\ &= -g_0x - g_0 - g_1(-x - 1) - g_1x \\ &= -g_0x - g_0 + g_1x + g_1 - g_1x \\ &= (-g_0 + g_1) - g_0x,\end{aligned}$$

and the product of the coefficients is $(-g_0) \cdot (-g_0 + g_1) = g_0^2 - g_0 \cdot g_1$. Since $g_0 \cdot g_1 > 0 \Rightarrow -g_0 \cdot g_1 < 0$, and since $|g_0 \cdot g_1| \geq |g_0^2|$, it follows that $g_0^2 - g_0 \cdot g_1 \leq 0$. Hence this generator will correspond to a shortest vector by the analysis performed above. Thus, an associate of the given generator of a principal ideal in $\mathbb{Z}[x]/(\Phi_3(x))$ will correspond to a solution of the SVP in the affiliated principal ideal lattice. Similarly, for any principal ideal $(g(x)) \triangleleft \mathbb{Z}[x]/(\Phi_m(x))$ where $m = 4, 6$, if $g(x)$ itself does not correspond to a solution of the SVP, then one may multiply $g(x)$ by units to find an associate polynomial that generates the same ideal which satisfies certain properties for corresponding to a solution of the SVP in the principal ideal lattice.

□

Example 4.2.2. *The SVP in the Coefficient Embedding of* $(3 + 2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$. *Recall the running example of* $(3+2x) \triangleleft \mathbb{Z}[x]/(\Phi_6(x))$. *The plot of the coefficient embedding of this ideal may be seen in Figure 2.3.*

Upon inspection of the plot in Figure 2.3, it is obvious that the SVP is solved only by two vectors. These vectors are

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} -3 \\ -2 \end{pmatrix}.$$

These two vectors correspond to the polynomials $(3+2x), (-3-2x) \in \mathbb{Z}[x]/(\Phi_m(x))$, *which are clearly both associates of* $(3+2x)$ *and hence generate the same ideal.*

In light of Theorem 4.2.1, one may question whether or not some generator of a principal ideal would correspond to a solution of the SVP in ideal lattices under the canonical embedding as well. The following result partially answers this question, showing that a generator for all one- and two-dimensional principal ideal lattices will correspond to a solution of the SVP under the canonical embedding. Results for higher dimensions are outside the scope of this work.

Theorem 4.2.3. *Let* $I = (g(\zeta_m)) \lhd O_{K_m}$ *be a principal ideal in the ring of cyclotomic integers for any* $m = 1, 2, 3, 4, 6$. *Then an associate of* $g(\zeta_m)$ *will correspond to a solution of the SVP in* $\sigma(I) \subset \mathbb{R}^{\varphi(m)}$ *relative to either the power or powerful basis.*

Proof.

This proof is very similar to that of Theorem 4.2.1 because of its computational nature. The result will only be shown for the case $m = 6$, which is isomorphic to the case $m = 3$. The other cases $(m = 1, 2, 4)$ are similar. This result will be proved using the power basis, but note that using the power(ful) basis for $m = 3$ implies that the result holds for the powerful basis when $m = 6$ because $K_3 = K_6$.

Let $(g(\zeta_6)) \lhd \mathbb{Z}[\zeta_6]$ be a principal ideal. Then $g(\zeta_6) = g_0 + g_1\zeta_6$ for some $g_0, g_1 \in \mathbb{Z}$, at least one of which is non-zero. The two embeddings $\sigma_{1,2} : \mathbb{Q}(\zeta_6) \to \mathbb{C}$ are defined by their action on ζ_6. We have $\sigma_1(\zeta_6) = \zeta_6$ and $\sigma_2(\zeta_6) = \overline{\zeta_6}$. The canonical embedding of $g(\zeta_6)$ is given by

$$\begin{aligned}\sigma(g(\zeta_6)) &= (g_0 + g_1\zeta_6, g_0 + g_1\overline{\zeta_6}) \\ &= \left(\frac{2g_0 + g_1 + g_1 i\sqrt{3}}{2}, \frac{2g_0 + g_1 - g_1 i\sqrt{3}}{2}\right).\end{aligned}$$

The squared Euclidean norm of this element $\sigma(g(\zeta_6)) \in \mathbb{C}^2$ is

$$\begin{aligned}\|\sigma(g(\zeta_6))\|_2^2 &= \left|\frac{2g_0 + g_1 + g_1 i\sqrt{3}}{2}\right|^2 + \left|\frac{2g_0 + g_1 - g_1 i\sqrt{3}}{2}\right|^2 \\ &= 2g_0^2 + 2g_0g_1 + 2g_1^2.\end{aligned}$$

Any arbitrary non-zero element of the ideal $h(\zeta_6) \in (g(\zeta_6)) \lhd \mathbb{Z}[\zeta_6]$ may be expressed as

$$\begin{aligned}h(\zeta_6) &= (f_0 + f_1\zeta_6) \cdot (g_0 + g_1\zeta_6) \\ &= (f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)\zeta_6.\end{aligned}$$

The canonical embedding of this element and the square of its Euclidean norm, respectively, are given by

$$\begin{aligned}\sigma(h(\zeta_6)) = \Big(&[(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)\zeta_6], \\ &[(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)\overline{\zeta_6}]\Big);\text{ and}\end{aligned}$$

$$
\begin{aligned}
\|\sigma(h(\zeta_6))\|_2^2 &= \Big|(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)\zeta_6\Big|^2 \\
&+ \Big|(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)\overline{\zeta_6}\Big|^2 \\
&= \left|\frac{2(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)i\sqrt{3}}{2}\right|^2 \\
&+ \left|\frac{2(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1) - (f_0g_1 + f_1g_0 + f_1g_1)i\sqrt{3}}{2}\right|^2 \\
&= 2\bigg(\frac{2(f_0g_0 - f_1g_1) + (f_0g_1 + f_1g_0 + f_1g_1)}{2}\bigg)^2 \\
&+ 2\bigg(\frac{(f_0g_1 + f_1g_0 + f_1g_1)\sqrt{3}}{2}\bigg)^2 \\
&= (f_0^2 + f_0f_1 + f_1^2) \cdot (2g_0^2 + 2g_0g_1 + 2g_1^2).
\end{aligned}
$$

Note that $(f_0^2 + f_0f_1 + f_1^2) \in \mathbb{Z}$ and observe

$$
\begin{aligned}
(f_0 + f_1)^2 \geq 0 &\Rightarrow f_0^2 + 2f_0f_1 + f_1^2 \geq 0 \\
&\Rightarrow f_0^2 + f_1^2 \geq -2f_0f_1 \\
&\Rightarrow f_0^2 + f_1^2 > \frac{1}{2}(f_0^2 + f_1^2) \geq -f_0f_1 \text{ since both } f_0, f_1 \text{ cannot be 0} \\
&\Rightarrow f_0^2 + f_1^2 > -f_0f_1 \\
&\Rightarrow f_0^2 + f_0f_1 + f_1^2 > 0 \\
&\Rightarrow f_0^2 + f_0f_1 + f_1^2 \geq 1 \text{ since } (f_0^2 + f_0f_1 + f_1^2) \in \mathbb{Z}.
\end{aligned}
$$

Hence $\|\sigma(h(\zeta_6))\|_2^2 \geq \|g(\zeta_6)\|_2^2$, and so the generator of the principal ideal will correspond to a solution of the SVP in the principal ideal lattice under the canonical embedding.

□

Example 4.2.4. *The SVP in the Canonical Embedding of* $(3+2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$*.*
The example of $(3+2\zeta_6) \triangleleft \mathbb{Z}[\zeta_6]$ *will be used once again. The plot of the canonical embedding of this ideal may be seen in Figure 2.1. From looking at this plot there seems to be several possible solutions to the SVP. By Theorem 3.2.14 the principal ideal lattice* $\sigma(I)$ *is WR, so there are at least four solutions to the SVP in* $\sigma(I)$*. In fact, there are six possible solutions to the SVP in* $\sigma(I)$*. Four of these solutions are given by*

$$\pm \begin{pmatrix} \frac{8}{\sqrt{2}} \\ \frac{-2\sqrt{3}}{\sqrt{2}} \end{pmatrix} \text{ and } \pm \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-5\sqrt{3}}{\sqrt{2}} \end{pmatrix}.$$

As shown in Example 2.4.1, these vectors correspond to the canonical embedding of elements $\pm(3+2\zeta_6) \in \mathbb{Z}[\zeta_6]$ *and* $\pm(-2+5\zeta_6) \in \mathbb{Z}[\zeta_6]$*, respectively. All four of these elements are associates of* $(3+2\zeta_6) \in \mathbb{Z}[\zeta_6]$*, and hence generate the same ideal.*

We return our focus to the quotient ring perspective of ideal lattices. The low-dimensional results presented in this section prompt an examination of principal ideal lattices in higher dimensions for a similar relationship. Principal ideals with a specific structure are considered prior to the general case. The following proposition addresses the case of a principal ideal generated by a polynomial of degree zero.

Proposition 4.2.5. *Let* $\mathcal{L} \cong (\alpha) \triangleleft \mathbb{Z}[x]/(f(x))$ *be a principal ideal lattice for some monic irreducible* $f(x) \in \mathbb{Z}[x]$ *of degree* n *and* $\alpha \in \mathbb{Z}$*. Then* $\alpha \in \mathbb{Z}[x]/(f(x))$ *will correspond to a solution of the SVP in* $\mathcal{L}$*.*

Proof.
Represent the lattice $\mathcal{L}$ with the rotation basis matrix of $\alpha \in \mathbb{Z}[x]/(f(x))$. Thus $\mathcal{L} =$

$\alpha \cdot I_n \cdot \mathbb{Z}^n$ where I_n is the $n \times n$ identity matrix. Then

$$\begin{aligned}\min_{0 \neq x \in \mathcal{L}} \|x\|_2 &= \min_{0 \neq y \in \mathbb{Z}^n} \|\alpha \cdot I_n \cdot y\|_2 \\ &= |\alpha| \cdot \min_{0 \neq y \in \mathbb{Z}^n} \|I_n \cdot y\|_2 \\ &= |\alpha| \cdot \min_{0 \neq y \in \mathbb{Z}^n} \|y\|_2 \\ &= |\alpha|\end{aligned}$$

because $\min_{0 \neq y \in \mathbb{Z}^n} \|y\| = 1$. Now observe that the norm of the vector corresponding to $\alpha \in \mathbb{Z}[x]/(f(x))$ is also equal to $|\alpha|$.

□

Observe that this result together with Theorem 4.1.10 imply that if a principal ideal is generated by an associate of some degree zero polynomial, then the vector corresponding to that degree zero polynomial will solve the SVP in the principal ideal lattice. Since the rings of cyclotomic integers are so well studied, many of the units in $\mathbb{Z}[\zeta_m]$ are known. Certain units of these rings, along with this observation, yield the corollary below.

Corollary 4.2.6. *Let $\mathcal{L} \cong (\alpha \cdot x^i) \lhd \mathbb{Z}[x]/(\Phi_m(x))$ be a principal ideal lattice for some $\alpha \in \mathbb{Z}$ and $i \in \{0, \dots, \varphi(m) - 1\}$. Then $\alpha \cdot x^i \in \mathbb{Z}[x]/(f(x))$ will correspond to a solution of the SVP in $\mathcal{L}$ for $i \in \{0, \dots, \varphi(m) - 1\}$.*

Proof.
Note that if $\varphi(m) = n$, then ζ_m^i is a unit of $\mathbb{Z}[\zeta_m]$ for all $i = 0, \dots, n-1$. Under the isomorphism $\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathbb{Z}[\zeta_m]$, it follows that x^i is a unit of $\mathbb{Z}[x]/(\Phi_m(x))$ for all $i = 0, \dots, n-1$. Thus, $\alpha \cdot x^i$ and α are associates for all $i = 0, \dots, n-1$, and they generate the same ideal by Corollary 4.1.11. Since $\mathcal{L}$ now corresponds to $(\alpha) \lhd \mathbb{Z}[x]/(f(x))$, we may

apply Proposition 4.2.5 and observe that $\|\alpha\|_2 = \|\alpha \cdot x^i\|_2$ for $i \in \{0, \ldots, \varphi(m) - 1\}$ to obtain the desired result.

□

This corollary will be important in determining the parameters of the experiments presented in this section. It has been shown that the SVP in all one- and two-dimensional principal ideal lattices $\mathcal{L} \cong I \lhd \mathbb{Z}[x]/(\Phi_m(x))$ will be solved by *some* generator of I. In higher dimensions, we have shown the same relationship when the ideal is generated by any monomial. To investigate the general case of whether or not some generator of a principal ideal will correspond to a solution of the SVP, Maple$^{\text{TM}}$ is used to conduct tests on a random sampling of principal ideal lattices. These experiments will be described, and the results discussed, in the remainder of this chapter.

4.2.1 Principal Ideal Lattice Experiments

The two principal ideal lattice experiments presented will be used to determine whether or not a relationship exists between a generator of the principal ideal and a solution to the SVP in its associated principal ideal lattice. We would like to experiment with higher dimensional principal ideal lattices to estimate the proportion for which the LLL algorithm will output a short vector corresponding to an associate of a known generator when the rotation basis matrix of this generator is given as the input for the algorithm. Similar testing for this relationship in ideal lattices under the canonical embedding is also of interest, but outside the scope of this work. All of the Maple$^{\text{TM}}$ procedures used in these experiments may be found in Appendix B. Each “sample” for these experiments will be conducted as follows:

1. Input a given cyclotomic index m with $\varphi(m) = n$.

2. Generate a random polynomial $g(x) \in \mathbb{Z}[x]/(\Phi_m(x))$, which yields the principal ideal $(g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$.

3. Construct the rotation basis matrix G for the corresponding ideal lattice.

$$G = \begin{pmatrix} g(x) & x \cdot g(x) & \ldots & x^{n-1} \cdot g(x) \end{pmatrix}$$

4. Input the matrix G into the LLL algorithm.

5. Determine if the short vector output corresponds to an associate of $g(x)$.

For the purpose of these experiments, we define a “success” to be an instance when the LLL outputs a short vector that does correspond to an associate of $g(x)$, which will also be a generator of the ideal. The first experiment samples a certain number of random principal ideal lattices from each cyclotomic index $m = 1, \ldots, 100$ with $\varphi(m) > 2$ to estimate the density of principal ideal lattices for which the LLL will output an associate of the generator. The second experiment is designed to estimate the density of this same occurrence for random principal ideal lattices within some range of cyclotomic indices.

We will now say a few words about our methodology. We have run these experiments on a large number of samples to reasonably conjecture whether or not a relationship between the generator of a principal ideal and a solution to the SVP exists. Our results will be used to provide empirical evidence that suggests a probabilistic method for solving the SVP in principal ideal lattices algebraically by finding the “shortest generator” of the corresponding principal ideal. There are some potential problems that may affect the validity and outcome of these experiments. First, the random polynomial generated by

Maple$^{\text{TM}}$ may not be truly random. For the purposes of this experiment we will assume that the random output provided by Maple$^{\text{TM}}$ is independent and identically distributed (i.i.d). This allows for the use of statistical inference techniques to estimate the proportion of principal ideal lattices from a given cyclotomic index in which the LLL's short vector output corresponds to an associate of the ideal's generator.

Another potential problem is that, by using only the rotation basis matrix of the generator to represent the lattice, it is possible that some underlying structure of this lattice basis will affect the behavior of the LLL algorithm. Gama and Nguyen [40] conducted extensive experiments to test the performance of several lattice reduction algorithms, and used at least 20 random lattice bases for each lattice to prevent any reduction algorithm from exploiting special properties of an input basis. If a relationship between the generator and LLL short vector output exists, then the rotation basis of a generator would potentially contain a short vector and maintain a special structure. It would be interesting to reduce at least 20 random lattice bases for each ideal lattice to see if the LLL still outputs an associate of the known generator. However, since our conjectured method of exploitation centers around finding a generator, reducing this one lattice basis should be sufficient to demonstrate the existence of a relationship between the algebraic and geometric structure of principal ideal lattices.

We set certain parameters on the random polynomial generated by Maple$^{\text{TM}}$ for the principal ideal. As a result of Corollary 4.2.6, it would be trivial to randomly generate a monomial for the purpose of these experiments. Also, since x^i is a unit of $\mathbb{Z}[x]/(\Phi_m(x))$, factoring out the appropriate power of x from a polynomial with no constant term would yield an associate polynomial having a non-zero constant term that generates the same ideal. To avoid having these cases affect our sampling we require that each randomly generated polynomial have at least two non-zero terms, including a non-zero constant term. The random polynomial is generated with the following Maple$^{\text{TM}}$ code:

$$\begin{aligned} g :=& \mathit{Generate}(\mathit{nonzeroint}(\text{range} = -99..99)) + x * \mathit{randpoly}(x, \\ &\text{coeffs} = \mathit{rand}(-99..99), \text{degree} = \mathit{Generate}(\mathit{integer}(\text{range} = 0..n-2)), \\ &\text{terms} = \mathit{Generate}(\mathit{integer}(\text{range} = 1..n-1))). \end{aligned}$$

This function generates a non-zero integer for the constant term, and then adds this term to a polynomial of degree no greater than $\varphi(m)-1 = n-1$ with no constant term, where m is the cyclotomic index from which samples are taken. The constant term is generated separately from the rest of the polynomial to ensure that this generator will meet our requirements. It is by default that this Maple$^{\text{TM}}$ function generates random coefficients for this polynomial in the range $[-99, 99]$.

The next step in setting up these experiments is determining the number of samples that will be required to use statistical inference techniques in estimating this proportion. Let β denote the bound on the error of our estimate and let $(1-\alpha)$ be the confidence coefficient. Denote by $z_{\alpha/2}$ the z value having an area of $\alpha/2$ to its right under the normal curve. The number of samples n can be determined with the inequality below.

$$z_{\alpha/2} \cdot \sqrt{\frac{p \cdot q}{n}} \leq \beta$$

Here p is the true population proportion of "successes" and $q = 1-p$. We choose $p = q = .5$ to maximize the value of the numerator, and also because the true population proportion is unknown. One may determine the number of samples required to construct the $(1-\alpha)$ confidence interval with bound β by solving for n in the above inequality.

$$
\begin{aligned}
0.03 \geq 1.645\sqrt{\frac{0.5 \cdot 0.5}{n}} &\Rightarrow n \geq 1068 \\
0.04 \geq 2.576\sqrt{\frac{0.5 \cdot 0.5}{n}} &\Rightarrow n \geq 1068 \\
0.05 \geq 1.645\sqrt{\frac{0.5 \cdot 0.5}{n}} &\Rightarrow n \geq 385
\end{aligned}
$$

The sample size of 1068 is chosen for the first experiment to reflect a 95% confidence interval of ±3% and a 99% confidence interval of ±4%. In the second experiment, the sample size 385 is chosen to reflect a 95% confidence interval of ±5%. These confidence intervals are interpreted in the following manner: by using 1068 samples in repeated sampling of this proportion, in the long run we expect that the true proportion will be contained in 95% of the intervals $(\hat{p} - 3\%, \hat{p} + 3\%)$ and contained in 99% of the intervals $(\hat{p} - 4\%, \hat{p} + 4\%)$, where $\hat{p}$ is the computed sample proportion. Similarly, using 385 samples in repeated sampling of this proportion would mean that we expect 95% of the intervals $(\hat{p} - 5\%, \hat{p} + 5\%)$ to contain the true proportion in the long run. In these experiments, it will be necessary to verify whether or not an ideal lattice vector corresponds to a unit of the ring $\mathbb{Z}[x]/(\Phi_m(x))$. This will be accomplished in our Maple$^{\text{TM}}$ program with linear algebra.

Theorem 4.2.7. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n. Suppose that $h(x) \in \mathbb{Z}[x]/(f(x))$, and denote by H it rotation basis matrix. Then $h(x)$ is a unit in $\mathbb{Z}[x]/(f(x))$ if and only if $H^{-1}e_1 \in \mathbb{Z}^n$ where e_1 denotes the standard unit vector.*

Proof.

Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n and let $R = \mathbb{Z}[x]/(f(x))$.

Define H as the rotation matrix

$$H = \begin{pmatrix} h(x) & x \cdot h(x) & \dots & x^{n-1} \cdot h(x) \end{pmatrix}.$$

having the ith column correspond to $x^i \cdot h(x) \mod f(x)$. Now observe that $h(x) \in R$ is a unit $\Leftrightarrow \exists\, u(x) \in R$ such that $h(x) \cdot u(x) \mod f(x) = 1 \in R \Leftrightarrow \exists\, u \in \mathbb{Z}^n$ such that $Hu = e_1 \Leftrightarrow H^{-1}e_1 \in \mathbb{Z}^n$.

□

In particular, the above result holds if $f(x)$ is taken to be a cyclotomic polynomial. Theorem 4.2.7 will be applied in the experiments to test whether or not the short vector output by LLL is an associate of the known generator. The following example shows in detail how we determine the existence of such a relationship for a given generator.

Example 4.2.8. *Let $g(x) = -7 - 94x - 55x^2 + 22x^3 \in \mathbb{Z}[x]/(\Phi_5(x))$ and consider the principal ideal lattice corresponding to $(g(x)) \triangleleft \mathbb{Z}[x]/(\Phi_5(x))$. This generator yields the following rotation basis matrix G for the lattice.*

$$G = \begin{pmatrix} -7 & -22 & 77 & 39 \\ -94 & -29 & 55 & 116 \\ -55 & -116 & 48 & 94 \\ 22 & -77 & -39 & 87 \end{pmatrix}$$

When the matrix G is given as input to the LLL algorithm, the matrix $LLL(G)$ is output *by the algorithm.*

$$LLL(G) = \begin{pmatrix} 70 & 10 & -17 & -32 \\ -39 & -7 & -87 & -22 \\ -7 & -77 & 22 & -39 \\ -17 & 32 & -10 & -109 \end{pmatrix}$$

The first column of this matrix is the short vector output of the LLL, which corresponds to the polynomial $f(x) = 70 - 39x - 7x^2 - 17x^3 \in \mathbb{Z}[x]/(\Phi_5(x))$. *We now find the element* $h(x) \in \mathbb{Z}[x]/(\Phi_5(x))$ *such that* $h(x) \cdot g(x) \mod \Phi_5(x) = f(x)$. *This is done by solving for the vector* h *in the following linear system.*

$$\begin{pmatrix} -7 & -22 & 77 & 39 \\ -94 & -29 & 55 & 116 \\ -55 & -116 & 48 & 94 \\ 22 & -77 & -39 & 87 \end{pmatrix} \cdot h = \begin{pmatrix} 70 \\ -39 \\ -7 \\ -17 \end{pmatrix}$$

$$\Rightarrow h = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

This vector h *corresponds to the polynomial* $h(x) = 1 + x^2 \in \mathbb{Z}[x]/(\Phi_5(x))$. *One may verify that* $(1 + x^2) \cdot (-7 - 94x - 55x^2 + 22x^3) \mod \Phi_5(x) = 70 - 39x - 7x^2 - 17x^3$. *Theorem 4.2.7 may now be used to check if* $h(x)$ *is a unit of* $\mathbb{Z}[x]/(\Phi_5(x))$. *If so, then the LLL output is an associate of the generator* $g(x) \in \mathbb{Z}[x]/(\Phi_5(x))$. *We construct the* *rotation matrix, H, of $h(x)$ and solve the system $Hu = e_1$ to apply Theorem 4.2.7.*

$$H \cdot u = e_1$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \end{pmatrix} \cdot u = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Rightarrow u = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 0 \end{pmatrix}$$

Since $H^{-1}e_1 \in \mathbb{Z}^n$, $h(x)$ is a unit of $\mathbb{Z}[x]/(\Phi_5(x))$. This may also be verified by computing $(1 + x^2) \cdot (-x - x^2) \mod \Phi_5(x) = 1$. Thus the LLL output is an associate of $g(x)$, and generates the same ideal.

Experiment 1

In the first experiment, 1068 random principal ideal lattices corresponding to principal ideals in $\mathbb{Z}[x]/(\Phi_m(x))$ will be sampled from each cyclotomic index $m = 1, \ldots, 100$ with $\varphi(m) > 2$. Recall that Theorem 4.2.1 addresses the cases when $\varphi(m) \leq 2$, which are noted separately from the results of this first experiment. Each sampled principal ideal lattice corresponds to a principal ideal generated by a random polynomial. The rotation basis matrix of this random generator will be given as input to the LLL algorithm. The program will then verify whether or not the short vector output corresponds to an associate of the ideal's generator. If so, then this instance is counted as a "success". Figure 4.1 is a plot that depicts the results of this experiment. The horizontal axis coincides with the cyclotomic indices while the vertical axis corresponds to the computed sample proportion for which the LLL output an associate of the generator. The complete results may be found in Appendix A.

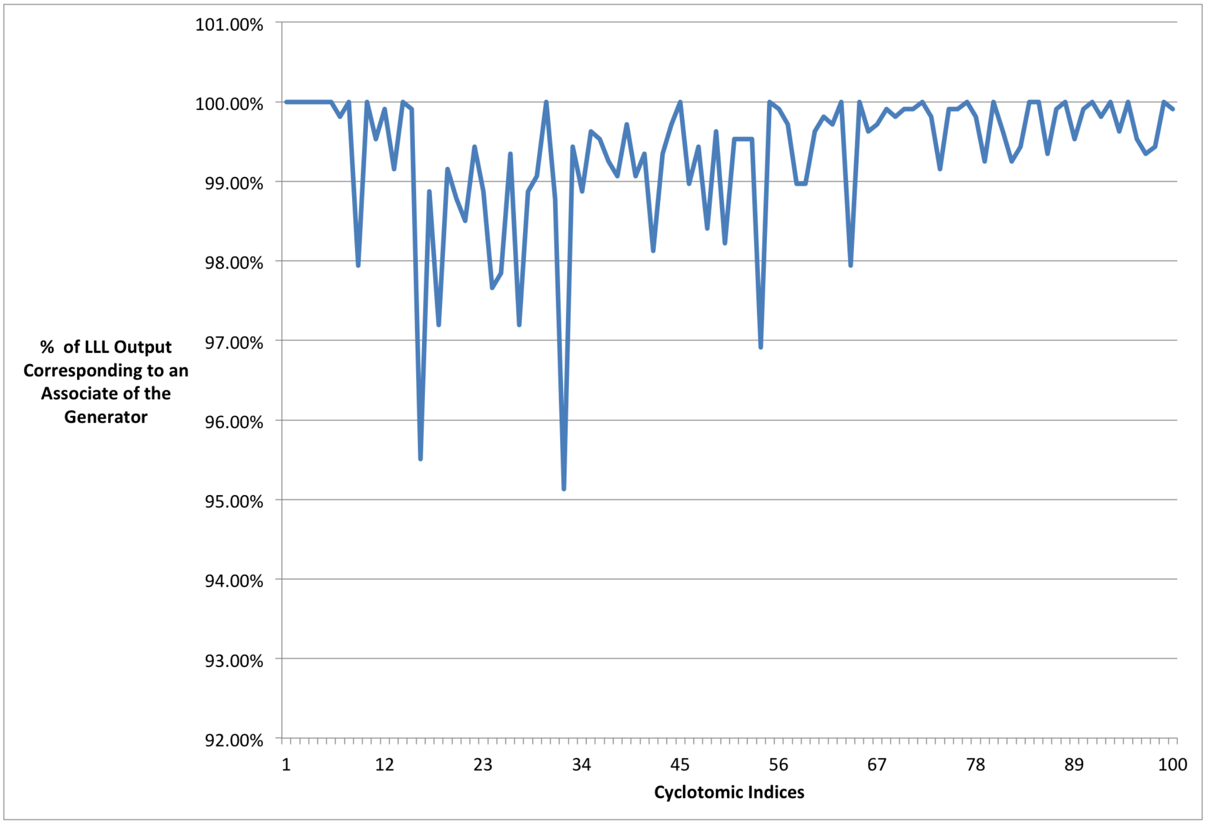

Figure 4.1: Experiment 1 Data Plot

The average of all computed sample proportions is 99.3%. Observe that the computed sample proportion for each index is greater than 95%. The lowest computed sample proportion is 95.13% for cyclotomic index $m = 32$. There seems to be a general upward trend in the computed proportion as the cyclotomic indices get larger, beginning with index $m = 16$. For cyclotomic indices $m \in [65, 100]$, the computed sample proportion is at least 99.16%. This may or may not be attributed to the fact that the number of possible generators subject to our constraints grows with the dimension.

It would be interesting if there was a particular dimension, or set of cyclotomic indices, for which the sampled proportions were either considerably above or below the average. While the computed sample proportion is generally lower in smaller dimensions, dimensions for which the computed proportion is drastically higher or lower than the average are not apparent. Likewise, aside from the indices $m = 16, 32$ both being powers of two, there does not appear to be a pattern in the cyclotomic indices for which the computed proportion is relatively higher or lower than the average.

It is clear that there is not a definite correspondence between a solution to the SVP in a principal ideal lattice and the associated ideal's generator. We would like to know why some principal ideal lattices did not exhibit this relationship. There is no obvious commonality in the principal ideals for which the LLL did not output a vector corresponding to an associate of the generator. It remains of interest to characterize the principal ideals for which this relationship does not hold. Example 4.2.9 provides an example of when the LLL did not output a vector corresponding to an associate of its generator.

Example 4.2.9. *Let* $g(x) = (-2 - 72x - 53x^2 - 39x^3) \triangleleft \mathbb{Z}[x]/(\Phi_{16}(x))$ *and consider the coefficient embedding of* $(g(x)) \triangleleft \mathbb{Z}[x]/(\Phi_{16}(x))$*. The rotation basis matrix of this generator* *is given by the matrix R.*

$$R = \begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 39 & 53 & 72 \\ -72 & -2 & 0 & 0 & 0 & 0 & 39 & 53 \\ -53 & -72 & -2 & 0 & 0 & 0 & 0 & 39 \\ -39 & -53 & -72 & -2 & 0 & 0 & 0 & 0 \\ 0 & -39 & -53 & -72 & -2 & 0 & 0 & 0 \\ 0 & 0 & -39 & -53 & -72 & -2 & 0 & 0 \\ 0 & 0 & 0 & -39 & -53 & -72 & -2 & 0 \\ 0 & 0 & 0 & 0 & -39 & -53 & -72 & -2 \end{pmatrix}$$

When the matrix R is given as input to the LLL algorithm, the short vector output is

$$\begin{pmatrix} 2 & 70 & -19 & -14 & -39 & 0 & 0 & 0 \end{pmatrix}^T.$$

One may verify that

$$(-1+x)\cdot(-2-72x-53x^2-39x^3) \mod \Phi_{16}(x) = 2+70x-19x^2-14x^3-39x^4.$$

Applying Theorem 4.2.7 reveals that $(-1+x)$ *is not a unit of* $\mathbb{Z}[x]/(\Phi_{16}(x))$*, meaning the short vector output by the LLL is not an associate of* $g(x)$*. Consequently the polynomial* $f(x) = 2+70x-19x^2-14x^3-39x^4$ *is not a generator of the ideal* $(g(x)) \triangleleft \mathbb{Z}[x]/(\Phi_{16}(x))$*.*

Additional examples of when the LLL did not output a vector corresponding to an associate of the generator include the three following ideals:

1. $(26 + 44x - 13x^3 - 34x^5 - 60x^7) \lhd \mathbb{Z}[x]/(\Phi_{16}(x))$;
2. $(-89 - 4x - 20x^2 + 52x^3 + 16x^4 - 60x^5 - 68x^6) \lhd \mathbb{Z}[x]/(\Phi_{16}(x))$; and
3. $(77 + 63x - 46x^3 + 77x^5 + 84x^6) \lhd \mathbb{Z}[x]/(\Phi_{16}(x))$.

Overall, the results of this experiment do indicate a high likelihood that the LLL will output a short vector corresponding to an associate of the generator when run on the generator's rotation basis matrix. This suggests that finding the "shortest generator" of a principal ideal, i.e. the generator corresponding to a vector of minimal norm, will most likely correspond to the same or better output as the LLL when the algorithm is given a generator's rotation basis matrix as input.

Experiment 2

A similar experiment is run to sample the density of principal ideal lattices for which the conjectured relationship between a shortest vector and the ideal's generator will hold. In the second experiment, 385 random principal ideal lattices corresponding to principal ideals $(g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$ are generated where m is a random cyclotomic index within some specified range. For each of these randomly selected cyclotomic indices m, a random polynomial is produced to generate a principal ideal $(g(x)) \lhd \mathbb{Z}[x]/(\Phi_m(x))$. The rotation basis matrix for $g(x)$ is then constructed and given as input to the LLL algorithm. The short vector output by the LLL is checked to see whether or not it corresponds to a generator of the ideal, and is again considered a "success" if it does.

The cyclotomic indices m for the second experiment were sampled from various ranges within the range of $1, \ldots, 150$. We required $\varphi(m) \geq 2$ to exclude the one-dimensional cases from this experiment. Table 4.1 displays our results. Like the outcome of our first experiment, these results indicate that the vector corresponding to the shortest generator of a randomly generated principal ideal in $\mathbb{Z}[x]/(\Phi_m(x))$ will most likely be at least as short as the shortest vector output by the LLL algorithm when run on a generator's rotation basis matrix.

Table 4.1: Experiment 2 Results

Cyclotomic Index Range	Successes	Samples	Percentage
[1, 25]	378	385	98.18%
[1, 50]	383	385	99.48%
[1, 75]	384	385	99.74%
[1, 100]	385	385	100.00%
[1, 125]	383	385	99.48%
[1, 150]	382	385	99.22%
[100, 150]	383	385	99.48%
[1, 25]	382	385	99.22%
[25, 50]	379	385	98.44%
[50, 75]	383	385	99.48%
[75, 100]	384	385	99.74%
[100, 125]	385	385	100.00%
[125, 150]	385	385	100.00%

It should be remarked here, as in [40], that the SVP in any lattice of dimension less than 70 is considered easy. Even if the dimension of principal ideal lattices corresponding to principal ideals in $\mathbb{Z}[x]/(\Phi_m(x))$ for $m \in [1, 150]$ is greater than 70, it may not be large enough to remain completely secure in practice. It is also noted in [40] that exhaustive search techniques are not feasible in dimension 100 and beyond because of their running time. If the dimension is at least 100, only approximation algorithms, such as the LLL and its variants, can be run for the SVP. The sampled principal ideal lattices in our experiments were not all large enough to be used in practice. However, demonstrating the existence of a probabilistic relationship between the generator of a principal ideal in $\mathbb{Z}[x]/(\Phi_m(x))$ and a solution to the SVP in the associated principal ideal lattice for $m \in [1, 150]$ supports the conjecture that this probabilistic relationship exists for all cyclotomic indices.

Chapter 5

Conclusions and Future Work

Many of the concepts presented in this dissertation have their roots firmly established in algebraic number theory and abstract algebra, which are both well-studied branches of mathematics. The abundance of resources and information available in these areas suggests that any future progress may heavily depend on new applications of existing ideas. The novel contributions presented in this work include meaningful results on the relationship between two embeddings of an ideal in the ring of cyclotomic integers, and demonstrated progress towards finding short vectors of principal ideal lattices algebraically.

Ideal lattices are at the center of many recent developments in lattice-based cryptography. While most algorithms that output a short vector in an ideal lattice operate geometrically, a few have successfully exploited their additional structure. The aim of this dissertation and future work is to further exploit the algebraic structure of ideal lattices in finding short vectors. It remains unknown whether or not the SVP can be solved algebraically in ideal lattices, however, our results have introduced a largely algebraic approach to this geometric problem in (principal) ideal lattices.

Significance of Results

We have justified studying ideal lattices as ideals of quotient rings through the work presented in Chapter 3. The relationship between the canonical and coefficient embeddings was examined thoroughly. We explicitly defined the matrix that relates these two particular embeddings, and presented results on the equivalence of SVP in any two geometric embeddings of an ideal. We also showed that the canonical embedding of an ideal $I \triangleleft O_K$ in some ring of algebraic integers is well-rounded if and only if the number field K is a cyclotomic number field. This led to the conclusion that the coefficient embedding of an ideal in O_{K_m} will have no more independent shortest vectors than the canonical embedding of the same ideal. Furthermore, our results give rise to the notion of solving the SVP in an ideal lattice under a particular embedding by first solving the SVP in a different embedding with more shortest vectors. That is, perhaps the SVP would be *easier* to solve in one embedding of an ideal, and then a solution could be mapped to the embedding of interest by the matrix that relates the two embeddings.

In Chapter 4 we presented a relationship between the algebraic structure of a principal ideal and the geometric structure of its corresponding lattice. It was shown for all one- and two-dimensional principal ideal lattices that some generator of the ideal will correspond to a solution of the SVP. For the higher dimensional cases, we provided empirical evidence of a probabilistic correspondence between the short vector output of the LLL algorithm on a particular lattice basis and a generator of the ideal. Indeed our results suggest that, by finding the "shortest generator" of a principal ideal in $\mathbb{Z}[x]/(\Phi_m(x))$, there is a high likelihood that the corresponding lattice vector will be at least as short as the LLL output on a generator's rotation basis matrix. Hence, for a probabilistic solution to the SVP in principal ideal lattices, the pure geometric problem of finding a short vector may be expressed as the more algebraic problem of finding a "short" generator. There are existing algorithms that determine whether or not an ideal in $\mathbb{Z}[\zeta_m]$ is principal and, if so, computes a generator (e.g. Algorithm 6.5.10 in [26]). Designing an algorithm that, given a generator, will then find its "shortest" associate is left for subsequent work.

Future Work

Many interesting research directions were outside the scope of this dissertation. In this work we ran experiments using the LLL lattice reduction algorithm to reduce a specific basis of a principal ideal lattice. Empirical evidence suggests that the "shortest generator" of a principal ideal may be used to somewhat predict the short vector output of the LLL on this particular basis. Perhaps finding a generator's rotation basis matrix would be beneficial if given as input to a specific lattice reduction algorithm in pre-processing. It remains to be seen if similar results are obtained using other bases for the sampled principal ideal lattices. Comparing the observations made with the generator's rotation basis matrix against other random lattice bases would provide more conclusive evidence of a relationship between the LLL's short vector output and a principal ideal's generator. This testing would also address whether or not there is some underlying structure in the generator's rotation basis being exploited by the LLL algorithm. Many other lattice reduction algorithms could be used in place of the LLL algorithm for these experiments as well. Determining if other algorithms exhibit a similar correspondence between their short vector output and a generator of the principal ideal is left for future assessment.

Additional areas of planned research include applying the results presented in this dissertation to further exploit the algebraic structure of ideal lattices in finding short vectors, which was the original motivation of our study. The observations made during this research lead to several conjectures on how this may be achieved in the case of principal ideal lattices. These conjectures include potential improvements to existing algorithms, and ideas for new ways of solving the SVP in principal ideal lattices. We hypothesize that sieving among vectors that correspond to generators of a principal ideal would be an effective method of finding a short vector. The results in this dissertation support that reducing vectors which correspond to generators of a principal ideal against each other will most likely produce a short vector. Enumeration algorithms search for short lattice vectors within some bounded region. Incorporating the length of a (shortest) generator in the construction of this region might produce a smaller bounded region, which may consequently improve the algorithm.

Finding the "shortest generator" of a principal ideal algebraically is another speculated approach to finding a short vector in principal ideal lattices. Experimental results indicate that this is a probabilistic solution to the SVP in principal ideal lattices. Quantifying the likelihood and conditions of such an event would allow for comparing this approach to solving the SVP with others. Determining the probability that this "shortest generator" will correspond to a solution of the SVP in principal ideal lattices is an area of anticipated research. It would also be interesting to construct theoretical bounds on the length of a "shortest generator". Perhaps there is an approximate version of the SVP in principal ideal lattices that is always solved by a vector corresponding to a "shortest generator".

While the focus of this work has been on principal ideals in cyclotomic quotient rings $\mathbb{Z}[x]/(\Phi_m(x))$, a generalization of our results is desired. We would like to show the existence of a similar correspondence between short vectors and generators of principal ideals in $\mathbb{Z}[x]/(f(x))$ where $f(x) \in \mathbb{Z}[x]/(f(x))$ is both monic and irreducible, but not cyclotomic. There is also potential to extend some results to arbitrary, i.e. non-principal, ideals in the ring $\mathbb{Z}[x]/(\Phi_m(x))$. Determining how the algebraic structure of ideals with more than one generator would relate to the geometric structure of its corresponding ideal lattice remains an open problem.

Once the algebraic structure of principal ideal lattices has been further exploited by algorithms that output a short vector, it will be interesting to see how these new algorithms compare to more popular lattice reduction algorithms. This would assess whether or not our conjectured manners of exploitation make certain algorithms faster and/or optimize their output in practice. Further experimentation, similar to that of [40], is required to analyze the performance of various reduction algorithms on ideal lattices. We remark that our current interest in this experimentation is with regards to principal ideal lattices, but this type of testing on ideal lattices in general is absent from the literature.

The authors of [40] ran extensive experiments to compare the performance of various lattice reduction algorithms on random bases of general lattices, and no analog for ideal lattices has been published. A standard way of generating ideal lattices to allow for testing algorithms was not available at the time Gama and Nguyen published their experimental results, but was made accessible in [95]. Results from such experiments on ideal lattices would allow one to somewhat anticipate the performance of a particular lattice reduction algorithm on an ideal lattice. Furthermore, algorithms that exploit the algebraic structure of ideal lattices were outside the scope of [40], but may be included in testing the performance of lattice reduction algorithms on ideal lattices. One may then confirm whether or not the algorithms that attempt to exploit this additional structure offer better, worse, or about the same performance in practice as other lattice reduction algorithms.

REFERENCES

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Symposium on Theory of Computing*, pages 99–108. Association for Computing Machinery, 1996.

[2] M. Ajtai. The shortest vector problem in ℓ_2 is NP-hard for randomized reductions (extended abstract). In *Symposium on Theory of Computing*, pages 10–19. Association for Computing Machinery, 1998.

[3] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Symposium on Theory of Computing*, pages 284–293. Association for Computing Machinery, 1997.

[4] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Symposium on Theory of Computing*, pages 601–610. Association for Computing Machinery, 2001.

[5] M. Ajtai, R. Kumar, and D. Sivakumar. Sampling short lattice vectors and the closest lattice vector problem. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity*, pages 53–57. IEEE, 2002.

[6] A. Andrade, A. Ferrari, C. Benedito, and S. Costa. Constructions of algebraic lattices. *Journal of Computational and Applied Mathematics*, 29(3):493–505, 2010.

[7] M. Artin. *Algebra*. Prentice Hall, Boston, MA, second edition, 2011.

[8] V. Arvind and P. Joglekar. Some sieving algorithms for lattice problems. In *Proceedings of the IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 25–36, 2008.

[9] L. Babai. On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[10] E. Bayer-Fluckiger. Determinants of integral ideal lattices and automorphisms with given characteristic polynomial. *Journal of Algebra*, 257:215–221, 2002.

[11] E. Bayer-Fluckiger. Ideal lattices. *A Panorama of Number Theory or The View from Baker's Garden*, pages 168–184, 2002.

[12] E. Bayer-Fluckiger. Upper bounds for euclidean minima of algebraic number fields. *Journal of Number Theory*, 121:305–323, 2006.

[13] E. Bayer-Fluckiger and G. Nebe. On the euclidean minimum of some real number fields. *Journal de Theorie des Nombres de Bordeaux*, 17(2):437–454, 2005.

[14] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. Algebraic lattice constallations: Bounds of performance. *IEEE Transactions on Information Theory*, 52:319–327, 2006.

[15] E. Bayer-Fluckiger and I. Suarez. Modular lattices over cyclotomic fields. *Journal of Number Theory*, 114:394–411, 2005.

[16] E. Bayer-Fluckiger and I. Suarez. Ideal lattices over totally real number fields and euclidean minima. *Archiv Mathematics*, 86:217–225, 2006.

[17] D. Bernstein. *Post-Quantum Cryptography*, chapter Introduction to Post-Quantum Cryptography, pages 1–13. Springer, Berlin, 2009.

[18] J. Blomer and S. Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. *Theory of Computer Science*, 410(18):1648–1665, 2009.

[19] J. Blomer and P. Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Symposium on Theory of Computing*, pages 711–720. Association for Computing Machinery, 1999.

[20] W. Bosma. Canonical bases for cyclotomic fields. *Applicable Algebra in Engineering, Communication and Computing*, 1:125–134, 1990.

[21] M. Bremner. *Lattice Basis Reduction - An Introduction to the LLL Algorithm and Its Applications.* CRC Press, 2012.

[22] J. Buchmann and R. Lindner. Density of ideal lattices (extended abstract). In *Algorithms and Number Theory*, volume 09221. Dagstuhl Seminar Proceedings, 2009.

[23] J. Buchmann, R. Lindner, and M. Ruckert. Explicit hard instances of the shortest vector problem. *PQCrypto*, 5299, LNCS:79–94, 2008.

[24] J. Cassels. *An Introduction to the Geometry of Numbers.* Springer-Verlag, 1971.

[25] C. Chen, C. Ku, and D. Yen. Cryptanalysis of large RSA exponent by using the LLL algorithm. *Applied Mathematics and Computation*, 169:516–525, 2005.

[26] H. Cohen. *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer-Verlag, 1993.

[27] J. Conway and N. Sloane. *Sphere Packings, Lattices and Groups.* Springer, 1998.

[28] D. Coppersmith. Finding a small root of a bivariate integer equation: Factoring with high bits known. In *Eurocrypt 1996: Advances in Cryptology*, pages 178–189. Springer, 1996.

[29] D. Coppersmith. Finding a small root of a univariate modular equation. In *Eurocrypt 1996: Advances in Cryptology*, pages 155–165. Springer, 1996.

[30] C. Coupe, P. Nguyen, and J. Stern. The effectiveness of lattice attacks against low-exponent RSA. In *PKC 1999: Public Key Cryptography*, pages 204–218. Springer, 1999.

[31] D. Dadush, C. Peikert, and S. Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In *IEEE 52nd Annual Symposium of Foundations of Computer Science*. IEEE Computer Society, 2011.

[32] J. Ding and R. Lindner. Identifying ideal lattices. *IACR Cryptology ePrint Archive*, 2007/322, 2007.

[33] C. Dwork. Positive applications of lattices to cryptography. *Mathematical Foundations of Computer Science 1997*, 1295 LNCS:44–51, 1997.

[34] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including complexity analysis. *Mathematics of Computation*, 44:463–471, 1985.

[35] L. Fukshansky. Personal communication, 2013.

[36] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices II. *International Journal of Number Theory*, 9(1):139–154, 2013.

[37] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *International Journal of Number Theory*, 8(1):189–206, 2012.

[38] L. Fukshansky and X. Sun. On the geometry of cyclic lattices. Preprint, 2013.

[39] N. Gama and P. Nguyen. Finding short lattice vectors within Mordell's inequality. In *Symposium on Theory of Computing*, pages 207–216. Association for Computing Machinery, 2008.

[40] N. Gama and P. Nguyen. Predicting lattice reduction. In *Eurocrypt 2008: Advances in Cryptology*, LNCS. Springer, 2008.

[41] N. Gama, P. Nguyen, and O. Regev. Lattice enumeration using extreme pruning. In *Eurocrypt 2010: Advances in Cryptology*, volume 6110. Springer, 2010.

[42] N. Gama and M. Schneider. SVP challenge. http://www.latticechallenge.org/svp-challenge, 2010.

[43] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Symposium on Theory of Computing*, pages 169–178. Association for Computing Machinery, 2009.

[44] C. Gentry and M. Szydlo. Cryptanalysis of the revised NTRU signature scheme. In *Eurocrypt 2002: Advances in Cryptology*, volume 2332, LNCS, pages 299–320. Springer, 2002.

[45] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In *Conference on Advances in Cryptology*, pages 112–131. Springer-Verlag, 1997.

[46] S. Hallgren and U. Vollmer. *Post-Quantum Cryptography*, chapter Quantum Computing, pages 15–32. Springer, 2009.

[47] G. Hanrot, X. Pujol, and D. Stehle. Algorithms for the shortest and closest lattice vector problems. In *IWCC 2011*, volume 6639, LNCS, pages 159–190, 2011.

[48] J. Hoffstein, J. Pipher, and J. Silverman. NTRU: A ring based public key cryptosystem. In *ANTS '98*, volume 1423, pages 267–288, 1998.

[49] J. Hoffstein, J. Pipher, and J. Silverman. *An Introduction to Mathematical Cryptography.* Springer, 2008.

[50] N. Howgrave-Graham and M. Szydlo. A method to solve cyclotomic norm equations. In *Algebraic Number Theory: 6th International Symposium - ANTS-VI*, volume 3076, LNCS, pages 272–279. Springer, 2004.

[51] T. Hungerford. *Algebra.* Graduate Texts in Mathematics. Springer-Verlag, 1974.

[52] I. Ipsen. *Numerical Matrix Analysis - Linear Systems and Least Squares.* Society for Industrial and Applied Mathematics, 2009.

[53] A. Joux and J. Stern. Lattice reduction: A toolbox for the cryptanalyst. *Journal of Cryptology*, 11(3):161–185, 1998.

[54] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Symposium on Theory of Computing.* Association for Computing Machinery, 1983.

[55] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.

[56] S. Khot. Hardness of approximating the shortest vector problem in lattices. In *45th Symposium on Foundations of Computer Science*, pages 126–135. IEEE Computer Society, 2004.

[57] R. Klima, N. Sigmon, and E. Stitzinger. *Applications of Abstract Algebra with Maple and Matlab.* Discrete Mathematics and Its Applications. Chapman and Hall/CRC, second edition, 2007.

[58] H. Koy and C. Schnorr. Segment LLL - reduction of lattice bases. In *Cryptography and Lattices Conference*, 2001.

[59] H. Koy and C. Schnorr. Segment and strong segment LLL - reduction of lattice bases. Technical report, University of Frankfurt, 2002.

[60] R. Kumar and D. Sivakumar. Complexity of SVP - a reader's digest. *SIGACT News*, 32:40–52, 2001.

[61] P. Kuo, M. Schneider, O. Dagdelen, J. Reichert, J. Buchmann, C. Cheng, and B. Yang. Extreme enumeration on GPU and in clouds - how many dollars you need to break SVP challenges. In *Cryptographic Hardware and Embedded Systems*, volume 6917, LNCS, pages 176–191. Springer, 2011.

[62] S. Lang. *Algebraic Number Theory.* Graduate Texts in Mathematics. Springer, second edition, 1994.

[63] A. Lenstra, H. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, pages 515–534, 1982.

[64] C. Ludwig. A faster lattice reduction method using quantum search. In *ISAAC*, pages 199–208, 2003.

[65] V. Lyubashevsky. *Towards Practical Lattice-Based Cryptography.* PhD thesis, University of California San Diego, 2008.

[66] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *In Automata, Languages and Programming*, volume 4052, LNCS, pages 144–155. Springer-Verlag, 2006.

[67] V. Lyubashevsky and D. Micciancio. Asymptotically efficient lattice-based digital signatures. In *Theory of Cryptography Conference '08*, 2008.

[68] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *IACR Cryptology ePrint Archive*, 2012/230, 2012.

[69] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In *Eurocrypt 2013: Advances in Cryptology.* Springer, 2013.

[70] Maple 17. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[71] A. May. *New RSA Vulnerabilities Using Lattice Reduction Methods.* PhD thesis, University of Paderborn, 2003.

[72] A. May and J. Silverman. Dimension reduction methods for convolution modular lattices. In *Cryptography and Lattices Conference*, volume 2146, LNCS, pages 110–125. Springer, 2001.

[73] R. McEliece. A public-key cryptosystem based on algebraic number theory. Dsn progress report, Jet Propulsion Laboratory, 1978.

[74] W. Mendenhall, R. Beaver, and B. Beaver. *Introduction to Probability and Statistics.* Thomson Brooks/Cole, twelfth edition, 2006.

[75] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 24:525–530, 1978.

[76] C. Meyer. *Matrix Analysis and Applied Linear Algebra.* Society for Industrial and Applied Mathematics, 2000.

[77] D. Micciancio. *On the Hardness of the Shortest Vector Problem.* PhD thesis, Massachusetts Institute of Technology, 1998.

[78] D. Micciancio. Improving lattice based cryptosystems using the Hermite normal form. In *Cryptography and Lattices Conference*, volume 2146, LNCS, pages 126–145. Springer, 2001.

[79] D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *Journal of Computing*, 30(6):2008–2035, March 2001.

[80] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst case complexity assumptions. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 356–365. IEEE, 2002.

[81] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way fuctions. *Computational Complexity*, 16(4):365–411, Dec 2007.

[82] D. Micciancio. The geometry of lattice cryptography. *Foundations of Security Analysis and Design VI*, 6858:185–210, 2012.

[83] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems - A Cryptographic Perspective.* Kluwer Academic Publishers, 2002.

[84] D. Micciancio and O. Regev. *Post-Quantum Cryptography*, chapter Lattice-Based Cryptography, pages 147–187. Springer, 2009.

[85] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *Symposium on Theory of Computing*, pages 351–358. Association for Computing Machinery, 2010.

[86] D. Micciancio and P. Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1468–1480. Society for Industrial and Applied Mathematics, 2010.

[87] R. Mollin. *Algebraic Number Theory.* Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 1999.

[88] P. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Cryptography and Lattices Conference*, pages 146–180, 2001.

[89] P. Nguyen and B. Vallee. *The LLL Algorithm - Survey and Applications*. Springer-Verlag, 2010.

[90] P. Nguyen and T. Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, July 2008.

[91] C. Peikert. Personal communication, 2012-2013.

[92] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography Conference '06*, volume 3876, pages 145–166, 2006.

[93] C. Peikert and A. Rosen. Lattices that admit worst-case to average-case connection factors. In *Symposium on Theory of Computing*, pages 478–487. Association for Computing Machinery, 2007.

[94] B. Peterson. Cartesian product of sets maple worksheet, October 2001. http://people.oregonstate.edu/~peterseb/mth355/docs/355f2001-cartesian-product.pdf

[95] T. Plantard and M. Schneider. Creating a challenge for ideal lattices. *IACR Cryptology ePrint Archive*, 2013/039, 2013.

[96] M. Pohst. On the computation of lattice vectors of minimal length, successive minima, and reduced bases with applications. *SIGSAM*, 15(1):37–44, 1981.

[97] M. Pohst. A modification of the LLL reduction algorithm. *Journal of Symbolic Computation*, 4:123–127, 1987.

[98] X. Pujol and D. Stehle. Rigorous and efficient short lattice vectors enumeration. In *Asiacrypt 2008*, volume 5350, pages 390–405, 2008.

[99] O. Regev. New lattice-based cryptographic constructions. *Journal of Association for Computing Machinery*, 51(6):899–942, 2004.

[100] O. Regev. Quantum computation and lattice problems. *SIAM Journal of Computing*, 33(3):738–760, 2004.

[101] O. Regev. Lattice-based cryptography. In *Eurocrypt 2006: Advances in Cryptology*, volume 4117, pages 131–141. Springer, 2006.

[102] M. Schneider. *Computing Shortest Lattice Vectors on Special Hardware*. PhD thesis, Technische Universitat Darmstadt, 2011.

[103] M. Schneider. Sieving for shortest vectors in ideal lattices. *IACR Cryptology ePrint Archive*, 2011/458, 2011.

[104] C. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[105] C. Schnorr. Factoring integers and computing discrete logarithms via diophantine approximation. *Eurocrypt 1991: Advances in Cryptology*, 547, LNCS:281–293, 1991.

[106] C. Schnorr. Block Korkin-Zolotarev bases and successive minima. *Combinatorics, Probability, and Computing*, 3:507–533, 1994.

[107] C. Schnorr. New practical algorithms for approximate shortest lattice vector, 2001.

[108] C. Schnorr. Accelerated and improved slide- and LLL-reduction. *Electronic Colloquium on Computational Complexity*, TR11-050, 2011.

[109] C. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–199, 1994.

[110] C. Schnorr and H. Horner. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. *Eurocrypt 1995: Advances in Cryptology*, 921:1–12, 1995.

[111] P. Shor. Algorithms for quantum computation: Discrete log and factoring. *35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[112] V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press, 2008.

[113] M. Simachew. A survey on euclidean number fields. Master's thesis, University of Bordeaux, 2009.

[114] D. Stehle and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Eurocrypt 2011: Advances in Cryptology*, pages 27–47, 2011.

[115] D. Stehle, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *Asiacrypt 2009*, volume 5912, LNCS, 2009.

[116] W. Stein. A brief introduction to classical and adelic algebraic number theory. http://modular.math.washington.edu/papers/ant/, 2004.

[117] M. Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In *Eurocrypt 2003: Advances in Cryptology*, volume 2656, LNCS, pages 433–448, 2003.

[118] J. van de Pol. Lattice-based cryptography. Master's thesis, Eindhoven University of Technology, 2011.

[119] O. Vasilenko. *Number-Theoretic Algorithms in Cryptography.* American Mathematical Society, 2007.

[120] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, 2003.

APPENDICES

Appendix A

Experiment 1 Results

Table A.1 contains the empirical data gathered from the first Principal Ideal Lattice experiment. In this experiment, a total of 1068 random principal ideals were sampled from each ring $\mathbb{Z}[x]/(\Phi_m(x))$ for $m = 1, \ldots, 100$ with $\varphi(m) > 2$. The number of successes in each cyclotomic index is reflected in this table, along with the computed sample proportion. Of the 101,460 total trials performed across the cyclotomic indices m with $\varphi(m) > 2$, the total number of successes was 100,753. This is an overall 99.3% success rate.

Table A.1: Complete Experiment 1 Results

Index m	$\varphi(m)$	Successes	Samples	Percentage
1	1	–	–	100.00%
2	1	–	–	100.00%
3	2	–	–	100.00%
4	2	–	–	100.00%
5	4	1068	1068	100.00%
6	2	–	–	100.00%
7	6	1066	1068	99.81%
8	4	1068	1068	100.00%
9	6	1046	1068	97.94%
10	4	1068	1068	100.00%
11	10	1063	1068	99.53%
12	4	1067	1068	99.91%
13	12	1059	1068	99.16%
14	6	1068	1068	100.00%
15	8	1067	1068	99.91%
16	8	1020	1068	95.51%
17	16	1056	1068	98.88%
18	6	1038	1068	97.19%
19	18	1059	1068	99.16%
20	8	1055	1068	98.78%
21	12	1052	1068	98.50%
22	10	1062	1068	99.44%
23	22	1056	1068	98.88%
24	8	1043	1068	97.66%
25	20	1045	1068	97.85%
26	12	1061	1068	99.34%
27	18	1038	1068	97.19%
28	12	1056	1068	98.88%
29	28	1058	1068	99.06%
30	8	1068	1068	100.00%
31	30	1055	1068	98.78%
32	16	1016	1068	95.13%
33	20	1062	1068	99.44%
34	16	1056	1068	98.88%

Table A.1 Continued

Index m	$\varphi(m)$	Successes	Samples	Percentage
35	24	1064	1068	99.63%
36	12	1063	1068	99.53%
37	36	1060	1068	99.25%
38	18	1058	1068	99.06%
39	24	1065	1068	99.72%
40	16	1058	1068	99.06%
41	40	1061	1068	99.34%
42	12	1048	1068	98.13%
43	42	1061	1068	99.34%
44	20	1065	1068	99.72%
45	24	1068	1068	100.00%
46	22	1057	1068	98.97%
47	46	1062	1068	99.44%
48	16	1051	1068	98.41%
49	42	1064	1068	99.63%
50	20	1049	1068	98.22%
51	32	1063	1068	99.53%
52	24	1063	1068	99.53%
53	52	1063	1068	99.53%
54	18	1035	1068	96.91%
55	40	1068	1068	100.00%
56	24	1067	1068	99.91%
57	36	1065	1068	99.72%
58	28	1057	1068	98.97%
59	58	1057	1068	98.97%
60	16	1064	1068	99.63%
61	60	1066	1068	99.81%
62	30	1065	1068	99.72%
63	36	1068	1068	100.00%
64	32	1046	1068	97.94%
65	48	1068	1068	100.00%
66	20	1064	1068	99.63%
67	66	1065	1068	99.72%

Table A.1 Continued

Index m	$\varphi(m)$	Successes	Samples	Percentage
68	32	1067	1068	99.91%
69	44	1066	1068	99.81%
70	24	1067	1068	99.91%
71	70	1067	1068	99.91%
72	24	1068	1068	100.00%
73	72	1066	1068	99.81%
74	36	1059	1068	99.16%
75	40	1067	1068	99.91%
76	36	1067	1068	99.91%
77	60	1068	1068	100.00%
78	24	1066	1068	99.81%
79	78	1060	1068	99.25%
80	32	1068	1068	100.00%
81	54	1064	1068	99.63%
82	40	1060	1068	99.25%
83	82	1062	1068	99.44%
84	24	1068	1068	100.00%
85	64	1068	1068	100.00%
86	42	1061	1068	99.34%
87	56	1067	1068	99.91%
88	40	1068	1068	100.00%
89	88	1063	1068	99.53%
90	24	1067	1068	99.91%
91	72	1068	1068	100.00%
92	44	1066	1068	99.81%
93	60	1068	1068	100.00%
94	46	1064	1068	99.63%
95	72	1068	1068	100.00%
96	32	1063	1068	99.53%
97	96	1061	1068	99.34%
98	42	1062	1068	99.44%
99	60	1068	1068	100.00%
100	40	1067	1068	99.91%

Appendix B

Maple$^{\text{TM}}$ Code

The Powerful Basis

Given a cyclotomic index m as input, the Maple$^{\text{TM}}$ procedures below were used to compute and output the powerful basis of O_{K_m}. The procedure *powerfulbasis* makes great use of the *mcarp* procedure found in [94]. These procedures require the Maple$^{\text{TM}}$ packages listed below.

```
with(ArrayTools): with(combinat, cartprod): with(LinearAlgebra):
with(ListTools): with(numtheory):
```

```
mcarp:=proc()
   local Z,k,x,y; option remember;
   if nargs=0 then
         Z:={};
      elif nargs=1 then
         Z:=args[1];
      else Z:={};
      for x in mcarp(seq(args[k], k=1 .. nargs-1)) do
         for y in args[nargs] do
            Z:=Z union{[op(x),y]};
         od;
      od;
   fi;
   return Z;
end proc:
```

```
primepowerdecomp:=proc(a::integer)
   local x,L,M,K,count,i;
   x:=a;
   L:=convert(factorset(x),list,nested=false);
   M:=[$1 .. nops(L)];
   K:=[$1 .. nops(L)];
   for i from 1 to nops(L) do
      count:=0;
      x:=x/L[i];
      while type(x,integer)=true do
         count:=count+1;
         x:=x/L[i];
      od;
      M:=subsop(i=count,M);
      x:=a;
   od:
   for i from 1 to nops(L) do
      K:=subsop(i=[L[i],M[i]],K);
   od;
   return K;
end proc:
```

```
powerfulbasis:=proc(m::integer)
   local x,L,B,K,M,i,j,Z,z,expo,R;
   x:=m;
   L:=convert(factorset(x),list,nested=false);
   K:=L;
   if nops(L)=1 then B:=[$0 .. phi(x)-1];
      else R:=primepowerdecomp(x);
         R:=convert(R,list,nested=false);
         for i from 1 to nops(L) do
            K[i]:=[$0 .. (phi(R[i][1]^(R[i][2]))-1)];
         od;
         for i from 1 to nops(K) do
            for j from 1 to nops(K[i]) do
               K[i][j]:=(K[i][j]*x)/(R[i][1]^(R[i][2]));
            od;
         od;
         M:=mcarp(seq(K[i],i=1 .. nops(K)));
         M:=convert(M,list,nested=false);
         for i from 1 to nops(M) do
            M[i]:=add(M[i][j],j=1 .. nops(M[i]));
            M[i]:=M[i] mod m;
         od;
         B:=sort(MakeUnique(Flatten(M)));
   fi;
   for i from 1 to nops(B) do
      Z[i]:=z;
   od;
   expo:=(x,y)--> x^y:
   B:=zip(expo,Z,B);
   return B;
end proc:
```

```
### Return TRUE if powerful basis is the power basis and FALSE if not.
check1:=proc(a::integer)
   local x,d,s;
   x:=a;
   d:=convert(factorset(x),list,nested=false);
   s:=nops(d);
   if s>1 then return "FALSE" else return "TRUE";
   fi;
end proc:

### Return TRUE if powerful basis is some power basis and FALSE if not.
check2:=proc(a::integer)
   local x,d,s;
   x:=a;
   if x mod 2=0 then x:=x/2 else x:=s;
   fi;
   d:=convert(factorset(x),list,nested=false);
   s:=nops(d);
   if s>1 then return "FALSE" else return "TRUE";
   fi;
end proc:
```

Principal Ideal Lattice Experiments

The Maple$^{\mathrm{TM}}$ procedures *PIGenerator*, *integervector*, *AssociateTest*, and *Experiment1* were used in the first principal ideal lattice experiment to generate a specified number of random principal ideal lattices arising from a given cyclotomic index, construct a rotation basis matrix for each of these principal ideal lattices, run the LLL algorithm on this particular lattice basis, and test whether or not the shortest vector output by LLL was an associate of the principal ideal's generator.

The procedure *Experiment2* performs a similar experiment on a specified number of random principal ideal lattices arising from cyclotomic rings with random index in some given range $[a, b]$ of cyclotomic indices. We require $3 \leq a < b$ to exclude the one-dimensional cases. Note that if $a = b$ then the second principal ideal lattice experiment is equivalent to the first. The Maple$^{\text{TM}}$ packages listed below are required.

```
with(ArrayTools): with(combinat): with(IntegerRelations):
with(LinearAlgebra): with(numtheory): with(PolynomialTools):
with(RandomTools):
```

```
PIGenerator:=proc(m::integer)
   local MthCyclo,n,g;
   MthCyclo:=cyclotomic(m,x);
   n:=degree(MthCyclo,x);
   g:=Generate(nonzeroint(range=-99 .. 99))+
   x*randpoly(x,coeffs=rand(-99 .. 99),
   degree=Generate(integer(range=0 .. n-2)),
   terms=Generate](integer(range=1 .. n-1)));
   return g;
end proc:
```

```
integervector:=proc(u::Vector)
   local count, i;
   count:=0;
   for i from 1 to Dimension(u) do
      if type(u[i],integer)=true then count:=count+0;
         else count:=count+1;
      fi;
   od;
   if count=0 then return Yes;
      else return No;
   fi;
end proc:
```

```
AssociateTest:=proc(m::integer)
   local p,pvec,gen,genvec,M,i,RotBasis,RotBasisLLL,e1,LLL1,h,RotH,u;
   p:=cyclotomic(m,x): pvec:=CoefficientVector(p,x):
   gen:=PIGenerator(m): genvec:=CoefficientVector(gen,x):
   genvec:=Vector[column]([genvec[],ZeroVector(degree(p)
      -Dimension(genvec))]): M:=Matrix(phi(m),phi(m)):
   for i from 1 to phi(m)-1 do
      M[i+1,i]:=1;
   od;
   for i from 1 to phi(m) do
      M[i,phi(m)]:=-CoefficientVector(p,x)[i];
   od; RotBasis:=Matrix(<genvec>):
   for i from 1 to phi(m)-1 do
      RotBasis:=<RotBasis|<MatrixVectorMultiply(M^i,genvec)>>;
   od; RotBasisLLL:=Transpose(LLL(Transpose(RotBasis))):
   e1:=Vector[column](phi(m)): e1[1]:=1: LLL1:=RotBasisLLL[ .. ,1];
   h:=LinearSolve(RotBasis,LLL1): RotH:=Matrix(<h>):
   for i from 1 to phi(m)-1 do
      RotH:=<RotH|<MatrixVectorMultiply(M^i,h)>>;
   od; u:=LinearSolve(RotH,e1):
   return integervector(u);
end proc:
```

```
samples:=1068; ## Enter the number of samples desired.
Experiment1:=proc(m::integer)
   local i,v,count;
   v:=[];
   for i from 1 to samples do
      v:=[v[],AssociateTest(m)];
   od;
   count:=0;
   for i from 1 to samples do
      if v[i]=Yes then count:=count+1;
         else count:=count+0;
      fi;
   od;
   print(Number of Successes=count, Number of Samples=samples);
end proc:
```

```
samples:=385; ## Enter the number of samples desired.
## Input integers 3 <= a < b for desired range of cyclotomic indices.
w:=convert(Generate(list(integer(range=a .. b),samples)),Vector):
Experiment2:=proc(v::Vector)
## Input the generated vector, w, of random cyclotomic indices.
   local i,count;
   count:=0;
   for i from 1 to Dimension(v) do
      v[i]:=AssociateTest(v[i]):
      if v[i]=Yes then count:=count+1;
      fi;
   od;
   count:=0;
   print(Number of Successes=count, Number of Trials=Dimension(v));
end proc:
```