Algebraic Constructions of Modular Lattices

Xiaolu Hou

DIVISION OF MATHEMATICAL SCIENCES

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

Supervised by

Assoc Prof. Frédérique OGGIER

A thesis submitted to the Nanyang Technological University

in partial fulfillment of the requirement for the degree of

Doctor of Philosophy of Mathematics

2017

Acknowledgment

Firstly, I would like to express my sincere gratitude to my supervisor, Assoc. Prof. Frédérique Oggier for her patience, motivation and guidance. Without her supervision and constant help, this thesis would have not been possible. Secondly, I would like to thank Prof. Christian Maire for the fruitful discussions we had together. I also thank the anonymous reviewers of this thesis for their valuable comments. I would also like to thank my collaborator Dr. Lin Fuchun for his help and encouragement. My thanks also go to Dr. Jérôme Ducoat and Dr. Nadya Markin for their help with concepts in algebraic number theory. I thank Dr. Punarbasu Purkayastha for his help with Sage. Last but not least, I would like to thank my family and friends for their constant support. Special thanks to my mother and my boyfriend Jakub for their company and care in my life.

Abstract

This thesis is dedicated to the constructions of modular lattices with algebraic methods. The goal is to develop new methods as well as constructing new lattices. There are three methods considered: construction from number fields, construction from totally definite quaternion algebras over number fields and construction from linear codes via generalized Construction A. The construction of Arakelov-modular lattices, which result in modular lattices, was first introduced in [6] for ideal lattices from cyclotomic fields. We generalize this construction to other number fields and also to totally definite quaternion algebras over number fields. We give the characterization of Arakelov-modular lattices over the maximal real subfield of a cyclotomic field with prime power degree and totally real Galois fields with odd degrees. Characterizations of Arakelov-modular lattices of trace type, which are special cases of Arakelov- modular lattices, are given for quadratic fields and maximal real subfields of cyclotomic fields with non-prime power degrees. Furthermore, we give the classification of Arakelov-modular lattices of level ℓ for ℓ a prime over totally definite quaternion algebras with base field the field of rationals.

Construction A is a well studied method to obtain lattices from codes via quotient of different rings, such as rings of integers, in which case mostly cyclotomic number fields have been considered. In this thesis, we will study Construction A over all totally real and CM fields. Using Construction A, the intersection between a lattice constructed from a linear complementary dual (LCD) code and its dual lattice is investigated. This is an attempt to find an equivalent definition to LCD codes for lattices.

Several new constructions of existing extremal lattices as well as a new extremal lattice are obtained from the above mentioned methods.

The mathematical concepts used in this thesis mainly involve algebraic number theory, class field theory, non commutative algebra and coding theory.

Contents

List of Tables

List of Figures

List of Publications

Conference Proceedings

1. X. Hou, F. Lin, F. Oggier, "Construction and secrecy gain of a family of $5-$modular lattices", in the Proceedings of the *IEEE Information Theory Workshop 2014 (ITW)*, IEEE, 2014.

2. X. Hou, F. Oggier, "On LCD codes and lattices", in the Proceedings of the *IEEE International Symposium on Information Theory 2016 (ISIT)*, IEEE, 2016.

Accepted Journal Papers

1. X. Hou, "Construction of Arakelov-modular lattices over totally quaternion algebras", to appear in *International Journal of Number Theory*, arXiv:1604.02875.

2. X. Hou, F. Oggier, "Modular lattices from a variation of Construction A over number fields", to appear in *Advances in Mathematics of Communications*, arXiv:1604.01583.

Submitted Journal Paper

1. X. Hou, "Construction of Arakelov-modular Lattices from Number Fields", arXiv: 1609.03134.

Chapter 1

Introduction

Lattice theory is a research topic that is related to a broad range of subjects, ranging from theoretical mathematics to real life applications. On the one hand, as lattices can be defined by quadratic forms and $\mathbb{Z}-$modules [22], the characterization and construction of lattices are closely connected to group theory (see e.g. [39, 40]), quadratic forms and abstract algebra [37]. On the other hand, due to the geometric structure of lattices, they are used in packing, covering, quantization and channel coding [19, 64]. Recently, the hardness of the shortest vector problem for lattices pushed the development of an important topic in post-quantum cryptography – lattice-based cryptography [9].

Among the aforementioned different applications of lattices, we will be mainly interested in the following:

- Sphere packing deals with the question of how densely can we put non-overlapping identical spheres in $\mathbb{R}^n$. When lattice points are used as the centers for those spheres we have a lattice packing. The question then becomes – what kind of lattice gives the densest lattice packing in $\mathbb{R}^n$?

- Kissing number problem asks how many identical spheres can be placed so that there is one central sphere which touches all the other spheres. Similar to lattice packing, taking the centers of spheres to be lattice points, people are interested in finding the highest possible kissing number for lattices in different dimensions.

- Coding theory is closely related to lattices in the setting of a wiretap channel, which consists of a sender, a legitimate receiver and an eavesdropper. Lattice codes are used to give confusion to the eavesdropper while guaranteeing integrity of information for the receiver.

More details about those motivations will be discussed in Chapter 2.

Early studies on lattices were focusing on unimodular lattices for their relation with modular forms and sphere packings (see e.g. [48]). Then in 1995, Quebbemann generalized the notion of unimodular lattices to define *modular lattices* [49]. Owing to their structural properties, modular lattices are widely studied and used. For example, by examining the associations between theta series of lattices and modular forms, upper bound on the minimum for some modular lattices were found [36, 51]. Furthermore, the analysis of their secrecy gain as lattice codes for wiretap channel is a new developing research topic [44].

Unsurprisingly, the construction of modular lattices has been gaining attention. The focus of this thesis will be on algebraic constructions of modular lattices. More precisely, we will be looking at three algebraic construction methods: construction from number fields, construction from quaternion algebras and generalized Construction A.

The construction of lattices from number fields was already introduced for unimodular lattices in [25, 15, 14, 4]. This construction obtains lattices from the ideals of rings of integers of number fields and hence the resulting lattices are called ideal lattices [5]. A good reference for the construction method is [19, Chapter 7] (see also [57, Chapter 4], [24, 16, 29, 60]). This method is generalized to construct modular lattices from different number fields by various researchers. In [2], constructions of modular lattices from vector spaces over imaginary quadratic fields are studied. In [6], they introduced the definition of Arakelov-modular lattices from CM fields and characterized the existence of Arakelov-modular lattices over cyclotomic fields. In Chapter 3, we will generalize this construction to quadratic number fields, maximal real subfields of cyclotomic fields and totally real number fields with odd degrees.

Orders of quaternions are a non-commutative generalization of rings of integers for number fields. Naturally, as a generalization of ideal lattices from number fields, ideal lattices constructed from quaternion algebras were also proposed [49, 2]. In Chapter 4, we study ideal lattices constructed from totally definite quaternion algebras over totally real number fields, and generalize the definition of Arakelov-modular lattices over number fields proposed in [6]. In particular, we prove for the case where the totally real number field is $\mathbb{Q}$, that for ℓ a prime integer, there always exists a totally definite quaternion over $\mathbb{Q}$ from which an Arakelov-modular lattice of level ℓ can be constructed. Furthermore, we prove the necessary existence conditions of Arakelov-modular lattices when the number field is either a totally real quadratic field or the maximal subfield of a cyclotomic field.

Another well studied algebraic construction of lattices is Construction A [19, 26], which constructs lattices from linear codes. In Chapter 5, we consider a variation of Construction A of lattices from linear codes based on two classes of number fields, totally real and CM Galois number fields. We propose a generic construction with explicit generator and Gram matrices, then focus on modular and unimodular lattices, obtained in the particular cases of totally real, respectively, imaginary, quadratic fields. Some relevant properties of modular lattices, such as minimal norm, theta series, kissing number and secrecy gain are analyzed. Interesting lattices are exhibited.

Furthermore, in Chapter 6 we will study the properties of another family of lattices that is constructed by Construction A from LCD (linear complimentary codes) codes [38], which are linear codes that trivially intersect their duals. This is an attempt to find an equivalent concept for lattices as to LCD codes. The basic properties of the intersection of a lattice with its dual will be studied and lattices obtained from the intersection of a code with its dual via Construction A are further discussed. Interesting examples are listed.

The computations in this thesis are mostly done by using SAGE [65] and Magma [12].

Chapter 2

Modular Lattices

In this chapter we give the definitions of modular lattice and some of its properties. Furthermore, in Section 2.2, we will discuss the motivations for constructing modular lattices. For the reference of the definitions, we refer the readers to [22, 19].

Definition 2.1. Let M_L be an invertible matrix in $\mathbb{R}^n$, a *lattice* $L \subseteq \mathbb{R}^n$ is defined by

$$L := \{\boldsymbol{x} M_L | \boldsymbol{x} \in \mathbb{Z}^n\}.$$

M_L is called a *generator matrix* of L and $G_L := M_L M_L^\top$ is called a *Gram matrix* of L.

Hence a lattice $L \subseteq \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$ [22, p.2]. In particular it is a free $\mathbb{Z}-$module of rank n. Another more algebraic definition of lattice is

Definition 2.2. A *lattice* is a pair (L, b), where L is a free $\mathbb{Z}-$module and $b : L \otimes_{\mathbb{Z}} \mathbb{R} \times L \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$ is a positive definite symmetric bilinear form.

We can see that the two definitions are equivalent: if L is a free $\mathbb{Z}-$module of rank n with $\mathbb{Z}-$basis $\{v_1, v_2, \ldots, v_n\}$, then (L, b) can be embedded in $\mathbb{R}^n$ as a lattice in the sense of Definition 2.1 with Gram matrix $G_L = (b(v_i, v_j))_{1 \le i,j \le n}$. On the other hand, any lattice $L \subseteq \mathbb{R}^n$ as in Definition 2.1 is associated with the standard Euclidean inner product, which is a positive definite symmetric bilinear form.

Example 2.3. Take $M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, we get the lattice $\mathbb{Z}^2 = \{(x_1, x_2) \in \mathbb{R}^2 : x_1, x_2 \in \mathbb{Z}\}$ with Gram matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. In the terminology of Definition 2.1, this lattice is the pair $(\mathbb{Z}^2, (\cdot, \cdot))$,

where $(\cdot,\cdot)$ is the Euclidean inner product:

$$\begin{aligned} \mathbb{R}^2 \times \mathbb{R}^2 &\rightarrow \mathbb{R} \\ ((x_1,x_2),(y_1,y_2)) &\mapsto x_1y_1 + x_2y_2. \end{aligned}$$

Note that the lattices we consider here are all *full rank* (see [19, p.43]), i.e. latices in Euclidean space of dimension n with generator matrices also with rank n. In this thesis, we will use Definition 2.2, but identify a lattice (L,b) with its embedding in $\mathbb{R}^n$ and sometimes we write L instead of (L,b) for simplicity.

2.1 Definitions

Let (L,b) be a lattice of *dimension* n (i.e. L is a free $\mathbb{Z}-$module of rank n) with generator matrix M_L and Gram matrix G_L. The set of rows of M_L, say $\{v_1,v_2,\ldots,v_n\}$, is called a *basis* of L, it forms the *fundamental parallelotope*

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n | 0 \leq \lambda_i < 1\}$$

of L. The volume of this fundamental parallelotope is called the *volume* of L, i.e.

$$vol(L) = vol(P) = |\det(M_L)|.$$

The square of the volume of L gives the *discriminant* of L:

$$disc(L) = \det(G_L) = \det(M_L)^2.$$

We define the *dual* of the lattice (L,b) to be the lattice (L^*,b), where

$$L^* := \{x \in L \otimes_{\mathbb{Z}} \mathbb{R} | b(x,y) \in \mathbb{Z}\ \forall y \in L\}.$$

If M is a generator matrix for L, then $M^* := (M^\top)^{-1}$ is a generator matrix for L^*.

If $L \subseteq L^*$, L is called *integral* and in this case [22]

$$vol(L) = vol(L^*)|L^*/L|, \quad disc(L) = |L^*/L|.$$

By the definition of Gram matrix, a lattice is integral if and only if its Gram matrix has

integral entries.

Definition 2.4. Two lattices (L_1, b_1) and (L_2, b_2) are said to be isometric if there exists a $\mathbb{Z}-$module isomorphism $\tau : L_1 \to L_2$ satisfying $b_2(\tau(x), \tau(y)) = b_1(x, y)$for all $x, y \in L_1$[22, p.3].

Definition 2.5. For an integral lattice (L, b) and a positive integer ℓ, if $(L^*, \ell b)$ is isometric to (L, b), i.e. if there exists a $\mathbb{Z}-$module isomorphism $\tau : L^* \to L$ such that $b(\tau(x), \tau(y)) = \ell b(x, y)$ for all $x, y \in L^*$, then L is called $\ell-$*modular* or *modular of level* ℓ [49].

When $\ell = 1$, we have a unimodular lattice.

Example 2.6. Consider the lattice $(L, (\cdot, \cdot))$ with generator matrix $M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}$, where $(\cdot, \cdot)$ is the Euclidean inner product. Then the lattice $(L^*, 5(\cdot, \cdot))$ has generator matrix $\sqrt{5}M^* = \sqrt{5}(M^\top)^{-1} = \begin{bmatrix} \frac{\sqrt{5}-1}{2} & \frac{1+\sqrt{5}}{2} \\ 1 & -1 \end{bmatrix}$. Recall that the set of rows of a generator matrix for a lattice forms its basis. By a change of basis, the matrix $M' = \begin{bmatrix} 1 & -1 \\ \frac{1+\sqrt{5}}{2} & \frac{\sqrt{5}-1}{2} \end{bmatrix}$ is also a generator matrix for $(L^*, 5(\cdot, \cdot))$. We have

$$M = M' \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

thus the map $\tau : (L^*, 5(\cdot, \cdot)) \to (L, (\cdot, \cdot))$, where τ is the reflection w.r.t. $x-$axis, establishes an isometry between $(L, (\cdot, \cdot))$ and $(L^*, 5(\cdot, \cdot))$. By definition, $(L, (\cdot, \cdot))$ is a $5-$modular lattice. This is further illustrated in Figure 2.1.

The constructions of $\ell-$modular lattices will be the main focus of this thesis. Besides the construction method, we will also analyze certain properties of the lattices. Definitions of the related properties are as follows:

Definition 2.7. For an integral lattice (L, b)

1. (L, b) is called *even* if $b(x, x) \in 2\mathbb{Z}$ for all $x \in L$ and *odd* otherwise.
2. The *minimum*, or *minimal norm*, of (L, b), denoted by μ_L, is

$$\min\{b(x, x) : x \in L, x \neq 0\}.$$

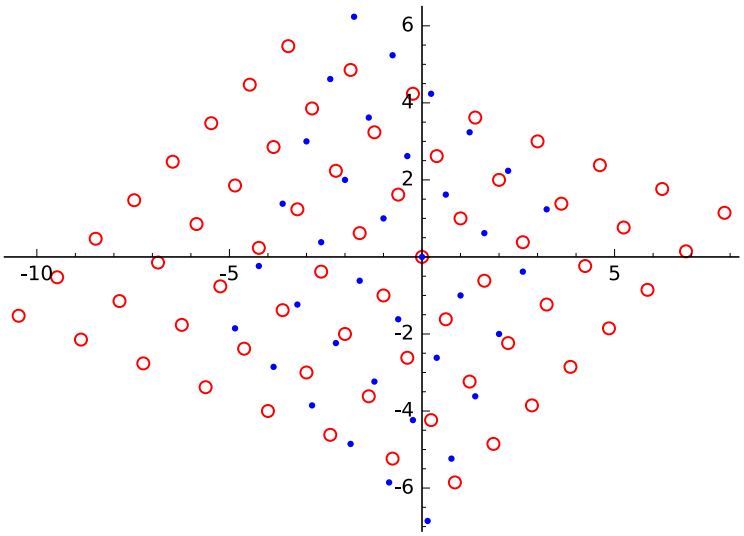

Figure 2.1: Lattice $(L, (\cdot,\cdot))$ (red circles) can be obtained from $(L^*, 5(\cdot,\cdot))$ (blue dots) by reflection w.r.t. $x-$axis, where L is the $5-$modular lattice from Example 2.6.

3. The *kissing number* of (L, b) is the cardinality of the set

$$\{x \in L : b(x,x) = \mu_L\}.$$

4. Let $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\,(\tau) > 0\}$. For $\tau \in \mathbb{H}$ let $q = e^{\pi i \tau}$. The *theta series* of the lattice L is the function

$$\Theta_L(\tau) := \sum_{\boldsymbol{x} \in L} q^{\|\boldsymbol{x}\|^2} = \sum_{m \in \mathbb{Z}_{\geq 0}} A_m q^m,$$

where the second equality holds because we took L to be integral and $A_m = |\{\boldsymbol{x} : \boldsymbol{x} \in L,\ \|\boldsymbol{x}\|^2 = m\}|$.

From the definitions we can see that the coefficient of q in the second term of Θ_L gives the kissing number of L, and the power of q in the second term gives its minimum.

Example 2.8. The lattice $(\mathbb{Z}^2, (\cdot,\cdot))$ in Example 2.3 has volume 1 and discriminant 1. Its dual is given by

$$\mathbb{Z}^* = \{(y_1, y_2) \in \mathbb{R}^2 : x_1 y_1 + x_2 y_2 \in \mathbb{Z}\ \forall x_x, x_2 \in \mathbb{Z}\} = \mathbb{Z}^2.$$

Thus it is an odd unimodular lattice. It has minimum 1 and its kissing number is given by

$$\left|\{(x_1, x_2) \in \mathbb{Z} : x_1^2 + x_2^2 = 1\}\right| = |\{(\pm 1, 0), (0, \pm 1)\}| = 4.$$

As mentioned earlier, in this thesis we give new constructions of several existing ex-

tremal lattices as well as a new extremal lattice. To give the definition of *extremal lattices*, we need the following terminologies:

Definition 2.9. 1. For a positive integer ℓ, an $\ell-$modular lattice (L, b) is said to be *strongly $\ell-$modular* if (L, b) is isometric to the lattice $(L^* \cap \frac{1}{m}L, mb)$ for all exact divisors m of ℓ (i.e. $m|\ell$ and $\gcd(\ell/m, m) = 1$) [50].

2. Two lattices (L_1, b_1) and (L_2, b_2) are said to be rationally equivalent if there exists a $\mathbb{Q}-$linear isomorphism

$$\varphi : L_1 \otimes_{\mathbb{Z}} \mathbb{Q} \to L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$$

such that $b_2(\varphi(x), \varphi(y)) = b_1(x, y)$ for all $x, y \in L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ (see [8, p.93] and [35, p.42]).

3. For a positive integer ℓ, define [51]

$$C^{(\ell)} = \sum_{d|\ell} \sqrt{d}\mathbb{Z}.$$

Remark 2.10. From the definition, for $\ell = 1$ or ℓ a prime, an $\ell-$modular lattice is also strongly $\ell-$modular.

In general, the upper bound on the minimum of a modular lattice is unknown. But for some special cases, the upper bounds were established, which then leads to the definition of *extremal lattice*.

Definition 2.11. Assume $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$. For each ℓ, define the corresponding D_ℓ to be respectively $\{24, 16, 12, 8, 8, 6, 4, 4, 4, 2\}$. Let (L, b) be a strongly $\ell-$modular lattice with minimum μ_L and dimension n such that (L, b) satisfies one of the three conditions:

1. Unimodular;
2. Even;
3. Odd and rationally equivalent to the direct sum of $n/\mathrm{Dim}C^{(\ell)}$ copies of $C^{(\ell)}$;

Then [49, 50, 51]

$$\mu_L \leq 2\left\lfloor \frac{n}{D_\ell} \right\rfloor + 2.$$

Unless (L, b) satisfies condition 3 above and ℓ is odd with $n = D_\ell - \mathrm{Dim}C^{(\ell)}$, then $\mu_L \leq 3$.

A lattice (L, b) which satisfies the above assumptions and also achieves the corresponding upper bound on minimum is called *extremal*.

For a detailed list of extremal lattices we refer the reader to the on-line lattice catalogue [56].

2.2 Motivations

The motivations to study modular lattices are from both mathematical interest and practical applications of lattices.

Number fields and quaternions. As the ring of integers of a number field and an order of a quaternion algebra are both $\mathbb{Z}-$modules, the construction and characterization of lattices can be related to the properties of number fields and quaternions. More precisely, the definition of the positive definite symmetric bilinear form associated to a lattice is from the trace form of the number fields (resp. quaternions), which then connects to the different of the ring of integers (resp. maximal orders). And the different gives us information about the ramification of ideals. The connections will be more clearly elaborated in the rest of this thesis.

Minimum and sphere packing. *Sphere packing* states the following problem [19]: how densely can we put infinitely many non-overlapping $(n-1)-$spheres in $\mathbb{R}^n$? Here, the *density* is defined to be the proportion of the space that is occupied by the spheres and an $(n-1)-$sphere refers to a unit sphere in $\mathbb{R}^n$ [1, p.16]. In particular, if we use a lattice $L \subset \mathbb{R}^n$ for sphere packing, we have a *lattice packing*. The question then becomes: if we draw spheres of radius

$$r = \frac{1}{2}\mu_L$$

with centers at points $x \in L$, what is the largest possible density? Recall the volume of (L, b) is defined to be the volume of the fundamental parallelotope of L:

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n | 0 \leq \lambda_i \leq 1\},$$

where $v_1, v_2, \ldots, v_n$ are the rows of a generator matrix of L. Note that this fundamental parallelotope is a building block for L, i.e. when we repeat this parallelotope infinitely many times to fill the whole space, there is exactly one lattice point in each copy. Hence the density for a lattice packing using the lattice (L, b) is

$$\frac{\text{volume of one sphere}}{\text{volume of fundamental parallelotope}} = \frac{\text{volume of one sphere}}{vol(L)}.$$

In the case when (L, b) is an $\ell-$modular lattice, we have $vol(L) = \ell^{n/4}$ [49, 50]. Since the volume of an $(n-1)-$sphere of radius r is $V_{n-1}r^n$ [19], where V_{n-1} is the volume of an $(n-1)-$sphere of radius 1, the density of the lattice packing is then given by

$$\frac{V_{n-1}r^n}{\ell^{n/4}}.$$

We can see that if the minimum of an $\ell-$modular lattice is bigger, the resulting lattice packing is denser.

Kissing number. Closely related to sphere packing is the so-called *kissing number* problem [22, Section 4.2]: given an $(n-1)-$sphere, what is the maximal number of (non-overlapping) $(n-1)-$spheres touching it? For lattice packing, this kissing number is given by the number of vectors whose length is equal to the minimum of the lattice, which are called *shortest vectors*.

Coding theory. Another motivation for studying lattices is from coding theory: An additive white Gaussian noise (AWGN) channel is a communication channel with a sender Alice, a receiver Bob and the noise is assumed to follow a Gaussian distribution [19, p.67]. Lattices can be used for encoding in such a channel: the transmitted signal is represented by a lattice point in Euclidean space and the decoding rule is to decode the received message to the nearest lattice point [19, p.69]. When the noise is big, the received message may be decoded to a wrong lattice point, resulting in a decoding error. For AWGN channels, lattices with higher densities are preferred so that the energy cost at the transmitter is low while still achieving a small error probability. Furthermore, if an eavesdropper (or wiretapper) Eve is also present in the channel, the channel is then called a Gaussian wiretap channel [63, 31]. Lattices can be used for encoding in such a channel by a coset encoding strategy [44]: take a lattice L_b and a sublattice $L_e \subset L_b$, consider the cosets L_b/L_e. A message that Alice intends to Bob is first mapped to a coset in L_b/L_e, then a random lattice point from the coset is chosen to be the encoded message. A good choice of the nested lattices $L_e \subset L_b$ should ensure reliability for Bob and induce confusion for Eve. In this thesis we are interested in one lattice encoding design criterion, *secrecy gain* [44], which gives an upper bound on Eve's knowledge of the encoded message. In Chapter 5, we will construct some examples of $\ell-$modular lattices for different values of ℓ and look at the relation between secrecy gain and the modularity ℓ of a lattice.

Chapter 3

Constructions from Number Fields

Recall that for a positive integer ℓ, a lattice (L, b) is said to be $\ell-$modular (or modular of level ℓ) if (L, b) is isometric to $(L^*, \ell b)$ (see Definition 2.5), where

$$L^* = \{x \in L \otimes_{\mathbb{Z}} \mathbb{R} : b(x, y) \in \mathbb{Z}\ \forall y \in L\}.$$

An *Arakelov-modular lattice* [6] of level ℓ is an ideal lattice constructed from a CM field such that this ideal lattice can be obtained from its dual by multiplication of an element with absolute value ℓ, which then gives an $\ell-$modular lattice (see Definition 3.2). Given an integer ℓ, in [6], the authors characterized all cyclotomic fields in which there exists an Arakelov-modular lattice of level ℓ. We would like to generalize this definition to a totally real number field and study the existence criteria of Arakelov-modular lattices over any totally real number fields or CM fields. Furthermore, we give the characterization of existence of Arakelov-modular lattices over the maximal real subfield of a cyclotomic field with prime power degree (Section 3.4.2) and totally real Galois fields with odd degrees (Section 3.4.4). Characterizations of Arakelov-modular lattices of trace type, which are special cases of Arakelov-modular lattices, are given for imaginary quadratic fields (Section 3.3.1), totally real quadratic fields (Section 3.4.1) and maximal real subfields of cyclotomic fields with non-prime power degrees (Section 3.4.3).

The necessary algebraic number theory background needed is given in Section 3.1. In Section 3.2, general criteria for the existence of Arakelov-modular lattices over totally real number fields or CM fields are discussed. The necessary and sufficient conditions for the existence of Arakelov-modular lattices are presented in Section 3.3 for CM fields and in Section 3.4 for totally real number fields. In Section 3.5 we list some examples of lattices constructed by the methods presented. In particular, one new extremal lattice will be given.

3.1 Number Fields

The materials from this section can be found in different books on algebraic number theory, see e.g. [21, 42, 59].

A *number field*, normally denoted by K in this thesis, is defined to be a finite field extension of the field of rational numbers, $\mathbb{Q}$. Namely, there exists a *basis* $\{v_1, v_2, \ldots, v_n\}$ consisting of elements from $K^\times := \{x \in K : x \neq 0\}$ such that K can be generated by this basis over $\mathbb{Q}$ and we say that K is of *degree* n, denoted by $[K : \mathbb{Q}] = n$. Furthermore, the elements of this basis can be chosen from the *ring of integers* of K, $\mathcal{O}_K$:

$$\mathcal{O}_K = \{x : x \in K \text{ such that } x \text{ satisfies a monic polynomial with integral coefficients}\}.$$

As suggested by the name, $\mathcal{O}_K$ is actually a ring. For this particular ring, a more generalized notion of ideals is studied: *fractional ideals*, which are finitely generated $\mathcal{O}_K-$submodules of K. They form an abelian group on the set of nonzero prime ideals of $\mathcal{O}_K$: every fractional ideal $\mathfrak{a}$ admits a unique representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \tag{3.1}$$

with $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for almost all $\mathfrak{p}$, where $\mathfrak{p}$ denotes a prime ideal of $\mathcal{O}_K$. Note that since $\mathcal{O}_K$ is a free $\mathbb{Z}-$module of rank n, fractional ideals are also free $\mathbb{Z}-$modules with rank n.

Take a prime integer $p \in \mathbb{Z}$, then the ideal generated by p in $\mathcal{O}_K$ satisfies

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{3.2}$$

for prime ideals $\mathfrak{p}_i$ and integers e_i, g. The exponent e_i is called the *ramification index*, and the degree of the field extension

$$f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}_p] \tag{3.3}$$

is called the *inertia degree* of $\mathfrak{p}_i$ over p. We have

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

- If $g = e_1 = 1$, p is said to be *inert*.
- If $e_i > 0$, $\mathfrak{p}_i$ is said to be *ramified*.
- If $e_1 = n$, p is said to be *totally ramified*.
- If $g = n$, p is said to be *split completely*.

For a number field of degree n, there are exactly n $\mathbb{Q}-$embeddings of K into $\mathbb{C}$, which we denote by $\sigma_1, \ldots, \sigma_n$. Hence each $\sigma_i : K \to \mathbb{C}$ is a field homomorphism that becomes the identity map on $\mathbb{Q}$.

- If $\sigma_i(K) \subseteq \mathbb{R}$ for all i, then K is said to be *totally real*.
- If there exists $F \subseteq K$, a totally real number field such that $[K : F] = 2$ and $\sigma_i(K) \nsubseteq \mathbb{R}\ \forall 1 \leq i \leq n$, then K is said to be a *CM field*.
- If $\sigma_i(K) = K$ for all i, then K is said to be a *Galois extension* of $\mathbb{Q}$. In this case, we use $\mathrm{Gal}(K/\mathbb{Q})$ to denote the set $\{\sigma_1, \ldots, \sigma_n\}$ and refer to it as the *Galois group* of $K/\mathbb{Q}$. Moreover, for (3.2) we would have $e_1 = e_2 = \cdots = e_g$. We denote this integer by e_p and refer to it as the *ramification index* of p. For (3.3), similarly we have $f_1 = f_2 = \cdots = f_g$. We denote this integer by f_p and refer to it as the *inertia degree* of p.

Take any $x \in K$, the *trace* of x, denoted by $\mathrm{Tr}_{K/\mathbb{Q}}(x)$, and the *norm* of x, $\mathrm{N}_{K/\mathbb{Q}}(x)$, in $K/\mathbb{Q}$ are given by:

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

When the field extension is clear from the context, the subscript $K/\mathbb{Q}$ will be omitted.

A basis of $\mathcal{O}_K$ over $\mathbb{Z}$, say $\{v_1, v_2, \ldots, v_n\}$, is also a basis of K over $\mathbb{Q}$. The *discriminant* of K is defined to be the determinant of the matrix $(\mathrm{Tr}(v_i v_j))_{i,j}$. The discriminant of K contains a lot of information about the number field. For example, in this thesis, we will study extensively one ideal - the *different* of K, $\mathcal{D}_K$ - whose inverse, which is a fractional ideal, is given by

$$\mathcal{D}_K^{-1} = \{x : x \in K, \mathrm{Tr}(xy) \in \mathbb{Z}\ \forall x \in \mathcal{O}_K\}, \tag{3.4}$$

and is called the *codifferent*. Let Δ_K denote the absolute value of the discriminant of K, then

$$|\mathcal{O}_K/\mathcal{D}_K| = \Delta_K.$$

3.2 Arakelov-modular Lattices

Let K be a totally real number field or a CM field with degree n and ring of integers $\mathcal{O}_K$. We consider K to be a Galois extension with Galois group $G = \{\sigma_1 = \text{identity}, \sigma_2, \ldots, \sigma_n\}$.

For K CM, we assume σ_{i+1} is the conjugate of σ_i, $(i = 1, 3, 5, \ldots, n-1)$. An *ideal lattice* [5] over K is a pair (I, b_α), where I is a fractional $\mathcal{O}_K-$ideal, $\alpha \in K^\times$ is totally positive (i.e. $\sigma_i(\alpha) > 0, 1 \leq i \leq n$) and

$$\begin{aligned} b_\alpha : I \times I &\to \mathbb{R} \\ (x, y) &\mapsto \mathrm{Tr}\left(\alpha x \bar{y}\right), \end{aligned}$$

is a positive definite symmetric bilinear form. Here Tr is the trace map on $K/\mathbb{Q}$, the conjugate $^-$ is complex conjugation and it is understood to be the identity map when K is totally real.

Remark 3.1. We would like to point out that by the above definition, for any $u \in K$, $b_\alpha(ux, y) = b_\alpha(x, \bar{u}y)$ (c.f. Lemma 4.3).

Note that here we consider the following twisted canonical embedding of $K \hookrightarrow \mathbb{R}^n$:

$$x \mapsto (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_n(\alpha)}\sigma_n(x))$$

for K totally real and

$$x \mapsto \sqrt{2}(\sqrt{\sigma_1(\alpha)}\mathrm{Re}\left(\sigma_1(x)\right), \sqrt{\sigma_2(\alpha)}\mathrm{Im}\left(\sigma_2(x)\right), \ldots, \sqrt{\sigma_{n-1}(\alpha)}\mathrm{Re}\left(\sigma_{n-1}(x)\right), \sqrt{\sigma_n(\alpha)}\mathrm{Im}\left(\sigma_n(x)\right))$$

for K CM. More specifically, a *generator matrix* for (I, b_α) as a lattice in $\mathbb{R}^n$ is given by

$$\begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_n) \end{bmatrix} \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \sqrt{\sigma_n(\alpha)} \end{bmatrix}$$

for K totally real and it is given by

$$\sqrt{2}\begin{bmatrix} \mathrm{Re}\left(\sigma_1(\omega_1)\right) & \mathrm{Im}\left(\sigma_2(\omega_1)\right) & \ldots & \mathrm{Re}\left(\sigma_{n-1}(\omega_1)\right) & \mathrm{Im}\left(\sigma_n(\omega_1)\right) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathrm{Re}\left(\sigma_1(\omega_n)\right) & \mathrm{Im}\left(\sigma_2(\omega_n)\right) & \ldots & \mathrm{Re}\left(\sigma_{n-1}(\omega_n)\right) & \mathrm{Im}\left(\sigma_n(\omega_n)\right) \end{bmatrix} \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \sqrt{\sigma_n(\alpha)} \end{bmatrix}$$

for K CM, where $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}-$basis for I.

Let $\mathcal{D}_K$ be the different of $K/\mathbb{Q}$. Recall that $\mathcal{D}_K^{-1} = \{x \in K : \mathrm{Tr}\left(xy\right) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}$. Then for an ideal lattice (I, b_α), its dual lattice is given by (I^*, b_α), where $I^* = \alpha^{-1}\mathcal{D}_K^{-1}\bar{I}^{-1}$ [6].

We generalize the definition of Arakelov-modular lattices over CM fields defined in [6] to totally real number fields:

Definition 3.2. Let ℓ be a positive integer, an ideal lattice (I, b_α) is said to be *Arakelov-modular of level* ℓ if there exists $\beta \in K^\times$ such that $I = \beta I^*$ and $\ell = \beta\bar{\beta}$.

For an Arakelov-modular lattice (I, b_α) of level ℓ, define $\varphi : I^* \to I$ to be $x \mapsto \beta x$, then $\ell b_\alpha(x, y) = b_\alpha(\varphi(x), \varphi(y))$. If furthermore, (I, b_α) is an integral lattice, then it is $\ell-$modular. But this is always true. For any fractional ideal $\mathfrak{a}$ and prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$, let $v_{\mathfrak{P}}(\mathfrak{a})$ denote the exponent of $\mathfrak{P}$ in the factorization of $\mathfrak{a}$ (see (3.1)), we have

Lemma 3.3. An Arakelov-modular lattice is integral.

Proof. Let (I, b_α) be an Arakelov-modular lattice of level ℓ and $\beta \in K$ such that $\ell = \beta\bar{\beta}$ and $I = \beta I^*$. If K is totally real, β satisfies the monic polynomial $x^2 - \ell \in \mathbb{Z}[x]$ and hence $\beta \in \mathcal{O}_K$. If K is CM, $I^* = \beta^{-1} I = \alpha^{-1}\mathcal{D}_K^{-1}\bar{I}^{-1}$ gives $\beta\mathcal{O}_K = \alpha\mathcal{D}_K I\bar{I}$. Take any prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$, we have $v_{\mathfrak{P}}(\beta) = v_{\bar{\mathfrak{P}}}(\beta)$. So $v_{\mathfrak{P}}(\beta) = \frac{1}{2} v_{\mathfrak{P}}(\ell) \geq 0$ and hence $\beta \in \mathcal{O}_K$.

For both cases we can conclude that $I = \beta I^* \subseteq I^*$ and we have (I, b_α) is integral. □

For simplicity, we write (I, α) instead of (I, b_α). When $\alpha = 1$ we say this lattice is of *trace type* [6]. For any prime integer p, let e_p denote its ramification index. Define

$$\begin{aligned} \Omega(K) &= \{p | p \text{ is a prime that ramifies in } K/\mathbb{Q}\}. \\ \Omega'(K) &= \{p | p \in \Omega(K) \text{ and } e_p \text{ is even}\}. \end{aligned}$$

We have

Lemma 3.4. Suppose there exists an Arakelov-modular lattice of level ℓ over K, where ℓ is square-free.

1. If K is totally real, $\ell | \prod_{p \in \Omega'(K)} p$. In particular, if K has an odd degree, we have $\ell = 1$.
2. If K is CM and its degree is not a multiple of 4, then $\ell | \prod_{p \in \Omega'(K)} p$.

Proof. 1. First we consider K totally real. By the definition of Arakelov-modular lattice, there exists $\beta \in K^\times$ such that $\ell = \beta\bar{\beta} = \beta^2$. We then have $\sqrt{\ell} \in K$, which gives $\mathbb{Q}(\sqrt{\ell}) \subseteq K$. As $\ell | \prod_{p \in \Omega'(\mathbb{Q}(\sqrt{\ell}))} p$ and K is Galois, we have $\ell | \prod_{p \in \Omega'(K)} p$. If furthermore, K has an odd degree, any prime that ramifies in K has an odd ramification index and we can conclude $\ell = 1$.

2. If K is CM with degree not a multiple of 4, then $\sqrt{-1} \notin K$, by Remark 3.5 of [6], $\sqrt{\ell} \in K$ or $\sqrt{-\ell} \in K$. Hence $\mathbb{Q}(\sqrt{\ell}) \subseteq K$ or $\mathbb{Q}(\sqrt{-\ell}) \subseteq K$. Similarly as above, for both cases, we can conclude $\ell | \prod_{p \in \Omega'(K)} p$.

□

From the relation $I^* = \alpha^{-1}\mathcal{D}_K^{-1}\bar{I}^{-1}$ and Definition 3.2 we can see that the existence of Arakelov-modular lattices is closely related to the factorization of primes and the different in a number field K. For cyclotomic fields, the factorization of primes and different are known, which is the main tool for the characterization of Arakelov-modular lattices over cyclotomic fields in [6].

Similarly, factorizations of primes and different can be calculated for quadratic fields and maximal real subfields of cyclotomic fields, hence similar techniques as in [6] were used to develop results in Sections 3.3, 3.4.1, 3.4.2 and 3.4.3.

However in general, it is not easy to calculate the factorization of the different of a number field. Nevertheless, for totally real number fields with odd degrees we will prove in Section 3.4.4 that the factorization of different involves only even exponent of prime ideals, then together with Lemma 3.4 we can characterize the existence of Arakelov-modular lattices over such number fields.

3.3 CM Fields

We first consider the case when K is CM. Let F be the maximal real subfield of K. For a positive integer ℓ, write $\ell = \ell_1\ell_2^2$, where $\ell_1, \ell_2 \in \mathbb{Z}_{>0}$ and ℓ_1 is square-free. If there is an Arakelov-modular lattice (I, α) of level ℓ over K, then the rescaled lattice $(I, \ell_2^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ_1 over K [6, Proposition 3.2]. Here we prove the converse result which allows us to restrict to the case when ℓ is square-free.

Proposition 3.5. Let K be a CM field and ℓ_1 be a square-free positive integer. Assume there is an Arakelov-modular lattice (I, α) of level ℓ_1. Take $\ell = \ell_1\ell_2^2$, where ℓ_2 is a positive integer. Then the rescaled lattice $(\ell_2 I, \ell_2^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ.

Proof. Let (I^*, α) be the dual of (I, α), then $(I^*, \ell_2^{-1}\alpha)$ is the dual of $(\ell_2 I, \ell_2^{-1}\alpha)$. Note that as α is totally positive, $\ell_2^{-1}\alpha$ is also totally positive. By the definition of Arakelov-modular lattice, there exists $\beta_1 \in K$ such that $\ell_1 = \beta_1\bar{\beta}_1$ and $I = \beta_1 I^*$. Let $\beta = \beta_1\ell_2$, then $\ell = \beta\bar{\beta}$ and $\ell_2 I = \ell_2\beta_1 I^* = \beta I^*$, which shows $(\ell_2 I, \ell_2^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ. □

From now on we consider ℓ to be square-free. Moreover, we note that

Proposition 3.6. There exists an Arakelov-modular lattice of level ℓ over K if and only if there exists $\alpha \in K^\times$ totally positive, $\beta \in K^\times$ such that $\ell = \beta\bar{\beta}$ and for any prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$,

1. if $\mathfrak{P} = \bar{\mathfrak{P}}$, $v_{\mathfrak{P}}(\alpha^{-1}\beta\mathcal{D}_K^{-1})$ is even;
2. if $\mathfrak{P} \neq \bar{\mathfrak{P}}$, $v_{\mathfrak{P}}(\alpha^{-1}\beta\mathcal{D}_K^{-1}) = v_{\bar{\mathfrak{P}}}(\alpha^{-1}\beta\mathcal{D}_K^{-1})$.

Proof. By the definition of Arakelov-modular lattice, there exists an Arakelov-modular lattice, say (I, α), if and only if α is totally positive, $\exists\beta \in K^\times$ such that $\ell = \beta\bar{\beta}$ and the decomposition $I\bar{I} = \alpha^{-1}\beta\mathcal{D}_K^{-1}$ is possible, which is equivalent to conditions 1 and 2 above. □

3.3.1 Imaginary Quadratic Number Fields

Suppose $K = \mathbb{Q}(\sqrt{-d})$, where d is a square-free positive integer. For any prime p that ramifies in $K/\mathbb{Q}$, p is totally ramified with a unique $\mathcal{O}_K$ prime ideal above it, which we denote by $\mathfrak{P}_p$.

Proposition 3.7. There exists an Arakelov-modular lattice of level ℓ of trace type over K if and only if $\ell = d$. Moreover, $(I, 1)$, where

$$I = \begin{cases} \mathfrak{P}_2^{-1} & d \equiv 1, 2 \bmod 4 \\ \mathcal{O}_K & d \equiv 3 \bmod 4 \end{cases},$$

is an Arakelov-modular lattice of level d.

Proof. If $d \equiv 1, 2 \bmod 4$, $\Omega'(K) = \Omega(K) = \{p : p|2d\}$, $\mathcal{D}_K = (2\sqrt{-d})$. If $d \equiv 3 \bmod 4$, $\Omega'(K) = \Omega(K) = \{p : p|d\}$, $\mathcal{D}_K = (\sqrt{-d})$. For any $p \in \Omega(K)$,

$$v_{\mathfrak{P}_p}(\mathcal{D}_K) = \begin{cases} 1 & p \text{ odd} \\ 2 & p = 2, d \equiv 1 \bmod 4 \\ 3 & p = 2, d \equiv 2 \bmod 4. \end{cases}$$

Suppose there exists an Arakelov-modular lattice of level ℓ. As $4 \nmid 2$, by Lemma 3.4, we only need to consider ℓ being a divisor of $\prod_{p\in\Omega(K)} p$. Take β such that $\ell = \beta\bar{\beta}$, by the proof

of Lemma 3.3,

$$v_{\mathfrak{P}_p}(\beta) = \frac{1}{2} v_{\mathfrak{P}_p}(\ell) = \begin{cases} 1 & p|\ell \\ 0 & p \nmid \ell \end{cases}.$$

By Proposition 3.6 and the above discussion,

$$\ell = \begin{cases} \prod_{p \text{ odd}, p|d} & d \equiv 1, 3 \bmod 4 \\ 2 \prod_{p \text{ odd}, p|d} & d \equiv 2 \bmod 4 \end{cases} = d.$$

On the other hand, take $\ell = d$. Then $\beta = \sqrt{-d}$ satisfies $\ell = \beta\bar{\beta}$ and

$$\beta \mathcal{D}_K^{-1} = \begin{cases} \frac{1}{2}\mathcal{O}_K & d \equiv 1, 2 \bmod 4 \\ \mathcal{O}_K & d \equiv 3 \bmod 4. \end{cases}$$

Take

$$I = \begin{cases} \mathfrak{P}_2^{-1} & d \equiv 1, 2 \bmod 4 \\ \mathcal{O}_K & d \equiv 3 \bmod 4 \end{cases},$$

then $I\bar{I} = \beta \mathcal{D}_K^{-1}$ shows $(I, 1)$ is an Arakelov-modular lattice of level d. □

Furthermore, we have the following observations:

1. For $d \equiv 3 \bmod 4$, $(\mathcal{O}_K, 1)$ has generator matrix M and Gram matrix G given by

$$M = \sqrt{2} \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & -\frac{\sqrt{d}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix}.$$

   Hence $(\mathcal{O}_K, 1)$ is an even $d-$modular lattice of dimension 2 with minimum 2.

2. For $d \equiv 2 \bmod 4$, $\{1, \frac{\sqrt{-d}}{2}\}$ is a basis for $\mathfrak{P}_2^{-1}$. Then $(\mathfrak{P}_2^{-1}, 1)$ has generator matrix M and Gram matrix G given by

$$M = \sqrt{2} \begin{bmatrix} 1 & 0 \\ 0 & -\frac{\sqrt{d}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 2 & 0 \\ 0 & \frac{d}{2} \end{bmatrix},$$

   which shows $(\mathfrak{P}_2^{-1}, 1)$ is an odd $d-$modular lattice of dimension 2 with minimum 2.

3. For $d \equiv 1 \bmod 4$, $\{1, \frac{1+\sqrt{-d}}{2}\}$ is a basis for $\mathfrak{P}_2^{-1}$. $(\mathfrak{P}_2^{-1}, 1)$ has generator matrix M and

Gram matrix G given by

$$M = \sqrt{2}\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & -\frac{\sqrt{d}}{2} \end{bmatrix},\ G = \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix}.$$

Hence $(\mathfrak{P}_2^{-1}, 1)$ is an odd $d-$modular lattice of dimension 2 with minimum 2.

3.4 Totally Real Number Fields

In this section we consider the case when K is a totally real number field. Let ℓ be a positive integer and write $\ell = \ell_1\ell_2^2$, where $\ell_1, \ell_2 \in \mathbb{Z}_{>0}$ and ℓ_1 is square-free. We have the following.

Proposition 3.8. There exists an Arakelov-modular lattice of level ℓ over K if and only if there exists an Arakelov-modular lattice of level ℓ_1 over K.

Proof. First, let (I, α) be an Arakelov-modular lattice of level ℓ over K, (I^*, α) be the dual lattice. Then $(\ell_2 I^*, \ell_2^{-1}\alpha)$ is the dual lattice of $(I, \ell_2^{-1}\alpha)$. Take $\beta \in K^\times$ such that $I = \beta I^*$, $\ell = \beta^2$. Let $\beta_1 = \frac{\beta}{\ell_2} \in K^\times$, then $\ell_1 = \beta_1^2$ and $I = \beta_1\ell_2 I^*$, which shows $(I, \ell_2^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ_1.

Conversely, let (I, α) be an Arakelov-modular lattice of level ℓ_1 over K and let (I^*, α) be the dual lattice. Then $(I^*, \ell_2^{-1}\alpha)$ is the dual of $(\ell_2 I, \ell_2^{-1}\alpha)$. Take $\beta_1 \in K^\times$ such that $\ell_1 = \beta_1^2$ and $I = \beta_1 I^*$. Let $\beta = \beta_1\ell_2$, then $\ell = \beta^2$ and $\ell_2 I = \ell_2\beta_1 I^* = \beta I^*$, which shows $(\ell_2 I, \ell_2^{-1}\alpha)$ is an Arakelov-modular lattice of level ℓ. □

From now on we consider ℓ to be square-free.

Proposition 3.9. There exists an Arakelov-modular lattice of level ℓ over K if and only if there exists $\alpha \in K^\times$ totally positive, $\beta \in K^\times$ such that $\ell = \beta^2$ and $v_{\mathfrak{P}}(\alpha^{-1}\beta\mathcal{D}_K^{-1})$ is even for any prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$.

Proof. By the definition of Arakelov-modular lattice, there exists an Arakelov-modular lattice, say (I, α), if and only if $\alpha \in K^\times$ is totally positive, $\exists\beta \in K^\times$ such that $\ell = \beta^2$ and the decomposition $I\bar{I} = I^2 = \alpha^{-1}\beta\mathcal{D}_K^{-1}$ is possible, which is equivalent to requiring $v_{\mathfrak{P}}(\alpha^{-1}\beta\mathcal{D}_K^{-1})$ to be even for all prime ideals $\mathfrak{P}$ in $\mathcal{O}_K$. □

3.4.1 Totally Real Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free positive integer. For any prime p that ramifies in $K/\mathbb{Q}$, p is totally ramified with a unique $\mathcal{O}_K$ prime ideal above it, which we denote by $\mathfrak{P}_p$.

Proposition 3.10. There exists an Arakelov-modular lattice of level ℓ of trace type over K if and only if $\ell = d$. Moreover, $(I, 1)$, where

$$I = \begin{cases} \mathfrak{P}_2^{-1} & d \equiv 2, 3 \bmod 4 \\ \mathcal{O}_K & d \equiv 1 \bmod 4 \end{cases},$$

is an Arakelov-modular lattice of level d.

Proof. If $d \equiv 2, 3 \bmod 4$, $\Omega'(K) = \Omega(K) = \{p : p|2d\}$, $\mathcal{D}_K = (2\sqrt{d})$. If $d \equiv 1 \bmod 4$, $\Omega'(K) = \Omega(K) = \{p : p|d\}$, $\mathcal{D}_K = (\sqrt{d})$. For any $p \in \Omega(K)$,

$$v_{\mathfrak{P}_p}(\mathcal{D}_K) = \begin{cases} 1 & p \text{ odd} \\ 2 & p = 2, d \equiv 3 \bmod 4 \\ 3 & p = 2, d \equiv 2 \bmod 4. \end{cases}$$

Suppose there exists an Arakelov-modular lattice of level ℓ. By Lemma 3.4, we only need to consider ℓ being a divisor of $\prod_{p \in \Omega(K)} p$. Take β such that $\ell = \beta^2$, then

$$v_{\mathfrak{P}_p}(\beta) = \frac{1}{2} v_{\mathfrak{P}_p}(\ell) = \begin{cases} 1 & p|\ell \\ 0 & p \nmid \ell \end{cases}.$$

By Proposition 3.9 and the above discussion,

$$\ell = \begin{cases} \prod_{p \text{ odd}, p|d} & d \equiv 1, 3 \bmod 4 \\ 2 \prod_{p \text{ odd}, p|d} & d \equiv 2 \bmod 4 \end{cases} = d.$$

On the other hand, take $\ell = d$. Then $\beta = \sqrt{d}$ satisfies $\ell = \beta^2$ and

$$\beta \mathcal{D}_K^{-1} = \begin{cases} \frac{1}{2}\mathcal{O}_K & d \equiv 2, 3 \bmod 4 \\ \mathcal{O}_K & d \equiv 1 \bmod 4. \end{cases}$$

Take

$$I = \begin{cases} \mathfrak{P}_2^{-1} & d \equiv 2, 3 \bmod 4 \\ \mathcal{O}_K & d \equiv 1 \bmod 4 \end{cases},$$

then $I^2 = \beta \mathcal{D}_K^{-1}$ shows $(I, 1)$ is an Arakelov-modular lattice of level d. □

Furthermore, we have the following observations:

1. For $d \equiv 1 \bmod 4$, $(\mathcal{O}_K, 1)$ has generator matrix M and Gram matrix G given by

$$M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix}.$$

   Hence $(\mathcal{O}_K, 1)$ is an odd $d-$modular lattice of dimension 2 with minimum 2.

2. For $d \equiv 2 \bmod 4$, $\{1, \frac{\sqrt{d}}{2}\}$ is a basis for $\mathfrak{P}_2^{-1}$. Then $(\mathfrak{P}_2^{-1}, 1)$ has generator matrix M and Gram matrix G given by

$$M = \begin{bmatrix} 1 & 1 \\ \frac{\sqrt{d}}{2} & -\frac{\sqrt{d}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 2 & 0 \\ 0 & \frac{d}{2} \end{bmatrix},$$

   which shows $(\mathfrak{P}_2^{-1}, 1)$ is an odd $d-$modular lattice of dimension 2 with minimum 1 for $d = 2$ and minimum 2 otherwise.

3. For $d \equiv 3 \bmod 4$, $\{1, \frac{1+\sqrt{d}}{2}\}$ is a basis for $\mathfrak{P}_2^{-1}$. $(\mathfrak{P}_2^{-1}, 1)$ has generator matrix M and Gram matrix G given by

$$M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix}.$$

   Hence $(\mathfrak{P}_2^{-1}, 1)$ is an even $d-$modular lattice of dimension 2 with minimum 2.

3.4.2 Maximal Real Subfield of a Cyclotomic Field – The Prime Power Case

Let p be an odd prime, r a positive integer and ζ_{p^r} a primitive p^rth root of unity. In this subsection we consider the case $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$. Let $\mathrm{Mod}_T(p^r)$ denote the set of ℓ such that there exists an Arakelov-modular lattice of trace type of level ℓ over $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ and let $\mathrm{Mod}(p^r)$ denote the set of ℓ such that there exists an Arakelov-modular lattice of level ℓ over $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$.

Recall that p is the only prime that ramifies and it is totally ramified with ramification index $\frac{p^r(p-1)}{2}$. From Lemma 3.4 we have

Corollary 3.11. 1. $\mathrm{Mod}_T(p^r) \subseteq \mathrm{Mod}(p^r) \subseteq \{1\}$ if $p \equiv 3 \bmod 4$,

2. $\mathrm{Mod}_T(p^r) \subseteq \mathrm{Mod}(p^r) \subseteq \{1, p\}$ if $p \equiv 1 \bmod 4$.

Let $\mathfrak{P}$ denote the prime ideal in $\mathcal{O}_K$ above p, then [59]

$$v_{\mathfrak{P}}(\mathcal{D}_K) = \frac{1}{2}(p^{r-1}(pr - r - 1) - 1) \equiv \begin{cases} 1 \bmod 2 & p \equiv 1 \bmod 4 \\ 0 \bmod 2 & p \equiv 3 \bmod 4 \end{cases} \tag{3.5}$$

We have the following characterization of Arakelov-modular lattices of trace type. For the more general case, characterizations of Arakelov-modular lattices will be given in Proposition 3.15.

Proposition 3.12. There exists an Arakelov-modular lattice of level ℓ of trace type over $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ if and only if $\ell \in \mathrm{Mod}_T(p^r)$, where $\mathrm{Mod}_T(p^r)$ is given by

1. $\mathrm{Mod}_T(p^r) = \{1\}$, if $p \equiv 3 \bmod 4$;
2. $\mathrm{Mod}_T(p^r) = \emptyset$, if $p \equiv 1 \bmod 8$;
3. $\mathrm{Mod}_T(p^r) = \{p\}$, if $p \equiv 5 \bmod 8$;

Proof. 1. If $p \equiv 3 \bmod 4$, 1 is a square in K with $1 = 1^2$. By (3.5), $v_{\mathfrak{P}}(\mathcal{D}_K^{-1})$ is even. Then by Proposition 3.9, $1 \in \mathrm{Mod}_T(p^r)$. By Corollary 3.11, $\mathrm{Mod}_T(p^r) = \{1\}$.

2. If $p \equiv 1 \bmod 8$, 1 is a square in K with $1 = 1^2$. By (3.5), $v_{\mathfrak{P}}(\mathcal{D}_K^{-1})$ is odd. Then by Proposition 3.9, $1 \notin \mathrm{Mod}_T(p^r)$. Now take $\ell = p$, we have $\sqrt{p} \in \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p) \cap \mathbb{R} \subseteq \mathbb{Q}(\zeta_{p^r}) \cap \mathbb{R} = K$ (see [62] p.17). Let $\beta = \sqrt{p}$, then $\ell = \beta^2$ and $v_{\mathfrak{P}}(\beta) = \frac{1}{4}p^{r-1}(p-1)$ is even. Hence $v_{\mathfrak{P}}(\beta\mathcal{D}_K^{-1})$ is odd and by Proposition 3.9, $p \notin \mathrm{Mod}_T(p^r)$. By Corollary 3.11, $\mathrm{Mod}_T(p^r) = \emptyset$.

3. If $p \equiv 5 \bmod 8$, same as above $1 \notin \mathrm{Mod}_T(p^r)$. Take $\ell = p$. Similarly, let $\beta = \sqrt{p}$, then $\ell = \beta^2$ and $v_{\mathfrak{P}}(\beta) = \frac{1}{4}p^{r-1}(p-1)$ is odd. Hence $v_{\mathfrak{P}}(\beta\mathcal{D}_K^{-1})$ is even and by Proposition 3.9, $p \in \mathrm{Mod}_T(p^r)$. By Corollary 3.11, $\mathrm{Mod}_T(p^r) = \{p\}$. □

Define

$$\begin{aligned} s_1 &:= v_{\mathfrak{P}}(\mathcal{D}_K^{-1}), \\ s_2 &:= \frac{1}{2}v_{\mathfrak{P}}(p) = \frac{1}{4}p^{r-1}(p-1) \end{aligned}$$

From the above proof we have

Corollary 3.13. If $p \equiv 3 \bmod 4$, $(\mathfrak{P}^{\frac{s_1}{2}}, 1)$ is a unimodular lattice over K. If $p \equiv 5 \bmod 8$, $(\mathfrak{P}^{\frac{s_1+s_2}{2}}, 1)$ is an Arakelov-modular lattice of level p over K.

Lemma 3.14. $\mathfrak{P} = (2 - 2\cos\frac{2\pi}{p^r})$ and $2 - 2\cos\frac{2\pi}{p^r}$ is totally positive in K.

Proof. Since $\sigma(\cos\frac{2\pi}{p^r}) < 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $2 - 2\cos\frac{2\pi}{p^r}$ is totally positive in K. Moreover,

$$(1 - \zeta_{p^r})(1 - \zeta_{p^r}^{-1}) = 2 - 2\cos\frac{2\pi}{p^r}$$

generates $\mathfrak{P}$. □

Proposition 3.15. There exists an Arakelov-modular lattice of level ℓ over $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ if and only if $\ell \in \mathrm{Mod}(p^r)$, where $\mathrm{Mod}(p^r)$ is given by

1. $\mathrm{Mod}(p^r) = \{1, p\}$, if $p \equiv 1 \bmod 4$;
2. $\mathrm{Mod}(p^r) = \{1\}$, if $p \equiv 3 \bmod 4$.

Proof. 1. Take $p \equiv 1 \bmod 4$, $\ell = 1$. Let $\alpha = (2 - 2\cos\frac{2\pi}{p^r})^{-1}$, by Lemma 3.14, α is totally positive. Moreover,

$$v_{\mathfrak{P}}(\alpha^{-1}\mathcal{D}_K^{-1}) = 1 + s_1$$

is even. By Proposition 3.9, $1 \in \mathrm{Mod}(p^r)$.

2. Take $p \equiv 1 \bmod 8$, $\ell = p$. Let $\alpha = (2 - 2\cos\frac{2\pi}{p^r})^{-1}$ and $\beta = \sqrt{p}$, then $\ell = \beta^2$ and

$$v_{\mathfrak{P}}(\alpha^{-1}\beta\mathcal{D}_K^{-1}) = 1 + s_1 + s_2$$

is even. By Proposition 3.9, $p \in \mathrm{Mod}(p^r)$.

By Corollary 3.11 and Proposition 3.12, the proof is completed. □

3.4.3 Maximal Real Subfield of a Cyclotomic Field – The Non-Prime Power Case

Let $m \not\equiv 2 \bmod 4$ be an integer which is not a prime power. Set $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. For any $p \in \mathbb{Q}$ a prime dividing m, write $m = p^{r_p}m'_p$ with $(p, m'_p) = 1$. Let $\mathfrak{P}_p$ be the prime ideal in $\mathcal{O}_K$ above p. We have $v_{\mathfrak{P}_p}(p) = p^{r_p-1}(p-1)$ and $v_{\mathfrak{P}_p}(\mathcal{D}_K) = p^{r_p-1}(pr_p - r_p - 1)$.

For any divisor d of m, define

$$d_{mod3} = \prod_{\substack{p|d \\ p\equiv 3 \bmod 4}} p, \qquad d_{mod1} = \prod_{\substack{p|d \\ p\equiv 1 \bmod 4}} p, \qquad \tilde{m} = \prod_{\substack{p\in\Omega(K) \\ p\neq 2}} p.$$

Lemma 3.16. 1. For any $d|m$, d_{mod1} is always a square in K.

2. For any $d|m$, d_{mod3} is a square in K if and only if one of the following conditions is satisfied:
   - m is even
   - m is odd and d_{mod3} has an even number of distinct prime factors
3. For m even, 2 is a square in K if and only if $m \equiv 0 \bmod 8$.

Proof. 1. For any odd prime $p|m$, $\mathbb{Q}(\zeta_p) \subseteq L$ and [62, p.17]

$$\sqrt{p} \in \mathbb{Q}(\zeta_p) \iff p \equiv 1 \bmod 4, \qquad \sqrt{-p} \in \mathbb{Q}(\zeta_p) \iff p \equiv 3 \bmod 4.$$

Part 1 follows immediately.

2. To prove 2, assume $p \equiv 3 \bmod 4$, then $\sqrt{-p} \in L$.

   If m is even, $i \in L$, $\sqrt{p} = \frac{\sqrt{-p}}{i} \in L \cap \mathbb{R} = K$.

   If m is odd and d_{mod3} has an even number of distinct prime factors,

$$\sqrt{d_{mod3}} = \prod_{\substack{p|d \\ p \equiv 3 \bmod 4}} \sqrt{p} = \prod_{\substack{p|d \\ p \equiv 3 \bmod 4}} \sqrt{-p} \in L \cap \mathbb{R} = K.$$

   On the other hand, assume m is odd, and d_{mod3}, a square in K, has an odd number of distinct prime factors. Let p_0 be any prime factor of d_{mod3}. We have $\sqrt{-p_0} \in L$ and

$$\sqrt{p_0} = \frac{\sqrt{d_{mod3}}}{\prod_{\substack{p|d_{mod3} \\ p \neq p_0}} \sqrt{p}} = \frac{\sqrt{d_{mod3}}}{\prod_{\substack{p|d_{mod3} \\ p \neq p_0}} \sqrt{-p}} \in L.$$

   So $i = \frac{\sqrt{-p_0}}{\sqrt{p_0}} \in L$, which implies $4|m$, a contradiction.

3. Now consider m even. If $8|m$, $\sqrt{2} \in \mathbb{Q}(\zeta_8) \cap \mathbb{R} \subseteq L \cap \mathbb{R} = K$.

   Conversely, if $\sqrt{2} \in K \subseteq L$, since $i \in L$, we have $\zeta_8 \in K$ and hence $8|m$.

□

Let $\mathrm{Mod}_T(m)$ denote the set of ℓ such that there exists an Arakelov-modular lattice of trace type of level ℓ over K.

Lemma 3.17. $\mathrm{Mod}_T(m) \neq \emptyset$ if and only if,

1. $m_{mod1} = 1$;

For any $\ell \in \mathrm{Mod}_T(m)$:

2. $\ell = \tilde{m}$ or $2\tilde{m}$, and $\ell | m$;

3. ℓ is a square in K.

Proof. First we assume $\mathrm{Mod}_T(m) \neq \emptyset$. For any $p \in \Omega(K)\backslash\{2\}$, $v_{\mathfrak{P}_p}(\mathcal{D}_K^{-1}) = -p^{r_p-1}(pr_p - r_p - 1)$ is odd. By Proposition 3.9, ℓ is a square, $p|\ell$ and $\frac{1}{2}v_{\mathfrak{P}_p}(\ell) = \frac{1}{2}p^{r_p-1}(p-1)$ must be odd. The proof then follows from Lemma 3.4.

Conversely, assume all conditions are satisfied. By Proposition 3.9, it suffices to prove $v_{\mathfrak{P}_p}(\beta\mathcal{D}_K^{-1})$ is even for all prime ideal $\mathfrak{P}_p$, where $v_{\mathfrak{P}_p}(\beta) = \frac{1}{2}v_{\mathfrak{P}_p}(\ell)$. Conditions 1 and 2 ensure that $v_{\mathfrak{P}_p}(\beta\mathcal{D}_K^{-1})$ is even for all prime ideal $\mathfrak{P}_p$. □

The above discussion gives the characterization of the existence of Arakelov-modular lattices of trace type over K, the maximal real subfield of the cyclotomic field generated by a primitive mth root of unity:

Proposition 3.18. Let $m \not\equiv 2 \bmod 4$ be a positive integer which is not a prime power.

If m has any prime factor $p \equiv 1 \bmod 4$, $\mathrm{Mod}_T(m) = \emptyset$.

Otherwise,

1. If m is odd and has an even number of distinct prime factors, $\mathrm{Mod}_T(m) = \{\tilde{m}\}$;

2. If m is odd and has an odd number of distinct prime factors, $\mathrm{Mod}_T(m) = \emptyset$;

3. If $m = 4m'$, where m' is odd, $\mathrm{Mod}_T(m) = \{\tilde{m}\}$;

4. If $m = 2^r m'$, where $r \geq 3$ and m' is odd, $\mathrm{Mod}_T(m) = \{\tilde{m}, 2\tilde{m}\}$.

3.4.4 Totally Real Number Fields with Odd Degree

Let K be a totally real Galois extension with odd degree n and let ℓ be a positive square-free integer. Let $\mathrm{Mod}(K)$ denote the set of ℓ such that there exists an Arakelov-modular lattice of level ℓ over K. By Lemma 3.4, $\mathrm{Mod}(K) \subseteq \{1\}$.

Proposition 3.19. Let K be a totally real Galois field with odd degree. Then $\mathrm{Mod}(K) = \{1\}$.

Proof. We claim that for any $\mathfrak{P}$ a prime ideal in $\mathcal{O}_K$, $v_{\mathfrak{P}}(\mathcal{D}_K)$ is even. By Proposition 3.9, taking $\alpha = 1$, the proof is completed.

Proof of claim: Fix $\mathfrak{P}$ a prime ideal in $\mathcal{O}_K$, take p such that $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$. Suppose p has ramification index e and inertia degree f. Let $\mathbb{Q}_p$, $K_{\mathfrak{P}}$ be the completion of $\mathbb{Q}$ (resp. K) with

respect to the $p-$adic valuation (resp. $\mathfrak{P}-$adic valuation). Then $K_{\mathfrak{P}}$ is a Galois extension of $\mathbb{Q}_p$ with degree ef [53, p.103]. Let $G(K_{\mathfrak{P}}|\mathbb{Q}_p)$ be the Galois group of $K_{\mathfrak{P}}/\mathbb{Q}_p$. For $i \geq 0$, define [53, p.61]

$$G_i := \{\sigma \in G(K_{\mathfrak{P}}|\mathbb{Q}_p) | v_{\mathfrak{P}}(\sigma(a) - a) \geq i + 1 \, \forall a \in \mathcal{O}_{K_{\mathfrak{P}}}\}.$$

Let $\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ be the different of $K_{\mathfrak{P}}/\mathbb{Q}_p$, then [53, p.64]

$$v_{\mathfrak{P}}(\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_p}) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

Since each G_i is a normal subgroup of $G(K_{\mathfrak{P}}|\mathbb{Q}_p)$ [53, p.62], which has odd cardinality, $v_{\mathfrak{P}}(\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_p})$ is even. As [42, p.196]

$$\mathcal{D}_{K/\mathbb{Q}} = \prod_{\mathfrak{P}} \mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_p},$$

we have $v_{\mathfrak{P}}(\mathcal{D}_{K/\mathbb{Q}})$ is even. □

Remark 3.20. By the above proof, for a totally real Galois field K with odd degree, $(\mathcal{D}_K^{-\frac{1}{2}}, 1)$ is an Arakelov-modular lattice of level 1, in particular, it is a unimodular lattice.

3.5 Examples

In this section we list some examples of lattices constructed using the methods discussed above. To our best knowledge, the lattice in Example 3.22 is new. In Table 3.1 and Example 3.21, we list a few constructions of existing lattices, note that the first three lattices in Table 3.1 and the lattice in Example 3.21 are extremal (see Definition 2.11).

ℓ	K	I	α	Dim	min	NAME
1	$\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$	$\mathfrak{P}_{13}^{-3}$	$(2 - 2\cos\frac{2\pi}{13})^{-1}$	6	1	$\mathbb{Z}^6$
7	$\mathbb{Q}(\zeta_{28} + \zeta_{28}^{-1})$	$\mathfrak{P}_7^{-1}\mathfrak{P}_2^{-1}$	1	6	2	$A6\hat{}(2)$
11	$\mathbb{Q}(\zeta_{44} + \zeta_{44}^{-1})$	$\mathfrak{P}_{11}^{-2}\mathfrak{P}_2^{-1}$	1	10	6	$A10\hat{}(3)$
23	$\mathbb{Q}(\zeta_{92} + \zeta_{92}^{-1})$	$\mathfrak{P}_{23}^{-5}\mathfrak{P}_2^{-1}$	1	22	12	$A22\hat{}(6)$

Table 3.1: Examples of lattices (I, α) obtained from K such that (I, α) is an Dim$-$dimensional Arakelov-modular lattice of level ℓ with minimum min and isometric to the existing lattice NAME from [56]. Here $\mathfrak{P}_p$ denotes the unique prime ideal in $\mathcal{O}_K$ above p.

Example 3.21. [An existing unique even extremal $3-$modular lattice] Take $K = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$, by Proposition 3.18 there exists a $6-$dimensional $3-$modular lattice over K. The

ideal lattice $(\mathfrak{P}_3^{-3}\mathfrak{P}_2^{-1}, 1)$ gives us such a lattice with minimum 2, where $\mathfrak{P}_3$ (resp. $\mathfrak{P}_2$) is the unique prime ideal in $\mathcal{O}_K$ above 3 (resp. 2). This lattice is the unique even extremal $6-$dimensional $3-$modular lattice [58].

Example 3.22. [New extremal unimodular lattice] Take K to be the unique $21-$dimensional subfield of the cyclotomic field $\mathbb{Q}(\zeta_{49})$. By Proposition 3.19, there exists a unimodular lattice over K. By Remark 3.20, $(\mathcal{D}_K^{-\frac{1}{2}}, 1)$ is such a lattice. Using Magma [12], we get this lattice has minimum 2, hence it is an extremal $21-$dimensional unimodular lattice.

The characterization of Arakelov-modular lattices deeply involves the properties of number fields. It can be formulated into a purely algebraic number theory problem (see Propositions 3.6 and 3.9). The well-known "Führerdiskriminantenproduktformel" [53, p.104] gives a formula for factorizing the different of a number field. Utilizing this formula and class field theory, the future work is to characterize the existence of Arakelov-modular lattices over totally real number fields with even degrees as well as CM fields which were not considered in this Chapter.

Chapter 4

Construction from Quaternion Algebras

In the previous chapter we studied Arakelov-modular lattices over number fields. In this chapter we will generalize the definition of Arakelov-modular lattices to totally definite quaternion algebras over totally real number fields.

Recall that (see Definition 2.5) for ℓ a positive integer, an $\ell-$*modular lattice* [49] is an integral lattice such that there exists a $\mathbb{Z}-$module isomorphism $\varphi : L^* \to L$ and

$$\ell b(x, y) = b(\varphi(x), \varphi(y)) \; \forall x, y \in L^*,$$

where $L^* = \{x \in L \otimes_{\mathbb{Z}} \mathbb{R} : b(x, y) \in \mathbb{Z} \; \forall y \in L\}$. When $\ell = 1$ we have a *unimodular lattice*.

As discussed in Chapter 3, a common way of constructing $\ell-$modular lattices is by using ideals of number fields [25, 3, 6], and the resulting lattices are then called *ideal lattices* [5]. In [25], a construction of unimodular lattices by ideal lattices over $\mathbb{Q}(\sqrt{-3})$ is given. A more general construction over cyclotomic extension of imaginary quadratic fields can be found in [3]. In this chapter, we generalize this notion to construct Arakelov-modular lattices from the ideals of totally definite quaternion algebras over totally real number fields.

The construction by ideals of quaternions was also used in [37] for two particular cases, $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\left(\frac{-1,-3}{\mathbb{Q}}\right)$, for constructing $2-$ and $3-$ modular lattices respectively. This is a special case of our construction (see Example 4.29).

We will discuss in details the definition of the bilinear form we use in Section 4.1 and introduce the definition of ideal lattices over totally definite quaternions in Section 4.2. In Section 4.3 the generalized notion of Arakelov-modular lattice is introduced. In Section 4.4,

we focus on the case where the underlying number field is the rational field, for which we obtain existence results and classify Arakelov-modular lattices for ℓ a prime. In particular, we will prove that, given any prime ℓ, there exists a totally definite quaternion algebra over $\mathbb{Q}$ over which an Arakelov-modular lattice of level ℓ can be constructed. In Section 4.5 we give necessary and sufficient conditions for the existence of Arakelov-modular lattices when the base field is the maximal real subfield of a cyclotomic field and has odd degree. Finally in Section 4.6 we study the existence conditions of Arakelov-modular lattice when the number field is a totally real quadratic field or a maximal real subfield of a cyclotomic field that has even degree.

4.1 Totally Definite Quaternion Algebras

Let K be a number field with degree $n = [K : \mathbb{Q}]$. Let $A = \left(\frac{a,b}{K}\right)$ be a quaternion algebra over K with standard basis $\{1, i, j, ij\}$, i.e., A is a 4-dimensional vector space over K with basis $\{1, i, j, ij\}$ such that

$$i^2 = a,\ j^2 = b,\ ij = -ji,$$

for some $a, b \in K^\times$.

Remark 4.1. When $a = b = -1$, and instead of a number field, we consider $\mathbb{R}$, $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is called Hamilton's quaternion and denoted by $\mathbb{H}$ [35, p.78].

The quaternion algebra A is a *central simple* $K-$algebra, i.e. the *center* of A, $Z(A) := \{x \in A : xy = yx\ \forall y \in A\}$, is given by K and A has no proper two-sided ideals.

A is equipped with a *canonical involution (or conjugation)* given by

$$\begin{aligned} {}^- : A &\to A \\ \alpha = x_0 + x_1 i + x_2 j + x_3 ij &\mapsto \bar{\alpha} = x_0 - x_1 i - x_2 j - x_3 ij, \end{aligned} \tag{4.1}$$

from which are defined the reduced trace on A:

$$\begin{aligned} \mathrm{tr}_{A/K} : A &\to K \\ \alpha &\mapsto \alpha + \bar{\alpha}, \end{aligned}$$

and similarly the reduced norm:

$$\begin{aligned} \mathrm{n}_{A/K} : A &\to K \\ \alpha &\mapsto \alpha\bar{\alpha}. \end{aligned}$$

For $\alpha = x_0 + x_1 i + x_2 j + x_3 ij \in A$

$$\begin{aligned} \mathrm{tr}_{A/K}(\alpha) &= \alpha + \bar{\alpha} = 2x_0 \\ \mathrm{n}_{A/K}(\alpha) &= \alpha\bar{\alpha} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2. \end{aligned} \tag{4.2}$$

In particular, if $A \cong M_2(K)$, the conjugation (4.1) is given by [35, p.79]

$$\overline{\begin{bmatrix} c & d \\ e & f \end{bmatrix}} = \begin{bmatrix} f & -d \\ -e & c \end{bmatrix}. \tag{4.3}$$

And

$$\begin{aligned} \mathrm{tr}_{A/K}\left(\begin{bmatrix} c & d \\ e & f \end{bmatrix}\right) &= \begin{bmatrix} c & d \\ e & f \end{bmatrix} + \begin{bmatrix} f & -d \\ -e & c \end{bmatrix} = \begin{bmatrix} c+f & 0 \\ 0 & c+f \end{bmatrix}, \\ \mathrm{n}_{A/K}\left(\begin{bmatrix} c & d \\ e & f \end{bmatrix}\right) &= \begin{bmatrix} c & d \\ e & f \end{bmatrix}\begin{bmatrix} f & -d \\ -e & c \end{bmatrix} = \begin{bmatrix} cf-de & 0 \\ 0 & cf-de \end{bmatrix}, \end{aligned} \tag{4.4}$$

i.e. $\mathrm{tr}_{A/K}(\alpha) =$ trace of α and $\mathrm{n}_{A/K}(\alpha) = \det(\alpha)$.

Suppose K has r_1 real places and r_2 pairs of complex places, so $n = [K : \mathbb{Q}] = r_1 + 2r_2$. Denote the embeddings of K in $\mathbb{C}$ by $\sigma_1, \ldots, \sigma_n$. Let K_v denote the completion of K at the Archimedean place corresponding to σ, then $A_v = A \otimes_K K_v \cong M_2(\mathbb{C})$ if σ is complex [35, p.93]. If σ is real, $A_v \cong \mathbb{H}$ or $M_2(\mathbb{R})$ [35, p.93]. We say A is *ramified* at the place corresponding to σ if $A_v \cong \mathbb{H}$ and *unramified* otherwise [35, p.99]. Similarly, let $\mathfrak{p}$ be a finite prime in K and $K_\mathfrak{p}$ be the completion of K at the corresponding non-Archimedean valuation. Then A is said to be *ramified* at $\mathfrak{p}$ if $A \otimes_K K_\mathfrak{p}$ is the unique division algebra over $K_\mathfrak{p}$. Otherwise, A is said to be *unramified* at $\mathfrak{p}$ [35, p.99]. Let $A_m = \left(\frac{\sigma_m(a), \sigma_m(b)}{L}\right)$, where $L = \mathbb{R}$ for $m = 1, 2, \ldots, r_1$ and $\mathbb{C}$ for $m = r_1 + 1, \ldots, r_1 + r_2$.

Denote the standard basis of A_m by $\{1, i_m, j_m, i_m j_m\}$, i.e.

$$i_m^2 = \sigma_m(a),\ j_m^2 = \sigma_m(b),\ i_m j_m = -j_m i_m.$$

Define $\hat{\sigma}_m : A \to A_m$ by

$$\hat{\sigma}_m(x_0 + x_1 i + x_2 j + x_3 ij) = \sigma_m(x_0) + \sigma_m(x_1) i_m + \sigma_m(x_2) j_m + \sigma_m(x_3) i_m j_m.$$

$\hat{\sigma}_m$ gives a ring homomorphism extending the embedding $\sigma_m : K \hookrightarrow L$.

Let s_1 be the number of real places at which A is ramified. Then the map [35, p.254]

$$\begin{aligned} \phi : A \otimes_{\mathbb{Q}} \mathbb{R} &\to \oplus \sum_{m=1}^{n} A_m \\ \alpha \otimes h &\mapsto (h\hat{\sigma}_1(\alpha), \ldots, h\hat{\sigma}_n(\alpha)) \end{aligned}$$

gives the following isomorphism

$$A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R} \cong \oplus s_1 \mathbb{H} \oplus (r_1 - s_1) M_2(\mathbb{R}) \oplus r_2 M_2(\mathbb{C}). \tag{4.5}$$

Note that $A_{\mathbb{R}}$ is a *semi-simple* $\mathbb{R}-$*algebra*, where for any field K, a semi-simple $K-$algebra B is an algebra for which there exist simple algebras $B_1, B_2, \ldots, B_t$ such that

$$B = B_1 \oplus B_2 \cdots \oplus B_t$$

and the centers of B_m are finite field extensions of K. Moreover, let F_m be the center of B_m and let $\mathrm{Tr}_{F_m/K}$ denote the trace map of F_m over K. For any $\boldsymbol{\beta} \in B$, the *reduced trace* of $\boldsymbol{\beta}$ in B can be defined as [52, p.121]

$$\mathrm{tr}_{B/K}(\boldsymbol{\beta}) = \sum_{m=1}^{t} \mathrm{tr}_{B_m/K}(\beta_m) = \sum_{m=1}^{t} \mathrm{Tr}_{F_m/K}\left(\mathrm{tr}_{B_m/F_m}(\beta_m)\right). \tag{4.6}$$

We can extend the conjugation on A to that on $A_{\mathbb{R}}$ by the conjugations on $\mathbb{H}$, $M_2(\mathbb{R})$ and conjugations on $M_2(\mathbb{C})$ (as a $\mathbb{C}-$algebra). In this manner, the map ϕ preserves this conjugation: For $m = 1, 2, \ldots, n$, let ρ_m denote the projection of ϕ onto one of the factors in (4.5). Take $\alpha = x_0 + x_1 i + x_2 j + x_3 ij \in A$, $h \in \mathbb{R}\backslash\{0\}$. For $m = 1, 2, \ldots, s_1$,

$$A_m = \left(\frac{\sigma(a), \sigma(b)}{\mathbb{R}}\right) \cong \mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right).$$

Let $\{1, i', j', i'j'\}$ denote the standard basis for $\mathbb{H}$. Under the isomorphism

$$\begin{array}{ccc} \left(\dfrac{\sigma_m(a), \sigma_m(b)}{\mathbb{R}}\right) & \xrightarrow{\sim} & \left(\dfrac{-1,-1}{\mathbb{R}}\right) \\ i_m & \mapsto & i' \\ j_m & \mapsto & j', \end{array}$$

we have

$$\rho_m(\alpha\otimes h) = m\text{th coordinate of } \phi(\alpha\otimes h) = h\hat{\sigma}_m(\alpha) = h\sigma_m(x_0)+h\sigma_m(x_1)i'+h\sigma_m(x_2)j'+h\sigma_m(x_3)i'j',$$

so by the conjugation on $\mathbb{H}$,

$$\overline{\rho_m(\alpha \otimes h)} = h\sigma_m(x_0) - h\sigma_m(x_1)i' - h\sigma_m(x_2)j' - h\sigma_m(x_3)i'j'.$$

As A can be embedded in $A_{\mathbb{R}}$ by identifying α with $\alpha \otimes 1$ for all $\alpha \in A$, we have

$$\overline{\rho_m(\alpha)} = \rho_m(\bar{\alpha}),$$

where the first conjugation is the conjugation on $\mathbb{H}$ and the second is the conjugation on A. In particular we have $\rho_m(\alpha \otimes h) = \overline{\rho_m(\alpha \otimes h)}$ iff $x_1 = x_2 = x_3 = 0$ iff $x \in K^\times$.

For $m = s_1 + 1, \ldots, r_1$,

$$A_m = \left(\frac{\sigma_m(a), \sigma_m(b)}{\mathbb{R}}\right) \cong M_2(\mathbb{R}) \cong \left(\frac{1,1}{\mathbb{R}}\right).$$

Let $\{1, i', j', i'j'\}$ denote the standard basis for $\left(\frac{1,1}{\mathbb{R}}\right)$. Consider $\sigma(a) > 0, \sigma(b) > 0$. Under the isomorphisms:

$$\begin{array}{ccccccc} \left(\frac{\sigma_m(a),\sigma_m(b)}{\mathbb{R}}\right) & \longrightarrow & \left(\frac{1,1}{\mathbb{R}}\right) & \longrightarrow & M_2(\mathbb{R}) \\ i & \mapsto & \sqrt{\sigma_m(a)}i' & \mapsto & \sqrt{\sigma_m(a)}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ j & \mapsto & \sqrt{\sigma_m(b)}j' & \mapsto & \sqrt{\sigma_m(b)}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \end{array}$$

we have $\rho_m(\alpha \otimes h)$ is the image of

$$h\sigma_m(x_0) + h\sigma_m(x_1)i' + h\sigma_m(x_2)j' + h\sigma_m(x_3)i'j'$$

in $M_2(\mathbb{R})$, that is

$$h\sigma_m(x_0)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + h\sigma_m(x_1)\sqrt{\sigma_m(a)}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} + h\sigma_m(x_2)\sqrt{\sigma_m(b)}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} + h\sigma_m(x_3)\sqrt{\sigma_m(ab)}\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$
$$= h\begin{bmatrix}\sigma_m(x_0)+\sigma_m(x_1)\sqrt{\sigma_m(a)} & \sigma_m(x_2)\sqrt{\sigma_m(b)}+\sigma_m(x_3)\sqrt{\sigma_m(ab)}\\ \sigma_m(x_2)\sqrt{\sigma_m(b)}-\sigma_m(x_3)\sqrt{\sigma_m(ab)} & \sigma_m(x_0)-\sigma_m(x_1)\sqrt{\sigma_m(a)}.\end{bmatrix}$$

By (4.3),

$$\overline{\rho_m(\alpha\otimes h)} = h\begin{bmatrix}\sigma_m(x_0)-\sigma_m(x_1)\sqrt{\sigma_m(a)} & -\sigma_m(x_2)\sqrt{\sigma_m(b)}-\sigma_m(x_3)\sqrt{\sigma_m(ab)}\\ -\sigma_m(x_2)\sqrt{\sigma_m(b)}+\sigma_m(x_3)\sqrt{\sigma_m(ab)} & \sigma_m(x_0)+\sigma_m(x_1)\sqrt{\sigma_m(a)}.\end{bmatrix},$$

similarly we have $\overline{\rho_m(\alpha)} = \rho_m(\bar{\alpha})$. Moreover, $\rho_m(\alpha\otimes h) = \overline{\rho_m(\alpha\otimes h)}$ if and only if $\rho_m(\alpha\otimes h)$ is a diagonal matrix, if and only if $\alpha\in K^\times$. For the cases when $\sigma_m(a)<0$, $\sigma_m(b)<0$, $\sigma_m(a)>0, \sigma_m(b)<0$ or $\sigma_m(a)<0, \sigma_m(b)>0$ we have similar results. Same for $m = r_1+1,\ldots,n$.

Thus we have $\phi(\bar{\alpha}) = \overline{\phi(\alpha)}$ for all $\alpha\in A$. And the set

$$\mathcal{P} := \{\boldsymbol{\alpha} : \boldsymbol{\alpha}\in A_{\mathbb{R}}, \boldsymbol{\alpha} = \bar{\boldsymbol{\alpha}}\} = \{\alpha\otimes h : \alpha\in K^\times\}$$

belongs to the center of $A_{\mathbb{R}}$.

Recall the reduced trace on A (4.2):

$$\begin{aligned}\mathrm{tr}_{A/K} : A &\to K\\ \alpha &\mapsto \alpha+\bar{\alpha},\end{aligned}$$

and the trace map on $K/\mathbb{Q}$ [42]:

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}} : K &\to \mathbb{Q}\\ x &\mapsto \sum_{m=1}^{n}\sigma_m(x).\end{aligned}$$

Let tr denote the reduced trace on the separable $\mathbb{R}-$algebra $A_{\mathbb{R}}$, then by (4.6), $\mathrm{tr}\,(\boldsymbol{x})$

$= \sum_{m=1}^{r_2} \mathrm{tr}_{A_m/\mathbb{R}}(x_m)$, which is

$$\begin{aligned}
&= \sum_{m=1}^{s_1} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(x_m) + \sum_{m=s_1+1}^{r_1} \mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}(x_m) + \sum_{m=r_1+1}^{m=r_1+r_2} \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{R}}(x_m) \\
&= \sum_{m=1}^{s_1} (x_m + \bar{x}_m) + \sum_{m=s_1+1}^{r_1} \text{trace of } x_m + \sum_{m=r_1+1}^{m=r_1+r_2} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\left(\mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}(x_m)\right) \\
&= \sum_{m=1}^{s_1} (x_m + \bar{x}_m) + \sum_{m=s_1+1}^{r_1} \text{trace of } x_m + \sum_{m=r_1+1}^{m=r_1+r_2} (\text{trace of } x_m + \overline{\text{trace of } x_m}), \qquad (4.7)
\end{aligned}$$

where the last conjugation is complex conjugation.

Take $\boldsymbol{\alpha} \in \mathcal{P}$, and define

$$\begin{aligned}
b_{\boldsymbol{\alpha}} : A_{\mathbb{R}} \times A_{\mathbb{R}} &\to \mathbb{R} \qquad (4.8) \\
(\boldsymbol{x}, \boldsymbol{y}) &\mapsto \mathrm{tr}(\boldsymbol{\alpha x \bar{y}})
\end{aligned}$$

where tr denote the reduced trace on the separable $\mathbb{R}-$algebra $A_{\mathbb{R}}$ given by Eq. (4.6).

Remark 4.2. Such a bilinear form $b_{\boldsymbol{\alpha}}$ can be more generally defined whenever there is a trace form and an involution on a separable algebra, it is usually called a hermitian scaled trace form in the literature [11, 28, 7].

Lemma 4.3. For $\boldsymbol{\alpha} \in \mathcal{P}$, $b_{\boldsymbol{\alpha}}$ is a non-degenerate symmetric bilinear form, and

$$b_{\boldsymbol{\alpha}}(\boldsymbol{ux}, \boldsymbol{y}) = b_{\boldsymbol{\alpha}}(\boldsymbol{x}, \bar{\boldsymbol{u}}\boldsymbol{y})$$

for all $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u} \in A_{\mathbb{R}}$.

Proof. Since tr is the reduced trace for the $\mathbb{R}-$separable algebra $A_{\mathbb{R}}$, it is a non-degenerate bilinear form. Now since $\boldsymbol{\alpha}$ is in the center of $A_{\mathbb{R}}$,

$$\mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m x_m \bar{y}_m) = \alpha_m x_m \bar{y}_m + y_m \bar{x}_m \alpha_m = \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m y_m \bar{x}_m)$$

for $m = 1, \ldots, s_1$. Thus

$$\begin{aligned}
b_{\boldsymbol{\alpha}}(\boldsymbol{x}, \boldsymbol{y}) &= \mathrm{tr}(\boldsymbol{\alpha x \bar{y}}) \\
&= \sum_{m=1}^{s_1} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m x_m \bar{y}_m) + \sum_{m=s_1+1}^{r_1} \mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}(\alpha_m x_m \bar{y}_m) \\
&\quad + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{R}}(\alpha_m x_m \bar{y}_m) \\
&= b_{\boldsymbol{\alpha}}(\boldsymbol{y}, \boldsymbol{x})
\end{aligned}$$

using a similar argument on $\mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}(\alpha_m x_m \bar{y}_m)$ for $m = s_1+1, \ldots, r_1$ and on $\mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}(\alpha_m x_m \bar{y}_m)$ for $m = r_1+1, \ldots, r_1+r_2$. This proves that $b_{\boldsymbol{\alpha}}$ is symmetric.

Now take any $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u} \in A_{\mathbb{R}}$, and consider $b_{\boldsymbol{\alpha}}(\boldsymbol{ux}, \boldsymbol{y}) = \mathrm{tr}(\boldsymbol{\alpha ux\bar{y}})$. For $m = 1, 2, \ldots, s_1$, using again that $\boldsymbol{\alpha}$ is in the center of $A_{\mathbb{R}}$,

$$\mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m u_m x_m \bar{y}_m) = \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(u_m \alpha_m x_m \bar{y}_m) = \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m x_m \bar{y}_m u_m)$$

and using a similar argument for $\mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}(\alpha_m x_m \bar{y}_m)$, $m = s_1+1, \ldots, r_1$, and for $\mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}(\alpha_m x_m \bar{y}_m)$, $m = r_1+1, \ldots, r_1+r_2$, we conclude that

$$b_{\boldsymbol{\alpha}}(\boldsymbol{ux}, \boldsymbol{y}) = b_{\boldsymbol{\alpha}}(\boldsymbol{x}, \bar{\boldsymbol{u}}\boldsymbol{y}).$$

□

When K is a totally real number field, and A is a quaternion algebra ramified at all the real places, i.e., $s_1 = r_1 = n$, we say that A is totally definite [52, 34.1]. For this case, define

$$\mathcal{P}_{>0} = \{\boldsymbol{\alpha} : \boldsymbol{\alpha} \in \mathcal{P}, \alpha_m > 0 \ \forall m\}.$$

Lemma 4.4. *$b_{\boldsymbol{\alpha}}$ is positive definite if and only if K is totally real, A is totally definite and $\boldsymbol{\alpha} \in \mathcal{P}_{>0}$.*

Proof. Take any $\boldsymbol{x} \in A_{\mathbb{R}}$, $b_{\boldsymbol{\alpha}}(\boldsymbol{x}, \boldsymbol{x})$ is given by $\mathrm{tr}(\boldsymbol{\alpha x\bar{x}})$, i.e.

$$\sum_{m=1}^{s_1} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha_m x_m \bar{x}_m) + \sum_{m=s_1+1}^{r_1} \mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}(\alpha_m x_m \bar{x}_m) + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{R}}(\alpha_m x_m \bar{x}_m).$$

Recall that $\boldsymbol{\alpha} \in Z(A_{\mathbb{R}})$ and $\boldsymbol{\alpha} = \bar{\boldsymbol{\alpha}}$, the above becomes

$$\sum_{m=1}^{s_1} \alpha_m \mathrm{tr}_{\mathbb{H}/\mathbb{R}}\left(\mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m)\right) + \sum_{m=s_1+1}^{r_1} \alpha_m \mathrm{tr}_{M_2(\mathbb{R})/\mathbb{R}}\left(\mathrm{n}_{M_2(\mathbb{R})/\mathbb{R}}(x_m)\right) + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{R}}(\alpha_m x_m \bar{x}_m),$$

which is

$$
\begin{aligned}
&= \sum_{m=1}^{s_1} 2\alpha_m \mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m) + \sum_{m=s_1+1}^{r_1} 2\alpha_m \det(x_m) + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\left(\mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}(\alpha_m x_m \bar{x}_m)\right) \\
&= \sum_{m=1}^{s_1} 2\alpha_m \mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m) + \sum_{m=s_1+1}^{r_1} 2\alpha_m \det(x_m) + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\left(\alpha_m \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}\left(\mathrm{n}_{M_2(\mathbb{C})/\mathbb{C}}(x_m)\right)\right) \\
&= \sum_{m=1}^{s_1} 2\alpha_m \mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m) + \sum_{m=s_1+1}^{r_1} 2\alpha_m \det(x_m) + \sum_{m=r_1+1}^{r_1+r_2} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\left(\alpha_m \mathrm{tr}_{M_2(\mathbb{C})/\mathbb{C}}(\det(x_m))\right) \\
&= \sum_{m=1}^{s_1} 2\alpha_m \mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m) + \sum_{m=s_1+1}^{r_1} 2\alpha_m \det(x_m) + \sum_{m=r_1+1}^{r_1+r_2} 2\alpha_m \left(\det(x_m) + \overline{\det(x_m)}\right),
\end{aligned}
$$

we can see that $\mathrm{tr}(\boldsymbol{\alpha}\boldsymbol{x}\bar{\boldsymbol{x}}) > 0$ for all $\boldsymbol{x} \in A_{\mathbb{R}}$ iff A is totally definite and $\alpha_m > 0$ for all m. □

In conclusion, we have proved the following

Proposition 4.5. Let K be a totally real number field, A a totally definite quaternion algebra over K, and take $\boldsymbol{\alpha} \in \mathcal{P}_{>0}$, then

$$
\begin{aligned}
b_{\boldsymbol{\alpha}} : A_{\mathbb{R}} \times A_{\mathbb{R}} &\to \mathbb{R} \\
(\boldsymbol{x}, \boldsymbol{y}) &\mapsto \mathrm{tr}(\boldsymbol{\alpha}\boldsymbol{x}\bar{\boldsymbol{y}})
\end{aligned}
$$

is a positive definite symmetric bilinear form.

The reduced trace of $\boldsymbol{x} \in A_{\mathbb{R}}$ for a totally definite quaternion algebra A

$$
\mathrm{tr}(\boldsymbol{x}) = \sum_{m=1}^{n} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(x_m) = \sum_{m=1}^{n} (x_m + \bar{x}_m)
$$

is alternatively simplified, for all $x \in A$, to

$$
\mathrm{tr}(x \otimes 1) = \sum_{m=1}^{n} (\sigma_m(x) + \overline{\sigma_m(x)}) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{tr}_{A/K}(x)\right). \tag{4.9}
$$

Similarly, the reduced norm of $\boldsymbol{x} \in A_{\mathbb{R}}$ [52, p.121] is

$$
\mathrm{n}(\boldsymbol{x}) = \prod_{m=1}^{n} \mathrm{n}_{\mathbb{H}/\mathbb{R}}(x_m) = \prod_{m=1}^{n} (x_m \bar{x}_m), \tag{4.10}
$$

and for any $x \in A$ [52, p.122 Theorem 9.27 and p. 121 (9.23)],

$$
\mathrm{n}(x \otimes 1) = \mathrm{n}_{A/\mathbb{Q}}(x) = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}(x)\right). \tag{4.11}
$$

When there is no confusion, we will write $\mathrm{tr}(x)$ (resp. $\mathrm{n}(x)$) instead of $\mathrm{tr}(x \otimes 1)$ (resp.

$\mathrm{n}(x \otimes 1)$).

4.2 Ideal Lattices in Totally Definite Quaternion Algebras

For the rest of this chapter, we consider K a totally real number field of degree n, and $A = \left(\frac{a,b}{K}\right)$ a totally definite quaternion algebra over K with standard basis $\{1, i, j, ij\}$. Let $\mathcal{O}_K$ be the ring of integers of K.

An ideal I of A is a finitely generated $\mathcal{O}_K-$module contained in A such that $I \otimes_{\mathcal{O}_K} K \cong A$. An order of A is an ideal of A which is also a subring of A. Let Λ be an order of A. We furthermore assume that Λ is maximal (that is, not properly contained in another order).

For a maximal order Λ of A, we define the following three sets of ideals of A [35, Section 6.7]

$$\mathcal{L}(\Lambda) = \{I : \mathcal{O}_\ell(I) = \Lambda\},\ \mathcal{R}(\Lambda) = \{I : \mathcal{O}_r(I) = \Lambda\},\ \ \mathcal{LR}(\Lambda) = \mathcal{L}(\Lambda) \cap \mathcal{R}(\Lambda), \tag{4.12}$$

where

$$\mathcal{O}_\ell(I) = \{\alpha \in A : \alpha I \subset I\},\ \ \mathcal{O}_r(I) = \{\alpha \in A : I\alpha \subset I\}$$

are respectively *the order on the left* of I and *the order on the right* of I [35, p.84].

Recall the definition of the *codifferent* of Λ over $\mathcal{O}_K$ or $\mathbb{Z}$ [52, p.217], or of $\mathcal{O}_K$ over $\mathbb{Z}$ [42, p.159], given respectively by

$$\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K} = \{x \in A : \mathrm{tr}_{A/K}(xy) \in \mathcal{O}_K\ \forall y \in \Lambda\} \in \mathcal{LR}(\Lambda) \tag{4.13}$$

$$\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}} = \{x \in A : \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{tr}_{A/K}(xy)\right) \in \mathbb{Z}\ \forall y \in \Lambda\} \tag{4.14}$$

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}} = \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}. \tag{4.15}$$

To each corresponds an inverse ideal called *different*, respectively $\mathcal{D}_{\Lambda/\mathcal{O}_K} \in \mathcal{LR}(\Lambda)$, $\mathcal{D}_{\Lambda/\mathbb{Z}}$ and $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$ (see Definition 3.4).

Definition 4.6. An ideal $I \subset A$ is called a *generalized two-sided ideal* of a maximal order Λ if there exist $t \in A^\times$ and $J \in \mathcal{LR}(\Lambda)$ such that $I = Jt = \{yt : y \in J\}$.

Consider a generalized two-sided ideal $I = Jt$ of Λ. Since $J \in \mathcal{LR}(\Lambda)$,

$$\mathcal{O}_\ell(Jt) = \{x \in A : xJt \subseteq Jt\} = \{x \in A : xJ \subseteq J\} = \mathcal{O}_\ell(J) = \Lambda,$$

so $I \in \mathcal{L}(\Lambda)$. Moreover, $J^{-1} \in \mathcal{LR}(\Lambda)$ and [52, Theorem 22.7 and Corollary 22.8]

$$J^{-1}J = \mathcal{O}_r(J) = \Lambda, \;\; JJ^{-1} = \mathcal{O}_\ell(J) = \Lambda, \;\; (J^{-1})^{-1} = J.$$

As $I^{-1} = (Jt)^{-1} = t^{-1}J^{-1}$,

$$II^{-1} = Jtt^{-1}J^{-1} = JJ^{-1} = \Lambda.$$

Consider $\bar{J} = \{\bar{x} : x \in J\}$,

$$\mathcal{O}_r(\bar{J}) = \{\alpha \in A : \bar{J}\alpha \subseteq \bar{J}\} = \{\alpha \in A : \bar{\alpha}J \subseteq J\} = \mathcal{O}_\ell(J) = \Lambda,$$

similarly, $\mathcal{O}_\ell(\bar{J}) = \Lambda$, so $\bar{J} \in \mathcal{LR}(\Lambda)$ and same as above, we have $\bar{J}^{-1} \in \mathcal{LR}(\mathcal{O})$,

$$\bar{J}^{-1}\bar{J} = \mathcal{O}_r(\bar{J}) = \Lambda, \;\; \bar{J}\bar{J}^{-1} = \mathcal{O}_\ell(\bar{J}) = \Lambda.$$

Then

$$\bar{I}^{-1} = \bar{J}^{-1}\bar{t}^{-1} \tag{4.16}$$

is a generalized two-sided ideal of Λ. Moreover,

$$\bar{I}^{-1}\bar{I} = \bar{J}^{-1}\bar{t}^{-1}\bar{t}\bar{J} = \bar{J}^{-1}\bar{J} = \Lambda. \tag{4.17}$$

Recall that for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the norm of $\mathfrak{a}$, we denote by $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$, is given by [42, p.34]

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|, \tag{4.18}$$

and in the case when $\mathfrak{a} = x\mathcal{O}_K$ is a principal ideal [42, p.35],

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(x)|. \tag{4.19}$$

For an ideal $J \in \mathcal{LR}(\Lambda)$ such that $J \subset \Lambda$, the *norm* of J, denoted by $\mathrm{N}_{A/K}(J)$ is defined to be [52, p.210] $\mathrm{ord}_{\mathcal{O}_K}\Lambda/J$, the *order ideal* of Λ/J, which is defined as follows [35, p.199]:

By the *Invariant Factor Theorem* for Dedekind domains, there exist elements m_1, m_2, m_3, m_4 in Λ and fractional $\mathcal{O}_K-$ideals J_1, J_2, J_3, J_4 and E_1, E_2, E_3, E_4 such that

$$\Lambda = J_1m_1 \oplus \cdots \oplus J_4m_4, \;\; J = E_1J_1m_1 \oplus \cdots \oplus E_4J_4m_4,$$

then $\Lambda/J \cong \mathcal{O}_K/E_1 \oplus \mathcal{O}_K/E_2 \oplus \mathcal{O}_K/E_3 \oplus \mathcal{O}_K/E_4$ and

$$\mathrm{ord}_{\mathcal{O}_K}\Lambda/J := E_1E_2E_3E_4. \tag{4.20}$$

If $J \nsubseteq \Lambda$, *norm* of J is defined to be [52, p.212]

$$\mathrm{N}_{A/K}(J) = x^{-4}\mathrm{N}_{A/K}(Jx),$$

where $x \in \mathcal{O}_K$ and $Jx \subset \Lambda$.

We also have the notion of *reduced norm* of an ideal J in A, denoted by $\mathrm{n}_{A/K}(J)$, which is the fractional ideal of $\mathcal{O}_K$ generated by the elements $\{\mathrm{n}_{A/K}(x) : x \in J\}$ [35, p.199]. Moreover, for $J \in \mathcal{LR}(\Lambda)$ [52, p.214],

$$\mathrm{N}_{A/K}(J) = \mathrm{n}_{A/K}(J)^2. \tag{4.21}$$

Take any $J \in \mathcal{LR}(\Lambda)$ and $x \in \mathcal{O}_K$ such that $Jx \subseteq \Lambda$ (we take $x = 1$ if $J \subseteq \Lambda$), then by the above, (4.20) and (4.18),

$$|\Lambda/Jx| = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{N}_{A/K}(Jx)\right) = \mathrm{N}_{K/\mathbb{Q}}\left(x^4\mathrm{N}_{A/K}(J)\right) = \mathrm{N}_{K/\mathbb{Q}}(x)^4\,\mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}(J)\right)^2. \tag{4.22}$$

Definition 4.7. For $I = Jt$ a generalized two-sided ideal of Λ, its *reduced norm* $\mathrm{n}(I)$ in $A_{\mathbb{R}}$ is by definition

$$\mathrm{n}(I) = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}(J)\right)\mathrm{n}(t).$$

Consider the following symmetric positive definite bilinear form:

$$\begin{aligned} b_\alpha : A_{\mathbb{R}} \times A_{\mathbb{R}} &\to \mathbb{R} \\ (x, y) &\mapsto \mathrm{tr}\left((\alpha \otimes 1)x\bar{y}\right), \end{aligned} \tag{4.23}$$

where $\alpha \in K^\times$ is totally positive and for simplicity, we write x, y instead of $\boldsymbol{x}, \boldsymbol{y}$ if there is no confusion. This is a particular case of the previous section, where we restrict to the case when $\boldsymbol{\alpha} = \alpha \otimes 1$ for $\alpha \in K^\times$. Note that $\alpha \otimes 1 \in \mathcal{P}_{>0}$ if and only if α is totally positive, i.e., $\sigma_i(\alpha) > 0$ for all $\sigma_i : K \hookrightarrow \mathbb{R}$.

Definition 4.8. An *ideal lattice* over a maximal order Λ is a pair (I, b_α), where $I = Jt$ is a generalized two-sided ideal of Λ.

Take an ideal lattice (I, b_α) over a maximal order Λ of A, where $I = Jt$ for some $t \in A^\times$ and $J \in \mathcal{LR}(\Lambda)$ is such that it admits a free $\mathcal{O}_K-$basis $\{v_1, v_2, v_3, v_4\}$. Let $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}-$basis for $\mathcal{O}_K$. Thus $\{\beta_i v_j\}_{\substack{1\le i\le n\\ 1\le j\le 4}}$ is a $\mathbb{Z}-$basis for Λ and $\{\beta_i v_j t\}_{\substack{1\le i\le n\\ 1\le j\le 4}}$ is a $\mathbb{Z}-$basis for I.

A Gram matrix of (I, b_α) is given by

$$G = (b_\alpha(\beta_k v_i t, \beta_m v_j t))_{\substack{1\le k,m\le n\\ 1\le i,j\le 4}}.$$

For fixed i, j, $(b_\alpha(\beta_k v_i t, \beta_m v_j t))_{1\le k,m\le n}$ is an $n \times n$ matrix whose coefficients are given by

$$b_\alpha(\beta_k v_i t, \beta_m v_j t) = \mathrm{tr}\left(\alpha\beta_k v_i t\overline{(\beta_m v_j t)}\right) = \mathrm{tr}\left(\alpha\beta_k v_i t\bar{t}\overline{\beta_m v_j}\right),$$

where α (identified with $\alpha \otimes 1$), β_k, $\beta_m, t\bar{t} = \mathrm{n}_{A/K}(t) \in K^\times$, so that, together with Eq. (4.9), we have

$$\begin{aligned} b_\alpha(\beta_k v_i t, \beta_m v_j t) &= \mathrm{tr}\left(\alpha \mathrm{n}_{A/K}(t)\,\beta_k\beta_m v_i\bar{v}_j\right)\\ &= \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{tr}_{A/K}\left(\alpha \mathrm{n}_{A/K}(t)\,\beta_k\beta_m v_i\bar{v}_j\right)\right)\\ &= \sum_{\ell=1}^{n}\sigma_\ell\left(\alpha \mathrm{n}_{A/K}(t)\,\beta_k\beta_m \mathrm{tr}_{A/K}(v_i\bar{v}_j)\right)\\ &= \sum_{\ell=1}^{n}\sigma_\ell(\alpha \mathrm{n}_{A/K}(t))\sigma_\ell(\beta_k\beta_m)\sigma_\ell(\mathrm{tr}_{A/K}(v_i\bar{v}_j)). \end{aligned}$$

Let $B = (\sigma_\ell(\beta_k))$, then for fixed i, j, $(b_\alpha(\beta_k v_i t, \beta_m v_j t))_{1\le k,m\le n} = BH_{ij}B^\top$, where

$$H_{ij} = \begin{bmatrix} \sigma_1(\alpha \mathrm{n}_{A/K}(n)\,\mathrm{tr}_{A/K}(v_i\bar{v}_j)) & \ldots & 0\\ \vdots & \ddots & \vdots\\ 0 & \ldots & \sigma_n(\alpha \mathrm{n}_{A/K}(n)\,\mathrm{tr}_{A/K}(v_i\bar{v}_j)) \end{bmatrix}.$$

Hence

$$G = \begin{bmatrix} B & 0 & 0 & 0\\ 0 & B & 0 & 0\\ 0 & 0 & B & 0\\ 0 & 0 & 0 & B \end{bmatrix}\begin{bmatrix} H_{11} & H_{12} & H_{13} & H_{14}\\ H_{21} & H_{22} & H_{23} & H_{24}\\ H_{31} & H_{32} & H_{33} & H_{34}\\ H_{41} & H_{42} & H_{43} & H_{44} \end{bmatrix}\begin{bmatrix} B^\top & 0 & 0 & 0\\ 0 & B^\top & 0 & 0\\ 0 & 0 & B^\top & 0\\ 0 & 0 & 0 & B^\top \end{bmatrix}. \tag{4.24}$$

Proposition 4.9. An ideal lattice (I, b_α) over a maximal order Λ of A, such that I has a

$\mathbb{Z}$-basis, has dimension $4n$, Gram matrix (4.24) and discriminant

$$\mathrm{n}(\alpha)^2 \mathrm{n}(I)^4 \mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^2,$$

where $\mathrm{n}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}(\alpha)\right)$ is the reduced norm of α in $A_{\mathbb{R}}/\mathbb{R}$, and $\mathrm{n}(I)$ is the reduced norm of I in $A_{\mathbb{R}}/\mathbb{R}$ (see Definition 4.7) and $\mathcal{D}_{\Lambda/\mathbb{Z}}$ is the different of Λ over $\mathbb{Z}$.

Proof. We are left to compute the discriminant of (I, b_α), which is the determinant of G:

$$\det(G) = (\det\left(BB^\top\right))^4 \det(H) = \det(B)^8 \det(H),$$

where $H = (H_{ij})$. After row and column permutations of H, we get

$$\begin{aligned}
\det(H) &= \prod_{\ell=1}^{n} \det\left(\sigma_\ell(\alpha \mathrm{n}_{A/K}(t) \mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right) \\
&= \prod_{\ell=1}^{n} \sigma_\ell(\det\left((\alpha \mathrm{n}_{A/K}(t) \mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right)) \\
&= \prod_{\ell=1}^{n} \sigma_\ell((\alpha \mathrm{n}_{A/K}(t))^4)\sigma_\ell(\det\left((\mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right)) \\
&= (\mathrm{N}_{K/\mathbb{Q}}\left(\alpha \mathrm{n}_{A/K}(t)\right))^4 \mathrm{N}_{K/\mathbb{Q}}\left((\det\left((\mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right)\right),
\end{aligned}$$

while

$$\det(B)^2 = \det\left((\sigma_i(\beta_j))\right)^2 = \Delta_K$$

where Δ_K is the discriminant of K by definition. Thus

$$\det(G) = \Delta_K^4 \mathrm{n}(\alpha)^2 \mathrm{n}(t)^4 \mathrm{N}_{K/\mathbb{Q}}\left((\det\left((\mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right)\right).$$

If $J = \Lambda$, that is $I = \Lambda t$, then

$$\det(G) = \Delta_K^4 \mathrm{n}(\alpha)^2 \mathrm{n}(t)^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right).$$

Indeed, since $\{v_1, v_2, v_3, v_4\}$ is a free $\mathcal{O}_K-$basis for Λ, the discriminant $\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)$ is the principal ideal [35, p.205]

$$\det\left((\mathrm{tr}_{A/K}(v_iv_j))_{i,j}\right)\mathcal{O}_K, \tag{4.25}$$

and

$$\det\left((\mathrm{tr}_{A/K}(v_i\bar{v}_j))_{i,j}\right)\mathcal{O}_K = \det\left((\mathrm{tr}_{A/K}(v_iv_j))_{i,j}\right)\mathcal{O}_K$$

by noting that $\det\left(\left(\mathrm{tr}_{A/K}\left(v_i\bar{v}_j\right)\right)_{i,j}\right) = \det\left(\left(\mathrm{tr}_{A/K}\left(v_iv_j\right)\right)_{i,j}\right)\det\left(\left(a_{kj}\right)_{k,j}\right)$ for $\left(a_{kj}\right)_{k,j} \in M_4(\mathcal{O}_K)$ an invertible matrix such that $\bar{v}_j = \sum_{k=1}^{4} a_{kj}v_k$. Then

$$\mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right) = |\mathrm{N}_{K/\mathbb{Q}}\left(\det\left(\left(\mathrm{tr}_{A/K}\left(v_i\bar{v}_j\right)\right)_{i,j}\right)\right)|.$$

Note that the determinant of a positive definite matrix is always positive.

If $I = Jt$, $J \neq \Lambda$, take $x \in \mathcal{O}_K$ such that $Jx \subseteq \Lambda$, then $Jt \subseteq \Lambda x^{-1}t$ and the discriminant of (I, b_α) is given by [22, p.2]

$$\begin{aligned}\mathrm{disc}\left(\left(I, b_\alpha\right)\right) &= \mathrm{disc}\left(\left(\Lambda x^{-1}t, b_\alpha\right)\right)\left|\Lambda x^{-1}t/Jt\right|^2 \\ &= \Delta_K^4 \mathrm{n}\left(\alpha\right)^2 \mathrm{n}\left(x^{-1}t\right)^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right)\left|\Lambda x^{-1}/J\right|^2\end{aligned}$$

where $\mathrm{n}\left(x^{-1}t\right)^4 = \mathrm{n}\left(t\right)^4 \mathrm{N}_{K/\mathbb{Q}}\left(x\right)^{-8}$ and by Eq. (4.21)

$$\left|\Lambda x^{-1}/J\right| = \left|\Lambda/Jx\right| = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{N}_{A/K}\left(Jx\right)\right) = \mathrm{N}_{K/\mathbb{Q}}\left(x\right)^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}\left(J\right)\right)^2.$$

Thus

$$\begin{aligned}\mathrm{disc}\left(\left(I, b_\alpha\right)\right) &= \Delta_K^4 \mathrm{n}\left(\alpha\right)^2 \mathrm{n}\left(t\right)^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right) \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}\left(J\right)\right)^4 \\ &= \Delta_K^4 \mathrm{n}\left(\alpha\right)^2 \mathrm{n}\left(I\right)^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right)\end{aligned}$$

and we are left to show that

$$\Delta_K^4 \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right) = \mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^2.$$

But [52, p.221]

$$\mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right)\right) = \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{n}_{A/K}\left(\mathcal{D}_{\Lambda/\mathcal{O}_K}\right)\right)^2 = \mathrm{n}\left(\mathcal{D}_{\Lambda/\mathcal{O}_K}\right)^2 = \frac{\mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^2}{\mathrm{n}\left(\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}\right)^2}$$

since $\mathcal{D}_{\Lambda/\mathbb{Z}} = \mathcal{D}_{\Lambda/\mathcal{O}_K}\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$. That [42, p.201]

$$\mathrm{N}_{K/\mathbb{Q}}\left(\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}\right) = \Delta_K$$

completes the proof. □

Let (I^*, b_α) be the dual lattice of (I, b_α), that is

$$I^* = \{x \in I \otimes_{\mathbb{Z}} \mathbb{R} : b_\alpha(x, y) \in \mathbb{Z}\ \forall y \in I\}.$$

Proposition 4.10. The dual of (I, b_α) is given by (I^*, b_α), where

$$I^* = \alpha^{-1}\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}\bar{I}^{-1} = \alpha^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}\bar{I}^{-1}.$$

Proof. Since $\{x : x \in A, \mathrm{tr}\,(xy) \in \mathbb{Z}\ \forall y \in \bar{J}\} = \mathcal{D}_{\Lambda/\mathbb{Z}}\bar{J}^{-1}$ [52, p.217],

$$\begin{aligned} I^* &= \{x : x \in I \otimes_{\mathbb{Z}} \mathbb{R},\ b_\alpha(x, y) \in \mathbb{Z},\ \ \forall y \in I\} \\ &= \{x : \mathrm{tr}\,(\alpha x\bar{y}) \in \mathbb{Z}\ \ \forall y \in Jt\} = \{x : \mathrm{tr}\,(\alpha xy) \in \mathbb{Z}\ \ \forall y \in \bar{t}\bar{J}\} \\ &= \alpha^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}\bar{J}^{-1}\bar{t}^{-1} = \alpha^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}\bar{I}^{-1}. \end{aligned}$$

Also since $\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}\bar{J}^{-1} \in \mathcal{LR}(\Lambda)$ [52, p.217],

$$I^* = \mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}\bar{J}^{-1}\alpha^{-1}\bar{t}^{-1} \tag{4.26}$$

is a generalized two-sided ideal of Λ and (I^*, b_α) is indeed an ideal lattice over Λ. □

Now we can give another calculation of discriminant of (I, b_α), as mentioned in Proposition 4.9, for the case when (I, b_α) is integral, i.e. when $I \subseteq I^*$.

Proposition 4.11. An integral ideal lattice (I, b_α) has dimension $4n$ and discriminant

$$\mathrm{n}\,(\alpha)^2\,\mathrm{n}\,(I)^4\,\mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^2.$$

Proof. First we notice that [52, p.212]

$$\mathrm{n}_{A/K}\left(\bar{J}^{-1}\right) = \mathrm{n}_{A/K}\left(\bar{J}\right)^{-1} = \mathrm{n}_{A/K}\,(J)^{-1} \Longrightarrow \mathrm{n}\left(\bar{J}^{-1}\right) = \mathrm{n}\,(J)^{-1}.$$

Let $\Lambda' = \Lambda\alpha^{-1}\bar{t}^{-1}$. Since Λ is a free $\mathbb{Z}-$module, Λ' is also a free $\mathbb{Z}-$module. Moreover,

$$|I^*/I| = \frac{|\Lambda'/I|}{|\Lambda'/I^*|}.$$

By Eq. (4.22), we have

$$\left|\Lambda'/I\right| = \left|\Lambda\alpha^{-1}\bar{t}^{-1}/Jt\right| = \left|\Lambda/J\mathrm{n}_{A/K}\left(t\right)\alpha\right| = \mathrm{n}\left(J\right)^2\mathrm{n}\left(t\right)^4\mathrm{n}\left(\alpha\right)^2$$

and

$$\left|\Lambda'/I^*\right| = \left|\Lambda\alpha^{-1}\bar{t}^{-1}/\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1}\alpha^{-1}\bar{t}^{-1}\right| = \left|\Lambda/\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1}\right| = \mathrm{n}\left(J\right)^{-2}\mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^{-2}.$$

We have [22, p.4]

$$\mathrm{disc}\left(\left(I,b_\alpha\right)\right) = \left|I^*/I\right| = \frac{\mathrm{n}\left(J\right)^2\mathrm{n}\left(t\right)^4\mathrm{n}\left(\alpha\right)^2}{\mathrm{n}\left(J\right)^{-2}\mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^{-2}} = \mathrm{n}\left(\alpha\right)^2\mathrm{n}\left(I\right)^4\mathrm{n}\left(\mathcal{D}_{\Lambda/\mathbb{Z}}\right)^2.$$

□

4.3 Arakelov-modular Lattices in Totally Definite Quaternion Algebras

We keep the notations from previous sections. Let K be a totally real number field with degree n, ring of integers $\mathcal{O}_K$, and embeddings $\{\sigma_1,\ldots,\sigma_n\}$. Let $A = \left(\frac{a,b}{K}\right)$ be a totally definite quaternion algebra over K, and let Λ be a maximal order in A.

Take $\alpha \in K^\times$ and let b_α be the positive definite bilinear form in Eq. (4.23). Let $I = Jt$ be a generalized two-sided ideal in Λ with $J \in \mathcal{LR}(\Lambda)$, $t \in A^\times$. Then (I, b_α) will denote an ideal lattice over Λ.

We first note that $J \in \mathcal{LR}(\Lambda)$ satisfies $J = \bar{J}$. Indeed, it is known [52, p.273] that the nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and the prime ideals $\mathfrak{P}$ of Λ are in one-to-one correspondence given by

$$\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}, \quad \mathfrak{P}|\mathfrak{p}\Lambda.$$

For a prime ideal $\mathfrak{P}$ of Λ, let then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. As for any $x \in \mathfrak{P} \cap \mathcal{O}_K$, $x = \bar{x}$, we have

$$\bar{\mathfrak{P}} \cap \mathcal{O}_K = \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p},$$

and it follows that $\bar{\mathfrak{P}} = \mathfrak{P}$. But since $\mathcal{LR}(\Lambda) = \{I : I \text{ an ideal in } A, \mathcal{O}_\ell(I) = \mathcal{O}_r(I) = \Lambda\}$ forms an abelian group generated by the prime ideals of Λ, $\bar{\mathfrak{P}} = \mathfrak{P}$ in turn implies $\bar{J} = J$.

Let ℓ denote a positive integer. Let $\mathcal{N}(\Lambda)$ be the normalizer of Λ [35, p.199]:

$$\mathcal{N}(\Lambda) = \{x \in A^{\times} : x\Lambda x^{-1} = \Lambda\},$$

which is a group with respect to multiplication. For any $x \in \mathcal{N}(\Lambda)$, $x\Lambda = \Lambda x \in \mathcal{LR}(\Lambda)$ [52, p.349].

In Chapter 3 we generalized the notion of Arakelov-modular lattice proposed in [6] for CM fields to totally real number fields (see Definition 3.2). Now we further generalize the definition of Arakelov-modular lattices to totally definite quaternion algebras .

Definition 4.12. We call an ideal lattice (I, b_α) *Arakelov-modular of level* ℓ if there exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$, $t \in A^{\times}$ such that

$$I = I^*\beta', \qquad \ell = \mathrm{n}_{A/K}(\beta) = \beta\bar{\beta},$$

where $\beta' = \bar{t}\beta\bar{t}^{-1}$ and $I = Jt$ for some $J \in \mathcal{LR}(\Lambda)$.

Remark 4.13.

1. We have

$$\beta'\bar{\beta}' = \bar{t}\beta\bar{t}^{-1}t^{-1}\bar{\beta}t = \mathrm{n}_{A/K}(t)^{-1}\beta\bar{\beta}\mathrm{n}_{A/K}(t) = \beta\bar{\beta} = \ell,$$

   thus $\ell = \mathrm{n}_{A/K}(\beta') = \beta'\bar{\beta}'$.

2. An ideal lattice that is Arakelov-modular of level ℓ is automatically integral. Indeed, from Eq. (4.26)

$$I^* = \mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1}\alpha^{-1}\bar{t}^{-1},$$

   $\mathcal{D}_{\Lambda/\mathbb{Z}}\bar{J}^{-1} \in \mathcal{LR}(\Lambda)$, and the fact that α is in the center of A, we have [35, p.218],

$$\mathcal{O}_r(I^*) = \bar{t}\mathcal{O}_r(\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1})\bar{t}^{-1} = \bar{t}\Lambda\bar{t}^{-1}.$$

   Since $\beta \in \Lambda$, $\beta' \in \bar{t}\Lambda\bar{t}^{-1}$, showing that $I = I^*\beta' \subseteq I^*$.

3. An Arakelov-modular lattice (I, b_α) is $\ell-$modular [49]. Consider the ideal lattice $(I^*, b_{\ell\alpha})$ and the map

$$\begin{aligned} \varphi : I^* &\to I = I^*\beta' \\ x &\mapsto x\beta'. \end{aligned}$$

Then φ is a $\mathbb{Z}-$module isomorphism with inverse

$$\begin{aligned} \varphi^{-1} : I &\to I^* \\ x &\mapsto \frac{1}{\beta'}x. \end{aligned}$$

Furthermore, for all $x, y \in I^*$,

$$\begin{aligned} b_\alpha(\varphi(x), \varphi(y)) &= b_\alpha(x\beta', y\beta') = \operatorname{tr}\left(\alpha x\beta'\bar{\beta}'\bar{y}\right) \\ &= \operatorname{tr}\left(\alpha x\ell\bar{y}\right) = \operatorname{tr}\left(\ell\alpha x\bar{y}\right) = b_{\ell\alpha}(x, y). \end{aligned}$$

Lemma 4.14. There exists an Arakelov-modular lattice (I, b_α) of level ℓ over Λ if and only if there exists $J \in \mathcal{LR}(\Lambda)$, $t \in A^\times$, $\alpha \in K$ totally positive, and $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$ and

$$J^2 = \mathrm{n}_{A/K}(t)^{-1}\, \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda).$$

Proof. By the above discussions, there exists an Arakelov-modular lattice of level ℓ if and only if there exists $\alpha \in K^\times$, totally positive, $t \in A^\times$, $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$, $J \in \mathcal{LR}(\Lambda)$ such that $\ell = \beta\bar{\beta}$ and

$$Jt = I = I^*\beta' = \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1}\bar{t}^{-1}\bar{t}\beta\bar{t}^{-1} = \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}\bar{J}^{-1}\beta\bar{t}^{-1}.$$

Furthermore, this is equivalent to

$$Jt\bar{t} = \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}J^{-1}\beta, \text{ i.e., } J\mathrm{n}_{A/K}(t) = \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}J^{-1}\beta.$$

Also, $\mathrm{n}_{A/K}(t) \in K$ which is in the center of A, and the above equality reduces to

$$J\beta^{-1}J = \mathrm{n}_{A/K}(t)^{-1}\, \alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}. \tag{4.27}$$

Note that as $\beta \in \mathcal{N}(\Lambda)$,

$$\mathcal{O}_r(J\beta^{-1}) = \beta\mathcal{O}_r(J)\beta^{-1} = \beta\Lambda\beta^{-1} = \Lambda,$$

the left hand side of the above equation is well-defined [52, p.196]. As $\beta \in \mathcal{N}(\Lambda)$, $\beta^{-1} \in$

$\mathcal{N}(\Lambda)$, so $\beta^{-1}\Lambda \in \mathcal{LR}(\Lambda)$. Since $J \in \mathcal{LR}(\Lambda)$,

$$J(\beta^{-1}\Lambda)J \subseteq J\beta^{-1}J.$$

On the other hand,

$$J\beta^{-1}J = \left\{ \sum_{\text{finite sum}} x\beta^{-1}y : x, y \in J \right\} \subseteq J(\beta^{-1}\Lambda)J.$$

Hence Eq. (4.27) is equivalent to

$$(\beta^{-1}\Lambda)J^2 = \mathrm{n}_{A/K}(t)^{-1}\,\alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1},$$

i.e.,

$$J^2 = \mathrm{n}_{A/K}(t)^{-1}\,\alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda)$$

which concludes the proof. □

For any ideal $T \in \mathcal{LR}(\Lambda)$, T has a factorization [35, p.193]

$$T = \prod_{i=1}^{k} \mathfrak{P}_i^{s_i},$$

where $\mathfrak{P}_i$ are prime ideals of Λ and we write $v_{\mathfrak{P}_i}(T) = s_i$. Using this notation, Lemma 4.14 becomes

Lemma 4.15. There exists an Arakelov-modular lattice (I, b_α) of level ℓ over Λ if and only if there exists $t \in A^\times$, $\alpha \in K$ totally positive, and $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$ and

$$v_{\mathfrak{P}}\left(\mathrm{n}_{A/K}(t)^{-1}\,\alpha^{-1}\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda)\right)$$

is even for all prime ideal $\mathfrak{P}$ of Λ.

Comparing with Chapter 3, the main difficulty in defining Arakelov-modular lattice results from the non-commutativity. For example, if $I = \beta' I^*$ in Definition 4.12, Remark 4.13-2 would not be true. And we do need $\beta \in \Lambda \cap \mathcal{N}(\Lambda)$ to have the nice result in Lemma 4.15. Lemma 4.15 can be seen as a generalization of Propositions 3.6 and 3.9 for number fields to the non-commutative case, so that the problem of constructing lattices can be formulated into questions regarding the properties of the quaternions and number fields.

Remark 4.16. 1. If we have two quaternion algebras over K, A and A' that both ramify at the same finite and infinite places over K, there exists a $K-$algebra isomorphism $\varphi : A \to A'$ [35, p.100]. If we have an ideal lattice (I, b_α) over some maximal order Λ in A, we can construct an ideal lattice $(I', b_{\alpha'})$ over the maximal order $\varphi(\Lambda)$ in A' such that (I, b_α) and (I', b'_α) are isomorphic. And vice versa.

2. Take two maximal orders Λ and Λ' in a quaternion algebra A over K that are conjugate to each other, i.e. there exists $u \in A^\times$ such that $\Lambda' = u\Lambda u^{-1}$. If we have an ideal lattice (Jt, b_α) over Λ, $(uJu^{-1}t, b_\alpha)$ will be an ideal lattice over Λ'. Consider the map

$$\begin{aligned} \psi : Jt &\to uJu^{-1}t \\ xt &\mapsto uxu^{-1}t, \end{aligned}$$

we have

$$\begin{aligned} \mathrm{tr}_{A/K}\left(\alpha uxu^{-1}t\overline{(uyu^{-1}t)}\right) &= \mathrm{tr}_{A/K}\left(\alpha uxu^{-1}t\bar{t}\bar{u}^{-1}\bar{y}\bar{u}\right) \\ &= \mathrm{tr}_{A/K}\left(\alpha \mathrm{n}_{A/K}(t)\,\mathrm{n}_{A/K}(u)^{-1}\, ux\bar{y}\bar{u}\right) \\ &= \mathrm{tr}_{A/K}\left(\alpha \mathrm{n}_{A/K}(t)\,\mathrm{n}_{A/K}(u)^{-1}\, \bar{u}ux\bar{y}\right) \\ &= \mathrm{tr}_{A/K}\left(\alpha xt\overline{yt}\right). \end{aligned}$$

Thus (Jt, b_α) and $(uJu^{-1}t, b_\alpha)$ are isomorphic.

Write $\ell = \ell_1^2\ell_2$, where $\ell_1, \ell_2 \in \mathbb{Z}_{>0}$ and ℓ_2 is square-free. In view of the following proposition, we will first focus on the case when ℓ is square-free.

Proposition 4.17. If there exists an Arakelov-modular lattice of level ℓ_2 over Λ, then there exists an Arakelov-modular lattice of level ℓ over Λ.

Proof. Let (Jt, b_α) be an Arakelov-modular lattice of level ℓ_2 over Λ. By Lemma 4.14, there exists $J \in \mathcal{LR}(\Lambda)$ and $t \in A^\times$, $\alpha \in K$ totally positive, and $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell_2 = \beta\bar{\beta}$ and

$$J^2 = \mathrm{n}_{A/K}(t)^{-1}\,\alpha^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}(\beta\Lambda).$$

Let $\tilde{\beta} = \ell_1\beta$, then $\ell = \tilde{\beta}\bar{\tilde{\beta}}$, $\ell_1\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ and

$$J^2 = \mathrm{n}_{A/K}(t)^{-1}\,(\ell_1\alpha)^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}(\ell_1\beta\Lambda) = \mathrm{n}_{A/K}(t)^{-1}\,(\ell_1\alpha)^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}(\tilde{\beta}\Lambda).$$

As $\ell_1 \in \mathbb{Z}$, $\ell_1\alpha \in K$ is totally positive. By Lemma 4.14 again, $(Jt, b_{\ell_1\alpha})$ is an Arakelov-modular lattice of level ℓ. □

So from now on, we consider ℓ to be a square-free positive integer unless otherwise stated.

4.3.1 Galois Extensions

For the rest of the chapter, we suppose that K is a totally real number field which is Galois with Galois group G.

For $p \in \mathbb{Z}$ a prime, we write $\mathfrak{p}|p$ to denote that $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ above p. Similarly, for $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$, we write $\mathfrak{P}|\mathfrak{p}$ to denote that $\mathfrak{P}$ is the prime ideal of Λ such that [52, p.273] $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$, $\mathfrak{P}|\mathfrak{p}\Lambda$. Let $\mathrm{Ram}(A)$, $\mathrm{Ram}_\infty(A)$ and $\mathrm{Ram}_f(A)$ denote the set of places, finite places, and infinite places respectively, at which A is ramified.

Suppose $\ell = \prod_{i=1}^{k} p_i$, where $p_i \in \mathbb{Z}$ are prime numbers. Then

$$\ell\mathcal{O}_K = \prod_{i=1}^{k}\left(\prod_{j=1}^{g_i}\mathfrak{p}_{ij}^{e_{p_i}}\right),\ p_i\mathcal{O}_K = \prod_{j=1}^{g_i}\mathfrak{p}_{ij}^{e_{p_i}}.$$

We have [52, p.194]

$$\ell\Lambda = \prod_{i=1}^{k}\left(\prod_{j=1}^{g_i}\mathfrak{P}_{ij}^{e_{p_i}m_{\mathfrak{p}_{ij}})}\right), \tag{4.28}$$

where $\mathfrak{P}_{ij}$ is the prime ideal above $\mathfrak{p}_{ij}$ in Λ and $m_{\mathfrak{p}_{ij}}$ is the *local index* [52, p.270] of A at $\mathfrak{p}_{ij}$, which takes value 2 if A ramifies at $\mathfrak{p}_{ij}$, and 1 otherwise. Assume there exists $\beta \in \mathcal{N}(\Lambda)\cap\Lambda$ that satisfies $\ell = \beta\bar{\beta}$. As $\beta\Lambda = \Lambda\beta \in \mathcal{LR}(\Lambda)$, $\beta\Lambda = \overline{\beta\Lambda} = \Lambda\bar{\beta}$, so

$$(\beta\Lambda)^2 = \Lambda\bar{\beta}\beta\Lambda = \ell\Lambda,$$

which gives

$$\beta\Lambda = \prod_{i=1}^{k}\left(\prod_{j=1}^{g_i}\mathfrak{P}_{ij}^{\frac{e_{p_i}m_{\mathfrak{p}_{ij}}}{2}}\right). \tag{4.29}$$

Remark 4.18. 1. If e_{p_i} is odd, then $\mathfrak{p}_{ij} \in \mathrm{Ram}_f(A)$ for all j, i.e., $\forall\mathfrak{p}_{ij}|p_i$, $\mathfrak{p}_{ij}$ is ramified.

2. Moreover, for any prime ideal $\mathfrak{P}$ of Λ

$$v_{\mathfrak{P}}(\beta\Lambda) = \frac{1}{2}v_{\mathfrak{P}}(\ell\Lambda) = \frac{1}{2}v_{\mathfrak{P}}(p\Lambda) = \frac{e_p m_{\mathfrak{p}}}{2},$$

where $\mathfrak{p} = \mathfrak{P}\cap\mathcal{O}_K$, $p = \mathfrak{p}\cap\mathbb{Z}$.

Now consider $p \in \mathbb{Z}$ such that there exists $\mathfrak{p}|p$ which is ramified, i.e. $m_{\mathfrak{p}} = 2$. Then for $\mathfrak{P}|\mathfrak{p}$,

$$v_{\mathfrak{P}}(\mathrm{n}_{A/K}(t)^{-1}\alpha^{-1}\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}})$$

is even and $v_{\mathfrak{P}}(\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}) = v_{\mathfrak{P}}((\prod_{\mathfrak{p}\in \mathrm{Ram}_f(A)}\mathfrak{P})^{-1}) = -1$ [52, p.273]. Thus to have an Arakelov-modular lattice, by Lemma 4.15, we must have $p|\ell$ and $v_{\mathfrak{P}}(\beta) = \frac{e_p m_{\mathfrak{p}}}{2} = e_p$ is odd. Then by the above remark, for all $\mathfrak{p}|p$, $\mathfrak{p} \in \mathrm{Ram}_f(A)$. Define

$$\begin{aligned} S_{\mathrm{Ram}} &:= \{p \in \mathbb{Z} | \text{ there exists } \mathfrak{p} \text{ above } p \text{ such that } \mathfrak{p} \in \mathrm{Ram}_f(A)\}. \\ \Omega(K) &:= \{p \in \mathbb{Z} | \ p \text{ is a prime that ramifies in } K/\mathbb{Q}\}. \\ \Omega'(K) &:= \{p \in \Omega(K) \text{ and } e_p \text{ is even}\}. \end{aligned}$$

To summarize:

Lemma 4.19. If there exists an Arakelov-modular lattice of level ℓ over Λ, then

$$\ell = \prod_{p\in S_{\mathrm{Ram}}} p \prod_{p\in\Omega''(K)} p,$$

where $\Omega''(K)$ is a subset of $\Omega'(K)$.

Moreover, for all $p \in S_{\mathrm{Ram}}$, the following two conditions

1. e_p is odd, i.e. $S_{\mathrm{Ram}} \cap \Omega'(K) = \emptyset$;

2. $\forall \mathfrak{p}|p$, $\mathfrak{p} \in \mathrm{Ram}_f(A)$,

are satisfied, which are equivalent to: for all $\mathfrak{p} \in \mathrm{Ram}_f(A)$,

a. $e(\mathfrak{p}|p)$ is odd, where $p = \mathfrak{p} \cap \mathbb{Z}$;

b. $\sigma(\mathfrak{p}) \in \mathrm{Ram}_f(A)$ for all $\sigma \in G$, the Galois group of $K/\mathbb{Q}$.

Remark 4.20. 1. Note that the above Lemma implies that if there exists an Arakelov-modular lattice of level ℓ over Λ, then we must have $\mathrm{disc}\,(A)\,|\ell\mathcal{O}_K$, where

$$\mathrm{disc}\,(A) = \prod_{\mathfrak{p}\in \mathrm{Ram}_f(A)} \mathfrak{p}$$

is the reduced discriminant of A [35, p.99].

2. For a totally real Galois field K, a quaternion algebra A over K, a maximal order Λ of

A and a positive integer ℓ satisfying the conditions in the above lemma, we have

$$\beta\Lambda = \prod_{p\in S_{\text{Ram}}}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{e_p}\prod_{p\notin S_{\text{Ram}},p|\ell}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{\frac{e_p}{2}},\quad \mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K} = \prod_{p\in S_{\text{Ram}}}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{-1},$$

where $\mathfrak{P}_i|\mathfrak{p}_i$ and $\mathfrak{p}_i|p$. Then

$$\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \prod_{p\in S_{\text{Ram}}}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{e_p-1}\prod_{p\notin S_{\text{Ram}},p|\ell}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{\frac{e_p}{2}}.$$

4.3.2 Galois Extensions of Odd Degree

A direct corollary of Lemma 4.19 is obtained when K is of odd degree.

Corollary 4.21. If $n = [K:\mathbb{Q}]$ is odd and there exists an Arakelov-modular lattice of level ℓ over Λ, then

$$\ell = \prod_{p\in S_{\text{Ram}}} p.$$

Proof. Since $n = [K:\mathbb{Q}]$ is odd, by Lemma 4.19, if $p \notin S_{\text{Ram}}$ then $p \nmid \ell$. Using Lemma 4.19 again we have

$$\ell = \prod_{p\in S_{\text{Ram}}} p.$$

□

Remark 4.22. If $\ell = \prod_{p\in S_{\text{Ram}}} p$, by Remark 4.20,

$$\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \prod_{p\in S_{\text{Ram}}}\left(\prod_{\mathfrak{p}_i|p}\mathfrak{P}_i\right)^{e_p-1}.$$

By Lemma 4.19 e_p is odd, then $v_{\mathfrak{P}}(\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda))$ is even for any $\mathfrak{P}$ a prime ideal in Λ.

4.4 Totally Definite Quaternion Algebras over $K = \mathbb{Q}$

Let $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a totally definite quaternion algebra over $\mathbb{Q}$. $\mathbb{Q}_p$ will denote the completion of $\mathbb{Q}$ at the non-Archimedean evaluation corresponding to the prime integer p [42]. As there is only one infinite place, the identity, and [35, p.93]

$$\left(\frac{a,b}{\mathbb{Q}}\right)\otimes_{\mathbb{Q}}\mathbb{R} \cong \left(\frac{a,b}{\mathbb{R}}\right),$$

A is totally definite if and only if $a < 0$ and $b < 0$ [35, p.92]. Note that since the cardinality of $\mathrm{Ram}(A)$ is even [35, p.99], there are an odd number of finite places where A is ramified at, i.e., $\mathrm{Ram}_f(A)$ has odd cardinality. Moreover, $S_{\mathrm{Ram}} = \mathrm{Ram}_f(A)$ for $K = \mathbb{Q}$.

Proposition 4.23. There exists an Arakelov-modular lattice of level ℓ over Λ if and only if $\ell = \prod_{p \in \mathrm{Ram}_f(A)} p$ and there exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$.

Proof. Take $\ell = \prod_{p \in \mathrm{Ram}_f(A)} p$ and $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$. By Remark 4.22,

$$\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}(\beta\Lambda) = \prod_{p \in \mathrm{Ram}_f(A)} \mathfrak{P}^{1-1} = \Lambda.$$

By Lemma 4.14, (Λ, b_1) is an Arakelov-modular lattice of level ℓ.

By Corollary 4.21 and Lemma 4.19, the proof is completed. □

4.4.1 Existence and Classification for ℓ Prime.

Now consider ℓ being a prime integer. Our goal is to characterize the existence of Arakelov-modular lattices for primes ℓ.

The above proposition and Remark 4.16 show that for each ℓ, it suffices to consider one quaternion A that ramifies at only ℓ. Since we are looking at quaternions over the rational field, all maximal orders in A are conjugate to each other [35, p.221]. By Remark 4.16 again, for each quaternion A we are analyzing, it suffices to consider just one maximal order Λ in A. Moreover, we have the following classification result

Proposition 4.24. Take ℓ a prime integer, A a quaternion algebra over $\mathbb{Q}$ that ramifies only at ℓ and Λ a maximal order of A. Any Arakelov-modular lattice of level ℓ over Λ is isomorphic to the lattice (Λ, b_1), which is an even lattice with minimum 2 and dimension 4.

Proof. Fix a quaternion algebra $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ that ramifies at only ℓ and a maximal order Λ. By the proof of Proposition 4.23, (Λ, b_1) is an Arakelov-modular lattice of level ℓ. For any $x \in \Lambda$, $b_1(x) = \mathrm{tr}_{A/\mathbb{Q}}(x\bar{x}) = \mathrm{tr}_{A/\mathbb{Q}}\left(\mathrm{n}_{A/\mathbb{Q}}(x)\right)$. As $\mathrm{n}_{A/\mathbb{Q}}(x) \in \mathbb{Z}$, $b_1(x) \in 2\mathbb{Z}$. Hence (Λ, b_1) is even. Moreover, since $b_1(1) = 2$, (Λ, b_1) has minimum 2. Now take any Arakelov-modular lattice (Jt, b_α) over Λ of level ℓ. By Lemma 4.14 and the proof of Proposition 4.23, the following equation holds:

$$J^2 = \mathrm{n}_{A/\mathbb{Q}}(t)^{-1}\alpha^{-1}\mathcal{D}^{-1}_{\Lambda/\mathbb{Z}}(\beta\Lambda) = \mathrm{n}_{A/\mathbb{Q}}(t)^{-1}\alpha^{-1}\Lambda.$$

As $\alpha, \mathrm{n}_{A/\mathbb{Q}}(t) \in \mathbb{Q}$, let $\gamma\ell^m = (\alpha \mathrm{n}_{A\mathbb{Q}}(t))^{-1}$, where m is an integer and $\gamma \in \mathbb{Q}$. For any prime p and $\mathfrak{P}$, the prime ideal above p in Λ, we have $v_{\mathfrak{P}}(\gamma\ell^m\Lambda)$ is even. If $p \neq \ell$ and p divides the numerator or denominator of γ, as $m_p = 1$, we must have the exponent of p in the factorization of γ is even. In particular, this implies $\sqrt{\gamma} \in \mathbb{Q}$. If $p = \ell$, then $p = \mathfrak{P}^2$ with $\mathfrak{P} = \beta\Lambda$. Thus we have $J = \sqrt{\gamma}\beta^m\Lambda$. As $\sqrt{\gamma} \in \mathbb{Q}$ and $\beta \in \mathcal{N}(\Lambda)$, $\sqrt{\gamma}\beta^m \in \mathcal{N}(\Lambda)$. So $J = \sqrt{\gamma}\beta^m\Lambda = \Lambda\sqrt{\gamma}\beta^m$. Then the lattice $(Jt, b_\alpha) = (\Lambda\sqrt{\gamma}\beta^m t, b_\alpha)$. Define

$$\begin{aligned} h : \Lambda &\to \Lambda\sqrt{\gamma}\beta^m t \\ x &\mapsto x\sqrt{\gamma}\beta^m t. \end{aligned}$$

h is a bijective $\mathbb{Z}-$module homomorphism, and hence an isomorphism. Moreover, $\forall x, y \in \Lambda$

$$\begin{aligned} b_\alpha(h(x), h(y)) &= b_\alpha(x\sqrt{\gamma}\beta^m t, y\sqrt{\gamma}\beta^m t) = \mathrm{tr}_{A/\mathbb{Q}}\left(\alpha x\sqrt{\gamma}\beta^m t\bar{t}\bar{\beta}^m\sqrt{\gamma}\bar{y}\right) \\ &= \mathrm{tr}_{A/\mathbb{Q}}\left(\alpha \mathrm{n}_{A/\mathbb{Q}}(t)\,\gamma\ell^m x\bar{y}\right) = \mathrm{tr}_{A/\mathbb{Q}}(x\bar{y}) = b_1(x, y). \end{aligned}$$

Thus (Jt, b_α) is isomorphic to (Λ, b_1). □

Recall that the *Hilbert symbol* $(a, b)_p$ (or $(a, b)_v$ for v corresponding to an infinite place) is defined to be -1 if A is ramified at p (or v) and 1 otherwise. Then for finite prime p, $(a, b)_p = -1$ if and only if $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is the unique division algebra over $\mathbb{Q}_p$ [35, p.87]. Hence we will be considering quaternion algebras $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ with $a < 0, b < 0$ such that $(a, b)_\ell = -1$ and $(a, b)_p = 1$ for all prime $p \neq \ell$.

Let $p \neq 2$ be a prime integer and let $a, b, c, x, y \in \mathbb{Q}^\times$, we have [61, p.24]

1. $(ax^2, by^2)_p = (a, b)_p$;
2. $(a, b)_p(a, c)_p = (a, bc)_p$;
3. $(a, b)_p = (b, a)_p$;
4. $(a, 1 - a)_p = 1$.

The following product formula [61, p.58] holds:

$$\prod_{v \in \{\text{ infinite places}\}} (a, b)_v \prod_{p \in \{\text{ finite places}\}} (a, b)_p = 1. \tag{4.30}$$

Thus, we can focus on the case when $a, b \in \{-1, -p\}$, where p is a prime.

For $a, b \in \mathbb{Z}$ and $p \neq 2$, we have [61, p.27]

$$(a,b)_p = \begin{cases} 1 & \text{if } p \nmid a, p \nmid b \\ \left(\frac{a}{p}\right) & \text{if } p \nmid a, p || b \end{cases}, \tag{4.31}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol, which is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a square } \bmod p \\ -1, & \text{otherwise} \end{cases}.$$

Recall that A is ramified at the unique infinite place (identity), by the product formula (4.30),

$$\prod_{p \in \{\text{ finite places}\}} (a,b)_p = -1. \tag{4.32}$$

We have the following cases:

1. $a = -1, b = -1$ or $b = -2$, by Eq. (4.31), $(a,b)_p = 1$ for all prime $p \neq 2$. Then by Eq. (4.32), $(a,b)_2 = -1$. Thus $\left(\frac{a,b}{\mathbb{Q}}\right)$ is ramified only at 2.

2. $a = -1, b = -p$, where $p \neq 2$, then by Eq. (4.31), $(a,b)_q = 1$ for all prime $q \neq 2, p$ and

$$(a,b)_p = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} -1 & p \equiv 3 \bmod 4. \\ 1 & p \equiv 1 \bmod 4. \end{cases}$$

By Eq. (4.32),

$$(a,b)_2 = \begin{cases} 1 & p \equiv 3 \bmod 4. \\ -1 & p \equiv 1 \bmod 4. \end{cases}$$

Thus $\left(\frac{-1,-p}{\mathbb{Q}}\right)$ is ramified only at p if $p \equiv 3 \bmod 4$ and it is ramified only at 2 if $p \equiv 1 \bmod 4$.

3. $a = -p, b = -p$, $\left(\frac{-p,-p}{\mathbb{Q}}\right) \cong \left(\frac{-p,-p^2}{\mathbb{Q}}\right) \cong \left(\frac{-1,-p}{\mathbb{Q}}\right)$.

4. $a = -2, b = -p$, where $p \neq 2$, then by Eq. (4.31), $(a,b)_q = 1$ for all prime $q \neq 2, p$ and

$$(a,b)_p = \left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} -1 & p \equiv 3, 5 \bmod 8. \\ 1 & p \equiv 1, 7 \bmod 8. \end{cases}$$

By Eq. (4.32),

$$(a,b)_2 = \begin{cases} 1 & p \equiv 3,5 \bmod 8. \\ -1 & p \equiv 1,7 \bmod 8. \end{cases}$$

Thus $\left(\frac{-2,-p}{\mathbb{Q}}\right)$ only ramifies at p if $p \equiv 3,5 \bmod 8$ and it only ramifies at 2 if $p \equiv 1,7 \bmod 8$.

6. $a = -p, b = -q$, $p \neq q \neq 2$, then by Eq. (4.31), $(a,b)_h = 1$ for all prime $h \neq 2, p, q$ and

$$(a,b)_p = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right),$$

$$(a,b)_q = \left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Recall the reciprocity law for Legendre symbols:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

If $p, q \equiv 1 \bmod 4$, $(a,b)_2 = -1$, $(a,b)_p = \left(\frac{q}{p}\right)$, $(a,b)_q = \left(\frac{p}{q}\right)$. Thus $\left(\frac{-p,-q}{\mathbb{Q}}\right)$ ramifies at only 2 iff $\left(\frac{p}{q}\right) = 1$.

If $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$, $(a,b)_2 = 1$, $(a,b)_p = \left(\frac{q}{p}\right)$, $(a,b)_q = -\left(\frac{p}{q}\right)$ and $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. Thus $\left(\frac{-p,-q}{\mathbb{Q}}\right)$ ramifies at only p iff $\left(\frac{p}{q}\right) = -1$ and only at q iff $\left(\frac{p}{q}\right) = 1$.

If $p, q \equiv 3 \bmod 4$, $(a,b)_2 = 1$, $(a,b)_p = -\left(\frac{q}{p}\right)$, $(a,b)_q = -\left(\frac{p}{q}\right)$ and $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. Thus $\left(\frac{-p,-q}{\mathbb{Q}}\right)$ ramifies at only p iff $\left(\frac{p}{q}\right) = -1$ and only at q iff $\left(\frac{p}{q}\right) = 1$.

With the above discussion, the following lemma enables us to prove the characterization result.

Lemma 4.25. If $p \equiv 1 \bmod 8$ is a prime, there exists a prime $q \equiv 3 \bmod 4$ such that $\left(\frac{p}{q}\right) = -1$.

Proof. As $p \equiv 1 \bmod 8$, $\left(\frac{p}{q}\right) = -1$ iff $\left(\frac{q}{p}\right) = -1$. Take any $c_1 \in \{1, 2, \ldots, p-1\}$ which is a quadratic non-residue [27, p.84] of p. By Chinese Reminder Theorem [27, p.95], there exists $c \in \{1, 2, \ldots, 4p\}$ such that $c \equiv c_1 \bmod p$ and $c \equiv 3 \bmod 4$. Clearly, $\gcd(c,p) = 1$ and $\gcd(c,4) = 1$, so $\gcd(c,4p) = 1$. By Dirichlet's Theorem [27, Theorem 15], there are infinitely many primes of the form $4pn + c$, where n denotes positive integers. □

Proposition 4.26. Take A a totally definite quaternion over $\mathbb{Q}$ that ramifies at only one finite prime p, then we have exactly one of the following scenarios:

1. $p = 2$, $A \cong \left(\frac{-1,-1}{\mathbb{Q}}\right)$.
2. $p \equiv 3 \bmod 4$, $A \cong \left(\frac{-1,-p}{\mathbb{Q}}\right)$.

3. $p \equiv 5 \bmod 8$, $A \cong \left(\frac{-2,-p}{\mathbb{Q}}\right)$.

4. $p \equiv 1 \bmod 8$, $A \cong \left(\frac{-p,-q}{\mathbb{Q}}\right)$, where $q \equiv 3 \bmod 4$ is a prime such that $\left(\frac{p}{q}\right) = -1$.

Now we can characterize the existence of Arakelov-modular lattices of level ℓ for ℓ a prime integer over totally definite quaternions over $\mathbb{Q}$.

Theorem 4.27. Let A be a totally definite quaternion over $\mathbb{Q}$ and let Λ be any maximal order of A. Then there exists an Arakelov-modular lattice of level ℓ, ℓ prime, over Λ if and only if one of the situations is satisfied:

1. $A \cong \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\ell = 2$

2. $A \cong \left(\frac{-1,-\ell}{\mathbb{Q}}\right)$ and $\ell \equiv 3 \bmod 4$.

3. $A \cong \left(\frac{-2,-\ell}{\mathbb{Q}}\right)$ and $\ell \equiv 5 \bmod 8$.

4. $A \cong \left(\frac{-q,-\ell}{\mathbb{Q}}\right)$ and $\ell \equiv 1 \bmod 8$, where $q \equiv 3 \bmod 4$ is a prime such that $\left(\frac{\ell}{q}\right) = -1$.

Proof. By Propositions 4.23 and 4.26, for each case it suffices to find Λ and $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$.

As usual, let $\{1, i, j, k\}$ be a standard basis for $A = \left(\frac{a,b}{\mathbb{Q}}\right)$, i.e. $i^2 = a, j^2 = b$, and $ij = k$.

Case 1: Suppose $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\ell = 2$, take Λ with basis $\{1, i, j, \frac{1+i+j+k}{2}\}$ is a maximal order of A [35, p.204]. Then $\beta = i - j$ satisfies $2 = \beta\bar{\beta}$ and $\beta \in \Lambda$. To prove $\beta \in \mathcal{N}(\Lambda)$, it suffices to show $\beta v \beta^{-1} \in \Lambda$ for all $v \in \{1, i, j, \frac{1+i+j+k}{2}\}$:

$$\begin{aligned} (1-j)i(i-j)^{-1} &= -j \in \Lambda \\ (1-j)j(i-j)^{-1} &= -i \in \Lambda \\ (1-j)\frac{1+i+j+k}{2}(i-j)^{-1} &= \frac{1-i-j-k}{2} \in \Lambda. \end{aligned}$$

Cases 2,3,4: For $\ell \neq 2$, $A \cong \left(\frac{-q,-\ell}{\mathbb{Q}}\right)$, where

$$q \begin{cases} = 1 & \ell \equiv 3 \bmod 4 \\ = 2 & \ell \equiv 5 \bmod 8 \cdot \\ \equiv 3 \bmod 4 \text{ is a prime such that } \left(\frac{\ell}{q}\right) = -1 & \ell \equiv 1 \bmod 8 \end{cases}$$

$\mathbb{Z}[1, i, j, k]$ is always an order in A (see [35, p.84]). Take a maximal order $\Lambda \supseteq \mathbb{Z}[1, i, j, ij]$ (the existence of such a maximal order is proved in [35, p.84]). In particular, we have $j \in \Lambda$. Since $\mathrm{n}_{A/\mathbb{Q}}(j) = \ell$, if we prove $j \in \mathcal{N}(\Lambda)$ we are done.

We have [35, p.353]

$$\mathcal{N}(\Lambda) = \{x \in A^* : x \in \mathcal{N}(\Lambda_p)\ \forall p \text{ a prime integer}\}.$$

If $p \neq \ell$, then $p \notin \text{Ram}_f(A)$ and [35, p.213]

$$\mathcal{N}(\Lambda_p) = \mathbb{Q}_p^* \Lambda_p^*.$$

As $-\frac{1}{\ell} \in \mathbb{Z}_p$ [42, p.99], $j \in \Lambda_p$, $\Lambda_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \Lambda$ [35, p.203] gives $j^{-1} = -\frac{j}{\ell} \in \Lambda_p$. Hence $j \in \Lambda_p^*$ and we have $j \in \mathcal{N}(\Lambda_p)$.

If $p = \ell$, $\mathcal{N}(\Lambda_p) = A_p^*$ [35, p.208] and hence $j \in \mathcal{N}(\Lambda_p)$.

We can then conclude $j \in \mathcal{N}(\Lambda)$. □

We also have constructive proofs for cases 2 and 3. We need the following result [35, p.84,214]

1. Λ is an order in A if and only if Λ is a ring of integers in A which contains $\mathbb{Z}$ and is such that $\mathbb{Q}\Lambda = A$.

2. An order Λ in A is maximal if and only if $\text{disc}\,(\Lambda/\mathbb{Z}) = \text{disc}\,(A)^2$.

Case 2. Suppose $A \cong \left(\frac{-1,-\ell}{\mathbb{Q}}\right)$ and $\ell \equiv 3 \bmod 4$, take Λ with basis $\{1, i, \frac{1+j}{2}, \frac{i+k}{2}\}$. Clearly $\mathbb{Z} \subseteq \Lambda$ and $\mathbb{Q}\Lambda = A$. By the above, to show Λ is a maximal order we need to show

- Λ is a subring of A;
- the elements of Λ are integers, i.e. $\text{tr}_{A/\mathbb{Q}}(x), \text{n}_{A/\mathbb{Q}}(x) \in \mathbb{Z}$ for all $x \in \Lambda$;
- $\text{disc}\,(\Lambda/\mathbb{Z}) = \text{disc}\,(A)^2 = \ell^2\mathbb{Z}$.

Since Λ is a free $\mathbb{Z}-$module, Λ is closed under addition. Also $1 \in \Lambda$. To prove Λ is closed under multiplication, we just need to prove the product of any two basis elements is still in Λ. Consider the following multiplication table,

$\cdot$	i	$\frac{1+j}{2}$	$\frac{i+k}{2}$
i	-1	$\frac{i+k}{2}$	$\frac{-1-j}{2}$
$\frac{1+j}{2}$	$\frac{i-k}{2}$	$\frac{1-\ell+2j}{4}$	$\frac{(\ell+1)i}{4}$
$\frac{i+k}{2}$	$\frac{-1+j}{2}$	$\frac{2k+(1-\ell)i}{4}$	$\frac{-1-\ell}{4}$

we have

$$\frac{i-k}{2} = i - \frac{i+k}{2} \in \Lambda, \ \ \frac{-1+j}{2} = \frac{1+j}{2} - 1 \in \Lambda$$

As $\ell \equiv 3 \bmod 4$, $4|(\ell+1)$, hence

$$\frac{1-\ell+2j}{4} = \frac{1+j}{2} - \frac{\ell+1}{4} \in \Lambda, \ \ \frac{(\ell+1)i}{4} \in \Lambda, \ \ \frac{2k+(1-\ell)i}{4} = \frac{i+k}{2} - \frac{(\ell+1)i}{4} \in \Lambda.$$

We have proved that Λ is closed under multiplication and hence Λ is a subring of A. As ℓ is odd, the following reduced trace table shows that the trace of the basis elements as well as that of the product of any two basis elements are all integers. Each entry of the table corresponds to the reduced trace of the product of the element from the left and that from the top. For example, $(1,1)-$entry is given by $\mathrm{tr}_{A/\mathbb{Q}}(1 \cdot i) = 0$.

$\mathrm{tr}_{A/\mathbb{Q}}(\cdot)$	i	$\frac{1+j}{2}$	$\frac{i+k}{2}$
1	0	1	0
i	-2	0	-1
$\frac{1+j}{2}$	0	$\frac{1-\ell}{2}$	0
$\frac{i+k}{2}$	-1	0	$\frac{-1-\ell}{2}$

Recall $\ell \equiv 3 \bmod 4$, the reduced norm table shows that the norm of each basis element and also that the norm of the sum of any two basis elements are integers. Each entry of the table here corresponds to the reduced norm of the sum of the element from the left and that from the top. For example, $(1,1)-$entry is given by $\mathrm{n}_{A/\mathbb{Q}}(0+i) = 1$.

$\mathrm{n}_{A/\mathbb{Q}}(+)$	i	$\frac{1+j}{2}$	$\frac{i+k}{2}$
0	1	$(1+\ell)/4$	$(\ell+1)/4$
1	2	$(\ell+9)/4$	$(5+\ell)/4$
i	4	$(5+\ell)/4$	$(9+\ell)/4$
$\frac{1+j}{2}$	$-$	$1+\ell$	$(1+\ell)/2$
$\frac{i+k}{2}$	$-$	$-$	$1+\ell$

Since the trace of the sum of two integers is an integer and the norm of the product of two integers is an integer we have proved the sum and the product of any two basis elements is still an integer in A. As a subring of A, it follows that all the elements in Λ are integers in A. Hence Λ is an order.

The reduced discriminant of the order $\mathbb{Z}[1,i,j,k]$ is

$$\det\left(\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2\ell & 0 \\ 0 & 0 & 0 & -2\ell \end{bmatrix}\right)\mathbb{Z} = 16\ell^2\mathbb{Z}.$$

Λ is obtained from $\mathbb{Z}[1,i,j,k]$ by a basis change matrix with determinant $\frac{1}{4}$ and hence

$$\operatorname{disc}(\Lambda) = 16\ell^2 \cdot \frac{1}{4^2}\mathbb{Z} = \ell^2\mathbb{Z}.$$

We have proved Λ is a maximal order. Take $\beta = j = -1 + 2\cdot\frac{1+j}{2} \in \Lambda$, then

$$jij^{-1} = -i \in \Lambda,\ \ j\frac{i+k}{2}j^{-1} = \frac{-i-k}{2} \in \Lambda,\ \ j\frac{1+j}{2}j^{-1} = \frac{1+j}{2} \in \Lambda.$$

This shows $j\Lambda j^{-1} \subseteq \Lambda$, since [52, p.349]

$$\mathcal{N}(\Lambda) = \{x \in A^\times : x\Lambda x^{-1} \subset \Lambda\},$$

we have $\beta \in \mathcal{N}(\Lambda)$. As $\beta\bar{\beta} = \ell$, by Proposition 4.23, there exists an Arakelov-modular lattice of level ℓ over Λ.

Case 3. Suppose $\Lambda \cong \left(\frac{-2,-\ell}{\mathbb{Q}}\right)$ and $\ell \equiv 5 \bmod 8$. In this case we take Λ with basis $\{i, \frac{1+i+j}{2}, j, \frac{2+i+k}{4}\}$. As in the previous case, we consider the following three tables and Λ can be proved to be an order.

$\cdot$	i	$\frac{1+i+j}{2}$	j	$\frac{2+i+k}{4}$
i	-2	$\frac{i-2+k}{2}$	k	$\frac{i-1-j}{2}$
$\frac{1+i+j}{2}$	$\frac{i-2-k}{2}$	$\frac{i+j}{2} - \frac{\ell-1}{4}$	$\frac{j+k-\ell}{2}$	$\frac{\ell+3}{8}i$
j	$-k$	$\frac{j-k-\ell}{2}$	$-\ell$	$\frac{2j-k+\ell i}{4}$
$\frac{2+i+k}{4}$	$\frac{i-1+j}{2}$	$\frac{(3-\ell)i+4j+2k}{8}$	$\frac{2j+k-\ell i}{4}$	$\frac{(1-\ell)+2i+2k}{8}$

$\mathrm{tr}_{A/\mathbb{Q}}(\cdot)$	i	$\frac{1+i+j}{2}$	j	$\frac{2+i+k}{4}$
1	0	1	0	1
i	-4	-2	0	-1
$\frac{1+i+j}{2}$	-2	$-\frac{\ell+1}{2}$	$-\ell$	0
j	0	$-\ell$	-2ℓ	0
$\frac{2+i+k}{4}$	-1	0	0	$\frac{1-\ell}{4}$

$\mathrm{n}_{A/\mathbb{Q}}(+)$	i	$\frac{1+i+j}{2}$	j	$\frac{2+i+k}{4}$
0	2	$(\ell+3)/4$	ℓ	$(\ell+3)/8$
1	3	$(11+\ell)/4$	$1+\ell$	$(19+\ell)/8$
i	8	$(\ell+19)/4$	$\ell+2$	$(\ell+27)/8$
$\frac{1+i+j}{2}$	-	$\ell+3$	$(9\ell+3)/4$	$(17+3\ell)/8$
j	-	-	4ℓ	$(9\ell+3)/8$
$\frac{2+i+j}{4}$	-	-	-	$(\ell+3)/2$

Then similarly, as Λ has discriminant $\ell^2\mathbb{Z}$, it is a maximal order. By direct computation, we can prove $\beta = j \in \Lambda \cap \mathcal{N}(\Lambda)$.

Remark 4.28. The above computations enable us to find Arakelov-modular lattices of level ℓ for all $\ell \equiv 3 \bmod 4$ and $\ell \equiv 5 \bmod 8$. Similar techniques can also be applied for square-free composite integers ℓ.

By Proposition 4.23, there exists an Arakelov-modular lattice of level ℓ over Λ.

Example 4.29.

1. Take $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and Λ with basis $\{1, i, j, \frac{1+i+j+k}{2}\}$, (Λ, b_1) is a $2-$modular lattice.
2. Take $A = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ and Λ with basis $\{1, i, \frac{1+j}{2}, \frac{i+k}{2}\}$, (Λ, b_1) is a $3-$modular lattice.
3. Take $A = \left(\frac{-2,-5}{\mathbb{Q}}\right)$ and Λ with basis $\{i, \frac{1+i+j}{2}, j, \frac{2+i+k}{4}\}$, (Λ, b_1) is a $5-$modular lattice.
4. Take $A = \left(\frac{-3,-17}{\mathbb{Q}}\right)$ and Λ with basis $\{1, \frac{1+i}{2}, \frac{3+i+3j+k}{6}, \frac{-3+i-2k}{6}\}$, (Λ, b_1) is a $17-$modular lattice.

Note that the same construction for Examples 1 and 2 above appeared in [37, p.266].

4.4.2 The Case when ℓ is a Positive Integer

Now we consider the case when ℓ is not necessarily square-free, i.e. ℓ being any positive integer. Let A be a totally definite quaternion algebra over $\mathbb{Q}$ and let Λ be any maximal

order of A. Let r_p denote the exponent of prime p in the prime factorization of ℓ, i.e. $\ell = \prod_p p^{r_p}$. If there exists an Arakelov-modular lattice of level ℓ over Λ, by Lemma 4.14 there exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$. And as in Eqs. (4.28) and (4.29) we have

$$\ell\Lambda = \prod_{p|\ell, \mathfrak{P}|p} \mathfrak{P}^{r_p m_p}, \quad \beta\Lambda = \prod_{p|\ell, \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p m_p}{2}}.$$

We can see that if m_p is odd, i.e. if $p \notin \mathrm{Ram}_f(A)$, r_p must be even. Then

$$\beta\Lambda = \prod_{r_p \text{ even},\, p \notin \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p}{2}} \prod_{p|\ell, p \in \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{r_p},$$

and

$$\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda) = \prod_{r_p \text{ even},\, p \notin \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p}{2}} \prod_{p|\ell, p \in \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{r_p - 1} \prod_{p \nmid \ell, p \in \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{-1}.$$

As $\mathrm{n}_{A/\mathbb{Q}}(t)^{-1}\alpha^{-1} \in \mathbb{Q}$, if $p \in \mathrm{Ram}_f(A)$, $v_{\mathfrak{P}}(\mathrm{n}_{A/\mathbb{Q}}(t)^{-1}\alpha^{-1})$ is even, thus we must have $\forall p \in \mathrm{Ram}_f(A)$, $p|\ell$ and r_p is odd.

Proposition 4.30. Take a positive integer $\ell = \prod_p p^{r_p}$, there exists an Arakelov-modular lattice over Λ if and only if the following conditions are all satisfied:

1. $\ell = \ell_1^2 \ell_2$, where $\ell_2 = \prod_{p \in \mathrm{Ram}_f(A)} p^{r_p}$, ℓ_1 is a positive integer coprime with ℓ_2;
2. For all $p|\ell_2$, r_p is odd;
3. There exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$.

Proof. In view of the above discussion, it suffices to prove that if the conditions are satisfied, then there exists an Arakelov-modular lattice of level ℓ. We have

$$\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda) = \prod_{p|\ell_1, \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p}{2}} \prod_{p|\ell_2, \mathfrak{P}|p} \mathfrak{P}^{r_p - 1}.$$

Let $\alpha = \ell_1$, then

$$\alpha^{-1}\mathcal{D}_{\Lambda/\mathbb{Z}}^{-1}(\beta\Lambda) = \prod_{p|\ell_2, \mathfrak{P}|p} \mathfrak{P}^{r_p - 1}.$$

As r_p are all odd for $p|\ell_2$, we can take

$$J = \prod_{p|\ell_2, \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p - 1}{2}} = \prod_{p \in \mathrm{Ram}_f(A), \mathfrak{P}|p} \mathfrak{P}^{\frac{r_p - 1}{2}}.$$

Let $t = 1$, $I = Jt$, then by Lemma 4.14, (I, b_α) is an Arakelov-modular lattice of level ℓ. □

Remark 4.31. If ℓ is square-free, then $\ell_1 = 1$, $r_p = 1$ for all $p|\ell_2$ and we get the same statement as in Proposition 4.23.

Since we are considering totally definite quaternion algebras A, $\mathrm{Ram}_f(A) \neq \emptyset$. Thus $\ell_2 \neq 1$, which implies

Corollary 4.32. There does not exist any Arakelov-modular lattice over Λ of level ℓ for ℓ a square.

In Table 4.1 we list some examples of Arakelov-modular lattices with level ℓ such that ℓ is not square-free, constructed from totally definite quaternion algebras over $\mathbb{Q}$. We also list the minimum and kissing number for the lattices obtained for comparison.

Recall from Definition 2.7 that the *minimum* of (L, b) is

$$\min\{b(x, x) : x \in L, x \neq 0\},$$

and the *kissing number* of (L, b) is

$$\text{cardinality of } \{x \in L : b(x, x) = \mu_L\}.$$

As mentioned in Section 2.2, those are two common properties attracting attentions due to their close connections to sphere packing and other research areas. Normally the goal is to find lattices with bigger minimum or bigger kissing number. The highest known kissing number for a lattice in dimension 4 is 24 [19, p.22]. The minima of extremal (see Definition 2.11) 4−dimensional ℓ−modular lattices are listed in Table 4.2 for interested readers. To the best of our knowledge, the lattices in Table 4.1 are new. In particular, the first row of Table 4.1 gives us a new lattice with kissing number 24 in dimension 4.

ℓ	ℓ_1	ℓ_2	(a, b)	I	α	min	kn
8	1	2^3	$(-1, -1)$	$\mathfrak{P}_2$	1	4	24
27	1	3^3	$(-1, -3)$	$\mathfrak{P}_3$	1	6	12
12	2	3	$(-1, -3)$	Λ	2	4	12

Table 4.1: Examples of lattices (I, b_α) obtained from $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ (here $\mathfrak{P}_p$ is the prime ideal above p) such that (I, b_α) is an even 4−dimensional Arakelov-modular lattice of level $\ell = \ell_1^2 \cdot \ell_2$ (ℓ_2 is coprime with ℓ_1) with minimum min and kissing number kn.

ℓ	1	2	3	5	6	7	11	14	15	23
Minimum	2	2	2	2	2	3	4	4	4	4

Table 4.2: Minima of extremal $4-$dimensional $\ell-$modular lattices

4.5 Maximal Real Subfield of Cyclotomic Field (odd degree)

Let $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, where ζ_{p^r} is a primitive p^rth root of unity, $p \equiv 3 \bmod 4$ is a prime and r is a positive integer. Then $K = \mathbb{Q}(\zeta_{p^r}) \cap \mathbb{R}$ is the maximal real subfield of $\mathbb{Q}(\zeta_{p^r})$. We have K is a totally real Galois extension with ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ and degree $n = [K : \mathbb{Q}] = \frac{p^r(p-1)}{2}$ [62, p.15]. Since $p \equiv 3 \bmod 4$, n is odd. For simplicity, we will write ζ instead of ζ_{p^r} if there is no confusion.

The only prime that ramifies in K is p and p is totally ramified. More precisely, let $\mathfrak{p}$ be the prime ideal in $\mathcal{O}_K$ above p, then

$$e_p = v_{\mathfrak{p}}(p) = \frac{p^{r-1}(p-1)}{2}.$$

Furthermore, $\mathfrak{p}$ is the only prime that ramifies in $\mathbb{Q}(\zeta)/K$ [62, p.16]. Let $\mathfrak{Q}$ be the prime ideal above $\mathfrak{p}$ in $\mathbb{Q}(\zeta)$, then $\mathfrak{p} = \mathfrak{Q}^2$ and $\mathcal{D}_{\mathbb{Q}(\zeta)/K} = \mathfrak{Q}$ [42, p.199]. We also have

$$\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathfrak{Q}^{p^{r-1}(pr-r-1)} \ [59, p.65],$$

and

$$\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathcal{D}_{\mathbb{Q}(\zeta)/K}\mathcal{D}_{K/\mathbb{Q}} \ [42, p.195].$$

Hence

$$v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}) = \frac{1}{2}(v_{\mathfrak{Q}}(\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}}) - v_{\mathfrak{Q}}(\mathcal{D}_{\mathbb{Q}(\zeta)/K})) = \frac{1}{2}(p^{r-1}(pr-r-1)-1).$$

As $p \equiv 3 \bmod 4$, $p^{r-1}(pr-r-1) \equiv 1 \bmod 4$ for all r. Then we have $v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}})$ is even.

As before, let A be a totally definite quaternion algebra over K and Λ be a maximal order of A. We have the following

Proposition 4.33. There exists an Arakelov-modular lattice of level ℓ over Λ if and only if all the following conditions are satisfied:

1. For all $p \in S_{\text{Ram}}$, if $\mathfrak{p}|p$, then $\mathfrak{p} \in \text{Ram}_f(A)$;

2.
$$\ell = \prod_{p \in S_{\text{Ram}}} p;$$

3. There exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$.

Proof. The necessity of the three conditions follows from Corollary 4.21.

Assume the three conditions are satisfied. Then by Remark 4.22 and the above the discussion
$$v_{\mathfrak{P}}(\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda))$$
is even for any $\mathfrak{P}$ a prime ideal in Λ. By Lemma 4.15, taking $\alpha = t = 1$, we get an Arakelov-modular lattice of level ℓ.

To be more specific, let $\mathfrak{p}_p$ be the prime ideal in $\mathcal{O}_K$ above p and $\mathfrak{P}_p$ the prime ideal in $\mathcal{O}_K$ above $\mathfrak{p}$. For any $p' \neq p$ a prime integer, $e_{p'} = 1$, so

- If $p \notin S_{\text{Ram}}$
$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \mathfrak{P}_p^{-\frac{1}{2}(p^{r-1}(pr-r-1)-1)}.$$

- If $p \in S_{\text{Ram}}$,
$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \mathfrak{P}_p^{-\frac{1}{2}(p^{r-1}(pr-r-1)-1)\cdot 2}\mathfrak{P}_p^{e_p-1} = \mathfrak{P}_p^{p^{r-1}(\frac{p-1}{2}-pr+r+1)}.$$

Let $I = \mathfrak{P}_p^{-\frac{1}{4}(p^{r-1}(pr-r-1)-1)}$ if $p \notin S_{\text{Ram}}$ and let $I = \mathfrak{P}_p^{\frac{1}{2}p^{r-1}(\frac{p-1}{2}-pr+r+1)}$ if $p \in S_{\text{Ram}}$. Then by Lemma 4.14, (I, b_1) is an Arakelov-modular lattice of level ℓ. □

4.5.1 Examples

In this section we give some examples for $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, $A = \left(\frac{a,b}{K}\right)$ with standard basis $\{1, i, j, k\}$, Λ a maximal order of A such that there exists Arakelov-modular modular lattices over Λ.

As mentioned in Section 4.4.2, the minimum and kissing number of a lattice are two properties attracting researchers' attentions and lattices with large minimum or large kissing number are more desirable [19]. In general it is difficult to calculate the upper bounds on the kissing numbers of lattices [19, p.21]. As the lattices we construct in this chapter are all of dimensions multiples of 4, for comparison, we list in Table 4.3 the highest kissing number presently known for lattices with dimension a multiple of 4, up to 128 [56]. And

in Table 4.4 we list the minima of extremal lattices (see Definition 2.11) in dimensions that are involved in our examples later.

Dim	4	8	12	16	20	24	28	32
KN	24	240	756	4320	17400	196560	197736	261120
Dim	36	40	44	48	64	72	80	128
KN	274944	399360	2708112	52416000	138458880	6218175600	6218175840	218044170240

Table 4.3: Highest kissing number, "KN", presently known for lattices with dimension a multiple of 4 up to dimension 128 [56]

Dim \ ℓ	1	2	3	5	6	7	11	14	15	23
8	2	2	2	4	4	4	6	6	6	10
12	2	2	4	4	4	6	8	8	8	14
20	2	4	4	6	6	8	12	12	12	12
24	4	4	6	8	8	10	14	14	14	26
36	4	6	8	10	10	14	20	20	20	38
40	4	6	8	12	12	14	22	22	22	42
44	4	6	8	12	12	16	24	24	24	46
84	8	12	16	22	22	30	44	44	44	86

Table 4.4: Minima of extremal Dim-dimensional $\ell-$modular lattices.

Construction of an existing lattice

We first give two constructions that both give the lattice 'G2^6' from the list [56].

Example 4.34. Take $p = 7, r = 1, A = \left(\frac{-1,-3}{K}\right)$, Λ with basis $\{1, i, i+j, 1+k\}$. Then $S_{\text{Ram}} = \{3\}$ and $\text{Ram}_f(A) = \{3\mathcal{O}_K\}$, so $\ell = 3$. Take $\beta = k$, then $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ and $\ell = \beta\bar{\beta}$. $(\mathfrak{P}_7^{-2}, b_1)$ gives an even modular lattice of level 3 and dimension 12 with minimum 2, which is the lattice 'G2^6'.

Example 4.35. Take $p = 3, r = 2, A = \left(\frac{-1,-3}{K}\right)$, Λ with basis $\{1, i, 3i+j, 3+k\}$. Then $S_{\text{Ram}} = \{3\}$ and $\text{Ram}_f(A) = \{3\mathcal{O}_K\}$, so $\ell = 3$. Take $\beta = j$, then $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ and $\ell = \beta\bar{\beta}$. $(\mathfrak{P}_3^{-3}, b_1)$ gives the same $12-$dimensional modular lattice of level 3.

For $p \notin S_{\text{Ram}}$

We list examples for $p \notin S_{\text{Ram}}$ in Table 4.5. Each row corresponds to one lattice, where we take $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, A a totally definite quaternion algebra that ramifies at only one finite place $\ell \neq p$ and Λ a maximal order of A. By Proposition 4.33, the ideal lattice (I, b_1) with $I = \mathfrak{P}_p^{-\frac{1}{4}(p^{r-1}(pr-r-1)-1)}$, where $\mathfrak{P}_p$ is the prime ideal in Λ over p, is an $\ell-$modular lattice. For simplicity, we use z to denote $\zeta_{p^r} + \zeta_{p^r}^{-1}$.

Dim	p	r	ℓ	(a,b)	min	kn
12	3	2	2	$(z-2,-2)$	2	72
12	3	2	5	$(-z^2-z,-5)$	2	72
12	3	2	7	$(-1,-7)$	2	12
12	3	2	11	$(-z^2-z,-11)$	2	72
12	3	2	13	$(-z^2-z-1,,-13)$	2	6
12	3	2	23	$(-1,-23)$	2	12
12	7	1	2	$(z^2+z-3,-2)$	2	72
12	7	1	5	$(z^2-4,,-20z^2)$	2	42
12	7	1	23	$(-z^2+z-1,-23)$	2	6
20	11	1	2	$(-1,-2)$	2	120
20	11	1	3	$(-1,-3)$	2	60
20	11	1	5	$(-2z^4-2z^3+2z^2+z-1,-5)$	2	10
20	11	1	7	$(-7,z^3-3z-2)$	2	10
20	11	1	23	$(-2,-23)$	2	10
36	3	3	2	$(-2,-z^8+8z^6-z^5-22z^4+5z^3+24z^2-6z-9)$	2	2
36	3	3	5	$(-5,-2z^8-3z^7+15z^6+23z^5-31z^4-50z^3+10z^2+23z+1)$	2	2
36	3	3	7	$(-7,-3z^8+3z^7+24z^6-21z^5-59z^4+40z^3+47z^2-15z-15)$	2	2
36	3	3	11	$(-11,z^8+z^7-7z^6-5z^5+15z^4+4z^3-11z^2+3z-1)$	2	2
36	3	3	23	$(-23,-3z^8-z^7+23z^6+7z^5-57z^4-16z^3+51z^2+11z-18)$	2	2
36	19	1	2	$(-2,z^8+z^7-7z^6-5z^5+15z^4+4z^3-11z^2+2z-1)$	2	18
36	19	1	3	$(-3,z^6+z^5-6z^4-5z^3+10z^2+5z-6)$	2	54
36	19	1	5	$(-5,6z^8+z^7-40z^6-10z^5+76z^4+33z^3-38z^2-27z-7)$	2	18
36	19	1	7	$(-7,2z^7-z^6-14z^5+7z^4+27z^3-12z^2-9z-2)$	2	18
36	19	1	11	$(-11,z^8+z^7-7z^6-7z^5+15z^4+15z^3-10z^2-9z-2)$	2	18
36	19	1	23	$(-23,z^8-7z^6+z^5+13z^4-7z^3-4z^2+8z-7)$	2	18
44	23	1	2	$(-2,z^{10}+2z^9-7z^8-14z^7+15z^6+29z^5-12z^4-18z^3+5z^2-4)$	2	22
44	23	1	3	$(-3,2z^{10}+2z^9-19z^8-17z^7+64z^6+48z^5-92z^4-49z^3+55z^2+11z-14)$	2	66
44	23	1	5	$(-5,-3z^{10}-z^9+25z^8+5z^7-66z^6-3z^5+55z^4-9z^3-3z^2+5z-8)$	2	22
44	23	1	7	$(-7,z^9+2z^8-7z^7-16z^6+13z^5+40z^4+z^3-31z^2-14z-2)$	2	22
44	23	1	11	$(-11,-z^{10}-z^9+10z^8+7z^7-37z^6-13z^5+62z^4+2z^3-43z^2+4z+1)$	2	22
84	7	2	2	$(-1,-2)$	4	1584
84	7	2	3	$(-1,-3)$	4	792

Table 4.5: Examples of lattices (I,b_1), where $I=\mathfrak{P}_p^{-\frac{1}{4}(p^{r-1}(pr-r-1)-1)}$ and $\mathfrak{P}_p$ is the prime ideal in Λ over p, obtained from $K=\mathbb{Q}(\zeta_{p^r}+\zeta_{p^r}^{-1})$, totally definite quaternion $A=\left(\frac{a,b}{K}\right)$ over K, $p\notin S_{\text{Ram}}$, such that (I,b_1) is $\ell-$modular with minimum min and kissing number kn.

For $p\in S_{\text{Ram}}$

We list a few examples for $p\in S_{\text{Ram}}$ in Table 4.6. Similarly as above, each row corresponds to one lattice, where we take $K=\mathbb{Q}(\zeta_{p^r}+\zeta_{p^r}^{-1})$, A a totally definite quaternion algebra that ramifies at only one finite place p and Λ a maximal order of A. By Proposition 4.33, the ideal lattice (I,b_1) with $I=\mathfrak{P}_p^{\frac{1}{2}p^{r-1}(\frac{p-1}{2}-pr+r+1)}$, where $\mathfrak{P}_p$ is the prime ideal in Λ over p, is an $\ell-$modular lattice.

4.6 Galois Extension with Even Degree

In this section, we will prove some existence results for the case when K is a totally real Galois extension with degree of extension $[K:\mathbb{Q}]$ being even. As before, A will be a totally definite quaternion algebra over K and Λ a maximal order of A. ℓ will be a positive square-

Dim	p	r	(a,b)	min	kn
12	7	1	$(-1,-7)$	4	84
20	11	1	$(-1,-11)$	6	220
36	3	3	$(-1,-3)$	2	108
44	23	1	$(-1,-23)$	12	1012

Table 4.6: Examples of lattices (I, b_1), where $I = \mathfrak{P}_p^{\frac{1}{2}p^{r-1}(\frac{p-1}{2}-pr+r+1)}$ and $\mathfrak{P}_p$ is the prime ideal in Λ over p, obtained from $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, totally definite quaternion $A = \left(\frac{a,b}{K}\right)$ over K, $p \in S_{\text{Ram}}$, such that (I, b_1) is $p-$modular with minimum min and kissing number kn.

free integer.

4.6.1 Totally Real Quadratic Field

Let $K = \mathbb{Q}(\sqrt{d})$ be a totally real quadratic field, where d is a square-free positive integer. The discriminant of K is (see [59, p.65] and [42, p.197])

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2,3 \bmod 4 \end{cases},$$

and

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \end{cases}, \quad \mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = \begin{cases} (\sqrt{d}) & \text{if } d \equiv 1 \bmod 4 \\ (2\sqrt{d}) & \text{if } d \equiv 2,3 \bmod 4 \end{cases}.$$

The set of primes ramified in $K/\mathbb{Q}$ are precisely those dividing Δ_K and the ramification index for any ramified prime is 2 [59, p.55]. So

$$\Omega'(K) = \Omega(K) = \begin{cases} \{p : p|d\} & d \equiv 1,2 \bmod 4 \\ \{p : p|d\} \cup \{2\} & d \equiv 3 \bmod 4 \end{cases}.$$

We have

Proposition 4.36. If the following conditions are satisfied, then there exists an Arakelov-modular lattice of level ℓ over Λ.

1. There exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$;

2.
$$\ell = \begin{cases} \prod_{p \in S_{\text{Ram}}} p \prod_{p \in \Omega(K), p \neq 2} p & d \equiv 3 \bmod 4 \\ \prod_{p \in S_{\text{Ram}}} p \prod_{p \in \Omega(K)} p & d \equiv 1, 2 \bmod 4 \end{cases};$$

3. $S_{\text{Ram}} \cap \Omega(K) = \emptyset$;

4. For all $p \in S_{\text{Ram}}$, if $\mathfrak{p}|p$, then $\mathfrak{p} \in \text{Ram}_f(A)$.

Proof. Assume all four conditions are satisfied. For any $p \in \Omega(K)$, let $\mathfrak{p}_p$ be the prime ideal above p in $\mathcal{O}_K$ and $\mathfrak{P}_p$ the prime ideal above $\mathfrak{p}_p$ in Λ. As $S_{\text{Ram}} \cap \Omega(K) = \emptyset$, if $p \in S_{\text{Ram}}$, $e_p = 1$. If $p \in \Omega(K)$, p is totally ramified with $e_p = 2$. We have

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\Lambda = \begin{cases} \prod_{p \in \Omega(K)} \mathfrak{P}_p^{-1} & d \equiv 1 \bmod 4 \\ \mathfrak{P}_2^{-2} \prod_{p \in \Omega(K), p \neq 2} \mathfrak{P}_p^{-1} & d \equiv 3 \bmod 4 \\ \mathfrak{P}_2^{-3} \prod_{p \in \Omega(K), p \neq 2} \mathfrak{P}_p^{-1} & d \equiv 2 \bmod 4 \end{cases}.$$

By Remark 4.20,

$$\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \begin{cases} \prod_{p \in \Omega(K)} \mathfrak{P}_p & d \equiv 1, 2 \bmod 4 \\ \prod_{p \in \Omega(K), p \neq 2} \mathfrak{P}_p & d \equiv 3 \bmod 4 \end{cases}.$$

Hence

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \begin{cases} \Lambda & d \equiv 1 \bmod 4 \\ \mathfrak{P}_2^{-2} & d \equiv 2, 3 \bmod 4 \end{cases}.$$

Then by Lemma 4.14, the ideal lattice (I, b_1), where

$$I = \begin{cases} \Lambda & d \equiv 1 \bmod 4 \\ \mathfrak{P}_2^{-1} & d \equiv 2, 3 \bmod 4 \end{cases},$$

is an Arakelov-modular lattice of level ℓ. □

4.6.2 Maximal Real Subfield of Cyclotomic Field – Prime Power Case

Consider $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ with $p \equiv 1 \bmod 4$. Similarly as in Section 4.5, $K = \mathbb{Q}(\zeta_{p^r}) \cap \mathbb{R}$ is a totally real number field. The only prime that ramifies in $K/\mathbb{Q}$ is p with ramification

index

$$e_p = \frac{p^{r-1}(p-1)}{2},$$

which is an even number. In particular we have $\Omega'(K) = \Omega(K)$. Moreover,

$$v_{\mathfrak{p}}(\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}) = \frac{1}{2}(p^{r-1}(pr-r-1)-1)$$

is odd, where $\mathfrak{p}$ is the prime ideal above p in $\mathcal{O}_K$. Then

Proposition 4.37. If the following conditions are satisfied, then there exists an Arakelov-modular lattice of level ℓ over Λ.

1. There exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$;
2. $$\ell = p \prod_{p' \in S_{\text{Ram}}} p';$$
3. $p \notin S_{\text{Ram}}$;
4. For all $p' \in S_{\text{Ram}}$, if $\mathfrak{p}'|p'$, then $\mathfrak{p}' \in \text{Ram}_f(A)$;
5. $p \equiv 5 \bmod 8$.

Proof. Assume all the conditions are satisfied. As $p \notin S_{\text{Ram}}$, for any $p' \in S_{\text{Ram}}$, $e_{p'} = 1$. Let $\mathfrak{P}$ be the ideal in Λ above $\mathfrak{p}$, which is the ideal in $\mathcal{O}_K$ above p. By the above

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\Lambda = \mathfrak{P}^{-\frac{1}{2}(p^{r-1}(pr-r-1)-1)}.$$

By Remark 4.20,

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \mathfrak{P}^{-\frac{1}{2}(p^{r-1}(pr-r-1)-1)+\frac{e_p}{2}}.$$

As $p \equiv 5 \bmod 8$, e_p is odd. $-\frac{1}{2}(p^{r-1}(pr-r-1)-1)$ is also odd. Thus by Lemma 4.14, the ideal lattice (I, b_1), where

$$I = \mathfrak{P}^{-\frac{1}{4}(p^{r-1}(pr-r-1)-1)+\frac{e_p}{4}}$$

is an Arakelov-modular lattice of level ℓ. □

4.6.3 Maximal Real Subfield of Cyclotomic Field – Non-prime Power Case

Consider $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m \not\equiv 2 \bmod 4$ not a prime power. Then $K = \mathbb{Q}(\zeta_m) \cap \mathbb{R}$ is the maximal real subfield of $\mathbb{Q}(\zeta_m)$. K is a totally real Galois extension with $\mathcal{O}_K = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$

and degree $n = \varphi(m) = m\prod_{p|m}(1-1/p)$ [62, p.15]. Suppose $m = \prod_{i=1}^{s} p_i^{r_i}$. The primes that are ramified in $K/\mathbb{Q}$ are precisely $p_1, \ldots, p_m$ and

$$e_{p_i} = p_i^{r_i-1}(p_i - 1),$$

which are even. In particular we have $\Omega'(K) = \Omega(K)$. Let $\{\mathfrak{p}_{ij}\}_{1\le j\le g_i}$ be the prime ideals in $\mathcal{O}_K$ above p_i with corresponding prime ideals $\{\mathfrak{P}_{ij}\}_{1\le j\le g_i}$ in Λ. Then

$$\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = \prod_{i=1}^{s}\left(\prod_{j=1}^{g_i}\mathfrak{p}_{ij}\right)^{p_i^{r_i-1}(p_i r_i - r_i - 1)}.$$

Proposition 4.38. If the following conditions are satisfied, then there exists an Arakelov-modular lattice of level ℓ over Λ:

1. For all $p|n$, $p \equiv 3 \bmod 4$;
2. There exists $\beta \in \mathcal{N}(\Lambda) \cap \Lambda$ such that $\ell = \beta\bar{\beta}$;
3. $\Omega(K) \cap S_{\text{Ram}} = \emptyset$;
4. For all $p \in S_{\text{Ram}}$, if $\mathfrak{p}|p$, then $\mathfrak{p} \in \text{Ram}_f(A)$;
5. $$\ell = \prod_{p\in S_{\text{Ram}}} p \prod_{i=1}^{s} p_i.$$

Proof. Assume all the conditions are satisfied, then

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\Lambda = \prod_{i=1}^{s}\left(\prod_{j=1}^{g_i}\mathfrak{P}_{ij}\right)^{-p_i^{r_i-1}(p_i r_i - r_i - 1)}.$$

By Remark 4.20,

$$\mathcal{D}^{-1}_{\mathcal{O}_K/\mathbb{Z}}\mathcal{D}^{-1}_{\Lambda/\mathcal{O}_K}(\beta\Lambda) = \prod_{i=1}^{m}\left(\prod_{j=1}^{g_i}\mathfrak{P}_{ij}\right)^{\frac{e_{p_i}}{2} - p_i^{r_i-1}(p_i r_i - r_i - 1)}.$$

As $p \equiv 3 \bmod 4$, $\frac{e_p}{2} - p_i^{r_i-1}(p_i r_i - r_i - 1)$ is even. And by Lemma 4.14, the lattice (I, b_1), where

$$I = \prod_{i=1}^{m}\left(\prod_{j=1}^{g_i}\mathfrak{P}_{ij}\right)^{\frac{e_{p_i}}{4} - \frac{1}{2}p_i^{r_i-1}(p_i r_i - r_i - 1)}$$

is an Arakelov-modular lattice of level ℓ. □

4.6.4 Examples

In Table 4.7 we list some examples of Arakelov-modular lattices constructed from totally definite quaternion algebras over Galois fields with even degree. Then we give a construction of an existing lattice $Q_8(1)$ [51] in Example 4.39.

Dim	ℓ	K	(a,b)	I	min	kn
8	6	$\mathbb{Q}(\sqrt{6})$	$(-1,-1)$	$\mathfrak{P}_2^{-1}$	2	24
8	14	$\mathbb{Q}(\sqrt{14})$	$(-1,-1)$	$\mathfrak{P}_2^{-1}$	2	24
24	13	$\mathbb{Q}(\zeta_{13}+\zeta_{13}^{-1})$	$(-1,-13)$	$\mathfrak{P}_{13}^{-1}$	8	72
24	21	$\mathbb{Q}(\zeta_{21}+\zeta_{21}^{-1})$	$(-1,-21)$	$\mathfrak{P}_7^{-1}$	12	744
40	5	$\mathbb{Q}(\zeta_{25}+\zeta_{25}^{-1})$	$(-1,-5)$	$\mathfrak{P}_5^{-6}$	4	120

Table 4.7: Examples of lattices (I, b_1) constructed from Galois field K with even degree, totally definite quaternion algebra $A = \left(\frac{a,b}{K}\right)$ over K, such that (I, b_1) is an even Arakelov-modular lattice of level ℓ with dimension Dim, minimum $\min$ and kissing number kn. Here $\mathfrak{P}_p$ denotes the prime ideal above p.

Construction of an existing lattice

Example 4.39. Take $d = \ell = 5$, $A = \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{d})}\right)$ which only ramifies at infinite places. By the proof of Proposition 4.36, (Λ, b_1) is an Arakelov-modular lattice of level 5 and dimension 8. Furthermore, this lattice is even with minimum 4 and hence it is the unique $8-$dimensional extremal (see Definition 2.11) $5-$modular lattice $Q_8(1)$ [51].

Remark 4.40. To the best of our knowledge, the lattices in Tables 4.5, 4.6 and 4.7 are new.

For a more general setting, as mentioned in Remark 4.2, whenever there is a trace form and an involution on a separable algebra, a positive definite symmetric bilinear form b_α can be defined with a proper choice of α. The concepts of ideal, order and different also exist for a separable $K-$algebra, where K is a field [52]. The future work will be generalizing the construction of Arakelov-modular lattices to separable algebras.

Chapter 5

Construction A over Number Fields

In this chapter, we present a variation of Construction A for constructing modular lattices. Let K be a Galois number field of degree n which is either totally real or a CM field. Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above the prime p. We have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$, where f is the inertia degree of p. Define ρ to be the map of reduction modulo $\mathfrak{p}$ componentwise as follows:

$$\begin{array}{rccc} \rho: & \mathcal{O}_K^N & \to & \mathbb{F}_{p^f}^N \\ & (x_1, \ldots, x_N) & \mapsto & (x_1 \bmod \mathfrak{p}, \ldots, x_N \bmod \mathfrak{p}) \end{array} \tag{5.1}$$

for some positive integer N. Let $C \subseteq \mathbb{F}_{p^f}^N$ be a linear code over $\mathbb{F}_{p^f}$, that is a k-dimensional subspace of $\mathbb{F}_{p^f}^N$. As ρ is a $\mathbb{Z}-$module homomorphism, $\rho^{-1}(C)$ is a submodule of $\mathcal{O}_K^N$. Since $\mathcal{O}_K$ is a free $\mathbb{Z}-$module of rank n, $\rho^{-1}(C)$ is a free $\mathbb{Z}-$module of rank nN. Let $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$ be the symmetric bilinear form defined by

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i) \tag{5.2}$$

where $\alpha \in K \cap \mathbb{R}$ and $\bar{y}_i$ denotes the complex conjugate of y_i if K is CM (and $\bar{y}_i$ is understood to be y_i if K is totally real). If α is furthermore totally positive, i.e., $\sigma_i(\alpha) > 0$, for $\sigma_1(\text{the identity}), \sigma_2, \ldots, \sigma_n$ all elements of the Galois group of K over $\mathbb{Q}$, then b is positive definite:

$$b_\alpha(\boldsymbol{x}, \boldsymbol{x}) = \sum_{i=1}^{N} \mathrm{Tr}\,(\alpha x_i \bar{x}_i) = \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha) |\sigma_j(x_i)|^2 > 0,$$

$\forall \boldsymbol{x} \in \mathcal{O}_K^N$, $\boldsymbol{x}$ nonzero. If we take α in the codifferent $\mathcal{D}_K^{-1} = \{x \in K : \mathrm{Tr}\,(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}$ of K, then $\mathrm{Tr}\,(\alpha x_i \bar{y}_i) \in \mathbb{Z}$.

The pair $(\rho^{-1}(C), b_\alpha)$ thus forms a lattice of rank (or dimension) nN, which is integral when $\alpha \in \mathcal{D}_K^{-1}$ but also in other cases, depending on the choice of C, as we will see several times next.

This method of constructing lattices from linear codes is usually referred to as Construction A [19]. The principle is well known, albeit not using the exact above formulation. The original binary Construction A, due to Forney [26], uses $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $\mathfrak{p} = 2$ and typically $\alpha = 1/2$ (sometimes α is chosen to be 1). The binary Construction A can also be seen as a particular case of the cyclotomic field approach proposed by Ebeling [22], which in turn is a particular case of the above construction. For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity, and note that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Take $\mathfrak{p} = (1 - \zeta_p)$ the prime ideal above p, and $\alpha = 1/p$. Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, this construction involves linear codes over $\mathbb{F}_p$. The case $p = 2$ is the binary Construction A. The generalization from cyclotomic fields to either CM fields or totally real number fields was suggested in [30] for the case where $\mathfrak{p}$ is totally ramified. The motivation to revisit Construction A using number fields came from coding theory for wireless communication, for which lattices built over totally real numbers fields and CM fields play an important role [43]. In particular, Construction A over number fields enables lattice coset encoding for transmission over wireless channels, and wireless wiretap channels [30]. It is also useful in the context of physical network coding [45].

The main interest in constructing lattices from linear codes is to take advantage of the code properties to obtain lattices with nice properties (see Section 2.2).

Here we recall some lattice definitions from Chapter 2. Certain definitions have equivalent formulations in coding theory, which are listed below. Given an arbitrary lattice (L, b) where L is a $\mathbb{Z}-$module and b is a symmetric bilinear form which is positive definite, then the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\boldsymbol{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} : b(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}\ \forall \boldsymbol{y} \in L\},$$

and (L, b) is

- integral if $L \subseteq L^*$,
- unimodular if $(L, b) \cong (L^*, b)$, i.e., there exists a $\mathbb{Z}-$module isomorphism $\tau : L \to L^*$ such that $b(\tau(x), \tau(y)) = b(x, y)$ for all $x, y \in L$, and
- *$d-$modular* (or *modular of level d*) if it is integral and $(L, b) \cong (L^*, db)$ for some positive integer d.

Given a linear code $C \subset \mathbb{F}_q^N$ of dimension k, q a prime power, its dual code $C^\perp$ is defined by

$$C^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^N : \boldsymbol{x} \cdot \boldsymbol{y} = \sum_{i=1}^{N} x_i y_i = 0 \ \forall \boldsymbol{y} \in C\} \tag{5.3}$$

and C is called

- *self-orthogonal* if $C \subseteq C^\perp$, and
- *self-dual* if $C = C^\perp$.

It is well known for the binary Construction A that $C \subseteq \mathbb{F}_2^N$ is self-dual if and only if $(\rho^{-1}(C), b_{\frac{1}{2}})$ is unimodular [22, 19]. More generally, for $K = \mathbb{Q}(\zeta_p)$, if $C \subseteq \mathbb{F}_p^N$ is self-dual, then $(\rho^{-1}(C), b_{\frac{1}{p}})$ is unimodular [22]. We will prove a converse of this statement for totally real number fields and CM fields with a totally ramified prime in Section 5.1.

Self-dual codes thus provide a systematic way to obtain modular lattices. This was used for example in [17], where $K = \mathbb{Q}(\sqrt{-2})$, $\mathfrak{p} = (3)$ and self-dual codes over the ring $\mathcal{O}_K/\mathfrak{p}$ were used to construct $2-$modular lattices. Similarly, in [18], it was shown that by taking $K = \mathbb{Q}(\zeta_3)$, where ζ_3 is the 3rd primitive root of unity, $\mathfrak{p} = (4)$, and self-dual codes over the ring $\mathcal{O}_K/\mathfrak{p}$, $3-$modular lattices can be constructed. In [2], the quadratic fields $\mathbb{Q}(\sqrt{-7})$ with $\mathfrak{p} = (2)$, $\mathbb{Q}(i)$ with $\mathfrak{p} = (2)$ and $\mathbb{Q}(\zeta_3)$ with $\mathfrak{p} = (2)$ or $\mathfrak{p} = (3)$, as well as totally definite quaternion algebras ramified at either 2 or 3 with $\mathfrak{p} = (2)$, were used to construct modular lattices from self-dual codes. An even more generalized version of Construction A is introduced in [54], where $\mathcal{O}_K$ is replaced by any lattice $L \subset \mathbb{R}^n$ and $\mathfrak{p}$ by pL for a prime p. It is then applied to construct unimodular lattices from self-dual linear codes.

Apart from modularity, large minimal norm is another classical property which has been well studied. This is normally achieved via Construction A by exploiting the dualities between the linear codes and the resulting lattices. For example, in [2], the association between MacWilliams identities for linear codes and theta series for lattices are established for the cases listed above to construct extremal lattices, lattices with the largest possible minimal norm (see Definition 2.11). Other duality relations also include the relation between the minimum weight of linear codes and the minimal norm of the corresponding lattices [17], or the connection between the weight enumerator of linear codes and the theta series of lattices [18], shown in both cases for the cases listed above. One classical motivation for finding lattices with the biggest minimum is to find the densest sphere packings, which can be applied to coding over Gaussian channels [54] (see Section 2.2).

In Section 5.1, generator and Gram matrices are computed for the generic case of Construction A over Galois number fields, either totally real or CM. Knowledge of these matri-

ces is important for applications, such as lattice encoding, or if one needs to compute the theta series of the lattice, as we will do in Section 5.3. It also gives one way to verify modularity, as will be shown both in Sections 5.2 and 5.4. From the generic construction, examples of lattices are obtained by considering specific number fields. We investigate the two most natural ones, namely totally real quadratic fields in Section 5.2, and totally imaginary quadratic fields in Section 5.4. Our techniques could be applied to other number fields, such as cyclotomic fields, or cyclic fields, but these directions are left open. Section 5.3 provides examples of lattices and of their applications: we construct modular lattices and compute their theta series (and their kissing number in particular), but also their minimal norm. The theta series allows to compute the secrecy gain of the lattice [44], a lattice invariant studied in the context of wiretap coding. Interesting examples are found – new constructions of known extremal lattices, modular lattices with large minimal norm – and numerical evidence gives new insight on the behavior of the secrecy gain.

5.1 Generator and Gram Matrices for Construction A

As above, we consider the nN-dimensional lattice $(\rho^{-1}(C), b_\alpha)$. Let Δ be the absolute value of the discriminant of K. We will adopt the row convention, meaning that a lattice generator matrix contains a basis as row vectors. The Gram matrix contains as usual the inner product between the basis vectors. The volume of a lattice is the absolute value of the determinant of a generator matrix, while the discriminant of a lattice is the determinant of its Gram matrix.

Lemma 5.1. The lattice $(\rho^{-1}(C), b_\alpha)$ has discriminant $\Delta^N p^{2f(N-k)} N(\alpha)^N$ and volume $\Delta^{N/2} p^{f(N-k)} N(\alpha)^{\frac{N}{2}}$.

Proof. For $N = 1$, $(\mathcal{O}_K, b_\alpha)$ is a lattice with discriminant $N(\alpha)\Delta$ [5]. Hence $(\mathcal{O}_K^N, b_\alpha)$ has discriminant $(N(\alpha)\Delta)^N$ and volume $(N(\alpha)\Delta)^{\frac{N}{2}}$. As ρ is a surjective $\mathbb{Z}-$module homomorphism and C has index $p^{f(N-k)}$ as a subgroup of $\mathbb{F}_{p^f}^N$, $\rho^{-1}(C)$ also has index $p^{f(N-k)}$ as a subgroup of $\mathcal{O}_K^N$ and we have [22]

$$vol((\rho^{-1}(C), b_\alpha)) = vol((\mathcal{O}_K^N, b_\alpha))|\mathcal{O}_K^N/\rho^{-1}(C)| = N(\alpha)^{N/2}\Delta^{\frac{N}{2}} p^{f(N-k)}.$$

□

Corollary 5.2. The dual lattice $(\rho^{-1}(C)^*, b_\alpha)$ has discriminant $\Delta^{-N} p^{-2f(N-k)} N(\alpha)^{-N}$ and

volume $\Delta^{-N/2}p^{-f(N-k)}N(\alpha)^{\frac{-N}{2}}$. Also the lattice $(\rho^{-1}(C^{\perp}), b_\alpha)$ has discriminant $\Delta^N p^{2fk}$ $N(\alpha)^N$ and volume $\Delta^{\frac{N}{2}}p^{fk}N(\alpha)^{\frac{N}{2}}$.

Let $\{v_1, \ldots, v_n\}$ be a $\mathbb{Z}-$basis for $\mathcal{O}_K$ and let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}-$basis for $\mathfrak{p}$. Recall that a generator matrix for a linear code C is a matrix whose rows form a basis for C. A generator matrix is said to be in standard (systematic) form if it is of the form $[I_k|X]$ [34, p.52]. Suppose C admits a generator matrix in the standard (systematic) form and let A be a matrix such that $[I_k \ (A \bmod \mathfrak{p})]$ is a generator matrix of C.

Proposition 5.3. For K a totally real number field of degree n with Galois group $\{\sigma_1$(the identity), $\ldots, \sigma_n\}$, a generator matrix for $(\rho^{-1}(C), b_\alpha)$ is given by

$$M_C = \begin{bmatrix} I_k \otimes M & A\widetilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & I_{N-k} \otimes M_p \end{bmatrix} (I_N \otimes D_\alpha), \tag{5.4}$$

where $M = (\sigma_j(v_i))_{i,j=1,\ldots,n}$, $M_p = (\sigma_j(w_i))_{i,j=1,\ldots,n}$ are respectively generator matrices for $(\mathcal{O}_K^N, b_1)$ and $(\mathfrak{p}^N, b_1)$, D_α is a diagonal matrix whose diagonal entries are $\sqrt{\sigma_i(\alpha)}$, $i = 1, \ldots, n$, and

$$A\widetilde{\otimes}M := [\sigma_1(A_1) \otimes M_1, \ldots, \sigma_n(A_1) \otimes M_n, \ldots, \sigma_n(A_{N-k}) \otimes M_1, \ldots, \sigma_n(A_{N-k}) \otimes M_n],$$

where we denote the columns of the matrices M, A by $M_i, i = 1, \ldots, n$, $A_j, j = 1, 2, \ldots, N-k$ and σ_i is understood componentwise, $i = 1, \ldots, n$.

Proof. Note that $\det(M) = \Delta^{\frac{1}{2}}$ is the volume of $(\mathcal{O}_K, b_1)$ [6] and similarly, $\det(M_p) = \Delta^{\frac{1}{2}}p^f$ is the volume of $(\mathfrak{p}, b_1)$.

The volume of the lattice generated by M_C is

$$\det(I_N \otimes D_\alpha)\det(I_k \otimes M)\det(I_{N-k} \otimes M_p) = N(\alpha)^{N/2}\Delta^{\frac{k}{2}}\left(\Delta^{\frac{1}{2}}p^f\right)^{N-k},$$

which agrees with the volume $N(\alpha)^{N/2}\Delta^{\frac{N}{2}}p^{f(N-k)}$ of $(\rho^{-1}(C), b_\alpha)$.

Define $\psi : \sigma(x) \mapsto x \in \mathcal{O}_K$ to be the inverse of the embedding

$$\sigma = (\sqrt{\sigma_1(\alpha)}\sigma_1, \ldots, \sqrt{\sigma_n(\alpha)}\sigma_n) : \mathcal{O}_K \hookrightarrow \mathbb{R}^n.$$

Then it suffices to prove that

$$\rho^{-1}(C) \supseteq \{\psi(\boldsymbol{x}M_C) : \boldsymbol{x} \in \mathbb{Z}^{nN}\},$$

or

$$C \supseteq \{\rho(\psi(\boldsymbol{x}M_C)) : \boldsymbol{x} \in \mathbb{Z}^{nN}\}.$$

For $j = 1, 2, \ldots, N$, let $\boldsymbol{u}_j = (u_{j1}, \ldots, u_{jn}) \in \mathbb{Z}^n$. Then $\boldsymbol{x} \in \mathbb{Z}^{nN}$ can be written as $\boldsymbol{x} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N)$. Let $x_j = \sum_{i=1}^n u_{ji} v_i$, then the sth entry of $\boldsymbol{u}_j M D_\alpha$ is given by

$$\sum_{i=1}^n u_{ji}\sigma_s(v_i)\sqrt{\sigma_s(\alpha)} = \sqrt{\sigma_s(\alpha)}\sigma_s\left(\sum_{i=1}^n u_{ji}v_i\right) = \sqrt{\sigma_s(\alpha)}\sigma_s(x_j).$$

Thus

$$\begin{aligned}
\boldsymbol{x}M_C &= [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N]\begin{bmatrix} I_k \otimes M & A\widetilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & I_{N-k}M_p \end{bmatrix}(I_N \otimes D_\alpha) \\
&= \left[\sigma(x_1), \ldots, \sigma(x_k), \sigma\left(\sum_{j=1}^k a_{j1}x_j + x'_{k+1}\right), \ldots, \sigma\left(\sum_{j=1}^k a_{j(N-k)}x_j + x'_N\right)\right],
\end{aligned}$$

where $x'_{k+1}, \ldots, x'_N$ are in the ideal $\mathfrak{p}$, then $\rho(x'_i) = 0$ for $i = k+1, \ldots, x_N$. We have

$$\begin{aligned}
& \rho(\psi(\boldsymbol{x}M_C)) \\
= \;& \rho(x_1, \ldots, x_k, \sum_{j=1}^k a_{j1}x_j + x'_{k+1}, \ldots, \sum_{j=1}^k a_{j(N-k)}x_j + x'_N) \\
= \;& (x_1 \bmod \mathfrak{p}, \ldots, x_k \bmod \mathfrak{p}, \sum_{j=1}^k a_{j1}x_j + x'_{k+1} \bmod \mathfrak{p}, \ldots, \sum_{j=1}^k a_{j(N-k)}x_j + x'_N \bmod \mathfrak{p}) \\
= \;& (x_1 \bmod \mathfrak{p}, \ldots, x_k \bmod \mathfrak{p})[I_k \; A \bmod \mathfrak{p}] \in C.
\end{aligned}$$

□

Lemma 5.4. The Gram matrix $G_C = M_C M_C^\top$ of $(\rho^{-1}(C), b_\alpha)$ is

$$G_C = \begin{bmatrix} \mathrm{Tr}\left(\alpha(I_k + AA^\top) \otimes M_1 M_1^\top\right) & \mathrm{Tr}\left(\alpha A \otimes M_1 M_{p,1}^\top\right) \\ \mathrm{Tr}\left(\alpha A \otimes M_1 M_{p,1}^\top\right)^\top & \mathrm{Tr}\left(\alpha I_{N-k} \otimes M_{p,1} M_{p,1}^\top\right) \end{bmatrix} \tag{5.5}$$

where $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$ is taken componentwise and $M_{p,1}$ denotes the first column of the matrix M_p.

Proof. Let $\tilde{D_\alpha} = D_\alpha D_\alpha^\top$ be the diagonal matrix with diagonal entries given by $\sigma_1(\alpha), \ldots,$

$\sigma_n(\alpha)$. For M_C in (5.4), a direct computation gives

$$G_C = \begin{bmatrix} I_k \otimes M\tilde{D}_\alpha M^\top + (A\widetilde{\otimes}M)(I_{N-k}\otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top & (A\widetilde{\otimes}M)(I_{N-k}\otimes \tilde{D}_\alpha M_p^\top) \\ (I_{N-k}\otimes M_p\tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top & I_{N-k}\otimes M_p\tilde{D}_\alpha M_p^\top \end{bmatrix}.$$

Using that $M_i = \sigma_i(M_1)$, $(1 \le i \le n)$, we have

$$\begin{aligned} (A\widetilde{\otimes}M)(I_{N-k}\otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top &= \mathrm{Tr}\left(\alpha AA^\top \otimes M_1M_1^\top\right) \\ I_k \otimes M\tilde{D}_\alpha M^\top &= \mathrm{Tr}\left(\alpha I_k \otimes M_1M_1^\top\right) \end{aligned}$$

thus showing that

$$I_k \otimes M\tilde{D}_\alpha M^\top + (A\widetilde{\otimes}M)(I_{N-k}\otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top = \mathrm{Tr}\left(\alpha(I_k + AA^\top)\otimes M_1M_1^\top\right).$$

Similarly, let $M_{p,i}$ denote the ith column of M_p, then using $\sigma_i(M_{p,1}) = M_{p,i}$ $(1 \le i \le n)$, we have

$$I_{N-k}\otimes M_p\tilde{D}_\alpha M_p^\top = \mathrm{Tr}\left(\alpha I_{N-k}\otimes M_{p,1}M_{p,1}^\top\right).$$

Moreover,

$$\begin{aligned} &(A\widetilde{\otimes}M)(I_{N-k}\otimes \tilde{D}_\alpha M_p^\top) = \\ &\begin{bmatrix} \sigma_1(a_{11})M_1 & \sigma_2(a_{11})M_2 & \dots & \sigma_n(a_{1,N-k})M_n \\ \vdots & \vdots & & \vdots \\ \sigma_1(a_{k,1})M_1 & \sigma_2(a_{k,2})M_2 & \dots & \sigma_n(a_{k,N-k})M_n \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha)M_{p,1}^\top & 0 & \dots & 0 \\ \sigma_2(\alpha)M_{p,2}^\top & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha)M_{p,n}^\top & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_{n-1}(\alpha)M_{p,n-1}^\top \\ 0 & 0 & \dots & \sigma_n(\alpha)M_{p,n}^\top \end{bmatrix} \\ &= \sigma_1(A\otimes \alpha M_1M_{p,1}^\top) + \sigma_2(A\otimes \alpha M_1M_{p,1}^\top) + \cdots + \sigma_n(A\otimes \alpha M_1M_{p,1}^\top) \\ &= \mathrm{Tr}\left(\alpha A \otimes M_1M_{p,1}^\top\right), \end{aligned}$$

□

When K is a CM number field, n is even and all embeddings of K into $\mathbb{C}$ are complex embeddings. Assume σ_{i+1} is the conjugate of σ_i for $i = 1, 3, 5, \dots, n-1$.

Lemma 5.5. Let K be a CM number field of degree n. Then

$$M = \sqrt{2}\begin{bmatrix} \operatorname{Re}(\sigma_1(v_1)) & \operatorname{Im}(\sigma_2(v_1)) & \operatorname{Re}(\sigma_3(v_1)) & \dots & \operatorname{Re}(\sigma_{n-1}(v_1)) & \operatorname{Im}(\sigma_n(v_1)) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \operatorname{Re}(\sigma_1(v_n)) & \operatorname{Im}(\sigma_2(v_n)) & \operatorname{Re}(\sigma_3(v_n)) & \dots & \operatorname{Re}(\sigma_{n-1}(v_n)) & \operatorname{Im}(\sigma_n(v_n)) \end{bmatrix} \tag{5.6}$$

is a generator matrix for the lattice $(\mathcal{O}_K, b_1)$ and $\det(M) = \Delta^{\frac{1}{2}}$.

Proof. The Gram matrix for $(\mathcal{O}_K, b_1)$ is $G = (\operatorname{Tr}(v_i\bar{v}_j))_{1\le i,j\le n}$. For $i = 1, 2, \dots, n$,

$$\begin{aligned}(MM^\top)_{ii} &= 2\sum_{j=1,3,\dots,n-1} (\operatorname{Re}(\sigma_j(v_i)))^2 + (\operatorname{Im}(\sigma_{j+1}(v_i)))^2 = 2\sum_{j=1,3,\dots,n-1} |\sigma_j(v_i)|^2 \\ &= 2\sum_{j=1,3,\dots,n-1} \sigma_j(|v_i|^2) = \operatorname{Tr}\left(|v_i|^2\right) = G_{ii}.\end{aligned}$$

For $i, j = 1, 2, \dots, n, i \neq j$,

$$\begin{aligned}(MM^\top)_{ij} &= 2\sum_{s=1,3,\dots,n-1} \operatorname{Re}(\sigma_s(v_i))\operatorname{Re}(\sigma_s(v_j)) + \operatorname{Im}(\sigma_{s+1}(v_i))\operatorname{Im}(\sigma_{s+1}(v_j)) \\ &= 2\sum_{s=1,3,\dots,n-1} \operatorname{Re}(\sigma_s(v_i))\operatorname{Re}(\sigma_s(v_j)) + \operatorname{Im}(\sigma_s(v_i))\operatorname{Im}(\sigma_s(v_j)) \\ &= 2\sum_{s=1,3,\dots,n-1} \operatorname{Re}(\sigma_s(v_i\bar{v}_j)) = \operatorname{Tr}(v_i\bar{v}_j) = G_{ij}.\end{aligned}$$

The determinant of M is then given by the volume of $(\mathcal{O}_K, b_1)$. □

Define

$$M_p = \sqrt{2}\begin{bmatrix} \operatorname{Re}(\sigma_1(\omega_1)) & \operatorname{Im}(\sigma_2(\omega_1)) & \operatorname{Re}(\sigma_3(\omega_1)) & \dots & \operatorname{Re}(\sigma_{n-1}(\omega_1)) & \operatorname{Im}(\sigma_n(\omega_1)) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \operatorname{Re}(\sigma_1(\omega_n)) & \operatorname{Im}(\sigma_2(\omega_n)) & \operatorname{Re}(\sigma_3(\omega_n)) & \dots & \operatorname{Re}(\sigma_{n-1}(\omega_n)) & \operatorname{Im}(\sigma_n(\omega_n)) \end{bmatrix}. \tag{5.7}$$

Then similarly M_p is a generator matrix for $(\mathfrak{p}, b_1)$ and has determinant $\Delta^{\frac{1}{2}}p^f$. As α is totally positive, all $\sigma_i(\alpha) \in \mathbb{R}$. Let D_α be a diagonal matrix whose diagonal entries are $\sqrt{\sigma_i(\alpha)}$, $i = 1, \dots, n$.

Proposition 5.6. Let K be a CM field with degree n and Galois group $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$, where σ_{i+1} is the conjugate of σ_i $(i = 1, 3, \dots, n-1)$. A generator matrix for $(\rho^{-1}(C), b_\alpha)$ is given by

$$M_C = \begin{bmatrix} I_k \otimes M & A\tilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & I_{N-k} \otimes M_p \end{bmatrix}(I_N \otimes D_\alpha), \tag{5.8}$$

where M and M_p are defined in (5.6) and (5.7) respectively. A is a matrix such that $[I_k \ (A \bmod \mathfrak{p})]$ is a generator matrix of C and

$$
\begin{aligned}
&A\widetilde{\otimes}M := [\mathrm{Re}\,(\sigma_1(A_1)) \otimes M_1 + \mathrm{Im}\,(\sigma_1(A_1)) \otimes M_2, \mathrm{Re}\,(\sigma_1(A_1)) \otimes M_2 - \mathrm{Im}\,(\sigma_1(A_1)) \otimes M_1,\\
&\mathrm{Re}\,(\sigma_3(A_1)) \otimes M_3 + \mathrm{Im}\,(\sigma_3(A_1)) \otimes M_4, \mathrm{Re}\,(\sigma_3(A_1)) \otimes M_4 - \mathrm{Im}\,(\sigma_3(A_1)) \otimes M_3, \ldots,\\
&\mathrm{Re}\,(\sigma_{n-1}(A_1)) \otimes M_{n-1} + \mathrm{Im}\,(\sigma_{n-1}(A_1)) \otimes M_n, \mathrm{Re}\,(\sigma_{n-1}(A_1)) \otimes M_n - \mathrm{Im}\,(\sigma_{n-1}(A_1)) \otimes M_{n-1},\\
&\ldots, \mathrm{Re}\,(\sigma_{n-1}(A_{N-k})) \otimes M_{n-1} + \mathrm{Im}\,(\sigma_n(A_{N-k})) \otimes M_n,\\
&\mathrm{Re}\,(\sigma_{n-1}(A_{N-k})) \otimes M_n - \mathrm{Im}\,(\sigma_{n-1}(A_{N-k})) \otimes M_{n-1}],
\end{aligned}
$$

where we denote the columns of the matrices M, A by $M_i, i = 1, \ldots, n$, $A_j, j = 1, 2, \ldots, N-k$, Re and Im are understood componentwise.

Proof. The volume of the lattice generated by M_C is

$$
\begin{aligned}
\det\,(I_k \otimes M) \det\,(I_{N-k} \otimes M_p) \det\,(I_N \otimes D_\alpha) &= \Delta^{\frac{k}{2}} \left(\Delta^{\frac{1}{2}} p^f\right)^{N-k} N(\alpha)^{N/2}\\
&= \Delta^{\frac{N}{2}} p^{f(N-k)} N(\alpha)^{N/2},
\end{aligned}
$$

which agrees with the volume of $(\rho^{-1}(C), b_\alpha)$.

Define $\psi : \sigma(x) \mapsto x \in \mathcal{O}_K$ to be the inverse of the embedding

$$
\sigma = \sqrt{2}(\sqrt{\sigma_1(\alpha)}\mathrm{Re}\,(\sigma_1)\,, \sqrt{\sigma_2(\alpha)}\mathrm{Im}\,(\sigma_2)\,, \ldots, \sqrt{\sigma_{n-1}(\alpha)}\mathrm{Re}\,(\sigma_{n-1})\,, \sqrt{\sigma_n(\alpha)}\mathrm{Im}\,(\sigma_n)) : \mathcal{O}_K \hookrightarrow \mathbb{R}^n.
$$

Then it suffices to prove

$$
\rho^{-1}(C) \supseteq \{\psi(\boldsymbol{x}M_C) : \boldsymbol{x} \in \mathbb{Z}^{nN}\},
$$

or

$$
\{\rho(\psi(\boldsymbol{x}M_C)) : \boldsymbol{x} \in \mathbb{Z}^{nN}\} \subseteq C.
$$

For $j = 1, 2, \ldots, N$, let $\boldsymbol{u}_j = (u_{j1}, \ldots, u_{jn}) \in \mathbb{Z}^n$. Then $\boldsymbol{x} \in \mathbb{Z}^{nN}$ can be written as $\boldsymbol{x} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N)$. Let $x_j = \sum_{i=1}^n u_{ji} v_i$, we have the tth entry of $\boldsymbol{u}_j M D_\alpha$ is

$$
\sqrt{2}\sum_{i=1}^{n} u_{ji}\mathrm{Re}\,(\sigma_t(v_i))\,\sqrt{\sigma_t(\alpha)} = \sqrt{2}\sqrt{\sigma_t(\alpha)}\sum_{i=1}^{n}\mathrm{Re}\,(\sigma_t(u_{ji}v_i)) = \sqrt{2}\sqrt{\sigma_t(\alpha)}\mathrm{Re}\,(\sigma_t(x_j))
$$

for t odd, or $\sqrt{2}\sqrt{\sigma_t(\alpha)}\mathrm{Im}\,(\sigma_t(x_j))$ for t even. And the stth entry $(1 \le s \le N-k, 1 \le t \le n)$

of $\boldsymbol{u}_j(A\widetilde{\otimes}M)(I_{N-k}\otimes D_\alpha)$ $(1\le j\le k)$ is

$$\begin{aligned}
&\sqrt{2}\sum_{i=1}^{n} u_{ji}\left[\mathrm{Re}\left(\sigma_t(a_{js})\right)\mathrm{Re}\left(\sigma_t(v_i)\right)+\mathrm{Im}\left(\sigma_t(a_{js})\right)\mathrm{Im}\left(\sigma_{t+1}(v_i)\right)\right]\sqrt{\sigma_t(\alpha)}\\
=\;&\sqrt{2}\sqrt{\sigma_t(\alpha)}\sum_{i=1}^{n}\mathrm{Re}\left(\sigma_t(a_{js})\right)\mathrm{Re}\left(\sigma_t(u_{ji}v_i)\right)+\mathrm{Im}\left(\sigma_t(a_{js})\right)\mathrm{Im}\left(\sigma_{t+1}(u_{ji}v_i)\right)\\
=\;&\sqrt{2}\sqrt{\sigma_t(\alpha)}\sum_{i=1}^{n}\mathrm{Re}\left(\sigma_t(a_{js}u_{ji}v_i)\right)=\sqrt{2}\sqrt{\sigma_t(\alpha)}\mathrm{Re}\left(\sigma_t(a_{js})x_j\right)
\end{aligned}$$

for t odd, or $\sqrt{2}\sqrt{\sigma_t(\alpha)}\mathrm{Im}\left(\sigma_t(a_{js})x_j\right)$ for t even.

Then

$$\begin{aligned}
\boldsymbol{x}M_C &= [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_N]\begin{bmatrix} I_k\otimes M & A\widetilde{\otimes}M\\ \mathbf{0}_{nN-nk,nk} & I_{N-k}\otimes M_p\end{bmatrix}(I_N\otimes D_\alpha)\\
&= \left[\sigma(x_1),\ldots,\sigma(x_k),\sigma\left(\sum_{j=1}^{k}a_{j1}x_j+x'_{k+1}\right),\ldots,\sigma\left(\sum_{j=1}^{k}a_{j(N-k)}x_j+x'_N\right)\right],
\end{aligned}$$

where $x'_{k+1},\ldots,x'_N$ are in the ideal $\mathfrak{p}$, and hence $\rho(x'_i)=0$ for $i=k+1,\ldots,N$. Then we have

$$\begin{aligned}
&\rho(\psi(\boldsymbol{x}M_C))\\
=\;&\rho(x_1,\ldots,x_k,\sum_{j=1}^{k}a_{j1}x_j+x'_{k+1},\ldots,\sum_{j=1}^{k}a_{j(N-k)}x_j+x'_N)\\
=\;&(x_1 \bmod \mathfrak{p},\ldots,x_k \bmod \mathfrak{p},\sum_{j=1}^{k}a_{j1}x_j+x'_{k+1} \bmod \mathfrak{p},\ldots,\sum_{j=1}^{k}a_{j(N-k)}x_j+x'_N \bmod \mathfrak{p})\\
=\;&(x_1 \bmod \mathfrak{p},\ldots,x_k \bmod \mathfrak{p})[I_k\ A \bmod \mathfrak{p}]\in C.
\end{aligned}$$

□

Remark 5.7.

1. Let $\boldsymbol{v}=[v_1,v_2,\ldots,v_n]^\top$, then

$$\begin{aligned}
A\widetilde{\otimes}M &= \sqrt{2}[\mathrm{Re}\left(\sigma_1(A_1\otimes\boldsymbol{v})\right),\mathrm{Im}\left(\sigma_2(A_1\otimes\boldsymbol{v})\right),\\
&\qquad \ldots,\mathrm{Re}\left(\sigma_{n-1}(A_1\otimes\boldsymbol{v})\right),\mathrm{Im}\left(\sigma_n(A_1\otimes\boldsymbol{v})\right),\ldots,\mathrm{Im}\left(\sigma_n(A_{N-k}\otimes\boldsymbol{v})\right)].
\end{aligned}$$

2. When p is totally ramified, the entries of $A \bmod \mathfrak{p}$ are in $\mathbb{F}_p$ and hence $A\widetilde{\otimes}M=A\otimes M$.

Proposition 5.8. The Gram matrix $G_C = M_C M_C^\top$ of $(\rho^{-1}(C), b_\alpha)$ is

$$G_C = \begin{bmatrix} \mathrm{Tr}\left(\alpha(I + AA^\dagger) \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right) & \mathrm{Tr}\left(\alpha A \otimes (\boldsymbol{v}\boldsymbol{\omega}^\dagger)\right) \\ \mathrm{Tr}\left(\alpha A^\top \otimes (\bar{\boldsymbol{\omega}}\boldsymbol{v}^\top)\right) & \mathrm{Tr}\left(\alpha I_{N-k} \otimes \boldsymbol{\omega}\boldsymbol{\omega}^\dagger\right) \end{bmatrix} \tag{5.9}$$

where $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$ is taken componentwise and $\boldsymbol{\omega} = [w_1, w_2, \ldots, w_n]^\top$. $\boldsymbol{v}^\dagger = \bar{v}^\top$, is the conjugate transpose of $\boldsymbol{v}$. Similarly $A^\dagger = \bar{A}^\top$, $\boldsymbol{\omega}^\dagger = \bar{\boldsymbol{\omega}}^\top$.

Proof. Let $\tilde{D}_\alpha = D_\alpha D_\alpha^\top$ be the diagonal matrix with diagonal entries given by $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. For M_C in (5.8), a direct computation gives

$$G_C = \begin{bmatrix} I_k \otimes M\tilde{D}_\alpha M^\top + (A\widetilde{\otimes}M)(I_{N-k} \otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top & (A\widetilde{\otimes}M)(I_{N-k} \otimes \tilde{D}_\alpha M_p^\top) \\ (I_{N-k} \otimes M_p\tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top & I_{N-k} \otimes M_p\tilde{D}_\alpha M_p^\top \end{bmatrix}.$$

By Remark 5.7,

$$\begin{aligned} & (A\widetilde{\otimes}M)(I_{N-k} \otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top \\ = \; & \mathrm{Tr}\left((\alpha A_1 \otimes \boldsymbol{v})(A_1^\dagger \otimes \boldsymbol{v}^\dagger)\right) + \cdots + \mathrm{Tr}\left((\alpha A_{N-k} \otimes \boldsymbol{v})(A_{N-k}^\dagger \otimes \boldsymbol{v}^\dagger)\right) \\ = \; & \mathrm{Tr}\left(\alpha A_1 A_1^\dagger \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right) + \cdots + \mathrm{Tr}\left(\alpha A_{N-k} A_{N-k}^\dagger \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right) \\ = \; & \mathrm{Tr}\left(\alpha(A_1 A_1^\dagger + \cdots + A_{N-k} A_{N-k}^\dagger) \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right) \\ = \; & \mathrm{Tr}\left(\alpha AA^\dagger \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right). \end{aligned}$$

Furthermore,

$$I_k \otimes M\tilde{D}_\alpha M^\top = \mathrm{Tr}\left(\alpha I_k \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right), \text{ and } I_{N-k} \otimes M_p\tilde{D}_\alpha M_p^\top = \mathrm{Tr}\left(\alpha I_{N-k} \otimes \boldsymbol{\omega}\boldsymbol{\omega}^\dagger\right).$$

Hence

$$I_k \otimes M\tilde{D}_\alpha M^\top + (A\widetilde{\otimes}M)(I_{N-k} \otimes \tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top = \mathrm{Tr}\left(\alpha(I_k + AA^\dagger) \otimes \boldsymbol{v}\boldsymbol{v}^\dagger\right).$$

Next, it can be computed that

$$(I_{N-k} \otimes M_p\tilde{D}_\alpha)(A\widetilde{\otimes}M)^\top = \mathrm{Tr}\left(\alpha A^\top \otimes (\bar{\boldsymbol{\omega}}\boldsymbol{v}^\top)\right)$$

which also gives

$$(A\widetilde{\otimes}M)(I_{N-k} \otimes \tilde{D}_\alpha M_p^\top) = \mathrm{Tr}\left(\alpha A \otimes (\boldsymbol{v}\boldsymbol{\omega}^\dagger)\right).$$

So the Gram Matrix is given by (5.9). □

In Sections 5.2 and 5.4 we will consider particular cases when $\alpha = 1/p$ or $1/(2p)$ for K a real quadratic field with $\mathfrak{p}$ inert and K an imaginary quadratic field with $\mathfrak{p}$ totally ramified. As we are interested in constructions of modular lattices, which are integral lattices, the following proposition justifies why we will focus on self-orthogonal codes in what follows.

Proposition 5.9. If C is not self-orthogonal, i.e., if $C \nsubseteq C^{\perp}$, then $(\rho^{-1}(C), b_\alpha)$ is not an integral lattice for any $\alpha \in \mathfrak{p}^{-1} \cap \mathbb{Q}$ when

1. K is totally real, or

2. K is a CM field and $\mathfrak{p}$ is totally ramified.

Proof. Let $\{\tilde{c_1}, \tilde{c_2}, \ldots, \tilde{c_k}\}$ be an $\mathbb{F}_{p^f}$ −basis for the linear code C. Let $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\}$ be a set of elements in $\mathcal{O}_K^N$ such that $\boldsymbol{c}_i$ is a preimage of $\tilde{c}_i$, $1 \leq i \leq k$. Notice that for $1 \leq i \leq k,\ 1 \leq j \leq n$,

$$\rho(v_j \boldsymbol{c}_i) = \rho(v_j)\rho(\boldsymbol{c}_i) = \rho(v_j)\tilde{c}_i.$$

As $\rho(v_j) \in \mathbb{F}_{p^f}$, $\rho(v_j \boldsymbol{c}_i) \in C$, i.e., $v_j \boldsymbol{c}_i \in \rho^{-1}(C)$ for all $1 \leq i \leq k$ and $1 \leq j \leq n$. Since $C \nsubseteq C^{\perp}$, take $\boldsymbol{c}_{i_1}, \boldsymbol{c}_{i_2}$ such that $\tilde{c}_{i_1} \cdot \tilde{c}_{i_2} \neq 0$, i.e., $\boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \notin \mathfrak{p}$. From $\{v_1, \ldots, v_n\}$, take v_{j_0} such that $v_{j_0} \notin \mathfrak{p}$. Suppose

$$b_\alpha(v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2}) = \alpha \mathrm{Tr}\left(v_{j_0} \boldsymbol{c}_{i_1} \cdot \bar{\boldsymbol{c}}_{i_2} \bar{v}_j\right) \in \mathbb{Z}$$

for all $1 \leq j \leq n$. As $\{v_j\}_{1 \leq j \leq n}$ forms a basis for $\mathcal{O}_K$, $\{\bar{v}_j\}_{1 \leq j \leq n}$ also forms a basis for $\mathcal{O}_K$, we have

$$\alpha \mathrm{Tr}\left(v_{j_0} \boldsymbol{c}_{i_1} \cdot \bar{\boldsymbol{c}}_{i_2} x\right) \in \mathbb{Z}\ \forall x \in \mathcal{O}_K.$$

By the definition of the codifferent $\mathcal{D}_K^{-1}$,

$$\alpha v_{j_0} \boldsymbol{c}_{i_1} \cdot \bar{\boldsymbol{c}}_{i_2} \in \mathcal{D}_K^{-1} \Longrightarrow v_{j_0} \boldsymbol{c}_{i_1} \cdot \bar{\boldsymbol{c}}_{i_2} \in \alpha^{-1}\mathcal{D}_K^{-1} \cap \mathcal{O}_K = \alpha^{-1}\mathcal{O}_K \subseteq \mathfrak{p}.$$

As $v_{j_0} \notin \mathfrak{p}$, we have $\boldsymbol{c}_{i_1} \cdot \bar{\boldsymbol{c}}_{i_2} \in \mathfrak{p}$. For K totally real, this is the same as $\boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \in \mathfrak{p}$. For K CM, as $\mathfrak{p}$ is totally ramified, by the proof from [30], $\beta \equiv \bar{\beta} \bmod \mathfrak{p}$ for all $\beta \in \mathcal{O}_K$. It goes as follows:

As $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, we can write $\beta = \beta' + \beta''$ with $\beta' \in \mathbb{Z}$ and $\beta'' \in \mathfrak{p}$. Since $\mathfrak{p}$ is the only

prime above p, $\bar{\mathfrak{p}} = \mathfrak{p}$ and we have $\bar{\beta''} \in \mathfrak{p}$. Thus

$$\bar{\beta} = \bar{\beta'} + \bar{\beta''} = \beta' + \bar{\beta''} \equiv \beta' \bmod \mathfrak{p} \equiv \beta \bmod \mathfrak{p}.$$

Then we can conclude $\boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \in \mathfrak{p}$. For both cases, we get a contradiction with the choice of $\boldsymbol{c}_{i_1}$ and $\boldsymbol{c}_{i_2}$.

Thus we must have $b_\alpha(v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2}) \notin \mathbb{Z}$ for at least one j $(1 \leq j \leq n)$. As $v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2} \in \rho^{-1}(C)$ for all j, we can conclude that the lattice $(\rho^{-1}(C), b_\alpha)$ is not integral. □

5.2 Modular Lattices from Totally Real Quadratic Fields

Let d be a positive square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$ be a totally real quadratic field with Galois group $\{\sigma_1, \sigma_2\}$ and discriminant Δ given by [42]:

$$\Delta = \begin{cases} d & d \equiv 1 \bmod 4 \\ 4d & d \equiv 2, 3 \bmod 4 \end{cases}.$$

Assume $p \in \mathbb{Z}$ is a prime which is inert in K, and consider the lattice $(\rho^{-1}(C), b_\alpha)$ where C is a linear (N, k) code over $\mathbb{F}_{p^2}$.

Let $\alpha = 1/p$ when $d \equiv 1 \bmod 4$ and let $\alpha = 1/(2p)$ when $d \equiv 2, 3 \bmod 4$. We will give two proofs that if C is self-dual (i.e., $C = C^\perp$), then the lattice $(\rho^{-1}(C), b_\alpha)$ is a d-modular lattice.

By the discussion from Section 5.1, a generator matrix for $(\rho^{-1}(C), b_\alpha)$ is (see (5.4))

$$M_C = \sqrt{\alpha} \begin{bmatrix} I_k \otimes M & A \widetilde{\otimes} M \\ \mathbf{0}_{2N-2k,2k} & I_{N-k} \otimes pM \end{bmatrix} \tag{5.10}$$

where $[I_k, (A \mod p\mathcal{O}_K)]$ is a generator matrix for C,

$$M = \begin{bmatrix} 1 & 1 \\ \sigma_1(v) & \sigma_2(v) \end{bmatrix}, \tag{5.11}$$

with $\{1, v\}$ a $\mathbb{Z}-$basis of $\mathcal{O}_K$, and

$$v = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \bmod 4 \\ \sqrt{d} & d \equiv 2, 3 \bmod 4 \end{cases}.$$

Also, the Gram matrix for $(\rho^{-1}(C), b_\alpha)$ is given by (see (5.5))

$$G_C = \alpha \begin{bmatrix} \mathrm{Tr}\left((I + AA^\top) \otimes M_1 M_1^\top\right) & p\mathrm{Tr}\left(A \otimes M_1 M_1^\top\right) \\ p\mathrm{Tr}\left(A \otimes M_1 M_1^\top\right)^\top & I_k \otimes p^2 M M^\top \end{bmatrix}. \tag{5.12}$$

Note that since p is inert, $M_p = pM$.

Lemma 5.10. If C is self-orthogonal, then the lattice $(\rho^{-1}(C), b_\alpha)$ with $\alpha = 1/p$ when $d \equiv 1 \bmod 4$ and $\alpha = 1/(2p)$ when $d \equiv 2, 3 \bmod 4$ is integral.

Proof. An equivalent definition of integral lattice is that its Gram matrix has integral coefficients, which is the case: $MM^\top$ has integral coefficients, both A and $I + AA^\top$ have coefficients in $\mathcal{O}_K$, thus $\mathrm{Tr}\left((I + AA^\top) \otimes M_1 M_1^\top\right)$ and $\mathrm{Tr}\left(A \otimes M_1 M_1^\top\right)$ have integral coefficients.

As C is self-orthogonal and $[I_k \;\; A \bmod (p)]$ is a generator matrix for C, $I_k + AA^\top \equiv 0 \bmod (p)$ (Lemma 5.11). Hence $(I_k + AA^\top) \otimes M_1 M_1^\top \in (p)$ and $\mathrm{Tr}\left((I_k + AA^\top) \otimes M_1 M_1^\top\right) \in p\mathbb{Z}$.

Finally, for the case $d \equiv 2, 3 \bmod 4$, any entry in $\alpha^{-1} G_C$ is an element of $\mathcal{O}_K$. Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, for any $x = a + b\sqrt{d} \in \mathcal{O}_K$, $\mathrm{Tr}(x) = 2a \in 2\mathbb{Z}$. □

We can tell the duality properties of a linear code from its generator matrix [34]:

Lemma 5.11. Let C be a linear code over $\mathbb{F}_q$, let B be a generator matrix for C. A matrix $H \in M_{(N-k)\times N}(\mathbb{F}_q)$ is a parity check matrix for C if and only if $HB^\top = \mathbf{0}$. In particular,

1. if $B = [I_k \; A]$, then $(-A^\top \; I_{N-k})$ is a parity check matrix for C;
2. C is self-dual iff $I + AA^\top = \mathbf{0}$.

Hence if C is self-dual and $[I_k \;\; (A \bmod p\mathcal{O}_K)]$ is a generator matrix of C, then $[(-A^\top \bmod p\mathcal{O}_K) \;\; I_k]$ is also a generator matrix of C and $N - k = k$.

We propose next two approaches to discuss the modularity of lattices obtained via the above method.

5.2.1 Approach I

We will use the knowledge of a generator matrix of the lattice.

Remark 5.12. Note that

1. If M is a generator matrix for (L, b), then $M^* := (M^\top)^{-1}$ is a generator matrix for (L^*, b).

2. (L, b) is $d-$modular if and only if $\frac{1}{\sqrt{d}}M$ is a generator matrix for (L^*, b).

   Here b denotes any positive symmetric bilinear form.

We get another generator matrix for $(\rho^{-1}(C), b_\alpha)$:

Proposition 5.13. If C is self-dual, another generator matrix of $(\rho^{-1}(C), b_\alpha)$ is

$$M'_C = \sqrt{\alpha}\begin{bmatrix} -A^\top \widetilde{\otimes} M & I_k \otimes M \\ I_k \otimes pM & \mathbf{0}_{2k,2k} \end{bmatrix} \tag{5.13}$$

with M as in (5.11), A such that $[I_k \ \ (A \bmod p\mathcal{O}_K)]$ is a generator matrix of C.

Proof. Let b_{ij} denote the entries of $-A^\top$. Keep the same notations as in the proof of Proposition 5.3. Define $\psi : \sigma(x) \mapsto x \in \mathcal{O}_K$ to be the inverse of the embedding $\sigma = (\sqrt{\sigma_1(\alpha)}\sigma_1, \sqrt{\sigma_2(\alpha)}\sigma_2) : \mathcal{O}_K \hookrightarrow \mathbb{R}^2$. For $j = 1, 2, \ldots, N$, let $\boldsymbol{u}_j = (u_{j1}, u_{j2}) \in \mathbb{Z}^2$. Then $\boldsymbol{x} \in \mathbb{Z}^{2N}$ can be written as $\boldsymbol{x} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N)$. Let $x_j = u_{j1} + u_{j2}v$ for $1 \le j \le N$. Using the formula for Schur complement, we can check that this matrix has the right determinant. We are left to show that lattice points are indeed mapped to codewords in C by ρ, i.e.

$$\{\rho(\psi(\boldsymbol{x}M_C)) : \boldsymbol{x} \in \mathbb{Z}^{2N}\} \subseteq C,$$

By a similar argument as in Proposition 5.3, we have

$$\begin{aligned} \boldsymbol{x}M_C &= [u_1, \ldots, u_k, \ldots, u_N]\sqrt{\alpha}\begin{bmatrix} -A^\top \widetilde{\otimes} M & I_k \otimes M \\ I_k \otimes pM & \mathbf{0}_{2k,2k} \end{bmatrix} \\ &= [\sigma(\sum_{j=1}^{k} b_{j1}x_j + x'_1), \ldots, \sigma(\sum_{j=1}^{k} b_{jk}x_j + x'_k), \sigma(x_1), \ldots, \sigma(x_k)], \end{aligned}$$

where $x'_1, \ldots, x'_k$ are in the ideal (p). Since x'_i reduces to zero mod (p), we have

$$\psi(\boldsymbol{x}) = \psi(\sigma(\sum_{j=1}^{k} b_{j1}x_j + x'_1)), \ldots, (\psi(\sigma(x_1)), \ldots),$$

and $\rho\psi(\boldsymbol{x})$ is indeed a codeword of C:

$$\begin{aligned} \rho\psi(\boldsymbol{x}) &= (\sum_{j=1}^{k} b_{j1}x_j + x'_1 \bmod (p), \ldots, x_1 \bmod (p), \ldots) \\ &= (x_1 \bmod (p), \ldots, x_k \bmod (p)) \cdot [-A^\top \bmod (p) \ \ I_k] \end{aligned}$$

□

To continue, we need the following lemma, which can be proved by direct computation (see Remark 5.12):

Lemma 5.14. 1. For $d \equiv 1 \bmod 4$, $(\mathcal{O}_K, b_1)$ is $d-$modular, i.e. $\frac{1}{\sqrt{d}} M = U M^*$ for some integral matrix U with determinant ± 1.

2. For $d \equiv 2, 3 \bmod 4$, define

$$M_{\mathfrak{p}_2^{-1}} = \frac{1}{\sqrt{2}} M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{bmatrix}.$$

Then $M_{\mathfrak{p}_2^{-1}}$ is a generator matrix for $(\mathcal{O}_K, \frac{1}{2} b_1)$ and $(\mathcal{O}_K, \frac{1}{2} b_1)$ is $d-$modular, i.e. $\frac{1}{\sqrt{d}} M_{\mathfrak{p}_2^{-1}} = U M^*_{\mathfrak{p}_2^{-1}}$ for some integral matrix U with determinant ± 1.

Proposition 5.15. Let C be a self-dual code. The lattice $(\rho^{-1}(C), b_\alpha)$ is d-modular.

Proof. **Case 1:** $d \equiv 1 \bmod 4$. By Remark 5.12, a generator matrix for the dual of $\rho^{-1}(C)$ with respect to the bilinear form $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \frac{1}{p} \sum_{i=1}^{N} \operatorname{Tr}(x_i y_i)$ is $(M_C^\top)^{-1}$, where M_C is given in (5.10). This can be computed using Schur complement:

$$\begin{aligned} & \sqrt{p} \begin{bmatrix} I_k \otimes M^* & \mathbf{0} \\ -\frac{1}{p}(I_k \otimes M^*)(A \widetilde{\otimes} M)^\top (I_k \otimes M^*) & \frac{1}{p} I_k \otimes M^* \end{bmatrix} \\ = & \frac{1}{\sqrt{p}} \begin{bmatrix} I_k \otimes pM^* & \mathbf{0} \\ -(I_k \otimes M^*)(A \widetilde{\otimes} M)^\top (I_k \otimes M^*) & I_k \otimes M^* \end{bmatrix}, \end{aligned}$$

By a change of basis, we get another generator matrix for the dual as

$$\frac{1}{\sqrt{p}} \begin{bmatrix} -(I_k \otimes M^*)(A \widetilde{\otimes} M)^\top (I_k \otimes M^*) & I_k \otimes M^* \\ I_k \otimes pM^* & \mathbf{0} \end{bmatrix}.$$

By Lemma 5.14, we get the following generator matrix (note that $I \otimes (UM^*) = (I \otimes U)(I \otimes M^*)$)

$$\frac{1}{\sqrt{dp}} \begin{bmatrix} -\sqrt{d}(I_k \otimes M^*)(A \widetilde{\otimes} M)^\top (I_k \otimes M^*) & I_k \otimes M \\ I_k \otimes pM & \mathbf{0} \end{bmatrix}.$$

By Proposition 5.13,

$$\frac{1}{\sqrt{p}} \begin{bmatrix} -A^\top \widetilde{\otimes} M & I_k \otimes M \\ I_k \otimes pM & \mathbf{0} \end{bmatrix}$$

can be seen to be another generator matrix, it suffices now to prove $\sqrt{d}(I_k \otimes M^*)(A \widetilde{\otimes} M)^\top$

$(I_k \otimes M^*) = A^\top \widetilde{\otimes} M$, which is equivalent to

$$\begin{aligned} & (I_k \otimes M)(A\widetilde{\otimes}M)^\top (I_k \otimes M^*) = A^\top \widetilde{\otimes} M \\ \iff \quad & (I_k \otimes M)(A\widetilde{\otimes}M)^\top = (A^\top \widetilde{\otimes} M)(I_k \otimes M^\top) \\ \iff \quad & (A\widetilde{\otimes}M)(I_k \otimes M^\top) = (I_k \otimes M)(A^\top \widetilde{\otimes} M)^\top \\ \iff \quad & \mathrm{Tr}\left(A \otimes M_1 M_1^\top\right) = (I_k \otimes M)(A^\top \widetilde{\otimes} M)^\top \end{aligned}$$

which can be checked by direct computations.

Case 1: $d \equiv 2, 3 \bmod 4$. Similarly, a generator matrix for the dual of $\rho^{-1}(C)$ with respect to the bilinear form $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \frac{1}{2p}\sum_{i=1}^{N} \mathrm{Tr}\,(x_i y_i)$ is $(M_C^\top)^{-1}$. Using Schur complement:

$$\begin{aligned} & \sqrt{p}\begin{bmatrix} I_k \otimes M^*_{\mathfrak{P}_2^{-1}} & \mathbf{0} \\ -\frac{1}{\sqrt{2p}}(I_k \otimes M^*_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) & \frac{1}{p} I_k \otimes M^*_{\mathfrak{P}_2^{-1}} \end{bmatrix} \\ = & \frac{1}{\sqrt{p}}\begin{bmatrix} I_k \otimes pM^*_{\mathfrak{P}_2^{-1}} & \mathbf{0} \\ -\frac{1}{\sqrt{2}}(I_k \otimes M^*_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) & I_k \otimes M^*_{\mathfrak{P}_2^{-1}} \end{bmatrix} \end{aligned}$$

By a change of basis and Lemma 5.14, we get another generator matrix for the dual as

$$\begin{aligned} & \frac{1}{\sqrt{p}}\begin{bmatrix} -\frac{1}{\sqrt{2}}(I_k \otimes M^*_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) & I_k \otimes M^*_{\mathfrak{P}_2^{-1}} \\ I_k \otimes pM^*_{\mathfrak{P}_2^{-1}} & \mathbf{0} \end{bmatrix} \\ = & \frac{1}{\sqrt{dp}}\begin{bmatrix} -\sqrt{\frac{d}{2}}(I_k \otimes M^*_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) & I_k \otimes M_{\mathfrak{P}_2^{-1}} \\ I_k \otimes pM_{\mathfrak{P}_2^{-1}} & \mathbf{0} \end{bmatrix} \end{aligned}$$

By Proposition 5.13,

$$\frac{1}{\sqrt{2p}}\begin{bmatrix} -A^\top \widetilde{\otimes} M & I_k \otimes M \\ I_k \otimes pM & \mathbf{0} \end{bmatrix}$$

can be seen to be another generator matrix, it suffices now to prove

$$\sqrt{d}(I_k \otimes M^*_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) = A^\top \widetilde{\otimes} M,$$

which is equivalent to

$$\begin{aligned}
& (I_k \otimes M_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top (I_k \otimes M^*_{\mathfrak{P}_2^{-1}}) = A^\top \widetilde{\otimes} M \\
\iff\ & (I_k \otimes M_{\mathfrak{P}_2^{-1}})(A\widetilde{\otimes}M)^\top = (A^\top \widetilde{\otimes} M)(I_k \otimes M^\top_{\mathfrak{P}_2^{-1}}) \\
\iff\ & (A\widetilde{\otimes}M)(I_k \otimes M^\top_{\mathfrak{P}_2^{-1}}) = (I_k \otimes M_{\mathfrak{P}_2^{-1}})(A^\top \widetilde{\otimes} M)^\top \\
\iff\ & (A\widetilde{\otimes}M)(I_k \otimes M^\top) = (I_k \otimes M)(A^\top \widetilde{\otimes} M)^\top \\
\iff\ & \mathrm{Tr}\left(A \otimes M_1 M_1^\top\right) = (I_k \otimes M)(A^\top \widetilde{\otimes} M)^\top,
\end{aligned}$$

which can be checked by direct computations. □

5.2.2 Approach II

In this subsection, let $C \subseteq \mathbb{F}_{p^2}^N$ be a linear code not necessarily having a generator matrix in the standard form. We consider the lattice $(\rho^{-1}(C), b_\alpha)$, where $\alpha = 1/p$ if $d \equiv 1 \bmod 4$ and $\alpha = 1/(2p)$ if $d \equiv 2, 3 \bmod 4$. Thus b_α is the following bilinear form (see (5.2)):

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \begin{cases} \frac{1}{p}\sum_{i=1}^N \mathrm{Tr}\left(x_i y_i\right) & d \equiv 1 \bmod 4 \\ \frac{1}{2p}\sum_{i=1}^N \mathrm{Tr}\left(x_i y_i\right) & d \equiv 2, 3 \bmod 4 \end{cases}.$$

Then the dual of $\rho^{-1}(C)$ is given by $(\rho^{-1}(C)^*, b_\alpha)$, where $\rho^{-1}(C)^* := \{\boldsymbol{x} \in K^N : b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}\ \forall \boldsymbol{y} \in \rho^{-1}(C)\}$. We have the following relation between the dual of $\rho^{-1}(C)$ and the lattice constructed from the dual of C:

Lemma 5.16. $\rho^{-1}(C^\perp) \subseteq \rho^{-1}(C)^*$.

Proof. Take any $\boldsymbol{x} \in \rho^{-1}(C^\perp)$ and $\boldsymbol{y} \in \rho^{-1}(C)$, we have

$$\begin{aligned}
\rho(\boldsymbol{x} \cdot \boldsymbol{y}) &= \rho\left(\sum_{i=1}^N x_i y_i\right) = \sum_{i=1}^N \rho(x_i)\rho(y_i) \\
&= \rho(\boldsymbol{x}) \cdot \rho(\boldsymbol{y}) = 0 \in \mathbb{F}_{p^2},
\end{aligned}$$

where the last equality follows from the definition of $C^\perp$ (see (5.3)). Then

$$\sum_{i=1}^N x_i y_i = \boldsymbol{x} \cdot \boldsymbol{y} \equiv 0 \bmod (p).$$

Since p is inert, $\sigma_2\left(\sum_{i=1}^N x_i y_i\right) \in (p)$, we have

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

In the case $d \equiv 2, 3 \bmod 4$, any element in $\mathcal{O}_K$ has even trace. In conclusion, we have $b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}$ and hence $\rho^{-1}(C^\perp) \subseteq \rho^{-1}(C)^*$ by definition. □

Corollary 5.17. Let C be a self-orthogonal linear code, then $\rho^{-1}(C)$ is integral.

Proof. As C is self-orthogonal, we have $C \subseteq C^\perp$. Hence by Lemma 5.16 $\rho^{-1}(C) \subseteq \rho^{-1}(C^\perp)$ $\subseteq \rho^{-1}(C)^*$. □

By Lemma 5.1 the discriminant of $\rho^{-1}(C)$ is

$$\left.\begin{array}{ll} \frac{1}{p^{2N}}(\Delta^N p^{4k}) = \Delta^N & d \equiv 1 \bmod 4 \\ \frac{1}{(2p)^{2N}}(\Delta^N p^{4k}) = \left(\frac{\Delta}{4}\right)^N & d \equiv 2, 3 \bmod 4 \end{array}\right\} = d^N$$

We have

Proposition 5.18. $\rho^{-1}(C)$ is $d-$modular.

Proof. We first prove $\frac{1}{\sqrt{d}}\rho^{-1}(C) = \rho^{-1}(C)^*$ as $\mathbb{Z}-$modules.

Take any $\boldsymbol{x} \in \frac{1}{\sqrt{d}}\rho^{-1}(C)$, $\boldsymbol{x} = \frac{1}{\sqrt{d}}\boldsymbol{x}'$ with $\boldsymbol{x}' \in \rho^{-1}(C)$. Take any $\boldsymbol{y} \in \rho^{-1}(C)$.

Case 1 For $d \equiv 1 \bmod 4$,

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{p}\sum_{i=1}^N \mathrm{Tr}\left(x_i y_i\right) = \frac{1}{p}\sum_{i=1}^N \mathrm{Tr}\left(\frac{1}{\sqrt{d}} x_i' y_i\right).$$

Since $x_i' \in \mathcal{O}_K$, $\frac{1}{\sqrt{d}}x_i' \in \mathcal{D}_K^{-1}$. We have

$$\mathrm{Tr}\left(\frac{1}{\sqrt{d}} x_i' y_i\right) \in \mathbb{Z} \Longrightarrow \mathrm{Tr}\left(\sum_{i=1}^N \frac{1}{\sqrt{d}} x_i' y_i\right) \in \mathbb{Z}.$$

By the same argument as in the proof of Lemma 5.16, we have $\sum_{i=1}^N x_i' y_i \in (p)$, so $\sum_{i=1}^N \frac{1}{\sqrt{d}} x_i' y_i \in p\mathcal{D}_K^{-1}$.

Since $\sigma_2(p) = p$, $\sigma_2(\mathcal{D}_K^{-1}) = \mathcal{D}_K^{-1}$, $\mathrm{Tr}\left(\sum_{i=1}^N \frac{1}{\sqrt{d}} x_i' y_i\right) \in p\mathcal{D}_K^{-1}$. We have $\mathrm{Tr}\left(\sum_{i=1}^N \frac{1}{\sqrt{d}} x_i' y_i\right) \in$ $p\mathcal{D}_K^{-1} \cap \mathbb{Z}$.

Case 2 For $d \equiv 2, 3 \bmod 4$,

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{2p}\sum_{i=1}^N \mathrm{Tr}\left(x_i y_i\right) = \frac{1}{p}\sum_{i=1}^N \mathrm{Tr}\left(\frac{1}{2\sqrt{d}} x_i' y_i\right).$$

Since $x_i' \in \mathcal{O}_K$, $\frac{1}{2\sqrt{d}}x_i' \in \mathcal{D}_K^{-1}$. We have

$$\mathrm{Tr}\left(\frac{1}{2\sqrt{d}}x_i'y_i\right) \in \mathbb{Z} \Longrightarrow \mathrm{Tr}\left(\sum_{i=1}^{N}\frac{1}{2\sqrt{d}}x_i'y_i\right) \in \mathbb{Z}.$$

Similarly we have $\sum_{i=1}^{N} x_i'y_i \in (p)$, so $\sum_{i=1}^{N}\frac{1}{2\sqrt{d}}x_i'y_i \in p\mathcal{D}_K^{-1}$.

Since $\sigma_2(p) = p$, $\sigma_2(\mathcal{D}_K^{-1}) = \mathcal{D}_K^{-1}$, $\mathrm{Tr}\left(\sum_{i=1}^{N}\frac{1}{2\sqrt{d}}x_i'y_i\right) \in p\mathcal{D}_K^{-1}$. Hence we have $\mathrm{Tr}\left(\sum_{i=1}^{N}\frac{1}{2\sqrt{d}}x_i'y_i\right) \in p\mathcal{D}_K^{-1} \cap \mathbb{Z}$.

By definition of different, $\mathcal{O}_K \subseteq \mathcal{D}_K^{-1}$, so $p\mathcal{O}_K \subseteq p\mathcal{D}_K^{-1}$, we have $p\mathcal{D}_K^{-1} \cap \mathbb{Z} \supseteq \mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$, which gives $p\mathcal{D}_K^{-1} \cap \mathbb{Z} = \mathbb{Z}$ or $p\mathbb{Z}$. But $p\mathcal{D}_K^{-1} \cap \mathbb{Z} = \mathbb{Z}$ implies $(p)|\mathcal{D}_K$, which is impossible as p is inert. We have $p\mathcal{D}_K^{-1} \cap \mathbb{Z} = p\mathbb{Z}$ and hence $b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}$.

We have proved $\frac{1}{\sqrt{d}}\rho^{-1}(C) \subseteq \rho^{-1}(C)^*$.

On the other hand,

$$vol(\frac{1}{\sqrt{d}}\rho^{-1}(C)) = vol(\rho^{-1}(C))\left|\rho^{-1}(C)/\frac{1}{\sqrt{d}}\rho^{-1}(C)\right| = \sqrt{d^N}\left(\frac{1}{\sqrt{d}}\right)^{2N} = d^{-\frac{N}{2}},$$

and [22]

$$vol(\rho^{-1}(C)^*) = \frac{1}{vol(\rho^{-1}(C))} = \frac{1}{\sqrt{d^N}} = d^{-\frac{N}{2}}.$$

Thus we have $\rho^{-1}(C)^* = \frac{1}{\sqrt{d}}\rho^{-1}(C)$. Define

$$\begin{aligned} h : (\rho^{-1}(C), b_\alpha) &\to (\rho^{-1}(C)^*, b_\alpha) \\ x &\mapsto \frac{1}{\sqrt{d}}x. \end{aligned}$$

By the above, h is a $\mathbb{Z}-$linear bijection. Take any $\boldsymbol{x}, \boldsymbol{y} \in \rho^{-1}(C)$,

$$\begin{aligned} d \cdot b_\alpha(h(\boldsymbol{x}), h(\boldsymbol{y})) &= d \cdot \mathrm{Tr}\left(\sum_{i=1}^{N}\alpha h(x)_i h(y)_i\right) \\ &= d \cdot \mathrm{Tr}\left(\sum_{i=1}^{N}\alpha\frac{1}{\sqrt{d}}x_i\frac{1}{\sqrt{d}}y_i\right) = d \cdot \mathrm{Tr}\left(\sum_{i=1}^{N}\alpha\frac{1}{d}x_iy_i\right) \\ &= \mathrm{Tr}\left(\sum_{i=1}^{N}\alpha x_iy_i\right) = b_\alpha(\boldsymbol{x}, \boldsymbol{y}). \end{aligned}$$

The proof is completed. □

5.3 Interesting Lattices from Totally Real Quadratic Fields

The previous section gave generic methods to construct modular lattices, out of which we now would like to find lattices with good properties in terms of minimal norm or secrecy gain. The following definitions hold for integral lattices. Let thus (L, b) be an integral lattice with generator matrix M_L. We further assume that the lattice is embedded in $\mathbb{R}^n$, and that b is the natural inner product. We will then denote the lattice by L for short. We recall some discussions from Section 2.2.

Definition 5.19. [19, 22] The *minimum*, or *minimal norm*, of L in $\mathbb{R}^n$, is

$$\mu_L := \min\{\|\boldsymbol{x}\|^2 : \boldsymbol{x} \in L\}, \tag{5.14}$$

which is the length of the shortest nonzero vector.

One motivation to consider the shortest nonzero vector comes from the sphere packing problem [19], which requires large minimum. Recall from Definition 2.11 that the upper bound on minimum has been established for a $d-$modular lattice which satisfies certain conditions. And a $d-$modular lattice that fulfills those conditions as well as achieves the corresponding upper bound on its minimum is called *extremal*.

Definition 5.20. [19, Chapter 2] Let $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\,(\tau) > 0\}$. For $\tau \in \mathbb{H}$ let $q = e^{\pi i \tau}$. The *theta series* of the lattice L is the function

$$\Theta_L(\tau) := \sum_{\boldsymbol{x} \in L} q^{\|\boldsymbol{x}\|^2} = \sum_{m \in \mathbb{Z}_{\geq 0}} A_m q^m, \tag{5.15}$$

where the second equality holds because we took L to be integral and $A_m = |\{\boldsymbol{x} : \boldsymbol{x} \in L,\ \|\boldsymbol{x}\|^2 = m\}|$.

The coefficient of q in the second term of Θ_L is called the kissing number of L, and the power of q in the second term gives its minimum. The theta series helps in determining bounds for the minimum [51] as well as classifying lattices [10]. It has also been used recently to define the notion of secrecy gain.

Definition 5.21. Let L be an $n-$dimensional lattice. The secrecy function of L is given by

$$\Xi = \frac{\Theta_{\sqrt[n]{vol(L)}\mathbb{Z}^n}(\tau)}{\Theta_L(\tau)}, \tau = yi, y > 0. \tag{5.16}$$

The secrecy gain χ_L is defined to be the maximum of the secrecy function w.r.t to y.

The geometrical symmetry of a $d-$modular lattice generates a local maximum in its secrecy function at $y = \frac{1}{d}$, which is defined to be the *weak secrecy gain*:

Definition 5.22. Let L be an $n-$dimensional $d-$modular lattice. The *weak secrecy gain* of L, denoted by χ_L^W, is given by [44]:

$$\chi_L^W = \frac{\Theta_{\sqrt[4]{d}\mathbb{Z}^n}(\tau)}{\Theta_L(\tau)}, \tau = \frac{i}{\sqrt{d}}, \tag{5.17}$$

noting that the volume of a $d-$modular lattice is $vol(L) = d^{\frac{n}{4}}$.

The secrecy gain characterizes the amount of confusion that a wiretap lattice code brings [44]. The weak secrecy gain χ_L^W is conjectured to be the secrecy gain itself. This conjecture is still open, but for large classes of unimodular lattices, it is known to be true [23, 47]. This motivates the study of the relationship between d and χ_L^W for $d-$modular lattices [32, 33]. Up to now, no clear conclusion has been drawn. We will construct some examples of $d-$modular lattices in Section 5.3 to gain more information regarding this problem.

Consider the $2N-$dimensional $d-$modular lattice $(\rho^{-1}(C), b_\alpha)$ with

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \begin{cases} \frac{1}{p}\sum_{i=1}^{N} \mathrm{Tr}\left(x_i y_i\right) & d \equiv 1 \bmod 4 \\ \frac{1}{2p}\sum_{i=1}^{N} \mathrm{Tr}\left(x_i y_i\right) & d \equiv 2, 3 \bmod 4 \end{cases}$$

obtained from a self-dual code $C \subseteq \mathbb{F}_{p^2}^N$, where p a prime inert in $K = \mathbb{Q}(\sqrt{d})$, for d a square-free positive integer. A generator matrix M_C is given by (5.10).

We thus consider next the following properties of those $d-$modular lattices:

• whether the lattice constructed is even or odd; recall that an integral lattice (L, b) is called *even* if $b(x, x) \in 2\mathbb{Z}$ for all $x \in L$ and *odd* otherwise.

• the minimum of the lattice;

• the theta series and secrecy gain of the lattice.

5.3.1 Even/Odd Lattices and Minimum

We will give general results for the first two properties in this subsection. By observing the Gram matrices, we have the following results

Proposition 5.23. The lattice $(\rho^{-1}(C), b_\alpha)$ is even if and only if $d \equiv 5 \bmod 8$, $p = 2$ and the diagonal entries of $I + AA^\top$ are elements from (4).

Proof. **Case 1**: $d \equiv 2, 3 \bmod 4$, 2 is always ramified, so p is an odd prime. And we have

$$MM^\top = \begin{bmatrix} 1 & 1 \\ 1+\sqrt{d} & 1-\sqrt{d} \end{bmatrix} \begin{bmatrix} 1 & 1+\sqrt{d} \\ 1 & 1-\sqrt{d} \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 2+2d \end{bmatrix}.$$

The lower right corner of the Gram matrix is given by

$$\frac{1}{2} I_k \otimes p \begin{bmatrix} 2 & 2 \\ 2 & 2+2d \end{bmatrix} = I_k \otimes \begin{bmatrix} p & p \\ p & p(1+d) \end{bmatrix}.$$

Hence the lattice is odd.

Case 2: $d \equiv 1 \bmod 4$ and p is an odd prime

$$MM^\top = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{bmatrix} \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix}.$$

The lower right corner of the Gram matrix is given by

$$I_k \otimes p \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix} = I_k \otimes \begin{bmatrix} 2p & p \\ p & p\frac{(1+d)}{2} \end{bmatrix}.$$

Hence the lattice is odd.

Case 3: When $d \equiv 1 \bmod 4$ and $p = 2$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. The minimum polynomial of $\frac{1+\sqrt{d}}{2}$ is $f(x) = x^2 - x + \frac{1-d}{4}$. We have

$$f(x) \equiv \begin{cases} x^2 - x \equiv x(x-1) \bmod 2 & d \equiv 1 \bmod 8 \\ x^2 - x + 1 \bmod 2 & d \equiv 5 \bmod 8 \end{cases}$$

So 2 is inert only when $d \equiv 5 \bmod 8$. In this case, the right lower corner of the Gram Matrix is

$$I_k \otimes 2 \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix} = I_k \otimes \begin{bmatrix} 4 & 2 \\ 2 & d+1 \end{bmatrix},$$

which has even diagonal entries.

Furthermore,

$$M_1 M_1^\top = \begin{bmatrix} 1 \\ \frac{1+\sqrt{d}}{2} \end{bmatrix} \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \end{bmatrix} = \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} & \frac{1+d+2\sqrt{d}}{4} \end{bmatrix}.$$

The left upper corner of the Gram Matrix is

$$\frac{1}{2}\mathrm{Tr}\left((I+AA^\top)\otimes M_1M_1^\top\right)=\mathrm{Tr}\left((I+AA^\top)\otimes\begin{bmatrix}\frac{1}{2} & \frac{1+\sqrt{d}}{4}\\ \frac{1+\sqrt{d}}{4} & \frac{1+d+2\sqrt{d}}{8}\end{bmatrix}\right).$$

Let $\{\boldsymbol{c}_1,\dots,\boldsymbol{c}_t\}$ be the rows of $[I\ A \bmod (2)]$, i.e. they form a basis for C. Let $\{\hat{\boldsymbol{c}}_1,\dots,\hat{\boldsymbol{c}}_k\}$ denote the rows of $[I\ A]$, i.e. $\hat{\boldsymbol{c}}_i$ is a preimage of $\boldsymbol{c}_i$. Then the diagonal entries of $\frac{1}{2}\mathrm{Tr}\left((I+AA^\top)\otimes M_1M_1^\top\right)$ are given by $\mathrm{Tr}\left(\frac{1}{2}\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right)$ and $\mathrm{Tr}\left(\frac{1+d+2\sqrt{d}}{8}\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right)$. The lattice is even iff $\forall i$, $\mathrm{Tr}\left(\frac{1}{2}\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right),\mathrm{Tr}\left(\frac{1+d+2\sqrt{d}}{8}\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right)\in 2\mathbb{Z}$, i.e.

$$\mathrm{Tr}\left(\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right),\mathrm{Tr}\left(\frac{1+d+2\sqrt{d}}{4}\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\right)\in 4\mathbb{Z}. \tag{5.18}$$

As $d\equiv 1 \bmod 4$,

$$\frac{1+\sqrt{d}}{2}=\frac{1+d+2\sqrt{d}}{4}-\frac{d-1}{4}$$

shows $\{1,\frac{1+d+2\sqrt{d}}{4}\}$ is a $\mathbb{Z}-$basis for $\mathcal{O}_K$. Then (5.18) is equivalent as $\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\in 4\mathcal{D}_K^{-1}$. Since $\hat{\boldsymbol{c}}_i\in\mathcal{O}_K$, $\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\in\mathcal{O}_K$, the lattice is even iff

$$\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i\in 4\mathcal{D}_K^{-1}\cap\mathcal{O}_K=4\mathcal{O}_K$$

$\hat{\boldsymbol{c}}_i\cdot\hat{\boldsymbol{c}}_i$ are exactly the diagonal entries of $I+AA^\top$ and the proof is completed. □

Next we look at the minimum of some of those lattices.

Consider $d\equiv 2,3 \bmod 4$. Let p be a prime such that $\left(\frac{d}{p}\right)=-1$, hence p is inert in $\mathbb{Q}(\sqrt{d})$ and the finite field $\mathbb{F}_{p^2}\cong\mathbb{F}_p(\omega)$, where ω satisfies the polynomial $x^2-d=0 \bmod p$. Let $C\subseteq\mathbb{F}_{p^2}^N$ be a self-dual linear code. Then each codeword $\boldsymbol{c}\in C$ can be written as $\boldsymbol{s}+\boldsymbol{t}\omega$ for some $\boldsymbol{s},\boldsymbol{t}\in\mathbb{F}_p^N$. For each coordinate of $\boldsymbol{c}$, we have $c_i=s_i+t_i\omega$. Note that each $\hat{\boldsymbol{c}}\in\mathcal{O}_K^N$ with $\hat{c}_i=s_i+t_i\sqrt{d}\in\mathcal{O}_K$, where s_i and t_i are considered as integers, is a preimage of $\boldsymbol{c}$. Furthermore, we can assume $s_i,t_i\in\{-\frac{p-1}{2},\frac{p-3}{2},\dots,-1,0,1,\dots,\frac{p-1}{2}\}$. We have proved that $(\rho^{-1}(C),b_\alpha)$ is an odd $d-$modular lattice of dimension $2N$. Moreover, we have

Lemma 5.24. For $d\equiv 2,3 \bmod 4$, the minimum of $(\rho^{-1}(C),b_\alpha)$ is given by

$$\min\left\{p,\ \min_{\boldsymbol{c}\in C\setminus\{\boldsymbol{0}\}}b_\alpha(\hat{\boldsymbol{c}},\hat{\boldsymbol{c}})\right\}$$

Proof. Take any $\boldsymbol{c}\in C$, then any $\boldsymbol{x}\in\rho^{-1}(\boldsymbol{c})$ is of the form $\boldsymbol{x}=\hat{\boldsymbol{c}}+p\boldsymbol{y}$ for some $\boldsymbol{y}\in\mathcal{O}_K^N$.

Write $y_i = a_i + b_i\sqrt{d}$ for $a_i, b_i \in \mathbb{Z}$. Then

$$x_i^2 = (c_i + py_i)^2 = ((s_i + pa_i) + (t_i + pb_i)\sqrt{d})^2, \mathrm{Tr}\left(x_i^2\right) = 2(s_i + pa_i)^2 + 2(t_i + pb_i)^2 d.$$

Since $a_i \in \mathbb{Z}$, $s_i \in \{-\frac{p-1}{2}, \frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$, the minimum value for $(s_i + pa_i)^2$ is s_i^2. Similarly, the minimum value for $(t_i + pb_i)^2$ is t_i^2.

For $\boldsymbol{c} \neq \mathbf{0}$, minimum value for $\mathrm{Tr}\left(x_i^2\right)$ is $2s_i^2 + 2t_i^2 d$ and we have

$$\min_{\boldsymbol{x} \in \rho^{-1}(\boldsymbol{c})} b_\alpha(\boldsymbol{x}, \boldsymbol{x}) = \frac{1}{2p} \sum_{i=1}^{N} 2(s_i^2 + t_i^2 d) = \frac{1}{2p} \sum_{i=1}^{N} \mathrm{Tr}\left(\hat{c}_i^2\right) = b_\alpha(\hat{\boldsymbol{c}}, \hat{\boldsymbol{c}}).$$

When $\boldsymbol{c} = \mathbf{0}$

$$b_\alpha(\boldsymbol{x}, \boldsymbol{x}) = \frac{1}{2p} \sum_{i=1}^{N} \mathrm{Tr}\left(x_i^2\right) = p \sum_{i=1}^{N} (a_i^2 + b_i^2 d),$$

which has minimum value p ($\boldsymbol{x} \neq \mathbf{0}$).

We have

$$\min_{\boldsymbol{x} \in \rho^{-1}(C)} b_\alpha(\boldsymbol{x}, \boldsymbol{x}) = \min_{\boldsymbol{c} \in C} \{ \min_{\boldsymbol{x} \in \rho^{-1}(\boldsymbol{c})} b_\alpha(\boldsymbol{x}, \boldsymbol{x}) \} = \min \left\{ p, \min_{\boldsymbol{c} \in C \setminus \{\mathbf{0}\}} b_\alpha(\hat{\boldsymbol{c}}, \hat{\boldsymbol{c}}) \right\}.$$

□

5.3.2 Construction of Existing Lattices

We present a construction from codes of some well known lattices.

Example 5.25. Take $d = 5$, $p = 2$, $N = 4$, $C \subseteq \mathbb{F}_4^4$ with generator matrix $[I \ A \bmod (2)]$ and $A \bmod (2)$ is given by

$$\begin{bmatrix} \omega^2 & \omega \\ -\omega & \omega^2 \end{bmatrix},$$

where $\omega \in \mathbb{F}_4$ satisfies $\omega^2 + \omega + 1 = 0$. Taking $\frac{1+\sqrt{5}}{2}$ to be the preimage of ω, we have

$$I + AA^\top = \begin{bmatrix} 2\sqrt{d} + 6 & 0 \\ 0 & 2\sqrt{d} + 6 \end{bmatrix}$$

By Proposition 5.23 L is an even 5-modular lattice of dimension 8. This lattice is actually the unique 5-modular even lattice of dimension 8 and minimum 4 ($Q_8(1)$ in Table 1 of [51]).

Example 5.26. Take $d = 6$, $p = 7$, $N = 4$, $C \subseteq \mathbb{F}_{25}^4$ with generator matrix $[I \ A \bmod (7)]$ and

$A \bmod (7)$ is given by

$$\begin{bmatrix} 2+\omega & 2-\omega \\ 2-\omega & -2-\omega \end{bmatrix},$$

where $\omega \in \mathbb{F}_{25}$ satisfies $\omega^2 = 2$. Then we get the unique 6-modular odd lattice of dimension 8 and minimum 3 ($O^{(6)}$ in Table 1 of [51]).

Example 5.27. Take $d = 3$, $p = 5$, $N = 6$, linear code $C \subset \mathbb{F}_{25}^6$ generated by $[I\ A \bmod (5)]$ and $A \bmod (5))$ is given by

$$\begin{bmatrix} \omega+1 & 2\omega+2 & 2 \\ 2\omega+1 & 2 & -\omega+2 \\ -\omega+3 & \omega+1 & 2\omega+1 \end{bmatrix}.$$

We get the unique $3-$modular odd lattice of dimension 12 and minimum 3 ($O^{(3)}$ in Table 1 of [51]).

Example 5.28. Take $d = 2$, $p = 5$, $N = 8$, $C \subseteq \mathbb{F}_{25}^8$ with generator matrix $[I\ A \bmod (5)]$. $A \bmod (5)$ is given by

$$\begin{pmatrix} 2\omega+1 & 4\omega+1 & 4\omega+3 & 4\omega+3 \\ \omega+3 & 2 & 0 & 3\omega+4 \\ 3\omega+3 & 0 & 2 & 4a+4 \\ 3\omega+2 & 3\omega+2 & 3\omega+1 & 1 \end{pmatrix}$$

where $\omega \in \mathbb{F}_{25}$ satisfies $\omega^2 = 2$. Taking $\sqrt{2}$ to be the preimage of ω, we have the unique odd 2-modular lattice of dimension 16 with minimum 3 (Odd Barnes-Wall lattice $O^{(2)}$ in Table 1 of [51]).

Example 5.29. Take $d = 5$, $p = 2$, $N = 6$, $C \subseteq \mathbb{F}_4^6$ with generator matrix $[I\ A \bmod (2)]$ and $A \bmod (2)$ is given by

$$\begin{bmatrix} \omega & 1 & \omega \\ 0 & \omega+1 & \omega \\ \omega+1 & \omega+1 & 1 \end{bmatrix},$$

where $\omega \in \mathbb{F}_4$ satisfies $\omega^2 + \omega + 1 = 0$. Taking $\frac{1+\sqrt{5}}{2}$ to be the preimage of ω, we have $(I + AA^\top)_{11} = \sqrt{5} + 5 \notin (4)$. By Proposition 5.23, we have an odd 5-modular lattice of dimension 12. We computed that this lattice has minimum 4, kissing number 60. It is an extremal 5-modular lattice in dimension 12 and it is isometric to the lattice $L_5(4,6)_c$ in [41].

5.3.3 Some Lattices with Large Minimum

We next present two lattices which, though not extremal, achieve a large minimum. "Large" means close to the bound that extremal lattices achieve. We also compute their theta series, so we can later on compute their weak secrecy gain. Evidence from unimodular lattices [32] suggests that a large minimum induces a large weak secrecy gain.

Example 5.30. Take $d = 7$, $p = 5$, $N = 4$, we get an odd $8-$dimensional $7-$modular lattice which is rationally equivalent to the direct sum of 4 copies of $C^{(7)}$ with minimum 3 and theta series $1 + 16q^3 + 16q^4 + O(q^5)$. Note that the upper bound for the minimum of such a modular lattice is 4 (see Definition 2.11).

Example 5.31. Take $d = 6$, $N = 6$, we can get three different $12-$dimensional $6-$modular lattices with minimum 3. They are odd, rationally equivalent to direct sum of 6 copies of $C^{(6)}$. But they are not strongly modular. To the best of our knowledge, they are new lattices. Their theta series are as follows:

$$1 + 4q^3 + 36q^4 + O(q^5)$$
$$1 + 12q^3 + 40q^4 + O(q^5)$$
$$1 + 16q^3 + 36q^4 + O(q^5).$$

5.3.4 Modular Lattices and their Weak Secrecy Gain

We are now interested in the relationship between the level d and the weak secrecy gain χ_L^W (see Definition 5.22). We list the weak secrecy gain of some lattices we have constructed for dimensions 8 (Table 5.1), 12 (Table 5.2) and 16 (Table 5.3). In the tables, each row corresponds to a lattice L

- labeled by 'No.';
- in dimension 'Dim';
- of level d (i.e., L is $d-$modular);
- with minimum μ_L (the norm of the shortest vector, see Definition 5.19);
- kissing number 'ks' (the number of lattice points with minimal norm);
- obtains weak secrecy gain χ_L^W (see Definition 5.22).

Then in the last column we give the first 10 coefficients of its theta series Θ_L (see Definition 5.20).

Remark 5.32. From the tables we have the following observations:

Table 5.1: Weak Secrecy Gain-Dimension 8

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
1	8	3	2	8	1.2077	1	0	8	64	120	192	424	576	920	1600
2	8	5	2	8	1.0020	1	0	8	16	24	96	128	208	408	480
3	8	5	4	120	1.2970	1	0	0	0	120	0	240	0	600	0
4	8	6	3	16	1.1753	1	0	0	16	24	48	128	144	216	400
5	8	7	2	8	0.8838	1	0	8	0	24	64	32	128	120	192
6	8	7	3	16	1.1048	1	0	0	16	16	16	80	128	224	288
7	8	11	3	8	1.0015	1	0	0	8	8	8	24	48	72	88
8	8	14	2	8	0.5303	1	0	8	0	24	0	32	8	24	64
9	8	14	3	8	0.9216	1	0	0	8	0	8	32	0	48	80
10	8	15	3	8	0.8869	1	0	0	8	0	8	24	0	64	32
11	8	15	4	8	1.0840	1	0	0	0	8	16	0	16	32	64
12	8	23	3	8	0.6847	1	0	0	8	0	0	24	0	8	40
13	8	23	5	16	1.0396	1	0	0	0	0	16	0	0	16	0
14	8	23	5	8	1.1394	1	0	0	0	0	8	0	8	24	24

Table 5.2: Weak Secrecy Gain-Dimension 12

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
15	12	3	1	12	0.4692	1	12	60	172	396	1032	2524	4704	8364	17164
16	12	3	1	4	0.8342	1	4	28	100	332	984	2236	5024	9772	16516
17	12	3	1	4	0.9385	1	4	12	100	428	984	2092	5024	9708	16516
18	12	3	2	24	1.2012	1	0	24	64	228	960	2200	5184	10524	16192
19	12	3	2	12	1.3650	1	0	12	64	300	960	2092	5184	10476	16192
20	12	3	3	64	1.5806	1	0	0	64	372	960	1984	5184	10428	16192
21	12	5	2	12	1.0030	1	0	12	24	60	240	400	984	2172	3440
22	12	5	4	60	1.6048	1	0	0	0	60	288	520	960	1980	3680
23	12	6	1	12	0.1820	1	12	60	160	252	312	556	1104	1740	2796
24	12	6	1	6	0.3845	1	6	20	58	132	236	460	936	1564	2478
25	12	6	2	8	0.9797	1	0	8	20	36	144	264	544	1244	2016
26	12	6	3	16	1.3580	1	0	0	16	36	96	256	624	1308	2112
27	12	6	3	12	1.3974	1	0	0	12	40	100	244	668	1284	2076
28	12	6	3	12	1.5044	1	0	0	4	36	132	256	660	1308	1980
29	12	7	1	12	0.1452	1	12	60	160	252	312	544	972	1164	1596
30	12	7	1	4	0.4645	1	4	12	32	60	168	416	580	876	1684
31	12	7	1	4	0.5806	1	4	4	16	84	152	208	580	1268	1908
32	12	7	2	12	0.7584	1	0	12	16	36	144	112	384	852	1056
33	12	7	2	8	0.8795	1	0	8	16	28	112	160	384	772	1152
34	12	7	3	4	1.4023	1	0	0	4	36	84	64	384	972	1368
35	12	11	1	8	0.1765	1	8	24	36	60	180	356	424	612	1204
36	12	11	1	4	0.2173	1	4	16	48	88	152	204	144	316	772
37	12	11	3	12	1.0726	1	0	0	12	0	12	108	72	108	436
38	12	14	1	8	0.1331	1	8	24	36	56	148	264	320	544	912
39	12	14	1	4	0.1534	1	4	16	48	88	152	204	144	280	628
40	12	14	3	12	0.9134	1	0	0	12	0	0	72	48	72	256
41	12	15	1	8	0.1313	1	8	24	32	32	112	292	352	328	744
42	12	15	1	4	0.3899	1	4	4	0	12	56	96	80	132	388
43	12	15	1	2	0.4661	1	2	0	10	32	30	44	96	128	186
44	12	15	2	6	0.5455	1	0	6	8	4	42	46	74	136	154
45	12	15	2	6	0.9217	1	0	2	2	4	24	20	46	100	154
46	12	15	3	4	1.0031	1	0	0	4	8	18	28	36	64	104
47	12	15	4	4	1.3573	1	0	0	0	4	10	12	48	72	108
48	12	15	5	4	1.5265	1	0	0	0	0	4	12	44	108	112
49	12	23	1	8	0.0698	1	8	24	36	56	144	228	192	316	652
50	12	23	1	4	0.0735	1	4	16	48	88	152	204	144	280	628
51	12	23	3	12	0.5690	1	0	0	12	0	0	60	0	0	172

Table 5.3: Weak Secrecy Gain-Dimension 16

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
52	16	3	2	16	1.4585	1	0	16	128	304	1408	6864	19584	47600	112768
53	16	3	2	12	1.6669	1	0	12	48	440	1808	6332	18864	47648	113968
54	16	3	2	8	1.7612	1	0	8	48	416	1808	6440	18864	48016	113968
55	16	3	2	4	1.8303	1	0	4	64	360	1728	6676	19008	48448	113728
56	16	5	2	2	1.7671	1	0	2	4	72	216	884	2452	6432	14520
57	16	5	4	240	1.6822	1	0	0	0	240	0	480	0	15600	0
58	16	5	4	112	1.9213	1	0	0	0	112	0	1248	2048	5872	16384
59	16	5	4	64	1.9855	1	0	0	0	64	192	864	2432	6448	14656
60	16	5	4	48	2.0079	1	0	0	0	48	256	736	2560	6640	14080
61	16	6	2	16	0.8582	1	0	16	16	112	256	560	1792	2928	7616
62	16	6	3	18	1.5662	1	0	0	18	44	122	392	1050	2896	7126
63	16	6	3	8	1.7693	1	0	0	8	32	124	376	1112	3000	7156
64	16	6	3	8	1.8272	1	0	0	8	16	120	448	1128	2992	7176
65	16	7	3	32	1.2206	1	0	0	32	32	32	416	768	1216	3648
66	16	7	3	6	1.7604	1	0	0	6	12	74	252	560	1536	3968
67	16	7	3	2	1.8381	1	0	0	2	16	86	212	496	1556	4072
68	16	11	3	16	1.0985	1	0	0	16	0	16	176	96	192	1072
69	16	11	3	16	1.1138	1	0	0	16	0	12	164	100	240	1092
70	16	14	3	16	0.8864	1	0	0	16	0	0	128	64	96	640
71	16	14	3	16	0.8933	1	0	0	16	0	0	124	52	100	676
72	16	15	4	6	1.5187	1	0	0	0	6	10	22	54	78	182
73	16	15	4	4	1.6192	1	0	0	0	4	4	34	40	74	182
74	16	15	4	4	1.7660	1	0	0	0	4	0	14	24	134	156
75	16	15	4	2	1.8018	1	0	0	0	2	4	10	38	84	208
76	16	15	5	4	1.9146	1	0	0	0	0	4	8	26	100	178
77	16	15	5	4	1.9344	1	0	0	0	0	4	4	36	74	170
78	16	15	5	2	1.8890	1	0	0	0	0	2	16	42	70	160
79	16	23	3	16	0.4715	1	0	0	16	0	0	112	0	0	464
80	16	23	3	16	0.4720	1	0	0	16	0	0	112	0	0	460

1. When the dimension increases, the weak secrecy gain χ_L^W tends to increase, a behavior which has been proved for unimodular lattices [32];

2. Fixing dimension and level d, a large minimum is more likely to induce a large χ_L^W, which is also consistent with the observations on unimodular lattices [32];

3. Fixing dimension, level d and minimum μ_L, a smaller kissing number gives a larger χ_L^W (see e.g. rows 13,14; 15,16,17; 73-75). It was shown for unimodular lattices [32] that when the dimension n is fixed, $n \leq 23$, the secrecy gain is totally determined by the kissing number, and the lattice with the best secrecy gain is the one with the smallest kissing number;

4. Fixing dimension, minimum μ_L, kissing number, a smaller level d gives a bigger χ_L^W. For example, in Table 5.4 we list some $16-$dimensional lattices obtaining minimum 3 and kissing number 16, with χ_L^W in descending order.

5. Lattices with high level d are more likely to have a large minimum, this is more obvious when the dimension increases, and results in bigger χ_L^W. For example, see rows 13,14,48,76-78.

Some of those observations can be reasoned by calculating the value of χ_L^W: by (5.17) and

Table 5.4: Weak Secrecy Gain-Dimension 16 and minimum 3

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
69	16	11	3	16	1.1138	1	0	0	16	0	12	164	100	240	1092
68	16	11	3	16	1.0985	1	0	0	16	0	16	176	96	192	1072
71	16	14	3	16	0.8933	1	0	0	16	0	0	124	52	100	676
70	16	14	3	16	0.8864	1	0	0	16	0	0	128	64	96	640
80	16	23	3	16	0.4720	1	0	0	16	0	0	112	0	0	460
79	16	23	3	16	0.4715	1	0	0	16	0	0	112	0	0	464

(5.15), take $\tau = \frac{i}{\sqrt{d}}$, the numerator of χ_L^W is given by

$$\begin{aligned}\Theta_{\sqrt[4]{d}\mathbb{Z}^n}\left(\frac{i}{\sqrt{d}}\right) &= \sum_{\boldsymbol{x}\in\sqrt[4]{d}\mathbb{Z}^n} q^{\|\boldsymbol{x}\|^2} = \sum_{\boldsymbol{x}\in\mathbb{Z}^n} q^{\sqrt{d}\|\boldsymbol{x}\|^2} \\ &= \sum_{\boldsymbol{x}\in\mathbb{Z}^n} e^{\pi\cdot i\cdot i\cdot\frac{1}{\sqrt{d}}\cdot\sqrt{d}\|\boldsymbol{x}\|^2} = \sum_{\boldsymbol{x}\in\mathbb{Z}^n} e^{-\pi\|\boldsymbol{x}\|^2},\end{aligned}$$

which is a constant. The denominator of χ_L^W is given by

$$\begin{aligned}\Theta_L\left(\frac{i}{\sqrt{d}}\right) &= \sum_{\boldsymbol{x}\in L} q^{\|\boldsymbol{x}\|^2} = \sum_{\boldsymbol{x}\in L} e^{i\pi\cdot\frac{i}{\sqrt{d}}\|x\|^2} \\ &= \sum_{\boldsymbol{x}\in L} e^{\frac{-\pi}{\sqrt{d}}\|\boldsymbol{x}\|^2} = \sum_{m\in\mathbb{Z}_{\geq 0}} A_m\left(e^{-\frac{\pi}{\sqrt{d}}}\right)^m,\end{aligned}$$

where A_m is the number of vectors in L with norm m. Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{d}}}$, which is less than 1. Then the following will be preferable for achieving a large weak secrecy gain.

1. Large minimum, which determines the lowest power of $e^{-\frac{\pi}{\sqrt{d}}}$ in the power series.
2. Small value of A_m, i.e., small kissing number.
3. Small value of d, so that $e^{-\frac{\pi}{\sqrt{d}}}$ is small.

However, from the three tables, the minimum seems to be more dominant than other factors, and as we mentioned in Remark 5.32 point 5, large d can still be preferable for high dimensions since it may result in large minima.

5.4 Imaginary Quadratic Field

Let d be a positive square-free integer. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with Galois group $\{\sigma_1, \sigma_2\}$, where σ_1 is the identity map and $\sigma_2 : \sqrt{-d} \mapsto -\sqrt{-d}$. The

absolute value of the discriminant of K, denoted by Δ, is given by [42]:

$$\Delta = \begin{cases} 4d & d \equiv 1, 2 \bmod 4 \\ d & d \equiv 3 \bmod 4 \end{cases}.$$

Assume $p \in \mathbb{Z}$ is a prime which is totally ramified in K and let $\mathfrak{p}$ be the unique $\mathcal{O}_K-$ideal above p. Then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. Consider the lattice $(\rho^{-1}(C), b_\alpha)$ where C is a linear (N, k) code over $\mathbb{F}_p$.

Let $\alpha = 1/p$ when $d \equiv 3 \bmod 4$ and let $\alpha = 1/(2p)$ when $d \equiv 1, 2 \bmod 4$. Similarly to Section 5.2, we will give two proofs that if C is self-orthogonal (i.e., $C \subseteq C^\perp$), then the lattice $(\rho^{-1}(C), b_\alpha)$ is integral and furthermore we will prove that for C self-dual and for d a prime, we get unimodular lattices.

5.4.1 Approach I

By the discussion from Section 5.1, a generator matrix for $(\rho^{-1}(C), b_\alpha)$ is (see (5.8))

$$M_C = \sqrt{\alpha} \begin{bmatrix} I_k \otimes M & A \otimes M \\ \mathbf{0}_{nN-nk,nk} & I_{N-k} \otimes M_p \end{bmatrix} \tag{5.19}$$

where $[I_k \ (A \mod \mathfrak{p})]$ is a generator matrix for C,

$$M = \sqrt{2} \begin{bmatrix} 1 & 0 \\ \mathrm{Re}\,(v) & -\mathrm{Im}\,(v) \end{bmatrix}, M_p = \sqrt{2} \begin{bmatrix} \mathrm{Re}\,(\omega_1) & -\mathrm{Im}\,(\omega_1) \\ \mathrm{Re}\,(\omega_2) & -\mathrm{Im}\,(\omega_2) \end{bmatrix} \tag{5.20}$$

with $\{1, v\}$ a $\mathbb{Z}-$basis of $\mathcal{O}_K$, $\{\omega_1, \omega_2\}$ a $\mathbb{Z}-$basis of $\mathfrak{p}$ and

$$v = \begin{cases} \frac{1+\sqrt{-d}}{2} & d \equiv 3 \bmod 4 \\ \sqrt{-d} & d \equiv 1, 2 \bmod 4 \end{cases}. \tag{5.21}$$

Its Gram matrix is (see (5.9))

$$G_C = \alpha \begin{bmatrix} (I + AA^\top) \otimes \mathrm{Tr}\left(\boldsymbol{v}\boldsymbol{v}^\dagger\right) & A \otimes \mathrm{Tr}\left(\boldsymbol{v}\boldsymbol{\omega}^\dagger\right) \\ A^\top \otimes \mathrm{Tr}\left(\bar{\boldsymbol{\omega}}\boldsymbol{v}^\top\right) & I_{N-k} \otimes \mathrm{Tr}\left(\boldsymbol{\omega}\boldsymbol{\omega}^\dagger\right) \end{bmatrix}, \tag{5.22}$$

where $\boldsymbol{v} = [1, v]^\top, \boldsymbol{\omega} = [\omega_1, \omega_2]^\top$.

Lemma 5.33. If C is self-orthogonal, i.e. $C \subseteq C^\perp$, then $(\rho^{-1}(C), b_\alpha)$ is an integral lattice.

Proof. To prove $(\rho^{-1}(C), b_\alpha)$ is integral, it suffices to prove all entries of its Gram matrix G_C in (5.22) has integral entries.

Take any $x \in \mathfrak{p}$, as $\mathfrak{p}$ is the only prime ideal above p, we have $\sigma_2(x) \in \mathfrak{p}$ and hence $\mathrm{Tr}(x) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. As $\boldsymbol{v}\boldsymbol{\omega}^\dagger$, $\bar{\boldsymbol{\omega}}\boldsymbol{v}^\top$, $\boldsymbol{\omega}\boldsymbol{\omega}^\top$ all have entries in $\mathfrak{p}$, $\alpha A \otimes \mathrm{Tr}\left(\boldsymbol{v}\boldsymbol{\omega}^\dagger\right), \alpha A^\top \otimes \mathrm{Tr}\left(\bar{\boldsymbol{\omega}}\boldsymbol{v}^\top\right)$ and $\alpha I_{N-k} \otimes \mathrm{Tr}\left(\boldsymbol{\omega}\boldsymbol{\omega}^\top\right)$ all have entries in $\mathbb{Z}$. Furthermore, by Lemma 5.11, as C is self-orthogonal, $I_k + AA^\top \bmod \mathfrak{p} \equiv \mathbf{0} \bmod p$ and hence $I_k + AA^\top$ has entries in $p\mathbb{Z}$. We have $\alpha(I + AA^\top) \otimes \mathrm{Tr}\left(\boldsymbol{v}\boldsymbol{v}^\dagger\right)$ has integral entries.

When $d \equiv 1, 2 \bmod 4$, $\mathrm{Tr}(x)$ is even for all $x \in \mathcal{O}_K$. The proof is completed. □

Proposition 5.34. If C is self-dual and $d = p$ is a prime, the lattice $(\rho^{-1}(C), b_\alpha)$ is unimodular.

Proof. By Lemma 5.33, the lattice $(\rho^{-1}(C), b_\alpha)$ is integral. It suffices to prove it has discriminant 1 [22]. By Lemma 5.1, $(\rho^{-1}(C), b_\alpha)$ has discriminant

$$\Delta^N p^{2k} N(\alpha)^N = \begin{cases} d^N d^N \left(\frac{1}{d^2}\right)^N & d \equiv 3 \bmod 4 \\ (4d)^N d^N \left(\frac{1}{(2d)^2}\right)^N & d \equiv 1, 2 \bmod 4 \end{cases} = 1.$$

□

5.4.2 Approach II

In this subsection, we consider $C \subseteq \mathbb{F}_p^N$ a linear code not necessarily having a generator matrix in the standard form. We will give another proof that the lattice $(\rho^{-1}(C), b_\alpha)$ is integral, where $\alpha = 1/p$ if $d \equiv 3 \bmod 4$ and $\alpha = 1/(2p)$ if $d \equiv 1, 2 \bmod 4$. Thus b_α is the following bilinear form (see (5.2)):

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \mapsto \begin{cases} \frac{1}{p} \sum_{i=1}^N \mathrm{Tr}(x_i \bar{y}_i) & d \equiv 1 \bmod 4 \\ \frac{1}{2p} \sum_{i=1}^N \mathrm{Tr}(x_i \bar{y}_i) & d \equiv 2, 3 \bmod 4 \end{cases}.$$

Then the dual of $(\rho^{-1}(C), b_\alpha)$ is given by $(\rho^{-1}(C)^*, b_\alpha)$, where $\rho^{-1}(C)^* := \{\boldsymbol{x} \in K^N : b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}\, \forall \boldsymbol{y} \in \rho^{-1}(C)\}$. We have the following relation between the dual of $(\rho^{-1}(C), b_\alpha)$ and the lattice constructed from the dual of C:

Lemma 5.35. $(\rho^{-1}(C^\perp), b_\alpha) \subseteq (\rho^{-1}(C)^*, b_\alpha)$.

Proof. Take any $\boldsymbol{x} \in \rho^{-1}(C^\perp)$ and $\boldsymbol{y} \in \rho^{-1}(C)$, then

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

which gives $\boldsymbol{x} \cdot \boldsymbol{y} \equiv 0 \bmod \mathfrak{p}$.

As $\mathfrak{p}$ is totally ramified, by the same argument as in Proposition 5.9, $\beta \equiv \bar{\beta} \bmod \mathfrak{p}$ for all $\beta \in \mathcal{O}_K$. Then we can conclude

$$\boldsymbol{x} \cdot \bar{\boldsymbol{y}} \equiv \boldsymbol{x} \cdot \boldsymbol{y} \bmod \mathfrak{p} \Longrightarrow \boldsymbol{x} \cdot \bar{\boldsymbol{y}} \in \mathfrak{p}.$$

As $\mathfrak{p}$ is the only prime above p, we have $\sigma_2(\boldsymbol{x} \cdot \bar{\boldsymbol{y}}) \in \mathfrak{p}$. Hence $\mathrm{Tr}\,(\boldsymbol{x} \cdot \bar{\boldsymbol{y}}) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and

$$b_\alpha(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{N} \mathrm{Tr}\,(\alpha x_i \bar{y}_i) = \mathrm{Tr}\,(\alpha \boldsymbol{x} \cdot \bar{\boldsymbol{y}}) \in \alpha p\mathbb{Z}.$$

In the case $d \equiv 2, 3 \bmod 4$, any element in $\mathcal{O}_K$ has even trace. In conclusion, we have $b_\alpha(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}$ and hence $\rho^{-1}(C^\perp) \subseteq \rho^{-1}(C)^*$ by definition. □

Corollary 5.36. Let C be a self-orthogonal linear code, then $(\rho^{-1}(C), b_\alpha)$ is integral.

Proof. As C is self-orthogonal, we have $C \subseteq C^\perp$. Hence by Lemma 5.35 $\rho^{-1}(C) \subseteq \rho^{-1}(C^\perp) \subseteq \rho^{-1}(C)^*$. □

Example 5.37. Take $d = 3$, $K = \mathbb{Q}\sqrt{-3}$, linear code $C \subseteq \mathbb{F}_3^4$ with generator matrix

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

$(\rho^{-1}(C), b_\alpha)$ is a unimodular lattice of dimension 8 with minimum 2. Thus it is the unique extremal $8-$dimensional unimodular lattice E_8 [19].

Chapter 6

Lattices from LCD Codes

In this chapter we will use the generalized Construction A discussed in Chapter 5 to construct another family of lattices from LCD codes. A linear code is said to have a complementary dual, or to be a linear complementary dual code (LCD) [38], if C meets its dual code $C^\perp$ trivially. Recall that given a linear code C of length n and dimension k, say over the finite field $\mathbb{F}_q$, for q a prime power, $C^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^n,\ \langle \boldsymbol{x}, \boldsymbol{c} \rangle = \sum_i x_i c_i = 0\ \forall \boldsymbol{c} \in C\}$. For example, the $(3, 2)$ binary parity check code is LCD: a generic codeword $\boldsymbol{c}$ is of the form $\boldsymbol{c} = (a_1, a_2, a_1 + a_2)$, $a_1, a_2 \in \mathbb{F}_2$. Its dual $C^\perp$ is the $(3, 1)$ repetition code, and $\langle \boldsymbol{x}, \boldsymbol{c} \rangle = 0$ for $\boldsymbol{x} = (b, b, b)$, $b \in \mathbb{F}_2$. Clearly $C = \{(1, 0, 1), (0, 1, 1), (1, 1, 0), (0, 0, 0)\}$ and $C^\perp = \{(0, 0, 0), (1, 1, 1)\}$ intersect trivially, that is in the whole zero codeword.

LCD codes were introduced by Massey [38], where he proved that asymptotically good LCD codes exist. Furthermore, he showed that LCD codes provide an optimum linear coding solution for the two-user binary adder channel, and he studied the maximum-likelihood decoding problem for LCD codes.

Recently, LCD codes have been proposed to provide counter-measures for side-channel attacks [13]. Constructions of LCD codes over rings have also been provided in [20], together with a linear programming bound on the largest size of an LCD code of given length and minimum distance.

The "continuous" equivalents of linear codes in coding theory are lattices. There are in fact a wealth of connections between linear codes and lattices, in particular via the so-called Constructions A,B,C,D,E [19]. Through these connections, the dual of a linear code is related to that of its corresponding lattice. It is thus natural to wonder how the notion of LCD codes would translate to lattices.

Related works include [55, Method 4], where binary Construction A is considered on

the intersection of binary codes, and [46, Section 82F], where a formula that relates the intersection of two lattices is given. It could be applied to intersect a lattice with its dual, though this does not seem to give insight to our computations so far.

In this section, we attempt to mimic the definition of LCD codes to lattices and report our basic observations in Section 6.1. It turns out that the notion of intersection between a lattice L and its dual L^* is much less natural than that of a linear code C and its dual $C^\perp$. We identified a lattice L_S that belongs to this intersection. We then compute a few lattices obtained from LCD codes via Construction A in Section 6.2. This as expected yields non-integral lattices, and a few interesting examples are reported. Connections between Construction A applied to the intersection of C and its dual and the lattice L_S are discussed in Section 6.3. This rises more generally the question of the lattices obtained as preimage of the intersection of a code and its dual via Construction A, which is discussed in Section 6.4. Finally we give some examples in Section 6.5.

6.1 Basic Observations

If C is a linear code with dual $C^\perp$, then both are vector subspaces and thus they surely must intersect in $\mathbf{0}$. It turns out that there are codes for which C and $C^\perp$ intersect exactly in $\mathbf{0}$. A lattice and its dual both must contain $\mathbf{0}$ too, however, for lattices whose vectors have rational inner products, and integer inner products in particular, it cannot be that only $\mathbf{0}$ is in the intersection, as we will see next.

Let M be a generator matrix for a lattice L in $\mathbb{R}^n$, with rows $v_1, \ldots, v_n$, meaning that the lattice L is generated as integral linear combinations of $v_1, \ldots, v_n$, and let $G = MM^\top$ be the corresponding Gram matrix. Hence

$$L = \{\boldsymbol{x} = \boldsymbol{u}M,\ \boldsymbol{u} \in \mathbb{Z}^n\},$$

and the $i,j-$entry of G is given by $\langle v_i, v_j \rangle = \sum_k v_{ik} v_{jk}$.

Let L^* be the dual lattice of L, that is

$$L^* = \{\boldsymbol{y} \in \mathbb{R}^n,\ \langle \boldsymbol{y}, \boldsymbol{x} \rangle \in \mathbb{Z},\ \forall \boldsymbol{x} \in L\}.$$

It has generator matrix $(M^\top)^{-1} = (M^{-1})^\top$.

Lemma 6.1. If the Gram matrix G of a lattice L has rational entries, then $L \cap L^*$ is a lattice

of dimension n. It contains as sublattice the lattice L_S with generator matrix SM, where S is a diagonal matrix with diagonal $s_1, \ldots, s_n$, and s_i is the least common multiple of the denominators of the entries of the ith row of G, $i = 1, \ldots n$.

Proof. Since the entries of G are rational numbers, let s be the least common multiple of all the denominators of the entries of G. Consider the vector

$$w := sv_1 + sv_2 + \cdots + sv_n,$$

for which we have $\langle w, v_i \rangle \in \mathbb{Z}\ \forall i$. This means $w \in L \cap L^*$.

Actually if we let s_i be the least common multiple of the denominators of the entries of row i of G and let $w_i = s_i v_i$, then $\langle w_i, v_j \rangle = s_i \langle v_i, v_j \rangle \in \mathbb{Z}$ and $w_i \in L \cap L^*$. The vectors $\{w_1, \ldots, w_n\}$ are linearly independent over $\mathbb{R}$, and generates a lattice L_S of dimension n, which is a sublattice of $L \cap L^*$, which is therefore also a lattice of dimension n. □

When the Gram matrix G has integral coefficients, then the lattice L is integral, which is well known [19] to be equivalent to $L \subseteq L^*$. In the above lemma, this corresponds to S being the identity matrix, in which case $L_S = L$ and $L \cap L^* = L$.

Lemma 6.2. Consider the lattice L_S of the previous lemma, with generator matrix SM. Then the index of L_S in L is $|\det(S)|$ and the index of L_S in L^* is $|\det(S)\det(G)|$.

Proof. Since the generator matrix of L_S is SM, we have a readily available expression for the basis vectors of L_S as a function of that of L, and thus the index in L is $|\det(S)|$. Then notice that

$$SM = (SMM^\top)(M^\top)^{-1} = (SG)(M^T)^{-1}$$

thus the index in L^* is $|\det(S)\det(G)|$. □

6.2 Construction A from LCD Codes

We next look at lattices obtained from LCD codes via special cases of the generalized Construction A as discussed in the beginning of Chapter 5 and Section 5.1. More precisely, let K be a Galois number field of degree $[K : \mathbb{Q}] = n$ that is either totally real or a CM field. Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. Then

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f},$$

where $p = \mathfrak{p} \cap \mathbb{Z}$ and f is the inertia degree of p. In this chapter we consider only two cases:

- K is totally real and p is either inert or totally ramified;
- K is a CM field and p is totally ramified.

Take N a positive integer and consider the map

$$\begin{aligned} \rho : \mathcal{O}_K^N &\to \mathbb{F}_{p^f}^N \\ (x_1, \ldots, x_N) &\mapsto (x_1 \bmod \mathfrak{p}, \ldots, x_N \bmod \mathfrak{p}). \end{aligned}$$

Define b to be the bilinear form

$$b : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R},\ (x, y) \mapsto \tfrac{1}{p} \textstyle\sum_{i=1}^N \mathrm{Tr}\left(x_i \bar{y}_i\right),$$

where $\bar{y}_i$ denotes the complex conjugate of y_i if K is CM (and $\bar{y}_i$ is understood to be y_i if K is totally real), i.e. we take $\alpha = \frac{1}{p}$ as in (5.2).

If we take any $C \subseteq \mathbb{F}_{p^f}^N$ a linear code, then the pair $(\rho^{-1}(C), b)$ is a lattice, as shown in Chapter 5. In this chapter, we will denote this lattice by Γ_C.

By Proposition 5.9 from Chapter 5 we know Γ_C is not an integral lattice. We are interested in the intersection between a lattice and its dual, which means here, the intersection of Γ_C and Γ_C^*. When a lattice is integral, some results are known to connect the lattice and its dual. However we are looking at rational lattices here.

We start by noticing connections between Γ_C and $\Gamma_{C^\perp}$.

Lemma 6.3. Let $C \subseteq \mathbb{F}_{p^f}^N$ be a linear code, then

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

Proof. Take $x \in \mathcal{O}_K^N$, then

$$x \in \Gamma_C \cap \Gamma_{C^\perp} \iff \rho(x) \in C \text{ and } \rho(x) \in C^\perp.$$

Moreover,

$$\rho(x) \in C \cap C^\perp \iff x \in \Gamma_{C \cap C^\perp}.$$

□

Example 6.4. If we consider the binary Construction A [19] for C the $(3,2)$ binary parity check code discussed in the introduction of this chapter, we have for generator matrix M_C and Gram matrix G_C of Γ_C respectively

$$M_C = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \; G_C = \begin{bmatrix} 1 & 1/2 & 1 \\ 1/2 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

For $C^\perp$, the $(3,1)$ repetition code, we have

$$M_{C^\perp} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \; G_{C^\perp} = \begin{bmatrix} 3/2 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

Finally, since $C \cap C^\perp = \mathbf{0}$, a generator matrix for $\Gamma_{C\cap C^\perp}$ is $\sqrt{2}I_3$ where I_3 is the 3-dimensional identity matrix.

Furthermore, the dual Γ_C^* of Γ_C has Gram matrix

$$\begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 3/2 \end{bmatrix}.$$

The least common multiple of the denominators of the entries of row i $(1 \leq i \leq 3)$ of G_C are $2, 2, 1$, by Definition of L_S in Lemma 6.1, the lattice L_S for Γ_C has thus generator matrix

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix} = \sqrt{2}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Notice that $L_S = \Gamma_{C\cap C^\perp}$. This is no coincidence, as we will show in Section 6.3.

For $K = \mathbb{Q}(\sqrt{5})$, it is known that a generator matrix of Γ_C is given by

$$M_C = \begin{bmatrix} I_K \otimes M & A\tilde{\otimes}M \\ \mathbf{0}_{2N-2k,2k} & I_{N-k} \otimes pM \end{bmatrix}$$

with

$$M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix},$$

and A such that $[I_k,\ (A \mod p\mathcal{O}_K)]$ is a generator matrix of C. Denoting the columns of M (resp. A) by M_i, $i = 1, 2$ (resp. A_i, $i = 1, \ldots, N-k$), we write $A\tilde{\otimes}M = [\sigma_1(A_1) \otimes M_1, \sigma_2(A_1) \otimes M_2, \ldots, \sigma_1(A_{N-k}) \otimes M_1, \sigma_2(A_{N-k}) \otimes M_2]$, for σ_1, σ_2 the embeddings of $\mathbb{Q}(\sqrt{5})$, applied componentwise.

Example 6.5. Consider $K = \mathbb{Q}(\sqrt{5})$. Take $p = 2$, a prime that is inert in K. Consider the linear code with generator matrix $(1\ \omega)$, where $\mathbb{F}_4 = \mathbb{F}_2(\omega)$. Then Γ_C has generator matrix

$$\begin{aligned} M_C &= \begin{bmatrix} 1 \otimes M & \frac{1+\sqrt{5}}{2} \otimes M_1 \ \frac{1-\sqrt{5}}{2} \otimes M_2 \\ 0 & 2 \otimes M \end{bmatrix} \\ &= \frac{1}{2\sqrt{2}} \begin{bmatrix} 2 & 2 & 1+\sqrt{5} & 1-\sqrt{5} \\ 1+\sqrt{5} & 1-\sqrt{5} & 3+\sqrt{5} & 3-\sqrt{5} \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 2+2\sqrt{5} & 2-2\sqrt{5} \end{bmatrix} \end{aligned}$$

and Gram matrix

$$G_C = \begin{bmatrix} 5/2 & 5/2 & 1 & 3 \\ 5/2 & 5 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 3 & 4 & 2 & 6 \end{bmatrix}$$

We get a lattice with minimum $5/2$, kissing number 8 and discriminant 25. The dual lattice has minimum $\frac{1}{2}$ and kissing number 8 with discriminant $\frac{1}{25}$.

Using $\mathbb{Q}(\sqrt{5})$ and $p = 2$, other lattices can be found as listed in Table 6.1.

6.3 The Lattice $\Gamma_{C \cap C^\perp}$

In this section we focus on the case where K is totally real and p a prime inert in K.

Let $\sigma_1, \ldots, \sigma_n$ be the n real embeddings of K, $\{v_1, \ldots, v_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and set

$$M = \begin{bmatrix} \sigma_1(v_1) & \sigma_2(v_1) & \ldots & \sigma_n(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(v_n) & \sigma_2(v_n) & \ldots & \sigma_n(v_n) \end{bmatrix}. \tag{6.1}$$

A	$\min(\Gamma_C)$	$K(\Gamma_C)$	$\mathrm{disc}\,(\Gamma_C)$
$\begin{bmatrix} 1+w & w \\ 1 & 1+w \end{bmatrix}$	$5/2$	8	5^4
$\begin{bmatrix} 1+w & 0 \\ 0 & 1+w \end{bmatrix}$	$5/2$	16	5^4
$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	2	4	5^4
$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$	2	4	5^6

Table 6.1: Examples of lattices Γ_C, obtained from $\mathbb{Q}(\sqrt{5})$, $p = 2$, C with generator matrix $[I_k\ A]$ over $\mathbb{F}_4 = \mathbb{F}_2(w)$, and their minimum $\min(\Gamma_C)$, kissing number $K(\Gamma_C)$ and discriminant $\mathrm{disc}\,(\Gamma_C)$.

By Proposition 5.3 and Lemma 5.4 from Chapter 5, a generator matrix for Γ_C is given by

$$M_C = \frac{1}{\sqrt{p}} \begin{bmatrix} I_k \otimes M & A\widetilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & pI_{N-k} \otimes M \end{bmatrix}, \tag{6.2}$$

where M was defined in (6.1). A is a matrix such that $[I_k\ (A \bmod \mathfrak{p})]$ is a generator matrix of C. Denote the columns of M, A by $M_i (i = 1, 2, \ldots, n)$, $A_j (j = 1, 2, \ldots, N-k)$, then

$$A\widetilde{\otimes}M := [\sigma_1(A_1) \otimes M_1, \ldots, \sigma_n(A_1) \otimes M_n, \ldots, \sigma_n(A_{N-k}) \otimes M_1, \sigma_n(A_{N-k}) \otimes M_n],$$

here σ_is are applied componentwise. Moreover, the Gram matrix for Γ_C is given by

$$G_C = \begin{bmatrix} \frac{1}{p}\mathrm{Tr}\left((I + AA^\top) \otimes M_1 M_1^\top\right) & \mathrm{Tr}\left(A \otimes M_1 M_1^\top\right) \\ \mathrm{Tr}\left(A \otimes M_1 M_1^\top\right)^\top & I_{N-k} \otimes pMM^\top \end{bmatrix}. \tag{6.3}$$

We have

Proposition 6.6. $\Gamma_C \cap \Gamma_C^* = \Gamma_{C \cap C^\perp}$ and $|\Gamma_C / \Gamma_{C \cap C^\perp}| = p^{nk}$.

Proof. Firstly, if we take any $y \in \Gamma_{C^\perp}$ and $x \in \Gamma_C$, then $\rho(y) \in C^\perp$, $\rho(x) \in C$. We have

$$\rho(y \cdot x) = \rho(y) \cdot \rho(x) = 0 \Longrightarrow y \cdot x \in (p).$$

and hence $\mathrm{Tr}\,(y \cdot x) \in p\mathbb{Z}$, and

$$b(y, x) = \frac{1}{p} \sum_{i=1}^{N} \mathrm{Tr}\,(y_i x_i) = \frac{1}{p} \mathrm{Tr}\,(y \cdot x) \in \mathbb{Z}.$$

We just proved $\Gamma_{C^\perp} \subseteq \Gamma_C^*$. By Lemma 6.3, we have $\Gamma_{C\cap C^\perp} \subseteq \Gamma_C \cap \Gamma_C^*$. Hence $\Gamma_C \cap \Gamma_C^* \neq \Gamma_{C\cap C^\perp}$ if and only if there exists Γ' such that $\Gamma_C \cap \Gamma_C^* \supset \Gamma' \supsetneq \Gamma_{C\cap C^\perp}$. Let Δ be the discriminant of the number field K. From the generator matrices, we can tell that for a linear code C_0 of dimension k_0, the lattice Γ_{C_0} has volume $vol(\Gamma_{C_0}) = \Delta^{\frac{N}{2}} p^{n(N-k)-\frac{nN}{2}}$. Then the quotient group $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ has order [19] $vol(\Gamma_{C\cap C^\perp})/vol(\Gamma_{C^\perp}) = p^{nN-nk}$ and $\Gamma_C^*/\Gamma_{C\cap C^\perp}$ has order $\Delta^N p^{nN-nk}$. As p is inert, we have $p \nmid \Delta$. Thus $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ is the unique Sylow $p-$subgroup of $\Gamma_C^*/\Gamma_{C\cap C^\perp}$ [21]. Then $\Gamma'/\Gamma_{C\cap C^\perp}$, as a $p-$subgroup of $\Gamma_C^*/\Gamma_{C\cap C^\perp}$, is contained in $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ [21], which then implies $\Gamma' \subset \Gamma_C$, a contradiction with our assumption that $\Gamma_{C\cap C^\perp} \subsetneq \Gamma'$. □

Let L_S be the lattice as defined in Section 6.1 for Γ_C, then

Proposition 6.7. $L_S = \Gamma_{C\cap C^\perp}$.

Proof. We know that $L_S \subseteq \Gamma_{C\cap C^\perp} \subseteq \Gamma_C$. It is enough to prove that

$$|\Gamma_C/\Gamma_{C\cap C^\perp}| = |\Gamma_C/L_S|.$$

We just proved $|\Gamma_C/\Gamma_{C\cap C^\perp}| = p^{nk}$. If we examine G_C, as all entries in A, I, M are elements from $\mathcal{O}_K$, thus all the entries of $\mathrm{Tr}\left(A \otimes M_1 M_1^\top\right)$, $\mathrm{Tr}\left(A \otimes M_1 M_1^\top\right)^\top$ and $I_{N-k} \otimes pMM^\top$ are integers.

Also, the entries of $\mathrm{Tr}\left((I + AA^\top) \otimes M_1 M_1^\top\right)$ are integers. We claim that:

For each row of the matrix $GC1 := \mathrm{Tr}\left((I + AA^\top) \otimes M_1 M_1^\top\right)$, there exists at least one entry that is not divisible by p.

As there are exactly nk rows in $GC1$, the definition of L_S implies

$$|\Gamma_C/L_S| = p^{nk} = |\Gamma_C/\Gamma_{C\cap C^\perp}|.$$

proof of claim: Let $\{\boldsymbol{c}_j\}_{1\leq j\leq k}$ be the rows of $[I\ A]$, then each $\rho(\boldsymbol{c}_j)$ is a codeword in C. The jth row of $I + AA^\top$ is given by $[\boldsymbol{c}_j \cdot \boldsymbol{c}_1,\ \boldsymbol{c}_j \cdot \boldsymbol{c}_2,\ \ldots \boldsymbol{c}_j \cdot \boldsymbol{c}_k]$, $(1 \leq j \leq k)$. The ith row of $M_1 M_1^\top$ is given by $[v_i v_1,\ v_i v_2,\ \ldots v_i v_n]$, $(1 \leq i \leq n)$. Thus the first n entries of the ijth row of $GC1$ is given by

$$[\boldsymbol{c}_j \cdot \boldsymbol{c}_1 v_i v_1,\ \boldsymbol{c}_j \cdot \boldsymbol{c}_1 v_i v_2, \ldots \boldsymbol{c}_j \cdot \boldsymbol{c}_1 v_i v_n],\ (1 \leq i \leq n, 1 \leq j \leq k).$$

Suppose there is one row of $GC1$ that consists of only multiples of p, then there exists one

$\boldsymbol{c}_{j_0}$ and one v_{i_0} such that

$$\frac{1}{p}\mathrm{Tr}\left(\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1 v_{i_0} v_k\right)\in\mathbb{Z}\ \forall 1\leq k\leq n.$$

As $\{v_k\}_{1\leq k\leq n}$ is a $\mathbb{Z}-$basis for $\mathcal{O}_K$, this implies

$$\frac{1}{p}\mathrm{Tr}\left(\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1 v_{i_0}\alpha\right)\in\mathbb{Z}\ \forall\alpha\in\mathcal{O}_K.$$

Then we must have

$$\frac{1}{p}\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1 v_{i_0}\in\mathcal{D}_K^{-1}\iff\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1 v_{i_0}\in p\mathcal{D}_K^{-1}.$$

But $\boldsymbol{c}_{j_0},\boldsymbol{c}_1,v_{i_0}\in\mathcal{O}_K$, we have $\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1 v_{i_0}\in(p)$. As $C\cap C^{\perp}=\{\mathbf{0}\}$, $\rho(\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1)\neq 0\implies\boldsymbol{c}_{j_0}\cdot\boldsymbol{c}_1\notin(p)$. This leaves us with the only option that $v_{i_0}\in(p)$. However, then this will imply $v_{i_0}v_k\in(p)$. As p is inert, we have $\mathrm{Tr}\left(v_{i_0}v_k\right)\in p\mathbb{Z}$ for all $1\leq k\leq n$. And hence the discriminant of K, $\det\left(\mathrm{Tr}\left(v_i v_j\right)\right)_{1\leq i,j\leq n}$, is divisible by p, which contradicts with the assumption that p is inert. This proves the claim. □

Example 6.8. The above result is not true in general. For example, if we take $K=\mathbb{Q}(\sqrt{5})$, $p=5$ is totally ramified in K. Consider the linear code $C\subseteq\mathbb{F}_5^2$ with generator matrix $(1\ 1)$. Take $M=\begin{bmatrix}1 & 1\\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2}\end{bmatrix}$, the generator matrix for Γ_C can be obtained as in (6.2):

$$\begin{aligned}M_C &= \frac{1}{\sqrt{5}}\begin{bmatrix}1\otimes M & 1\otimes M\\ 0 & \begin{matrix}\sqrt{5} & \sqrt{5}\\ \frac{\sqrt{5}+5}{2} & \frac{5-\sqrt{5}}{2}.\end{matrix}\end{bmatrix}\\ &= \frac{1}{2\sqrt{5}}\begin{bmatrix}1 & 1 & 1 & 1\\ 1+\sqrt{5} & 1-\sqrt{5} & 1+\sqrt{5} & 1-\sqrt{5}\\ 0 & 0 & 2\sqrt{5} & -2\sqrt{5}\\ 0 & 0 & 5+\sqrt{5} & 5-\sqrt{5}\end{bmatrix}\end{aligned}$$

and Gram matrix is given by

$$G_C=\begin{bmatrix}4/5 & 2/5 & 0 & 1\\ 2/5 & 6/5 & 1 & 1\\ 0 & 1 & 2 & 1\\ 1 & 1 & 1 & 3\end{bmatrix}.$$

This gives L_S with generator matrix

$$\frac{1}{2\sqrt{5}}\begin{bmatrix}5&0&0&0\\0&5&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&1&1&1\\1+\sqrt{5}&1-\sqrt{5}&1+\sqrt{5}&1-\sqrt{5}\\0&0&2\sqrt{5}&-2\sqrt{5}\\0&0&5+\sqrt{5}&5-\sqrt{5}\end{bmatrix}$$
$$=\frac{1}{2\sqrt{5}}\begin{bmatrix}10&10&10&10\\5+5\sqrt{5}&5-5\sqrt{5}&5+5\sqrt{5}&5-5\sqrt{5}\\0&0&2\sqrt{5}&-2\sqrt{5}\\0&0&5+\sqrt{5}&5-\sqrt{5}\end{bmatrix}$$

and Gram matrix

$$G_{LS}=\begin{bmatrix}20&10&0&5\\10&30&5&5\\0&5&2&1\\5&5&1&3\end{bmatrix}.$$

However, $\Gamma_{C\cap C^\perp}$ is the preimage of $\mathbf{0}$, i.e., the lattice $(\mathfrak{p}^N, b)$, which has Gram matrix

$$G_{\Gamma_{C\cap C^\perp}}=\begin{bmatrix}2&1&1&-2\\1&3&3&-1\\1&3&6&-2\\-2&-1&-2&4\end{bmatrix}.$$

In this case $L_S \subsetneq \Gamma_{C\cap C^\perp}$.

The difference of behavior of L_S in that it is either $\Gamma_{C\cap C^\perp} = \Gamma_C \cap \Gamma_C^*$ or it is a sublattice could be a first attempt at defining a "LCD lattice". We next looking at the properties of $\Gamma_{C\cap C^\perp}$ as a modular lattice.

6.4 The Lattice $\Gamma_{C\cap C^\perp}$ as a Modular Lattice

In the last section we proved if K is totally real and $\mathfrak{p}$ is inert $\Gamma_{C\cap C^\perp} = L_S$. In this section, we will look at the relationship between $\Gamma_{C\cap C^\perp}$ and its dual for a more general setting as mentioned in Section 6.2:

- either K is totally real and p is either inert or totally ramified;

- or K is a CM field and p is totally ramified.

Suppose $[K:\mathbb{Q}] = n$. Let Δ denote the absolute value of the discriminant of K. As $C \cap C^{\perp}$ is self-orthogonal, by the construction of the lattice $\Gamma_{C\cap C^{\perp}}$, we have

Lemma 6.9. $\Gamma_{C\cap C^{\perp}} = (\mathfrak{p}^N, b)$ is an integral lattice of dimension nN.

We will use Γ_N to denote the lattice $\Gamma_{C\cap C^{\perp}}$, with N indicating that the dimension is nN. When $N = 1$, we have the *ideal lattice* $(\mathfrak{p}, b)$, which has discriminant $p^{-n}N(\mathfrak{p})^2\Delta = p^{2f-n}\Delta$ [5]. Recall that the discriminant of a lattice is the determinant of its Gram matrix [19]. Thus

Lemma 6.10. Γ_N has discriminant $p^{N(2f-n)}\Delta^N$.

An integral lattice L is said to be an $\ell-$modular lattice, for a positive integer ℓ, if there exists an integral matrix U with determinant ± 1 and a matrix B satisfying $BB^{\top} = I$ such that $\sqrt{\ell}UM^*B = M$, where M, M^* are the generator matrices for L and L^* respectively.

Proposition 6.11. If the lattice Γ_1 is $\ell-$modular, then the lattices Γ_N are $\ell-$modular for all N.

Proof. Let M_p be a generator matrix for Γ_1, then

$$M_{pN} := \begin{bmatrix} M_p & 0 & \dots & 0 \\ 0 & M_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_p \end{bmatrix}$$

is a generator matrix for Γ_N. Moreover, $M_p^* := (M_p^{\top})^{-1}$ is a generator matrix for the dual of Γ_1, Γ_1^*, and

$$M_{pN}^* := \begin{bmatrix} M_p^* & 0 & \dots & 0 \\ 0 & M_p^* & \dots & 0 \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \dots & M_p^* \end{bmatrix}$$

is a generator matrix for Γ_N^*. If Γ_1 is an $\ell-$modular lattice, then there exist U_p, an integral matrix with determinant ± 1, and B_p, a matrix satisfying $B_pB_p^{\top} = I$, such that $\sqrt{\ell}U_pM_p^*B_p =$

M_p. Let

$$U_{pN} := \begin{bmatrix} U_p & 0 & \dots & 0 \\ 0 & U_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & U_p \end{bmatrix}$$

and

$$B_{pN} := \begin{bmatrix} B_p & 0 & \dots & 0 \\ 0 & B_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B_p \end{bmatrix}.$$

Then $\sqrt{\ell}U_{pN}M_{pN}^*B_{pN} = M_{pN}$. We can then conclude Γ_N is $\ell-$modular. □

By Lemma 6.10 and [49], if Γ_N is an $\ell-$modular lattice,

$$p^{N(2f-n)}\Delta^N = \ell^{\frac{nN}{2}} \iff p^{2f-n}\Delta = \ell^{\frac{n}{2}} \iff \Delta = \ell^{\frac{n}{2}}p^{n-2f}.$$

Proposition 6.12. If Γ_N is an $\ell-$modular lattice, then $p|\ell$. If furthermore p is inert, then $p^2||\ell$.

Proof. By the above, we have $\Delta = \ell^{\frac{n}{2}}p^{n-2f}$. If p is inert, $f = n$ and $p \nmid \Delta$, $\Delta = \ell^{\frac{n}{2}}p^{n-2n} = \ell^{\frac{n}{2}}p^{-n}$. As Δ is an integer, we must have $p^2||\ell$.

If p is totally ramified, $f = 1$ and $\Delta = \ell^{\frac{n}{2}}p^{n-2}$. Suppose $(\ell, p) = 1$. Recall that $|N(\mathcal{D}_K)| = \Delta$, $N(\mathfrak{p}) = p^f = p$. Then we have $\mathfrak{p}^{n-2}||\mathcal{D}_K$. By [42], if p is tamely ramified, $\mathfrak{p}^{n-1}||\mathcal{D}_K$ and if p is widely ramified, $\mathfrak{p}^n|\mathcal{D}_K$. Thus $\mathfrak{p}^{n-2}||\mathcal{D}_K$ is impossible. □

Now we consider the special case when $\ell = p$.

By Proposition 6.12, we can assume p is totally ramified. If Γ_N is $p-$modular,

$$\Delta = p^{\frac{n}{2}}p^{n-2} = p^{\frac{3n}{2}-2}$$

and p is the only prime that ramifies in K.

Let s be the integer that $\mathcal{D}_K = \mathfrak{p}^s$, then

$$N(\mathfrak{p}^s) = p^s = p^{\frac{3n}{2}-2} \implies s = \frac{3n}{2} - 2.$$

Proposition 6.13. If $p \neq 2$ is tamely ramified, Γ_N is $p-$modular if and only if

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \bmod 4 \end{cases}$$

Proof. If p is tamely ramified, we have $\frac{3n}{2} - 2 = n - 1$, i.e., $n = 2$. Then K is a quadratic number field with absolute value of discriminant equal to p, hence the conclusion.

Conversely, let $p \equiv 2, 3 \bmod 4$ and $K = \mathbb{Q}(\sqrt{p})$. Then $\Gamma_1 = (\mathfrak{p}, b) = (\sqrt{p}, b)$ and Γ_1^* is $(\mathfrak{p}^*, b)$, where [5]

$$\mathfrak{p}^* = p\mathcal{D}_K^{-1}\mathfrak{p}^{-1} = \mathfrak{p}^2\mathfrak{p}^{-1}\mathfrak{p}^{-1} = \mathcal{O}_K.$$

Consider the map

$$\begin{aligned} \varphi : \mathfrak{p}^* &\to \mathfrak{p} \\ x &\mapsto \sqrt{p}x, \end{aligned}$$

then φ is a bijective $\mathbb{Z}-$module homomorphism, and hence a $\mathbb{Z}-$ isomophism. Moreover,

$$b(\varphi(x), \varphi(y)) = b(\sqrt{p}x, \sqrt{p}y) = \frac{1}{p}\mathrm{Tr}\left(\sqrt{p}x\sqrt{p}y\right) = pb(x, y).$$

Thus $(\mathfrak{p}^*, pb) \cong (\mathfrak{p}, b)$ as lattices and $(\mathfrak{p}, b)$ is a $p-$modular lattice. By Proposition 6.11, the lattices Γ_N are $p-$modular for all N.

Now let $p \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{-p})$. Then $\Gamma_1 = (\mathfrak{p}, b) = (\sqrt{-p}, b)$ and the dual of Γ_1 is $(\mathfrak{p}^*, b)$, where

$$\mathfrak{p}^* = p\mathcal{D}_K^{-1}\mathfrak{p}^{-1} = \mathfrak{p}^2\mathfrak{p}^{-1}\mathfrak{p}^{-1} = \mathcal{O}_K.$$

Then by the same argument as above Γ_1 is $p-$modular.

By Proposition 6.11, the lattices Γ_N are $p-$modular for all N. □

6.5 Examples

As before, take K a totally real number field with $\mathfrak{p}$ inert or totally ramified, or K a CM field with $\mathfrak{p}$ totally ramified. Let f be the inertia degree of $p = \mathfrak{p} \cap \mathbb{Z}$. By [20], a linear code C over a finite field is an LCD code if and only if its generator matrix G satisfies $\det\left(GG^\top\right) \neq 0$.

To construct the examples, we find some matrices A such that $G = [I \ (A \bmod \mathfrak{p})]$ satisfies $\det\left(GG^\top\right) \neq 0$.

By Lemma 5.1 from Chapter 5, Γ_C has dimension nN, discriminant $\Delta^N p^{2f(N-k)-nN}$. By Lemma 6.10 and Lemma 6.9, $\Gamma_{C\cap C^\perp}$ is an integral lattice with dimension nN and discriminant $\Delta^N p^{2fN-nN}$.

6.5.1 Extremal $3-$modular Lattices

We first give two constructions that result in extremal $3-$modular lattices. From Definition 2.11, a $6-$ or $8-$dimensional even $3-$modular lattice is extremal if its minimum is equal to 2. For the construction, we made use of Proposition 6.13:

Example 6.14. 1. Let $K = \mathbb{Q}(\sqrt{-3})$, $p = 3$, $k = 2$, $N = 3$, $A = (0\ 1)^\top$. Then Γ_C has discriminant 3^{-1}, minimum $\frac{2}{3}$ and kissing number 6. $\Gamma_{C\cap C^\perp}$ is a $6-$dimensional extremal 3-modular even lattice with discriminant 3^3, minimum 2 and kissing number 18.

2. Let $K = \mathbb{Q}(\sqrt{-3})$, $p = 3$, $k = 1$, $N = 4$, $A = (1\ 1\ 1)^\top$. Then Γ_C has discriminant 3^2, minimum 2 and kissing number 24. $\Gamma_{C\cap C^\perp}$ is a $8-$dimensional extremal 3-modular even lattice with discriminant 3^4, minimum 2 and kissing number 24.

6.5.2 K Totally Real Quadratic Number Field, p Inert

When $K = \mathbb{Q}(\sqrt{d})$, $(d > 0)$ is a totally real quadratic field and p an inert prime in K, $\mathcal{O}_K/(p) \cong \mathbb{F}_{p^2}$. $f = 2, n = 2$, hence Γ_C has discriminant $\Delta^N p^{2N-4k}$. $\Gamma_{C\cap C^\perp}$ has discriminant $\Delta^N p^{2N}$. Both lattices have dimension $2N$.

In Table 6.2 we list some examples of lattices Γ_C with discriminant $\operatorname{disc}(\Gamma_C)$ minimum $\min(\Gamma_C)$ kissing number $K(\Gamma_C)$ and the corresponding lattice $\Gamma_{C\cap C^\perp}$ with discriminant $\operatorname{disc}(\Gamma_{C\cap C^\perp})$ minimum $\min(\Gamma_{C\cap C^\perp})$ kissing number $K(\Gamma_{C\cap C^\perp})$. Where ω is such that $\mathbb{F}_{p^2} = \mathbb{F}_p(\omega)$.

Dim	d	p	A	$\operatorname{disc}(\Gamma_C)$	$\min(\Gamma_C)$	$K(\Gamma_C)$	$\operatorname{disc}(\Gamma_{C\cap C^\perp})$	$\min(\Gamma_{C\cap C^\perp})$	$K(\Gamma_{C\cap C^\perp})$
4	5	2	(0)	5^2	1	2	$5^2\cdot 2^4$	4	4
4	7	5	(4)	28^2	4/5	2	$28^2\cdot 5^4$	10	4
4	21	2	(0)	21^2	1	2	$21^2\cdot 2^4$	4	4
6	5	2	$(1\ 1)$	$5^3\cdot 2^2$	3	8	$5^3\cdot 2^6$	4	6
6	3	5	$(2\ 1)^\top$	$12^3\cdot 5^{-2}$	4/5	2	$12^3\cdot 5^6$	10	6
6	7	5	$(1\ 1)$	$28^3\cdot 5^2$	6/5	2	$28^3\cdot 5^6$	10	6
8	5	2	$\begin{bmatrix}1+\omega & 0\\ 0 & 1+\omega\end{bmatrix}$	5^4	5/2	16	$5^4\cdot 2^8$	4	8
8	3	5	$\begin{bmatrix}\omega & 4\omega+2\\ \omega+3 & \omega+2\end{bmatrix}$	12^4	18/5	2	$12^4\cdot 5^8$	4	8
12	5	2	$\begin{bmatrix}1 & 1 & 0\\ 1 & 1 & 0\\ 1 & 0 & 1\end{bmatrix}$	5^6	2	4	$5^6\cdot 2^{12}$	4	12

Table 6.2: Examples of lattices Γ_C and $\Gamma_{C\cap C^\perp}$ obtained from $\mathbb{Q}(\sqrt{d})$, p inert and C with generator matrix $[I_k\ A]$.

6.5.3 K Totally Real Quadratic Field, $\mathfrak{p}$ Totally Ramified

When $K = \mathbb{Q}(\sqrt{d}),\ (d > 0)$ is a totally real quadratic field and $\mathfrak{p}$ totally ramified in K, $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. $f = 1, n = 2$, hence Γ_C has discriminant $\Delta^N p^{-2k}$. $\Gamma_{C\cap C^\perp}$ has discriminant Δ^N. Both lattices have dimension $2N$.

Recall that p is totally ramified in K if and only if $p|d$ or $p = 2$ and $d \equiv 2, 3 \bmod 4$.

We consider $p \neq 2$, as $n = 2$, p is tamely ramified. By Proposition 6.13, $\Gamma_{C\cap C^\perp}$ is a $p-$modular lattice if and only if $p \equiv 1 \bmod 4$ and $d = p$. Examples for $\Gamma_{C\cap C^\perp}$ not a modular lattice can be found in Table 6.3. And in Table 6.4 we list some examples where $\Gamma_{C\cap C^\perp}$ are $5-$modular lattices.

Dim	d	p	A	disc (Γ_C)	min(Γ_C)	$K(\Gamma_C)$	disc $(\Gamma_{C\cap C^\perp})$	min$(\Gamma_{C\cap C^\perp})$	$K(\Gamma_{C\cap C^\perp})$
6	3	3	$(1\,0)^\top$	$2^6 \cdot 3^{-1}$	$2/3$	2	12^3	2	6
10	7	7	$(1\,1\,1\,1)$	$2^{10} \cdot 7^3$	$10/7$	2	28^5	2	10
12	11	11	$\begin{bmatrix}1 & 1\\ 1 & 1\\ 1 & 1\end{bmatrix}$	$2^{12} \cdot 11^{-2}$	$4/11$	12	$2^{12} \cdot 11^6$	2	12

Table 6.3: Examples of lattices Γ_C and $\Gamma_{C\cap C^\perp}$ obtained from $\mathbb{Q}(\sqrt{d})$, p ramified and C with generator matrix $[I_k\ A]$.

Dim	A	disc (Γ_C)	min(Γ_C)	$K(\Gamma_C)$	disc $(\Gamma_{C\cap C^\perp})$	min$(\Gamma_{C\cap C^\perp})$	$K(\Gamma_{C\cap C^\perp})$
6	$(1\ 1)$	5	$6/5$	2	5^3	2	6
10	$\begin{bmatrix}1 & 1\\ 1 & 1\\ 1 & 1\end{bmatrix}$	5^{-1}	$4/5$	6	5^5	2	10
12	$\begin{bmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$	1	$4/5$	2	5^6	2	12

Table 6.4: Examples of lattices Γ_C and $\Gamma_{C\cap C^\perp}$ obtained from $\mathbb{Q}(\sqrt{5})$, $p = 5$ and C with generator matrix $[I_k\ A]$ such that $\Gamma_{C\cap C^\perp}$ is a $5-$modular lattice.

6.5.4 K Imaginary Quadratic Number Field, $\mathfrak{p}$ Totally Ramified

When $K = \mathbb{Q}(\sqrt{d}),\ (d < 0)$ is an imaginary quadratic field and $\mathfrak{p}$ totally ramified in K, $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. $f = 1, n = 2$, hence Γ_C has discriminant $\Delta^N p^{-2k}$, $\Gamma_{C\cap C^\perp}$ has discriminant Δ^N and both lattices have dimension $2N$.

We consider $p \neq 2$, as $n = 2$, p is tamely ramified. By Proposition 6.13, $\Gamma_{C\cap C^\perp}$ is a $p-$modular lattice if and only if $p \equiv 3 \bmod 4$ and $d = -p$. Examples for $\Gamma_{C\cap C^\perp}$ not a modular lattice can be found in Table 6.5, where we take the number field $K = \mathbb{Q}(\sqrt{-5})$ and $p = 5$. And in Table 6.6 we list some examples where $\Gamma_{C\cap C^\perp}$ are $3-$modular lattices.

Dim	A	$\operatorname{disc}(\Gamma_C)$	$\min(\Gamma_C)$	$K(\Gamma_C)$	$\operatorname{disc}(\Gamma_{C\cap C^\perp})$	$\min(\Gamma_{C\cap C^\perp})$	$K(\Gamma_{C\cap C^\perp})$
6	$(1\ 1)$	$2^6\cdot 5$	$6/5$	2	$2^6\cdot 5^3$	2	6
8	$(1\ 1)$	2^8	$6/5$	4	$2^8\cdot 5^4$	2	8
12	$\begin{bmatrix}1&1&1\\1&1&2\\1&1&1\end{bmatrix}$	2^{12}	$4/5$	2	$2^{12}\cdot 5^6$	2	12
16	$\begin{bmatrix}1&1&1\\1&1&2\\1&1&1\\1&1&1\\1&1&1\end{bmatrix}$	$2^{16}\cdot 5^{-2}$	$4/5$	12	$2^{16}\cdot 5^8$	2	16

Table 6.5: Examples of lattices Γ_C and $\Gamma_{C\cap C^\perp}$ obtained from $\mathbb{Q}(\sqrt{-5})$, $p=5$ and C with generator matrix $[I_k\ A]$.

Dim	A	$\operatorname{disc}(\Gamma_C)$	$\min(\Gamma_C)$	$K(\Gamma_C)$	$\operatorname{disc}(\Gamma_{C\cap C^\perp})$	$\min(\Gamma_{C\cap C^\perp})$	$K(\Gamma_{C\cap C^\perp})$
12	$\begin{bmatrix}1&1&1&0\\0&1&0&1\end{bmatrix}$	3^2	2	90	3^6	2	36
16	$\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\1&1&1&1&1\end{bmatrix}$	3^2	2	102	3^8	2	48

Table 6.6: Examples of lattices Γ_C and $\Gamma_{C\cap C^\perp}$ obtained from $\mathbb{Q}(\sqrt{-3})$, $p=3$ and C with generator matrix $[I_k\ A]$ such that $\Gamma_{C\cap C^\perp}$ is a $3-$modular lattice.

6.5.5 K Cyclotomic Field, $\mathfrak{p}$ Totally Ramified

Let $K=\mathbb{Q}(\zeta_{p^r})$, where p is a prime and r is a positive integer. Then K is CM and the only prime that is totally ramified is p. We consider $\mathfrak{p}$, the prime ideal above p. Now $f=1, n=\varphi(p^r)=p^{r-1}(p-1)$, where φ is the Euler function. Then Γ_C has discriminant $\Delta^N p^{2(N-k)-nN}$, $\Gamma_{C\cap C^\perp}$ has discriminant $\Delta^N p^{2N-nN}$ and both lattices have dimension nN.

Example 6.15. Let $p=5,\ r=1,\ k=2,\ N=3,\ A=(1\ 3)^\top$. Then Γ_C has discriminant 5^{-1}, minimum $\frac{8}{5}$ and kissing number 50. $\Gamma_{C\cap C^\perp}$ is a $12-$dimensional even lattice with discriminant 5^3, minimum 2 and kissing number 60.

Example 6.16. Then Γ_C has discriminant 7, minimum 2 and kissing number 126. $\Gamma_{C\cap C^\perp}$ is a $18-$dimensional even lattice with discriminant 7^3, minimum 2 and kissing number 126.

Chapter 7

Conclusion and Future Work

The thesis was dedicated to the construction of modular lattices. Three methods were discussed: construction from number fields, construction from quaternion algebras and construction from linear codes via generalized Construction A over number fields.

Our starting point was the construction of Arakelov-modular lattices proposed in [6]. We generalized this construction to other CM fields as well as totally real number fields. The main results include:

- Characterization of Arakelov-modular lattices of trace type over quadratic number fields;
- Characterization of Arakelov-modular lattices of trace type over maximal real subfields of cyclotomic fields of the form $\mathbb{Q}(n)$, where n is not a prime power;
- Characterization of Arakelov-modular lattices over maximal real subfields of cyclotomic fields of the form $\mathbb{Q}(p^r)$ for p an odd prime;
- Characterization of Arakelov-modular lattices over totally real Galois fields with odd degrees.

The definition of Arakelov-modular lattices is also generalized to totally definite quaternion algebras over a number field K. The main contributions are:

- Characterization and classification of Arakelov-modular lattices of level ℓ for ℓ a prime when $K = \mathbb{Q}$;
- Necessary and sufficient conditions for the existence of Arakelov-modular lattices when K is the maximal real subfield of a cyclotomic field and has odd degree.

- Existence conditions of Arakelov-modular lattices when K is a totally real quadratic field or a maximal real subfield of a cyclotomic field that has even degree.

The third method discussed is a generalized Construction A over number fields, which constructs modular lattices over a number field K using linear codes. We have done the following:

- Compute the generator and Gram matrices for the generic case of constructing over both totally real number fields and CM fields;
- Prove the modularity of the lattices obtained from generalized Construction A when K is a quadratic number field;
- Construct examples of lattices and compute their kissing numbers and minimal norms.

Furthermore, using the above generalized Construction A, we construct lattices from LCD (linear complementary dual) code and study the relationship between such a lattice and its dual.

The results in this thesis leave several open questions, for example:

- Characterization of Arakelov-modular lattices over Galois fields with even degree;
- Characterization of Arakelov-modular lattices from totally definite quaternion algebras over higher degree number fields;
- Study the modularity of lattices obtained from generalized Construction A over number fields K with degree bigger than 2;
- A proper definition of "LCD" lattice and the characterization of such lattices.

Bibliography

[1] C.C. Adams and R. D. Franzosa, "Introduction to topology: pure and applied", *Upper Saddle River: Pearson Prentice Hall*, 2008.

[2] C. Bachoc, "Applications of coding theory to the construction of modular lattices", *Journal of Combinatorial Theory*, **78** (1997), 92–119.

[3] C. Batut, H.-G. Quebbemann and R. Scharlau, "Computations of cyclotomic lattices", *Experimental Mathematics*, **4** (1995), 175–179.

[4] E. Bayer-Fluckiger, "Definite unimodular lattices having an automorphism of given characteristic polynomial", *Commentarii Mathematici Helvetici*, **59** (1984), 509–538.

[5] E. Bayer-Fluckiger, "Ideal Lattices", A Panorama of Number Theory or The View from Bakers Garden, edited by Gisbert Wustholz Cambridge Univ. Press, Cambridge (2002), 168–184.

[6] E. Bayer-Fluckiger and I. Suarez, "Modular lattices over Cyclotomic Fields", *Journal of Number Theory*, **114** (2005), 394–411.

[7] G. Berhuy, "Réalisation de formes $\mathbb{Z}$-bilinéaires symétriques comme formes trace hermitiennes amplifiées", *Journal de théorie des nombres de Bordeaux*, **12** (2000), 25–36.

[8] S. Berman (Ed), "Vertex operator algebras in mathematics and physics", *American Mathematical Soc.*, 2003.

[9] D.J. Bernstein, J. Buchmann, and E. Dahmen, "Post-quantum cryptography", *Springer Science & Business Media*, 2009.

[10] S. Böcherer and G. Nebe, "On theta series attached to maximal lattices and their adjoints", *J.Ramanujan Math. Soc.*, **3** (2009), 265–284.

[11] R. Brusamarello, I. Dias, and A. Paques, "On scaled trace forms over commutative rings", *East-West Journal of Mathematics*, **8** (2006).

[12] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, **24** (1997), 235–265.

[13] C. Carlet and S. Guilley, "Complementary Dual Codes for Counter-Measures to Side-Channel Attacks", *Coding Theory and Applications, Springer International Publishing*, **3** (2015), 97–105.

[14] M. Craig, "Extreme forms and cyclotomy", *Mathematika*, **25** (1978), 44–56.

[15] M. Craig, "A cyclotomic construction for Leech's lattice", *Mathematika*, **25** (1978), 236–241.

[16] M. Craig, "Automorphisms of prime cyclotomic lattices", preprint.

[17] R. Chapman, S.T. Dougherty, P. Gaborit and P. Solé, "2-modular lattices from ternary codes", *Journal De Théorie Des Nombres De Bordeaux*, **14** (2002), 73–85.

[18] K.S. Chua and P. Solé, "Eisenstein lattices, Galois rings, and Theta Series", *European Journal of Combinatorics*, **25** (2004), 179–185.

[19] J.H. Conway and N.J.A. Sloane, "Sphere packings, lattices and groups", *Springer*, New York, 1988.

[20] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé, "The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices", preprint, arXiv:1506.01955 (2015).

[21] D. Dummit and R. Foote, "Abstract Algebra Third edition", *John Wiley and Sons, Inc.*, Hoboken, 2004.

[22] W. Ebeling, "Lattices and codes: a course partially based on lecturers by F. Hirzebruch Advanced Lectures in Mathematics", *Springer*, Germany, 2013.

[23] A.-M. Ernvall-Hytönen, "On a conjecture by Belfiore and Solé on some lattices", *IEEE Transactions on Information Theory*, **58** (2012), 5950–5955.

[24] W. Feit, "On integral representations of finite groups", *Proceedings of the London Mathematical Society*, **3** (1974), 633–683.

[25] W. Feit, "Some lattices over $\mathbb{Q}\sqrt{-3}$", *Journal of Algebra* **52** (1978), 248–263.

[26] G.D. Forney, "Coset codes-Part I: Introduction and geometrical classification", *IEEE Trans. Inform. Theory*, **34** (1988), 1123–1151.

[27] G.H. Hardy and E,M, Wright, "An introduction to the theory of numbers", *Oxford University Press*, 1938.

[28] D.W. Lewis, "Scaled trace forms of central simple algebras", *Bull. Belg. Math. Soc. Simon Stevin*, **3** (1996), 281–294.

[29] S.N. Litsin and M. A. Tsfasman, "Algebraic-geometric and number-theoretic packings of spheres", *Uspekhi Mat. Nauk*, **40** (1985), 185–186.

[30] W. Kositwattanarerk, S.S. Ong and F. Oggier, "Construction a of lattices over number fields and block fading wiretap coding", *IEEE Transactions on Information Theory*, **61** (2015), 2273–2282.

[31] S.K. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wire-tap channel", *Information Theory IEEE Transactions on*, **24** (1978), 451–456.

[32] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions", *IEEE Trans. Inf. Theory*, **59** (2013), 3295–3303.

[33] F. Lin, F. Oggier and P. Solé, "2- and 3-modular lattice wiretap codes in small dimensions", *Applicable Algebra in Engineering, Communication and Computing*, **26** (2015), 571–590.

[34] S. Ling, C. Xing, "Coding theory: a first course", *Cambridge University Press*, 2004.

[35] C. Maclachlan and A.W. Reid, "The arithmetic of hyperbolic 3-manifolds", Graduate Text in Math., *Springer-Verlag*, Berlin, 2003.

[36] C.L. Mallows, A.M. Odlyzko and N.J.A. Sloane, "Upper bounds for modular forms, lattices and codes", *J. Algebra*, **36** (1975), 68–76.

[37] J. Martinet, "Perfect lattices in Euclidean spaces", *Springer Science & Business Media*, 2013.

[38] J.L. Massey, "Linear codes with complementary duals", *Discrete Mathematics*, **106** (1992), 337–342.

[39] G. Nebe, "Finite subgroups of $\mathrm{GL}_{24}(\mathbb{Q})$", *Experimental Mathematics*, **5** (1996), 163–195.

[40] G. Nebe, "Finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ for $25 \leq n \leq 31$", *Commun. Algeb.*, 24 (1996), 2341–2397.

[41] G. Nebe and K. Schindelar, "S-extremal strongly modular lattices", *Journal de théorie des nombres de Bordeaux*, **19** (2007), 683–701.

[42] J. Neukirch, "Algebraic Number Theory", *Springer-Verlag*, New York, 1999.

[43] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels", *Foundations and Trends in Communications and Information Theory*, **1** (2004), 333–415.

[44] F. Oggier, J.-C. Belfiore and P. Soleé, "Lattice codes for the wiretap Gaussian channel: Construction and analysis", *IEEE Transactions on Information Theory*, **62** (2016), 5690–5708.

[45] F. Oggier and J.-C. Belfiore, "Enabling multiplication in lattice codes via Construction A", in the proceedings of *the IEEE Information Theory Workshop 2013 (ITW)*, IEEE, 2013.

[46] O. T. OMeara, "Introduction to quadratic forms", *Springer Verlag*, 1971.

[47] J. Pinchak and B.A. Sethuraman, "The Belfiore-Solé Conjecture and a certain technique for verifying it for a given lattice", *Information Theory and Applications Workshop (ITA)*, (2014), 1–3.

[48] H.-G. Quebbemann, "A construction of integral lattices", *Mathematika*, **31** (1984), 137–140.

[49] H.-G. Quebbemann, "Modular lattices in Euclidean Spaces", *Journal of Number Theory*, **54** (1995), 190–202.

[50] H.-G. Quebbemann, "Atkin-Lehner eigenforms and strongly modular lattices", *L'Enseign. Math.*, **43** (1997), 55–65.

[51] E. Rains and N.J.A.Sloane, "The shadow theory of modular and unimodular lattices", *Journal of Number Theory*, **73** (1999), 359–389.

[52] I. Reiner, "Maximal orders", *Academic Press*, New York, 1975.

[53] J-P. Serre, "Local fields", *Springer Science & Business Media*, New York, 1979.

[54] N.J.A. Sloane, "Codes over GF(4) and complex lattices", *Journal of Algebra*, **52** (1978), 168–181.

[55] N. J. A. Sloane and B. Beferull-lozano, "Quantizing using lattice intersections", *Journal of Discrete and Computational Geometry*, 2003, 799–824.

[56] N. J. A. Sloane and G. Nebe, "Catalogue of Lattices", published electronically at http://www.research.att.com/njas/lattices/.

[57] C.G. Lekkerkerker, "Geometry of Numbers", *Elsevier*, Amsterdam, 1969

[58] R. Scharlau and R. Schulze-Pillot, "Extremal lattices", *Algorithmic algebra and number theory*, Springer Berlin Heidelberg (1999), 139–170.

[59] H.P.F. Swinnerton-Dyer, "A brief guide to Algebraic Number Theory", *Cambridge University Press*, 2001.

[60] O. Taussky, "Introduction into connections between algebraic number theory and integral matrices", Appendix 2 to H. Cohn "A classical invitation to algebraic numbers and class fields, 2nd printing", *Springer*, (1988), 305–21.

[61] M-F Vigneras, "The arithmetic of quaternion algebras", preprint (2006).

[62] L. Washington, "Introduction to Cyclotomic Fields", *Springer-Verlag*, Berlin, 1982.

[63] A.D. Wyner, "The wiretap channel", *Bell Syst. Tech. J.*, **54** (1975), 1355–1387.

[64] R. Zamir, "Lattices are everywhere", *Proc. 4th Ann. Workshop on Inf. Theory and Its Appl.*, (ITA 2009), 392–421.

[65] SageMath, the Sage Mathematics Software System (Version 7.1), The Sage Developers, 2016, http://www.sagemath.org.