DISCRETE MATHEMATICS

Master thesis
Code Design for Rayleigh Fading Channels using Algebraic Number Theory

Terkel Haar Jakobsen
Thomas Dam Petersen

Under the supervision of
Oliver Wilhelm Gnilke

AALBORG UNIVERSITY
STUDENT REPORT

School of Engineering and Science
Department of Mathematical Sciences
Skjernvej 4a
9000 Aalborg
http://www.math.aau.dk/

Title:

Code Design for Rayleigh Fading Channels using Algebraic Number Theory

Project:

Master thesis

Project period:

Spring 2020

Project group:

5.239b

Participants:

Terkel Haar Jakobsen
Thomas Dam Petersen

Supervisor:

Oliver Wilhelm Gnilke

number of pages: 73
Finished the 3rd of june 2020

Abstract:

In this report we investigate how algebraic number theory can be used to construct lattice codes used in wireless communication systems. We give the desired properties of such codes in both the case of a single input single output system (SISO) as well as a multiple input multiple output system (MIMO), and show how codes with the desired properties can be obtained in the SISO case and in the case of 2 transmit and 2 receive antennas using algebraic number theory. We also describe a decoding algorithm, known as the sphere decoder, which efficiently solves the closest vector problem. The sphere decoder is implemented in MATLAB and is used to simulate the error rates of the different coding schemes.

1 Danish Resume

I denne specialeafhandling undersøger vi, hvordan algebraisk talteori kan bruges til at konstruere gitre til brug i trådløse kommunikationssystemer. I første omgang beskæftiger vi os med systemer bestående af en enkelt sendeantenne og en enkelt modtageantenne. I dette system bliver beskeder sendt i form af vektorer taget fra en mængde af gitterpunkter. Vi er på udkig efter gitre med maksimal diversitet, hvilket defineres i kapitel 4 som et gitter, hvor koefficienterne er forskellig fra 0 for alle ikke-nul punkter i gitteret. Blandt gitre med maksimal diversitet er gitre med høj minimal produktafstand at foretrække. For et n-dimensionelt gitter, Λ, er den minimale produktafstand givet ved:

$$d_{p,min}(\Lambda) = \min \left\{ \prod_{j=1}^{n} |x_j| \;\middle|\; \mathbf{x} \in \Lambda, \mathbf{x} \neq \mathbf{0} \right\}.$$

For at konstruere disse gitre, beskriver vi algebraiske tallegemer og kanoniske indlejringer af disse i de komplekse tal i kapitel 5. Vi viser, at der findes præcis n kanoniske indlejringer af et tallegeme af grad n. Ved hjælp af disse kanoniske indlejringer, anvendt på ringen af algebraiske heltal i et totalt reelt tallegeme, konstruerer vi generatormatricen for et gitter med maksimal diversitet. Ved at anvende en såkaldt snoet kanonisk indlejring på en base for et ideal af heltalsringen af et totalt reelt tallegeme, kan vi konstruere et gitter med maksimal diversitet og følgende minimale produktafstand:

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{|disc_K|}}. \tag{1.1}$$

For at gøre afkodning af den transmitterede besked lettere, ønsker vi at anvende et gitter, som er en roteret version af $\mathbb{Z}^n$. Vi viser, hvordan sådanne gitre kan konstrueres ud fra cyklotomiske tallegemer.

I kapitel 7 beskæftiger vi os med et system med flere sender- og modtagerantenner, hvor beskederne sendes som matricer. Vi opstiller en række kriterier, som matricerne skal opfylde. Vi beskriver, hvordan en 2×2 matrixkode, der opfylder kriterierne, kan konstrueres ud fra en cyklisk divisionsalgebra. Denne kode kaldes den gyldne kode.

I kapitel 6 beskriver vi en algoritme, kaldet sphere decoder, som kan bruges til effektivt at afkode beskederne. Vi simulerer 10^7 sendte beskeder og bruger sphere decoderen til at afkode beskederne, og beregner derudfra fejlraten for de forskellige konstruktioner.

Preface 2

This master thesis was written in the spring of 2020 during the dark times of the COVID-19 pandemic by two mathematics students from Aalborg University. The framework for the project is discrete mathematics with focus on algebraic number theory. We refer to our literature in the Vancouver format. At the beginning of each section, it is stated which source the particular section is based on. If other sources are used in the section, it will be referenced immediately after the given statement.

Definitions, theorems, propositions, lemmas, corollaries and examples are numbered by section, while equations are numbered by chapter. When referring to these, it is done by writing "by Theorem x", or "by Equation (x)", if it is an equation. A proof ends with a black square and an example ends with a blank square. Both are in the lower right corner.

Understanding this project requires knowledge of basic algebra including group, ring and field theory as well as basic linear algebra and probability theory.

We would like to thank our supervisor Oliver Wilhelm Gnilke.

Contents

Introduction 3

Rayleigh fading models are used to model the effect of the surrounding environment on a radio signal in wireless communication. Reflection, diffraction and scattering degrades the signal as it travels from the transmitter to the receiver [17]. In the case of a single transmit antenna and a single receive antenna, known as a single input, single output system (SISO), information is transmitted using $n-$dimensional real vectors, $\mathbf{x} = [x_1, \ldots, x_n]^T$, as codewords. These codewords are taken from some finite set $S \subseteq \mathbb{R}^n$ called a signal constellation. In this thesis, we assume that the wireless channel can be modeled as an independent Rayleigh flat fading channel. This means that if we assume that perfect channel state information is available at the receiver, the model is given by [12, p.342]:

$$\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n}, \tag{3.1}$$

where $*$ denotes componentwise multiplication, $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]^T$ is a vector of independent real Rayleigh distributed random variables and $\mathbf{n} = [n_1, \ldots, n_n]^T$ is a vector of independent and identically distributed normal random variables with mean 0 and variance $\frac{N_0}{2}$, i.e. Gaussian white noise.

The goal is for the receiver to be able to decode the received signal, $\mathbf{r}$. We assume that the receiver knows the coefficients α_i. Then maximum likelihood detection requires minimization of the following metric [12, p. 342]:

$$m(x \mid \mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2. \tag{3.2}$$

The minimization of this metric can be very complex. However if the signal constellation is a subset of the lattice, $\Lambda = \{\mathbf{x} = M\boldsymbol{\lambda} \mid \boldsymbol{\lambda} \in \mathbb{Z}^m\}$, it is possible to apply a more efficient algorithm, called the sphere decoder, in order to decode the message. This algorithm is presented in chapter 6.

Not all lattices are equally suitable for constructing signal constellations. We want to use a constellation which minimizes the probability of making an error when decoding a received signal, i.e. minimize the probability that the metric in Equation (3.2) leads to the wrong constellation point $\mathbf{x}$. We call this the codeword error probability of the constellation, $P_e(S)$. Since S only consists of a finite subset of the entire lattice, we have $P_e(S) \leq P_e(\Lambda)$, where $P_e(\Lambda)$ is the probability that the metric in Equation (3.2) leads to the wrong point $\mathbf{x}$, when considering the

entire lattice. We then have:

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{\mathbf{y} \neq \mathbf{x}} P(\mathbf{x} \to \mathbf{y}), \tag{3.3}$$

where the sum runs over all the lattice points $\mathbf{y}$, which are different from the transmitted signal $\mathbf{x}$, and where $P(\mathbf{x} \to \mathbf{y})$ denotes the probability that the transmitted message $\mathbf{x}$ is decoded as the point $\mathbf{y}$. For large signal to noise ratios we have [12, p. 343]:

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2} \frac{(4N_0)^l}{d_p^{(l)}(\mathbf{x}, \mathbf{y})^2} \tag{3.4}$$

where

$$d_p^{(l)}(\mathbf{x}, \mathbf{y}) = \prod_{x_i \neq y_i} |x_i - y_i| \tag{3.5}$$

is called the *l-product distance* of $\mathbf{x}$ and $\mathbf{y}$, when $\mathbf{x}$ and $\mathbf{y}$ differ in l components. Let $L = \min(l)$ be the minimum number of distinct components between any two constellation points. We call L the *diversity order*. The dominant terms in 3.3 are found for $l = L$, and among the terms with the same diversity order, the dominant term is found for $d_{p,min} = \min d_p^{(L)}$ [12, p. 343]. If the diversity order L equals the dimension of the lattice n, the constellation is said to have *maximal diversity*. The object of the first chapters of this report is therefore to find maximal diversity lattice constructions with high $d_{p,min}$.

Advances in wireless communications has led to systems of multiple transmit and receive antennas in order to increase the data rates. The result is a more complex coding problem, where information is transmitted as matrices [14, p. 3]. We treat this case in chapter 7, with focus on the case of 2 transmit and 2 receive antennas, and a matrix code called the golden code.

Lattice Theory 4

In order to construct maximal diversity lattices, we will need some elementary lattice theory.

4.1 Elementary Lattice Theory

This section is based on [12, ch. 3].

We start by simply defining what we mean by the term lattice.

Definition 4.1.1 (Lattice, basis, dimension)

Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ be a set of linearly independent vectors in $\mathbb{R}^n$. A *lattice* is a set of points in $\mathbb{R}^n$ of the form

$$\Lambda = \left\{ \mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i \mid \lambda_i \in \mathbb{Z} \right\}. \tag{4.1}$$

The *dimension* of the lattice is m, and $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a *basis* of the lattice.

Note that $span(\Lambda)$ is an m-dimensional vector subspace of $\mathbb{R}^n$. So associating each vector $\mathbf{v}_1, \ldots \mathbf{v}_m$ with the corresponding basis vector in $\mathbb{R}^m$, we have for each element of Λ, a unique corresponding vector in $\mathbb{R}^m$. Thus we can consider $(\Lambda, +)$ a subgroup of $(\mathbb{R}^m, +)$, since for every $\mathbf{x}_1 \in \Lambda$ and $\mathbf{x}_2 \in \Lambda$ we have $(\mathbf{x}_1 - \mathbf{x}_2) \in \Lambda$.

For any given lattice, the basis can be chosen in many different ways. This can be seen in Figure 4.1, where 2 different bases $\{\mathbf{v}_1, \mathbf{v}_2\}$ and $\{\mathbf{u}_1, \mathbf{u}_2\}$ are shown. The basis vectors all span, what is known as a fundamental parallelotope.

Definition 4.1.2 (Fundamental parallelotope)

Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be the basis vectors of a given lattice. The parallelotope consisting of the points

$$c_1\mathbf{v}_1 + \ldots + c_m\mathbf{v}_m, \quad 0 \leq c_i < 1 \tag{4.2}$$

is called a *fundamental parallelotope* of the lattice.

The fundamental parallelotope constitutes a fundamental region, which means that if repeated, the fundamental parallelotope can fill the entire space with exactly one lattice point in each copy of the parallelotope.

Definition 4.1.3 (Generator matrix, Gram matrix)
Given a lattice with basis vectors:

$$\mathbf{v}_1 = \begin{bmatrix} v_{11} \\ v_{12} \\ \vdots \\ v_{1n} \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} v_{21} \\ v_{22} \\ \vdots \\ v_{2n} \end{bmatrix}, \ldots, \mathbf{v}_m = \begin{bmatrix} v_{m1} \\ v_{m2} \\ \vdots \\ v_{mn} \end{bmatrix},$$

We define the *generator matrix*, M, for the lattice as:

$$M = \begin{bmatrix} v_{11} & v_{21} & \ldots & v_{m1} \\ v_{12} & v_{22} & \ldots & v_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \ldots & v_{mn} \end{bmatrix}. \tag{4.3}$$

The matrix $G = M^T M$ is called a *Gram matrix* for the lattice.

Using the generator matrix, the lattice can now be defined as:

$$\Lambda = \{\mathbf{x} = M\boldsymbol{\lambda} \mid \boldsymbol{\lambda} \in \mathbb{Z}^m\}.$$

From Definition 4.1.3, it is seen that the (i, j)th entry of the Gram matrix is the inner product $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \mathbf{v}_i^T \mathbf{v}_j$.

Definition 4.1.4 (Integral lattice)
A lattice is said to be *integral* if all entries of its Gram matrix are in $\mathbb{Z}$.

Now, it might not be clear from the above that an integral lattice is well-defined. It must be independent of choice of basis, and thus of choice of Gram matrix. The following proposition shows that this is the case, since if one Gram matrix is an integer matrix so is every other Gram matrix.

Proposition 4.1.5
A lattice is integral if and only if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \Lambda$

Proof.
Assume Λ is an integral lattice, and let $\mathbf{x}, \mathbf{y} \in \Lambda$, where $\mathbf{x} = \sum_{i=1}^m \lambda_i \mathbf{v}_i$ and $\mathbf{y} = \sum_{j=1}^m \mu_j \mathbf{v}_j$ with $\lambda_i, \mu_j \in \mathbb{Z}$. Then $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^m \sum_{j=1}^m \lambda_i \mu_j \mathbf{v}_i^T \mathbf{v}_j$. Since Λ is integral, $\mathbf{v}_i^T \mathbf{v}_j \in \mathbb{Z}$ for all i, j, so that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$. The other implication is trivial. ■

For our purpose we will only need to consider *full-rank lattices*, i.e. n-dimensional lattices in $\mathbb{R}^n$. Thus from this point on, when we write lattice, we always mean a full-rank lattice. For these lattices the generator matrix is square, and thus the absolute value of the determinant of the generator matrix is the volume of the fundamental parallelotope.

Definition 4.1.6 (Volume of a lattice)
The *volume of a lattice* Λ is the volume of the fundamental parallelotope:

$$vol(\Lambda) = |\det(M)| = \sqrt{\det(G)}.$$

Since the fundamental parallelotope is a fundamental region, we can think of each lattice point as occupying the volume $vol(\Lambda)$ in $\mathbb{R}^n$.

Definition 4.1.7 (Determinant of a lattice)
The *determinant of a lattice* Λ with Gram matrix G is defined as:

$$\det(\Lambda) = \det(G) = (\det(M))^2.$$

Since the volume of the fundamental parallelotope is independent of the choice of lattice basis (see Figure 4.1), the determinant of the lattice is also independent of the choice of basis. We say it is an *invariant of the lattice*. From the above definitions it is clear that $vol(\Lambda) = \sqrt{\det(\Lambda)}$.

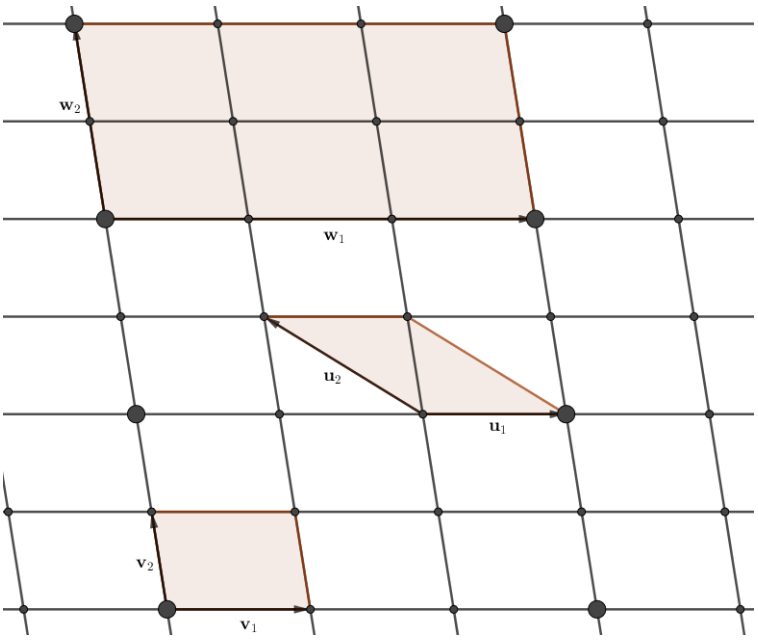

Figure 4.1: *The small points constitute a 2-dimensional lattice in* $\mathbb{R}^2$ *with bases* $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ *and* $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$. *The larger points constitute a sublattice with basis* $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$. *The shaded parallelograms are fundamental parallelotopes of the respective lattices.*

Next we give two definitions, which are important when applying lattice theory to code design for fading channels.

Definition 4.1.8 (Diversity)
Let Λ be an n-dimensional lattice. Let m be the maximal number of coefficients that are 0 of all non-zero points in the lattice. Then the *diversity* of the lattice is $n - m$. If the diversity of Λ is n, we call Λ a *maximal diversity lattice*.

For example the lattice in Figure 4.1 has diversity 1. As mentioned in the introduction, we shall be particularly interested in maximal diversity lattices with high minimum product distance.

Definition 4.1.9 (Minimum product distance)
The *minimum product distance* of a maximal diversity, $n-$dimensional lattice, Λ, is given by:

$$d_{p,min}(\Lambda) = \min \left\{ \prod_{j=1}^{n} |x_j| \;\middle|\; \mathbf{x} \in \Lambda, \mathbf{x} \neq \mathbf{0} \right\}. \tag{4.4}$$

Definition 4.1.10 (Sublattice)
Let Λ be a n-dimensional lattice and M a generator matrix for the lattice. A *sublattice* of Λ is given by:

$$\Lambda' = \{\mathbf{x} = MB\boldsymbol{\lambda} \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}, \tag{4.5}$$

where B is an $n \times n$ integer matrix.

As previously mentioned the lattice, Λ, has a group structure, and therefore the sublattice, Λ', is a normal subgroup of Λ, which allows us to consider the quotient group Λ/Λ'. Similarly to the index of a subgroup, we now define the index of a sublattice.

Definition 4.1.11 (Index of the sublattice)
Let Λ' be a sublattice as defined in definition 4.1.10. The *index* of Λ' is the cardinality of the quotient group Λ/Λ'.

Proposition 4.1.12
Let Λ' be a sublattice of a lattice, Λ. Then the index of Λ' is given by:

$$|\Lambda/\Lambda'| = \frac{vol(\Lambda')}{vol(\Lambda)} = \frac{|\det(MB)|}{|\det(M)|} = |\det(B)|. \tag{4.6}$$

Proof.
The cardinality of the quotient group is the number of cosets $\mathbf{x} + \Lambda'$ of Λ' in Λ, whereby $\mathbf{x} \in \Lambda$. Let S be a set containing exactly one element of each coset of Λ'. Note that $|S| = |\Lambda/\Lambda'|$ is clearly finite since the number of lattice points of Λ within a fundamental parallelotope of Λ'

is finite, and any point outside of the parallelotope is in the same coset as some point within it. For the same reason we may assume without loss of generality that all the points of S belong to the same fundamental parallelotope of Λ'. Since this parallelotope is a fundamental region, we may fill all space with copies of it. But by doing so, we also reconstruct all of Λ by copying the points of S, since we know from group theory that [8, p. 63]:

$$\Lambda = \bigcup_{\mathbf{x} \in S} (\mathbf{x} + \Lambda').$$

This implies that $vol(\Lambda') = |S| vol(\Lambda)$, and the first equality follows. The second equality follows from Definition 4.1.6, while the third follows from elementary linear algebra. ■

Example 4.1.13
In figure 4.1 a lattice with basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ as well as a sublattice with basis $\{\mathbf{w}_1, \mathbf{w}_2\}$ is shown. We have:

$$\begin{bmatrix} \mathbf{w}_1 & \mathbf{w}_2 \end{bmatrix} = MB = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} B = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}.$$

We see that the determinant of B and therefore also the cardinality of the quotient group is 6. The elements of Λ/Λ' can be written as $\{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$ and the group operation is component-wise addition modulo 3 and 2 respectively. □

4.2 Equivalent Lattices

This chapter is based on [12, ch. 3].
For any lattice a simple way to find a sublattice is to compute it's scaled version by an integer factor.

Definition 4.2.1 (Scaled lattice)
Let Λ be a lattice. The lattice:

$$\Lambda' = c\Lambda, \quad c \in \mathbb{R},$$

is called a *scaled lattice* of Λ. If $c \in \mathbb{Z}$ then Λ' is a sublattice of Λ.

We say that a lattice and its scaled lattice are equivalent. More generally we make the following definition.

Definition 4.2.2 (Equivalent lattices)
Let Λ and Λ' be lattices. If Λ' can be obtained from Λ by using either a rotation, a reflection, a change of scale or a combination hereof, the lattices are said to be *equivalent*.

This means that lattices are equivalent if and only if their generator matrices M and M' are related by $M' = BMUc$, where B is a real orthogonal matrix, U is a unimodular matrix and c is a nonzero constant. To see why this holds true, we remember that a multiplication by an orthogonal matrix corresponds to performing either a rotation or a reflection, and, as we will show, a unimodular matrix can be used to relate different generator matrices of the same lattices. We first define what is meant by a unimodular matrix.

Definition 4.2.3 (Unimodular matrix [10])
A matrix $U \in \mathbb{Z}^{n\times n}$ is *unimodular* if it has a multiplicative inverse in $\mathbb{Z}^{n\times n}$, i.e. there is a matrix $V \in \mathbb{Z}^{n\times n}$ such that $VU = UV = I$.

It follows from the definition that if U is a unimodular matrix then so is its inverse. Furthermore it is easily seen that the determinant of a unimodular matrix is ± 1, since the determinant of an integer matrix is an integer.

Proposition 4.2.4 ([10])
Let M and M' be generator matrices for the lattices Λ and Λ' respectively. Then Λ=Λ' if and only if there exist a unimodular matrix U such that $M' = MU$.

Proof.
We first assume that $M' = MU$ for some unimodular matrix U. Since U is unimodular, so is U^{-1}, and they are therefore both integer matrices. Since $M' = MU$ each column in M' is an integral linear combination of the columns in M. Thus using the definition of a lattice we have that $\Lambda' \subseteq \Lambda$. The same holds true for $M = M'U^{-1}$ and it follows that $\Lambda \subseteq \Lambda'$.
We now assume that M and M' generate the same lattice i.e. $\Lambda = \Lambda'$. From the definition of a lattice it follows that there exist integer matrices U and V such that $M' = MU$ and $M = M'V$. Combining the two equations we get $M' = M'VU$, which can be rewritten as $M'(I-VU) = O$, where O is the zero matrix. Since M' has linearly independent columns, it is nonsingular, and thus $I - VU = O$, which implies that $VU = I$, by which it follows that U is unimodular. ■

To conclude this chapter we define what is meant by lattice sphere packing and coverings.

Definition 4.2.5 (Lattice sphere packing and covering, packing and covering radius)
Given a lattice, Λ, a *lattice sphere packing* is obtained by centering on every lattice point, identical spheres of maximal radius such that the spheres do not overlap. The radius of the packed spheres is called the *packing radius* of Λ.
Similarly a *lattice covering* is obtained by centering on every lattice point, identical overlapping spheres of minimal radius such that every point of space is lying on or within at least one sphere. The radius of the covering spheres is called the *covering radius* of Λ.

Note that the covering radius is also the maximum distance from any point $\mathbf{x} \in \mathbb{R}^n$ to the nearest lattice point, which will be useful to us when considering decoding in chapter 6.

Algebraic Number Theory 5

In this chapter the algebraic number theory needed to build algebraic lattice constructions will be reviewed.

5.1 Number Fields

This section is based on [12, ch. 5].
We start by considering what is meant by a field extension.

Definition 5.1.1 (Field extension [19] p. 22)
Let L be a field. If $K \subseteq L$, is a field with respect to the same operations as L restricted to K, then L is said to be an *extension field* of K. We say that K is a *subfield* of L, and the pair (L, K) is called a *field extension* denoted by L/K.

A familiar example is the field extension $\mathbb{C}/\mathbb{Q}$, where $\mathbb{C}$ is the field of complex numbers and $\mathbb{Q}$ is the field of rational numbers. Another example is an extension of $\mathbb{Q}$ obtained by "adding" $\sqrt{2}$ as well as all the multiples and all the powers of $\sqrt{2}$ to $\mathbb{Q}$. This way we can build a new field, that we denote $\mathbb{Q}(\sqrt{2})$, given by all elements of the form $x = a+b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Addition and multiplication is defined in the natural way $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2}$ and $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}$. To see that this is indeed a field, note that it is clearly closed under addition and multiplication, and that every element $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ has a multiplicative inverse $x^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. More generally, for fields $K \subseteq L$, we denote this type of field extension by some set of elements $S = \{\alpha_1, \ldots, \alpha_n\} \subseteq L$ by $K(S)$ or simply $K(\alpha_1, \ldots, \alpha_n)$. In other words, $K(S)$ is the smallest extension field of K, which contains S.

Definition 5.1.2 (Adjunction [19] p. 23)
Let L/K be a field extension, and let $S \subseteq L$ be a subset of L. The smallest subfield of L, which contains K and S is denoted by $K(S)$ and is called the *adjunction* of S to K.

Furthermore, given a field extension L/K, then L constitutes a vector space over K, where vector addition is addition in L and scalar multiplication is given by $av \in L$ for $a \in K$ and $v \in L$. The axioms required for L to be a vector space are all easily seen to be satisfied, since K and L are fields. Returning to our example of $\mathbb{Q}(\sqrt{2})$, this field forms a vector space over $\mathbb{Q}$ with basis $\{1, \sqrt{2}\}$. Therefore $\mathbb{Q}(\sqrt{2})$ has dimension 2, when considered a vector space over $\mathbb{Q}$.

Definition 5.1.3 (Finite extension)
Let L/K be a field extension. The dimension of L when considered a vector space over K is called the *degree* of L over K and is denoted by $[L : K]$. If $[L : K]$ is finite, L is said to be a *finite extension* of K.

We will be particularly interested in the finite extensions of $\mathbb{Q}$.

Definition 5.1.4 (Number field)
A finite extension of $\mathbb{Q}$ is called a *number field*.

Note that a number field, K, can be written as $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some elements $\alpha_1, \ldots, \alpha_n \in K$. To see this, take some element $\alpha_1 \in K$, such that $\alpha_1 \notin \mathbb{Q}$. If $K = \mathbb{Q}(\alpha_1)$ we are done. Otherwise, take some element $\alpha_2 \in K$ such that $\alpha_2 \notin \mathbb{Q}(\alpha_1)$ and form $\mathbb{Q}(\alpha_1, \alpha_2)$. Continuing in this manner, we will eventually get $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, since K is a finite extension.

Definition 5.1.5 (Algebraic element)
Let L/K be a field extension, and let $\alpha \in L$. If there exists a nonzero polynomial, $p \in K[X]$, such that $p(\alpha) = 0$, we call α *algebraic over* K or simply *algebraic*.

For example $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is algebraic, since it is a root of the polynomial $X^2 - 2$. Algebraic elements over $\mathbb{Q}$ are called algebraic numbers.

Let L/K be a field extension, and let $\alpha \in L$ be an algebraic element of K. Then there exists a polynomial $p \in K[X]$, such that $p(\alpha) = 0$. By dividing this polynomial by its leading coefficient, we obtain a monic polynomial, $\tilde{p}$ that also satisfy $\tilde{p}(\alpha) = 0$. Thus there exist at least one monic polynomial, $p \in K[X]$, of minimal degree such that $p(\alpha) = 0$. We claim that this polynomial is unique. To see this, assume for contradiction that another monic polynomial, q, of minimal degree such that $q(\alpha) = 0$ exists. Then we also have $(p - q)(\alpha) = 0$, but since both p and q are monic and of the same degree, $p - q$ is a polynomial of smaller degree than p and q. This is a contradiction since a monic polynomial which have α as a root can now be obtained by dividing $p - q$ by its leading coefficient. This allows us to make the following definition [18, p. 59]:

Definition 5.1.6 (Minimal polynomial)
Let L/K be a field extension, and let $\alpha \in L$ be algebraic. The unique monic polynomial, $p \in K[X]$ of minimal degree such that $p(\alpha) = 0$ is called the *minimal polynomial* of α over K. We denote the minimal polynomial of α by p_α.

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$, since there is no monic polynomial of degree one or zero over $\mathbb{Q}$, that has $\sqrt{2}$ as a root.

Proposition 5.1.7 ([18] p. 59)
Let L/K be a field extension, and let $\alpha \in L$ be algebraic. The minimal polynomial p_α is irreducible over K.

Proof.
Assume that p_α is reducible over K. Then $p_\alpha = fg$ for some polynomials $f, g \in K[X]$ with $0 < deg(f) < deg(p_\alpha)$ and $0 < deg(g) < deg(p_\alpha)$. However $p_\alpha(\alpha) = f(\alpha)g(\alpha) = 0$, but since L is a field and $f(\alpha), g(\alpha) \in L$ we have either $f(\alpha) = 0$ or $g(\alpha) = 0$. This contradicts that p_α is the minimal polynomial of α. Thus p_α is irreducible over K. ■

Definition 5.1.8 (Algebraic extension)
Let $K/\mathbb{Q}$ be a field extension. If all elements of K are algebraic over $\mathbb{Q}$, we say that K is an *algebraic extension* of $\mathbb{Q}$.

Returning to our example of $\mathbb{Q}(\sqrt{2})$ it is easily verified by insertion, that any $a + b\sqrt{2} = \alpha \in \mathbb{Q}(\sqrt{2})$ is a root of the polynomial $p_\alpha(X) = X^2 - 2aX + a^2 - 2b^2$. Thus $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of $\mathbb{Q}$.

Proposition 5.1.9 ([19] p. 23)
Let L/K be a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K(\alpha)$ is a finite extension of K.

Proof.
Let $[K(\alpha) : K] = n < \infty$, then the set of powers of α, $P_\alpha = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ constitutes a linearly dependent set in the vector space $K(\alpha)$ over K, since $|P_\alpha| > n$. It follows that α is algebraic.
We now let α be algebraic with minimal polynomial p_α of degree m. We claim that $K(\alpha)$ is the vector space over K spanned by $1, \alpha, \ldots, \alpha^{m-1}$, which we denote by V. V is obviously closed under addition and subtraction. To see that it is also closed under multiplication, note that $\alpha^m = -p_\alpha(\alpha) + \alpha^m = q(\alpha)$ has deg$(q) < m$, since the leading entry in p_α is α^m. Thus any polynomial in α can be reduced to a polynomial of degree less than m. Hence V is closed

under multiplication and thus forms a ring. To see that V is also a field we need to show that if $0 \neq v \in V$ then $v^{-1} \in V$. An element $v \in V$ can be written $v = h(\alpha)$ where $h \in K[X]$ and $\deg(h) < m$. Since p_α is irreducible and $\deg(p) > \deg(h)$, p and h are coprime, and it follows from the extended Euclidean algorithm that there exist $f, g \in K[X]$ such that:

$$f(X)p(X) + g(X)h(X) = 1 \Rightarrow \tag{5.1}$$

$$1 = f(\alpha)p(\alpha) + g(\alpha)h(\alpha) = g(\alpha)h(\alpha), \tag{5.2}$$

which shows that $\frac{1}{v} = g(\alpha) \in V$. Thus $K(\alpha)$ is in fact the vector space V. It follows that $[K(\alpha) : K] = \dim(V) = m < \infty$. ■

The above proof actually shows more than stated in the proposition.

Corollary 5.1.10
Let $K(\alpha)$ be a finite extension of K, then $[K(\alpha) : K] = \deg(p_\alpha)$, where p_α is the minimal polynomial of α over K, and $K(\alpha) = K[\alpha]$.

Proof.
This result follows from the proof of Proposition 5.1.9. ■

We now wish to show that any number field, can be build from $\mathbb{Q}$ and a single algebraic number $\theta \in K$. In order to do this we first need to define the derivative of $p \in K[X]$ and how to find the derivative of a product of polynomials. We do this in accordance with [8].

Definition 5.1.11 (Derivative)
Let K be a field and $p = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$. Then

$$D(p) = a_n n X^{n-1} + a_{n-1}(n-1)X^{n-2} + \cdots + a_1$$

is called the *derivative* of p.

We can view $K[X]$ as the set of functions $p : \mathbb{N} \to K$, such that a polynomial of degree n is given by $p(0) + p(1)X + p(2)X^2 + \cdots + p(n)X^n$, where $p(n) \neq 0$ and $p(m) = 0$ for $m > n$. The derivative can then be rephrased as $D(p)(n-1) = np(n)$ for $n \geq 1$.

Lemma 5.1.12 ([8] p. 153)
Let $p, f \in K[X]$. Then

$$D(pf) = pD(f) + D(p)f.$$

Proof.
By viewing polynomials formally as maps $\mathbb{N} \to K$, as described before the lemma, we have:

$$\begin{aligned}
(pD(f) + D(p)f)(n-1) &= \sum_{i+j=n-1} p(i)D(f)(j) + \sum_{i+j=n-1} D(p)(i)f(j) \\
&= \sum_{i+j=n-1} p(i)(j+1)f(j+1) + \sum_{i+j=n-1} (i+1)p(i+1)f(j) \\
&= \sum_{i+j=n} p(i)jf(j) + \sum_{i+j=n} ip(i)f(j) \\
&= \sum_{i+j=n} (i+j)p(i)f(j) = n \sum_{i+j=n} p(i)f(j) \\
&= n(pf)(n) = D(pf)(n-1),
\end{aligned}$$

where $n \geq 1$ and the second and last equal sign follows from the identity $D(f)(n-1) = nf(n)$. ■

Using Lemma 5.1.12 we can prove the following proposition.

Proposition 5.1.13 ([19] p. 18)
Let K be a field of characteristic zero. A nonzero polynomial p over K is divisible by the square of a polynomial of degree > 0 if and only if p and $D(p)$ have a common factor of degree > 0.

Proof.
Suppose that p is divisible by the square of a polynomial of degree > 0. That is $p = f^2 g$. Then by Lemma 5.1.12 we have:

$$D(p) = f^2 D(g) + 2fD(f)g, \tag{5.3}$$

which shows that f is a common factor of degree > 0 of p and $D(p)$.
We prove the converse statement by contraposition. Suppose that p has no squared factor. Then for any irreducible factor f of p we have that $p = fg$ where f and g are coprime. By taking the derivative, we get

$$D(p) = fD(g) + D(f)g. \tag{5.4}$$

In order for f to be common factor of p and $D(p)$, f would have to be a factor of $D(f)$ since f and g are coprime, or $D(f)$ would have to equal zero. Since $\deg(D(f)) < \deg(f)$ it follows that $D(f)$ must equal zero. Since K has characteristic zero, this implies that f is a constant. Since f was an arbitrary irreducible factor of p, this applies to all factors of p. Thus p and $D(p)$ have no common factor of degree > 0. ■

Corollary 5.1.14 ([19] p. 18)
Let $p \in K[X]$ be an irreducible polynomial and K a subfield of $\mathbb{C}$, then p has no repeated roots in $\mathbb{C}$.

Proof. Suppose p is irreducible over K. Then, by proposition 5.1.13, p and $D(p)$ must be coprime in $K[X]$, since a common factor would be a squared factor of p in contradiction with p being irreducible. It follows that there exist polynomials $g, f \in K[X]$ and hence in $\mathbb{C}[X]$ so that $gp + fD(p) = 1$. Thus p and $D(p)$ are coprime in $\mathbb{C}[X]$ and since they have no common factor of degree > 0, it follows from proposition $5.1.13$ that p has no repeated roots in $\mathbb{C}$. ■

We are now ready to prove the following proposition.

Proposition 5.1.15 ([19] p. 40)
If K is a number field then $K = \mathbb{Q}(\alpha)$ for some algebraic number α, called a *primitive element*.

Proof. Let $K = K_1(\gamma, \theta)$ where K_1 is a subfield of K. If we can show that $K = K_1(\alpha)$ for some α, then the result follows by induction. Let p and q be the minimal polynomial over K_1 of γ and θ respectively, and let their factorizations over $\mathbb{C}$ be given as:

$$p(X) = (X - \gamma_1) \dots (X - \gamma_n), \tag{5.5}$$
$$q(X) = (X - \theta_1) \dots (X - \theta_m), \tag{5.6}$$

where $\gamma_1 = \gamma$ and $\theta_1 = \theta$. From corollary 5.1.14 it follows that the roots of both polynomials are distinct. Which means that for each i and each $k \neq 1$ there is at most one $t \in K_1$ so that:

$$\gamma_i + t\theta_k = \gamma + t\theta. \tag{5.7}$$

Since there can only be a finite amount of such equations, it is possible to choose a $c \neq 0$ in K_1 so that:

$$\gamma_i + c\theta_k \neq \gamma + c\theta, \tag{5.8}$$

for all $1 \leq i \leq n$ and $2 \leq k \leq m$. We now define $\alpha = \gamma + c\theta$, and by using this definition we will prove that $K_1(\alpha) = K_1(\gamma, \theta)$. That $K_1(\alpha) \subseteq K_1(\gamma, \theta)$ is trivial, and we therefore only

need to prove that $\theta \in K_1(\alpha)$, since $\gamma = \alpha - c\theta$. We have:

$$p(\alpha - c\theta) = p(\gamma) = 0, \tag{5.9}$$

and if we define the polynomial:

$$r(X) = p(\alpha - cX) \in K_1(\alpha)[X], \tag{5.10}$$

then θ is a root in both $q(X)$ and $r(X)$ as polynomials over $K_1(\alpha)$. Now let ϵ be a common root of q and r then $\epsilon \in \{\theta_1, \ldots, \theta_m\}$ and $\alpha - c\epsilon \in \{\gamma_1, \ldots, \gamma_n\}$ or equivalently $\alpha \in \{\gamma_1 + c\epsilon, \ldots, \gamma_n + c\epsilon\}$. Since c was chosen such that $\gamma_i + c\theta_k \neq \gamma + c\theta = \alpha$ for $2 \leq k \leq m$, we have only one common root given by $\epsilon = \theta$. Now let h be the minimal polynomial of θ over $K_1(\alpha)$. Then $h(X)|q(X)$ and $h(X)|r(X)$. As we have just shown q and r have just one common root in $\mathbb{C}$, and thus $\deg(h) = 1$, so $h(X) = X + \mu$ for $\mu \in K_1(\alpha)$. Since $0 = h(\theta) = \theta + \mu$, we have that $\theta = -\mu \in K_1(\alpha)$ as required. ■

Definition 5.1.16 (Algebraic integer)
If $\alpha \in \mathbb{C}$ is a root of a monic polynomial with coefficients in the ring of integers $\mathbb{Z}$, we say that α is an *algebraic integer*.

We wish to show that the set of algebraic integers, which are contained in a number field, K, forms a ring. First we need the following important result.

Theorem 5.1.17 ([18] p. 45)
Let K, L and M be subfields of $\mathbb{C}$, such that $K \subseteq L \subseteq M$. Then

$$[M : K] = [M : L][L : K]. \tag{5.11}$$

Proof.
Let $S_1 = \{x_i \in L \mid i \in I\}$ be a basis for L as a vector space over K, and let $S_2 = \{y_j \in M \mid j \in J\}$ be a basis for M over L. We wish to show that $S = \{x_i y_j \in M \mid i \in I, j \in J\}$ is a basis for M over K, and that $|S| = |S_1||S_2|$.
We start by showing that the elements in S are linearly independent. Let:

$$\sum_{i,j} k_{ij} x_i y_j = \sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0, \quad k_{ij} \in K. \tag{5.12}$$

Since $\sum_i k_{ij} x_i \in L$ and the y_j form a basis for M over L, it follows that:

$$\sum_i k_{ij} x_i = 0, \quad \forall j \in J. \tag{5.13}$$

By the same argument for the vector space L over K we find that $k_{ij} = 0$, thus proving that the elements in S are linearly independent, and that $|S| = |S_1||S_2|$.
Now let $x \in M$, then it can be written as a linear combination of the basis vectors y_j:

$$x = \sum_j \lambda_j y_j, \tag{5.14}$$

with coefficients $\lambda_j \in L$. Similarly we have for every $j \in J$ that:

$$\lambda_j = \sum_i \lambda_{ij} x_i, \quad \lambda_{ij} \in K. \tag{5.15}$$

We thus have that:

$$x = \sum_{i,j} \lambda_{ij} x_i y_i \tag{5.16}$$

and so the $x_i y_j$ span M. ■

We will also need the following result regarding the set of all algebraic numbers.

Proposition 5.1.18 ([19] p. 39)
The set of algebraic numbers, $\mathbb{A}$, is a subfield of the field of complex numbers, $\mathbb{A} \subseteq \mathbb{C}$.

Proof.
Let $\alpha, \beta \in \mathbb{A}$ be algebraic numbers. By Proposition 5.1.9, $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$, i.e. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. Since $\beta \in \mathbb{A}$ is algebraic over $\mathbb{Q}$ it is also algebraic over $\mathbb{Q}(\alpha)$. Thus by the same Proposition $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ is finite. By Theorem 5.1.17, we have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Hence $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is finite. Thus for any element $\gamma \in \mathbb{Q}(\alpha, \beta)$, $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is finite, and thus γ is an algebraic number by Proposition 5.1.9. This implies that $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{A}$. Since $\mathbb{Q}(\alpha, \beta)$ is a field, we have $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{Q}(\alpha, \beta)$ and for $\beta \neq 0$ we have $\frac{\alpha}{\beta} \in \mathbb{Q}(\alpha, \beta)$. Hence these numbers are also contained in $\mathbb{A}$, which shows that $\mathbb{A}$ is a field. ■

Now we only need to prove that the algebraic integers is a subring of the algebraic numbers. In order to do that we need the following lemma.

Lemma 5.1.19 ([19] p. 46)
A complex number θ is an algebraic integer if and only if the additive group generated by all powers $1, \theta, \theta^2, \ldots$ is finitely generated.

Proof.
Let θ be an algebraic integer. Then for some $n \in \mathbb{N}$ and some $a_i \in \mathbb{Z}$ we have:

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0. \tag{5.17}$$

Consider the additive group, Γ, generated by $1, \theta, \ldots, \theta^{n-1}$. We prove by strong induction that all powers of θ lies in Γ. It follows from Equation (5.17) that $\theta^n \in \Gamma$. Let $m \geq n$, and assume $\theta^k \in \Gamma$ for all $k \leq m$. Then

$$\theta^{m+1} = \theta^{m+1-n}\theta^n \tag{5.18}$$

$$= \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - \ldots - a_1\theta - a_0) \tag{5.19}$$

$$= -a_{n-1}\theta^m - \ldots - a_1\theta^{m+2-n} - a_0\theta^{m+1-n} \in \Gamma \tag{5.20}$$

by the induction hypothesis. Thus every power of θ is in Γ, which proves one implication.
To prove the other implication, suppose that the additive group, Γ, generated by the powers $1, \theta, \theta^2, \ldots$ is finitely generated. Suppose that Γ has the following generators $V = \{v_1, \ldots, v_n\}$. Since Γ was also generated by $1, \theta, \theta^2, \ldots$, each $v \in V$ can be written as a polynomial in θ with integer coefficients. It follows that θv_i is also such a polynomial, and hence there exists integers $b_{ij} \in \mathbb{Z}$ such that:

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j. \tag{5.21}$$

This gives us an equation for each $v_i \in V$, which can be written as a system of homogeneous equations:

$$\begin{bmatrix} b_{11} - \theta & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} - \theta & \ldots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{nn} - \theta \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{5.22}$$

Since we have a solution $\mathbf{v} \neq \mathbf{0} \in \mathbb{C}^n$, the determinant:

$$\begin{vmatrix} b_{11} - \theta & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} - \theta & \ldots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{nn} - \theta \end{vmatrix} \tag{5.23}$$

is zero. By cofactor expansion we see that θ is a root in a monic polynomial with integer coefficients. ■

Theorem 5.1.20 ([19] p. 47)
The algebraic integers form a subring of the field of algebraic numbers.

Proof.
Let θ, ϕ be algebraic integers. The multiplicative identity, 1, is clearly an algebraic integer. Thus

by the subring test, we only need to show that $\theta - \phi$ and $\theta\phi$ are algebraic integers. By Lemma 5.1.19 there are finitely generated groups Γ_θ and Γ_ϕ containing $1, \theta, \theta^2, \ldots$ and $1, \phi, \phi^2, \ldots$ respectively. Say $v_1, \ldots, v_n$ generates Γ_θ and $w_1, \ldots, w_m$ generates Γ_ϕ. Then $\{v_i w_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ generates the additive set product group $\Gamma_\theta\Gamma_\phi = \{gh \mid g \in \Gamma_\theta,\ h \in \Gamma_\phi\}$. The set product is a group since Γ_θ and Γ_ϕ are subgroups of the abelian group $(\mathbb{C}, +)$, such that $\Gamma_\theta\Gamma_\phi = \Gamma_\phi\Gamma_\theta$, which by [16, p. 39] implies that $\Gamma_\theta\Gamma_\phi$ is a subgroup of $(\mathbb{C}, +)$. Since all powers of $\theta - \phi$ and $\theta\phi$ are linear combinations of the elements $\theta^i\phi^j \in \Gamma_\theta\Gamma_\phi$, all the powers of $\theta - \phi$ and $\theta\phi$ also lie in the group $\Gamma_\theta\Gamma_\phi$. Since $\Gamma_\theta\Gamma_\phi$ is abelian and finitely generated, the subgroups generated by all powers of $\theta - \phi$ and $\theta\phi$ respectively are also finitely generated [16, p. 36]. It follows by Lemma 5.1.19 that $\theta - \phi$ and $\theta\phi$ are algebraic integers. ■

Definition 5.1.21

Let K be a number field, and $\mathbb{B}$ the set of algebraic integers. The set

$$\mathcal{O}_K = K \cap \mathbb{B} \tag{5.24}$$

is called the *ring of integers* of K.

We see that $\mathcal{O}_K$ is a subring of K, since K and $\mathbb{B}$ are subrings of $\mathbb{C}$. Further $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ and $\mathbb{Z} \subseteq \mathbb{B}$ so $\mathbb{Z} \subseteq \mathcal{O}_K$.

Lemma 5.1.22 ([19] p. 49)

Let K be a number field. Then for $\alpha \in K$ there exists some non-zero $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_K$.

Proof.

Let $\alpha \in K$. Then α is the root of some polynomial $p_\alpha = X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \ldots + \frac{a_1}{b_1}X + \frac{a_0}{b_0}$, where $a_i, b_i \in \mathbb{Z}$ for $i = 0, \ldots, n-1$. Define $c = b_{n-1}b_{n-2}\ldots b_0$. Then α is also a root of $c^n p_\alpha \in \mathbb{Z}[X]$. This implies that $c\alpha$ is a root of the polynomial $X^n + c\frac{a_{n-1}}{b_{n-1}}X^{n-1} + \ldots + c^{n-1}\frac{a_1}{b_1}X + c^n\frac{a_0}{b_0}$, which has coefficients in $\mathbb{Z}$. Thus $c\alpha \in \mathcal{O}_K$. ■

Corollary 5.1.23 ([19] p. 49)

Let K be a number field. Then $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathcal{O}_K$.

Proof.

By Proposition 5.1.15 $K = \mathbb{Q}(\alpha)$ for some algebraic number α. By Lemma 5.1.22 there exists some non-zero $c \in \mathbb{Z}$ such that $\theta = c\alpha \in \mathcal{O}_K$. Since $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha)$ the corollary follows. ■

5.2 The Canonical Embedding

This section is based on [12, ch. 5].
In order to construct lattices from number fields, we need to consider embeddings of the number field into $\mathbb{C}$. These are introduced in this section.

Definition 5.2.1 (Free module [16] p. 335)
Let R be a commutative ring (with multiplicative identity, 1). An *R-module* is an abelian group M together with a scalar multiplication that assigns to each pair $(r, u) \in R \times M$, an element $ru \in M$, such that the following holds for all $r, s \in R$ and $u, v \in M$:

$$\begin{aligned} r(u+v) &= ru + rv \\ (r+s)u &= ru + su \\ (rs)u &= r(su) \\ 1u &= u. \end{aligned}$$

The elements of R are called scalars. If M has a basis consisting of n elements, then we call M a *free module of rank n*.

In the above definition, a basis is defined in the usual sense. That is, a basis is a set $B = \{b_1, \ldots, b_n\} \subseteq M$ such that the elements are linearly independent:

$$r_1 b_1 + \ldots + r_n b_n = 0_M \implies r_1 = \ldots = r_n = 0_R, \quad \text{for } r_1, \ldots, r_n \in R,$$

and such that B generates M. That is, any $u \in M$ can be written as a linear combination of the elements of B:

$$u = r_1 b_1 + \ldots + r_n b_n, \quad \text{where } r_1, \ldots, r_n \in R.$$

Proposition 5.2.2
Let K be a number field of degree n. The ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n.

Proof.
The proof will be postponed for now, but can be found on page 30. ■

We will be particularly interested in a certain form of basis.

Definition 5.2.3 (Integral basis)
Let $\{\omega_1, \omega_2 \cdots, \omega_n\}$ be a basis of the $\mathbb{Z}$-module $\mathcal{O}_K$, so that any element $\beta \in \mathcal{O}_K$ can be written $\beta = \sum_{i=1}^{n} a_i \omega_i$ with $a_i \in \mathbb{Z}$. Then $\{\omega_1, \omega_2 \cdots, \omega_n\}$ is called an *integral basis* for K.

We now turn our attention to how a number field K can be represented, or as we say embedded, into $\mathbb{C}$.

Definition 5.2.4 ($\mathbb{Q}$-homomorphism)
Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be two field extensions. A $\mathbb{Q}$-*homomorphism* is a ring homomorphism $\varphi : K \to L$ that satisfies $\varphi(a) = a$ for all $a \in \mathbb{Q}$.

Definition 5.2.5 (Embedding of number field into $\mathbb{C}$)
Let K be a number field. An *embedding* of K into $\mathbb{C}$ is a $\mathbb{Q}$-homomorphism $\varphi : K \to \mathbb{C}$.

Note that an embedding is injective since K is a field. To see this, assume that for some $\alpha \in K$, $\alpha \neq 0$ we have $\sigma_i(\alpha) = 0$. Then

$$1 = \sigma_i(1) = \sigma_i(\alpha\alpha^{-1}) = \sigma_i(\alpha)\sigma_i(\alpha^{-1}) = 0,$$

which is a contradiction. To describe the embeddings of a number field into $\mathbb{C}$ we first need the notion of isomorphic field extensions. To define this, note that a field extension L/K can be thought of as a monomorphism (an injective field homomorphism) $j : K \to L$. Up until this point we have thought of elements $k \in K$ as also lying in the extension field $k \in L$. But with the monomorphism formulation, we can distinguish between the element $k \in K$ and the image $j(k) \in L$.

Definition 5.2.6 (Isomorphic field extensions [18] p. 33)
Let $i : K \to L$ and $j : \tilde{K} \to \tilde{L}$ be field extensions. If there exists field isomorphisms $\lambda : K \to \tilde{K}$ and $\mu : L \to \tilde{L}$ such that for any $k \in K$ we have $\mu(i(k)) = j(\lambda(k))$, we call the field extensions *isomorphic*.

Note that if $K = \tilde{K}$ (i.e. λ is the identity), and we use the same convention $i(k) = k \in L$ and $j(k) = k \in \tilde{L}$ as we have done up until this point, then L/K and $\tilde{L}/K$ are isomorphic if there is an isomorphism $\mu : L \to \tilde{L}$ such that $\mu(k) = k$ for all $k \in K$. However the monomorphism formulation is practical to use in order to distinguish which fields the different elements belong to.

Lemma 5.2.7 ([18] p. 39)
Let α and β be algebraic over some field K with the same minimal polynomial p over K. Then the two extensions $K(\alpha)$ and $K(\beta)$ are isomorphic, and the isomorphism can be taken to map α to β.

Proof.
We set $n = deg(p) - 1$. By Corollary 5.1.10, every $x \in K(\alpha)$ is uniquely expressible in the

form

$$x = x_0 + x_1\alpha + \ldots + x_n\alpha^n, \tag{5.25}$$

where $x_0, \ldots, x_n \in K$. We define the map $\phi : K(\alpha) \to K(\beta)$ by

$$\phi(x) = x_0 + x_1\beta + \ldots + x_n\beta^n, \tag{5.26}$$

which by Corollary 5.1.10 corresponds to a unique $y \in K(\beta)$. Thus ϕ is a bijection.
It follows from the definition of ϕ and Corollary 5.1.10 that $\phi(x + y) = \phi(x) + \phi(y)$ for any $x, y \in K(\alpha)$. We need to show that $\phi(xy) = \phi(x)\phi(y)$. Let $f, g, h \in K[X]$ be the polynomials of degree less than $deg(p)$ such that $x = f(\alpha)$, $y = g(\alpha)$ and $xy = h(\alpha)$. Then

$$f(\alpha)g(\alpha) - h(\alpha) = xy - xy = 0. \tag{5.27}$$

By Proposition 5.1.7 p is irreducible, and so p divides $fg - h$, since they have a common root. Thus there exists a polynomial $q \in K[X]$ such that $fg = pq + h$. Since p is also the minimal polynomial of β, we have $f(\beta)g(\beta) = h(\beta)$. This implies that

$$\phi(x)\phi(y) = \phi(f(\alpha))\phi(g(\alpha)) = f(\beta)g(\beta) = h(\beta) = h(\phi(\alpha)) = \phi(xy), \tag{5.28}$$

since ϕ fixes K so that $\phi(f(X)) = f(\phi(X))$, and similarly for g and h. This shows that ϕ is an isomorphism. Since ϕ is the identity on K, the two field extensions are isomorphic. Clearly ϕ maps α to β. ■

Corollary 5.2.8
Let α and β be algebraic over K with the same minimal polynomial. There is a unique isomorphism $\sigma : K(\alpha) \to K(\beta)$ such that $\sigma(\alpha) = \beta$ and such that σ is the identity on K.

Proof.
The existence follows from Lemma 5.2.7. Let σ be such an isomorphism. Since it maps α to β, it also maps α^2 to β^2 and so on for all the powers of α and β. Since σ is the identity on K it follows that it must be the isomorphism defined by Equation (5.26). Hence it is unique. ■

Theorem 5.2.9 ([19] p. 41)
Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. There are exactly n distinct embeddings of K into $\mathbb{C}$, $\sigma_i : K \to \mathbb{C}$, $i \in \{1, \ldots, n\}$. The elements $\sigma_i(\theta) = \theta_i$, are the distinct zeros in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$.

Proof.
Let $\theta_1, \ldots, \theta_n$ be the zeros of the minimal polynomial p of θ. From Corollary 5.1.14 we know that these are distinct. It follows that each θ_i also has minimal polynomial p, as p is irreducible. From Corollary 5.2.8 we have that there is a unique isomorphism $\sigma_i = \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ such that $\sigma_i(\theta) = \theta_i$, which fixes $\mathbb{Q}$. Thus there are at least n distinct embeddings of K into $\mathbb{C}$.
Now suppose $\sigma : K \to \mathbb{C}$ is an embedding. Then σ is the identity on $\mathbb{Q}$. Thus

$$0 = \sigma(p(\theta)) = p(\sigma(\theta)), \tag{5.29}$$

which implies, that $\sigma(\theta)$ is one of the roots θ_i of p, and hence σ is one of the n distinct σ_i from the first part of the proof. ■

Definition 5.2.10 (Field polynomial [19] p. 42)
Let $K = \mathbb{Q}(\theta)$ be a field extension of degree n, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings into $\mathbb{C}$. The *field polynomial* of an element $\alpha \in K$ is the polynomial over K given by

$$f_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)). \tag{5.30}$$

Proposition 5.2.11 ([19] p. 43)
Let $K = \mathbb{Q}(\theta)$ be a number field. For $\alpha \in K$ the field polynomial f_α is a power of the minimal polynomial p_α.

Proof.
Since p_α is irreducible and α is a root of both p_α and f_α it follows that $f_\alpha = p_\alpha^m h$ for some $m \in \mathbb{N}$ and $h \in K[X]$ such that p_α and h are coprime. Since f_α and p_α are monic, so is h.
We wish to show that h is constant. So assume for contradiction that h is not constant. Then h has some root in $\mathbb{C}$, which must be shared by f_α, which means it must be one of the $\sigma_j(\alpha)$, say $\sigma_i(\alpha)$. Now this root may be written as $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\theta_i)$, whereby $r \in K[X]$ is the polynomial, such that $r(\theta) = \alpha$. We define $g(X) = h(r(X)) \in K[X]$. Then $g(\theta_i) = 0$. The minimal polynomial, p_θ, of θ over $\mathbb{Q}$ is also the minimal polynomial of each θ_j. Since θ_i is a root of both g and the irreducible p_θ, it follows that p_θ divides g. This implies that each θ_j is a root of g. In particular $g(\theta) = 0$. Thus

$$h(\alpha) = h(r(\theta)) = g(\theta) = 0. \tag{5.31}$$

But if α is a root of h, then p_α divides h, which is a contradiction, since they were coprime. Thus h is constant, and since it is monic, we must have $h = 1$, so that $f_\alpha = p_\alpha^m$. ■

The following result is a version of what is known as Gauss' Lemma.

Lemma 5.2.12 ([19] p. 19)
Let $f \in \mathbb{Z}[X]$, and suppose that $f = gh$ where $g, h \in \mathbb{Q}[X]$. Then there exist $\lambda \in \mathbb{Q}, \lambda \neq 0$, such that $\lambda g, \lambda^{-1}h \in \mathbb{Z}[X]$.

Proof.
By taking the product, n, of the denominators of each coefficient in g and h we can rewrite $f = gh$ as:

$$nf = g'h', \tag{5.32}$$

where $g', h' \in \mathbb{Z}[X]$ are rational multiples of g, h and $n \in \mathbb{Z}$. Since $f \in \mathbb{Z}[X]$ this means that n divides the coefficients of $g'h'$. As we will show every prime factor of n either divides all the coefficients of g' or all those of h'. Thus by dividing the equation successively by the prime factors of n we get:

$$f = \tilde{g}\tilde{h}, \tag{5.33}$$

where $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ are rational multiples of g and h respectively. That is $\tilde{g} = \lambda g$ for $\lambda \in \mathbb{Q}$ thereby $\tilde{h} = \lambda^{-1}h$ and the result follows.
Thus we only need to prove that if

$$g' = g_0 + g_1X + \cdots + g_rX^r \in \mathbb{Z}[X] \tag{5.34}$$

$$h' = h_0 + h_1X + \cdots + h_sX^s \in \mathbb{Z}[X], \tag{5.35}$$

and a prime p divides all the coefficients of $g'h'$, then p must divide all the coefficients of g' or all the coefficients of h'. Assume for contradiction that p divides all the coefficients of $g'h'$ but does not divide all the coefficients of g' or all the coefficients of h'. Then we may consider the smallest i, such that p does not divide g_i and the smallest j such that p does not divide h_j. The coefficient of X^{i+j} in the product $g'h'$ is

$$g_0h_{i+j} + g_1h_{i+j-1} + \cdots + g_ih_j + \cdots + g_{i+j-1}h_1 + g_{i+j}h_0. \tag{5.36}$$

Since p divides $g_0, g_1, \ldots, g_{i-1}$ and $h_0, h_1, \ldots, h_{j-1}$, the only term that p does not divide in the coefficient of X^{i+j} is g_ih_j, and therefore p cannot divide the coefficient of X^{i+j} in $g'h'$, which is a contradiction. ■

Gauss' Lemma allows us to prove Eisensteins criterion, which we will need later.

Proposition 5.2.13 ([19] p. 20)
Let

$$f = a_0 + a_1X + \dots a_nX^n \in \mathbb{Z}[X], \tag{5.37}$$

and p be a prime such that:

(i) $p \nmid a_n$,

(ii) $p \mid a_i$ for $i = 0, 1, \dots, n-1$,

(iii) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Z}$, and hence irreducible over $\mathbb{Q}$.

Proof.
If f is irreducible over $\mathbb{Z}$, then Gauss' Lemma 5.2.12 implies that it is also irreducible over $\mathbb{Q}$, hence we only need to show that f have only constant factors over $\mathbb{Z}$. Assume for contradiction that $f = gh$ where

$$g = g_0 + g_1X + \dots + g_rX^r \tag{5.38}$$

$$h = h_0 + h_1X + \dots + h_sX^s, \tag{5.39}$$

where $g_i, h_j \in \mathbb{Z}$ for all i, j, and $r, s \geq 1$ and $r + s = n$. We have $a_0 = g_0h_0$ so (ii) implies that p divides either g_0 or h_0, while (iii) implies that p does not divide both g_0 and h_0. We may assume without loss of generality that p divides g_0 but not h_0. Now, (i) implies that p does not divide all the coefficients of g, so we may consider the smallest j such that p does not divide g_j. Then

$$a_j = g_0h_j + g_1h_{j-1} + \dots + g_jh_0, \tag{5.40}$$

where $j \leq r < n$. All the terms on the right are divisible by p, except the last. Therefore p does not divide a_j, which contradicts (ii). ■

We will need the following useful criterion for a number to be an algebraic integer.

Lemma 5.2.14
Let K be a number field, and let $\alpha \in K$ be an algebraic number, then $\alpha \in \mathcal{O}_K$ if and only if its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Proof.
Let p be the minimal polynomial of α over $\mathbb{Q}$. If $p \in \mathbb{Z}[X]$ then α is an algebraic integer.
Conversely if α is an algebraic integer, then $q(\alpha) = 0$ for some monic $q \in \mathbb{Z}[X]$, and $q = ph$

for some $h \in \mathbb{Q}[X]$, since p is irreducible. From Lemma 5.2.12 it follows that $\lambda p \in \mathbb{Z}[X]$, for some $0 \neq \lambda \in \mathbb{Q}$, and that λp divides q since $q = \lambda p \lambda^{-1} h$. Since q and p are both monic it follows that h is monic, and that $\lambda, \lambda^{-1} \in \mathbb{Z}$. Hence $\lambda = \pm 1$ and $p \in \mathbb{Z}[X]$. ■

Lemma 5.2.15
An algebraic integer is a rational number if and only if it is a rational integer.

Proof.
We wish to show that $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$. That $\mathbb{Z} \subseteq \mathbb{B} \cap \mathbb{Q}$ is trivial. Now let $\alpha \in \mathbb{B} \cap \mathbb{Q}$, since $\alpha \in \mathbb{Q}$ its minimal polynomial over $\mathbb{Q}$ is $X - \alpha$. Since $\alpha \in \mathbb{B}$ it follows from lemma 5.2.14 that the coefficients of the minimal polynomial belongs to $\mathbb{Z}$. Hence $\alpha \in \mathbb{Z}$, so that $\mathbb{B} \cap \mathbb{Q} \subseteq \mathbb{Z}$. ■

Definition 5.2.16 (Norm and trace)
Let K be a number field of degree n with embeddings σ_i, and let $x \in K$. The elements $\sigma_1(x), \sigma_2(x) \ldots, \sigma_n(x)$ are called the *conjugates* of x and

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr(x) = \sum_{i=1}^{n} \sigma_i(x) \tag{5.41}$$

are called the *norm* and *trace* of x respectively.

Proposition 5.2.17
Let K be a number field. If $x \in \mathcal{O}_K$, we have $N(x), Tr(x) \in \mathbb{Z}$.

Proof.
From Proposition 5.2.11 we have that the field polynomial $f_x(X)$ is a power of the minimal polynomial $p_x(X)$. From Lemma 5.2.14 we have that $p_x \in \mathbb{Z}[X]$ and hence $f_x \in \mathbb{Z}[X]$. Since $N(x)$ and $Tr(x)$ corresponds to the coefficients of X^0 and X^{n-1} in $f_x(X)$ respectively, it follows that $N(x), Tr(x) \in \mathbb{Z}$. ■

Definition 5.2.18 (Discriminant of a basis [19] p. 44)
Let $K = \mathbb{Q}(\theta)$ be a number field with embeddings σ_i and with basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, and let M be the $n \times n$ matrix with entries: $M_{i,j} = \sigma_i(\alpha_j)$. The *discriminant of the basis* is given by $\det(M)^2$ and denoted $\Delta[\alpha_1, \ldots, \alpha_n]$.

Proposition 5.2.19 ([19] p. 44)
Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be two different bases of a number field K. Then there exists an invertible matrix C with entries: $C_{i,j} \in \mathbb{Q}$ so that

$$\Delta[\beta_1, \ldots, \beta_n] = \text{det}(C)^2 \Delta[\alpha_1, \ldots, \alpha_n]. \tag{5.42}$$

Proof.
Let $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ and $\{\beta_1, \beta_2, \cdots, \beta_n\}$ be two different bases of K. Then for each $k \in \{1, \ldots, n\}$, we have for some $c_{i,k} \in \mathbb{Q}$:

$$\beta_k = \sum_{i=1}^{n} c_{i,k}\alpha_i, \quad \text{and} \tag{5.43}$$

$$\sigma_h(\beta_k) = \sum_{i=1}^{n} c_{i,k}\sigma_h(\alpha_i), \quad h = 1, \ldots, n \tag{5.44}$$

where the $\sigma_h's$ are the n embeddings into $\mathbb{C}$, and the second equality follows since σ_h fixes $\mathbb{Q}$. Thus the matrix H with entries: $H_{i,j} = \sigma_i(\beta_j)$ can be written as a product of the matrix M with entries: $M_{i,j} = \sigma_i(\alpha_j)$ and the matrix C with entries: $C_{i,j} = c_{i,j}$. From the product formula for determinants it follows that the discriminant of the basis $\{\beta_1, \beta_2, \cdots, \beta_n\}$ is given by:

$$\Delta[\beta_1, \ldots, \beta_n] = \text{det}(H)^2 = \text{det}(C)^2 \Delta[\alpha_1, \ldots, \alpha_n]. \tag{5.45}$$

To see that C is invertible, assume that the columns in C are linearly dependent. Then for some j, the $j'th$ column C_j can be written $C_j = \sum_{i \neq j} a_i C_i$. Since the entries in C_j is given by the coefficients of β_j when written with regard to the basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ we have that:

$$\beta_j = \sum_{i=1}^{n} c_{i,j}\alpha_i = \sum_{i=1}^{n} \sum_{k \neq j} a_k c_{i,k}\alpha_i = \sum_{k \neq j} a_k \sum_{i=1}^{n} c_{i,k}\alpha_i = \sum_{k \neq j} a_k \beta_k \tag{5.46}$$

in contradiction with $\{\beta_1, \beta_2, \cdots, \beta_n\}$ being a basis. ■

The matrix C in Proposition 5.2.19 is called a transition matrix from $\{\beta_1, \ldots, \beta_n\}$ to $\{\alpha_1, \ldots, \alpha_n\}$.

Proposition 5.2.20 ([19] p. 51)
Let $\{\omega_1, \omega_2, \ldots, \omega_n\}, \omega_i \in \mathcal{O}_K$ be a basis for a number field K. The discriminant $\Delta[\omega_1, \ldots, \omega_n]$ belongs to $\mathbb{Z}$.

Proof.
We proceed as in [1]. As usual we denote the n embeddings of K into $\mathbb{C}$ by σ_i, $i = 1, \ldots, n$. Using Definition 5.2.18, we have:

$$\Delta[\omega_1,\ldots,\omega_n] = \det\left(\begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n) \end{bmatrix}\right)^2 \tag{5.47}$$

$$= \det\left(\begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_n) \end{bmatrix}\begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n) \end{bmatrix}\right). \tag{5.48}$$

The (i,j) entry in the matrix product in Equation (5.48) is given by $\sigma_1(\omega_i)\sigma_1(\omega_j)+\sigma_2(\omega_i)\sigma_2(\omega_j)+\ldots+\sigma_n(\omega_i)\sigma_n(\omega_j) = Tr(\omega_i\omega_j)$, since $\sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sigma_k(\alpha_i\alpha_j),\ k = 1,\ldots,n$ because σ_k is a homomorphism. Since $\omega_i,\ i = 1,\ldots,n$ is an algebraic integer, it follows from Proposition 5.2.17, that the matrix product in Equation (5.48) has entries in $\mathbb{Z}$. Thus $\Delta[\omega_1,\ldots,\omega_n] \in \mathbb{Z}$. ■

Corollary 5.2.21 ([11] p. 76)
Let $\{\omega_1,\omega_2,\ldots,\omega_n\}$ and $\{\gamma_1,\gamma_2,\ldots,\gamma_n\}$ be two integral bases for a number field K. Then

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n] = \Delta[\gamma_1,\gamma_2,\ldots,\gamma_n]. \tag{5.49}$$

Proof.
From Proposition 5.2.19 we have that:

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n] = \det(C)^2\Delta[\gamma_1,\gamma_2,\ldots,\gamma_n], \tag{5.50}$$

where it follows from the proof of Proposition 5.2.19 that $\det(C) \in \mathbb{Z}$, since the entries $C_{ij} \in \mathbb{Z}$ because the bases are integral. Thus

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n] \mid \Delta[\gamma_1,\gamma_2,\ldots,\gamma_n] \in \mathbb{Z} \tag{5.51}$$

by Proposition 5.2.20. By the same argument we have that:

$$\Delta[\gamma_1,\gamma_2,\ldots,\gamma_n] \mid \Delta[\omega_1,\omega_2,\ldots,\omega_n] \in \mathbb{Z}. \tag{5.52}$$

Thereby

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n] = \pm\Delta[\gamma_1,\gamma_2,\ldots,\gamma_n], \tag{5.53}$$

however by Equation (5.50), the minus sign is not possible. ■

This allows us to make the following definition.

Definition 5.2.22 (Discriminant of a number field)
Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be an integral basis of a number field K. The *discriminant* of K is defined as the discriminant of the basis:

$$disc_K = \Delta[\omega_1, \omega_2, \ldots, \omega_n]. \tag{5.54}$$

To proceed, we first need a result on symmetric polynomials.

Definition 5.2.23 (Symmetric polynomial [19] p. 25)
Let $R[X_1, \ldots, X_n]$ be a multivariate polynomial ring, and let S_n be the symmetric group of permutations on the set $\{1, 2, \ldots, n\}$. A polynomial $p \in R[X_1, \ldots, X_n]$ is *symmetric* if for all permutations $\pi \in S_n$ we have

$$p(X_1, \ldots, X_n) = p(X_{\pi(1)}, X_{\pi(2)}, \ldots, X_{\pi(n)}). \tag{5.55}$$

We state the needed result without proof.

Lemma 5.2.24 ([19] p. 27)
Let L/K be a field extension. Let $p \in K[X]$ be a polynomial of degree n with roots $\theta_1, \ldots, \theta_n \in L$. If $h(X_1, \ldots X_n) \in K[X_1, \ldots, X_n]$ is symmetric, then $h(\theta_1, \ldots, \theta_n) \in K$.

Proof. A proof can be found in [19, p. 25-27]. ■

Proposition 5.2.25 ([19] p. 44)
Let $K = \mathbb{Q}(\theta)$ be a number field. The discriminant of any basis for K is rational and non-zero.

Proof.
Denote the conjugates of θ by $\theta_1, \ldots, \theta_n$. Then the discriminant of the basis $\{1, \theta, \ldots, \theta^{n-1}\}$ is given by:

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (\det(\Theta))^2, \tag{5.56}$$

where Θ is the matrix with entries $\Theta_{i,j} = \theta_i^{j-1}$. A determinant of this form is called a Vandermonde determinant, and as shown in [2], it is given by

$$V = \det(\Theta) = \prod_{1 \leq i < j \leq n} (\theta_j - \theta_i). \tag{5.57}$$

Now, consider the polynomial $\tilde{V} \in \mathbb{Q}(X_1, \ldots, X_n)$ defined by $\tilde{V}(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n}(X_j - X_i)$. Notice that

$$\tilde{V}^2(X_1, \ldots, X_n) = \left(\prod_{1 \leq i < j \leq n} (X_j - X_i) \right)^2 = \prod_{1 \leq i < j \leq n} (X_j - X_i)^2, \tag{5.58}$$

is a symmetric polynomial. Thus by Lemma 5.2.24 we have:

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = V^2 = \tilde{V}^2(\theta_1, \ldots, \theta_n) \in \mathbb{Q}. \tag{5.59}$$

By Corollary 5.1.14, the θ_i are distinct, so that $\Delta[1, \theta, \ldots, \theta^{n-1}]$ is non-zero.
Let $\{\alpha_1, \ldots, \alpha_n\}$ be any basis for K. By Proposition 5.2.19, we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det(C))^2 \Delta[1, \theta, \ldots, \theta^{n-1}] \tag{5.60}$$

for some invertible matrix C with entries in $\mathbb{Q}$. This shows that $\Delta[\alpha_1, \ldots, \alpha_n]$ is also rational and non-zero. ■

We now give the proof of Proposition 5.2.2. For the sake of clarity, we write the proposition here as well:

> Let K be a number field of degree n. The ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n.

Proof. [19, p. 51]
We wish to show that there exists a basis of n elements over $\mathbb{Z}$.
From Corollary 5.1.23 we have that $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathcal{O}_K$, and hence there exists a basis for K consisting of algebraic integers. From Proposition 5.2.20 we have that the discriminant of a basis consisting of algebraic integers belongs to $\mathbb{Z}$. Thus we select a basis $\{\omega_1, \omega_2, \ldots, \omega_n\}$ such that $|\Delta[\omega_1, \omega_2, \ldots, \omega_n]|$ is minimal, and we claim that this is an integral basis. If this is not the case, then there is a $\omega \in \mathcal{O}_K$ such that:

$$\omega = a_1\omega_1 + \ldots + a_n\omega_n \tag{5.61}$$

for $a_i \in \mathbb{Q}$, not all in $\mathbb{Z}$. We choose the numbering such that $a_1 \notin \mathbb{Z}$. Hence $a_1 = a + r$ for $a \in \mathbb{Z}$ and $0 < r < 1$. By defining

$$\psi_1 = \omega - a\omega_1 \quad \text{and} \quad \psi_i = \omega_i \quad \text{for} \quad i \in \{2, \ldots, n\}, \tag{5.62}$$

we have a new basis $\{\psi_1, \ldots, \psi_n\}$ consisting of algebraic integers. The transition matrix from $\{\psi_1, \ldots, \psi_n\}$ to $\{\omega_1, \ldots, \omega_n\}$ is given by:

$$\begin{bmatrix} a_1 - a & 0 & 0 & \cdots & 0 \\ a_2 & 1 & 0 & \cdots & 0 \\ a_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \cdots & 1 \end{bmatrix},$$

which is easily seen to have determinant $a_1 - a = r$. It follows from Proposition 5.2.19 that

$$\Delta[\psi_1, \ldots, \psi_n] = r^2 \Delta[\omega_1, \ldots, \omega_n], \tag{5.63}$$

and since $0 < r < 1$, this contradicts the fact that $|\Delta[\omega_1, \ldots, \omega_n]|$ was minimal. Hence $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is an integral basis consisting of n elements. ■

Definition 5.2.26 (Signature)
Let K be a number field with embeddings $\sigma_1, \ldots, \sigma_n$ into $\mathbb{C}$. Let r_1 be the number of embeddings with image in $\mathbb{R}$, and let $2r_2$ be the number of embeddings with image not contained in $\mathbb{R}$, so that $2r_2 = n - r_1$. The pair (r_1, r_2) is called the *signature* of K. If $r_2 = 0$, we call K a *totally real* number field. If $r_1 = 0$, we call K a *totally complex* number field.

Let $K = \mathbb{Q}(\theta)$ be a number field with embeddings $\sigma_1, \ldots, \sigma_n$. If $a \in \mathbb{C}\backslash\mathbb{R}$ is the image of some $x \in K$ under some embedding, σ_i, then the complex conjugate $\overline{a}$ is the image of x under some other embedding, σ_j, i.e. $\overline{a} = \sigma_j(x)$. To see that this is true, remember that $x \in K$ can be written as $x = x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}$, where $x_0, \ldots, x_{n-1} \in \mathbb{Q}$ (Corollary 5.1.10). From Theorem 5.2.9 we have that $\sigma_i(x) = x_0 + x_1\theta_i + \ldots + x_{n-1}\theta_i^{n-1}$, and that θ_j, $j = 1, \ldots, n$ are the roots in the minimal polynomial for θ over $\mathbb{Q}$. Thus we have by the complex conjugate root theorem, that $\overline{\theta_i} = \theta_j$, and hence that $\overline{a} = \overline{\sigma_i(x)} = \sigma_j(x)$ for some $j \in \{1, \ldots, n\}$, since $\sigma_j(x) = x_0 + x_1\theta_j + \ldots + x_{n-1}\theta_j^{n-1}$. This allows us to make the following definition.

Definition 5.2.27 (Canonical embedding)
Let K be a number field with embeddings $\sigma_1, \ldots, \sigma_n$, and order the σ_i's such that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}, 1 \leq i \leq r_1$, and σ_{j+r_2} is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The homomorphism $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ defined by:

$$\sigma(x) = \Big[\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)\Big]^T \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \tag{5.64}$$

is called a *canonical embedding*.

Note that the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$:

$$\sigma(x) = \Big[\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)\Big]^T \in \mathbb{R}^n$$

where $\Re$ and $\Im$ denotes the real and imaginary part respectively.

5.3 Algebraic Lattices

This section is based on [12, ch. 5].
The following result allows us to construct lattices from number fields.

Proposition 5.3.1 ([19] p. 154)
Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis for a number field K, and let σ be the canonical embedding. Then $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ are linearly independent over $\mathbb{R}$.

Proof.
Let (r_1, r_2) be the signature of K we need to prove that the determinant of the matrix:

$$D = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \Re\sigma_{r_1+1}(\alpha_1) & \cdots & \Re\sigma_{r_1+1}(\alpha_n) \\ \Im\sigma_{r_1+1}(\alpha_1) & \cdots & \Im\sigma_{r_1+1}(\alpha_n) \\ \vdots & \vdots & \vdots \\ \Re\sigma_{r_1+r_2}(\alpha_1) & \cdots & \Re\sigma_{r_1+r_2}(\alpha_n) \\ \Im\sigma_{r_1+r_2}(\alpha_1) & \cdots & \Im\sigma_{r_1+r_2}(\alpha_n) \end{bmatrix} \tag{5.65}$$

is non-zero. The matrix D can be transformed to the following matrix E by elementary row operations:

$$E = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \Re\sigma_{r_1+1}(\alpha_1) + i\Im\sigma_{r_1+1}(\alpha_1) & \cdots & \Re\sigma_{r_1+1}(\alpha_n) + i\Im\sigma_{r_1+1}(\alpha_n) \\ \Re\sigma_{r_1+1}(\alpha_1) - i\Im\sigma_{r_1+1}(\alpha_1) & \cdots & \Re\sigma_{r_1+1}(\alpha_n) - i\Im\sigma_{r_1+1}(\alpha_n) \\ \vdots & \vdots & \vdots \\ \Re\sigma_{r_1+r_2}(\alpha_1) + i\Im\sigma_{r_1+r_2}(\alpha_1) & \cdots & \Re\sigma_{r_1+r_2}(\alpha_n) + i\Im\sigma_{r_1+r_2}(\alpha_1) \\ \Re\sigma_{r_1+r_2}(\alpha_1) - i\Im\sigma_{r_1+r_2}(\alpha_1) & \cdots & \Re\sigma_{r_1+r_2}(\alpha_n) - i\Im\sigma_{r_1+r_2}(\alpha_1) \end{bmatrix} \tag{5.66}$$

$$= \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+1}(\alpha_n) \\ (\sigma_{r_1+1}(\alpha_1))^* & \cdots & (\sigma_{r_1+1}(\alpha_n))^* \\ \vdots & \vdots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_n) \\ (\sigma_{r_1+r_2}(\alpha_1))^* & \cdots & (\sigma_{r_1+r_2}(\alpha_n))^* \end{bmatrix}, \tag{5.67}$$

where * denotes the complex conjugate. Since no rows were interchanged and r_2 rows were multiplied by $-2i$ in the transformation of D to E we have:

$$(-2i)^{r_2} \det(D) = \det(E) = \pm\sqrt{\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n]}. \tag{5.68}$$

From Proposition 5.2.25 we have that the discriminant is non-zero, and therefore $\det(D) \neq 0$ as required. ■

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for K. Since $\sigma(\omega_i)$, $i = 1, \ldots, n$ are linearly independent as vectors in $\mathbb{R}^n$, the image of $\mathcal{O}_K$ under σ defines a full rank lattice with basis $\{\sigma(\omega_1), \ldots, \sigma(\omega_n)\}$. The generator matrix for this lattice is given by:

$$M = \begin{bmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & \vdots & \vdots \\ \sigma_{r_1}(\omega_1) & \cdots & \sigma_{r_1}(\omega_n) \\ \Re\sigma_{r_1+1}(\omega_1) & \cdots & \Re\sigma_{r_1+1}(\omega_n) \\ \Im\sigma_{r_1+1}(\omega_1) & \cdots & \Im\sigma_{r_1+1}(\omega_n) \\ \vdots & \vdots & \vdots \\ \Re\sigma_{r_1+r_2}(\omega_1) & \cdots & \Re\sigma_{r_1+r_2}(\omega_n) \\ \Im\sigma_{r_1+r_2}(\omega_1) & \cdots & \Im\sigma_{r_1+r_2}(\omega_n) \end{bmatrix} \tag{5.69}$$

Definition 5.3.2 (Algebraic lattice)
Let $\mathcal{O}_K$ be the ring of integers of a number field K, and let σ be the canonical embedding. Then we call the image of $\mathcal{O}_K$ under σ the *algebraic lattice* over K.

The proof of Proposition 5.3.1 shows the following result.

Corollary 5.3.3
Let $disc_K$ be the discriminant of a number field K with signature (r_1, r_2), and let M be the generator matrix for the algebraic lattice, Λ, over K. Then the volume of the lattice is given by:

$$vol(\Lambda) = |\det(M)| = 2^{-r_2}\sqrt{|disc_K|}. \tag{5.70}$$

Consequently, the determinant of the lattice is given by:

$$det(\Lambda) = 2^{-2r_2}|disc_K|. \tag{5.71}$$

Proof.
The generator matrix M is identical to the matrix D from Equation (5.65), except now the basis is integral. Therefore the proof of Proposition 5.3.1 shows that:

$$(-2i)^{r_2}\det(M) = \pm\sqrt{\Delta[\omega_1, \omega_2, \ldots, \omega_n]} = \pm\sqrt{disc_K} \tag{5.72}$$

It easily follows that $|\det(M)| = 2^{-r_2}\sqrt{|disc_K|}$. ■

For the sake of clarity we emphasize the correspondence between a lattice point $\mathbf{x} \in \Lambda \subset \mathbb{R}^n$ and an algebraic integer $x \in \mathcal{O}_K$. A lattice point has the form:

$$\mathbf{x} = \Big[x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+2r_2}\Big]^T \tag{5.73}$$

$$= \Big[\textstyle\sum_{i=1}^n \lambda_i \sigma_1(\omega_i), \ldots, \sum_{i=1}^n \lambda_i \Re\sigma_{r_1+1}(\omega_i), \ldots, \sum_{i=1}^n \lambda_i \Im\sigma_{r_1+r_2}(\omega_i)\Big]^T \tag{5.74}$$

$$= \Big[\sigma_1(\textstyle\sum_{i=1}^n \lambda_i \omega_i), \ldots, \Re\sigma_{r_1+1}(\sum_{i=1}^n \lambda_i \omega_i), \ldots, \Im\sigma_{r_1+r_2}(\sum_{i=1}^n \lambda_i \omega_i)\Big]^T \tag{5.75}$$

for some λ_i in $\mathbb{Z}$, and an integral basis $\{\omega_1, \omega_2, \ldots, \omega_n\}$ of K. Thus

$$\mathbf{x} = \Big[\sigma_1(x), \ldots, \Re\sigma_{r_1+1}(x), \ldots \Im\sigma_{r_1+r_2}(x)\Big]^T = \sigma(x) \tag{5.76}$$

for $x = \sum_{i=1}^n \lambda_i \omega_i \in \mathcal{O}_K$.

Proposition 5.3.4
Let Λ be the algebraic lattice over a number field K with signature (r_1, r_2). Then the diversity of Λ is given by:

$$L = r_1 + r_2. \tag{5.77}$$

Proof.
Let $\mathbf{x} \neq \mathbf{0}$ be an arbitrary point of the lattice Λ. We may write $\mathbf{x}$ as in Equation (5.76):

$$\mathbf{x} = \Big[\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)\Big]^T = \sigma(x), \tag{5.78}$$

for some algebraic integer $x \in \mathcal{O}_K$. Since $\mathbf{x} \neq \mathbf{0}$, we have $x \neq 0$. Say $\sigma_j(x) = a + ib$. Then we can not have that both $a = 0$ and $b = 0$, since σ_j is injective. Because the first r_1 coefficients are real, they are therefore non-zero. Of the last $2r_2$ coefficients, at most r_2 can be zero for the same reason. Thus $L \geq r_1 + r_2$.
Now, consider the multiplicative identity, $1 \in \mathcal{O}_K$. Since $\sigma_j(1) = 1$, we have exactly $r_1 + r_2$ non-zero coefficients in $\sigma(1)$. Therefore $L = r_1 + r_2$. ■

From the above result, we see that we now have a way to build lattices with maximal diversity.

Corollary 5.3.5
Algebraic lattices build over totally real number fields have maximal diversity $L = n$.

Proof.
A totally real number field has signature $(r_1, r_2) = (n, 0)$, and the result follows from Proposition 5.3.4. ■

Let R be a commutative ring. A principal ideal is of the form $\mathcal{I} = \{xy \mid y \in R\}$ for some $x \in R$. We denote such a principle ideal by $\mathcal{I} = \langle x \rangle_R$ or simply $\langle x \rangle$ if it is clear which ring it is an ideal of.

Definition 5.3.6 (Norm of ideal)
Let $\mathcal{I} = \langle x \rangle_{\mathcal{O}_K}$ be a principal ideal of the ring of integers of a number field K. Then we define the *norm of the ideal* by $N(\mathcal{I}) = |N(x)|$.

To see that the norm of a principal ideal is well-defined, assume that $\mathcal{I} = \langle x \rangle = \langle y \rangle$. Then there exists some $a, b \in \mathcal{O}_K$, such that $x = ay$ and $y = bx$. Thus $x = abx$, so that $ab = 1$. Then $1 = N(1) = N(ab) = N(a)N(b)$, and $N(a), N(b) \in \mathbb{Z}$, by Proposition 5.2.17. Thus $N(a) = N(b) = \pm 1$, so that $N(x) = N(a)N(y) = \pm N(y)$ [9, p. 16].
Previously we saw that the key to building an algebraic lattice was the existence of a $\mathbb{Z}$-basis in K. Since $\mathcal{O}_K$ has such a basis it could be used to obtain an algebraic lattice. The following proposition shows that the ideals of $\mathcal{O}_K$ exhibits the same structure.

Proposition 5.3.7
Every ideal $\mathcal{I} \neq \{0\}$ of $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\{v_1, v_2, \ldots, v_n\}$ where n is the degree of K.

Proof.
From Proposition 5.2.2 we have that $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n, so that $\mathcal{O}_K \cong \mathbb{Z}^n$ as additive groups. In [19, Theorem 1.12] it is shown that a subgroup of a free $\mathbb{Z}$-module of rank n is a free $\mathbb{Z}$-module of rank $s \leq n$, and that the index of the subgroup is finite if and only if the ranks of the groups are equal ([19, Theorem 1.13]). Thus we need to show that $\mathcal{O}_K/\mathcal{I}$ is finite and the result follows. Let $a \in \mathcal{I}$, $a \neq 0$ and let $p_a = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} + X^m \in \mathbb{Z}[X]$ be the minimal polynomial of a. Then $\langle a \rangle_{\mathcal{O}_K} \subseteq \mathcal{I}$, and $\langle a_0 \rangle_{\mathcal{O}_K} \subseteq \langle a \rangle_{\mathcal{O}_K}$, since $a(a_1 + \cdots + a_{m-1}a^{m-2} + a^{m-1}) = -a_0$, so that a divides a_0 in $\mathcal{O}_K$. Since $a_0 \in \mathbb{Z}$, we have that $\mathbb{Z}^n/a_0\mathbb{Z}^n$ is finite, and it follows that $\mathcal{O}_K/\mathcal{I}$ is also finite, since $\mathcal{O}_K \cong \mathbb{Z}^n$. ■

Proposition 5.3.7 implies that Proposition 5.3.1 extends to a basis for an ideal, and thus we may build a lattice, $\Lambda' = \sigma(\mathcal{I})$, from an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ analogous to what we did with $\mathcal{O}_K$. Since $\mathcal{I} \subseteq \mathcal{O}_K$, the lattice is a sublattice of the algebraic lattice, Λ, over K. We also call Λ' an algebraic lattice. Proposition 5.3.4 extends to the lattice Λ', so that lattices built from ideals over totally real number fields have maximal diversity. For emphasis we write this as a separate Corollary.

Corollary 5.3.8
Let $\mathcal{I}$ be an ideal of the ring of integers of a totally real number field, K, of degree n, and let σ be the canonical embedding. The algebraic lattice $\Lambda' = \sigma(\mathcal{I}) \subset \mathbb{R}^n$ has maximal diversity, $L = n$.

For a principal ideal, we have the following result.

Proposition 5.3.9 ([14] p. 64)
Let $\mathcal{I}$ be a principal ideal of the ring of integers of a totally real number field, K, of degree n, and let σ be the canonical embedding. The volume of the algebraic lattice, $\Lambda' = \sigma(\mathcal{I}) \subset \mathbb{R}^n$, is given by

$$vol(\Lambda') = N(\mathcal{I})\sqrt{|disc_K|}. \tag{5.79}$$

Proof.
Let $\mathcal{I} = \langle x \rangle$ and let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be an integral basis for K. Then $\{x\omega_1, x\omega_2, \ldots, x\omega_n\}$ is a basis for $\mathcal{I}$ since for every, $k = \sum_{i=1}^{n} \lambda_i \omega_i \in \mathcal{O}_K$ we have $kx = \sum_{i=1}^{n} \lambda_i x\omega_i \in \mathcal{I}$. The generator matrix for Λ' is then given by:

$$M = \begin{bmatrix} \sigma_1(x\omega_1) & \ldots & \sigma_1(x\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x\omega_1) & \ldots & \sigma_n(x\omega_n) \end{bmatrix} = \begin{bmatrix} \sigma_1(x) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(x) \end{bmatrix} \begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n) \end{bmatrix} \tag{5.80}$$

and the volume of the lattice is easily seen to be:

$$vol(\Lambda') = |\det(M)| = |N(x)\sqrt{disc_K}| = N(\mathcal{I})\sqrt{|disc_K|}. \tag{5.81}$$

■

5.4 Ideal Lattices

This section is based on [12, ch. 6]

Definition 5.4.1 (Twisted canonical embedding)
Let K be a totally real number field with the embeddings into $\mathbb{C}$ given by $\{\sigma_i\}_{i=1}^{n}$. Let $\alpha \in K$ be such that $\sigma_i(\alpha) > 0$ for all i. Then we define a *twisted canonical embedding*, $\sigma_\alpha : K \to \mathbb{R}^n$ by

$$\sigma_\alpha(x) = \left[\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x)\right]^T, \tag{5.82}$$

where $\alpha_i = \sigma_i(\alpha)$ for $i = 1, \ldots, n$.

Using the twisted canonical embeddings we define an ideal lattice.

Definition 5.4.2 (Ideal lattice)
Let $\mathcal{I} \subseteq \mathcal{O}_K$ be an ideal of $\mathcal{O}_K$ and $\sigma_\alpha(x)$ be a twisted canonical embedding as defined in Definition 5.4.1. A lattice of the form $\Lambda = \sigma_\alpha(\mathcal{I})$ is called an *ideal lattice*.

Let $\{\omega_1, \dots \omega_n\}$ be a $\mathbb{Z}$-basis of the ideal $\mathcal{I} \subseteq \mathcal{O}_K$, then the generator matrix M of the ideal lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ is given by:

$$M = \begin{bmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \cdots & \sqrt{\alpha_1}\sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sqrt{\alpha_n}\sigma_n(\omega_1) & \cdots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{bmatrix} = \begin{bmatrix} \sqrt{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\alpha_n} \end{bmatrix} \begin{bmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{bmatrix} \tag{5.83}$$

Note that $\sigma_\alpha(\mathcal{I})$ is a full-rank, maximal diversity lattice by the same argument as in the proof of Proposition 5.3.4, since the multiplication by $\sqrt{\alpha_i}$ does not change any non-zero coefficient to zero. Proposition 5.3.9 implies the following.

Proposition 5.4.3
Let $\Lambda = \sigma_\alpha(\mathcal{I})$ be an ideal lattice. Then

$$\det(\Lambda) = N(\alpha)N(\mathcal{I})^2|disc_K|. \tag{5.84}$$

Proof.
The setup is the same as in Proposition 5.3.9, except now the generator matrix is multiplied by the diagonal matrix

$$\begin{bmatrix} \sqrt{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\alpha_n} \end{bmatrix}, \tag{5.85}$$

which has determinant $\sqrt{N(\alpha)}$. Therefore the result follows by the same argument as in Proposition 5.3.9. ■

Proposition 5.4.4
Let $\sigma_\alpha(\mathcal{I})$ be an ideal lattice. The image of the function $q_\alpha(x, y) = \text{Tr}(\alpha xy)$, for $x, y \in \mathcal{I}$, is in $\mathbb{Z}$:

$$q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}.$$

Proof.
The generator matrix of $\sigma_\alpha(\mathcal{I})$ is given in equation (5.83). The entries in the corresponding Gram matrix $G = M^T M$ is given by:

$$G_{ij} = \sum_{k=1}^{n} \sqrt{\alpha_k}\sigma_k(\omega_i)\sqrt{\alpha_k}\sigma_k(\omega_j) \tag{5.86}$$

$$= \sum_{k=1}^{n} \alpha_k \sigma_k(\omega_i\omega_j) \tag{5.87}$$

$$= \mathrm{Tr}(\alpha\omega_i\omega_j). \tag{5.88}$$

We have that $\omega_i, \omega_j \in \mathcal{I}$, and therefore $\alpha\omega_i\omega_j \in \mathcal{I} \subseteq \mathcal{O}_K$, and by Proposition 5.2.17 it follows that $\mathrm{Tr}(\alpha\omega_i\omega_j) \in \mathbb{Z}$. Since αxy can be written as a sum of terms on the form $\lambda_k\alpha\omega_i\omega_j$, where $i, j \in \{1, \ldots, n\}$ and $\lambda_k \in \mathbb{Z}$, the result follows. ■

Lemma 5.4.5

Let $\mathcal{I}$ be a principal ideal of the ring of integers, $\mathcal{O}_K$, of a number field K. Then

$$\min\{|N(x)| \mid x \in \mathcal{I},\ x \neq 0\} = N(\mathcal{I}). \tag{5.89}$$

Proof.

Let $a \in \mathcal{I}$ be a generator: $\mathcal{I} = \langle a \rangle$. Then by definition $N(\mathcal{I}) = |N(a)|$. Let $x \in \mathcal{I}$, $x \neq 0$ be arbitrary. Then $x = ay$ for some non-zero $y \in \mathcal{O}_K$. Therefore $|N(x)| = |N(a)||N(y)| \geq N(\mathcal{I})$, by Proposition 5.2.17. ■

Let $\mathbf{x} \in \sigma_\alpha(\mathcal{I})$. Then it can be written:

$$\mathbf{x} = \left[\sum_{i=1}^{n} \lambda_i\sqrt{\alpha_1}\sigma_1(\omega_1), \ldots, \sum_{i=1}^{n} \lambda_i\sqrt{\alpha_n}\sigma_n(\omega_1)\right]^T, \quad \lambda_i \in \mathbb{Z} \tag{5.90}$$

$$= \sigma_\alpha(x) \tag{5.91}$$

for $x = \sum_{i=1}^{n} \lambda_i\omega_i \in \mathcal{I} \subseteq \mathcal{O}_K$.

Proposition 5.4.6

Let $\mathcal{I}$ be a principal ideal of the ring of integers, $\mathcal{O}_K$, of a number field K. The minimum product distance of an ideal lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ is

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{|disc_K|}}. \tag{5.92}$$

Proof.

Let $\mathbf{x}$ be a lattice point and $x \in \mathcal{I}$ such that $\mathbf{x} = \sigma_\alpha(x)$. Then

$$d_{p,min}(\Lambda) = \min\left\{\prod_{j=1}^{n}|x_j| \;\middle|\; \mathbf{x}\in\Lambda, \mathbf{x}\neq\mathbf{0}\right\} = \min\left\{\prod_{j=1}^{n}|\sqrt{\alpha_j}\sigma_j(x)| \;\middle|\; x\in\mathcal{I}, x\neq 0\right\} \tag{5.93}$$

$$= \sqrt{N(\alpha)}\min\{|N(x)| \mid x\in\mathcal{I}, x\neq 0\} \tag{5.94}$$

$$= \sqrt{N(\alpha)}N(\mathcal{I}) \tag{5.95}$$

$$= \sqrt{\frac{\det(\Lambda)}{|disc_K|}}. \tag{5.96}$$

where the last two equalities follows from Lemma 5.4.5 and Proposition 5.4.3 respectively. ■

5.5 The Cyclotomic Construction of Rotated $\mathbb{Z}^n$ Lattices

This section is based on [12, ch. 7].

When implementing lattice codes it might be a complex task to decode the message due to a complicated labeling of the lattice points that requires the use of a look-up table. Another thing to consider when choosing which lattice to use is constellation shaping, which affects the energy efficiency of the communication. The lattices $\mathbb{Z}^n = \{[x_1,\dots,x_n]^T \mid x_i \in \mathbb{Z}\}$ offer a good compromise between shaping gain and easy bit labeling [12, section 2.4]. In this section we give a construction of rotated $\mathbb{Z}^n$ lattices from cyclotomic fields for $n = \frac{p-1}{2}$, where $p \geq 5$ is a prime. We begin by introducing the cyclotomic fields.

Definition 5.5.1 (Cyclotomic field)
Let $\zeta_m = e^{2\pi i/m}$ be a primitive $m-$th root of unity. The number field $\mathbb{Q}(\zeta_m)$ is called a *cyclotomic field*.

We first state a classical result regarding cyclotomic fields, which is difficult to prove.

Proposition 5.5.2
Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field. Then the ring of integers is given by:

$$\mathcal{O}_K = \mathbb{Z}[\zeta_m]. \tag{5.97}$$

Proof.
A proof can be found in e.g. [21]. ■

We will focus on the case where $m = p \geq 5$ is a prime.

Proposition 5.5.3

Let p be a prime, and let ζ_p be a primitive p'th root of unity. Then

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1. \tag{5.98}$$

Proof.

By Corollary 5.1.10 it suffices to show that the degree of the minimal polynomial of ζ_p is $p-1$. Now let

$$P(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1. \tag{5.99}$$

We wish to prove that $P(X)$ is irreducible over $\mathbb{Q}$ and thereby the minimal polynomial of ζ_p. It is sufficient to show that $P(X)$ is irreducible over $\mathbb{Z}$, since by Gauss' lemma 5.2.12 this implies that it is irreducible over $\mathbb{Q}$. By the binomial theorem we have:

$$P(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} \tag{5.100}$$

$$= X^{p-1} + pX^{p-2} + \frac{p(p-1)}{2}X^{p-3} \ldots + \frac{p(p-1)}{2}X + p \tag{5.101}$$

and since p divides every coefficients except for the leading term and p^2 doesn't divide the constant term, it follows from Eisenstein's criterion 5.2.13 that $P(X+1)$ is irreducible over $\mathbb{Z}$. Therefore $P(X)$ is also irreducible, since if $P(X) = f(X)g(X)$ for $f(X), g(X) \in \mathbb{Z}[X]$, then we also have that $P(X+1) = f(X+1)g(X+1) = h(X)k(X)$ for $h(X), k(X) \in \mathbb{Z}[X]$.
To see that $P(X)$ is in fact the minimal polynomial of ζ_p, let $f(X)$ be some monic polynomial of least degree, such that $\deg(f(X)) < \deg(P(X))$ and $f(\zeta_p) = 0$. Then $P(X) = q(X)f(X) + r(X)$ for some $q, r \in \mathbb{Z}[X]$, where $\deg(r(X)) < \deg(f(X))$. Then $P(\zeta_p) = q(\zeta_p)f(\zeta_p) + r(\zeta_p) \implies 0 = 0 + r(\zeta_p)$, which implies $r(X) = 0$, because otherwise f was not of least degree. But $r(X) = 0$ implies that $P(X)$ is reducible, which is a contradiction. Thus $P(X)$ is the minimal polynomial of ζ_p. ■

Note that the above proof also shows that

$$1 = -\zeta_p^{p-1} - \zeta_p^{p-2} - \ldots - \zeta_p, \tag{5.102}$$

since ζ_p is a root of the polynomial in Equation (5.99). Since $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is a basis for $\mathbb{Q}(\zeta_p)$, so is $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$.

Definition 5.5.4 (Maximal real subfield)

Let $\mathbb{Q}(\zeta_p)$ be a cyclotomic field. We call the subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subset \mathbb{Q}(\zeta_p)$ the *maximal real subfield* of $\mathbb{Q}(\zeta_p)$.

Since $\zeta_p + \zeta_p^{-1} = 2\cos\left(\frac{2\pi}{p}\right)$ is real, $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is a totally real number field, and thus $\zeta_p \notin \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, since $\zeta_p \notin \mathbb{R}$. Consider the polynomial $f(X) = X^2 - (\zeta_p + \zeta_p^{-1})X + 1 = (X - \zeta_p)(X - \zeta_p^{-1})$. Since ζ_p is a root of $f \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})[X]$, and no monic polynomial over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of degree smaller than 2 has ζ_p as a root, f is the minimal polynomial of ζ_p over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Hence by Corollary 5.1.10, we have $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$, which justifies the term maximal real subfield [21, p. 16]. From Proposition 5.5.3 and Theorem 5.1.17, we thus have $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2}$.

Proposition 5.5.5 ([21] p. 16)
Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be a maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. Then the ring of integers of K is given by $\mathcal{O}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Proof.
We begin by showing that $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subseteq \mathcal{O}_K$. As noted before, $\mathbb{Z} \subseteq \mathcal{O}_K$, and thus, we only need to show that $\zeta_p + \zeta_p^{-1} \in \mathcal{O}_K$. Notice that the additive group generated by $1, \zeta_p + \zeta_p^{-1}, (\zeta_p + \zeta_p^{-1})^2, \ldots$ is a subgroup of the group generated by $\zeta_p^{-(p-1)}, \zeta_p^{-(p-2)}, \ldots, \zeta_p^{p-1}$. A subgroup of a finitely generated abelian group is finitely generated [16, p. 36]. Thus it follows by Lemma 5.1.19, that $\zeta_p + \zeta_p^{-1} \in \mathcal{O}_K$.
Assume $\alpha = a_0 + a_1(\zeta_p + \zeta_p^{-1}) + \ldots + a_m(\zeta_p + \zeta_p^{-1})^m \in K$, is an algebraic integer, where $m \leq \frac{p-3}{2}$. We may assume that $a_m \notin \mathbb{Z}$ since the terms where $a_i \in \mathbb{Z}$ may be removed as they belong to $\mathcal{O}_K$, as shown above. Then, multiplying by ζ_p^m, we get:

$$\zeta_p^m \alpha = \zeta_p^m a_0 + \zeta_p^m a_1(\zeta_p + \zeta_p^{-1}) + \ldots + \zeta_p^m a_m(\zeta_p + \zeta_p^{-1})^m. \tag{5.103}$$

Expanding this as a polynomial in ζ_p, we see that the constant term is a_m, and the leading term is $a_m\zeta_p^{2m}$. Since α is an algebraic integer in K, it is also an algebraic integer in $\mathbb{Q}(\zeta_p)$. Therefore it follows from Proposition 5.5.2 that $\zeta_p^m\alpha$ is an algebraic integer in $\mathbb{Q}(\zeta_p)$. Thus we have $\zeta_p^m\alpha \in \mathbb{Z}[\zeta_p]$, also by Proposition 5.5.2. Since $\zeta_p^{p-1} = -1 - \zeta_p - \ldots - \zeta_p^{p-2}$ by Equation (5.102), it follows that $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is an integral basis for $\mathbb{Z}[\zeta_p]$. Since $2m \leq p - 3$, the set $\{1, \zeta_p, \ldots, \zeta_p^{2m}\}$ forms a subset of an integral basis for $\mathbb{Z}[\zeta_p]$. It follows that $a_m \in \mathbb{Z}$, which finishes the proof. ■

One of the reasons for using maximal real subfields of cyclotomic fields for constructing lattices is that the discriminant is easy to compute.

Proposition 5.5.6 ([12] p. 396)
The discriminant of a maximal real subfield, $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of a cyclotomic field is given by $disc_K = p^{\frac{p-3}{2}}$.

Proof. This is a standard result in algebraic number theory and can be calculated by using [20, Th. 21, p. 46]. ■

Proposition 5.5.7
let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be a maximal real subfield of a cyclotomic field. Then $\{\zeta_p^j + \zeta_p^{-j}\}_{j=1}^{\frac{p-1}{2}}$ is an integral basis for K. We denote these basis elements by $e_j = \zeta_p^j + \zeta_p^{-j}$.

Proof.
Let $\alpha \in \mathcal{O}_K$ be an algebraic integer of K. Then it is also an algebraic integer of $\mathbb{Q}(\zeta_p)$. From Proposition 5.5.2 and Equation (5.102), we have that $\{\zeta_p, \ldots, \zeta_p^{p-1}\}$ is an integral basis for $\mathbb{Q}(\zeta_p)$. Thus we have $\alpha = \sum_{j=1}^{p-1} a_j \zeta_p^j$ for some $a_j \in \mathbb{Z}$. But since K is totally real, we have $\overline{\alpha} = \alpha$, so that $\alpha = \sum_{j=1}^{p-1} a_j \zeta_p^{-j} = \sum_{j=1}^{p-1} a_j \zeta_p^{p-j}$. Therefore, $a_j = a_{p-j}$ for all $1 \leq j \leq \frac{p-1}{2}$. Hence we may write $\alpha = \sum_{j=1}^{\frac{p-1}{2}} a_j(\zeta_p^j + \zeta_p^{p-j}) = \sum_{j=1}^{\frac{p-1}{2}} a_j e_j$, which finishes the proof. ■

Note that the $\frac{p-1}{2}$ embeddings of $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ into $\mathbb{C}$ can be found using the minimal polynomial of ζ_p given in equation 5.99, which shows that the embeddings of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$ is given by $\sigma_i(\zeta_p) = \zeta_p^i$ for $i \in \{1, \ldots, p-1\}$. Since σ_i is a homomorphism the embeddings of K into $\mathbb{C}$ are then given by:

$$\sigma_i(e_j) = \zeta_p^{ij} + \zeta_p^{-ij}. \tag{5.104}$$

We are now ready to construct a lattice equivalent to $\mathbb{Z}^{\frac{p-1}{2}}$.

Theorem 5.5.8 ([12] p. 396)
Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be a maximal real subfield of a cyclotomic field, and let $\alpha = \frac{1}{p}(1-\zeta_p)(1-\zeta_p^{-1}) \in K$, where $\zeta_p = e^{\frac{2\pi i}{p}}$. Then the ideal lattice $\sigma_\alpha(\mathcal{O}_K)$ is equivalent to $\mathbb{Z}^{\frac{p-1}{2}}$.

Proof.
First, we need to check that the conjugates of α are positive, $\sigma_j(\alpha) > 0$ for $j = 1, \ldots, \frac{p-1}{2}$. We denote the conjugates by $\alpha_j = \sigma_j(\alpha)$. It follows from Equation (5.104) that

$$\alpha_j = \frac{1}{p}(1-\zeta_p^j)(1-\zeta_p^{-j}) = \frac{1}{p}(2-(\zeta_p^j + \zeta_p^{-j})) = \frac{1}{p}\left(2 - 2\cos\left(\frac{2j\pi}{p}\right)\right). \tag{5.105}$$

Since $1 \leq j \leq \frac{p-1}{2}$ we clearly have $\alpha_j > 0$, which means that $\sigma_\alpha(\mathcal{O}_K)$ is indeed an ideal lattice. By Proposition 5.5.7 and Equation (5.88), we have that the (i,j)-entry of the Gram matrix of the lattice is given by $G_{ij} = Tr(\alpha(\zeta_p^i + \zeta_p^{-i})(\zeta_p^j + \zeta_p^{-j})) = Tr(\alpha e_i e_j)$. To compute the Gram matrix, note first that by Equation (5.102), we have:

$$Tr(e_j) = Tr(\zeta_p^j + \zeta_p^{-j}) = \sum_{i=1}^{\frac{p-1}{2}} \sigma_i(\zeta_p^j + \zeta_p^{-j}) \tag{5.106}$$

$$= \sum_{i=1}^{\frac{p-1}{2}} (\zeta_p^{ij} + \zeta_p^{-ij}) \tag{5.107}$$

$$= \zeta_p^j \sum_{i=1}^{\frac{p-1}{2}} (\zeta_p^i + \zeta_p^{p-i}) \tag{5.108}$$

$$= \sum_{i=1}^{p-1} \zeta_p^i = -1, \quad j = 1, 2, \ldots, \frac{p-1}{2}, \tag{5.109}$$

where the second to last equality follows by reducing the exponent modulo p. Using this we obtain:

$$Tr(\alpha e_j) = \sum_{i=1}^{\frac{p-1}{2}} \alpha_i(\zeta_p^{ij} + \zeta_p^{-ij}) \tag{5.110}$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{p}(2 - (\zeta_p^i + \zeta_p^{-i}))(\zeta_p^{ij} + \zeta_p^{-ij}) \tag{5.111}$$

$$= \frac{1}{p}\left(\sum_{i=1}^{\frac{p-1}{2}} 2(\zeta_p^{ij} + \zeta_p^{-ij}) - \sum_{i=1}^{\frac{p-1}{2}} \left(\zeta_p^{(j+1)i} + \zeta_p^{(j-1)i} + \zeta_p^{-(j+1)i} + \zeta_p^{-(j-1)i}\right)\right) \tag{5.112}$$

$$= \frac{1}{p}\left(-2 - \sum_{i=1}^{\frac{p-1}{2}} \left(\zeta_p^{(j+1)i} + \zeta_p^{-(j+1)i}\right) - \sum_{i=1}^{\frac{p-1}{2}} \left(\zeta_p^{(j-1)i} + \zeta_p^{-(j-1)i}\right)\right) \tag{5.113}$$

$$= \begin{cases} -1, \text{ if } j \equiv \pm 1 \pmod{p} \\ 0, \text{ otherwise} \end{cases}, \tag{5.114}$$

where the last equality follows from the fact that if $j \equiv \pm 1 \pmod{p}$, then one of the sums in Equation (5.113) equals $p - 1$ and the other equals -1 and otherwise both sums equals -1.
Using the result above, we are now ready to compute $Tr(\alpha e_i e_j)$. We begin with the case $i = j$:

$$Tr(\alpha e_j e_j) = \sum_{i=1}^{\frac{p-1}{2}} \alpha_i(\zeta_p^{2ij} + \zeta_p^{-2ij} + 2) \tag{5.115}$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \alpha_i(\zeta_p^{2ij} + \zeta_p^{-2ij}) + \sum_{i=1}^{\frac{p-1}{2}} 2\alpha_i \tag{5.116}$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \alpha_i(\zeta_p^{2ij} + \zeta_p^{-2ij}) + 2\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{p}(2 - (\zeta_p^i + \zeta_p^{-i})) \tag{5.117}$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \alpha_i(\zeta_p^{2ij} + \zeta_p^{-2ij}) + \frac{2}{p}\left(\frac{2(p-1)}{2} + 1\right) \tag{5.118}$$

$$= \begin{cases} -1 + 2 = 1, \text{ if } j = \frac{p-1}{2} \text{ i.e } 2j \equiv -1 \pmod{p} \\ 2, \text{ otherwise} \end{cases}, \tag{5.119}$$

where the last equality follows from Equation (5.114), and the fourth equality follows from Equation (5.109). For the case $i \neq j$, we get:

$$Tr(\alpha e_i e_j) = \sum_{k=1}^{\frac{p-1}{2}} \alpha_k(\zeta_p^{k(i+j)} + \zeta_p^{-k(i+j)}) + \sum_{k=1}^{\frac{p-1}{2}} \alpha_k(\zeta_p^{k(i-j)} + \zeta_p^{-k(i-j)}) \tag{5.120}$$

$$= \begin{cases} -1, \text{ if } |i-j| = 1 \\ 0, \text{ otherwise} \end{cases}, \tag{5.121}$$

where the last equality follows from Equation (5.114), and the fact that $0 < i, j \leq \frac{p-1}{2}$ implies that $i + j \not\equiv \pm 1 (\text{mod } p)$.

Thus the Gram matrix of the lattice $\sigma_\alpha(\mathcal{O}_K)$ is given by:

$$G = \begin{bmatrix} 2 & -1 & 0 & \dots & & 0 \\ -1 & 2 & -1 & & & \\ 0 & -1 & 2 & & & \vdots \\ & & & \ddots & & \\ \vdots & & & & 2 & -1 & 0 \\ & & & & -1 & 2 & -1 \\ 0 & & \dots & & 0 & -1 & 1 \end{bmatrix}. \tag{5.122}$$

We define the following unimodular $\frac{p-1}{2} \times \frac{p-1}{2}$ matrix:

$$U = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ -1 & 1 & 0 & \dots & 0 \\ 0 & -1 & \ddots & & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \dots & 0 & -1 & 1 \end{bmatrix}. \tag{5.123}$$

Computing the matrix product shows that:

$$G = U^T I U. \tag{5.124}$$

Hence, denoting the generator matrix of $\sigma_\alpha(\mathcal{O}_K)$ by M, we may write:

$$G = M^T M = U^T I U = (IU)^T (IU). \tag{5.125}$$

Since I is a generator matrix of $\mathbb{Z}^{\frac{p-1}{2}}$, it suffices to show that $M = PIU$ for an orthogonal matrix P, because then the lattice $\sigma_\alpha(\mathcal{O}_K)$ is equivalent to $\mathbb{Z}^{\frac{p-1}{2}}$ by Definition 4.2.2 and Proposition 4.2.4.

We will show the existence of P using Equation (5.125) and polar decomposition. Since M and U are invertible matrices they have a unique polar decomposition given by [5]:

$$M = P_1\sqrt{M^T M}, \qquad \text{and} \qquad U = P_2\sqrt{U^T U} \tag{5.126}$$

respectively, where P_1 and P_2 are orthogonal matrices. But by Equation (5.125) we have $\sqrt{M^T M} = \sqrt{U^T U}$ so that $P_1^{-1} M = P_2^{-1} U$, or by rearranging, $M = P_1 P_2^{-1} U$. Since $P = P_1 P_2^{-1}$ is orthogonal, we are done. ■

The generator matrix of an ideal lattice, was given in Equation (5.83). In this case, it can be written as a product of the matrix R with elements $R_{i,j} = \sigma_i(e_j) = 2\cos\left(\frac{2\pi ij}{p}\right)$ and the diagonal matrix $A = \text{diag}\left(\sqrt{\sigma_i(\alpha)}\right)$. So that the generator matrix for the rotated $\mathbb{Z}^n$ lattice is given by:

$$M = AR. \tag{5.127}$$

Proposition 5.5.9

Let $\sigma_\alpha(\mathcal{O}_K)$ be an ideal lattice of dimension $n = \frac{p-1}{2}$ as defined in Theorem 5.5.8, then

$$d_{p,min}(\sigma_\alpha(\mathcal{O}_K)) = p^{-\frac{n-1}{2}}. \tag{5.128}$$

Proof.

From Proposition 5.4.6 we have that:

$$d_{p,min}(\sigma_\alpha(\mathcal{O}_K)) = \sqrt{\frac{\det(\sigma_\alpha(\mathcal{O}_K))}{|disc_K|}} = \frac{1}{\sqrt{|disc_K|}}, \tag{5.129}$$

since it follows from Equation (5.124), that the Gram matrix, G, of $\sigma_\alpha(\mathcal{O}_K)$ has determinant 1. From Proposition 5.5.6 we have that $disc_K = p^{\frac{p-3}{2}} = p^{n-1}$, and it follows that:

$$d_{p,min}(\sigma_\alpha(\mathcal{O}_K)) = p^{-\frac{n-1}{2}}. \tag{5.130}$$

■

Example 5.5.10

We now give an example of how to build a rotated $\mathbb{Z}^2$ lattice with maximal diversity. From Theorem 5.5.8 we know that this can be built from the field $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where $p = 5$. The generator matrix can then be found using Equation (5.127). Since $p = 5$ the matrix R has elements $R_{i,j} = 2\cos\left(\frac{2\pi ij}{5}\right)$. From Equation (5.105) we have that $\sigma_i(\alpha) = \frac{1}{5}\left(2 - 2\cos\left(\frac{2i\pi}{5}\right)\right)$, so the matrix $A = \text{diag}\left(\sqrt{\frac{1}{5}\left(2 - 2\cos\left(\frac{2\pi}{5}\right)\right)}, \sqrt{\frac{1}{5}\left(2 - 2\cos\left(\frac{4\pi}{5}\right)\right)}\right)$. We then have:

$$M = AR \approx \begin{bmatrix} 0.3249 & -0.8507 \\ -1.3764 & 0.5257 \end{bmatrix}. \tag{5.131}$$

From Proposition 5.5.9 we have that the minimum product distance of this lattice code is:

$$d_{p,min}(\sigma_\alpha(\mathcal{O}_K)) = 5^{-\frac{1}{2}}. \tag{5.132}$$

This lattice is actually the optimal rotated $\mathbb{Z}^2$ lattice in terms of highest minimum product distance [13]. □

6 The Sphere Decoder

6.1 The Algorithm

This section is based on [12, Ch. 4].
In order to decode a received message, we need to be able to determine the closest lattice point to a given received point. If we were to search through every lattice point this would be an computationally heavy task. Instead we only search through points inside a sphere of a given radius $\sqrt{C}$ centered on the received point. This is the basic premise in the sphere decoder algorithm. In order to ensure that there is a point inside this sphere, we set $\sqrt{C}$ equal to the covering radius of the lattice as defined in Definition 4.2.5. The sphere decoder may be more efficient with a smaller initial choice of $\sqrt{C}$. The initial choice of $\sqrt{C}$ may even be adapted to the variance of the additive noise [12, p. 363]. By choosing a smaller search radius, we may find no points in the sphere. In this case we subsequently try with a larger search radius, until a point is found. We will not be considering the efficiency of the sphere decoder, so we use the covering radius as the search radius. In [7], an upper bound for the number of arithmetic operations of the sphere decoder is calculated. For a given lattice and search radius, the complexity is shown to be polynomial.

We consider the lattice $\Lambda = \{\mathbf{x} = M\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}^n\}$ and let the received point be denoted by $\mathbf{r} = M\boldsymbol{\rho}$, where $\boldsymbol{\rho} = [\rho_1, \dots, \rho_n]^T \in \mathbb{R}^n$. The problem we need to solve is then:

$$\min_{\mathbf{x}\in\Lambda} ||\mathbf{r} - \mathbf{x}||^2 = \min_{\mathbf{w}\in\Lambda-\mathbf{r}} ||\mathbf{w}||^2. \tag{6.1}$$

Note that $\mathbf{w} = M\boldsymbol{\xi}$, where $\boldsymbol{\xi} = [\xi_1, \dots, \xi_n]^T \in \mathbb{R}^n$ for $\xi_i = u_i - \rho_i$, and we therefore search in the lattice $\Lambda_r = \{\mathbf{w} = M\boldsymbol{\xi} | \boldsymbol{\xi} \in \mathbb{R}^n\}$ centered at $\mathbf{r}$. Points inside a sphere of radius $\sqrt{C}$ in this lattice satisfies the following inequality:

$$||\mathbf{w}||^2 = Q(\boldsymbol{\xi}) = \boldsymbol{\xi}^T M^T M \boldsymbol{\xi} = \boldsymbol{\xi}^T G \boldsymbol{\xi} = \sum_{i=1}^{n}\sum_{j=1}^{n} G_{ij}\xi_i\xi_j \leq C. \tag{6.2}$$

Since the inner product is symmetric and positive definite, the Gram matrix is symmetric and positive definite. Thus we can find its Cholesky's factorization $G = R^T R$, where R is an upper triangular matrix. Then

$$Q(\boldsymbol{\xi}) = \boldsymbol{\xi}^T R^T R \boldsymbol{\xi} = ||R\boldsymbol{\xi}||^2 = \sum_{i=1}^{n} \left(R_{ii}\xi_i + \sum_{j=i+1}^{n} R_{ij}\xi_j \right)^2 \leq C. \tag{6.3}$$

By making the substitutions $Q_{ii} = R_{ii}^2$ for $i = 1, \ldots, n$ and $Q_{ij} = \frac{R_{ij}}{R_{ii}}$ for $i = 1, \ldots, n$ and $j = i+1, \ldots, n$ this can be rewritten as:

$$Q(\boldsymbol{\xi}) = \sum_{i=1}^{n} Q_{ii} \left(\xi_i + \sum_{j=i+1}^{n} Q_{ij} \xi_j \right)^2 = \sum_{i=1}^{n} Q_{ii} U_i^2 \leq C, \tag{6.4}$$

where

$$U_i = \xi_i + \sum_{j=i+1}^{n} Q_{ij} \xi_j, \quad i = 1, \ldots, n. \tag{6.5}$$

We are now able to find an interval which U_n must belong to and thereby all the possible values of U_n. For each of these values we can then work backwards and determine the possible values of U_{n-1} given U_n and so on. The ranges are given as follows:

$$\begin{aligned} -\sqrt{\frac{C}{Q_{nn}}} \leq & U_n \leq \sqrt{\frac{C}{Q_{nn}}} \\ -\sqrt{\frac{C - Q_{nn}U_n^2}{Q_{n-1,n-1}}} \leq & U_{n-1} \leq \sqrt{\frac{C - Q_{nn}U_n^2}{Q_{n-1,n-1}}} \\ & \vdots \end{aligned} \tag{6.6}$$

By replacing $\xi_i = u_i - \rho_i$ in Equation (6.5) and inserting the resultant U_i in Equation (6.6) we get the ranges for the integer components of $\mathbf{x}$:

$$\begin{aligned} \left\lceil -\sqrt{\frac{C}{Q_{nn}}} + \rho_n \right\rceil \leq & u_n \leq \left\lfloor \sqrt{\frac{C}{Q_{nn}}} + \rho_n \right\rfloor \\ \left\lceil -\sqrt{\frac{C - Q_{nn}\xi_n^2}{Q_{n-1,n-1}}} + \rho_{n-1} - Q_{n-1,n}\xi_n \right\rceil \leq & u_{n-1} \leq \left\lfloor \sqrt{\frac{C - Q_{nn}\xi_n^2}{Q_{n-1,n-1}}} + \rho_{n-1} - Q_{n-1,n}\xi_n \right\rfloor \\ & \vdots \end{aligned} \tag{6.7}$$

In general we have for the i'th component that:

$$\begin{aligned} & \left\lceil -\sqrt{\frac{1}{Q_{ii}} \left(C - \sum_{l=i+1}^{n} Q_{ll} \left(\xi_l + \sum_{j=l+1}^{n} Q_{lj} \xi_j \right)^2 \right)} + \rho_i - \sum_{j=i+1}^{n} Q_{ij} \xi_j \right\rceil \leq \\ & u_i \leq \\ & \left\lfloor \sqrt{\frac{1}{Q_{ii}} \left(C - \sum_{l=i+1}^{n} Q_{ll} \left(\xi_l + \sum_{j=l+1}^{n} Q_{lj} \xi_j \right)^2 \right)} + \rho_i - \sum_{j=i+1}^{n} Q_{ij} \xi_j \right\rfloor . \end{aligned} \tag{6.8}$$

In practice the bounds are updated recursively by using the following definitions:

$$S_i = S_i(\xi_{i+1}, \ldots, \xi_n) = \rho_i - \sum_{j=i+1}^{n} Q_{ij}\xi_j \tag{6.9}$$

$$T_{i-1} = T_{i-1}(\xi_i, \ldots \xi_n) = C - \sum_{l=i}^{n} Q_{ll}\left(\xi_l + \sum_{j=l+1}^{n} Q_{lj}\xi_j\right)^2 \tag{6.10}$$

$$= T_i - Q_{ii}(u_i - S_i)^2. \tag{6.11}$$

Using these, the bounds of the i'th component are given by:

$$\left\lceil -\sqrt{\frac{T_i}{Q_{ii}}} + Si \right\rceil \leq u_i \leq \left\lfloor \sqrt{\frac{T_i}{Q_{ii}}} + Si \right\rfloor. \tag{6.12}$$

We also see that when a lattice point inside the sphere is found, its distance to the center, and therefore the received point is given by:

$$Q(\boldsymbol{\xi}) = \sum_{i=1}^{n} Q_{ii}\left(\xi_i + \sum_{j=i+1}^{n} Q_{ij}\xi_j\right)^2 = C - T_1 + Q_{11}(u_1 - S_1)^2. \tag{6.13}$$

The algorithm works in an order from the n'th dimension down to the first dimension. It starts by taking the smallest u_n satisfying the bounds in Equation (6.12) then finding smallest u_{n-1} satisfying the bounds given by the u_n and so on. If at some point u_k there is no u_{k-1} satisfying the bounds, the algorithm traces back to u_{k-1} and proceeds from $u_{k-1} + 1$ if this value satisfies the given bounds. When the algorithm reaches the 1'st dimension we have found a vector inside the sphere, and its distance from $\mathbf{r}$ is given by Equation (6.13). This value is compared to the minimum square distance d^2 (initially set equal to C) found so far in the search. If it is smaller we have a new candidate for the closets point, and we continue the search with a new sphere of this radius. If not we trace back to the previously computed u_2 and proceed as usual. A flow chart of the algorithm can be seen in Figure 6.1.

When decoding a message sent through a fading channel with perfect CSI at the receiver, we simply apply the sphere decoding algorithm to the lattice where each component has been compressed or enlarged by a known factor α_i. Hence if we send a point from the lattice $\Lambda = \{\mathbf{x} = M\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}^n\}$, we consider the lattice $\Lambda_f = \{\mathbf{x} = AM\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}^n\}$, where $A = diag(\alpha_1, \ldots, \alpha_n)$. Then by applying the algorithm to the lattice Λ_f in order to decode the received point $\mathbf{r}$, the decoded point $\hat{\mathbf{x}}_f \in \Lambda_f$ will have the same integer components $(\hat{u_1}, \ldots, \hat{u_n})$ as $\hat{\mathbf{x}} \in \Lambda$.

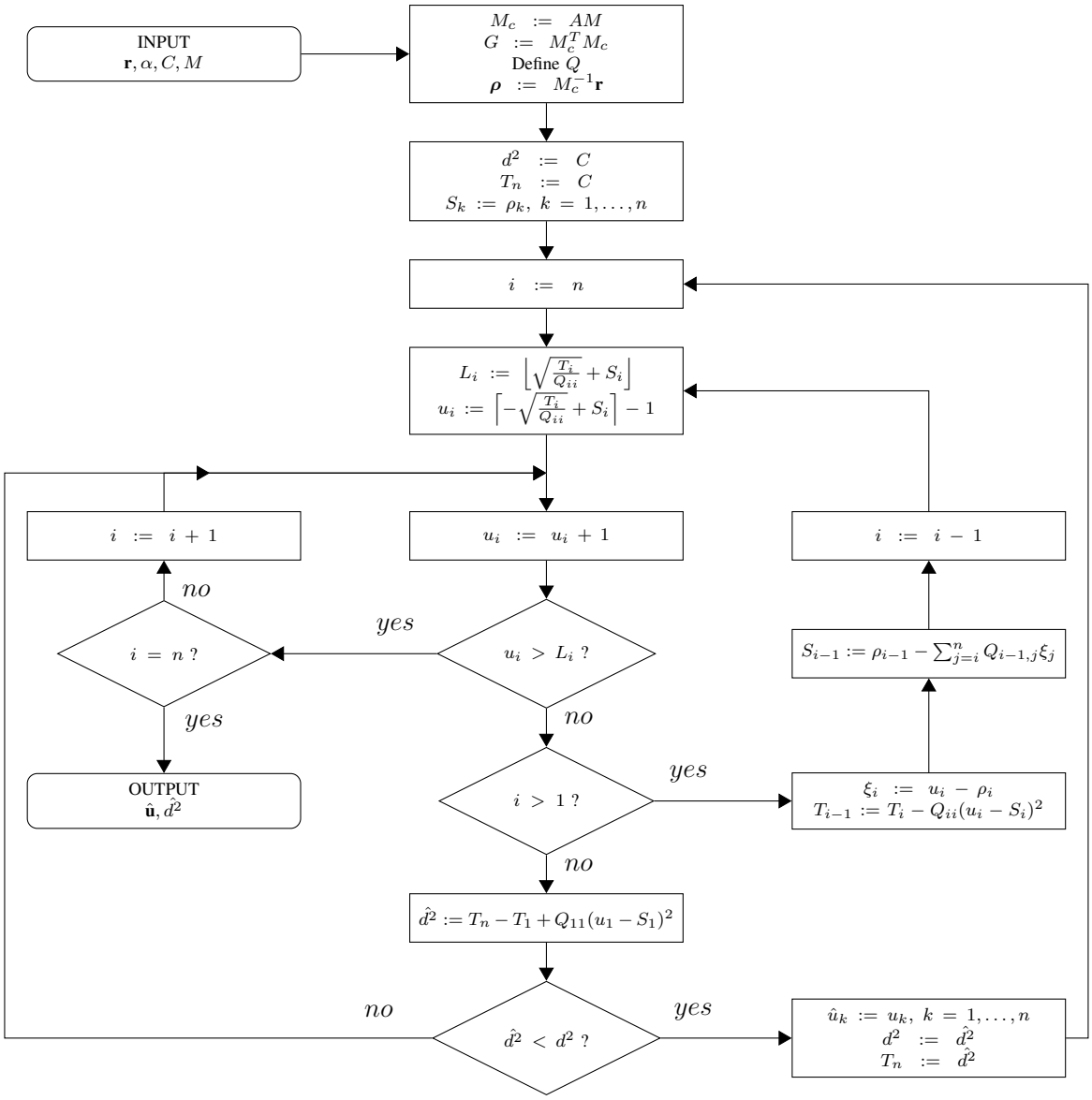

Figure 6.1: *Flow chart of the sphere decoder algorithm.* $A = diag(\alpha_1, \ldots, \alpha_n)$*, and* Q *is defined as described in this section. [12, p. 367]*

6.2 Application of the Sphere Decoder

The algorithm was implemented in MATLAB and can be seen in Appendix A. Using this we can compare the error rate in decoding messages sent by using the $\mathbb{Z}^2$ lattice and a rotated $\mathbb{Z}^2$ lattice. The generator of the optimal rotated $\mathbb{Z}^2$ lattice was found in Example 5.5.10. In order to compare the error rates of the two lattice codes, we have generated $10.000.000$ uniformly distributed random 2-dimensional integer vectors, $\mathbf{u}_i$, with entries between -100 and 100. For every $\mathbf{u}_i$ we have generated a Rayleigh distributed random 2-dimensional vector $\boldsymbol{\alpha}_i$ with scale parameter 1 and a normal distributed random 2-dimensional vector, $\mathbf{n}_i$ with mean 0 and variance

0.01. Thus we simulated 10.000.000 received points for each of the two lattice codes:

$$\mathbf{r}_i = \boldsymbol{\alpha}_i * M\mathbf{u}_i + \mathbf{n}_i \tag{6.14}$$

where M denotes the generator matrix of the respective lattice, and $*$ denotes component-wise multiplication. The resulting received vectors, $\mathbf{r}_i$, were then decoded using the sphere decoder with the corresponding generator matrix. We calculated the error rate for each lattice as $error\ rate = \frac{number\ of\ wrongly\ decoded\ integer\ vectors}{10.000.000}$. The simulation were repeated with Gaussian noise with variance $\sigma^2 = 0.02,\ 0.03, \ldots,\ 0.1$. The resulting error rates can be seen in Figure 6.2. The error rates of the rotated lattice are significantly lower than those of the $\mathbb{Z}^2$ lattice.

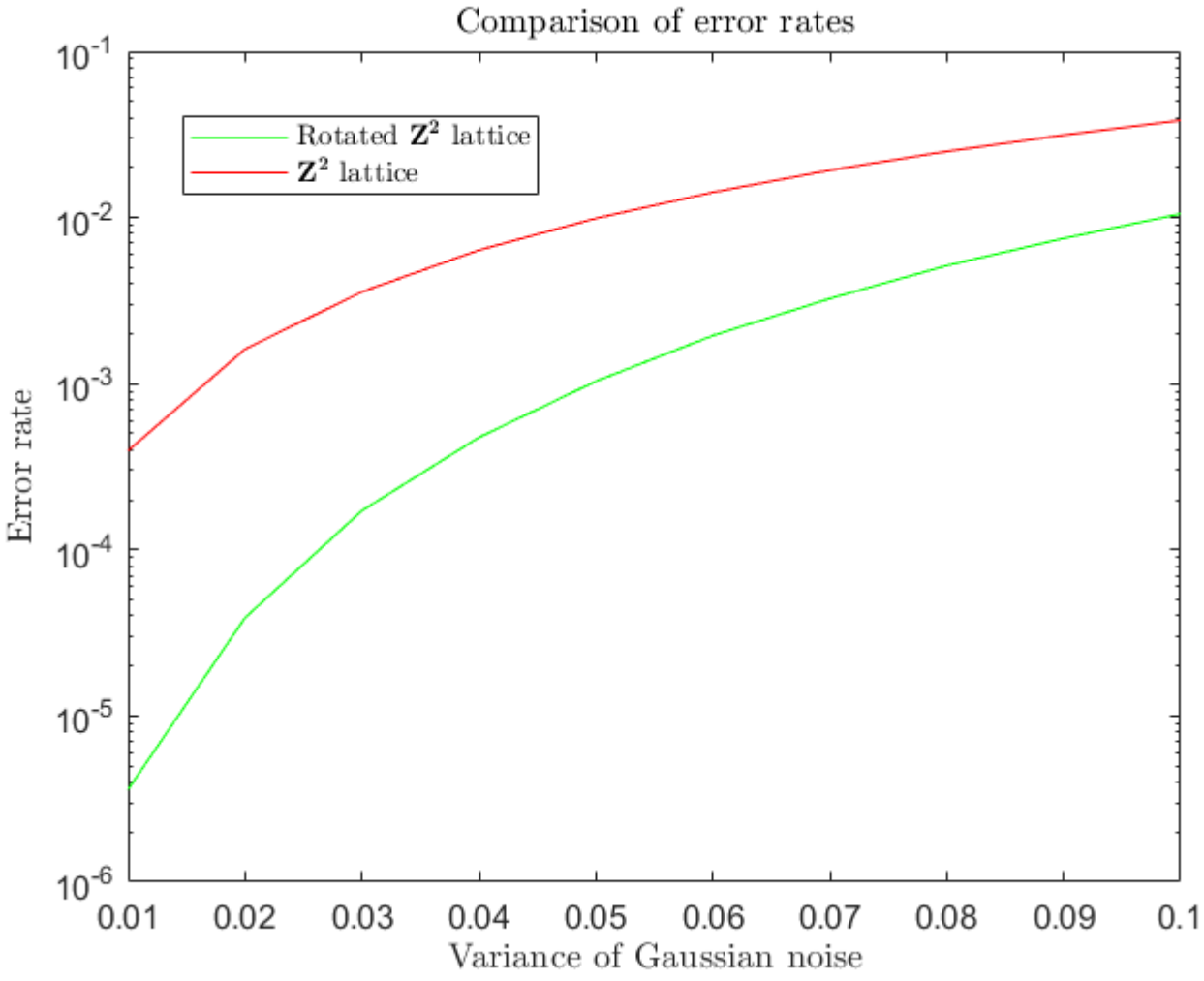

Figure 6.2: *Error rates of the rotated $\mathbb{Z}^2$ lattice code (green) and the $\mathbb{Z}^2$ lattice code (red).*

The MIMO Case 7

So far we have considered a communication system with one antenna at the transmitter and one antenna at the receiver, which is called a single-input and single-output system or SISO. When multiple antennas are available at both the transmitter and receiver, we call it a multiple-input and multiple-output system, abbreviated MIMO. The multiple antennas in a MIMO channel allows for a higher data throughput than in a SISO channel. MIMO technologies are used in many modern wireless communication systems. For example the common WiFi protocols IEEE 802.11n and 802.11ac supports MIMO technologies [3]. In this chapter we describe how to build suitable codes for MIMO channels using cyclic division algebras.

7.1 The MIMO System Model

This section is based on [14, ch. 2].
We consider a system with n_r receive antennas and n_t transmit antennas. If we consider a time interval of T symbol durations, the channel can then be expressed as[14, p. 6]:

$$Y_{n_r \times T} = H_{n_r \times n_t} X_{n_t \times T} + Z_{n_r \times T}. \tag{7.1}$$

The i, j entries in the channel matrix H corresponds to the channel coefficient between the jth transmit and the ith receive antenna. These channel coefficients are modelled as complex Gaussian random variables with zero mean and unit variance $\mathcal{N}_c(0, 1)$, which means it is a Rayleigh fading model. The entries in Z corresponds to the spatially and temporally additive white noise and is modelled as complex Gaussian random variables with mean 0 and variance N_0. The i, k entry of X corresponds to the signal transmitted from the ith antenna during the kth symbol interval, $1 \leq k \leq T$. We assume that the channel coefficients are known at the receiver and remain constant during T symbol durations and that H is independent of X and Z. Each matrix, X, is called a codeword and a set, $\mathcal{C}$, of codewords is called a codebook. We restrict ourselves to the case of square matrices, (i.e. $n_r = n_t = T$), and only consider linear codes.

Definition 7.1.1 (Linear code)
Let $\mathcal{C}$ be a codebook. Then $\mathcal{C}$ is called a *linear code* if:

$$\forall X, X' \in \mathcal{C} : X \pm X' \in \mathcal{C}. \tag{7.2}$$

Any linear code will obviously have to contain an infinite amount of codewords. Like in the SISO case, our object is to minimize the codeword error probability $P(e)$. In the same way

that we carved a signal constellation from an infinite lattice in the SISO case, we carve a finite codebook from a linear code. If $|\mathcal{C}|$ denotes the cardinality of such a finite code carved from a linear code, then an upper bound for the error probability is given by[14, p. 11]:

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{X \neq O} P(O - X), \tag{7.3}$$

where O is the zero-matrix and

$$P(O - X) \leq \left(\frac{\Delta^{\frac{1}{r}}}{4N_0} \right)^{-rn_r} \tag{7.4}$$

where r denotes the rank of X, and Δ is the product of the non-zero eigenvalues of $XX^\dagger$. As a result the asymptotically dominant terms have the lowest exponent rn_r. If every codeword X in the codebook have full rank the code is said to be fully diverse. For a fully diverse code every exponent is n_r^2 and since the determinant is equal to the product of eigenvalues, the dominant term in Equation (7.3) will be the one with minimum determinant:

$$\Delta_{\min}(\mathcal{C}) = \min_{X \neq O} \det(XX^\dagger), \tag{7.5}$$

where $\mathcal{C}$ is the codebook. Therefore we will be interested in constructing full diversity codes with large minimum determinant. Here the minimum determinant is taken over the codewords in some finite codebook. We may also require that the determinants of the linear codes, from which the finite codebook is carved, are bounded away from zero, since adaptive modulation schemes require transmission of different size constellations [14, p. 19]. This is also called the *non-vanishing determinant* property. A finite code, $\mathcal{C}$ carved from a linear code $\mathcal{C}_\infty$ will have minimum determinant $\Delta_{\min}(\mathcal{C}) \geq \Delta_{\min}(\mathcal{C}_\infty) = \liminf\{\det(XX^\dagger) \mid O \neq X \in \mathcal{C}_\infty\})$ so by considering linear codes with large minimum determinant, we will have large minimum determinant for any finite codebook carved from the linear code. Therefore our focus will be on constructing full diversity linear codes with large minimum determinant. Finally, in order to save on the average transmitted energy we will require that our codebooks exhibit what is referred to as *cubic shaping*. In practice this means that each layer of a codeword (defined later in 7.2.7), when written on the form (7.19), can be written as a product, $M\mathbf{v}$, of a unitary matrix M and a vector $\mathbf{v}$ containing the information symbols [14, p. 66].

7.2 Cyclic Division Algebras

This section is based on [14, ch. 4].
We begin by defining what is meant by an algebra.

Definition 7.2.1 (Algebra)
Let F be a field. An *algebra*, $\mathcal{A}$, over F is a set with operations of addition and multiplication, which are maps $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$, as well as scalar multiplication, which is a map $F \times \mathcal{A} \to \mathcal{A}$, such that:

1. $\mathcal{A}$ is a vector space over F with with respect to addition and scalar multiplication,
2. $\mathcal{A}$ is a ring with respect to addition and multiplication,
3. $(\lambda a)b = a(\lambda b) = \lambda(ab)$ for any $\lambda \in F$ and any $a, b \in \mathcal{A}$.

Note that property 2 in Definition 7.2.1 assures that the algebra is associative, and that multiplication is distributive over addition. Also, we use the convention that a ring must have a multiplicative identity element, and therefore an algebra also has a multiplicative identity element. In other literature, an algebra does not necessarily have a multiplicative identity, and those that do are called unital or unitary algebras. With our definition every algebra is unital. We will be particularly interested in division algebras.

Definition 7.2.2 (Division algebra)
A division algebra, $\mathcal{A}$, is a non-zero algebra in which every non-zero element, $a \in \mathcal{A}$, has a multiplicative inverse, $a^{-1} \in \mathcal{A}$ such that $aa^{-1} = 1$, where $1 \in \mathcal{A}$ is the multiplicative identity element.

In Definition 5.2.4 we introduced the notion of $\mathbb{Q}-$homomorphisms, which allowed us to consider embeddings of a number field into $\mathbb{C}$. Now, we will restrict our attention to automorphisms on an extension field.

Definition 7.2.3 (K-automorphisms)
Let L/K be a field extension. A K-automorphism is an isomorphism, $\varphi : L \to L$, which fixes K, i.e. $\varphi(a) = a$ for all $a \in K$.

Proposition 7.2.4 ([18] p. 72)
Let L/K be a field extension, then the set of all K-automorphisms of L forms a group under composition of maps.

Proof.
Let α and β be K-automorphisms of L. Then $\alpha\beta$ is cearly an automorphism, and for $k \in K$ we have that $\alpha\beta(k) = \alpha(k) = k$, so $\alpha\beta$ is a K-automorphism. Composition of maps is associative, the identity map on L is obviously a K-automorphism, and finally α^{-1} is a K-automorphism of L, since it is obviously an automorphism and:

$$k = \alpha^{-1}\alpha(k) = \alpha^{-1}(k). \tag{7.6}$$

Thus the set of all K-automorphisms of L is a group. ■

The group of all K-automorphisms of L is denoted by $Aut(L/K)$. This allows us to make the following definition.

Definition 7.2.5 (Galois extension, Galois group [6] p. 9)
Let K be a number field and let L/K be a finite field extension. Then L/K is a *Galois extension* if $|Aut(L/K)| = [L : K]$. We call the group consisting of all the $K-$automorphisms of L the *Galois group* of L/K, denoted by $Gal(L/K)$.

When K is a number field, we call a field extension, L/K a number field extension. We are now ready to define the family of cyclic algebras.

Definition 7.2.6 (Cyclic algebra)
Let L/K be a Galois extension of degree n, such that its Galois group $Gal(L/K)$ is cyclic with generator σ. Let $0 \neq \gamma \in K$. We construct a non-commutative algebra, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$ as follows:

$$\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L \tag{7.7}$$

such that e satisfies

$$e^n = \gamma \text{ and } \lambda e = e\sigma(\lambda) \text{ for } \lambda \in L, \tag{7.8}$$

and $\oplus$ denotes the direct sum. Such an algebra is called a *cyclic algebra*.

We wish to show that $\mathcal{A} = (L/K, \sigma, \gamma)$ from Definition 7.2.6 is in fact an algebra over L. The vector space structure comes naturally, as an element $x \in A$ can be written as $x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}$ with $x_i \in L$ for $i = 0, \ldots, n-1$. Addition and scalar multiplication is defined in the following way. For $x, y \in \mathcal{A}$ and $\lambda \in L$ we have:

$$\begin{aligned} x + y &= (x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}) + (y_0 + ey_1 + \ldots + e^{n-1}y_{n-1}) && (7.9)\\ &= (x_0 + y_0) + e(x_1 + y_1) + \ldots + e^{n-1}(x_{n-1} + y_{n-1}), && (7.10)\\ \lambda x &= \lambda x_0 + \lambda e x_1 + \ldots + \lambda e^{n-1}x_{n-1} && (7.11)\\ &= x_0\lambda + ex_1\sigma(\lambda) + \ldots + e^{n-1}x_{n-1}\sigma^{n-1}(\lambda), && (7.12) \end{aligned}$$

where we used the rule $\lambda e = e\sigma(\lambda)$ in the last equality. With these operations, the axioms for a vector space are easily seen to be satisfied.
We need to describe the multiplication in $\mathcal{A}$ to see that it forms a ring. Let $(x_0 + ex_1 + \ldots + e^{n-1}x_{n-1})$ and $(y_0 + ey_1 + \ldots + e^{n-1}y_{n-1})$ be two elements in $\mathcal{A}$ then the product xy consists of terms on the form $e^k x_k e^h y_h = e^{k+h}\sigma^h(x_k)y_h$, where $k, h \in \{0, \ldots, n-1\}$. Thus remembering

that $e^n = \gamma$ the product can be written as:

$$xy = A_0 + eA_1 + \ldots + e^{n-1}A_{n-1}, \text{ where} \tag{7.13}$$

$$A_0 = \sum_{k+h=0} \sigma^h(x_k)y_h + \sum_{k+h=n} \gamma\sigma^h(x_k)y_h \tag{7.14}$$

$$A_1 = \sum_{k+h=1} \sigma^h(x_k)y_h + \sum_{k+h=n+1} \gamma\sigma^h(x_k)y_h \tag{7.15}$$

$$\vdots$$

$$A_{n-1} = \sum_{k+h=n-1} \sigma^h(x_k)y_h. \tag{7.16}$$

Thus the product xy can be written, in the basis $\{1, e, \ldots, e^{n-1}\}$, as the matrix equation:

$$xy = \begin{bmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \ldots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \sigma^{n-1}(x_0) \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-2} \\ y_{n-1} \end{bmatrix} \tag{7.17}$$

Since multiplication is equivalent to the above matrix multiplication, it follows that $\mathcal{A}$ is a ring with respect to addition and multiplication. It also follows that $(\lambda a)b = a(\lambda b) = \lambda(ab)$ for any $\lambda \in F$ and any $a, b \in \mathcal{A}$, and thus $\mathcal{A} = (L/K, \sigma, \gamma)$ is an algebra. Equation (7.17) also shows how we may think of elements of $\mathcal{A}$ as matrices in $M_n(L)$. It is these matrices that later will be used to build a codebook. In general this means that if L/K has degree n each coefficient x_k of x will encode n information symbols. These n information symbols belonging to a given x_k are distributed within one layer of the codeword defined as follows.

Definition 7.2.7 (Layer)
A *layer* l of the codeword, is defined for $l = 1, \ldots, n$ as the set of matrix entries in positions:

$$(k, (l + k - 1)\text{mod}(n) + 1), \text{ for } k = 1, \ldots, n. \tag{7.18}$$

Each layer can, up to multiplication by γ, be written as a vector of the form:

$$\begin{bmatrix} x_k & \sigma(x_k) & \ldots & \sigma^{n-1}(x_k) \end{bmatrix}^T, \quad k = 0, \ldots n-1. \tag{7.19}$$

An algebra which is both a cyclic algebra and a division algebra is called a cyclic division algebra. In a cyclic division algebra $\mathcal{A}$, the matrix in Equation (7.17) is invertible, and we are therefore able to construct fully diverse codes using elements from $\mathcal{A}$ and their corresponding matrices in $M_n(L)$. We therefore wish to determine when a cyclic algebra is actually a cyclic division algebra. First we make an equivalent definition of how a field extension L/K is embedded into $\mathbb{C}$. In a number field the embeddings were defined by the distinct zeros of the

minimum polynomial, p_θ, of θ (see Theorem 5.2.9). Thus we can think of $\mathbb{Q}(\theta)$ as being build by adding the n roots of the polynomial p_θ to $\mathbb{Q}$. In the same way we can add the n roots of p_θ to a number field $\mathbb{Q}(\alpha)$ and still have the n embeddings, now fixing $\mathbb{Q}(\alpha)$. The embeddings are still defined by $\sigma_i(\theta) = \theta_i$, where θ_i are the n distinct roots of p_θ. This requires that p_θ is also the minimal polynomial of θ over $\mathbb{Q}(\alpha)$, i.e. $[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\alpha)] = n$. Thus there are at least n embeddings from $\mathbb{Q}(\alpha, \theta) \to \mathbb{C}$, which fixes $\mathbb{Q}(\alpha)$, and as we will show now, there are exactly n of these embeddings. Assume for contradiction that there are $n + 1$ distinct embeddings,

$$\sigma_i : \mathbb{Q}(\alpha, \theta) \to \mathbb{C},\ i = 1, \ldots, n + 1, \tag{7.20}$$

which fixes $\mathbb{Q}(\alpha)$. Say $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$. Then by Theorem 5.2.9, we have m distinct embeddings

$$\varphi_j : \mathbb{Q}(\alpha) \to \mathbb{C},\ j = 1, \ldots, m, \tag{7.21}$$

which fixes $\mathbb{Q}$. This implies that there are $(n + 1)m$ distinct embeddings of the form $\varphi_j \circ \sigma_i : \mathbb{Q}(\alpha, \theta) \to \mathbb{C}$, which fixes $\mathbb{Q}$. By Theorem 5.2.9, this implies that $[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}] = (n + 1)m$. But by Theorem 5.1.17 we have $[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = nm$, which is clearly a contradiction. This allows us to make the following definition.

Definition 7.2.8 (Relative embeddings)
Let L/K be a number field extension of degree n. The n homomorphisms from L into $\mathbb{C}$, which fixes K, are called the *relative embeddings* of L into $\mathbb{C}$.

Equivalent to Definition 5.2.16 we define the relative norm and trace of a field extension using the relative embeddings.

Definition 7.2.9 (Relative Norm and trace)
Let L/K be a number field extension of degree n and let $\sigma_1, \ldots, \sigma_n$ denote the n relative embeddings of L into $\mathbb{C}$. Let $x \in L$ then the *relative norm and trace* of x is given by:

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x). \tag{7.22}$$

In order to determine when a cyclic algebra is actually a cyclic division algebra, a sufficient condition can be found for an algebra of degree 2,

Example 7.2.10
Let $\mathcal{A}$ be an algebra of degree 2, and $x \in \mathcal{A}$ with the corresponding matrix $X \in M_2(L)$ then

$$\det(X) = \begin{vmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{vmatrix} = x_0\sigma(x_0) - x_1\gamma\sigma(x_1) = N_{L/K}(x_0) - \gamma N_{L/K}(x_1). \tag{7.23}$$

Thus

$$\det(X) = 0 \Leftrightarrow \gamma = N_{L/K}(x_o x_1^{-1}) \tag{7.24}$$

and $\mathcal{A}$ is a cyclic division algebra if and only if γ is not a relative norm of some element of L. □

A similar statement regarding algebras of any dimension n can be made, although this will not be proved in this project.

Proposition 7.2.11 ([14] p. 57)
Let L/K be a cyclic extension of degree n with Galois group $Gal(L/K) = \langle\sigma\rangle$. If $\gamma, \gamma^2, \ldots, \gamma^{n-1} \in K$ are not a relative norm of some element of L, then $(L/K, \sigma, \gamma)$ is a cyclic division algebra.

Proof. A proof can be found in [15, p. 279]. ■

In the next section we construct a fully diverse linear code with non-vanishing determinant and cubic shaping, known as the golden code.

7.3 The Golden Code

This section is based on [14, sec. 5.2].
To construct the golden code we first consider the number field $\mathbb{Q}(\sqrt{5})$. We are interested in its ring of integers.

Proposition 7.3.1 ([19] p. 60)
The ring of integers of $K = \mathbb{Q}(\sqrt{5})$ is given by $\mathcal{O}_K = \{k_1 + k_2\theta \mid k_1, k_2 \in \mathbb{Z}, \theta = \frac{1+\sqrt{5}}{2}\}$.

Proof.
Let $\alpha \in K$. Then $\alpha = r + s\sqrt{5}$ for some $r, s \in \mathbb{Q}$. Thus we may write $\alpha = \frac{a+b\sqrt{5}}{c}$ for some $a, b, c \in \mathbb{Z}$, $c \neq 0$, such that no prime divides all of a, b and c. By Lemma 5.2.14, α is an algebraic integer if and only if the coefficients of the minimal polynomial

$$p_\theta(X) = \left(X - \left(\frac{a + b\sqrt{5}}{c}\right)\right)\left(X - \left(\frac{a - b\sqrt{5}}{c}\right)\right) \tag{7.25}$$

$$= X^2 - \frac{2a}{c}X + \frac{a^2 - 5b^2}{c^2} \tag{7.26}$$

are integers, so assume that they are. Assume for contradiction that a and c has a common prime factor, p. Since $\frac{a^2-5b^2}{c^2}$ is an integer, this implies that p divides b, since p^2 can not divide 5. This contradicts our assumption that no prime divides all of a, b, c. Thus a and c have no

common prime factors. Therefore, since $\frac{2a}{c}$ is an integer, we have $c = 1$ or $c = 2$. If $c = 1$ then $\alpha = \frac{2a+2b\sqrt{5}}{2} = (a-b) + 2b\frac{1+\sqrt{5}}{2}$ is of the form $k_1 + k_2\theta$. So we may assume $c = 2$. Then a must be odd, and since $\frac{a^2-5b^2}{4}$ is an integer, b must also be odd. Then $\alpha = \frac{a+b\sqrt{5}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{5}}{2}$ is of the form $k_1 + k_2\theta$. So $\mathcal{O}_K \subset \{k_1 + k_2\theta \mid k_1, k_2 \in \mathbb{Z}, \theta = \frac{1+\sqrt{5}}{2}\}$.
For the other inclusion, note that any number of the form $\alpha = k_1 + k_2\theta$ can be obtained from one of the cases $c = 1$ or $c = 2$ above. To see this, assume first that k_2 is odd. Then we must have $c = 2$, and from $\alpha = \frac{a-b}{2} + b\frac{1+\sqrt{5}}{2}$ we see that we can choose $b = k_2$ and $a = 2k_1 + b$, so that $\alpha = k_1 + k_2\theta = \frac{a-b}{2} + b\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$. Now assume that k_2 is even. Then we must have $c = 1$ and from $\alpha = (a-b) + 2b\frac{1+\sqrt{5}}{2}$, we see that we can choose $b = \frac{k_2}{2}$ and $a = k_1 + \frac{k_2}{2}$, so that $\alpha = k_1 + k_2\theta = (a-b) + 2b\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$. Hence $\mathcal{O}_K = \{k_1 + k_2\theta \mid k_1, k_2 \in \mathbb{Z}, \theta = \frac{1+\sqrt{5}}{2}\}$. ■

The actual field extension we need to construct the golden code is the number field extension $L/K = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$. It seems likely by comparing with Proposition 7.3.1, that the ring of integers of L should be $\mathcal{O}_L = \{k_1 + k_2\theta \mid k_1, k_2 \in \mathbb{Z}[i],\ \theta = \frac{1+\sqrt{5}}{2}\}$, where $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. This is indeed the case [14, p. 59].
To see that L/K is a Galois extension, note that the minimal polynomial of $\sqrt{5}$ is $X^2 - 5$ so L/K is a field extension of degree 2 and we can define two automorphisms of $\mathbb{Q}(i, \sqrt{5})$ as follows, $a, b \in \mathbb{Q}(i)$:

$$\sigma_1 :\ a + b\sqrt{5} \to a + b\sqrt{5} \tag{7.27}$$

$$\sigma_2 :\ a + b\sqrt{5} \to a - b\sqrt{5}. \tag{7.28}$$

We see that σ_2 is the generator for the Galois group. Thus we may construct the cyclic algebra $\mathcal{A} = (L/K, \sigma, i)$, where $\sigma : a + b\sqrt{5} \to a - b\sqrt{5}$, and use this to build the golden code. By only using elements of $\mathcal{O}_L$ a codeword from this algebra is of the form:

$$\begin{bmatrix} a + b\theta & i(c + d\sigma(\theta)) \\ c + d\theta & a + b\sigma(\theta) \end{bmatrix} \tag{7.29}$$

where $a, b, c, d \in \mathbb{Z}[i]$. By definition the codebook consisting of these codewords are linear and since we transmit 4 information symbols a, b, c, d per 2×2 matrix the code is called *full rate*. Since i is not a relative norm of any element of L, as shown in [14, p. 72], $\mathcal{A}$ is a cyclic division algebra, and the code is therefore fully diverse.
In order to add the shaping property to the code, we recall that each layer of a codeword can be written as a vector of the form in Equation (7.19). This vector can be written as a product of a matrix M and a vector $\mathbf{v}$ containing the information symbols. Cubic shaping is achieved if M is chosen such that it is unitary. In our case the information symbols are a, b, c, d and one way of choosing M is therefore given by:

$$M = \begin{bmatrix} 1 & \theta \\ 1 & \sigma(\theta) \end{bmatrix}. \tag{7.30}$$

This is not a unitary matrix, and thus in order to get the shaping property, we need to change the codebook in a way that preserves the full diversity. Let $\alpha = (1 + i - i\theta)$, then

$$M' = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} 1 & \theta \\ 1 & \sigma(\theta) \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & \alpha\theta \\ \sigma(\alpha) & \sigma(\alpha\theta) \end{bmatrix} \tag{7.31}$$

is a unitary matrix, and the shaping property can therefore be added to the code by letting each layer be determined by M'. A codeword X belonging to the golden code thus takes the form:

$$X = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & i\sigma(\alpha)(c + d\sigma(\theta)) \\ \alpha(c + d\theta) & \sigma(\alpha)(a + b\sigma(\theta)) \end{bmatrix}, \tag{7.32}$$

where $a, b, c, d \in \mathbb{Z}[i]$. Note that this corresponds to multiplying each codeword from Equation (7.29) by $A = \frac{1}{\sqrt{5}} diag(\alpha, \sigma(\alpha))$ from the right, and therefore it does not affect the full diversity of the code. When a, b, c, d can take any value in $\mathbb{Z}[i]$ we have an infinite code and we now find the minimum determinant of this code. Since $\alpha\sigma(\alpha) = 2 + i$, $\theta + \sigma(\theta) = 1$ and $\theta\sigma(\theta) = -1$, we have:

$$\det(X) = \frac{2 + i}{5}((a + b\theta)(a + b\sigma(\theta)) - i(c + d\theta)(c + d\sigma(\theta)) \tag{7.33}$$

$$= \frac{1}{2 - i}(a^2 + ab - b^2 - i(c^2 + cd - d^2)). \tag{7.34}$$

Since $a^2+ab-b^2-i(c^2+cd-d^2)$ is the determinant of a codeword of the form in Equation (7.29) from the cyclic division algebra $\mathcal{A}$, it follows that $a^2+ab-b^2-i(c^2+cd-d^2) \neq 0$ for $X' \neq O$. Therefore, since $a, b, c, d \in \mathbb{Z}[i]$, the non-trivial minimum of $|a^2 + ab - b^2 - i(c^2 + cd - d^2)|^2$ is 1 and we have that:

$$\Delta_{\min}(\mathcal{C}_\infty) = \liminf\{\det(XX^\dagger) \mid O \neq X \in \mathcal{C}_\infty\}) = \frac{1}{5}, \tag{7.35}$$

which yields a lower bound for the minimum determinant of any finite codebook carved from the linear code.

QAM-symbols

This section is based on [4]

The reason we use $\mathbb{Q}(i)$ as the base field is so that the information symbols are elements of $\mathbb{Z}[i]$. A set of the form $\{2(a + bi + \frac{\pm 1 \pm i}{2}) \mid -n \leq a, b \leq n,\ a, b \in \mathbb{Z}\}$, where $n \in \mathbb{N}$, is called a (square) $2^{2(n+1)}-$QAM constellation, and it is a $2^{2(n+1)}$ element subset of $\mathbb{Z}[i]$. For example for $n = 1$, we get the $16-$QAM constellation of Figure 7.1.

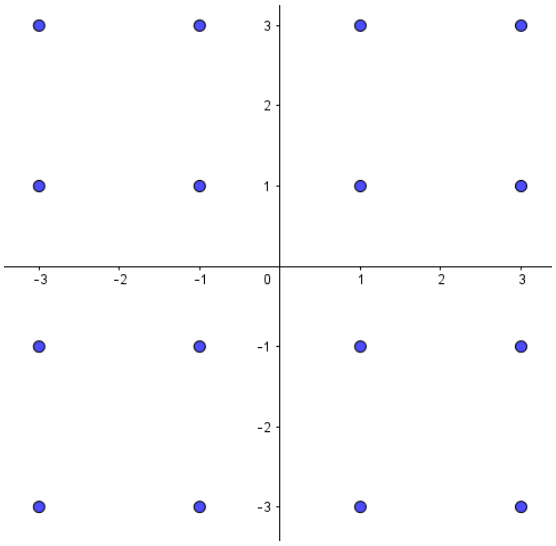

Figure 7.1: *The* $16-$*QAM constellation.*

Each symbol of a 2^m-QAM constellation represents a bit string of length m. Thus the throughput is higher for larger m, but it comes at a price. The energy needed to transmit a symbol is higher, the farther the symbol is from $\mathbf{0}$. To gain a higher throughput by increasing m, we thus either need a more powerful transmitter, or we need to decrease the distance between symbols, or a combination of the two. By decreasing the distance between symbols, which in practice means the transmitted signals will have a smaller difference in amplitudes and in phase-change, we get a higher error rate. Because of the even distribution of symbols in QAM constellations along with the flexibility of adjusting the constellation size to the quality of the communication channel, QAM is used in many modern wireless communication systems, including the IEEE 802.11 WiFi protocols. [3]

7.4 Decoding the Golden Code

This section is based on [14, sec. 2.4].
In this section we show how a message sent by using the golden code, can be decoded using the sphere decoder. In order to use the sphere decoder we need to write the received matrix, Y as a vector. We do this by applying the column-wise matrix vectorization function $vec(\cdot)$:

$$vec(Y) = \begin{bmatrix} \Re(Y_{11}) & \Im(Y_{11}) & \Re(Y_{21}) & \cdots & \Re(Y_{22}) & \Im(Y_{22}) \end{bmatrix}^T \tag{7.36}$$

and thus rewriting the original channel model (7.1) as:

$$vec(Y) = vec(HX) + vec(Z). \tag{7.37}$$

Which again can be written as:

$$vec(Y) = \begin{bmatrix} ri(H_{11}) & ri(H_{12}) & 0 & 0 \\ ri(H_{21}) & ri(H_{22}) & 0 & 0 \\ 0 & 0 & ri(H_{11}) & ri(H_{12}) \\ 0 & 0 & ri(H_{21}) & ri(H_{22}) \end{bmatrix} vec(X) + vec(Z) \tag{7.38}$$

where $ri(\cdot)$ replaces each complex entry, H_{ij} of the matrix H with the 2×2 matrix:

$$ri(H_{ij}) = \begin{bmatrix} \Re(H_{ij}) & -\Im(H_{ij}) \\ \Im(H_{ij}) & \Re(H_{ij}) \end{bmatrix}. \tag{7.39}$$

Thus the MIMO case has been reformulated as a lattice decoding problem, and all we need to know is the lattice generator matrix, in order to use the sphere decoder. We find the generator matrix by vectorizing the golden code:

$$X = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & i\sigma(\alpha)(c + d\sigma(\theta)) \\ \alpha(c + d\theta) & \sigma(\alpha)(a + b\sigma(\theta)) \end{bmatrix}, \tag{7.40}$$

as

$$vec(X) = \frac{1}{\sqrt{5}} \begin{bmatrix} \Re(\alpha(a + b\theta)) \\ \Im(\alpha(a + b\theta)) \\ \Re(\alpha(c + d\theta)) \\ \Im(\alpha(c + d\theta)) \\ \Re(i\sigma(\alpha)(c + d\sigma(\theta))) \\ \Im(i\sigma(\alpha)(c + d\sigma(\theta))) \\ \Re(\sigma(\alpha)(a + b\sigma(\theta))) \\ \Im(\sigma(\alpha)(a + b\sigma(\theta))) \end{bmatrix} =$$

$$\frac{1}{\sqrt{5}} \begin{bmatrix} \Re(\alpha) & -\Im(\alpha) & \theta\Re(\alpha) & -\theta\Im(\alpha) & 0 & 0 & 0 & 0 \\ \Im(\alpha) & \Re(\alpha) & \theta\Im(\alpha) & \theta\Re(\alpha) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \Re(\alpha) & -\Im(\alpha) & \theta\Re(\alpha) & -\theta\Im(\alpha) \\ 0 & 0 & 0 & 0 & \Im(\alpha) & \Re(\alpha) & \theta\Im(\alpha) & \theta\Re(\alpha) \\ 0 & 0 & 0 & 0 & -\Im(\sigma(\alpha)) & -\Re(\sigma(\alpha)) & -\sigma(\theta)\Im(\sigma(\alpha)) & -\sigma(\theta)\Re(\sigma(\alpha)) \\ 0 & 0 & 0 & 0 & \Re(\sigma(\alpha)) & -\Im(\sigma(\alpha)) & \sigma(\theta)\Re(\sigma(\alpha)) & -\sigma(\theta)\Im(\sigma(\alpha)) \\ \Re(\sigma(\alpha)) & -\Im(\sigma(\alpha)) & \sigma(\theta)\Re(\sigma(\alpha)) & -\sigma(\theta)\Im(\sigma(\alpha)) & 0 & 0 & 0 & 0 \\ \Im(\sigma(\alpha)) & \Re(\sigma(\alpha)) & \sigma(\theta)\Im(\sigma(\alpha)) & \sigma(\theta)\Re(\sigma(\alpha)) & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Re(a) \\ \Im(a) \\ \Re(b) \\ \Im(b) \\ \Re(c) \\ \Im(c) \\ \Re(d) \\ \Im(d) \end{bmatrix} \tag{7.41}$$

and we see that $vec(X)$ is of the form $M\mathbf{u}$, $u \in \mathbb{Z}^8$. Note that the Gram matrix of the lattice generated by M is $M^T M = I_8$, and the lattice is therefore a rotated version of the $\mathbb{Z}^8$ lattice. The error rates of the rotated $\mathbb{Z}^8$ lattice given by M, the cyclotomic constructed $\mathbb{Z}^8$ lattice and the $\mathbb{Z}^8$ lattice was compared in MATLAB. For the simulation, the transmitted information symbols were modelled as a uniformly distributed random variable with sample space $\{a + bi \mid 0 \leq a, b \leq 100,\ a, b \in \mathbb{Z}\}$. The entries of H were modelled as independent $\mathcal{N}_c(0, 1)$ distributed random variables, while the complex additive Gaussian white noise of Z had variance $\sigma^2 =$

$0.01, 0.02, \ldots, 0.1$. The same channel matrix, H, is used in the sphere decoder for all three lattices. The result of the simulation is shown in figure 7.2. The errorrates of the golden code are the lowest for all the simulated variances.

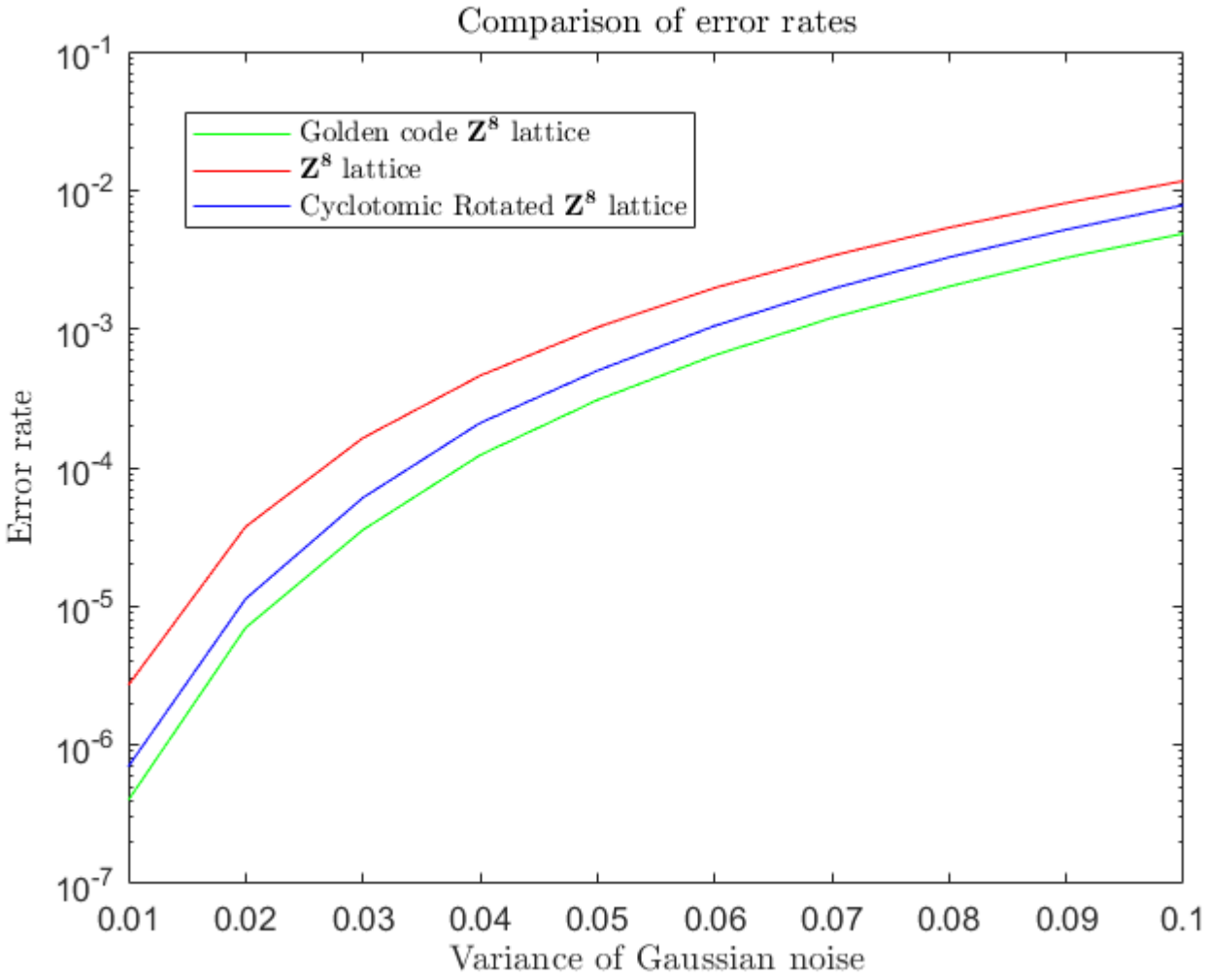

Figure 7.2: *Error rates of the rotated $\mathbb{Z}^8$ lattice code obtained from the golden code (green), the $\mathbb{Z}^8$ lattice code (red), and the rotated $\mathbb{Z}^8$ lattice code obtained from the cyclotomic construction (blue).*

Conclusion 8

In order to design signal constellations that minimizes the codeword error probability, in both the SISO and the MIMO case, one may utilize the incredibly rich theory of algebraic numbers. As such we have shown in this report that by applying the canonical embedding of a totally real algebraic number field to its ring of integers one obtains a lattice constellation of maximal diversity in the SISO case. Furthermore if the lattice is build by applying the twisted canonical embedding to an ideal of the ring of integers, we have found that the minimum product distance of such a lattice is given by:

$$\sqrt{\frac{\det(\Lambda)}{|disc_K|}}. \tag{8.1}$$

Although the construction of ideal lattices yields lattice constellation of maximal diversity for which it is possible to compute the minimum product distance, not every such lattice is of practical use. The reason for this is that a given lattice may result in a very complex bit labeling procedure, or loss in average energy. A lattice constellation which offer a good comprise between the complexity of bit labeling and energy loss, is the integral lattice or a rotated version hereof. By applying the twisted canonical embedding to the ring of integers of a maximal real subfield of a cyclotomic field, we get a rotated version of the integral lattice. This lattice constellation thus contains the desired properties, while still being of practical use.

In the MIMO case we found that in order to construct linear codes with large minimum determinant one may use the structure of cyclic division algebras build from finite number field extensions. By viewing each element of the cyclic division algebra as matrices on the form (7.17) we can construct a codebook. In the case of two transmit and two receive antennas a code with the desired properties known as the golden code can be build from the cyclic division algebra $(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i),\sigma,i)$ where σ is the $\mathbb{Q}(i,\sqrt{5})$ automorphism defined by $\sigma : a+b\sqrt{5} \rightarrow a-b\sqrt{5}$, where $a, b \in \mathbb{Q}(i)$. In both the SISO and MIMO case, we have run simulations, which shows a significantly lower error rate for the algebraic codes than for a regular $\mathbb{Z}^n$ lattice code.

Bibliography

[1] *Integral bases*. 2016, URL https://mathcourses.nfshost.com/archived-courses/mat-521-2016-spring/lectures/20-integral-bases.pdf.

[2] *Vandermonde Determinant*. 2019, URL https://proofwiki.org/wiki/Vandermonde_Determinant.

[3] *IEEE 802.11*. 2020, URL https://en.wikipedia.org/wiki/IEEE_802.11.

[4] *Quadrature Amplitude Modulation*. Accessed may 4, 2020, URL https://www.open.edu/openlearn/science-maths-technology/exploring-communications-technology/content-section-1.7.

[5] Garrett Buffington. *Polar decomposition of a lattice*, 2014. URL http://buzzard.ups.edu/courses/2014spring/420projects/math420-UPS-spring-2014-buffington-polar-decomposition.pdf.

[6] Mark Dickinson. *Galois Theory: the Proofs, the Whole Proofs, and Nothing But the Proofs*, URL http://www.pitt.edu/~gmc/algebra/galoistheory.pdf.

[7] U. Fincke and M. Post. *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, 1985, Mathematics of computation.

[8] Niels Lauritzen. *Concrete Abstract Algebra*. Cambridge University Press, 2003. ISBN 978-0-521-53410-9.

[9] Daniel A. Marcus. *Number Fields*. Springer, 2nd edition edition, 2018. ISBN 978-3-319-90232-6.

[10] Danielle Micciancio. *Introduction to lattices*, 2012. URL https://cseweb.ucsd.edu/classes/wi12/cse206A-a/lec1.pdf.

[11] Richard A. Mollin. *Algebraic Number Theory*. CRC Press, 2nd edition edition, 2011. ISBN 1439845999, 9781439845998.

[12] Frédérique Oggier and Emanuele Viterbo. *Algebraic Number Theory and Code Design for Rayleigh Fading Channels*, 2004, Foundations and Trends™ in Communications and Information Theory, volume 1 issue 3.

[13] Frédérique Oggier and Emanuele Viterbo. *Full Diversity Rotations*, 2005. URL https://ecse.monash.edu/staff/eviterbo/rotations/rotations.html.

[14] Frédérique Oggier, Jean-Claude Belfiore, and Emanuele Viterbo. *Cyclic Division Algebras: A Tool for Space-Time Coding*, 2007, Foundations and Trends™ in Communications and Information Theory, volume 4 No. 1.

[15] Richard S. Pierce. *Associative Algebras*. Springer, 1982. ISBN 0-387-90693-2.

[16] Steven Roman. *Fundamentals of Group Theory, An Advanced Approach*. Birkhäuser Boston, 2012. ISBN 978-0-8176-8300-9.

[17] Bernard Sklar. *Rayleigh fading channels in mobile digital communication systems. I. Characterization*, July 1997, IEEE Communications Magazine, vol. 35, no. 7, pp. 90-100.

[18] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC mathematics, 2nd edition edition, 2003. ISBN 1-58488-393-6.

[19] Ian Stewart and David Tall. *Algebraic Number Theory*. Chapman and Hall ltd., 1979. ISBN 978-0-412-13840-9.

[20] H. P. F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. University Press, Cambridge, 2001. ISBN 0-521-00423-3.

[21] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1982. ISBN 0-387-90622-3.

Appendix A

```
function [uh,dsqh] = SD(r,alpha,C,M)
Mc=diag(alpha)*M;
G=Mc'*Mc;
n=length(r);
R=chol(G);
Q=zeros(n);
L=zeros(n,1);
u=zeros(n,1);
uh=u;
xi=zeros(n,1);
for j1=1:n
   for j2=j1:n
      if j1==j2
         Q(j1,j1)=R(j1,j1)^2;
      else
         Q(j1,j2)=R(j1,j2)/R(j1,j1);
      end
   end
end
rho=Mc^(-1)*r;
dsq=C;
dsqh='No vector in the sphere. Try a larger radius.';
T=zeros(n,1);
T(n)=C;
S=rho;
flag1=1;
flag2=1;
flag3=1;
while flag1==1
   flag2=1;
   i=n;
while flag2==1
   flag3=1;
   L(i)=floor(sqrt(T(i)/Q(i,i))+S(i));
   u(i)=ceil(-sqrt(T(i)/Q(i,i))+S(i))-1;
   while flag3==1
      u(i)=u(i)+1;
      if u(i)>L(i)
         if i==n
            flag1=0;
            flag2=0;
            flag3=0;
            continue;
         else
            i=i+1;
            continue;
         end
      else
```

```
49          if i>1
50             xi(i)=u(i)-rho(i);
51             T(i-1)=T(i)-Q(i,i)*(u(i)-S(i))^2;
52             count=0;
53             for j1=i:n
54                count=count+Q(i-1,j1)*xi(j1);
55             end
56             S(i-1)=rho(i-1)-count;
57             i=i-1;
58             flag3=0;
59             continue;
60          else
61             dsqh=T(n)-T(1)+Q(1,1)*(u(1)-S(1))^2;
62             if dsqh<dsq
63                uh=u;
64                dsq=dsqh;
65                T(n)=dsqh;
66                flag3=0;
67                flag2=0;
68                continue;
69             else
70                continue;
71             end
72          end
73       end
74    end
75 end
76 end
77 end
```