# Lattice codes for wiretap fading channels

Ong, Soon Sheng

2014

Ong, S. S. (2014). Lattice codes for wiretap fading channels. Doctoral thesis, Nanyang Technological University, Singapore.

https://hdl.handle.net/10356/60697

https://doi.org/10.32657/10356/60697

# LATTICE CODES FOR WIRETAP FADING CHANNELS


ONG SOON SHENG

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

*A thesis submitted to the Nanyang Technological University in partial fulfillment of the requirements for the degree of Doctor of Philosophy*

2014

# Acknowledgements

First of all, I would like to express my heartfelt thank to my supervisor, Prof. Frédérique Oggier for giving me this precious opportunity to work on this research project in completing my PhD degree. Besides improving my mathematical understanding, she has inspired me to be a better mathematics educator. Indeed her patient guidance will always be in my mind and be part of my teaching philosophy. Finally I'm grateful to have her as my awesome supervisor. Merci beaucoup!

Secondly I would like to thank my collaborator, Dr.Wittawat Kositwattanarerk during my research studies. Also thanks to the anonymous reviewers for the useful comments on past publications. Special thanks to Basu and Jia Ning for the technical guidance in Sage and Matlab during my graduate studies.

Thirdly I would like to thank all my teachers and professors who taught me before, directly or indirectly. Thanks for their guidance, encouragement and inspiration.

Next I would like to thank my beloved family members and relatives for always giving me their caring words and warm support. I own my utmost gratitude to my parents for giving me their best in my life.

Also I would like to thank Anderson, Basu, Chien Lung, Chin Hong, Choon Yee, Chun Ping, Dr.Lim Boon Hock, Fuchun, Han Mao, Jerome, Jun Jie, Kelvin, Khi Poay, Kin Sung, Kooi Yeong, Lam Chye, Liming, Meng Chwin, Ming Ming, Peng Hoe, Rafael, Suet Hoay, Wei Gie, Yan Wei, Zhou Yang and all other friends for their kind friendships and encouragement. Also thanks to my spiritual supports from Venerables and fellow dharma friends.

Last but not least, I owe my appreciation for those who are present in my life. Thanks for everything!

# Abstract

This thesis is dedicated to the design of wiretap codes for fading channels, that is, codes that promise both reliability and confidentiality for wireless channels.

By upper bounding the eavesdropper's probability of correctly decoding a confidential message, we begin by deriving a code design criterion that characterizes confidentiality for finite lattice constellations. We consider wiretap lattice codes built from number fields, or more precisely ideal lattice codes. Ideal lattice codes are known to be good for reliability and we refine our code design criterion for this type of lattice codes yielding an optimization of a sum of inverse of algebraic norms. In order to construct good wiretap lattice codes for fast fading channels, we analyse sums of inverse of algebraic norms by studying the units and non-units with small norms in number fields. We compare different underlying number fields with respect to the wiretap codes they provide.

Encoding of wiretap codes is done via coset encoding, where each codeword sent is chosen randomly from a coset of codewords. Motivated by the need to perform coset encoding with lattices built from number fields, we propose a generalization of Construction A of lattices over number fields from linear codes. The lattice construction is of interest on its own, but also serves for encoding slow fading wiretap codes.

# Contents

# List of Figures

# List of Tables

# List of Publications

## Proceedings of Conferences

[1] (Joint work with F. Oggier) Lattices from Totally Real Number Fields with Large Regulator, *International Workshop on Coding and Cryptography (WCC) 2013*, Bergen, Norway, pp. 438–447.

[2] (Joint work with W. Kositwattanarerk and F. Oggier) Wiretap Encoding of Lattices from Number Fields using Codes over $\mathbb{F}_p$, *IEEE International Symposium on Information Theory (ISIT) 2013*, Istanbul, Turkey, pp. 2612–2616.

## Journals

[1] (Joint work with F. Oggier) Lattices from Totally Real Number Fields with no Small Norm Elements, *Designs, Codes and Cryptography*, special issue, February 2014.

[2] (Joint work with W. Kositwattanarerk and F. Oggier) Construction A of Lattices over Number Fields and Block Fading Wiretap Coding, submitted to *IEEE Transactions on Information Theory*, December 2013.

# Chapter 1

# Introduction

The security in wireless communications has become one of the major concerns in communication systems nowadays. Our work is dedicated to the study of security in wireless communications from an information theoretical point of view. We exploit the eavedropper's noise inherently present over communication channels and apply a coding strategy to confuse the eavedropper by adding random bits to information bits. This technique stems from the pioneering works by Wyner who introduced wiretap channels. A wiretap channel is a broadcast channel where a legitimate sender Alice communicates to two users, a legimitate recipient Bob, and an eavesdropper Eve. This work is related to wiretap coding for fading channels with the use of algebraic number theory and classical coding theory. Indeed algebraic number theory is known to provide mathematical tools to design codes for fading channels.

The structure of this thesis is organized as follows. We begin in Chapter 2 by introducing wiretap coding for fading channels. After illustrating the assumptions on wiretap fading system model, we recall briefly the 2 types of wiretap fading channels that we focus on this thesis, namely *fast fading channels* and *slow fading channels*. Next we elaborate our major research problem which can be summarized as minimizing the probability of correct decoding for the eavedropper through the design of wiretap lattice codes. We derive a code design criterion that characterizes wiretap codes that reduces Eve's probability of correct decoding, when *lattice coset encoding* is performed. Chapter 2 also contains the necessary definitions and facts about lattices for dealing with wiretap lattice codes.

In Chapter 3, we propose the design of wiretap lattice codes through *ideal lattices*. To begin with, we recall some terminolgy from algebraic number theory which will be needed to define ideal lattices and analyse code design criteria in the context of ideal lattices. Before the end of Chapter 3, we propose ideal lattice codes and identify the lattice code parameters related to code design criteria which are analysed in Chapters 4 and 5.

In Chapter 4, we analyse ideal lattice codes for fast fading channels. Applying the knowledge of algebraic number theory, we optimize lattice code parameters based on number fields with particular properties, guided by the code design criteria for reliability and confidentiality.

In Chapter 5, we propose a general lattice construction from linear codes which can be seen as a generalization of Construction A. We analyse this construction for certain number fields. This generalization of Construction A also provides a method to perform coset coding and we illustrate wiretap encoding of ideal lattices for slow fading channels.

Finally we conclude this thesis and mention some possible future works related to the design of wiretap codes for fading channels.

# Chapter 2

# Wiretap Coding for Fading Channels

To motivate our research problems, we consider a wiretap channel (see Figure 2.1) as introduced by Wyner [34] which consists of two discrete memoryless channels: one is called the *main channel* that models the communication between the legitimate users, Alice and Bob, whereas the other is known as the *wiretapper's channel*, that can be viewed as a degraded version of the main channel, which is exploited by the eavesdropper, Eve, to get information from the main channel.

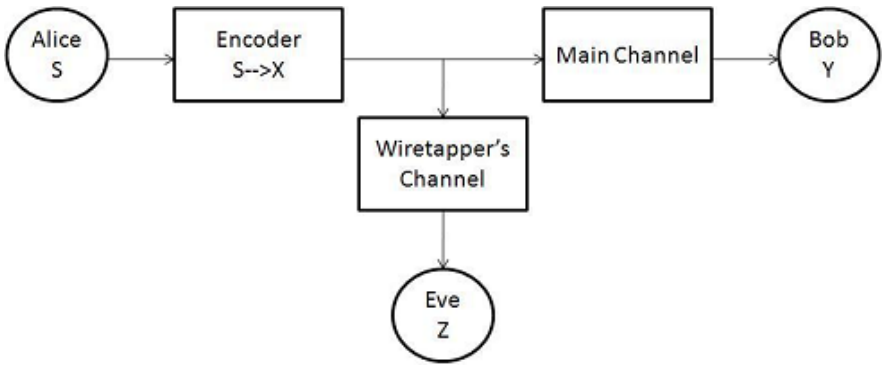


**Figure 2.1: A Wiretap Channel** - Let S be the message to be sent, S is encoded into X, then Y and Z are the noisy messages received.

By exploiting the noise difference between the main channel and the wiretapper's channel, Wyner showed that there exist codes, called *wiretap codes*, such that it is possible for Alice to communicate with Bob reliably and confidentially. Thus the design

of wiretap codes has for goals that Bob decodes the message sent by Alice correctly while at the same time, the message sent is kept secret from Eve.

From an information theoretic aspect, Wyner defined the *perfect secrecy capacity* as the maximum amount of information that Alice can send to Bob while insuring that Eve gets a negligible amount of information. Wyner's work on wiretap channels has since then been generalized to many channels (see [15]), whose secrecy capacity has been studied. In particular, the secrecy capacity of the Gaussian wiretap channel was analysed over additive white Gaussian noise (AWGN) channel (see [14]). Although the related explicit wiretap code constructions remain elusive for most classes of channels, recent constructions of wiretap codes with examples from different types of physical channel can be found in [18].

Progress has been made recently on the wiretap code design for Gaussian Channels. The secrecy gain and the flatness factor (see respectively [24] and [19]) have been proposed as code design criteria for AWGN wiretap channels, in order to maximize the confusion at the eavesdropper, and wiretap lattice codes satisfying the former criterion have been studied [17]. The constructed wiretap lattice codes are relating the secrecy gain to Eve's probability of correct decision in decoding the message, $P_{c,e}$.

Let us recall the background of Gaussian wiretap channels, that is, broadcast channels where the sender (Alice) sends a signal to a legitimate receiver (Bob), while an illegitimate eavesdropper (Eve) can listen to the transmission. It is modeled by

$$\begin{aligned} y &= x + v_b \\ z &= x + v_e \end{aligned}$$

where $x \in \mathbb{R}$ is the transmitted signal, both $y, z \in \mathbb{R}$ are the received signals, $v_b$ and $v_e$ denote the Gaussian noise at Bob, respectively Eve's side, both with zero mean, and respective variance $\sigma_b^2$ and $\sigma_e^2$. In practice, a $k$-bit message $\mathbf{s} = (s_1, s_2, ..., s_k)$ is encoded into a sequence of $n$ signals $\mathbf{x} = (x_1, x_2, ..., x_n) \in \mathbb{R}^n$ which is then transmitted over the Gaussian wiretap channel. Let $\mathbf{v} = (v_1, v_2, ..., v_n)$ be the Gaussian noise of the overall transmission. The received signal $\mathbf{y} = (y_1, y_2, ..., y_n) \in \mathbb{R}^n$ is then

$$\mathbf{y} = \mathbf{x} + \mathbf{v}$$

where the noise vector $\mathbf{v}$ has the probability distribution with zero mean and variance $\sigma^2$, namely

$$p_{0,\sigma^2}(\mathbf{v}) = \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\|\mathbf{v}\|^2/2\sigma^2},$$

where $\|\mathbf{v}\| = v_1^2 + ... + v_n^2$. Thus an AWGN wiretap channel is then modeled by

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e \end{aligned}$$

where $\mathbf{y}$ and $\mathbf{z}$ denote the received signals by Bob and Eve respectively. Lattice coding is often used for Gaussian channels: Alice chooses $\mathbf{x} \in \Lambda_b$ where $\Lambda_b$ is an $n$-dimensional real lattice intended to Bob. Note that the design of $\Lambda_b$ is used to increase Bob's probability of correct decision in decoding the message, $P_{c,b}$ and it is a classical problem in ensuring the reliability for Bob (see [24]). Instead we are dealing with the goal of confidentiality for Alice by studying the problem of maximizing Eve's confusion. In order to do so, we motivate the design of wiretap codes built from *lattices*. Thus we will provide some relevant terminology related to lattices in Section 2.1 before describing lattice coset encoding for wiretap channels in Section 2.2. In Section 2.3, we provide the background on 2 types of fading channels namely *Fast Fading Wiretap Channels* and *Slow(Block) Fading Wiretap Channels* which are the focus of this thesis.

## 2.1 Background on Lattices

We begin with the introduction of some relevant terminology related to lattices such as *generator matrix*, *Gram matrix*, *sublattice*, *integral lattice*, *dual lattice*, and *Voronoi region*. The following definitions and facts about lattices are mainly found in [5], [25] and [7], to which the reader may refer for more details.

A lattice $\Lambda$ is a discrete additive subgroup of $\mathbb{R}^n$. Here discrete means that there is an $\epsilon > 0$ such that any two distinct lattice points $\mathbf{x}$ and $\mathbf{y}$ are at distance at least $\|\mathbf{x} - \mathbf{y}\| \geq \epsilon$. For example, $\mathbb{Z}^n$ is a lattice because the set of integral vectors in $\mathbb{Z}^n$ forms an additive group and the distance between any two distinct integral vectors is at least 1.

**Definition 1.** *Let* $\{\mathbf{v}_1,...,\mathbf{v}_n\}$ *form a linearly independent set of column vectors in* $\mathbb{R}^n$. *The set of points*

$$\Lambda = \left\{ \mathbf{x} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i, \lambda_i \in \mathbb{Z} \right\}$$

*is called a lattice of dimension* $n$, *and* $\{\mathbf{v}_1, ..., \mathbf{v}_n\}$ *is called a* basis *of the lattice. Thus,* $\mathbf{v}_1,...,\mathbf{v}_n$ *are basis vectors of the lattice and we call the elements inside a lattice as lattice points.*

**Definition 2.** *The matrix*

$$M = (\mathbf{v}_1 \ \mathbf{v}_2 \ \dots \ \mathbf{v}_n)$$

*whose columns are the basis vectors* $\mathbf{v}_1$,$\mathbf{v}_2$,...,$\mathbf{v}_n$ *of a lattice* $\Lambda$ *is called a* generator matrix *for the lattice. The matrix* $G = M^T M$ *is called a* Gram matrix *for the lattice, where* $M^T$ *denotes the transposition of the matrix* $M$*. Note that each entry of this Gram matrix* $G$ *can be computed by inner products among basis vectors of a lattice, since columns of the generator matrix* $M$ *consist of basis vectors of a lattice. More precisely, the lattice can be defined by its generator matrix as*

$$\Lambda = \{\mathbf{x} = M\lambda | \lambda \in \mathbb{Z}^n\}.$$

- For the above lattice generated by a square matrix $M$, we call it a *full-rank lattice.* We will only consider full-rank lattices in our study.
- Given two generator matrices $M_1$ and $M_2$, we say that the lattices produced are equivalent if and only if $M_1 = cUM_2B$ where $c$ is a nonzero constant, $U$ is a matrix with integer entries amd determinant $\pm 1$ (unimodular integer matrix) and $B$ is a real orthogonal matrix (with $BB^T = I_n$).

**Definition 3.** *Any subgroup of a lattice* $\Lambda$ *is called a sublattice of* $\Lambda$*.*

**Remark 1.** *It is always possible to find a sublattice of a given lattice* $\Lambda$ *by taking its scaled version by an integer factor.*

**Definition 4.** *A lattice* $\Lambda$ *is called an* integral lattice *if all entries in its Gram matrix belong to* $\mathbb{Z}$*.*

**Definition 5.** *Let* $\Lambda \subset \mathbb{R}^n$ *be an integral lattice.* $\Lambda$ *is even when*

$$\mathbf{x} \cdot \mathbf{x} \in 2\mathbb{Z} \ \forall \mathbf{x} \in \Lambda,$$

*otherwise it is odd.*

**Definition 6.** *The determinant or discriminant of a lattice* $\Lambda$ *is defined to be the determinant of its Gram matrix* $G$*, namely*

$$\det(\Lambda) = disc(\Lambda) = \det(G).$$

*Note that it does not depend on the choice of the lattice basis.*

**Definition 7.** *For full rank lattices, the square root of the determinant of its Gram matrix $G$ is the volume of the lattice, and is denoted by* $\mathrm{vol}(\Lambda)$. *Equivalently,*

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

**Definition 8.** *Let $\Lambda \subset \mathbb{R}^n$ be an integral lattice. The dual lattice $\Lambda^*$ of $\Lambda$ is*

$$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{y} \cdot \mathbf{x} \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\},$$

*where $\cdot$ is the usual inner product. When $\Lambda = \Lambda^*$, the lattice $\Lambda$ is said to be unimodular.*

**Remark 2.** *For an integral lattice $\Lambda$, we have $\Lambda \subseteq \Lambda^*$. Moreover, when $\Lambda$ is integral, we have disc($\Lambda$) $= |\Lambda^*/\Lambda|$.*

**Definition 9.** *The Voronoi region of a lattice $\Lambda$ of dimension $n$, denoted by $\mathcal{V}(\Lambda)$ is defined to be for any point $\mathbf{x} \in \Lambda$ the set of points in $\mathbb{R}^n$ that are closer to $\mathbf{x}$ than any other points of $\Lambda$.*

**Remark 3.** *A Voronoi region contains only one lattice point. The translation of a Voronoi region by another lattice point produces another Voronoi region.*

**Theorem 1. [Poisson Summation Formula]***[7] Let $\Lambda \subset \mathbb{R}^n$ be an arbitrary lattice, and let $f : \mathbb{R}^n \to \mathbb{C}$ be a function which satisfies the followings (C1), (C2) and (C3):*

*(C1)* $\int_{\mathbb{R}^n} |f(\mathbf{x})| d\mathbf{x} < \infty$

*(C2) The series* $\sum_{\mathbf{x}\in\Lambda} |f(\mathbf{x}+\mathbf{u})|$ *converges uniformly for all $\mathbf{u}$ belonging to a compact subset of $\mathbb{R}^n$.*

*The condition (C1) implies the existence of the Fourier transform $\hat{f}$ of $f$, which is defined by the formula*

$$\hat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \mathbf{x}\cdot\mathbf{y}} d\mathbf{x}.$$

*The condition (C2) implies that the function $F(\mathbf{u}) := \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}+\mathbf{u})$ is continuous on $\mathbb{R}^n$. The third condition will be:*

*(C3) The series* $\sum_{\mathbf{y}\in\Lambda^*} \hat{f}(\mathbf{y})$ *is absolutely convergent.*

*Then*

$$\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = \frac{1}{\mathrm{vol}(\Lambda)} \sum_{\mathbf{y}\in\Lambda^*} \hat{f}(\mathbf{y}).$$

*Proof.* Omitted. [7] □

## 2.2 Lattice Coset Encoding for Wiretap Channels

In this section, we study an encoding strategy called *coset encoding* [34], in the context of lattices.

To send a $k$-bit message $\mathbf{s}$ over a Gaussian wiretap channel [24], Alice performs lattice encoding by mapping the message $\mathbf{s}$ into a vector $\mathbf{x} \in \mathbb{R}^n$ which belongs to a lattice $\Lambda_b$ intended to Bob, that is

$$\mathbf{x} = M_b\lambda,\ \lambda \in \mathbb{Z}^n$$

where $M_b$ is the generator matrix of the lattice $\Lambda_b$. At the same time, Alice wants to prevent Eve who is an eavedropper from getting any message information, hence she uses the following strategy called *coset encoding*.

Consider a sublattice $\Lambda_e$ of $\Lambda_b$ and a partition of $\Lambda_b$ into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$. The message intended for Bob, $\mathbf{s}$ is labelled by $\mathbf{s} \mapsto \Lambda_e + \mathbf{c}_{(\mathbf{s})}$. Next the transmitted lattice point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \subset \Lambda_b$ is chosen randomly. Equivalently,

$$\mathbf{x} = \mathbf{r} + \mathbf{c}_{(\mathbf{s})} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \Leftrightarrow \text{random vector } \mathbf{r} \in \Lambda_e.$$

The rationale of using coset encoding is that it provides a labeling of the lattice point of $\Lambda_b$ with a mixture of information bits($\mathbf{c}_{(\mathbf{s})}$) and random bits ($\mathbf{r} \in \Lambda_e$). With the assumptions that the wiretapper's channel is noisier than the main channel for Bob, it was shown that it is possible to achieve secure communication [14] using lattice codes where Eve decodes the random bits but not the data bits. The code constructions are however not explicit and finding them is still under study (see [16]). In this thesis, we will similarly consider lattice wiretap codes, but for wiretap fading channels.

## 2.3 Wiretap Fading Channels

As mentioned, we study the design of lattice wiretap codes based on 2 kinds of fading channels namely *Slow Fading Wiretap Channels* and *Fast Fading Wiretap Channels*.

The background on both fading channels is recalled next, before we derive a code design criterion for both wiretap fading channels.

We consider the transmission of data over a single antenna fading channel. This wireless channel is modeled as an independent Rayleigh fading channel. We assume that perfect channel state information (CSI) is available at both receivers. The discrete time model of the channel is given by

$$r' = \alpha' x + n'$$

where $x \in \mathbb{C}$ is a symbol from a complex signal set, $n'$ is the complex white Gaussian noise and $\alpha'$ the complex zero mean Gaussian fading coefficient.

With the aid of an in-phase/quadrature component interleaver, it is possible to remove the phase of the complex fading coefficients to obtain a real fading which is Rayleigh distributed and guarantee that the fading coefficients are independent from one real symbol to the next [25, sec 2.1]. This explains also why the models below are defined over real channels.

### 2.3.1 Slow Fading Wiretap Channels

We consider that the communication channel between Alice and Bob, resp. Eve is a block fading channel with coherence time $N$. This is modeled by

$$\begin{array}{rcl} Y & = & \mathsf{diag}(\mathbf{h}_b)X + V_b, \text{ and} \\ Z & = & \mathsf{diag}(\mathbf{h}_e)X + V_e \end{array} \tag{2.1}$$

where the transmitted signal $X$ is an $n \times N$ matrix, and the $n \times N$ matrices $V_b$ and $V_e$ are the Gaussian noise at Bob and Eve respectively. By channel assumption, $V_b$ and $V_e$ have zero mean and variance $\sigma_b^2$ and $\sigma_e^2$ respectively. The fading matrices can be given explicitly by

$$\begin{aligned} \mathsf{diag}(\mathbf{h}_b) &= \mathsf{diag}(|h_{b,1}|, \ldots, |h_{b,n}|) \text{ and} \\ \mathsf{diag}(\mathbf{h}_e) &= \mathsf{diag}(|h_{e,1}|, \ldots, |h_{e,n}|) \end{aligned}$$

where the fading coefficients $h_{b,i}, h_{e,i}$ are complex Gaussian random variables with variance $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, so that $|h_{b,i}|, |h_{e,i}|$ are Rayleigh distributed with parameter $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, for all $i = 1, \ldots, n$.

### 2.3.2 Fast Fading Wiretap Channels

Here we suppose that the transmission occurs over a fast Rayleigh fading channel with coherence time $N = 1$. Bob and Eve respectively receive the vectors $\mathbf{y}$ and $\mathbf{z}$ given by

$$\begin{array}{rcl} \mathbf{y} & = & \mathsf{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} & = & \mathsf{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e, \end{array} \tag{2.2}$$

where the transmitted signal $\mathbf{x} \in \mathbb{R}^n$ is a $n \times 1$ column vector, and the $n \times 1$ column vectors $\mathbf{v}_b$ and $\mathbf{v}_e$ denote the Gaussian noise at Bob, respectively Eve's side, both with zero mean, and respective variance $\sigma_b^2$ and $\sigma_e^2$, and

$$\mathsf{diag}(\mathbf{h}_b) = \begin{pmatrix} |h_{b,1}| & & \\ & \ddots & \\ & & |h_{b,n}| \end{pmatrix}, \mathsf{diag}(\mathbf{h}_e) = \begin{pmatrix} |h_{e,1}| & & \\ & \ddots & \\ & & |h_{e,n}| \end{pmatrix}$$

are the channel matrices containing the fading coefficients where $h_{b,i}, h_{e,i}$ are complex Gaussian random variables with variance $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, so that $|h_{b,i}|, |h_{e,i}|$ are Rayleigh distributed, $i = 1, \ldots, n$, with parameter $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$.

## 2.4 Code Design Criteria for Wiretap Fading Channels

In order to design wiretap codes for the Rayleigh fading channel, a design criterion has been proposed in [23] dealing with infinite lattice constellations by relying on the fact that once the fading is fixed, one deals with a Gaussian channel and the results of [24] can be applied. In our study, we will derive the code design criterion based on the case of *finite lattice constellations* for both fast and block fading channels.

In practice when we use a lattice code, we send a finite constellation carved from a lattice and this finite constellation is obtained through the intersection between the whole lattice and some bounding region $\mathcal{R}$. It is known that [24] gives a bound on Eve's probability of error assuming that the lattice constellation is infinite. Though the lattice bound for infinite lattice constellations does provide an upper bound for finite constellations, this bound obtained may not always be working since the series inside the bound may not be convergent. Thus we will need to rederive an upper bound for finite constellations. This means that we first need a finite constellation version of the bound of [24], which we compute below.

**Proposition 1.** *[27] Suppose transmission over a Gaussian wiretap channel, where coset coding is performed using the nested lattices $\Lambda_e \subset \Lambda_b$, and a finite constellation is sent, determined by a bounded region $\mathcal{R}$ around the origin. Suppose that the Fourier transform of the characteristic function $\chi_{\mathcal{R}}$ is even. Then Eve's probability $P_{c,e}$ of correct decision is upper bounded by*

$$P_{c,e} \leq \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\mathrm{vol}(\Lambda_b)\sum_{\mathbf{t}\in\Lambda_e\cap\mathcal{R}} e^{-\|\mathbf{t}\|^2/2\sigma_e^2},$$

*where* $\mathrm{vol}(\Lambda_b)$ *denotes the volume of* $\Lambda_b$.

*Proof.* Eve's probability $P_{c,e}$ of correct decision when doing coset decoding after transmission over a Gaussian channel is

$$P_{c,e} = \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\sum_{\mathbf{t}\in\Lambda_e\cap\mathcal{R}}\int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2}d\mathbf{u} \tag{2.3}$$

where $\mathcal{V}(\Lambda_b)$ denotes the Voronoi region of $\Lambda_b$, and the sum over $\mathbf{t}$ takes into account the randomization introduced by coset encoding. Then

$$\begin{aligned} P_{c,e} &= \int_{\mathcal{V}(\Lambda_b)} \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\sum_{\mathbf{t}\in\Lambda_e\cap\mathcal{R}} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2}d\mathbf{u} \\ &= \int_{\mathcal{V}(\Lambda_b)} \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\sum_{\mathbf{t}\in\Lambda_e} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2}\chi_{\mathcal{R}}(\mathbf{t})d\mathbf{u}, \end{aligned}$$

where $\chi_{\mathcal{R}}(\mathbf{t})$ is 1 if $\mathbf{t}\in\mathcal{R}$ and 0 otherwise.

Denote

$$f(\mathbf{t}) = e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2}\chi_{\mathcal{R}}(\mathbf{t}).$$

The Poisson summation formula for lattices (refer to Theorem 1) holds and yields

$$\sum_{\mathbf{t}\in\Lambda_e} f(\mathbf{t}) = \mathrm{vol}(\Lambda_e)^{-1}\sum_{\mathbf{t}^\star\in\Lambda_e^\star}\hat{f}(\mathbf{t}^\star)$$

where $\Lambda_e^\star$ is the dual lattice of $\Lambda_e$. We next compute $\hat{f}(\mathbf{t}^\star)$, which by definition is

$$\begin{aligned} \hat{f}(\mathbf{t}^\star) &= \int_{\mathbb{R}^n} e^{-2\pi i\langle\mathbf{t}^*,\mathbf{v}\rangle} f(\mathbf{v})d\mathbf{v} \\ &= \int_{\mathbb{R}^n} e^{-2\pi i\langle\mathbf{t}^*,\mathbf{v}\rangle}\underbrace{e^{\frac{-||\mathbf{u}||^2-2\langle\mathbf{u},\mathbf{v}\rangle-||\mathbf{v}||^2}{2\sigma_e^2}}}_{f_1(\mathbf{v})}\underbrace{\chi_{\mathcal{R}}(\mathbf{v})}_{f_2(\mathbf{v})}d\mathbf{v} \\ &= \int_{\mathbb{R}^n}\hat{f}_1(\mathbf{t}^*-\mathbf{w})\hat{f}_2(\mathbf{w})d\mathbf{w}, \end{aligned}$$

using the convolution theorem, where

$$\begin{aligned}
\hat{f}_1(\mathbf{w}) &= \int_{\mathbb{R}^n} e^{-2\pi i\langle \mathbf{w},\mathbf{v}\rangle} e^{\frac{-||\mathbf{u}||^2-2\langle \mathbf{u},\mathbf{v}\rangle-||\mathbf{v}||^2}{2\sigma_e^2}} d\mathbf{v} \\
&= \prod_{j=1}^{n} \int e^{-2\pi i w_j v_j} e^{\frac{-u_j^2-2u_jv_j-v_j^2}{2\sigma_e^2}} dv_j \\
&= \prod_{j=1}^{n} e^{\frac{-u_j^2}{2\sigma_e^2}} \int e^{-2\left(\pi i w_j+\frac{u_j}{2\sigma_e^2}\right)v_j} e^{\frac{-v_j^2}{2\sigma_e^2}} dv_j \\
&= \prod_{j=1}^{n} \sqrt{2\pi\sigma_e^2} e^{-2\sigma_e^2\pi^2 w_j^2} e^{2\pi i w_j u_j} \\
&= \sqrt{2\pi\sigma_e^2}^n e^{-2\sigma_e^2\pi^2||\mathbf{w}||^2} e^{2\pi i\langle \mathbf{w},\mathbf{u}\rangle}
\end{aligned}$$

using

$$\int_{\mathbb{R}} e^{-ax^2} e^{-2bx} dx = \sqrt{\pi/a} e^{b^2/a},\ a>0. \tag{2.4}$$

This shows that

$$\begin{aligned}
\hat{f}(\mathbf{t}^\star) &= \int_{\mathbb{R}^n} \hat{f}_1(\mathbf{t}^*-\mathbf{w})\hat{f}_2(\mathbf{w}) d\mathbf{w} \\
&= \sqrt{2\pi\sigma_e^2}^n \int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2} e^{2\pi i\langle \mathbf{t}^*-\mathbf{w},\mathbf{u}\rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w}
\end{aligned}$$

and

$$\begin{aligned}
\sum_{\mathbf{t}^\star\in\Lambda_e^\star} \hat{f}(\mathbf{t}^\star) &= \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^\star\in\Lambda_e^\star} e^{2\pi i\langle \mathbf{t}^*,\mathbf{u}\rangle} \int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2} e^{-2\pi i\langle \mathbf{w},\mathbf{u}\rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w} \\
&= \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^\star\in\Lambda_e^\star} \cos(2\pi\langle \mathbf{t}^*,\mathbf{u}\rangle) \int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2} e^{-2\pi i\langle \mathbf{w},\mathbf{u}\rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w} \\
&\le \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^\star\in\Lambda_e^\star} \int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2} e^{-2\pi i\langle \mathbf{w},\mathbf{u}\rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w}
\end{aligned}$$

by noting that the sine term of the exponential averages out to zero when summing over all lattice points, and where the last inequality follows from the fact that the cosine term takes its maximum value (that is 1) when $\mathbf{u}\in\Lambda$.

Using a similar argument, write $e^{-2\pi i\langle \mathbf{w},\mathbf{u}\rangle} = \cos(2\pi\langle \mathbf{w},\mathbf{u}\rangle) - i\sin(2\pi\langle \mathbf{w},\mathbf{u}\rangle)$ and note that for a given $\mathbf{u}$, the integral over $\mathbb{R}^n$ will make the sine term alternate, so that $-e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}$ and $e^{-2\sigma_e^2\pi^2||\mathbf{t}^*+\mathbf{w}||^2}$ both will appear as a factor of $i\sin(2\pi\langle \mathbf{w},\mathbf{u}\rangle)\hat{f}_2(\mathbf{w})$ ($\hat{f}_2(\mathbf{w})$ is even by hypothesis), and the sum over all lattices averages out to zero, since

the four terms $-e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}$, $e^{-2\sigma_e^2\pi^2||\mathbf{t}^*+\mathbf{w}||^2}$ and $-e^{-2\sigma_e^2\pi^2||-\mathbf{t}^*-\mathbf{w}||^2}$, $e^{-2\sigma_e^2\pi^2||-\mathbf{t}^*+\mathbf{w}||^2}$ appear as a factor of $i\sin(2\pi\langle\mathbf{w},\mathbf{u}\rangle)\hat{f}_2(\mathbf{w})$. Thus

$$\sum_{\mathbf{t}\in\Lambda_e} f(\mathbf{t}) \leq \mathrm{vol}(\Lambda_e)^{-1}\sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^\star\in\Lambda_e^\star}\int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}\hat{f}_2(\mathbf{w})d\mathbf{w}.$$

This yields a first upper bound on Eve's probability $P_{c,e}$ of making a correct decision:

$$\begin{aligned} P_{c,e} &\leq \mathrm{vol}(\Lambda_e)^{-1}\int_{\mathcal{V}(\Lambda_b)}\left(\sum_{\mathbf{t}^\star\in\Lambda_e^\star}\int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}\hat{f}_2(\mathbf{w})d\mathbf{w}\right)d\mathbf{u} \\ &= \frac{\mathrm{vol}(\Lambda_b)}{\mathrm{vol}(\Lambda_e)}\sum_{\mathbf{t}^\star\in\Lambda_e^\star}\int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}\hat{f}_2(\mathbf{w})d\mathbf{w}. \end{aligned}$$

To obtain an expression which depends on $\Lambda_e$ instead of $\Lambda_e^\star$, we denote this time

$$f(\mathbf{t}^\star) = \int_{\mathbb{R}^n} e^{-2\sigma_e^2\pi^2||\mathbf{t}^*-\mathbf{w}||^2}\hat{f}_2(\mathbf{w})d\mathbf{w},$$

and the Poisson summation formula for lattices now gives

$$\sum_{\mathbf{t}^\star\in\Lambda_e^\star} f(\mathbf{t}^\star) = \mathrm{vol}(\Lambda_e)\sum_{\mathbf{t}\in\Lambda}\hat{f}(\mathbf{t})$$

where $\hat{f}(\mathbf{t}) = \int_{\mathbb{R}^n} e^{-2\pi i\langle\mathbf{t},\mathbf{v}\rangle}f(\mathbf{v})d\mathbf{v}$, and we recognize that $\hat{f}(\mathbf{t})$ is actually the Fourier transform of the convolution of $e^{-2\sigma_e^2\pi^2||\mathbf{v}||^2}$ and $\hat{f}_2(\mathbf{v})$. We then obtain the product of Fourier transforms, that is

$$\begin{aligned} \hat{f}(\mathbf{t}) &= \left(\int_{\mathbb{R}^n} e^{-2\pi i\langle\mathbf{t},\mathbf{v}\rangle}e^{-2\pi^2\sigma_e^2||\mathbf{v}||^2}d\mathbf{v}\right)f_2(\mathbf{t}) \\ &= \left(\prod_{j=1}^n\int_{\mathbb{R}} e^{-2\pi i t_j v_j}e^{-2\pi^2\sigma_e^2 v_j^2}dv_j\right)f_2(\mathbf{t}) \\ &= \left(\frac{1}{\sqrt{2\pi\sigma_e^2}}\right)^n\prod_{j=1}^n e^{\frac{-t_j^2}{2\sigma_e^2}}\chi_{\mathcal{R}}(\mathbf{t}) \\ &= \left(\frac{1}{\sqrt{2\pi\sigma_e^2}}\right)^n e^{-\frac{||\mathbf{t}||^2}{2\sigma_e^2}}\chi_{\mathcal{R}}(\mathbf{t}) \end{aligned}$$

using again (2.4).

Finally the probability of making a correct decision for Eve is summarized by

$$P_{c,e} \leq \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\mathrm{vol}(\Lambda_b)\sum_{\mathbf{t}\in\Lambda_e\cap\mathcal{R}} e^{-\|\mathbf{t}\|^2/2\sigma_e^2}. \tag{2.5}$$

□

**Remark 4.** *One may take the region $\mathcal{R}$ to be a cube centered around the origin. This will satisfy the hypothesis of the proposition. In the case the shaping region does not satisfy the hypothesis it can always be inserted into a cube of the right size, which will serve as an upper bound.*

Using lattice encoding, recall that the message sent by Alice intended to Bob is transmitted as a codeword $\mathbf{x} \in \Lambda_b$, that is

$$\mathbf{x} = M_b\lambda,\ \lambda \in \mathbb{Z}^n,$$

where $M_b$ is the generator matrix of the lattice $\Lambda_b$. We can rewrite the fast fading channel in (2.2) accordingly:

$$\begin{array}{rcl} \mathbf{y} & = & \mathsf{diag}(\mathbf{h}_b)M_b\lambda + \mathbf{v}_b \\ \mathbf{z} & = & \mathsf{diag}(\mathbf{h}_e)M_b\lambda + \mathbf{v}_e, \end{array} \tag{2.6}$$

and we interpret $\mathsf{diag}(\mathbf{h}_b)M_b$, respectively $\mathsf{diag}(\mathbf{h}_e)M_b$ as the generator matrix of the lattice $\Lambda_{b,\mathbf{h}_b}$, respectively $\Lambda_{b,\mathbf{h}_e}$ and these are the lattices intended to Bob as seen through Bob's and Eve's channel respectively.

Using the above proposition, we are now ready to derive a code design criterion for fast fading and block fading wiretap channels.

**Corollary 1.** *[27] Suppose transmission over a fast fading wiretap channel as described in (2.2), where coset coding is performed using the lattices $\Lambda_e \subset \Lambda_b$, under the same hypothesis as in the above proposition. Then Eve's average probability $\bar{P}_{c,e}$ of correct decision is upper bounded by*

$$\bar{P}_{c,e} \leq \left(\frac{\sigma_{h,e}^2}{\sigma_e^2}\right)^{n/2} \mathrm{vol}(\Lambda_b) \sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R}} \prod_{i=1}^{n} \frac{1}{\left(1 + |x_i|^2(\sigma_{h,e}^2/\sigma_e^2)\right)^{3/2}}. \tag{2.7}$$

*Proof.* The proof technique is the same as that of [23]. Once the fading coefficients are fixed, the channel (2.2) becomes a Gaussian wiretap channel, where the lattice point sent now belongs to a new lattice which includes the fading matrix: if $\mathbf{x}$ is a lattice point of the form $\mathbf{x} = M\mathbf{u}$, $\mathbf{u} \in \mathbb{Z}^n$, where $M$ is the generator matrix of the lattice in use, then $\mathsf{diag}(\mathbf{h}_b)M\mathbf{u}$ still belongs to a lattice, with generator matrix $\mathsf{diag}(\mathbf{h}_b)M$. The upper bound of the proposition is then used, and the average probability of error is computed over different fading realizations (using that the coefficients are Rayleigh distributed). □

**Remark 5.** *Note that the upper bound in the above corollary is very similar to that obtained for fast fading channels classically [25], except for the sum. Indeed, Bob is not affected by the randomization introduced by $\Lambda_e$, since Alice transmits based on Bob's channel. For Bob, his average error probability $\bar{P}_{e,b}$ when sending a lattice point (of the finite constellation $\mathcal{R}$) is*

$$\bar{P}_{e,b} \leq \frac{1}{2} \prod_{x_i \neq 0} \frac{4\sigma_b^2}{|x_i|^2}.$$

*The usual design for fast fading channels is to minimize $\bar{P}_{e,b}$ and then simplified to give that the dominant term*

$$\frac{1}{\prod_{x_i \neq 0} |x_i|^2} \tag{2.8}$$

*should be minimized. In particular, the $n$ components of every lattice point should be non-zero, property referred to as full diversity.*

**Definition 10.** *The diversity of a lattice $\Lambda \in \mathbb{R}^n$ is defined by*

$$div(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \#\{i \mid x_i \neq 0, i = 1, ..., n\}.$$

As the property of diversity of a lattice is closely related to the code design [25] for reliable transmission, ideally we would like all the non-zero vectors $\mathbf{x} \in \Lambda_e$ to have only non-zero coefficients. Thus we are looking for full diversity (where the diversity is the length $n$ of the vector) lattice in order to minimize Bob's probability of error in decoding. The study of diversity is well understood in the context of *ideal lattices* which will be addressed in the next chapter.

Recall that our focus is to minimize the probability $P_{c,e}$ of Eve's correct decision in doing coset decoding. Some simplication of the sum from (2.7) and comparison to the dominant term in (2.8), yields as wiretap code design criterion to minimize

$$\sum_{\mathbf{x} \in \Lambda_e \cap \mathcal{R}} \prod_{i=0}^{n} \frac{1}{|x_i|^3} \tag{2.9}$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\forall x_i \neq 0$. It may not give the best bound but a first understanding of the situation.

On the other hand, when we are dealing with a block fading channel, we look at the $Nn-$dimensional lattice structure of the transmitted signal and we vectorize the

received signal in (2.1) to obtain

$$\begin{aligned}\mathrm{vec}(Y) &= \mathrm{vec}(\mathsf{diag}(\mathbf{h}_b)X) + \mathrm{vec}(V_b)\\ &= \begin{pmatrix} \mathsf{diag}(\mathbf{h}_b) & & \\ & \ddots & \\ & & \mathsf{diag}(\mathbf{h}_b) \end{pmatrix} \mathrm{vec}(X) + \mathrm{vec}(V_b)\end{aligned}$$

$$\begin{aligned}\mathrm{vec}(Z) &= \mathrm{vec}(\mathsf{diag}(\mathbf{h}_b)X) + \mathrm{vec}(V_b)\\ &= \begin{pmatrix} \mathsf{diag}(\mathbf{h}_b) & & \\ & \ddots & \\ & & \mathsf{diag}(\mathbf{h}_b) \end{pmatrix} \mathrm{vec}(X) + \mathrm{vec}(V_b),\end{aligned}$$

and we interpret the $n \times L$ codeword $X$ as coming from a lattice by writing

$$\mathrm{vec}(X) = M_b\lambda, \text{resp, } \mathrm{vec}(X) = M_e\lambda$$

where $\lambda \in \mathbb{Z}^{Nn}$ and $M_b$ (resp. $M_e$) denotes the $Nn \times Nn$ generator matrix of the lattice intended to Bob (resp. Eve). Similar to the setting of fast fading channels, we interpret $\mathsf{diag}(\mathsf{diag}(\mathbf{h}_b), ..., \mathsf{diag}(\mathbf{h}_b))M_b$, respectively $\mathsf{diag}(\mathsf{diag}(\mathbf{h}_e), ..., \mathsf{diag}(\mathbf{h}_e))M_e$ as the generator matrix of the lattice $\Lambda_{b,\mathbf{h}_b}$, respectively $\Lambda_{b,\mathbf{h}_e}$ and these are the lattices intended to Bob as seen through Bob's and Eve's channel respectively.

**Corollary 2.** *Suppose transmission over a block fading wiretap channel as described in (2.1), where coset coding is performed using the lattices $\Lambda_e \subset \Lambda_b$, under the same hypothesis as in the above proposition. Then Eve's average probability $\bar{P}_{c,e}$ of correct decision is upper bounded by*

$$\bar{P}_{c,e} \leq \left(\frac{\sigma_{h,e}^2}{\sigma_e^2}\right)^{n/2} \mathrm{vol}(\Lambda_b) \sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R}} \prod_{i=1}^{n} \frac{1}{\left(1 + \|x_i\|^2 (\sigma_{h,e}^2/\sigma_e^2)\right)^{\frac{N}{2}+1}}. \tag{2.10}$$

*Proof.* Use the vectorization of the transmitted signal $X$ and the received signals $Y$ and $Z$, then apply the proof of Corollary 1. □

**Remark 6.** *Like for fast fading channels, for slow fading channels, we want to ensure that full diversity is achieved so we identify the dominant term*

$$\sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R}} \prod_{i=1}^{n} \frac{1}{\|\mathbf{x}_i\|^{N+2}}$$

*to be minimized where $\mathbf{x} = (x_1, \ldots, x_n)$ and $x_i \neq 0$, $\forall i$.*

In summary, given the region $\mathcal{R}$ that describes a finite constellation carved into the infinite lattice $\Lambda_e$, we want to minimize the probability $P_{c,e}$ of Eve's correct decision in decoding. Namely:

for fast fading channels, we want to minimize

$$\sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R}} \prod_{i=0}^{n} \frac{1}{|x_i|^3}$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ and $x_i \neq 0$, $\forall i$;

for slow fading channels, we want to minimize

$$\sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R}} \prod_{||\mathbf{x}_i||\neq 0} \frac{1}{||\mathbf{x}_i||^{N+2}}$$

where $\mathbf{x}_i$ is the $i$th row of some $n \times L$ matrix $X$ such that $\mathbf{x} = \mathsf{vec}(X)$ is a point in $\Lambda_e$.

# Chapter 3

# Wiretap Codes from Ideal Lattices

In the previous chapter, we defined our coding problems to be the construction of good wiretap lattice codes based on the proposed code design criterion. In order to construct lattice codes, in this chapter, we introduce algebraic lattices, obtained by applying a twisted canonical embedding of an algebraic number field to its ring of integers. In particular, we study a family of algebraic lattices endowed with a *trace form* called ideal lattices and from there, we further identify wiretap code design criteria for *ideal lattices*. To begin with, we introduce some concepts of algebraic number theory which will be needed.

## 3.1 Some Concepts from Algebraic Number Theory

We assume that the reader has some basic knowledge of abstract algebra especially of basic field theory and Galois theory. In this section, we introduce some basic concepts of algebraic number theory by including the relevant definitions and results which will be needed to introduce *ideal lattices*.

In the beginning of this section, we define algebraic number fields and rings of integers. We then introduce some terminology related to ramification, embeddings and the discriminant of a number field. Finally, we introduce cyclotomic fields which will be number fields that we focus on.

For further reading on algebraic number theory, the reader may refer to [31], [21] and [28].

### 3.1.1 Algebraic Number Fields

**Definition 11.** *An algebraic number field (or simply* number field*) is a finite field extension of the field of rational numbers, $\mathbb{Q}$.*

**Definition 12.** *A quadratic field is a number field of degree 2 over $\mathbb{Q}$.*

In order to illustrate several concepts from algebraic number theory, we will include examples based on quadratic fields.

**Definition 13.** *Let $L/K$ be a field extension, and let $\alpha \in L$. If there exists a non-zero irreducible monic (coefficient of highest power equals to 1) polynomial $p \in K[X]$ such that $p(\alpha) = 0$, we say that $\alpha$ is algebraic over $K$. Such a polynomial is called the minimal polynomial of $\alpha$ over $K$.*

**Example 1.** *The polynomials $X^2 - 3$ and $X^2 + 1$ are respectively the minimal polynomials of $\sqrt{3}$ and $\sqrt{-1}$ over $\mathbb{Q}$.*

### 3.1.2 The Ring of Integers of a Number Field

**Definition 14.** *Let $K$ be a number field. An element $\alpha \in K$ is an* algebraic integer *if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$.*

**Definition 15.** *The set of algebraic integers of a number field $K$ is a ring called the* ring of integers *of $K$, denoted by $\mathcal{O}_K$. For a proof that $\mathcal{O}_K$ is a ring, see [31].*

**Theorem 2.** *[31] If $K$ is a number field, then $K = \mathbb{Q}(\theta)$ for an algebraic integer $\theta \in \mathcal{O}_K$.*

**Example 2.** *Consider a quadratic field $\mathbb{Q}(\theta)$ where $\theta$ is an algebraic integer. Then $\theta$ is a root of $X^2+aX+b$ ($a, b \in \mathbb{Z}$). By taking $a^2-4b = t^2d$ where both $t$ and $d$ are integers, the quadratic fields are precisely those of the form $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ for $d$ a squarefree rational integer.*

**Remark 7.** *A quadratic field is said to be real if $d$ is positive, imaginary if $d$ is negative.*

**Example 3.** *$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ are real and imaginary quadratic fields respectively.*

**Theorem 3.** *[31] Let $K$ be a number field of degree $n$. The ring of integers $\mathcal{O}_K$ of $K$ forms a free $\mathbb{Z}$-module*[1] *of rank $n$ (that is, there exists a basis of $n$ elements over $\mathbb{Z}$).*

**Definition 16.** *Let $\{w_i\}_{i=1}^n$ be a basis of the $\mathbb{Z}$-module $\mathcal{O}_K$, so that we can uniquely write any element of $\mathcal{O}_K$ as $\sum_{i=1}^n a_i w_i$ with $a_i \in \mathbb{Z}$ for all $i$. We say that $\{w_i\}_{i=1}^n$ is an* integral basis *of $K$.*

Integral bases are in general not easy to compute. The case of quadratic fields is an exception.

**Theorem 4.** *[31] Let $d$ be a squarefree rational integer. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

1. $\mathbb{Z}\left[\sqrt{d}\right]$ *if* $d \not\equiv 1 \pmod 4$,
2. $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *if* $d \equiv 1 \pmod 4$.

**Example 4.** *The integral basis of $\mathbb{Q}(\sqrt{d})$ is thus*

1. $\{1, \sqrt{d}\}$ *if* $d \not\equiv 1 \pmod 4$,
2. $\{1, \frac{1+\sqrt{d}}{2}\}$ *if* $d \equiv 1 \pmod 4$.

*In particular, $\{1, \sqrt{2}\}$ and $\{1, \frac{1+\sqrt{5}}{2}\}$ are integral bases of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ respectively.*

### 3.1.3 Ramification

In the ring of integers of a number field $\mathcal{O}_K$, a prime $p$ of $\mathbb{Z}$ may not remain a prime. For example, in the ring of integers of $\mathbb{Q}(\sqrt{2})$, $7 = (3+\sqrt{2})(3-\sqrt{2})$. Thanks to Kummer and Dedekind, it is known that the ideal generated by $p$ in this ring can be uniquely factored as a product of prime ideals. This scenario may be loosely described as *ramification*. Before we introduce *Dedekind domain*, we recall some concepts about *ideals*.

**Definition 17.** *An ideal $\mathcal{I}$ of a commutative ring $R$ is an additive subgroup of $R$ such that for all $r \in R$, then $r\mathcal{I} \subseteq \mathcal{I}$.*

[1] The concept of a module over a ring is a generalization of the notion of vector space. The scalars may lie in any arbitrary ring instead of a field.

**Definition 18.** *An ideal $\mathfrak{I}$ of $R$ is proper if $\mathfrak{I} \neq R$. We say that is it non-trivial if $\mathfrak{I} \neq R$ and $\mathfrak{I} \neq 0$.*

**Definition 19.** *An ideal $\mathfrak{I}$ of $R$ is principal if it is of the form*

$$\mathfrak{I} = xR = \{xy,\ y \in R\},\ x \in \mathfrak{I}.$$

**Definition 20.** *A principal ideal domain (PID) is an integral domain in which every ideal is principal.*

The case when $\mathcal{O}_K$ is a principal ideal domain will be of particular interest for our study. The class number of $K$, denoted by $h_K$, is a measure of how principal a ring of integers is. When $\mathcal{O}_K$ is a principal ideal domain, we have $h_K = 1$. For a formal definition of the class number of $K$, the reader may refer for example to [9].

We know that the norm of a principal ideal is computed by taking the absolute value of the norm of its generator as defined next.

**Definition 21.** *[31] Let $\mathfrak{I} = x\mathcal{O}_K$ be a principal ideal of $\mathcal{O}_K$. Its norm is defined by $N(\mathfrak{I}) = |N(x)|$, where $N(x)$ is the norm of an element $x$ (see Definition 31).*

**Definition 22.** *A maximal ideal in the ring $R$ is a proper ideal that is not contained in any strictly larger proper ideal.*

**Definition 23.** *A prime ideal in a commutative ring $R$ is a proper ideal $\mathfrak{p}$ of $R$ such that for any $x, y \in R$, we have that*

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}.$$

**Definition 24.** *A* Dedekind domain *is an integral domain $R$ such that*

1. *Every ideal is finitely generated;*
2. *Every nonzero prime ideal is a maximal ideal;*
3. *$R$ is integrally closed in its field of fractions*

$$F = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}.$$

*The above last condition means that whenever $\alpha/\beta \in F$ and satisfies a monic polynomial $f \in R[X]$, then $\alpha/\beta \in R$.*

**Remark 8.** *The above first condition is equivalent to each of the conditions*

1. *Any ascending chain of ideals stablilizes.*

2. *Every non-empty set $S$ of ideals contains a maximal element $I_0$, meaning that $I_0 \in S$, and there is no element of $S$ which contains $I_0$ properly.*

*A ring satisfying the above two conditions is called a Noetherian ring.*

**Theorem 5.** *[21] The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

**Theorem 6.** *[21] Every nonzero proper ideal in a Dedekind domain is uniquely factored as a product of prime ideals, up to reordering.*

**Corollary 3.** *[21] Every nonzero proper ideal of the ring of integers $\mathcal{O}_K$ can be factored uniquely into prime ideal(s), up to reordering.*

**Definition 25.** *Let $(p)$ be a prime ideal of $\mathbb{Z}$ for a prime $p$. A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to* lie over *$p$ if $\mathfrak{p} \cap \mathbb{Z} = (p)$.*

Since $\mathcal{O}_K$ is a Dedekind domain, for any nonzero prime ideal $(p)$ of $\mathbb{Z}$, the extension $p\mathcal{O}_K$ of $(p)$ to $\mathcal{O}_K$ is a nonzero proper ideal of $\mathcal{O}_K$ and hence it can be uniquely written as

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_g$ are distinct nonzero prime ideals of $\mathcal{O}_K$ and $e_i$ are positive integers. Moreover, $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field which is a finite extension of the finite field $\mathbb{Z}/(p)$.

**Definition 26.** *The positive integer $e_i$ above is called the ramification index of $\mathfrak{p}_i$ over $(p)$ and is denoted by $e(\mathfrak{p}_i/(p))$; the field degree $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/(p)]$ is called the residue class degree (or the inertial degree) of $\mathfrak{p}_i$ over $(p)$ and is denoted by $f(\mathfrak{p}_i/(p))$. If $e_i > 1$ for some $i$, then we say that $(p)$ is ramified in $\mathcal{O}_K$. Otherwise, it is said to be unramified.*

**Theorem 7.** *[20] Let $\mathcal{O}_K$ be as above and $n = [K : \mathbb{Q}]$. Suppose $(p)$ is a prime ideal of $\mathbb{Z}$. We have*

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

*where $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_g$ are distinct nonzero prime ideals of $\mathcal{O}_K$ and $e_1, e_2, ..., e_g$ are positive integers. Then, upon denoting $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/(p)]$, we have*

$$\sum_{i=1}^{g} e_i f_i = n.$$

**Definition 27.** *We say that $p$ is inert if $(p)\mathcal{O}_K = \mathfrak{p}_1$ is prime, in which case we have $g = 1$, $e_1 = 1$ and $f(\mathfrak{p}_1/(p)) = n$. We say that $p$ is totally ramified if $(p)\mathcal{O}_K = \mathfrak{p}_1^n$ that is $e_1 = n$, $g = 1$, and $f(\mathfrak{p}_1/(p)) = 1$. Moreover, we say that $p$ is totally split if $(p)\mathcal{O}_K = \prod_{i=1}^{n} \mathfrak{p}_i$, that is $g = n$ and $f(\mathfrak{p}_i/(p)) = e_i = 1,\ \forall i$.*

**Remark 9.** *If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ appears in the factorization of $(p)\mathcal{O}_K$, we say that $\mathfrak{p}$ divides $p$ denoted by $\mathfrak{p}|p$.*

**Theorem 8.** *[20] Let $K$ be a normal number field. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be two primes of $\mathcal{O}_K$ lying over $(p)$, then $e(\mathfrak{q}/(p)) = e(\mathfrak{q}'/(p))$ and $f(\mathfrak{q}/(p)) = f(\mathfrak{q}'/(p))$.*

**Corollary 4.** *Let $\mathfrak{p}$ be a prime ideal of a Galois field extension, then*

$$\sum_{i=1}^{g} e_i f_i = efg = n$$

*where $e = e(\mathfrak{p}/(p))$ and $f = f(\mathfrak{p}/(p))$. Moreover, there exists only a finite number of prime ideals in $\mathcal{O}_K$ lying over $(p)$.*

**Example 5.** *For a quadratic field $K$, the possibilities for the factorization of $(p)$ in $\mathcal{O}_K$ are*

$$(p)\mathcal{O}_K = \begin{cases} (p) \text{ is prime.} \Leftrightarrow p \text{ is inert in } K. \\ \mathfrak{p}\mathfrak{q},\ \mathfrak{p} \neq \mathfrak{q} \Leftrightarrow p \text{ totally splits in } K. \\ \mathfrak{p}^2 \Leftrightarrow p \text{ ramifies in } K. \end{cases}$$

**Example 6.** *Let $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ with ring of integers $\mathbb{Z}[i]$, the ideals $(5)\mathbb{Z}[i] = (2+i)(2-i)$ and $(2)\mathbb{Z}[i] = (1+i)^2$. These say that 5 and 2 are totally split prime and ramified prime respectively.*

### 3.1.4 Field Embeddings

After recalling the definition of field embeddings, we introduce the notion of *norm*, *trace* and *discriminant* of a number field. In the end of this section, we notice that field embeddings allow us to transform the ring of integers of a number field into a lattice in the Euclidean space which serves our purpose.

**Definition 28.** *Let $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ be two field extensions of $\mathbb{Q}$. We call $\varphi : K_1 \to K_2$ a* $\mathbb{Q}$-homomorphism *if $\varphi$ is a ring homomorphism that satisfies $\varphi(a) = a$ for all $a \in \mathbb{Q}$, i.e., that fixes $\mathbb{Q}$. Recall that if $A$ and $B$ are rings, a ring homomorphism is a map $\psi : A \to B$ that satisfies, for all $a, b \in A$*

*(1)* $\psi(a+b) = \psi(a) + \psi(b)$,

*(2)* $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$,

*(3)* $\psi(1) = 1$.

**Definition 29.** *A $\mathbb{Q}$-homomorphism $\varphi : K \to \mathbb{C}$ is called an* embedding *of $K$ into $\mathbb{C}$ and by the properties of ring homomorphism, it is an injective map.*

**Definition 30.** *Let $K = \mathbb{Q}(\theta)$ be a number field of degree $n$ over $\mathbb{Q}$. There are exactly $n$ embeddings of $K$ into $\mathbb{C} : \sigma_i \to \mathbb{C}$, $i = 1, ..., n$, defined by $\sigma_i(\theta) = \theta_i$, where $\theta_i$ are the distinct zeros on $\mathbb{C}$ of the minimal polynomial of $\theta$ over $\mathbb{Q}$.*

**Example 7.** *We define the two embeddings from $\mathbb{Q}(\sqrt{d})$ into $\mathbb{C}$, namely the identity and conjugation mappings as follows,*

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d},$$

$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

**Definition 31.** *Let $K$ be a number field of degree $n$ and $x \in K$. The elements*

$$\sigma_1(x), \sigma_2(x), ..., \sigma_n(x)$$

*are the conjugates of $x$. The norm of $x$ is defined as*

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

*whereas the trace of $x$ is defined as*

$$\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

**Example 8.** *Using the embeddings defined in Example 7, we compute the norm and trace of of any element in $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ respectively, we obtain as follows,*

$$\begin{aligned} N_{K/\mathbb{Q}}(a + b\sqrt{d}) &= \sigma_1(a + b\sqrt{d}) \cdot \sigma_2(a + b\sqrt{d}) &= a^2 - b^2 d, \\ \mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) &= \sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) &= 2a. \end{aligned}$$

We further list down some properties of the norm and trace.

**Theorem 9.** *[12] Let $L$ be a finite dimensional extension field of $N$ and let $x, y \in L$. Then $N_{L/N}(xy) = N_{L/N}(x)N_{L/N}(y)$.*

**Theorem 10.** *[29][Transitivity of the Norm and Trace] If $L \subseteq M \subseteq N$ and $a \in N$, then*

*(i)* $N_{M/L} \circ N_{N/M}(a) = N_{N/L}(a)$

*(ii)* $\mathrm{Tr}_{M/L} \circ \mathrm{Tr}_{N/M}(a) = \mathrm{Tr}_{N/L}(a)$

*where $\circ$ denotes composition of map.*

**Theorem 11.** *[31] For any $x \in K$,we have $N_{K/\mathbb{Q}}(x)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Q}$. If $x \in \mathcal{O}_K$, we have $N_{K/\mathbb{Q}}(x)$, $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.*

**Corollary 5.** *The norm $N_{K/\mathbb{Q}}(\alpha)$ of an element $\alpha$ of $\mathcal{O}_K$ is equal to $\pm 1$ if and only if $\alpha$ is a unit of $\mathcal{O}_K$.*

**Definition 32.** *The elements $a, b$ in a ring are called associates if $a = ub$ for some unit $u$.*

**Corollary 6.** *For an element $v$ in a ring, its associates have the same norm.*

**Definition 33.** *Let $\{w_1, w_2, ..., w_n\}$ be an integral basis of $K$. The* discriminant *of $K$ is defined as $d_K = \det[(\sigma_j(w_i))_{i,j=1}^n]^2$.*

**Theorem 12.** *[31] The discriminant $d_K$ of a number field belongs to $\mathbb{Z}$.*

**Theorem 13.** *[31] Let $d$ be a squarefree rational integer. Then the discriminant $d_K$ of the ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

*(1)* $4d$ *if* $d \not\equiv 1 \pmod 4$,

*(2)* $d$ *if* $d \equiv 1 \pmod 4$.

The prime factorization of the discriminant provides important information about ramification. Indeed, the following result that relates the discriminant with the ramification is known.

**Theorem 14.** *[20] Let $K$ be a number field. Let $p$ be a prime in $\mathbb{Z}$. A prime $p \in \mathbb{Z}$ is ramified in $\mathcal{O}_K$ if and only if $p$ divides $d_K$.*

**Corollary 7.** *There is only a finite number of ramified primes.*

*Proof.* The discriminant contains only a finite number of prime divisors. □

**Example 9.** *Consider the quadratic fields* $\mathbb{Q}(\sqrt{3})$ *and* $\mathbb{Q}(\sqrt{5})$*. Their discriminants are* 12 *and* 5 *respectively. Only* 2 *and* 3 *ramify in* $\mathbb{Q}(\sqrt{3})$ *whereas the only ramified prime in* $\mathbb{Q}(\sqrt{5})$ *is* 5*.*

**Definition 34.** *Let* $\{\sigma_1, \sigma_2, ..., \sigma_n\}$ *be the* $n$ *distinct embeddings of* $K$ *into* $\mathbb{C}$*. Let* $r_1$ *be the number of embeddings with image in* $\mathbb{R}$*, and* $r_2$ *the number of pairs of complex conjugate embeddings with image in* $\mathbb{C}$ *so that*

$$r_1 + 2r_2 = n.$$

*The pair* $(r_1, r_2)$ *is called the* signature *of* $K$*. If* $r_2 = 0$*, we have a* totally real *number field. If* $r_1 = 0$ *we have a* totally complex *number field.*

**Example 10.** *For a quadratic field, its signature is either* $(2, 0)$ *or* $(0, 1)$*. In other words, a quadratic field is either a totally real number field or a totally complex number field.*

In fact, the signature of a number field is related to the following well known theorem which describes the group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$.

**Theorem 15.** *[21, p.42, Dirichlet's Units Theorem] The group of units* $\mathcal{O}_K^*$ *of* $\mathcal{O}_K$ *is the direct product of the finite cyclic group* $\mu(K)$ *and a free abelian group of rank* $r_1 + r_2 - 1$ *where the numbers* $r_1$ *and* $r_2$ *are as described in Definition 34.*

**Remark 10.** *Note that the finite cyclic group* $\mu(K)$ *is the group of roots of unity of* $K$*.*

**Example 11.** *If* $d$ *is a positive squarefree rational integer, then the group of units* $\mathcal{O}_K^*$ *of the real quadratic field* $K = \mathbb{Q}(\sqrt{d})$ *is* $\mathcal{O}_K^* \cong \{-1, 1\} \times C$*, where* $C$ *a free abelian group of rank 1. This implies that there exist infinitely many other units in real quadratic fields. Except quadratic imaginary fields and the rational field, all other number fields have strictly positive rank for their group of units. In other words, all other number fields have infinitely many units except for quadratic imaginary fields and the rational field* $\mathbb{Q}$*.*

In general a Galois number field is either totally real or totally imaginary which is proven in the following lemma.

**Lemma 1.** *Let* $K/\mathbb{Q}$ *be a number field that is Galois over* $\mathbb{Q}$*. Then* $K$ *is either totally real or totally imaginary.*

*Proof.* For all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma : K \hookrightarrow \bar{\mathbb{Q}}$ yields an automorphism of $K$, where $\bar{Q}$ is the algebraic closure of $\mathbb{Q}$. In particular, $\sigma(K) = K$. Since $K/\mathbb{Q}$ is a finite separable extension, by the Primitive Element Theorem, $K = \mathbb{Q}(\theta)$. Then the minimal polynomial of $\theta$, $\mu_\theta$ either has a real root or it does not. Moreover, since $K$ is normal extension, all the roots of $\mu_\theta$ are in $K$. Assume there is one real root, $\alpha$ and for some $\sigma' \in \mathrm{Gal}(K/\mathbb{Q})$, we have

$$\sigma' : \mathbb{Q}(\theta) \hookrightarrow \mathbb{Q}(\alpha) \subset \mathbb{R}$$

since $\sigma' : \theta \mapsto \alpha$. Hence, $K \subset \mathbb{R}$.

□

**Definition 35.** *A number field $K$ is called a CM-field if there exists a totally real number field $F$ such that $K$ is a totally imaginary quadratic extension of $F$. Clearly all imaginary quadratic extensions are CM-fields.*

**Definition 36.** *Let $\{\sigma_1, \sigma_2, ..., \sigma_n\}$ be the $n$ distinct embeddings of $K$ into $\mathbb{C}$. Arrange all the embeddings in such a way that for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$ and $\sigma_{j+r_2}$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. We call canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ the homomorphism defined by*

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), \sigma_{r_1+1}(x), ..., \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

*If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$*

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), ..., \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)) \in \mathbb{R}^n$$

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

**Remark 11.** *The canonical embedding is an injective ring homomorphism. Thus it gives an injective map between the elements of a number field $K$ and the vectors of $\mathbb{R}^n$ and this will be useful when we construct algebraic lattices.*

Next we introduce *cyclotomic fields* which are well known families of number fields. We will use cyclotomic fields often in the next chapters. So in the next section, we recall some definitions and properties of cyclotomic fields which will be needed later on.

### 3.1.5 Cyclotomic Fields

**Definition 37.** *An n-th* root of unity *denoted by $\alpha$ is a root of the polynomial $X^n - 1$. An n-th root of unity is* primitive *if $\alpha^k \neq 1$ for $k = 1, 2, ..., n-1$. We denote by $\zeta_n$ a primitive n-th root of unity.*

**Definition 38.** *[30] A cyclotomic field is a number field obtained by adjoining a complex primitive n-th root of unity, $\zeta_n$ to the rational field $\mathbb{Q}$. The minimal polynomial of $\zeta_n$ over $\mathbb{Q}$ divides $X^n - 1$, so its roots are nth roots of unity and consequently, powers of $\zeta_n$.*

**Remark 12.** *[30] A cyclotomic field K is a Galois field extension and its Galois group $Gal(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. Thus the degree of the field extension $[K : \mathbb{Q}]$ is given by $\varphi(n)$ where $\varphi(n)$ is the Euler's phi function.*

**Definition 39.** *$K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the totally real maximal subfield of $\mathbb{Q}(\zeta_n)$. Note that $\zeta_n$ is a root of polynomial $X^2 - (\zeta_n + \zeta_n^{-1})X + 1 = 0$ over $K^+$. Thus $[K : K^+] = 2$. This further implies that $[K^+ : \mathbb{Q}] = \varphi(n)/2$.*

**Example 12.** *$\mathbb{Q}(\zeta_n)$ is a CM-field since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the totally real maximal subfield of $\mathbb{Q}(\zeta_n)$.*

**Theorem 16.** *[33] The rings of integers of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ are $\mathbb{Z}[\zeta_n]$ and $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ respectively.*

**Theorem 17.** *[21] Let $K = \mathbb{Q}(\zeta_p)$ and $p, q$ be distinct rational primes, then $q$ is unramified in $K$ and in fact*

$$(q)\mathcal{O}_K = \mathfrak{q}_1 ... \mathfrak{q}_t$$

*with mutually distinct prime ideals $\mathfrak{q}_i$ and each of inertial degree $f = f(\mathfrak{q}_i/q)$ equal to the order of $q$ in $(\mathbb{Z}/p)^\times$,i.e., $f$ is the least natural number such that*

$$q^f \equiv 1 \pmod{p}.$$

**Theorem 18.** *[6] Let $p$ be an odd prime, $r$ a positive integer and $K'$ a subfield of $\mathbb{Q}(\zeta_{p^r})$ with $[K' : \mathbb{Q}] = up^j$ where $p$ does not divide $u$. Then the discriminant of $K'$, up to sign, $d_{K'} = p^{u((j+2)p^j - \frac{p^{j+1}-1}{p-1})-1}$.*

**Remark 13.** *Let $p$ be an odd prime. Since $\mathbb{Q}(\zeta_{p^r})$ is a Galois field extension whose Galois group is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^*$, a cyclic group, it is well known that there is one-to-one correspondence between the subfields of $\mathbb{Q}(\zeta_{p^r})$ and the divisors of $(p-1)p^{r-1}$*

*which is the degree of* $\mathbb{Q}(\zeta_{p^r})$ *over* $\mathbb{Q}$*. Thus we can notice that* $u$ *from the above theorem is a divisor of* $p-1$ *and* $j \leq r-1$*. Furthermore, all subfields of* $\mathbb{Q}(\zeta_{p^r})$ *are Galois extensions and by Lemma 1, each subfield of* $\mathbb{Q}(\zeta_{p^r})$ *is either totally real or totally imaginary.*

**Theorem 19.** *[33] For* $p$ *prime, the discriminant of* $\mathbb{Q}(\zeta_{p^r})$ *is* $\pm p^{p^{r-1}(pr-r-1)}$*, where we have* $-$ *if* $p^r = 4$ *or* $p \equiv 3 \pmod 4$*, and we have* $+$ *otherwise.*

**Example 13.** $K = \mathbb{Q}(\zeta_7)$*: For any prime* $q$ *other that 7, using Theorem 17,*

$$q^f \equiv 1 \pmod 7$$

*giving a way to calculate the inertial degree* $f$ *of* $q$*.*

- *Case 1:*
  $q \equiv 1 \pmod 7$*, we obtain* $f = 1$ *which implies a totally split prime.*
- *Case 2:*
  $q \equiv 3, 5 \pmod 7$*, we obtain* $f = 6$ *which implies an inert prime.*
- *Case 3:*
  $q \equiv 2, 4, 6 \pmod 7$*, we obtain* $f = 2, 3$ *which implies a non-totally split prime.*

*We list down some small primes based on their ramification.*

- *Inert primes: 3, 5, 17, 19, 31*
- *Split primes: 2, 11, 13, 23, 29, 37, 41*
- *Ramified primes: 7 (By Theorem 19 and Theorem 14)*

## 3.2 Ideal Lattices

With the tools from algebraic number theory and lattice theory from the previous chapter, we are ready to study the lattices obtained from algebraic number fields. We refer to those lattices as "algebraic lattices". We introduce the definition and properties of ideal lattices and provide some examples of such lattices. Finally we introduce ideal lattice codes that address the main problem of this thesis.

### 3.2.1 Definitions and Properties

To begin with, we introduce algebraic lattices using the following theorem.

**Theorem 20.** *[31] Let $\{\omega_1, \omega_2, ..., \omega_n\}$ be an integral basis of a number field $K$. Recall that $\sigma$ is the canonical embedding as defined in Definition 36. The $n$ vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, ..., n$ are linearly independent over $\mathbb{R}^n$, so they define a full rank lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.*

We express the lattice $\Lambda = \sigma(\mathcal{O}_K)$ using its generator matrix $M'$ as

$$\Lambda = \left\{ \mathbf{x} = M'\lambda \ \in \mathbb{R}^n \mid \lambda \in \mathbb{Z}^n \right\},$$

where $M'$ is given explicitly by

$$\begin{pmatrix} \sigma_1(w_1) & \dots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \Im\sigma_{r_1+1}(w_1) & \dots & \Re\sigma_{r_1+r_2}(w_1) & \Im\sigma_{r_1+r_2}(w_1) \\ \sigma_1(w_2) & \dots & \sigma_{r_1}(w_2) & \Re\sigma_{r_1+1}(w_2) & \Im\sigma_{r_1+1}(w_2) & \dots & \Re\sigma_{r_1+r_2}(w_2) & \Im\sigma_{r_1+r_2}(w_2) \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \sigma_1(w_n) & \dots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \Im\sigma_{r_1+1}(w_n) & \dots & \Re\sigma_{r_1+r_2}(w_n) & \Im\sigma_{r_1+r_2}(w_n). \end{pmatrix}^T$$

Thus a lattice point $\mathbf{x} \in \Lambda \subset \mathbb{R}^n$ is of the form

$$\begin{aligned} \mathbf{x} &= (x_1, x_2, ..., x_{r_1}, x_{r_1+1}, ..., x_{r_1+2r_2})^T \\ &= (\sum_{i=1}^{n} \lambda_i \sigma_1(w_i), ..., \sum_{i=1}^{n} \lambda_i \Re\sigma_{r_1+1}(w_i), ..., \sum_{i=1}^{n} \lambda_i \Im\sigma_{r_1+r_2}(w_i))^T \\ &= (\sigma_1(\sum_{i=1}^{n} \lambda_i w_i), ..., \Re\sigma_{r_1+1}(\sum_{i=1}^{n} \lambda_i w_i), ..., \Im\sigma_{r_1+r_2}(\sum_{i=1}^{n} \lambda_i w_i))^T \\ &= (\sigma_1(x), ..., \Re\sigma_{r_1+1}(x), ..., \Im\sigma_{r_1+r_2}(x))^T \\ &= \sigma(x)^T \end{aligned}$$

for some $\lambda_i \in \mathbb{Z}$ and $x = \sum_{i=1}^{n} \lambda_i \omega_i$ an algebraic integer. This establishes a correspondence between a vector $\mathbf{x} \in \mathbb{R}^n$ and an algebraic integer $x \in \mathcal{O}_K$.

Thanks to the existence of an integral basis of $K$, we can embed $\mathcal{O}_K$ into $\mathbb{R}^n$ and construct algebraic lattices. There are other subsets of $\mathcal{O}_K$ which also contain a $\mathbb{Z}$-integral basis of same rank as $\mathcal{O}_K$. They are the *ideals* of $\mathcal{O}_K$ which are described in the previous section.

**Theorem 21** ([31], p.115)**.** *For a given number field $K$, every ideal $\mathcal{I} \neq \{0\}$ of $\mathcal{O}_K$ has a $\mathbb{Z}-$basis $\{\mu_1, ..., \mu_m\}$ where $m$ is the degree of $K$.*

Instead of using the whole ring of integers to build algebraic lattices, we consider ideals of the ring of integers and use them to construct *ideal lattices*. In a sense, ideal lattices are generalized versions of algebraic lattices.

**Definition 40.** *Let $K$ be a CM–field. An ideal lattice is an integral lattice $\Lambda = (\mathfrak{I}, q_\alpha)$ formed by an $\mathcal{O}_K$-ideal $\mathfrak{I}$ and a positive definite symmetric bilinear form $q_\alpha$:*

$$q_\alpha : \mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}, \quad q_\alpha(x,y) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x \bar{y}), \quad \forall x, y \in \mathfrak{I}$$

*where $\alpha \in \mathcal{O}_K$ is totally positive (i.e., $\sigma_i(\alpha) > 0$ for all $i$) and $\bar{y}$ denotes the complex conjugation of $y$.*

- *(integral lattice): $q_\alpha(x,y) \in \mathbb{Z}, \ \forall x, y \in \mathfrak{I}$.*
- *(positive definite): $q_\alpha(x,x) > 0, \ \forall x \in \mathfrak{I} \setminus \{0\}$.*
- *(symmetric bilinear form): $q_\alpha(x,y) = q_\alpha(y,x), \ \forall x, y \in \mathfrak{I}$.*

*In particular, when $K$ is a totally real number field, we obtain an ideal lattice $\Lambda = (\mathfrak{I}, q_\alpha)$ by having $q_\alpha(x,y) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha xy), \ \forall x, y \in \mathfrak{I}$.*

**Remark 14.** *The element $\alpha$ has a "twisting" effect which is useful to obtain different types of lattices over the same ring of integers. In fact, $\alpha$ could be taken outside $\mathcal{O}_K$ under different conditions, but the case where $\alpha \in \mathcal{O}_K$ is enough for our purpose. By adjoining a twisting element $\alpha$ to the embeddings, the generalized version of a canonical embedding, called twisted canonical embedding $\sigma_\alpha : K \to \mathbb{R}^n$, is introduced, namely*

$$\sigma_\alpha(x)^T \ = \ (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}, ..., \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x))^T$$

*where $\alpha_i = \sigma_i(\alpha)$, $i = 1, 2, ..., r_1 + r_2$ and $(r_1, r_2)$ denotes the signature of $K$.*

If $\{\mu_1, \ldots, \mu_n\}$ is a $\mathbb{Z}$-basis of $\mathfrak{I}$, by applying the twisted canonical embedding, the generator matrix $M'$ of the corresponding ideal lattice $\Lambda_\mathfrak{I} = \{\mathbf{x} = M''\lambda | \lambda \in \mathbb{Z}^n\}$ is given by

$$M'' = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\mu_1) & \ldots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\mu_1) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\mu_1) & \ldots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\mu_1) \\ \sqrt{\alpha_1}\sigma_1(\mu_2) & \ldots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\mu_2) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\mu_2) & \ldots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\mu_2) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \sqrt{\alpha_1}\sigma_1(\mu_n) & \ldots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\mu_n) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\mu_n) & \ldots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\mu_n) \end{pmatrix}^T \tag{3.1}$$

where $\alpha_j = \sigma_j(\alpha)$, for $j = 1, 2, ..., r_1 + r_2$.

**Remark 15.** *One easily verifies that the Gram matrix $(M'')^T M''$ is given by*

$$\{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\, \mu_i \mu_j)\}_{i,j=1}^n.$$

*Also notice that $M'$ as obtained earlier on is a particular case of $M''$ by taking $\alpha = 1$ and $\mathfrak{I} = \mathcal{O}_K$.*

**Theorem 22.** *[1] The volume* $\mathrm{vol}(\Lambda_{\mathfrak{I}})$ *of the lattice* $\Lambda_{\mathfrak{I}} = (\mathfrak{I}, q_\alpha)$ *is*

$$\mathrm{vol}(\Lambda_{\mathfrak{I}}) = \det(\Lambda_{\mathfrak{I}})^{1/2} = \det(\{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\,\omega_i\omega_j)\}_{i,j=1}^{n})^{1/2} = (N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\mathfrak{I})^2|d_K|)^{1/2}$$

*where* $d_K$ *is the discriminant of* $K$*.*

**Remark 16.** *It is worth to recall that the discriminant is related to the ramification. Thus the above theorem indicates that the volume* $\mathrm{vol}(\Lambda_{\mathfrak{I}})$ *of the lattice* $\Lambda_{\mathfrak{I}}$ *in turn depends on the ramification.*

**Theorem 23.** *[30] Let* $d_K$ *be the discriminant of* $K$*, let* $\mathcal{O}_K$ *be the ring of integers of* $K$*, and let* $\mathfrak{I}$ *be a non-zero integral ideal of* $\mathcal{O}_K$*. Then* $\sigma(\mathcal{O}_K)$ *and* $\sigma(\mathfrak{I})$ *are lattices. Moreover,*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|d_K|} \text{ and } \mathrm{vol}(\Lambda_{\mathfrak{I}}) = 2^{-r_2}\sqrt{|d_K|}N_{K/\mathbb{Q}}(\mathfrak{I})$$

*where* $r_2$ *is the number of pairs of complex conjugate embeddings with image in* $\mathbb{C}$*.*

The ramification in a given number field thus influences the possible volumes that a lattice over this number field can take, which then gives a necessary condition for the existence of a lattice , as illustrated in the following examples, to find the $\mathbb{Z}^n$ lattice.

### 3.2.2 Some Examples of Ideal Lattices

For $K = \mathbb{Q}(\sqrt{5})$ of degree 2, its ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Let $\sigma_1, \sigma_2$ be the two real embeddings which are the identity and the conjugation mappings respectively of $K$. We will assume $\mathfrak{I} = \mathcal{O}_K$. Furthermore, we have $d_K = 5$ and obtain the necessary condition

$$N(\alpha) \cdot 5 = c^2$$

where $c$ is an integer for obtaining the $\mathbb{Z}^2$ lattice. Notice that the Gram matrix $G$ is the identity matrix for $\mathbb{Z}^2$.

To look for a suitable $\alpha \in K$ whose norm is 5, we look at the prime $\mathfrak{p}$ above 5 and take

$$\alpha = 3 - \frac{1+\sqrt{5}}{2} \in \mathfrak{p}.$$

To verify its norm, $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (3 - \frac{1+\sqrt{5}}{2})(3 - \frac{1-\sqrt{5}}{2}) = 5$.

By taking $\mathfrak{I} = \mathcal{O}_K$, $\alpha = 3 - \frac{1+\sqrt{5}}{2}$ and by applying the twisted canonical embedding, the lattice generator matrix $M$ is given by

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\frac{1+\sqrt{5}}{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}^T.$$

Next we compute the Gram matrix $G = M^T M$ as follows,

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) \\ \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})^2) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})^2) \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

By normalization, we obtain the $\mathbb{Z}^2$ ideal lattice built over $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ with lattice generator matrix $\frac{1}{\sqrt{5}}M$.

**Remark 17.** *In general, although we have a necessary condition from Theorem 22 for obtaining $\mathbb{Z}^2$ lattices, that is $N(\alpha)N(\mathfrak{I})^2|d_K| = c^2$, it is not sufficient to guarantee that the lattices obtained are equivalent to a scaled version of $\mathbb{Z}^2$ lattices.*

Now we consider the construction of ideal lattices on $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ which is of degree $\frac{p-1}{2}$ over $\mathbb{Q}$. We have $\mathfrak{I} = \mathcal{O}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ (Theorem 16) and $d_K = p^{\frac{p-3}{2}}$ (Theorem 18).

Before we illustrate the construction, we have the following lemmas.

To obtain the $\mathbb{Z}^n$ ideal lattices, we will find a suitable $\alpha$ based on the necessary condition derived from Theorem 23 namely

$$N(\mathfrak{I})N(\alpha)|d_K| = N(\alpha)p^{\frac{p-3}{2}} = p^{\frac{p-1}{2}}.$$

Observe that $N(\alpha)$ has to be $p$. In order to find $N(\alpha)$ of norm $p$, we will make use of the following lemmas and the transitivity of norm from Theorem 10.

**Lemma 2.** *The $p^r$th cyclotomic polynomial of $\mathbb{Q}(\zeta_{p^r})$ denoted by $\Psi_{p^r}(X)$ equals to $t^{p-1} + t^{p-2} + ... + t^2 + t + 1$ where $t = X^{p^{r-1}}$.*

*Proof.* Proof by induction and using the fact that $X^n - 1 = \prod_{d|n} \Psi_d(X)$. Applying Eisenstein's criterion to verify its irreducibility.

□

**Lemma 3.** *For any prime power $p^r$, $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1 - \zeta_{p^r}) = p$.*

*Proof.* First, let $p(X) = \Psi_{p^r}(X)$, thus $p(1) = p$. The Galois conjugates of $\zeta_{p^r}$ over $\mathbb{Q}$ are exactly the powers of $\zeta_{p^r}^k$ as $k$ runs through $(\mathbb{Z}/p^r\mathbb{Z})^*$. On the other hand, $p(X)$ can be expressed as $\prod_k (X - \zeta_{p^r}^k)$. Hence, $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1 - \zeta_{p^r}) = \prod_k (1 - \zeta_{p^r}^k) = p(1) = p$. □

Since we consider $r = 1$, we notice that $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p^k) = p$ for $k = 1, ..., p-1$ and further compute that $N_{\mathbb{Q}(\zeta_p + \zeta_{p^{-1}})/\mathbb{Q}}(1 - \zeta_p^k) = (1 - \zeta_p^k)(1 - \zeta_{p^{-1}}^k)$.

**Proposition 2.** *[25] Consider $\alpha = (1 - \zeta_p)(1 - \zeta_p^{-1})$ and $x, y \in \mathcal{O}_K$,*

$$\Lambda = (\mathcal{O}_K, \frac{1}{p}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x y)) \text{ is equivalent to } \mathbb{Z}^{\frac{p-1}{2}}.$$

*Proof.* Using the trace from Definition 31 and taking $\sigma_l(e_k) = \zeta_p^{lk} + \zeta_p^{-lk}$ as embeddings of $K$ into $\mathbb{C}$, compute $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i e_j)$ where $\{e_k = \zeta_p^k + \zeta_p^{-k}\}_{k=1}^{\frac{p-1}{2}}$. The Gram matrix obtained is the Gram matrix of the lattice $\mathbb{Z}^{\frac{p-1}{2}}$ after taking the new basis $\{e'_1, ..., e'_{\frac{p-1}{2}}\}$, where $e'_{\frac{p-1}{2}} = e_{\frac{p-1}{2}}$ and $e'_k = e_k + e'_{k+1}$, $k = 1, 2, ..., \frac{p-3}{2}$.[25] □

### 3.2.3 Ideal Lattice Codes

In the previous chapter, we introduced the transmission of wiretap lattice codes over fading channels and summarized their code design criterion. Now we want to refine the code design criterion when ideal lattices codes are used, both in terms of reliability and secure transmission. Let us start with reliability. Recall from [3], [25] that the main code design criterion for reliability is to maximize the diversity of the lattice, which is to obtain low error probability for Bob.

Using the generator matrix $M''$ of the lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ from (3.1), a lattice point $\mathbf{x}$ from an ideal lattice is of the form

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}, ..., \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x))^T$$

where $x = \sum_{i=1}^{n} \lambda_i \mu_i$ and $\lambda_i \in \mathbb{Z}$.

**Remark 18.** *Recall that there is an injective map between a lattice point $\mathbf{x} \in \Lambda = (\mathcal{I}, q_\alpha) \subseteq \mathbb{R}^n$ and an algebraic integer $x = \sum_{i=1}^{n} \lambda_i \mu_i \in \mathcal{I} \subseteq \mathcal{O}_K$, $\lambda_i \in \mathbb{Z}$, where $\{\mu_1, \ldots, \mu_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{I}$.*

**Lemma 4.** *If $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{R}^n$ is a non-zero vector from ideal lattices constructed over $\mathcal{O}_K$, then all its components are non-zero as well.*

*Proof.* If $x_j = \sqrt{\alpha_j}\sigma_j(\sum_{i=1}^{n}\lambda_i\mu_i) = 0$ for some $j$, then $\sum_{i=1}^{n}\lambda_i\mu_i = 0$ since $\sqrt{\alpha_j} > 0$. This further implies that every $x_i$ must be zero since $\sigma_j$ is ring homomorphism. This contradicts the assumption that $\mathbf{x}$ is a non-zero vector. □

**Theorem 24.** *[3] Ideal lattices exhibit a diversity*

$$L = r_1 + r_2.$$

**Corollary 8.** *Ideal lattices built over totally real number fields (that is with signature $(r_1, r_2) = (n, 0)$) have maximal diversity $L = n$.*

**Remark 19.** *Corollary 8 shows that ideal lattices constructed over totally real number fields give full diversity lattices, the first design criterion for reliable transmission.*

Next we consider the code design for confidentiality. The code design for confidentiality over fast fading channels as described in the previous chapter, when choosing $\Lambda_b$ and $\Lambda_e \subset \Lambda_b$ to be ideal lattices from a totally real number field $K$ of degree $n$, becomes

$$\begin{aligned}\sum_{\mathbf{x}\in\Lambda_e\cap\mathcal{R},\mathbf{x}\neq 0}\prod_{x_i\neq 0}\frac{1}{|x_i|^3} &= \sum_{x\in\mathcal{I}\cap\mathcal{R}',x\neq 0}\prod_{i=1}^{n}\frac{1}{(\sqrt{\alpha_i}|\sigma_i(x)|)^3} \\ &= \sum_{x\in\mathcal{I}\cap\mathcal{R}',x\neq 0}\frac{1}{(\sqrt{N_{K/\mathbb{Q}}(\alpha)}|N_{K/\mathbb{Q}}(x)|)^3} \qquad (3.2)\end{aligned}$$

since $\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^{n}\lambda_i\mu_i \in \mathcal{I}$, and $\mathcal{R}'$ is some subset of $\mathcal{I}$ corresponding to $\mathcal{R}$. In this thesis, we will further consider the case where $K$ is a Galois extension, and $\mathcal{I}$ is a principal, to start with (in whole generality, a Galois extension is not needed to build an ideal lattice, and the ideal does not have to be principal). In that case, $x \in \mathcal{I} = (\beta)\mathcal{O}_K$, $N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(x')$ for some $x' \in \mathcal{O}_K$, and we see from (3.2) that the sum which becomes of interest is

$$\sum_{x\in\mathcal{O}_K\cap\mathcal{B},x\neq 0}\frac{1}{|N_{K/\mathbb{Q}}(x)|^3}. \qquad (3.3)$$

We write $\mathcal{B}$ to emphasize that we are interested in finite sums, ideally $\mathcal{B}$ should be computed as a function of $\mathcal{R}$, though that may not always be easy to do.

It is worth repeating that since $\Lambda_e$ is a sublattice of $\Lambda_b$, both lattices will be obtained as ideal lattices over $\mathcal{O}_K$. This is consistent with the design of $\Lambda_b$, since this lattice will also benefit of the full diversity property coming from choosing $K$ totally real, and full

diversity is indeed the design criterion for reliability over fast Rayleigh fading channels as explained above.

**Remark 20.** *It is important to keep in mind that we are comparing two coding strategies via (3.3), and for such a comparison to make sense, lattices $\Lambda_e$ of same volume should be compared. In particular, choosing an ideal of big norm is not a valid strategy, since it essentially inflates the volume of the lattice considered.*

In summary, we refine the code design criterion for fading channels using ideal lattices and translate it into a sum of inverse of algebraic norms in number fields as the following.

For fast fading channels, we want to minimize

$$\sum_{x \in \mathcal{O}_K \cap \mathcal{B}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$$

where $\mathcal{B}$ denotes finite constellations.

For block fading channels, we want to minimize

$$\sum_{\mathbf{x} \in \mathcal{O}_K^N \cap \mathcal{B}, \mathbf{x} \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(\|\mathbf{x}\|)|^{N+2}} \tag{3.4}$$

where $\mathbf{x} = (x_1, ..., x_N),\ x_i \in \mathcal{O}_K$.

**Remark 21.** *We will focus on the case of fast fading channels, which is analysed in next chapter. We will not study the case of block fading channels in term of minimization of* (3.4)*, however coset encoding for block fading channels is discussed in Section 5.4.*

# Chapter 4

# Ideal Lattice Codes for Fast Fading Wiretap Channel

Recall from the previous chapter that the code design criterion for wiretap ideal lattice codes is the minimization of the following finite sum of inverse of algebraic norms,

$$\sum_{x \in \mathcal{O}_K \cap \mathcal{B}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3} \tag{4.1}$$

where $K$ and $\mathcal{O}_K$ denote a number field and its ring of integers respectively. Note that the finite region $\mathcal{B}$ ensures that the sum is finite. The minimization of similar sums have been looked at in the context of the Diversity Multiplexing Trade-Offs (DMT) [32].

In this chapter, we focus on the design of ideal lattices codes over totally real number fields for fast fading channels by identifying the number field parameters that minimize the sum in (4.1).

From the sum in (4.1), we can observe that the dominant terms are the units of $K$ (which have norm $\pm 1$) and algebraic integers with small norms. The density of units of a number field $K$ is described by the *regulator* of $K$ whereas those algebraic integers with the absolute value of norm at least 2 will depend on the ramification in the number field $K$ and as well the density of units since those associates of algebraic integers share the same norm by Corollary 6. One code design criterion for reliable transmission is to consider number fields with small discriminants. As most number fields with small discriminants have class number one, we restrict our study to number fields with class number one. Note that the correlation between small discriminants and class number

one is deduced from the class number formula. This explains why we only consider the case of class number of $K$, $h_K = 1$.

We begin with the effect of algebraic integers with small nonunit norms which is described by the ramification in Section 4.1. Then we focus on the units and *regulator* in Section 4.2 and analyse the effect of a regulator on the sum (4.1) which is to be minimized over different number fields. Finally we present numerical results from the analysis of the previous sections in Section 4.3.

## 4.1 Small Norms

To analyse the effect of the ramification of prime numbers, we start with the following example.

**Example 14.** *Consider the following two totally real number fields, $K_1$ and $K_2$,*

1. *Number field $K_1$,*
   (a) *$K_1 = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, where $\zeta_{16}$ is a primitive 16th root of unity.*
   (b) *$[K_1 : \mathbb{Q}] = \varphi(16)/2 = 4$.*
   (c) *The ring of integers $\mathcal{O}_{K_1} = \mathbb{Z}[\zeta_{16} + \zeta_{16}^{-1}]$.*
   (d) *The discriminant, $d_{K_1} = 2048$.*
   (e) *It contains elements of norm 2 (in particular $(1 - \zeta_{16})(1 - \zeta_{16}^{-1})$ has norm 2). We take as an integral basis $\nu_i = (\zeta_{16} + \zeta_{16}^{-1})^i,\ i = 0, 1, 2, 3$ and $\mathcal{B}(b) = \{\sum_{i=0}^{3} a_i \nu_i,\ a_i \in [-b, \ldots, b]\}$.*
2. *Number field $K_2$ with the minimal polynomial $X^4 - X^3 - 5X^2 + 2X + 4$,*
   (a) *$[K_2 : \mathbb{Q}] = 4$.*
   (b) *The discriminant $d_{K_2} = 2225$.*
   (c) *We take as integral basis (computed numerically) $\mu_i = \theta^i,\ i = 0, 1, 2$ and $\mu_3 = (\theta + \theta^2 + \theta^3)/2$, with $\mathcal{B}(b) = \{\sum_{i=0}^{3} a_i \mu_i,\ a_i \in [-b, \ldots, b]\}$.*

*Elements of small norms as well as (3.3) for different choices of $\mathcal{B}(b)$ are computed numerically using Sage and shown in Table 4.1. We observe that $K_2$ gives smaller sums for the three choices of b, despite having a larger number of units every time ($[1, x]$ refers to $x$ elements having a norm whose absolute value is 1). This illustrates the weight of the elements with the absolute value of norm 2 in the sum, and the fact*

**Table 4.1:** The sum (3.3) is computed for $K_1$ (in the 2nd column) and $K_2$ (in the 3rd column) for different values of $b$ (in the 1st column). We observe that $K_2$ gives smaller sums, despite a higher number of units (in the 4rth and 5th columns, $[x, y]$ refers to the number of elements $y$ with norm in absolute value equal to $x$).

| $b$ | $K_1$ | $K_2$ | small norms in $K_1$ | small norms in $K_2$ |
|---|---|---|---|---|
| $b = 4$ | 133.00 | 130.43 | [1,120],[2,92],[4,84] | [1,128],[4,152] |
| $b = 8$ | 281.71 | 269.68 | [1,252],[2,212],[4,178] | [1,264],[4,354] |
| $b = 15$ | 491.07 | 479.09 | [1,438],[2,378],[4,320] | [1,468],[4,690] |

*that they may not be neglected. Furthermore, elements of norm up to 4 are enough here to describe the behavior of the sums. For instance, for $K_1$ and $b = 4$ (but this is true for every case)*

$$120 + \frac{92}{2^3} + \frac{84}{4^3} = 120 + 11.5 + 1.3125 = 132.8125 \simeq 133.$$

*These two fields were chosen for a fair comparison, since they are both totally real, have the same degree, and discriminants close to each other. To make things even more complicated, the above computations are sensible to a choice of integral basis. For example, for $K_2$, another integral basis is $\{1, (\theta + \theta^2 + \theta^3)/2, \theta^2, \theta^3\}$, which yields as small norms [1,96],[4,120] and sum 97.90 for $b = 4$, [1,226], [4,290] and sum 230.61 for $b = 8$ and [1,414],[4,566] with sum 422.99 for $b = 15$.*

This example illustrates the role that elements of smaller nonunit norms may play in understanding (3.3). With the help of ramification theory of number fields, the approach that we will thus adopt is to analyse the behaviour of norms and further to identify number fields with no element of smaller norms.

Let $p$ be a rational prime, then clearly $p$ belongs to the principal ideal $p\mathcal{O}_K$, and by considering the prime factorization of $p\mathcal{O}_K$, we have

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals. If $K$ is Galois, recall that $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^e$, that is $e_i = e$ for all $i$.

In particular, if $p$ is totally ramified ($g = 1$ and $e_1 = n$) or if $p$ totally splits ($g = n$ and all the ramification indices are 1), then

$$N(\mathfrak{p})^n = p^n, \text{ or } \prod_{i=1}^{n} N(\mathfrak{p}_i) = p^n$$

shows the existence of an ideal above $p$ of norm $p$. If this ideal is principal, then the generators will have norm $p$. This argument shows how to find elements of norm $p$. On the other hand, when $e = g = 1$ (such a prime $p$ is called an inert prime), this will force the smallest norm involving only the prime $p$ to be at least $p^n$. Indeed, suppose that there exists an element $x \in \mathcal{O}_K$ whose norm is $p^j$ for some positive $j$. Then $N(x\mathcal{O}_K) = |N_{K/\mathbb{Q}}(x)| = p^j$ and by definition $|\mathcal{O}_K/x\mathcal{O}_K| = p^j$, which shows that $p^j \subset x\mathcal{O}_K$, thus $p^j\mathcal{O}_K \subset x\mathcal{O}_K$ and $x\mathcal{O}_K | p^j\mathcal{O}_K$. Since $p\mathcal{O}_K$ is prime ($e = g = 1$), it must be that $x\mathcal{O}_K = p^{j'}\mathcal{O}_K$ for some $j' \leq j$, and $N(x\mathcal{O}_K) = N(p\mathcal{O}_K)^{j'} = p^{nj'}$, showing that $j \geq n$.

### 4.1.1 Maximal Real Subfields of Cyclotomic Fields

Let $\zeta_p$ denote a primitive $p$th root of unity, and consider the cyclotomic field $\mathbb{Q}(\zeta_p)$. Recall from Chapter 3, it has degree $p-1$ over $\mathbb{Q}$, and its maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ has degree $(p-1)/2$ over $\mathbb{Q}$. They have respective rings of integers $\mathbb{Z}[\zeta_p]$ and $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. The ramification in $\mathbb{Q}(\zeta_p)$ is well understood from the theorem 17.

Since we will be looking at subfields of $\mathbb{Q}(\zeta_p)$, it is useful to remember that the ramification and the residual index satisfy transitivity, namely

$$e(\mathfrak{q}_L/q) = e(\mathfrak{q}_L/\mathfrak{q}_K)e(\mathfrak{q}_K/q),\ f(\mathfrak{q}_L/q) = f(\mathfrak{q}_L/\mathfrak{q}_K)f(\mathfrak{q}_K/q), \tag{4.2}$$

for the tower $L/K/\mathbb{Q}$ and $\mathfrak{q}_L$ a prime above $\mathfrak{q}_K$, and $\mathfrak{q}_K$ a prime above $q$.

Consider the special case when $p = 2p' + 1$, with $p'$ a prime. It is then easy to make sure that small primes stay inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

**Lemma 5.** *[26] Suppose that $p = 2p' + 1$, where both $p$ and $p'$ are prime (such a prime $p'$ is called a Sophie Germain prime). Then the primes smaller than $p$ are inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

*Proof.* Let $q$ be a prime smaller than $p$. By forcing $p = 2p' + 1$ with $p'$ prime, the degree of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is now $p'$ over $\mathbb{Q}$. Since

$$p' = e(\mathfrak{q}_i/q)f(\mathfrak{q}_i/q)g(\mathfrak{q}_i/q)$$

for every prime $\mathfrak{q}_i$ above $q$ and $e(\mathfrak{q}_i/q) = 1$ when $q$ is distinct from $p$ (if $e(\mathfrak{q}_i/q) > 1$, then by transitivity (4.2) $q$ should ramify in $\mathbb{Q}(\zeta_p)$), we deduce that either (1) $f(\mathfrak{q}_i/q) = 1$ and $g(\mathfrak{q}_i/q) = p'$, or (2) $f(\mathfrak{q}_i/q) = p'$ and $g(\mathfrak{q}_i/q) = 1$. Suppose $f(\mathfrak{q}_i/q) = 1$ and

$g(\mathfrak{q}_i/q) = p'$, by applying the transitivity of the residual index in $\mathbb{Q}(\zeta_p)$ and Theorem 17, either $q \equiv 1 \pmod{p}$, or $q^2 \equiv 1 \pmod{p}$.

The former case cannot happen if $q$ is smaller than $p$.

The latter case is also impossible. Here are two reasons why this is the case. Firstly: $q^2 \equiv 1 \pmod{p}$ means that $q$ is an element of order 2. But in the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, generated by some element $a$, the elements of order 2 are of the form $a^k$ with $(p-1)/\gcd(p-1,k) = 2$, that is $2p'/\gcd(2p',k) = 2$, implying that $k$ must be an odd multiple of $p'$, that is $k = p'$. Now this element of order 2 has to be $a^{p'} = p-1$, since $(p-1)^2 \equiv 1 \pmod{p}$. Alternatively: $q^2 \equiv 1 \pmod{p}$ is equivalent to $(q-1)(q+1) = 0 \pmod{p}$, that is $p$ divides $(q-1)$ or $(q+1)$. But $q < p$ so $p$ cannot divide $(q-1)$, and $p$ cannot divide $q+1$ either, since $p-1$ is even.

This shows that $f(\mathfrak{q}_i/q) = p'$ and $q$ is inert. □

**Example 15.** *Consider $\mathbb{Q}(\zeta_{23})$, with $23 = 2 \cdot 11 + 1$. The primes 2, 3, 5, 7, 11, 13, 17, 19 are all inert in $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$.*

We could extend this technique to consider a totally real subfield $K$ of $\mathbb{Q}(\zeta_p)$ of degree $[K : \mathbb{Q}] = p'$, when $p = mp' + 1$. Indeed, the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, that is, it is a cyclic group of order $p-1 = mp'$. Let us denote by $\sigma$ its generator. Then $\sigma^{p'}$ generates a subgroup of order $m$, to which corresponds a subfield $K = \mathbb{Q}(\zeta_p)^{\langle\sigma^{p'}\rangle}$ which is fixed by $\langle\sigma^{p'}\rangle$, which is of degree $p'$ over $\mathbb{Q}$. Since $p'$ is prime, the same argument as in the proof of Lemma 5 shows that if $q$ is a prime different from $p$, then $q$ cannot ramify. Either it is inert, or it splits totally.

**Example 16.** *Consider $\mathbb{Q}(\zeta_{67})$, with $67 = 6 \cdot 11 + 1$. Let $\sigma$ be the generator of the Galois group of $\mathbb{Q}(\zeta_{67})/\mathbb{Q}$. The subgroup $\langle\sigma^{11}\rangle$ has order 6, with corresponding fixed field $K$, which is totally real and of degree 11 over $\mathbb{Q}$. Its minimal polynomial is $X^{11} - X^{10} - 30X^9 + 63X^8 + 220X^7 - 698X^6 - 101X^5 + 1960X^4 - 1758X^3 + 35X^2 + 243X + 29$. Since*

$$11 = f(\mathfrak{q}_i/q)g(\mathfrak{q}_i/q)$$

*we have that $f(\mathfrak{q}_i/q)$ is either 1 or 11. Let us assume that this is 1. Using the transitivity formula (4.2)*

$$f(\mathfrak{q}_L/q) = f(\mathfrak{q}_L/\mathfrak{q}_i)$$

*thus $f(\mathfrak{q}_L/q)$ is either 1, 2, 3, or 6, with $L = \mathbb{Q}(\zeta_{67})$. A direct computation using Theorem 17 shows that 2, 7, 11, 13, 17, 19 and 23 are inert. On the other hand, $29^3 \equiv 1 \pmod{67}$.*

**Figure 4.1:** The cyclotomic field $\mathbb{Q}(\zeta_p)$ with $p$ prime and its subfield of degree $(p-1)/f$ for $f$ a divisor of $p-1$.

$$\begin{array}{rl} L = \mathbb{Q}(\zeta_p) & \supset \mathfrak{q}_{K,1}\mathcal{O}_L = \mathfrak{q}_{L,1}\cdots\mathfrak{q}_{L,s} \\ {\scriptstyle f}\Big| {\scriptstyle G_f} & \\ K = \mathbb{Q}(\zeta_p)^{\langle\sigma^f\rangle} & \supset q\mathcal{O}_K = \mathfrak{q}_{K,1}\cdots\mathfrak{q}_{K,r} \\ {\scriptstyle e=(p-1)/f}\Big| {\scriptstyle G/G_f} & \\ \mathbb{Q} & \end{array}$$

**Remark 22.** *Note that number fields considered in both Examples 15 and 16 are comparable since they have the same dimension over* $\mathbb{Q}$.

### 4.1.2 Other Totally Real Subfields of Cyclotomic Fields

We next consider more generally totally real subfields of $\mathbb{Q}(\zeta_p)$, with $p$ a prime. As recalled earlier, the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, that is, it is a cyclic group of order $p-1$. Let us denote by $\sigma$ its generator. If $f|p-1$, set $e=(p-1)/f$. Then $\sigma^f$ generates a subgroup of order $f$, that we denote by $G_f$, to which corresponds a subfield $K=\mathbb{Q}(\zeta_p)^{\langle\sigma^f\rangle}$ which is fixed by $G_f=\langle\sigma^{p'}\rangle$, which is of degree $e$ over $\mathbb{Q}$ (see Figure 4.1). The Galois group of $K/\mathbb{Q}$ is the quotient group $G/G_f$. Let $q\in\mathbb{Z}$ be a prime, $q\neq p$, and let $\mathfrak{q}_K\in\mathcal{O}_K$ be a prime lying over $q$, and $\mathfrak{q}_L\in\mathcal{O}_L$ be a prime lying over $\mathfrak{q}_K$. The decomposition groups $D_{\mathfrak{q}_K}$ of $\mathfrak{q}_K$ and $D_{\mathfrak{q}_L}$ of $\mathfrak{q}_L$ are respectively, by definition, the groups

$$D_{\mathfrak{q}_L}=\{\sigma\in G,\ \sigma(\mathfrak{q}_L)=\mathfrak{q}_L\},\ D_{\mathfrak{q}_K}=\{\tau\in G/G_f,\ \tau(\mathfrak{q}_K)=\mathfrak{q}_K\}.$$

Using the orbit-stabilizer theorem and since the Galois Group acts transitively on its set of prime ideals,

$$g(\mathfrak{q}_K/q)=[G/G_f:D_{\mathfrak{q}_K}]=r,\ g(\mathfrak{q}_L/q)=[G:D_{\mathfrak{q}_L}]=s$$

giving us a way to determine whether $r=1$ (that is $q$ is inert in $K$) using decomposition groups. Now let $\mathbb{Q}(\zeta_p)^{D_{\mathfrak{q}_L}}=L^{D_{\mathfrak{q}_L}}$ be the subfield of $L$ fixed by $D_{\mathfrak{q}_L}$. Since $q$ cannot ramify in $L$, $e(\mathfrak{q}_L/q)=1$ and

$$p-1=f(\mathfrak{q}_L/q)g(\mathfrak{q}_L/q)=[L:L^{D_{\mathfrak{q}_L}}][L^{D_{\mathfrak{q}_L}}:\mathbb{Q}]=|D_{\mathfrak{q}_L}||G/D_{\mathfrak{q}_L}|$$

showing that $|D_{\mathfrak{q}_L}| = f(\mathfrak{q}_L/q)$, that is, $D(\mathfrak{q}_L)$ is a subgroup of the cyclic group $G = \langle\sigma\rangle$ of order $f(\mathfrak{q}_L/q)$, which is the order of $q \pmod p$ (by Theorem 17). We are then left to compute $g(\mathfrak{q}_K/q) = [G/G_f : D_{\mathfrak{q}_K}] = r$, that is the index of the subgroup generated by the image of $q$ in $G/G_f$, which can be computed to be $(p-1)/\mathrm{lcm}(f, f(\mathfrak{q}_L/q))$. In summary:

**Proposition 3.** *[27] Let $K$ be a subfield of $\mathbb{Q}(\zeta_p)$ for $p$ a prime, and let $q \neq p$ be a prime. Suppose that $[K : \mathbb{Q}] = (p-1)/f$, for $f$ some divisor of $p-1$. If the least common multiple of $f$ and of the order of $q \pmod p$ is $p-1$, then $q$ is inert in $K$.*

Since we are interested in comparing different number fields, we will start by looking at fields of degree 5. For that, we will apply this proposition on subfields of the cyclotomic fields $\mathbb{Q}(\zeta_p)$ with $p = 2m+1$ and $5|m$. Indeed, in this case, its maximal real subfield has degree $m$, and we will find a suitable subfield. This gives us $p \in \{11, 31, 41, 61, 71\}$.

**Example 17.** *The prime 3 splits in $\mathbb{Q}(\zeta_{41})$ since $f = 8$ and the order of 3 (mod 41) is 8, thus $g(\mathfrak{q}_K/3) = 5$.*

**Example 18.** *The prime 2 is inert in $\mathbb{Q}(\zeta_{31})$ since $f = 6$ and the order of 2 (mod 31) is 5, thus $(p-1)/\mathrm{lcm}(6,5) = 1$. Similary, 3 is inert, since the order of 3 mod 31 is 30. On the other hand, 5 splits, since the order of 5 (mod 31) is 3 and $g(\mathfrak{q}_K/5) = 30/\mathrm{lcm}(3,6) = 5$.*

Similar computations show that 11 and 23 are the smallest primes which are not inert in $\mathbb{Q}(\zeta_{61})$ and $\mathbb{Q}(\zeta_{71})$ respectively.

Among those totally real fields with inert small primes, we now look at those with small number of units as considered next.

## 4.2 Units

As mentioned, the units are dominant terms for the sum (4.1). In order to understand the density of units, we will introduce the *regulator* of number field $K$ as described in the following.

Let $K$ be a number field of degree $d$ and signature $(r_1, r_2)$. Set $r = r_1 + r_2 - 1$. Let $w$ be the number of roots of unity in $K$.

**Table 4.2:** Some totally real number fields $K$ with their small primes and regulator. The first column describes $K$ as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, the second column is the regulator $R$, the third column is the minimal polynomial of $K$, and the fourth column gives the first small prime which is not inert.

| $K \subset \mathbb{Q}(\zeta_p)$ | $R$ | $p(X)$ | primes |
|---|---|---|---|
| $\mathbb{Q}(\zeta_{11})$ | 1.63 | $X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$ | 11 ramifies |
| $\mathbb{Q}(\zeta_{31})$ | 30.37 | $X^5 - 9X^4 + 20X^3 - 5X^2 - 11X - 1$ | 5 splits |
| $\mathbb{Q}(\zeta_{61})$ | 93.768 | $X^5 + X^4 - 24X^3 - 17X^2 + 41X - 13$ | 11 splits |
| $\mathbb{Q}(\zeta_{71})$ | 70.611 | $X^5 + X^4 - 28X^3 + 37X^2 + 25X + 1$ | 23 splits |
| $\mathbb{Q}(\zeta_{23})$ | 1014.31 | $X^{11} + X^{10} - 10X^9 - 9X^8 + 36X^7 + 28X^6$ | |
| | | $-56X^5 - 35X^4 + 35X^3 + 15X^2 - 6X - 1$ | 23 ramifies |
| $\mathbb{Q}(\zeta_{67})$ | 330512.24 | $X^{11} - X^{10} - 30X^9 + 63X^8 + 220X^7 - 698X^6$ | |
| | | $-101X^5 + 1960X^4 - 1758X^3 + 35X^2 + 243X + 29$ | 29 splits |

**Definition 41.** *[4] Let $\{e_1, \ldots, e_r\}$ be a basis for the group of units modulo the group of roots of unity. The regulator of $K$ is*

$$R = |\det(\log|\sigma_i(e_j)|)_{1\leq i,j\leq r}|,$$

*where $|\sigma_i(e_j)|$ denotes the absolute value for the real embeddings, and the square of the complex absolute value for the complex ones.*

To associate the regulator and the number of units, the best known bound on the number of units is given in the following.

**Theorem 25.** *[8] The number of units $U(q)$ such that $\max_{1\leq i\leq d}|\sigma_i(u)| < q$ in $K$ is given by*

$$U(q) = \frac{w(r+1)^r}{Rr!}(\log q)^r + O((\log q)^{r-1-(cR^{2/r})^{-1}})$$

*as $q \to \infty$ and $c = 6 \cdot 2 \cdot 10^{12} d^{10}(1 + 2\log d)$.*

We might use this result on $U(q)$ to evaluate the amount of units in the region $\mathcal{B}$ of interest, that is of elements of norm 1 in (3.3), since one can always take the maximum of $\max_{1\leq i\leq d}|\sigma_i(u)|$ over every unit in $\mathcal{B}$ to define $q$. Since we focus on totally real number fields, $w = 2$ (the only roots of unity are $\pm 1$), $r_2 = 0$ and $r_1 = d$, so that $r = d - 1$. Thus the regulator is the only factor that distinguishes two totally real numbers of same degree.

However, we note that the results on regulators of number fields are not easily found. To have a sense of the range to which regulators belong, we compute numerically

regulators corresponding to totally real number fields identified earlier as having all their small primes inert (we discard $\mathbb{Q}(\zeta_{41})$, see Example 17). Note that the numerical computations are not obvious either, since they require units computations, which are lengthy, when the degree of the number fields increases. Examples of number fields can be found in Table 4.2, where we recall the smallest prime which is not inert, as computed in the previous section. We observe that maximal real subfields have very small regulators. Note that all number fields of degree 5 and 11 in Table 4.2 are totally real by Lemma 1 and their signatures of number fields.

The case of degree 5 shows that the choice of the regulator is making a huge difference, since the dominant term for $U(q)$ is

$$\frac{2 \cdot 5^4}{4!R}(\log q)^4 = \frac{625}{12R}(\log q)^4$$

yielding respectively

$$\sim 0.4(\log q)^4, \ \sim 32(\log q)^4$$

for the smallest (1.63 for $\mathbb{Q}(\zeta_{11})$) and biggest (93.768 for $\mathbb{Q}(\zeta_{61})$) regulators shown in Table 4.2.

Theorem 25 is an asymptotic result, holding for a region defined by $q$, when $q$ grows to infinity. In our scenario, we are on the contrary interested in small regions, corresponding to the signal constellation transmitted. In order to get a sense of how valid it is to use this bound to evaluate the density of units in the regions considered, we computed (3.3) for $\mathcal{B}(6)$ for the number fields of degree 5 of Table 4.2. We observe that the regulator predicts very well which number field is giving the smallest sum: when the regulator increases, the sum decreases. The difference between the smallest and biggest sum is also huge (roughly of a factor of 30), though not as huge as predicted (roughly of a factor of 80). Other experiments with other integral bases gave variations of the above results, but with the same overall behavior. Since the discriminants of the number fields considered are needed to normalize two lattices to have the same volume, the discriminants are also indicated in Table 4.3.

**Remark 23.** *Elements of small norms have the biggest contributions to these sums. We first narrow down our study to number fields where small primes are inert, to prevent the existence of elements of small norms. This is motivated by examples of fields where elements which are not units but have small norms contribute as much as*

**Table 4.3:** Some totally real number fields $K$ with their small primes, discriminant $d_K$, regulator and class number $h_K$. The first column describes $K$ as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, the second column is the regulator $R$, the third column is discriminant $d_K$ of $K$, and the fourth column gives the first small prime which is not inert. The last column computes (3.3) for $\mathcal{B}(6)$.

| $K \subset \mathbb{Q}(\zeta_p)$ | $R$ | $d_K$ | $h_K$ | primes | (3.3) for $\mathcal{B}(6)$ |
|---|---|---|---|---|---|
| $\mathbb{Q}(\zeta_{11})$ | 1.63 | $11^4$ | 1 | 11 ramifies | 1352.66 |
| $\mathbb{Q}(\zeta_{31})$ | 30.36 | $31^4$ | 1 | 5 splits | 90.22 |
| $\mathbb{Q}(\zeta_{61})$ | 93.768 | $61^4$ | 1 | 11 splits | 44.12 |
| $\mathbb{Q}(\zeta_{71})$ | 70.611 | $71^4$ | 1 | 23 splits | 60.01 |
| $\mathbb{Q}(\zeta_{23})$ | 1014.31 | $23^{10}$ | 1 | 23 ramifies | |
| $\mathbb{Q}(\zeta_{67})$ | 330512.24 | $67^{10}$ | 1 | 29 splits | |

*the units. Then, among these number fields, those with less units are identified through their regulator. Current bounds on the regulator seem to characterize the behavior of the sum of inverse norms, even for small constellation sizes. This gives a first set of number fields candidate to provide good lattice wiretap codes.*

## 4.3 Numerical Results

In this section, we provide some numerical results, to get some intuition on the behaviour of the sum of inverse of algebraic norm (4.1). We start with quadratic fields, since they are the number fields best understood.

### 4.3.1 Quadratic Fields

To look at the effect of the regulator on the sum (4.1), we do some numerical experiments with quadratic fields. We use the MATLAB software to compute the sum (4.1) based on different finite regions of lattice points in quadratic fields. The program represents algebraic integers as lattice points on the 2-dimensional Cartesian plane as shown in Figure 4.2. Note that $\mathcal{B}$ in the sum from (4.1) is assumed to be the square grid centered at the origin of different sizes. See Table 4.4, for an example of MATLAB code for $\mathcal{O}_K$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ for a squarefree $d$. Recall

from Theorem 4, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \ | a, b \in \mathbb{Z}\}$ if $d \not\equiv 1 \pmod 4$ whereas $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b\frac{1+\sqrt{d}}{2} \ | a, b \in \mathbb{Z}\}$ if $d \equiv 1 \pmod 4$.

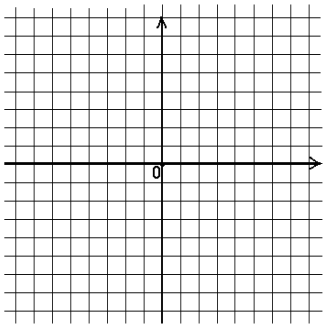


**Figure 4.2: Lattice points** - The grid points represent lattice points.

**Remark 24.** *When we run seriessum(r) on MATLAB for some positive values of the integer $r$, the above algorithm steps will compute the sum (4.1) over all algebraic integers within the square grid centered at the origin of size $r$ where the coordinates of both axes of the Cartesian plane range in $[-r, r]$ respectively.*

**Example 19.** *Using the algorithm, we plot the graphs for the sum over Gaussian integers and Eisenstein integers within square grids centered at the origin of size $r$ where $r$ is at most 50, in Figure 4.3 and Figure 4.4 respectively where both of these number fields contain finitely many units, namely the units of Gaussian integers are $\pm 1, \ \pm i$ whereas the units of Eisenstein integers are $\pm 1, \ \pm\omega, \ \pm\omega^2$ where $\omega = \frac{-1+\sqrt{-3}}{2} = e^{\frac{2\pi i}{3}}$. Since the rings of integers of Gaussian integers and Eisenstein integers contain only 4 and 6 units respectively, both sums converge even when the square grids contain all units. In both cases, most of the weight of the sum is reached when $r = 5$. The sum is smaller for $\mathbb{Z}[i]$ which can be easily explained by the number of units.*

Thus compared to $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ has more weight in terms of units but less in terms of non-units elements. Next we have an example from real quadratic fields where their number of units are infinite.

**Example 20.** *Modifying the algorithm, we plot the graphs for the sums over $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ within square grids centred at origin of size $r$ at most 50 based on with only units, without units and the whole ring of integers in the Figure 4.5 and Figure 4.6 respectively. From the figures, clearly the units weight more.*

*Furthermore, we compare that for a same $r$, the sum over $\mathbb{Z}[\sqrt{2}]$ is smaller than the sum over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. By computation using Sage, we note that the regulator of $\mathbb{Z}[\sqrt{2}]$*

**Table 4.4:** An example of MATLAB code for $\mathcal{O}_K$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ for a squarefree $d$.

```
function y = seriessum(limit)

a = zeros(2*limit+1);
b = zeros(2*limit+1);

for i = -limit:limit
    a(i+limit+1,:) = -limit:limit;
    b(:,i+limit+1) = (-limit:limit)';
end

N=a.^2+b.^2; % Norm of Gaussian Integers.
S=1./N.^3;  % Replace N by the norm of ring of integers of
            % different quadratic fields. For example,
            % norm of Eisenstein Integers is a.^2+b.^2+a.*b.

S(isinf(S)) = 0;
y = sum(sum(S));
```

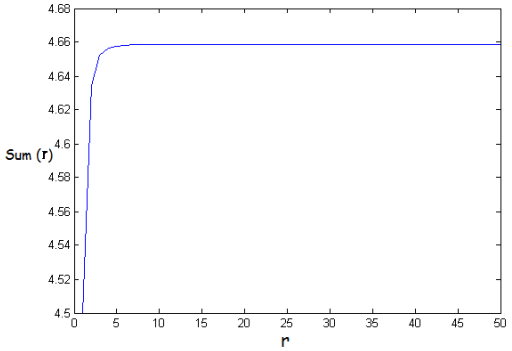


**Figure 4.3: Imaginary Quadratic Field 1** - The sum (4.1) based on Gaussian integers. The contribution of non-units clearly is less that 1, ($\approx 0.66$) for $r \leq 50$.

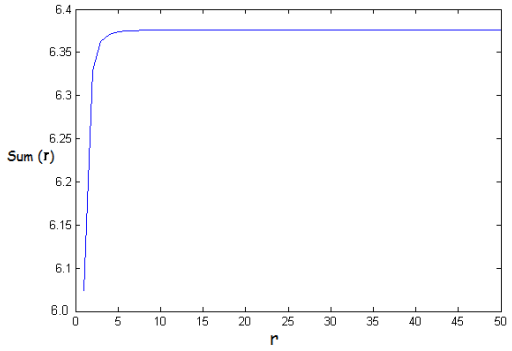


**Figure 4.4: Imaginary Quadratic Field 2** - The sum (4.1) based on Eisenstein integers. The contribution of non-units elements is $\approx 0.36$ for $r \leq 50$.

*equals to 0.88137 and is larger than the regulator of* $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ *which equals to 0.48121. This provides some beacon for the effect of regulator on the sum (4.1). Indeed, we expect the larger regulator to give a smaller sum which is numerically confirmed.*

### 4.3.2 Cyclotomic Fields

After quadratic fields, the next best understood number fields are cyclotomic fields. We present some numerical computations of number fields from the family of cyclotomic fields in Table 4.5, where the regulator of the number fields and the ramification of prime numbers are given.

In Table 4.5, we classify cyclotomic fields of same degrees into groups, then we compute their regulators and study the ramification of prime numbers so that this information can be utilized to evaluate how large the range of regulators can be, given the degree. For cyclotomic fields with the same degree, for a very small range of regulators among those number fields, the ramification of prime numbers may weight more.

Finally, we present next in Section 4.3.3 some numerical results on totally real number fields of degree 3 which are obtained from cyclotomic fields.

### 4.3.3 Totally Real Number Fields of Degree 3

Let $p$ be an odd prime and denote $\zeta_p$ be a primitive $p-$th root of unity of the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. Then $\mathbb{Q}(\zeta_p)$ is cyclic extension of degree $p-1$ over $\mathbb{Q}$ with its Galois

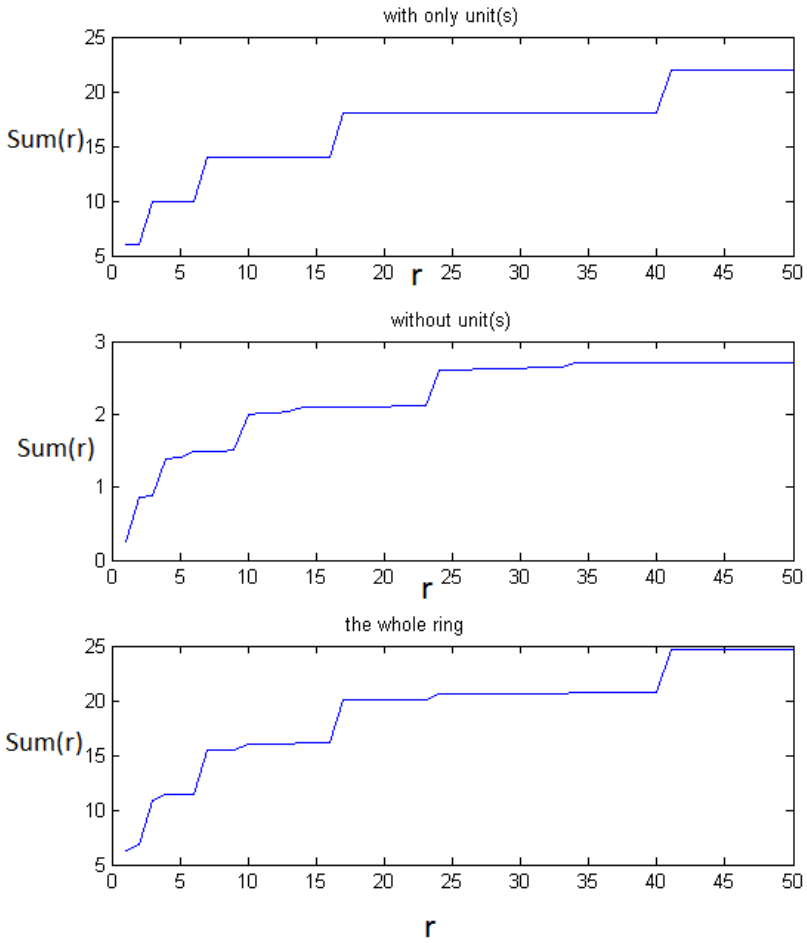


**Figure 4.5: Real Quadratic Field 1** - The sums (4.1) based on $\mathbb{Z}[\sqrt{2}]$ plotted based on with only units, without units and the whole ring of integers.

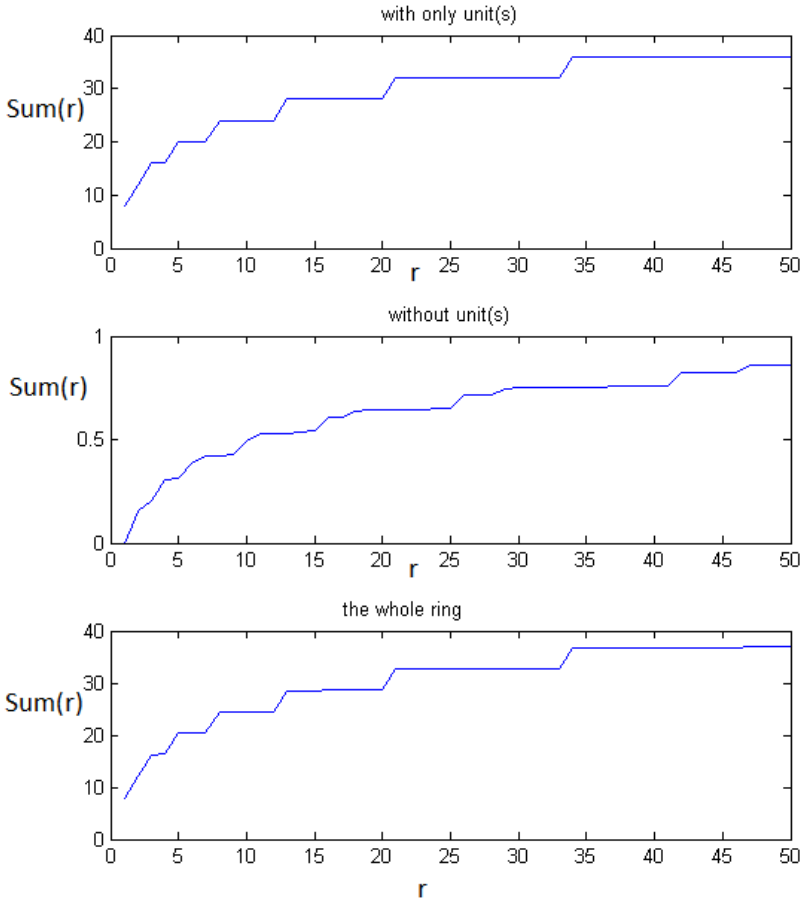


**Figure 4.6: Real Quadratic Field 2** - The sums (4.1) based on $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ plotted based on with only units, without units and the whole ring of integers.

**Table 4.5:** Some cyclotomic fields $K$ with its regulator $R$ (second column) and first small prime that is not inert (last column).

| Cyclotomic fields of degree 4 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_5)$ | 0.9624 | 5 ramifies |
| $\mathbb{Q}(\zeta_8)$ | 1.7627 | 2 ramifies |
| $\mathbb{Q}(\zeta_{12})$ | 1.3170 | 2 ramifies |

| Cyclotomic fields of degree 6 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_7)$ | 2.1018 | 2 splits |
| $\mathbb{Q}(\zeta_9)$ | 3.3971 | 3 ramifies |

| Cyclotomic fields of degree 8 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{15})$ | 4.6618 | 2 splits |
| $\mathbb{Q}(\zeta_{16})$ | 19.534 | 2 ramifies |
| $\mathbb{Q}(\zeta_{20})$ | 7.4112 | 2 ramifies |
| $\mathbb{Q}(\zeta_{24})$ | 10.643 | 2 ramifies |

| Cyclotomic fields of degree 10 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{11})$ | 26.1711 | 3 splits |

| Cyclotomic fields of degree 12 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{13})$ | 120.7840 | 3 splits |
| $\mathbb{Q}(\zeta_{21})$ | 70.3994 | 2 splits |
| $\mathbb{Q}(\zeta_{28})$ | 123.2527 | 2 ramifies |
| $\mathbb{Q}(\zeta_{36})$ | 162.8377 | 2 ramifies |

| Cyclotomic fields of degree 16 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{17})$ | 3640.01 | 2 splits |
| $\mathbb{Q}(\zeta_{32})$ | 15753.95 | 2 ramifies |
| $\mathbb{Q}(\zeta_{40})$ | 3557.07 | 2 ramifies |
| $\mathbb{Q}(\zeta_{48})$ | 5982.16 | 2 ramifies |
| $\mathbb{Q}(\zeta_{60})$ | 1560.86 | 2 splits |

| Cyclotomic fields of degree 18 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{19})$ | 22305.90 | 5 splits |
| $\mathbb{Q}(\zeta_{27})$ | 40934.03 | 3 ramifies |

| Cyclotomic fields of degree 20 | $R$ | primes |
|---|---|---|
| $\mathbb{Q}(\zeta_{25})$ | 161406.84 | 5 ramifies |
| $\mathbb{Q}(\zeta_{33})$ | 62791.39 | 2 splits |
| $\mathbb{Q}(\zeta_{44})$ | 140601.25 | 2 ramifies |

**Table 4.6:** Totally real cyclic number fields $K'$ of degree 3 with the first column describes $K'$ as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, the second column is the minimal polynomial of $K'$, the third column is the regulator $R$, the fourth column is $h_{K'}$, the class number of $K'$ and the fifth column is $d_{K'}$, discriminant of $K'$.

| $K' \subset \mathbb{Q}(\zeta_p)$ | $p(X)$ | $R$ | $h_{K'}$ | $d_{K'}$ |
|---|---|---|---|---|
| $\mathbb{Q}(\zeta_7)$ | $X^3 + X^2 - 2X - 1$ | 0.525 | 1 | 49 |
| $\mathbb{Q}(\zeta_{13})$ | $X^3 + X^2 - 4X + 1$ | 1.365 | 1 | 169 |
| $\mathbb{Q}(\zeta_{19})$ | $X^3 + X^2 - 6X - 7$ | 1.952 | 1 | 361 |
| $\mathbb{Q}(\zeta_{31})$ | $X^3 + X^2 - 10X - 8$ | 12.196 | 1 | 961 |
| $\mathbb{Q}(\zeta_{37})$ | $X^3 + X^2 - 12X + 11$ | 3.126 | 1 | 1369 |
| $\mathbb{Q}(\zeta_{43})$ | $X^3 + X^2 - 14X + 8$ | 18.922 | 1 | 1849 |
| $\mathbb{Q}(\zeta_{61})$ | $X^3 + X^2 - 20X - 9$ | 13.709 | 1 | 3721 |
| $\mathbb{Q}(\zeta_{67})$ | $X^3 + X^2 - 22X + 5$ | 19.703 | 1 | 4489 |
| $\mathbb{Q}(\zeta_{73})$ | $X^3 + X^2 - 24X - 27$ | 19.248 | 1 | 5329 |
| $\mathbb{Q}(\zeta_{79})$ | $X^3 + X^2 - 26X + 41$ | 4.698 | 1 | 6241 |
| $\mathbb{Q}(\zeta_{97})$ | $X^3 + X^2 - 32X - 79$ | 5.168 | 1 | 9409 |

group denoted by $G$. For $3|p-1$, there exists a unique subfield of degree 3, $K'$ in $\mathbb{Q}(\zeta_p)$ which is also Galois since its corresponding subgroup is normal in $G$. Furthermore, $[K' : \mathbb{Q}] = 3$, there exists a real embedding of $K'$ into $\mathbb{C}$ and using Lemma 1, we have that $K'$ is a totally real number field of degree 3.

So now we present numerical computations of $K'$ in Table 4.6

# Chapter 5

# Construction A of Ideal Lattices and Wiretap Encoding

In this chapter, we propose a generalized construction of lattices over a number field from linear codes and detail its application to wiretap encoding for block fading wiretap channels.

Recall from Chapter 2 that the wiretap encoding we use for wiretap channels is lattice coset encoding. The underlying idea of such a wiretap encoding is to have two nested lattices $\Lambda_e \subset \Lambda_b$ where $\Lambda_b$ is represented as a union of cosets of $\Lambda_e$. Information symbols are used to label the cosets, and random bits are introduced to pick a lattice point randomly within this coset. This randomized encoding is meant to provide confidentiality between the two legitimate players, in the presence of an eavesdropper.

We begin this chapter below with the introduction of some terminology related to classical coding theory. Note that this section also requires the background on lattices from Chapter 2 and algebraic number theory from Chapter 3. In Section 5.1, we present a general ideal lattice construction from linear codes, which is a generalization of Construction A of lattices from binary codes. Parameters and properties are studied in Section 5.2 and Section 5.3. The application to wiretap encoding for block fading channels is discussed in Section 5.4 .

Before starting, let us recall the notion of *linear code*, *generator matrix of a linear code* and *parity-check matrix of the dual code*.

**Definition 42.** *Let $\mathbb{F}_q$ be the finite field of $q$ elements where $q$ is a prime power. An $(N, k)$ linear code $C$ is a $k$-dimensional vector subspace of the Hamming space $\mathbb{F}_q^N$.*

**Definition 43.** *The dual code $C^\perp$ of $C$ is given by*

$$C^\perp = \{\mathbf{y} \in \mathbb{F}_q^N \mid \mathbf{y} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{x} \in C\}.$$

*When $C = C^\perp$, the code $C$ is said to be self-dual.*

In coding theory, a basis of a linear code is represented in the form of *generator matrix* while a matrix that represents a basis of the dual code is called *parity-check matrix*.

**Definition 44.**

- *A generator matrix for a linear code $C$ is a matrix $G'$ whose rows form a basis for $C$.*
- *A parity-check matrix $H$ for a linear code $C$ is a generator matrix for the dual code $C^\perp$.*

Connections between lattices and linear codes have been classically studied (see [7] for an excellent course on the topic, or [5] for an exhaustive list of relevant results). Construction of lattices from binary codes are referred to as "Construction A".

**Definition 45** (Construction A)**.** *Let $\rho : \mathbb{Z}^N \to \mathbb{F}_2^N$ be the reduction* $\bmod 2$ *componentwise. Let $C$ be an $(N, k)$ binary linear code of length $N$. Then $\Lambda = \rho^{-1}(C)$ is a lattice. We write*

$$\Lambda = 2\mathbb{Z}^N + C = \bigcup_{c \in C} (2\mathbb{Z}^N + c).$$

From a coding point of view, Construction A is of practical interest since it provides an efficient method for encoding lattice codes which serves our goal in this chapter. Recent works in this direction include [11] where Barnes-Wall lattices are obtained from linear codes over polynomial rings, resulting in an explicit method of bit-labeling complex Barnes-Wall lattice codes.

Hence we propose a method for encoding ideal lattice codes over the ring of integers of a totally real number field so as to ensure full diversity as described in Chapter 3. In particular we study the case of $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ using a linear code over $\mathbb{F}_p$. This generalizes the well-known Construction $A$ to lattices obtained from number fields (see [7] when the number field is the cyclotomic field $\mathbb{Q}(\zeta_p)$) which further provides an efficient coset encoding for lattice codes .

## 5.1 A General Ideal Lattice Construction

To start with, let us set up the notations. Let $\mathbb{F}_q$ be the finite field with $q$ elements, where $q$ is a prime power. We use the term code to mean an $(N, k)$ linear code over $\mathbb{F}_q$, that is, $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^N$. Once again, to recall the background on lattices and algebraic number theory, the reader can refer to Chapters 2 and 3.

**Definition 46.** *An integral lattice $\Gamma$ is a free $\mathbb{Z}$-module of finite rank together with a positive definite symmetric bilinear form $\langle\ ,\ \rangle : \Gamma \times \Gamma \to \mathbb{Z}$.*

Let $K$ be a number field of degree $n$, with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p} \in \mathcal{O}_K$ be a prime above $p$, where $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_{p^f}$ since recall from Chapter 3 that $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension over $\mathbb{Z}/p\mathbb{Z}$ of degree $f$, which is the residual degree of $\mathfrak{p}$.

Let $C$ be an $(N, k)$ linear code over $\mathbb{F}_{p^f}$. We define $\Gamma_C$ to be the lattice obtained as the "preimage" of $C$ in $\mathcal{O}_K^N$. The precise definition is given as follows.

**Definition 47** (Generalized Construction A over number fields)**.** *Let $\rho : \mathcal{O}_K^N \to \mathbb{F}_{p^f}^N$ be the mapping defined by the reduction modulo the ideal $\mathfrak{p}$ in each of the $N$ coordinates. Define*

$$\Gamma_C := \rho^{-1}(C) \subset \mathcal{O}_K^N.$$

To see why $\Gamma_C$ forms a lattice, we first note that $\rho^{-1}(C)$ is a subgroup of $\mathcal{O}_K^N$ since $C$ is a subgroup of $\mathbb{F}_{p^f}^N$ and $\rho$ is a group homomorphism. Furthermore, $\mathcal{O}_K^N$ is a free $\mathbb{Z}$-module of rank $nN$, and so it follows that $\rho^{-1}(C)$ is also a free $\mathbb{Z}$-module. Now, since $|\mathcal{O}_K^N/\mathfrak{p}^N| < \infty$, $\rho^{-1}(C)$ and $\mathcal{O}_K^N$ must have the same rank as a $\mathbb{Z}$-module. We conclude that $\rho^{-1}(C)$ is a $\mathbb{Z}$-module of rank $nN$.

**Remark 25.** *Note that a variation of Construction A built on number fields is available in [22].*

Let $\mathbf{x} = (x_1, \ldots, x_N)$ and $\mathbf{y} = (y_1, \ldots, y_N)$ be vectors in $\mathcal{O}_K^N$. Then, $\rho^{-1}(C)$ forms a lattice with the positive definite symmetric bilinear form

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i), \tag{5.1}$$

where $\alpha \in \mathcal{O}_K$ is totally positive, meaning that $\sigma_i(\alpha) > 0$ for all $i$. The totally positive condition ensures that the trace form is positive definite; if $\sigma_i(\alpha) > 0$ for all $i$ and $\mathbf{x}$ is

not the zero vector, then, by the definition of trace,

$$\begin{aligned}\langle \mathbf{x}, \mathbf{x} \rangle &= \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i x_i) \\ &= \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha) \sigma_j(x_i)^2 > 0.\end{aligned}$$

If $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i)$ belongs to $\mathbb{Z}$ for all $i$ since $x_i, y_i \in \mathcal{O}_K$. Consequently, $\langle \mathbf{x}, \mathbf{y} \rangle$ is an integer. Thus, a totally positive $\alpha \in \mathcal{O}_K$ guarantees that $\Gamma_C$ together with the bilinear form (5.1) is an integral lattice. Though, as will be shown later, depending on the code $C$, other choices of $\alpha$ might be possible.

A generator matrix for the lattice $\Gamma_C = \rho^{-1}(C)$ is computed next. Recall that each of the $N$ coordinates of a lattice point $\mathbf{x} = (x_1, \ldots, x_N) \in \Gamma_C$ is an element of $\mathcal{O}_K$ since $\Gamma_C \subset \mathcal{O}_K^N$. Here, $\Gamma_C$ has rank $nN$ as a free $\mathbb{Z}$-module, so we are interested in a $\mathbb{Z}$-basis of $\Gamma_C$. Let $\{\nu_1, \ldots, \nu_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then, a generator matrix for the lattice formed by $\mathcal{O}_K$ together with the standard trace form $\langle w, z \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in \mathcal{O}_K$, is given by

$$M := \begin{pmatrix} \sigma_1(\nu_1) & \sigma_2(\nu_1) & \ldots & \sigma_n(\nu_1) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\nu_n) & \sigma_2(\nu_n) & \ldots & \sigma_n(\nu_n) \end{pmatrix} \tag{5.2}$$

since $MM^T = \mathrm{Tr}_{K/\mathbb{Q}}(\nu_i \nu_j)$. A vector $w$ in this lattice is thus a linear combination of the rows of $M$: $w = \sum_{i=1}^{n} w_i \nu_i$ is embedded as

$$(\sigma_1(\sum_{j=1}^{n} w_j \nu_j), \ldots, \sigma_n(\sum_{i=j}^{n} u_j \nu_j)), \text{ and } \langle w, z \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$$

which is the case of the ideal lattices as discussed in Chapter 3 by taking $N = 1$ and $\alpha = 1$ for the bilinear form in (5.1).

We now give one last ingredient before we derive a generator matrix for the lattice $\Gamma_C$. Recall that $\mathfrak{p}$ is a $\mathbb{Z}$-module of rank $n$. It then has a $\mathbb{Z}$-basis $\mu_1, \ldots, \mu_n$ given by $\mu_i = \sum_{j=1}^{n} \mu_{ij} \nu_j$, $\mu_{ij} \in \mathbb{Z}$, so that

$$\begin{pmatrix} \sigma_1(\mu_1) & \ldots & \sigma_n(\mu_1) \\ \vdots & & \vdots \\ \sigma_1(\mu_n) & \ldots & \sigma_n(\mu_n) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} \mu_{1j} \sigma_1(\nu_j) & \ldots & \sum_{j=1}^{n} \mu_{1j} \sigma_n(\nu_j) \\ \vdots & & \vdots \\ \sum_{j=1}^{n} \mu_{nj} \sigma_1(\nu_j) & \ldots & \sum_{j=1}^{n} \mu_{nj} \sigma_n(\nu_j) \end{pmatrix} = DM$$

where $D := (\mu_{i,j})_{i,j=1}^{n}$.

Recall that the discriminant of the lattice is defined to be the determinant of the Gram matrix $G$, namely $disc(\Lambda) = \det(G)$.

**Proposition 4.** *The lattice $\Gamma_C$ is a sublattice of $\mathcal{O}_K^N$ with discriminant*

$$disc(\Gamma_C) = d_K^N (p^f)^{2(N-k)}$$

*where $d_K$ is the discriminant of $K$. It is given by the generator matrix*

$$M_C = \begin{pmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{n(N-k),nk} & I_{N-k} \otimes DM \end{pmatrix}$$

*where $\otimes$ is the tensor (also known as Kronecker) product of matrices, $(I_k \quad A) \mod \mathfrak{p}$ is a generator matrix of $C$, $M$ is the matrix of embeddings of a $\mathbb{Z}$-basis of $\mathcal{O}_K$ given in (5.2), and $DM$ is the matrix of embeddings of a $\mathbb{Z}$-basis of $\mathfrak{p}$.*

*Proof.* The bilinear form $\langle w, z \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in \mathcal{O}_K$, has determinant $d_K$ over $\mathcal{O}_K$ since $d_K = \det(MM^T)$ by definition. Thus, the bilinear form $\langle x, y \rangle = \sum_{i=1}^N \mathrm{Tr}(x_i y_i)$ has determinant $d_K^N$ over $\mathcal{O}_K^N$. The map $\rho$ of reduction $\mod \mathfrak{p}$ is surjective, and $\rho^{-1}(C)$ is of index $(p^f)^{N-k}$, therefore the discriminant of $\Gamma_C$ is

$$disc(\Gamma_C) = d_K^N (p^f)^{2N-2k}.$$

It is clear from the shape of the generator matrix $M_C$ that this lattice has the right rank. Note that the first $nk$ rows of $M_C$ correspond to an embedding of a basis for $C$ and the last $n(N-k)$ rows of $M_C$ correspond to an embedding of a basis for $\mathfrak{p}$. To make this more precise, let us write $u_i = (u_{i1}, \ldots, u_{in}) \in \mathbb{Z}^n$ where $x_i = \sum_{l=1}^n u_{il}\nu_l$, $i = 1, \ldots, N$, and define $\sigma = (\sigma_1, \ldots, \sigma_n) : \mathcal{O}_K \to \mathbb{R}^n$ to be the canonical embedding of $K$. We have

$$\sigma_j(x_i) = \sigma_j \left( \sum_{l=1}^n u_{il}\nu_l \right) = u_i \cdot (M_{lj})_{l=1}^n$$

and

$$\begin{aligned} & (u_1, \ldots, u_k, u_{k+1}, \ldots, u_N) \begin{pmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{n(N-k),nk} & I_{N-k} \otimes DM \end{pmatrix} \\ = \quad & (\sigma(x_1), \ldots, \sigma(x_k), \sum_{j=1}^k a_{j1}\sigma(x_j) + \sigma(x'_{k+1}), \ldots, \sum_{j=1}^k a_{j,N-k}\sigma(x_j) + \sigma(x'_N)) \end{aligned}$$

where $x'_{k+1}, \ldots, x'_N$ are in the ideal $\mathfrak{p}$. It is not hard to see that the above vector is an element in $\Gamma_C$. Indeed, if we define

$$\psi : \sigma(x_i) = (\sigma_1(x_i), \ldots, \sigma_n(x_i)) \mapsto x_i = \sum_{l=1}^n u_{il}\nu_l \in \mathcal{O}_K,$$

then applying $\psi$ and $\rho$ componentwise in order gives

$$c = (\rho(\psi(\sigma(x_1))), \ldots, \rho(\psi(\sigma(x_k))), \sum_{j=1}^{k} a_{j1}\rho(\psi(\sigma(x_j))), \ldots, \sum_{j=1}^{k} a_{j,N-k}\rho(\psi(\sigma(x_j)))),$$

since $x'_i$ reduces to zero modulo $\mathfrak{p}$. Now, $c$ is a codeword of the code $C$ given by

$$c = (\rho(\psi(\sigma(x_1))), \ldots, \rho(\psi(\sigma(x_k))) \cdot (I_k \;\; A).$$

Finally, the absolute value of determinant of $M_C$ can be computed as

$$\begin{aligned} |\det(M_C)| &= |\det(I_k \otimes M)\det(I_{N-k} \otimes DM)| \\ &= |\det(M)|^k |\det(DM)|^{N-k} \\ &= |\det(M)|^N |\det(D)|^{N-k} \\ &= \sqrt{d_K}^N N(\mathfrak{p})^{N-k} \\ &= \sqrt{d_K}^N (p^f)^{N-k}, \end{aligned}$$

showing that $M_C$ generates a lattice with the same volume as $\Gamma_C$, which completes the proof of the proposition. □

For $\mathbf{x} = (x_1, \ldots, x_N) \in \Gamma_C \subset \mathcal{O}_K^N$, we have that $x_i = \sum_{j=1}^{n} x_{ij}\nu_j$ for $i = 1, \ldots, k$, and $x$ is embedded into $\mathbb{R}^{nN}$ as

$$\begin{aligned} \mathbf{x} &= (\sigma(x_1), \ldots, \sigma(x_k), \sum_{j=1}^{k} a_{j,1}\sigma(x_j) + \sigma(x'_{k+1}), \ldots, \sum_{j=1}^{k} a_{j,N-k}\sigma(x_j) + \sigma(x'_N)) \\ &= (\sigma_1(x_1), ..., \sigma_n(x_1), ..., \sigma_1(x_{k+1}), ..., \sigma_n(x_{k+1}), ..., \sigma_1(x_N), ..., \sigma_n(x_N), \end{aligned}$$

where $x_{k+1} = \sum_{j=1}^{k} a_{j,1}x_j + x'_{k+1}, ..., x_N = \sum_{j=1}^{k} a_{j,N-k}x_j + x'_N$.

Then,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i).$$

**Corollary 9.** *The lattice $\Gamma_C$ has Gram matrix*

$$\begin{pmatrix} GG^T \otimes \mathrm{Tr}(\nu_i\nu_j) & A \otimes \mathrm{Tr}(\mu_i\nu_j) \\ A^T \otimes \mathrm{Tr}(\mu_i\nu_j) & I_{N-k} \otimes \mathrm{Tr}(\mu_i\mu_j) \end{pmatrix}$$

*where $\mu_1, \ldots, \mu_n$ is a $\mathbb{Z}$-basis of $\mathfrak{p}$, and $G = (I_k \;\; A)$. In particular, $\Gamma_C$ is an integral lattice when $A$ is integral (this is always the case if $f = 1$).*

*Proof.* By definition, the Gram matrix of $\Gamma_C$ is

$$\begin{aligned} M_C M_C^T &= \begin{pmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{n(N-k),nk} & I_{N-k} \otimes DM \end{pmatrix} \begin{pmatrix} I_k \otimes M^T & \mathbf{0}_{nk,n(N-k)} \\ A^T \otimes M^T & I_{N-k} \otimes M^T D^T \end{pmatrix} \\ &= \begin{pmatrix} (I_k + AA^T) \otimes MM^T & A \otimes MM^T D^T \\ A^T \otimes DMM^T & I_{N-k} \otimes DMM^T D^T \end{pmatrix} \\ &= \begin{pmatrix} GG^T \otimes \mathrm{Tr}(\nu_i \nu_j) & A \otimes \mathrm{Tr}(\mu_i \nu_j) \\ A^T \otimes \mathrm{Tr}(\mu_i \nu_j) & I_{N-k} \otimes \mathrm{Tr}(\mu_i \mu_j) \end{pmatrix}. \end{aligned}$$

It follows that the entries of this matrix are integers when $A$ has integral entries, and thus $\Gamma_C$ is an integral lattice. □

A similar construction is obtained from a CM-field. We provide an outline next, in less details, since we will be mostly interested in the totally real case. Recall that a CM-field is a totally imaginary quadratic extension of a totally real number field. If $K$ is a CM-field and $\alpha \in \mathcal{O}_K \cap \mathbb{R}$ is totally positive, then $\rho^{-1}(C)$ forms a lattice with the positive definite symmetric bilinear form

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i), \tag{5.3}$$

where $\bar{y}_i$ denotes the complex conjugate of $y_i$. Since $\sigma_i$ commutes with the complex conjugation and $\sigma_i(\alpha) > 0$ for all $i$, we have for $\mathbf{x}$ not the zero vector that

$$\begin{aligned} \langle \mathbf{x}, \mathbf{x} \rangle &= \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{x}_i) \\ &= \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha) |\sigma_j(x_i)|^2 > 0. \end{aligned}$$

Again, whether $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i) \in \mathbb{Z}$ depends on the choice of $\alpha$, and $\alpha \in \mathcal{O}_K$ is a sufficient condition, as that makes $\alpha x_i \bar{y}_i \in \mathcal{O}_K$ for all $x_i, y_i \in \mathcal{O}_K$. A generator matrix for this lattice is obtained similarly as above, with the exception that now $\sigma_{r_1+1}, \ldots, \sigma_n$ are complex embeddings. One thus chooses one complex embedding per pair and separates its real and imaginary parts to get

$$\sigma = (\sigma_1, \ldots, \sigma_{r_1}, \Re(\sigma_{r_1+1}), \Im(\sigma_{r_1+1}), \ldots, \Re(\sigma_{r_1+r_2}) \Im(\sigma_{r_1+r_2}))$$

and

$$\mathbf{x} = (\sigma_1(\sum_{j=1}^{n} u_j \nu_j), \ldots, \Re(\sigma_{r_1+1}(\sum_{j=1}^{n} u_j \nu_j)), \ldots, \Im(\sigma_{r_1+r_2}(\sum_{j=1}^{n} u_j \nu_j))).$$

## 5.2 The Case of a Totally Ramified Prime

Variations of the above construction have been considered in the literature. We keep the notations adopted so far. In particular, when $N = 1$, i.e., codes are not involved, the problem reduces to understanding which lattices can be obtained on the ring of integers of a number field as illustrated in ideal lattice codes from Chapter 3 (also see [2] for example). The quotient $\mathcal{O}_K/p\mathcal{O}_K$ has been considered in [22], where the lattice obtained from the ideal $\mathfrak{p}\mathcal{O}_K/p\mathcal{O}_K$ has been studied for $\mathfrak{p}$ a prime above $p$ with large ramification index. In the cases explored, the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is a polynomial ring, and the ideal $\mathfrak{p}\mathcal{O}_K/p\mathcal{O}_K$ corresponds to one of its ideals, which in turn defines a code over the given polynomial ring.

We will focus on the case where $K$ is a Galois extension and the prime $\mathfrak{p}$ is chosen so that $\mathfrak{p}$ is totally ramified. Therefore, we have $p\mathcal{O}_K = \mathfrak{p}^n$, $e = n$, and $f = 1$.

Now, let $C' \subset \mathbb{F}_p^N$ be a linear code over $\mathbb{F}_p$ of length $N$, and let $\rho : \mathcal{O}_K^N \to \mathbb{F}_p^N$ be the mapping defined by the reduction modulo the prime ideal $\mathfrak{p}$ on every coordinate. We consider (see Definition 47) the lattice

$$\Gamma_{C'} := \rho^{-1}(C') \subset \mathcal{O}_K^N.$$

We know from the previous section that $\Gamma_{C'}$ is an integral lattice of rank $nN$ with respect to the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i)$ for a totally positive element $\alpha \in \mathcal{O}_K \cap \mathbb{R}$. If $K$ is totally real, then $\bar{y}_i = y_i$, and this notation allows us to treat both the cases of totally real and CM-field at the same time.

Next we will show that if $C' \subset C'^{\perp}$, then $\sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i) \in p\mathbb{Z}$, and thus we can normalize the positive definite symmetric bilinear form by a factor of $1/p$, or equivalently, choose $\alpha = 1/p$.

**Lemma 6.** *Let $C' \subset \mathbb{F}_p^N$ be a code such that $C' \subset C'^{\perp}$. Then, $\Gamma_{C'}$ is an integral lattice with respect to the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$.*

*Proof.* It suffices to show that $\langle \mathbf{x}, \mathbf{y} \rangle$ as defined is an integer for all $\mathbf{x}, \mathbf{y} \in \Gamma_{C'}$. Let

$\mathbf{x} = (x_1, \ldots, x_N)$ and $\mathbf{y} = (y_1, \ldots, y_N)$ be elements in $\Gamma_{C'} = \rho^{-1}(C')$. We have

$$\begin{aligned}\rho(\mathbf{x} \cdot \mathbf{y}) &= \rho\left(\sum_{i=1}^{N} x_i y_i\right) \\ &= \sum_{i=1}^{N} \rho(x_i)\rho(y_i) \\ &= \rho(\mathbf{x}) \cdot \rho(\mathbf{y}) \\ &= 0 \in \mathbb{F}_p\end{aligned}$$

where the last equality follows from the fact that $\rho(x), \rho(y) \in C'$ and $C' \subset C'^{\perp}$. It follows that

$$\sum_{i=1}^{N} x_i y_i = \mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod{\mathfrak{p}}.$$

We are going to show next that $\bar{y_i} \equiv y_i \mod \mathfrak{p}$ for all $i = 1, \ldots, N$. Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, for each $i$, one can write $y_i \in \mathcal{O}_K$ as $y_i = y_i' + y_i''$ where $y_i' \in \mathbb{Z}$ and $y_i'' \in \mathfrak{p}$. Note that $\bar{\cdot}$ is the automorphism of $K$ induced by complex conjugation. Since $K$ is a Galois extension, the Galois group acts transitively on the ideals above $p$. However, the only prime above $p$ is $\mathfrak{p}$, so we must have $\bar{y}_i'' \in \mathfrak{p}$. It follows that $\bar{y_i} = y_i' + \bar{y}_i'' \equiv y_i' + y_i'' = y_i \mod \mathfrak{p}$ as desired.

Therefore,

$$\sum_{i=1}^{N} x_i y_i \equiv \sum_{i=1}^{N} x_i \bar{y_i} \equiv 0 \pmod{\mathfrak{p}}.$$

Again, as $\mathfrak{p}$ is the only prime above $p$, all conjugates of $\sum_{i=1}^{N} x_i \bar{y_i}$ must lie in $\mathfrak{p}$, and so must its trace. In other words,

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i \bar{y_i}\right) \in \mathfrak{p},$$

implying that

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i \bar{y_i}\right) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}.$$

Now, by linearity of the trace,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y_i}/p) = \frac{1}{p}\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i \bar{y_i}\right),$$

and so we may conclude that $\Gamma_{C'}$ is integral. □

**Remark 26.** Note that instead of considering the lattice $\rho^{-1}(C')$ with

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i / p),$$

we can alternatively consider the lattice $\rho^{-1}(C')/\sqrt{p}$ with $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i)$.

Next, we derive some parameters of $\Gamma_{C'}$ where the code $C'$ is chosen so that $C \subset C'^{\perp}$. Let $G = (I_k \;\; A)$ be a generator matrix for $C'$. First, by Proposition 4, the generator matrix for $\Gamma_{C'}$ is

$$M_{C'} = \frac{1}{\sqrt{p}} \begin{pmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{n(N-k),nk} & I_{N-k} \otimes DM \end{pmatrix}.$$

Its discriminant is then

$$disc(\Gamma_{C'}) = d_K^N p^{2N-2k-nN}.$$

Indeed, by Corollary 9,

$$disc(\Gamma_{C'}) = (\frac{1}{p})^{nN} d_K^N (p^f)^{2(N-k)} = d_K^N \frac{p^{2(N-k)}}{p^{nN}}.$$

The Gram matrix of $\Gamma_{C'}$ is

$$\frac{1}{p} \begin{pmatrix} GG^T \otimes \mathrm{Tr}(\nu_i \nu_j) & A \otimes \mathrm{Tr}(\mu_i \nu_j) \\ A^T \otimes \mathrm{Tr}(\mu_i \nu_j) & I_{N-k} \otimes \mathrm{Tr}(\mu_i \mu_j) \end{pmatrix}.$$

We know from Lemma 6 that $\Gamma_{C'}$ is an integral lattice, so we may expect entries of the Gram matrix of $\Gamma_{C'}$ to be integers. This is certainly the case since $G$ is a generator matrix for a code $C' \subset C'^{\perp}$ over $\mathbb{F}_p$ (so $p$ divides every entry of $GG^T$) and $\mu_i \nu_j, \mu_i \mu_j \in \mathfrak{p}$ for all $i$ and $j$ (so $p$ divides every entry of $\mathrm{Tr}(\mu_i \nu_j)$ and $\mathrm{Tr}(\mu_i \nu_j)$).

Several particular cases of the above constructions have been considered in the literature. We provide some of them here in the following examples.

**Example 21.** The following construction is discussed in Section 5.2 of [7]. Let $p$ be an odd prime, and let $\zeta_p$ be the primitive $p^{\text{th}}$ root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. The degree of $K$ over $\mathbb{Q}$ is $p-1$, and $p$ is totally ramified, with $p\mathcal{O}_K = (1-\zeta_p)^{p-1}$. Thus, take the prime ideal $\mathfrak{p} = (1-\zeta_p)$ with the residue field $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$ and the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i / p)$. Since $\mathbb{Q}(\zeta_p)$ is a CM-field, this bilinear form corresponds to (5.3) with $\alpha = 1/p$. It was proven that, given a code $C'$ over $\mathbb{F}_p$, if $C' \subset C'^{\perp}$ then $\rho^{-1}(C')$ is an integral lattice of rank $N(p-1)$.

**Example 22.** A particularly well-known construction of lattices from codes is when $p = 2$ in the previous example. In such case, $\zeta_p = -1$, $\mathcal{O}_K = \mathbb{Z}$, and $\mathfrak{p} = 2\mathbb{Z}$, yielding the so-called Construction A (see Section 1.3 of [7]). To obtain lattices of rank $N$ from binary linear codes of length $N$, we consider

$$\Gamma_{C'} = \frac{1}{\sqrt{2}}\rho^{-1}(C'),$$

with $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} \mathrm{Tr}(x_i y_i)$ (see Remark 26). A generator matrix for this lattice is

$$M_C = \frac{1}{\sqrt{2}} \begin{pmatrix} I_k & A \\ 0 & 2I_{N-k} \end{pmatrix},$$

which may be obtained as a particular case of Proposition 4.

## 5.3 Maximal Totally Real Subfields of Cyclotomic Fields

Since we consider the case where $\mathfrak{p}$ is a prime above $p$ which totally ramifies in $K$, cyclotomic fields and their subfields are natural candidates to study. Let $p$ be an odd prime, and let $\zeta_{p^r}$ be a primitive $p^r$th root of unity.

Let us start by considering $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ the maximal totally real subfield of the cyclotomic field $K = \mathbb{Q}(\zeta_{p^r})$, $r \geq 1$, with respective rings of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$ [33, p.16]. The degree of $K^+$ over $\mathbb{Q}$ is $\frac{p^{r-1}(p-1)}{2}$. The prime $p$ totally ramifies in $K$:

$$p\mathcal{O}_K = \mathfrak{P}^{p^{r-1}(p-1)},$$

where $\mathfrak{P}$ is a prime principal ideal with generator $1 - \zeta_{p^r}$ and residue field $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. We write $e(\mathfrak{P}|p) = p^{r-1}(p-1)$ for its ramification index, and by transitivity of ramification indices

$$p^{r-1}(p-1) = e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p)$$

for $\mathfrak{p}$ the prime above $p$ in $K^+$. This is enough to conclude that $e(\mathfrak{p}|p) = p^{r-1}(p-1)/2$, and the prime $p$ also totally ramifies in $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$:

$$p\mathcal{O}_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$$

with

$$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{K^+} = (1 - \zeta_{p^r})(1 - \zeta_{p^r}^{-1}).$$

**Lemma 7.** *Consider the number field $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$. Let $C \subset \mathbb{F}_p^N$ be a $k$-dimensional code such that $C \subset C^\perp$. Then the lattice $\Gamma_C$ given in Definition 47 together with the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^N \mathrm{Tr}_{K^+/\mathbb{Q}}(\alpha x_i y_i)$ is an integral lattice of rank $Np^{r-1}(p-1)/2$.*

This follows immediately from what was done in the previous section. A generator matrix for the lattice $\Gamma_C = \rho^{-1}(C)$ is obtained as described in Proposition 4, namely

$$M_C = \frac{1}{\sqrt{p}} \begin{pmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{n(N-k),nk} & I_{N-k} \otimes DM \end{pmatrix}$$

where as usual $G = (I_k \;\; A)$ is the generator matrix of $C$. Here $\mathfrak{p}$ is principal, generated by $(2 - \zeta_{p^r} - \zeta_{p^r}^{-1})$. A $\mathbb{Z}$-basis of $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ is $\{\zeta_{p^r}^i + \zeta_{p^r}^{-i}\}_{i=0}^{n-1}$. The matrix $M$ is thus obtained from this $\mathbb{Z}$-basis, by applying the $n$ embeddings of $K$, which are of the form $\sigma_k(\zeta_{p^r} + \zeta_{p^r}^{-1}) = \zeta_{p^r}^i + \zeta_{p^r}^{-i}$, with $i$ coprime to $p$.

In the case $r = 1$, that is $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, more can be said [13].

**Lemma 8.** *Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and let $C \subset \mathbb{F}_p^N$ be a $k$-dimensional code such that $C \subset C^\perp$. Then*

$$\Gamma_C^* = \Gamma_{C^\perp}.$$

*Proof.* Let $\mathbf{x} \in \Gamma_C$, $\mathbf{y} \in \Gamma_{C^\perp}$. Then by definition of these lattices, $\rho(\mathbf{x}) \in C$ and $\rho(\mathbf{y}) \in C^\perp$, and it follows by definition of $C^\perp$ that $\rho(\mathbf{x}) \cdot \rho(\mathbf{y}) \equiv 0 \pmod p$. By redoing the argument in the proof of Lemma 6, we deduce that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$, and thus $\Gamma_{C^\perp} \subset \Gamma_C^*$.

The discriminant of $\Gamma_C$ is

$$disc(\Gamma_C) = p^{N-2k}.$$

This follows from the fact that

$$disc(\Gamma_C) = d_{K^+}^N p^{2N-2k-N(p-1)/2} = (p^{(p-1)/2-1})^N p^{2N-2k-N(p-1)/2},$$

since $d_{K^+} = p^{(p-1)/2-1}$.

It then follows that

$$\mathrm{vol}(\mathbb{R}^{nN}/\Gamma_C) = (p^{N-2k})^{1/2} = p^{\frac{N}{2}-k}$$

and

$$\mathrm{vol}(\mathbb{R}^{nN}/\Gamma_C^*) = p^{k-\frac{N}{2}}.$$

On the other hand, the dimension of $C^\perp$ is $N - k$, and so

$$disc(\Gamma_{C^\perp}) = p^{N-2(N-k)} = p^{2k-N},$$

implying that

$$\mathrm{vol}(\mathbb{R}^{nN}/\Gamma_{C^\perp}) = p^{k-\frac{N}{2}}.$$

We may now conclude that $\Gamma_C^* = \Gamma_{C^\perp}$. □

**Corollary 10.** *Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let $C \subset \mathbb{F}_p^N$ be a $k$-dimensional code such that $C \subset C^\perp$. Then the lattice $\Gamma_C$ given in Definition 47 together with the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^N \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i)$ is an integral lattice of rank $Np^{r-1}(p-1)/2$. In addition, if $C$ is self-dual, then $\Gamma_C$ is an odd unimodular lattice.*

*Proof.* By an odd integral lattice, we mean an integral lattice $\Gamma$ which contains a vector $\mathbf{x} \in \Gamma$ such that $\langle \mathbf{x}, \mathbf{x} \rangle$ is an odd integer. Indeed, take $\mathbf{x} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1}, 0, \ldots, 0) \in \Gamma$. Then

$$\begin{aligned}
\langle \mathbf{x}, \mathbf{x} \rangle &= \mathrm{Tr}_{K^+/\mathbb{Q}}((2 - \zeta_p - \zeta_p^{-1})^2/p) \\
&= \frac{1}{p}\mathrm{Tr}_{K^+/\mathbb{Q}}(6 - 4(\zeta_p + \zeta_p^{-1}) + (\zeta_p^2 + \zeta_p^{-2})) \\
&= \frac{6(p-1)}{2p} + \frac{-3}{p}\mathrm{Tr}_{K^+/\mathbb{Q}}(\zeta_p + \zeta_p^{-1}) \\
&= \frac{6(p-1)}{2p} + \frac{3}{p} = 3
\end{aligned}$$

since $\zeta_p + \zeta_p^{-1}$ and $\zeta_p^2 + \zeta_p^{-2}$ are conjugate, and using that

$$\begin{aligned}
\mathrm{Tr}_{K^+/\mathbb{Q}}(\zeta_p + \zeta_p^{-1}) &= \mathrm{Tr}_{K^+/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K^+}(\zeta_p)) \\
&= \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1.
\end{aligned}$$

If $C$ is self-dual, then by the above Lemma 8, $\Gamma_C^* = \Gamma_{C^\perp} = \Gamma_C$ and $\Gamma_C$ is a unimodular lattice. □

**Example 23.** Fix $p = 5$, $K = \mathbb{Q}(\zeta_5)$ and $K^+ = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$, with $\rho : \mathbb{Z}[\zeta_5 + \zeta_5^{-1}]^2 \to \mathbb{F}_5^2$. Let $\xi = \zeta_5 + \zeta_5^{-1}$. The degree of $K^+/\mathbb{Q}$ is 2, the two embeddings of $K$ are $\sigma_1$ which is the identity and $\sigma_2$ which maps $\zeta_5 + \zeta_5^{-1}$ to $\zeta_5^2 + \zeta_5^{-2}$, that is $\sigma_2(\xi) = -1 - \xi$.

Consider the self-dual code of length 2 over $\mathbb{F}_5$ given by a generator matrix

$$G = \begin{pmatrix} 1 & 2 \end{pmatrix},$$

that is, $C = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$. Then, $\Gamma_C$ is an odd positive definite unimodular lattice of rank 4, and the only such lattice is $\mathbb{Z}^4$ [5].

Consider now the Cartesian product of the code $C$ by itself, that is, the code $C_2$ over $\mathbb{F}_5$ given by a generator matrix

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

Then, $\Gamma_{C_2}$ is an odd positive definite unimodular lattice of rank 8, which is $\mathbb{Z}^8$.

We next compute a generator matrix for the lattice $\Gamma_C$ explicitly. We choose the basis $\{1, \xi\}$ for $\mathcal{O}_K$, and it follows that the generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle x, y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy/5)$, $x, y \in \mathcal{O}_K$, is

$$M = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 \\ \xi & \sigma_2(\xi) \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 \\ \xi & -1-\xi \end{pmatrix}.$$

The generator matrix for $\Gamma_C$ as a free $\mathbb{Z}$-module of rank 4 is

$$M_C = \begin{pmatrix} M & 2M \\ \mathbf{0} & DM \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 2 & 2 \\ \xi & -1-\xi & 2\xi & 2(-1-\xi) \\ 0 & 0 & 2-\xi & 2-(-1-\xi) \\ 0 & 0 & \xi(2-\xi) & (-1-\xi)(2-(-1-\xi)) \end{pmatrix}$$

where

$$D = \begin{pmatrix} 2 & -1 \\ -1 & 3 \end{pmatrix}$$

and $DM$ is the matrix of embeddings of the ideal $\mathfrak{p} = (2-\xi)$.

The constructions from $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ are particularly useful for coding applications to fading channels (recall from Proposition 2 that $\mathbb{Z}^{\frac{p-1}{2}}$ is obtained over $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$), as will be discussed in next section.

We conclude this section by mentioning two other families of subfields of $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ that can be used to obtain lattices from codes.

Since the maximal totally real subfield $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r})$ has degree $p^{r-1}(p-1)/2$, its Galois group contains a subgroup of order $p^{r-1}$, namely its unique Sylow $p$-subgroup, which itself contains a cyclic subgroup $P$ of order $p$. Let $K^P$ be the subfield fixed by $P$, which has degree $p^{r-2}(p-1)/2$ over $\mathbb{Q}$. Let $\mathfrak{p}$ be the prime in $K^P$ above $p$. As before

$$p^{r-1}\frac{(p-1)}{2} = e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p)$$

and thus $\mathfrak{p}$ is totally ramified. Let $C \subset \mathbb{F}_p^N$ be a $k$-dimensional code with $C \subset C^\perp$. Then the field $K^P$ enables the construction of lattices of rank $Np^{r-2}(p-1)/2$, with respect to the bilinear form $\langle x, y\rangle = \sum_{i=1}^N \mathrm{Tr}_{K^P/\mathbb{Q}}(x_i y_i/p)$.

When $r = 2$, $K^+ = \mathbb{Q}(\zeta_{p^2} + \zeta_{p^2}^{-1})$ contains a subextension of degree $p$ over $\mathbb{Q}$, which again, as above, provides lattices of rank $N\frac{p-1}{2}$ from a code $C$ with $C \subset C^\perp$.

**Example 24.** Take $p = 5$, $r = 2$ and $K = \mathbb{Q}(\zeta_{25})$ contains the subfield of degree 5, given by the minimal polynomial

$$p(X) = X^5 - 10X^3 + 5X^2 + 10X + 1.$$

## 5.4 Wiretap Encoding of Ideal Lattices for Block Fading Channels

In this section, we focus on the application to wiretap encoding for block fading channels.

Let $K$ be a totally real number field of degree $n$ with $n$ embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n$ of $K$ into $\mathbb{C}$ and ring of integers $\mathcal{O}_K$. As before, $K$ is assume to contain a prime $\mathfrak{p}$ above $p$ which totally ramifies. Let $C \subset C^{\perp}$ be a linear $(N, k)$ code, with generator matrix

$$G = \begin{pmatrix} I_k & A \end{pmatrix}.$$

Recall that $x_j \in \mathcal{O}_K$ is written as $x_j = \sum_{l=1}^{n} x_{jl}\nu_l$ in an integral basis $\nu_1, \ldots, \nu_n$, and that

$$\sigma(x_j) = (\sigma_1(x_j), \ldots, \sigma_n(x_j))$$

is the canonical embedding of $K$.

A lattice point $\mathbf{x}$ in $\Gamma_C$ is given by

$$\mathbf{x} = (\sigma(x_1), \ldots, \sigma(x_k), \sum_{j=1}^{k} a_{j1}\sigma(x_j) + \sigma(x'_{k+1}), \ldots, \sum_{j=1}^{k} a_{j,N-k}\sigma(x_j) + \sigma(x'_N))$$

with $x'_{k+1}, \ldots, x'_N \in \mathfrak{p}$, which can be rearranged into an $n \times N$ matrix $X$ as follows:

$$X = \left(\sigma(x_1)^T, \ldots, \sigma(x_k)^T, (\textstyle\sum_{j=1}^{k} a_{j1}\sigma(x_j) + \sigma(x'_{k+1}))^T, \ldots, (\sum_{j=1}^{k} a_{j,N-k}\sigma(x_j) + \sigma(x'_N))^T\right)$$

that is, with normalization,

$$X = \frac{1}{\sqrt{p}} \begin{pmatrix} \sigma_1(x_1) & \ldots & \sigma_1(\sum_{j=1}^{k} a_{j1}x_j + x'_{k+1}) & \ldots & \sigma_1(\sum_{j=1}^{k} a_{j,N-k}x_j + x'_N) \\ \sigma_2(x_1) & \ldots & \sigma_2(\sum_{j=1}^{k} a_{j1}x_j + x'_{k+1}) & \ldots & \sigma_2(\sum_{j=1}^{k} a_{j,N-k}x_j + x'_N) \\ \vdots & & \vdots & & \vdots \\ \sigma_n(x_1) & \ldots & \sigma_n(\sum_{j=1}^{k} a_{j1}x_j + x'_{k+1}) & \ldots & \sigma_n(\sum_{j=1}^{k} a_{j,N-k}x_j + x'_N) \end{pmatrix}.$$

Now coset encoding is performed by setting $\Lambda_b = \rho^{-1}(C)/\sqrt{p} = \Gamma_C$ and $\Lambda_e = \mathfrak{p}^N/\sqrt{p}$, using the fact that

$$\frac{\rho^{-1}(C)}{\sqrt{p}} = \frac{1}{\sqrt{p}}\left(\mathfrak{p}^N + C\right) = \frac{1}{\sqrt{p}} \bigcup_{c_i \in C} \left(\mathfrak{p}^N + c_i\right).$$

In words, the choice of $(x_1, \ldots, x_k)$ determines a coset of $\mathfrak{p}^N$, since

$$(\rho(x_1), \ldots, \rho(x_k)) = (\mathfrak{p} + c_{i1}, \ldots, \mathfrak{p} + c_{ik})$$

and consequently

$$\begin{aligned}
&(\rho(x_1), \ldots, \rho(x_k), \textstyle\sum_{j=1}^{k} a_{j1}\rho(x_j), \ldots, \sum_{j=1}^{k} a_{j,N-k}\rho(x_j)) \\
&= (\mathfrak{p} + c_{i1}, \ldots, \mathfrak{p} + c_{ik}, \ldots \mathfrak{p} + c_{in}) \\
&= \mathfrak{p}^N + c_i,
\end{aligned}$$

for $c_i$ a codeword in $C$. This explains why lattices obtained from number fields are good for wiretap encoding.

# Chapter 6

# Conclusion and Future Works

This thesis is dedicated to the study of lattice codes for wiretap fading channels. It begins by addressing the questions of designing wiretap lattice codes for both fast fading and slow fading channels.

For fast fading channels, using our derived upper bound on Eve's probability of correctly decoding the confidential message intended to Bob for finite constellations, we obtain a code design criterion to characterize the confusion that a lattice code induces for Eve. Since ideal lattices are known to be suited for transmission between Alice and Bob over fast fading channels, we rewrite the code design criterion in terms of ideal lattices, which translates into a sum of inverse algebraic norms in number fields. Using the new derived code design criterion, this thesis studies these sums of inverse norms over certain number fields. In particular, elements of small norms have the biggest contributions to these sums. From there, we narrow down our study to number fields where small primes are inert, so as to prevent the existence of nonunit elements of small norms. This is motivated by the computation using examples of fields where elements which are not units but have small norms contribute as much as the units to overall sum. After that, by relating the regulator with the existence of units, we identify those number fields with less units. We notice that current bounds on the regulator seem to characterize the behavior of the sum of inverse norms, even for small constellation sizes. This gives a first set of number fields candidate to provide good lattice wiretap codes.

The picture for wiretap lattice codes is however more complex, since it involves the design of not only $\Lambda_e$ (the lattice designed to confuse Eve), but also $\Lambda_b$ (the lattice

that provides reliability for Bob). Though this has not been made completely explicit in this particular context of coset encoding, the discriminant $d_K$ of the number field $K$ is known [2, 10] to play a role in the design of $\Lambda_b$, and in fact, it is usually preferred to be not too big (this is on top of already knowing that the discriminant should not be too large since it is used for normalization). Table 4.3 illustrates how the discriminant $d_K$ grows with the regulator. This suggests that the optimal design might be a trade-off between the discriminant and the regulator, and that further benefits in terms of confusion could be obtained by considering the ramification of small primes. This is a natural direction for further study.

As for slow fading channels, this thesis proposes a construction of lattices over number fields using linear codes over finite fields, mimicking Construction A from binary codes. We study more into details the case of Galois number fields, where there is a prime that totally ramifies. Maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{p^r})$ are particularly considered. Application to coset encoding for block fading wiretap channels is presented, showing why the proposed algebraic lattices are suited for coset encoding, but also to optimize the code design criterion for wiretap codes. Future work involves further study of the obtained lattices. In particular, recall from (3.4), we want to minimize

$$\sum_{\mathbf{x}\in\mathcal{O}_K^N\cap\mathcal{B},\mathbf{x}\neq 0}\frac{1}{|N_{K/\mathbb{Q}}(\|\mathbf{x}\|)|^{N+2}}$$

where $\mathbf{x}=(x_1,...,x_N)$, $x_i\in\mathcal{O}_K$, and finding among algebraic lattices those which further optimize this design criterion is open.

# References


[1] E. Bayer-Fluckiger. Lattices and number fields. *Contemporary Mathematics*, vol. 241:pp. 69–84, 1999. 33

[2] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. Algebraic lattice constellations: Bounds on performance. *IEEE Transactions on Information Theory*, vol.52, no.1, 2006. 64, 74

[3] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore. Good lattice constellations for both rayleigh fading and gaussian channels. *IEEE Transactions on Information Theory*, vol. 42, n.2:pp. 502–518, 1996. 35, 36

[4] N. Childress. *Class Field Theory.* Springer, 2008. 46

[5] J. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups.* Springer. 5, 58, 69

[6] T. P. da Nbrega Neto, J. O. D. Lopes, and J. C. Interlando. On computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$. *Journal of Number Theory*, 96, 2002. 29

[7] W. Ebeling. *Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch.* Springer, 2013. 5, 7, 58, 66, 67

[8] G.R. Everest and J.H. Loxton. Counting algebraic units with bounded height. *Journal of Number Theory, 44*, 1993. 46

[9] D. Fretwell. *Class Field Theory.* GRIN Verlag, 2013. 22

[10] X. Giraud, E. Boutillon, and J.-C. Belfiore. Algebraic tools to build modulation schemes for fading channels. *IEEE Trans. on Information Theory*, 43, no.3, 1997. 74

[11] J. Harshan, E. Viterbo, and J.-C. Belfiore. Practical encoders and decoders for euclidean codes from barnes-wall lattices. preprint, `http://arxiv.org/abs/1203.3282`. 58

[12] G. J. Janusz. *Algebraic Number Fields*, volume 7. American Mathematical Society, 1996. 25

[13] W. Kositwattanarerk, S.S. Ong, and F. Oggier. Wiretap encoding of lattices from number fields using codes over $\mathbb{F}_p$. *IEEE International Symposium on Information Theory (ISIT) 2013, Istanbul, Turkey, pp. 2612–2616.* 68

[14] S. K. Leung-Yan-Cheong and M. E. Hellman. The gaussian wire-tap channel. *IEEE Transactions on Information Theory*, IT-24, July 1978. 4, 8

[15] Y. Liang, H.V. Poor, and S. Shamai. Information theoretic security. *Now Publisherst*, vol. 5, Issue 4–5, 2009. 4

[16] F. Lin. Lattice coding for the gaussian wiretap channel-a study on the secrecy gain. *NTU PhD Thesis*, 2013. 8

[17] F. Lin and F. Oggier. A classification of unimodular lattice wiretap codes in small dimensions. *IEEE Transactions on Information Theory*, to appear, `arxiv.org/pdf/1201.3688`, 2012. 4

[18] F. Lin and F. Oggier. *Coding for wiretap channels in Physical Layer Security in Wireless Communications.* Auerbach Publications, CRC Press, Taylor and Francis Group, November 2013. 4

[19] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé. Semantically secure lattice codes for the gaussian wiretap channel. preprint, `http://arxiv.org/abs/1210.6673`, 2012. 4

[20] D.A. Marcus. *Number Fields.* Springer, 1977. 23, 24, 26

[21] J. Neukirch. *Algebraic Number Theory.* Springer, 1999. 20, 23, 27, 29

[22] F. Oggier and J.-C. Belfiore. Enabling multiplication in lattice codes via construction a. *International Information Theory Workshop (ITW) 2013.* 59, 64

[23] F. Oggier and J.-C. Belfiore. Lattice code design for the rayleigh fading wiretap channel. *International Conference on Communications (ICC 2011)*. 10, 14

[24] F. Oggier, P. Solé, and J.-C. Belfiore. Lattice codes for the wiretap gaussian channel: Construction and analysis. preprint, `http://arxiv.org/abs/1103.4086`, 2011. 4, 5, 8, 10

[25] F. Oggier and E. Viterbo. *Algebraic Number Theory and Code Design for Rayleigh Fading Channels*. Now Publishers Inc, 2005. 5, 9, 15, 35

[26] S.S. Ong and F. Oggier. Lattices from totally real number fields with large regulator. *International Workshop on Coding and Cryptography (WCC) 2013, Bergen, Norway, pp. pp. 438–447*. 42

[27] S.S. Ong and F. Oggier. Lattices from totally real number fields with no small norm elements. *preprint, Special Issue of Designs, Codes and Cryptography 2013*. 11, 14, 45

[28] P. Ribenboim. *Classical Theory of Algebraic Numbers*. Springer, 2001. 20

[29] L.H. Rowen. *Graduate Algebra: Commutative View*. GSM Vol. 73, American Mathematical Society, 2006. 26

[30] P. Samuel. *Algebraic Theory of Numbers*. Dover Publications,Inc, 1970. 29, 33

[31] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters, third edition, 2002. 20, 21, 22, 26, 31

[32] R. Vehkalahti and H.F. Lu. Inverse determinant sums and connections between fading channel information theory and algebra. preprint, `http://arxiv.org/abs/1111.6289`, 2011. 39

[33] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer, 2007. 29, 30, 67

[34] A. Wyner. The wire-tap channel. *Bell.System Tech. Journal*, vol. 54, October 1975. 3, 8