UNIVERSITY OF SOUTHAMPTON

Faculty of Social and Human Sciences

School of Mathematics

Performance of Codes Based on Crossed Product Algebras

by

Richard Paul Slessor

Thesis for the degree of Doctor of Philosophy

May 2011

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF SOCIAL AND HUMAN SCIENCES

SCHOOL OF MATHEMATICS

Doctor of Philosophy

PERFORMANCE OF CODES BASED ON CROSSED PRODUCT ALGEBRAS

by Richard Paul Slessor

The work presented in this thesis is concerned with algebraic coding theory, with a particular focus on space-time codes constructed from crossed product algebras. This thesis is divided into three parts. In the first part we will present a method for constructing codes from crossed product algebras and derive bounds on their performance. The second part concerns itself with codes constructed from cyclic algebras. Finally in the third part, constructions based on biquadratic crossed product algebras are considered.

It is well known that two important design criteria in the construction of space-time codes are the rank criterion and the determinant criterion. The rank criterion is closely linked to the notion of fully diverse codes. Constructing codes that are fully diverse led to the study of codes based on division algebras. To give explicit constructions of codes, central simple algebras were considered and in particular crossed product algebras. In this thesis we derive bounds on the minimum determinant of codes constructed from crossed product algebras.

A lot of work has focused on constructing codes based on cyclic division algebras. The well known perfect space-time block codes are codes that satisfy a variety of coding constraints that make them very efficient for coding. We consider the performance of these codes and prove that the best known examples are optimal with respect to the coding gain.

Finally we consider codes based on biquadratic crossed product algebras, where the Galois group of the underlying field extension is isomorphic to the Klein four-group. It has been shown that these codes can satisfy a large number of coding criteria and exhibit very good performance. We prove the optimality of the best known code.

Contents

List of Figures

Acknowledgements

First and foremost, my biggest thanks has to go to Grégory Berhuy for all his guidance in supervising my research. Furthermore, for giving up so much of his time to answer my naïve questions and make me feel welcome during my visits to Grenoble. I would also like to thank my supervisor Gareth Jones and my advisor Bernhard Koeck for all their support and encouragement. I am particularly grateful to Frédérique Oggier for all her advice and for her help with my talk at the GTEM summer school at EPFL. My thanks also goes to Brita Nucinkis for some much appreciated words of encouragement.

The last few years wouldn't have been the same without all the post-grads at the University of Southampton and I would like to take this opportunity to thank all of you for making it so enjoyable. In particular to all the post-grads who started at the same time as me, it was a great three years and I particularly like the social side of it. I would also like to thank SUBC for some fantastic memories throughout my time at Southampton. Finally I would like to thank my family and friends, especially my housemate, for all their support and reassurance. This definitely wouldn't have been finished without you.

Introduction

Due to the rise in use of wireless communication, there has been a great deal of interest in investigating how the amount of information transmitted can be increased. Following the work in [13], [14], [42] and [43], a lot of research has considered **MIMO** (multiple-input multiple-output) communication, since it is shown that MIMO systems can be used to increase the amount of transmitted information.

The design criteria of MIMO codes with perfect channel state information (CSI) that was established in [14] led to the development of **space-time codes**[42], specifically **space-time trellis codes** (STTCs). In this thesis we will be concerned with another class of space-time codes called **space-time block codes** (STBCs) [41]. A STBC $\mathcal{C}$ consists of a set of $n_t \times T$ matrices with entries in $\mathbb{C}$.

In [42] a bound on the pairwise probability of error of a space-time code is derived, i.e. a bound on the probability of receiving a message and decoding it incorrectly. Obviously for an efficient code we would like the probability of an error occurring to be as small as possible. This bound led the authors to develop two design criteria: the **rank criterion** and the **determinant criterion**. The rank criterion states that in order to maximise the **diversity gain** we require the difference of any two distinct matrices $X, X' \in \mathcal{C}$ to be full rank. A code satisfying this property is called **fully diverse**. Once the rank criterion has been satisfied, the determinant criterion states that in order to maximise the **coding gain**, the determinant of $(X - X')\overline{(X - X')}^t$, taken over all pairs of distinct codewords in $\mathcal{C}$, must be maximised.

Finding codes that are fully diverse led to an interest in constructing codes from division algebras [34], in particular cyclic division algebras. This work generated a lot of interest and in [37] constructions of codes based on crossed product algebras were given. An approach based on cyclic division algebras, which differs from

[34] was given in [29]. This paper introduced **perfect space-time block codes** (PSTBCs). These codes satisfy a large number of properties including an energy constraint that is related to the cubic lattice $\mathbb{Z}^n$. In [29] the authors give examples of perfect codes in dimensions $2, 3, 4$ and 6.

In [5] it is shown that PSTBCs only exist in these dimensions, although by relaxing the definition slightly PSTBCs can exist for any number of antennas [11]. We will largely be interested in the former case. The optimality of perfect codes has been studied and in [27] it is shown that the golden code, a PSTBC of dimension 2 presented in [3], is optimal with respect to the coding gain.

Codes from non-cyclic division algebras that satisfy a variety of coding constraints including the energy constraint have also been investigated. In [4] the authors consider biquadratic crossed product algebras and construct a code with good performance in dimension 4.

We would like now to introduce the MIMO transmission system and certain important aspects of wireless communication. Following this we will briefly discuss the pairwise probability of error discussed above.

The Transmission Scheme

Modelling the Communication Channel

The basic structure of a MIMO system is as follows: encoded signals are transmitted from n_t transmit antennas and then received by n_r receive antennas. However the transmission is not flawless. The signals are attenuated due to various obstacles in the channel environment. Furthermore a signal can be reflected several times before reaching its destination, as well as being interfered by (and interfering with) other signals. This effect on the signal is known as **fading**. In addition, the **noise** in the environment must also be considered.

Let x_{it} represent the complex signal transmitted by the i^{th} antenna at time t and let y_{jt} represent the signal received by the j^{th} antenna at time t. Also denote by h_{ji} the fading from the i^{th} transmit antenna to the j^{th} receive antenna and let v_{jt} denote the noise at the j^{th} receive antenna at time t. All of these coefficients are assumed to be complex.

Consider the case of two transmit antennas and two receive antennas. This can

be modelled as follows:

$$y_{1t} = h_{11}x_{1t} + h_{12}x_{2t} + v_{1t}$$
$$y_{2t} = h_{21}x_{1t} + h_{22}x_{2t} + v_{2t}$$

Note that the fading coefficients h_{ji} are approximated to be constant over some period of time. We are able to do this, as it is reasonable to assume that there is a time interval T during which the channel remains constant. This period T is called the **coherence interval**.

Consider the case above of two transmit antennas and two receive antennas with a coherence interval $T = 2$. The first antenna receives consecutively a signal which is the sum of two transmitted signals with fading and some noise:

$$y_{11} = h_{11}x_{11} + h_{12}x_{21} + v_{11}$$
$$y_{12} = h_{11}x_{12} + h_{12}x_{22} + v_{12}$$

Similarly, the second antenna receives

$$y_{21} = h_{11}x_{12} + h_{12}x_{22} + v_{21}$$
$$y_{22} = h_{21}x_{12} + h_{22}x_{22} + v_{22}$$

The above equations can be written as the matrix equation

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \cdot \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} + \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \quad (1)$$

It is easy to see that this model can be expanded to n_t transmit antennas, n_r receive antennas and an arbitrary coherence interval T. At time t the n_t transmit antennas each send one signal, this can be written as the vector $\mathbf{x}_t = \begin{pmatrix} x_{1t} \\ \vdots \\ x_{n_t t} \end{pmatrix}$. Each x_{it} will be received by all n_r receive antennas, so a given x_{it} follows n_r different paths, each with a given fading coefficient h_{ji}, to reach its n_r destinations. Therefore a given receive antenna will obtain a signal that is the sum of n_t transmitted signals with fading and some noise. So for a given coherence interval T, during which the channel is assumed constant, Equation 1 can be rewritten as

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \cdot \mathbf{X}_{n_t \times T} + \mathbf{V}_{n_r \times T}. \quad (2)$$

We will sometimes drop the subscripts and simply rewrite Equation 2 as

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{V}$$

As we have seen, in this system a transmitter sends a message $\mathbf{X}$ and it is then up to the receiver to recover this original message from their received signal $\mathbf{Y}$. A crucial point is how sure can a receiver be of recovering the correct message from its received signal, or in other words how reliable is the system. This is where **coding** comes into play. The basic idea is that instead of sending a message directly, we first encode the message to get a **codeword**, which is a function of the original data and will again be denoted by $\mathbf{X}$. It is the codeword that is then transmitted and we call the set of all possible codewords the **codebook** denoted by $\mathcal{C}$. Our system then consists of a set of **information symbols**, i.e. the data to be sent, which is the input to an **encoder**. The encoder then maps the information symbols to a codeword $\mathbf{X}$ that is then transmitted. The receiver obtains $\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{V}$. It is the role of a **decoder** to recover the original information symbols from $\mathbf{Y}$, see Figure 1.

Since the encoding here is done over space (multiple antennas) and time (multiple time slots), this type of coding is known as **Space-Time Coding**.

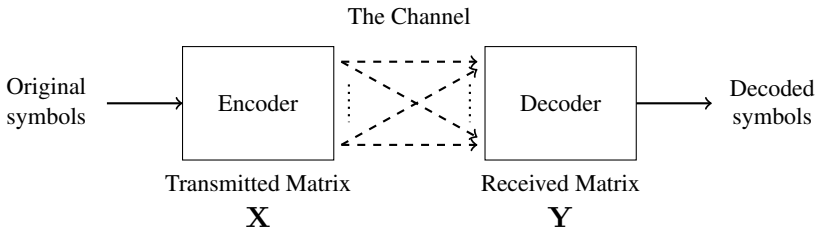


Figure 1: Transmission Scheme

Transmission Channel

We now go into a little more detail on the fading channel in our communication system. Throughout this thesis we will assume that the receiver has perfect **Channel State Information** (CSI), i.e. the receiver has perfect knowledge of the fading matrix $\mathbf{H}$. This is also known as the **coherent** case. This can be achieved via

the introduction of pilot symbols that can then be used to estimate the channel accurately.

The channel we will consider is the **Rayleigh Fading channel**. In this system the elements of the channel matrix $\mathbf{H}$ are assumed to be independent, complex-gaussian random variables with zero mean. As mentioned earlier, we will assume that our channel remains constant for some coherence interval T, this is known as the **quasi-static fading channel**. For further information on fading channels see [7].

Furthermore we will assume that the noise in our channel is **Additive White Gaussian Noise** (AWGN). In this case the elements of the noise matrix $\mathbf{V}$ are independent, complex-gaussian distributed elements with zero mean and variance σ^2.

Coding Requirements

Diversity

A key difference between wireless and wired environments is that in the wireless setting the attenuation of a signal, due to fading, must be considered. If this attenuation is too severe a receiver will not be able to reliably recover a transmitted signal. Therefore a less-attenuated copy of the transmitted signal must also be provided to the receiver. This method is known as **diversity**. The notion of diversity is considered the most important factor in reliable wireless communication [42]. There are various different diversity techniques including:

- **Temporal diversity**: The same signal is transmitted in multiple time slots. In this way the receiver is provided with replicas of the transmitted signal via redundancy in the temporal domain.
- **Frequency diversity**: The same signal is transmitted on multiple frequency channels. In this way the receiver is provided with replicas of the transmitted signal via redundancy in the frequency domain.
- **Spatial diversity**: The same signal is transmitted using multiple transmit antennas and/or multiple receive antennas. In this way the receiver is provided with replicas of the transmitted signal via redundancy in the spatial domain.

Performance Criterion

A question to ask at this point is what process does the receiver follow in order to decode the received matrix $\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{V}$. In our system the receiver knows the codebook $\mathcal{C}$ and also the fading matrix $\mathbf{H}$. They are therefore able to compute the **faded codebook** $\{\mathbf{H} \cdot \mathbf{X} | \mathbf{X} \in \mathcal{C}\}$. One can then choose to decode $\mathbf{Y}$ as the codeword that minimises the distance between $\mathbf{H} \cdot \mathbf{X}$ and $\mathbf{Y}$. Therefore our decoded codeword $\hat{\mathbf{X}}$ is taken to be an element of the following set:

$$\{\mathbf{X} \in \mathcal{C} : \|\mathbf{H} \cdot \mathbf{X} - \mathbf{Y}\|^2 = \min_{\mathbf{X} \in \mathcal{C}} \|\mathbf{H} \cdot \mathbf{X} - \mathbf{Y}\|^2\}$$

with our norm taken to be the **Frobenius norm**, $\|M\|^2 = Tr(MM^\dagger)$, where Tr denotes the matrix trace and $M^\dagger$ denotes the conjugate transpose of M.

It is clear that an error will have occurred in our decoding if $\hat{\mathbf{X}} \neq \mathbf{X}$. We are able to formalise the reliability of our channel by computing the **pairwise probability of error**, namely, the probability of sending $\mathbf{X}$ and decoding it incorrectly as $\hat{\mathbf{X}} \neq \mathbf{X}$. We will write this probability as $\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}})$.

An upper bound for this probability in the case of Rayleigh Space-Time codes has been formulated in [42]. We first set some notation. We define the **codeword distance matrix** as

$$\mathbf{A}(\mathbf{X}, \hat{\mathbf{X}}) = (\mathbf{X} - \hat{\mathbf{X}})(\mathbf{X} - \hat{\mathbf{X}})^\dagger.$$

Let r be the rank of $\mathbf{A}$ and denote by $\lambda_1, \ldots, \lambda_r$ the non-zero eigenvalues of $\mathbf{A}$. Denote by $E_s = \mathbb{E}(|x_{ij}|^2)$, where $\mathbf{X} = (x_{ij})_{i,j}$. An important measure is that of the **Signal-to-Noise Ratio** (SNR). We define the SNR at the receiver as

$$\frac{\mathbb{E}(\|\mathbf{H} \cdot \mathbf{X}\|^2)}{\mathbb{E}(\|\mathbf{V}\|^2)} = \frac{n_t E_s}{N_0}.$$

where N_0 is the **noise power spectral density**. The authors in [42] then show that an upper bound for the pairwise probability of error $\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}})$ is given by

$$\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}}) \leq \Big(\prod_{i=1}^{r} \lambda_i\Big)^{-n_r} \cdot \Big(\frac{E_s}{4N_0}\Big)^{-rn_r}. \tag{3}$$

Note this is an asymptotic bound.

The **diversity gain** of the code is defined as $\min\{rn_r\}$ taken over all possible codewords. This upper bound for $\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}})$ leads to the following design criterion [42]:

- **Rank Criterion**: In order to achieve the maximum diversity gain $n_t n_r$, we ask that the rank of $(\mathbf{X} - \hat{\mathbf{X}})$ for any codewords $\mathbf{X} \neq \hat{\mathbf{X}} \in \mathcal{C}$ must be maximal.

- **Determinant Criterion**: If a maximum diversity gain is the target, then the minimum determinant of $\mathbf{A}(\mathbf{X}, \hat{\mathbf{X}})$, taken over all possible $\mathbf{X} \neq \hat{\mathbf{X}} \in \mathcal{C}$, must be maximised.

To expand on the determinant criterion, consider the case of **full rank** codes. In this instance we have that $det(\mathbf{A}) = \prod_{i=1}^{n_t} \lambda_i \neq 0$ (for $\mathbf{X} \neq \hat{\mathbf{X}}$) and we say that the code is **fully diverse**. As mentioned earlier, division algebras provide us with a means of constructing codes that are fully diverse.

We set the following notation:

$$\delta_{\min}(\mathcal{C}) = \inf \{|det(\mathbf{X} - \hat{\mathbf{X}})|^2 \mid \mathbf{X} \neq \hat{\mathbf{X}} \in \mathcal{C}\}.$$

The real number $\delta_{\min}(\mathcal{C})$ is called the **minimum determinant** of the code. In the **square** case ($n_t = n_r = T$) with common value denoted n, Equation 3 can be rewritten as

$$\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}}) \leq \frac{\kappa}{\delta_{\min}(\mathcal{C})^n}, \tag{4}$$

where κ is a function that depends on the minimum determinant and the SNR. The function κ is a decreasing function that converges to zero as the SNR tends to infinity. Furthermore, as the size of the minimum determinant increases, so does the speed of convergence. Hence a large minimum determinant $\delta_{\min}(\mathcal{C})$ means that our code $\mathcal{C}$ will have a small pairwise probability of error (for a SNR not too large). Further details can be found in [42].

A major factor in the design of codes is how to ensure that the minimum determinant is bounded away from zero. The construction of such codes will be discussed in Section 2.1.

The first chapter in this thesis gives the necessary definitions and results from the theory of number fields and central simple algebras that will be needed in our study. In particular, it introduces the notion of a crossed product algebra and a cyclic algebra.

Chapter 2 then explains how we are able to construct codes that satisfy certain coding properties from crossed product algebras. It introduces an important coding

constraint, called the energy constraint and links this notion to the theory of complex ideal lattices. We end the chapter by providing bounds on the performance of codes constructed from crossed product algebras.

In Chapter 3 we restrict ourselves to codes based on cyclic algebras. We introduce perfect space-time block codes and give several examples. We then consider the optimality of these perfect codes.

Then in Chapter 4 we consider biquadratic codes. We detail their construction and give the best known example. Finally we consider the optimality of this example.

Chapter 1

Mathematical Background

This chapter is concerned with providing the mathematical framework that will be necessary to study the codes in this thesis. We first introduce some ideas from algebraic number theory, because it will be shown that the performance of the codes we will consider is closely linked to the discriminant ideal of a number field extension. Our starting point for this discussion is the field of rational numbers $\mathbb{Q}$. A finite algebraic extension of $\mathbb{Q}$ is known as an (algebraic) **number field** and the set of algebraic integers of a field K forms a ring called the **ring of integers** of K, denoted $\mathcal{O}_K$. It is well known that the ring of integers of a number field is a **Dedekind domain**. As one might expect the ring of integers of $\mathbb{Q}$ is simply $\mathbb{Z}$. A lot of our work will be based around extensions of algebraic number fields and their respective rings of integers.

We then go on to introduce central simple algebras, which play a key part in the construction of the codes. Our focus will be on crossed product algebras and cyclic algebras. As mentioned in the Introduction, division algebras will play a key part in our discussion.

1.1 Hermitian Lattices

Before providing details on algebraic number fields, we would like to introduce a few generalities on **hermitian lattices**.

Definition 1.1.1. *Let $K/\mathbb{Q}$ be a totally imaginary quadratic field extension with non-trivial automorphism $K \to K$, $u \mapsto \bar{u}$, i.e. $K = \mathbb{Q}(\sqrt{-z})$ for some $z \in \mathbb{Z}^+$.*

*A **hermitian $\mathcal{O}_K$-lattice** is a pair (M, h), where M is a free $\mathcal{O}_K$-module and $h : M \times M \to \mathcal{O}_K$ is a hermitian form with respect to complex conjugation $^-$.*

Consider two hermitian $\mathcal{O}_K$-lattices (M, h) and (M', h'). If there exists an $\mathcal{O}_K$-module isomorphism $f : M \tilde{\to} M'$ satisfying

$$h(x, y) = h'(f(x), f(y)) \text{ for all } x, y \in M$$

*then (M, h) and (M', h') are said to be **isomorphic**.*

*The lattice (M, h) is called **positive definite** if $h(x, x) > 0$ for all $x \in M \backslash \{0\}$.*

Definition 1.1.2. *The hermitian $\mathcal{O}_K$-lattice $(\mathcal{O}_K^n, h_0)$ where $n \geq 1$ and*

$$h_0 : \mathcal{O}_K^n \times \mathcal{O}_K^n \to \mathcal{O}_K, \quad (x, y) \mapsto \bar{x}^t y$$

*is called the **cubic lattice** of rank n.*

Remark A hermitian $\mathcal{O}_K$-lattice (M, h) is isomorphic to the cubic lattice if and only if M has an orthonormal $\mathcal{O}_K$-basis with respect to the hermitian form h. In this case (M, h) is positive definite.

Proposition 1.1.3. *Let (M, h) be a hermitian $\mathcal{O}_K$ lattice and let $e_1, \ldots, e_n$ be an $\mathcal{O}_K$-basis of M. Then the determinant of the matrix $H = (h(e_i, e_j))$ lies in $\mathbb{Z}$ and is independent of the chosen basis.*

Proof. By the definition of the hermitian form h, every entry of H and therefore the determinant of H lies in $\mathcal{O}_K$. Furthermore the matrix H is a hermitian matrix, i.e. $H = \bar{H}^t$, which implies $det(H) = det(\overline{H}) = \overline{det(H)}$. Therefore the determinant of H also lies in $\mathbb{R}$. Hence $det(H) \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$, since $K/\mathbb{Q}$ is a totally imaginary quadratic field extension.

Now under a change of basis of M the determinant of H is multiplied by a non-zero element of $\mathcal{O}_K$ of the form $\bar{\alpha}\alpha$, where α is an invertible element of $\mathcal{O}_K$. Hence $\bar{\alpha}\alpha$ is a real positive unit of $\mathcal{O}_K$. Since $K/\mathbb{Q}$ is a totally imaginary quadratic field extension, we see that $\bar{\alpha}\alpha = 1$. □

Definition 1.1.4. *The **determinant** of the lattice (M, h) is defined as the determinant of the matrix $(h(e_i, e_j))$ for any $\mathcal{O}_K$-basis $e_1, \ldots, e_n$ of M.*

Proposition 1.1.5. *If (M, h) is isomorphic to the cubic lattice, then $det(M, h) = 1$.*

Proof. Assume (M, h) is isomorphic to the cubic lattice. Then by the remark above there exists an orthonormal $\mathcal{O}_K$-basis and therefore the matrix H is necessarily the identity matrix. Hence $det(M, h) = 1$. □

1.2 Algebraic Number Fields

The theory of ideals is key to the study of number fields. We therefore introduce some basic notions of ideals and a very important theorem that describes the factorisation of an ideal in the ring of integers of a number field.

Definition 1.2.1. *Let R be an integral domain and K its field of fractions. An R-submodule M of K is called a **fractional ideal** of R if $xM \subseteq R$ for some non-zero x in R. Note that integral ideals (i.e. ideals in the standard definition) can be seen as fractional ideals by simply taking x equal to one.*

Definition 1.2.2. *Let R be an integral domain and K its field of fractions. A submodule M of K is called **invertible** if there exists some submodule N of K such that $MN = R$.*

Theorem 1.2.3. *[23] If I is a non-zero fractional ideal of a Dedekind domain R, then I has a unique prime ideal factorisation $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots\mathfrak{p}_r^{n_r}$, with $n_i \in \mathbb{Z}$ and almost all $n_i = 0$. Consequently, the non-zero fractional ideals form a group under multiplication.*

Definition 1.2.4. *Let I and J be non-zero integral ideals in a Dedekind domain R. We say that I **divides** J, denoted $I|J$, if $J = KI$ for some integral ideal K.*

Proposition 1.2.5. *[6] Let I and J be non-zero integral ideals, then $I|J$ if and only if $J \subseteq I$.*

Remark It is therefore clear that $I|K$ if each prime ideal factor of I is also a factor of J.

As mentioned in Definition 1.1.1, a quadratic field K is called totally imaginary if $K = \mathbb{Q}(\sqrt{-z})$ for some $z \in \mathbb{Z}^+$. We can expand this definition for a number field of arbitrary degree.

Definition 1.2.6. *A number field K is called **totally real** if the image of every embedding from K into $\mathbb{C}$ lies in $\mathbb{R}$ and called **totally imaginary** if the image of every embedding from K into $\mathbb{C}$ does not lie in $\mathbb{R}$.*

Definition 1.2.7. *Let K be a number field. If K is totally imaginary and a quadratic extension of a totally real field, then K is called a* ***CM-field****.*

Definition 1.2.8. *Let K be a number field closed under complex conjugation. A unit u in K is called* ***unimodular*** *if $|u|^2 := u \cdot \bar{u} = 1$.*

Theorem 1.2.9. *[8] Let K be a number field closed under complex conjugation. Then K contains unimodular units that are not roots of unity if and only if K is totally imaginary and not a CM-field.*

1.2.1 Decomposition of Prime Ideals

Given an extension of number fields L/K of degree n, we will need to examine how prime ideals of $\mathcal{O}_K$ decompose into prime ideals of $\mathcal{O}_L$. We have the following diagram:

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ \mathcal{O}_K & \subseteq & \mathcal{O}_L \end{array}$$

Note that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. Now consider a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, which we will sometimes refer to as a prime ideal of K. What can we say about the distinct prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ in the following equation

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

for some $e_i \in \mathbb{N}$, known as the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$, denoted $e_{\mathfrak{P}_i|\mathfrak{p}}$. There are in fact three possibilities:

- $\mathfrak{p}$ remains **inert** in $\mathcal{O}_L$: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$
- $\mathfrak{p}$ **splits** in $\mathcal{O}_L$: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_m$, $m > 1$
- $\mathfrak{p}$ **ramifies** in $\mathcal{O}_L$: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, where at least one $e_i > 1$.

We will often be interested simply in whether a prime ideal ramifies or does not ramify. If a prime ideal $\mathfrak{p}$ remains inert or splits in $\mathcal{O}_L$ then it is said to be

unramified. We can illustrate the point above with a simple example. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, with $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L = \mathbb{Z}[i]$. We consider the decomposition of the primes 2, 3 and 5 in $\mathbb{Z}[i]$.

- 3 remains inert in $\mathbb{Z}[i]$: $(3)\mathbb{Z}[i] = (3)$
- 5 splits in $\mathbb{Z}[i]$: $(5)\mathbb{Z}[i] = (1+2i)\cdot(1-2i)$
- 2 ramifies in $\mathbb{Z}[i]$: $(2)\mathbb{Z}[i] = (1-i)^2$
  since $(1+i)$ and $(1-i)$ differ only by a unit in $\mathbb{Z}[i]$.

In each of these cases we say that $\mathfrak{P}_i$ **lies above** $\mathfrak{p}$.

Lemma 1.2.10. *A prime ideal $\mathfrak{P}_i \subset \mathcal{O}_L$ lies above $\mathfrak{p}$ if and only if $\mathfrak{P}_i \bigcap \mathcal{O}_K = \mathfrak{p}$.*

Proof. If $\mathfrak{P}_i$ lies above $\mathfrak{p}$ then clearly $\mathfrak{p} \subset \mathfrak{P}_i \cap K$ and $\mathfrak{P}_i \cap K \neq \mathcal{O}_K$. As $\mathfrak{p}$ is maximal, this implies $\mathfrak{p} = \mathfrak{P}_i \cap K$. For the converse we have $\mathfrak{p} \subset \mathfrak{P}$, which implies $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$. Hence $\mathfrak{P}$ must occur in the factorisation of $\mathfrak{p}\mathcal{O}_L$. □

Definition 1.2.11. *If $\mathfrak{P}_i$ lies above $\mathfrak{p}$ we will denote by $f_{\mathfrak{P}_i|\mathfrak{p}}$ the degree of the residue class field extension $\mathcal{O}_L/\mathfrak{P}_i$ over $\mathcal{O}_K/\mathfrak{p}$ and call it the **residue class degree** (of $\mathfrak{P}_i$ over $\mathfrak{p}$).*

Theorem 1.2.12. *[19] We keep the notation above and suppose that*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

with distinct prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ and $e_i > 0$. Let $f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$. Then

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

We should also note that there are two types of ramification.

Definition 1.2.13. *Let $\mathfrak{p}$ be a prime ideal that ramifies in L/K, so $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ where at least one $e_i > 1$. Let $\mathfrak{P}_i$ be a prime ideal of $\mathcal{O}_L$ with $e_{\mathfrak{P}_i|\mathfrak{p}} > 1$ and let p be the characteristic of the residue class field $\mathcal{O}_K/\mathfrak{p}$. If $p \nmid e_{\mathfrak{P}_i|\mathfrak{p}}$ then we say that $\mathfrak{P}_i$ is **tamely ramified** over $\mathfrak{p}$ and **wildly ramified** otherwise.*

We say that a prime ideal $\mathfrak{p}$ **splits completely** in L/K if $\mathfrak{p}\mathcal{O}_L$ is a product of $[L:K]$ distinct prime ideals. We will sometimes be interested in the decomposition of a prime ideal in the compositum of two extensions.

Proposition 1.2.14. *Let K_1 and K_2 be two extensions of K. Let $\mathfrak{p}$ be a prime ideal of K that splits completely in K_1 and K_2. Then $\mathfrak{p}$ also splits completely in the compositum K_1K_2. Furthermore if $\mathfrak{p}$ is a prime ideal of K that is unramified in K_1 and K_2, then $\mathfrak{p}$ is also unramified in K_1K_2.*

Proof. See [22], proof of Proposition 4.9.1 and Proposition 4.9.2. □

In the case where L/K is a Galois extension we can be more specific about the decomposition of a prime ideal $\mathfrak{p}$.

Proposition 1.2.15. *[19] Assume L/K is Galois of degree n. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. The action of $\mathrm{Gal}(L/K)$ transitively permutes the prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Furthermore for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and for any prime ideals $\mathfrak{P}_i, \mathfrak{P}_j \subseteq L$ that lie above $\mathfrak{p}$ we have $e_{\mathfrak{P}_i|\mathfrak{p}} = e_{\mathfrak{P}_j|\mathfrak{p}}$. If we denote this common value by e then*

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e. \tag{1.1}$$

All the residue class degrees $f_{\mathfrak{P}_i|\mathfrak{p}}$ are equal and if we denote them by f we have

$$efg = n.$$

Hence in a Galois extension L/K we can talk about the ramification index e of a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. As mentioned above, in Equation 1.1 of Proposition 1.2.15 if $g = n$ (and hence $e = f = 1$) the prime ideal $\mathfrak{p}$ is said to **split completely** in L/K and if $e = n$ then $\mathfrak{p}$ is said to be **totally ramified** in L/K. It is then clear that in a Galois extension L/K of prime degree, the only possibilities for a given prime ideal $\mathfrak{p}$ are for $\mathfrak{p}$ to be inert, to split completely or to be totally ramified.

Two important objects in the study of number fields are the **trace** and **norm**. Assume L is a finite extension of K. We can define a function $r_x : L \to L$ by $r_x(y) = yx$. By regarding L as a finite dimensional vector space over K we can see that r_x is a linear map. If we take a K-basis $w_1, \ldots, w_n$ of L then we can associate to r_x the matrix (a_{ij}) where

$$r_x(w_i) = w_i x = \sum_j a_{ij} w_j.$$

Now define $trace(r_x) := trace(a_{ij})$ and $det(r_x) := det(a_{ij})$. These are independent of the choice of basis, therefore the following definition makes sense.

Definition 1.2.16. *The **trace** (of an element) of L/K is defined as $\mathrm{Tr}_{L/K}(x) = trace(r_x)$ and the **norm** (of an element) of L/K is defined as $\mathrm{N}_{L/K}(x) = det(r_x)$.*

Proposition 1.2.17. *[19] Let L/K be a finite extension of degree n. Let $x, y \in L$ and $a \in K$. Then the following hold:*

- $\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$
- $\mathrm{Tr}_{L/K}(ax) = a\mathrm{Tr}_{L/K}(x)$
- $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$
- $\mathrm{N}_{L/K}(ax) = a^n\mathrm{N}_{L/K}(x)$
- *Let $K \subset L \subset M$ be a tower of fields. Then*

$$\mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x))$$
$$\mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(x))$$

In the case where L/K is a Galois extension with Galois group consisting of the automorphisms σ_i the following hold:

$$\mathrm{Tr}_{L/K}(x) = \sum_{j=0}^{n-1} \sigma_j(x), \quad \mathrm{N}_{L/K}(x) = \prod_{j=0}^{n-1} \sigma_j(x).$$

We can also talk of the **norm of an ideal** in an extension of number fields.

Definition 1.2.18. *Let I be an ideal of $\mathcal{O}_L$. The **norm** of I denoted $\mathcal{N}_{L/K}(I)$ is defined as the ideal of $\mathcal{O}_K$ generated by all the elements $\mathrm{N}_{L/K}(a)$ with $a \in I$. If L/K is a Galois extension with Galois group G then*

$$\mathcal{N}_{L/K}(I) = \prod_{\sigma \in G} \sigma(I) \cap \mathcal{O}_K.$$

Proposition 1.2.19. *[19] Let I and J be ideals of $\mathcal{O}_L$. Then $\mathcal{N}_{L/K}(IJ) = \mathcal{N}_{L/K}(I)\,\mathcal{N}_{L/K}(J)$.*

We will use the notation $\mathcal{N}_{L/K}$ throughout this thesis to indicate that we are considering an ideal in K as opposed to an element. In terms of absolute norms, for an ideal $I \subseteq \mathcal{O}_L$ we define $\mathrm{N}_{L/\mathbb{Q}}(I) := |\mathcal{O}_L/I|$ and $\mathcal{N}_{L/\mathbb{Q}}(I) := \mathrm{N}_{L/\mathbb{Q}}(I)\mathbb{Z}$, that is the ideal generated by the integer $\mathrm{N}_{L/\mathbb{Q}}(I)$. This corresponds with the definition given above.

Proposition 1.2.20. *[19] Let L/K be an extension of number fields and let $\mathfrak{P} \subseteq \mathcal{O}_L$ be a prime ideal above a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Then*

$$\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}}.$$

Let I be a fractional ideal of $\mathcal{O}_L$ with

$$I = \prod \mathfrak{P}_i^{a_i}$$

Let $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}_K$ and $f_i = f_{\mathfrak{P}_i|\mathfrak{p}_i}$. Then

$$\mathcal{N}_{L/K}(I) = \prod \mathfrak{p}_i^{a_i f_i}.$$

Proposition 1.2.21. *[20] Let I and J be ideals of $\mathcal{O}_L$ with $I|J$. Then $\mathcal{N}_{L/K}(I)|\mathcal{N}_{L/K}(J)$. Furthermore $\mathcal{N}_{L/K}(I) = \mathcal{N}_{L/K}(J)$ if and only if $I = J$.*

1.2.2 Kummer Extensions

In this thesis we will often be concerned with a certain type of extension known as a **Kummer extension**. Before introducing Kummer extensions and some of their properties we set some notation. Let I be a fractional ideal of K and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. We denote by $v_{\mathfrak{p}}(I)$ the power of $\mathfrak{p}$ appearing in the unique prime ideal factorisation of I. For any $x \in K$ we will denote $v_{\mathfrak{p}}(x\mathcal{O}_K)$ simply by $v_{\mathfrak{p}}(x)$. Similarly, we will write $\mathfrak{p}|x$ to mean $\mathfrak{p}|x\mathcal{O}_K$. If $\mathcal{O}_K$ is a principal ideal domain then any prime ideal $\mathfrak{p}$ is generated by a prime element $\pi \in \mathcal{O}_K$. For brevity we write v_π in place of $v_{(\pi)}$. Furthermore the integer $v_\pi(x)$ does not depend on the choice of π. Finally we will write $a \equiv b \pmod{\mathfrak{p}}$ to mean $(a-b) \in \mathfrak{p}$.

Definition 1.2.22. *A finite extension of number fields of the form $K(\sqrt[n]{a})/K$ for some $a \in K$, where K contains n distinct roots of unity is known as a **Kummer extension**.*

A Kummer extension is necessarily a Galois extension. Furthermore a lot is known about the ramification of a given prime ideal $\mathfrak{p}$ in a Kummer extension. We give three of the main results.

Proposition 1.2.23. *[21] Let K be a field that contains n distinct roots of unity and let $X^n - a$ be an irreducible polynomial in $\mathcal{O}_K[X]$. Furthermore let $L = K(\sqrt[n]{a})$.*

1. *If $\mathfrak{p}$ is a prime ideal of K with $\mathfrak{p} \nmid na$, then $\mathfrak{p}$ is unramified and decomposes into a product of s prime ideals in L, where s is the maximal divisor of n such that the congruence $x^s \equiv a \pmod{\mathfrak{p}}$ has a solution in $\mathcal{O}_K$.*

2. *If $\mathfrak{p}|a$ and $\mathfrak{p} \nmid n$, then the ramification index of $\mathfrak{p}$ is $n/\gcd(v_{\mathfrak{p}}(a), n)$. In particular, $\mathfrak{p}$ is ramified if and only if $n \nmid v_{\mathfrak{p}}(a)$, and totally ramified if and only if $v_{\mathfrak{p}}(a)$ is prime to n.*

For the case $\mathfrak{p}|n$ we will restrict ourselves to the case when the degree of our Kummer extension is a prime number, say l. Recall that in this case a prime ideal $\mathfrak{p}$ of K will either remain inert, split completely or be totally ramified in the extension $K(\sqrt[l]{a})/K$.

Proposition 1.2.24. *[22] Let $\mathfrak{p}$ be a prime ideal of K with $l \nmid v_{\mathfrak{p}}(a)$. Then $\mathfrak{p}$ is ramified in $K(\sqrt[l]{a})/K$.*

Now assume that $l|v_{\mathfrak{p}}(a)$ and denote by lh the exact power of $\mathfrak{p}$ that divides a. Define an element b by $v_{\mathfrak{p}}(b) = -h$ and $v_{\mathfrak{q}}(b) \geq 0$ for prime ideals $\mathfrak{q} \neq \mathfrak{p}$. Then ab^l will not be divisible by $\mathfrak{p}$ and $K(\sqrt[l]{a}) \simeq K(\sqrt[l]{ab^l})$. Therefore, there remains only one case for us to consider, namely $v_{\mathfrak{p}}(a) = 0$ and $\mathfrak{p}|l$. For the primitive l^{th} root of unity ζ define $\lambda = 1 - \zeta$ and set $w = v_{\mathfrak{p}}(\lambda)$.

Theorem 1.2.25. *[22] Let $\mathfrak{p}$ be a prime ideal of K with $\mathfrak{p}|l$ and $v_{\mathfrak{p}}(a) = 0$. Then the following properties hold:*

1. *$\mathfrak{p}$ splits in L if the congruence*

$$x^l \equiv a (\text{mod } \mathfrak{p}^{wl+1})$$

has a solution in $\mathcal{O}_K$.

2. *$\mathfrak{p}$ is inert in L if the congruence in 1 is insolvable but*

$$x^l \equiv a (\text{mod } \mathfrak{p}^{wl})$$

has a solution in $\mathcal{O}_K$.

3. $\mathfrak{p}$ *is ramified in* L *if the congruence in* 2 *is insolvable.*

1.2.3 The Different and Discriminant

An important result in algebraic number theory is that in a number field only finitely many prime ideals ramify. We will now provide a more precise description of this fact.

Definition 1.2.26. *Let* L/K *be an extension of number fields and* I *a fractional ideal of* $\mathcal{O}_L$*. Then the set*

$$\mathcal{D}_{L/K}^{-1}(I) := \{x \in L : Tr_{L/K}(xI) \subseteq \mathcal{O}_K\}$$

is called the ***codifferent of*** I ***over*** K*.*

We call the inverse of the codifferent of an ideal I over K simply the **different of** I **over** K, denoted $\mathcal{D}_{L/K}(I)$. In the case when $I = \mathcal{O}_L$ then $\mathcal{D}_{L/K}(I)$ is called the **different ideal** of L/K and denoted simply $\mathcal{D}_{L/K}$. It is this object that we will be most interested in.

We have the following relation on the differents in a tower of field extensions:

Theorem 1.2.27 (Tower of Differents Theorem)**.** *[22] Let* $K \subset L \subset M$ *be a tower of number fields. Then*

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L} \cdot \mathcal{D}_{L/K}.$$

Definition 1.2.28. *The* ***relative discriminant ideal*** $\mathfrak{d}_{L/K}$ *of* L/K *is defined as*

$$\mathfrak{d}_{L/K} = \mathcal{N}_{L/K}(\mathcal{D}_{L/K}).$$

Note if $K = \mathbb{Q}$ then $\mathfrak{d}_{L/\mathbb{Q}}$ is a principal ideal in $\mathbb{Z}$. We can therefore talk about the **absolute discriminant** d_L of a number field L, where d_L is defined to be the unique positive generator of $\mathfrak{d}_{L/\mathbb{Q}}$.

For the discriminant ideal there is a theorem equivalent to that of Theorem 1.2.27 called the **Tower of Discriminants Theorem**:

Theorem 1.2.29. *[22] Let* $K \subset L \subset M$ *be a tower of number fields. Then*

$$\mathfrak{d}_{M/K} = \mathcal{N}_{L/K}(\mathfrak{d}_{M/L}) \cdot \mathfrak{d}_{L/K}^{[M:L]}.$$

The following proposition shows how the ramification in a field extension L/K is linked to the different $\mathcal{D}_{L/K}$.

Proposition 1.2.30. *[22] Let $\mathfrak{p}$ be an ideal of K and let $\mathfrak{P}$ be an ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let $e = e_{\mathfrak{P}|\mathfrak{p}}$. Then*

- $v_{\mathfrak{P}}(\mathcal{D}_{L/K}) = e - 1$ *if $\mathfrak{p}$ is tamely ramified*
- $v_{\mathfrak{P}}(\mathcal{D}_{L/K}) > e - 1$ *if $\mathfrak{p}$ is wildly ramified*
- $\mathfrak{P} \nmid \mathcal{D}_{L/K}$ *if $\mathfrak{p}$ is unramified*

This now allows us to compute the discriminant ideal of L/K, or at least give a bound on its divisors, by calculating all prime ideals of K that ramify in L and deciding if they ramify tamely or wildly. We now give a very well known theorem in number theory.

Theorem 1.2.31. *[22] A prime ideal $\mathfrak{p}$ of K ramifies in L/K if and only if it is a divisor of the discriminant ideal of L/K.*

The following results will be useful in the sequel.

Proposition 1.2.32. *Let K be a number field and $L = K(\alpha)$, where α is a root of an Eisenstein polynomial $f(X)$ at $\mathfrak{p}$ in $\mathcal{O}_K[X]$. Then $\mathfrak{p}$ is totally ramified in L.*

Proof. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e\mathfrak{A}$ where $1 \leq e \leq n$ and $\mathfrak{P} \nmid \mathfrak{A}$. Now

$$f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$$

where $c_i \equiv 0 \pmod{\mathfrak{p}}$ (and therefore $c_i \equiv 0 \pmod{\mathfrak{P}^e}$) for $0 \leq i \leq n-1$. The equation $f(\alpha) = 0$ then implies that $\alpha^n \equiv 0 \pmod{\mathfrak{P}}$ and hence $\alpha \equiv 0 \pmod{\mathfrak{P}}$ since $\mathfrak{P}$ is prime. If we consider the intermediate terms in $f(\alpha)$ we see that $c_i\alpha^i \equiv 0 \pmod{\mathfrak{P}^{e+1}}$ for $1 \leq i \leq n-1$, hence

$$\alpha^n + c_0 \equiv 0 \pmod{\mathfrak{P}^{e+1}}.$$

Since f is an Eisenstein polynomial $c_0 \not\equiv 0 \pmod{\mathfrak{p}^2}$, so $c_0\mathcal{O}_L = \mathfrak{P}^e\mathfrak{B}$ where $\mathfrak{P} \nmid \mathfrak{B}$. Therefore $c_0 \not\equiv 0 \pmod{\mathfrak{P}^{e+1}}$, which implies $\alpha^n \not\equiv 0 \pmod{\mathfrak{P}^{e+1}}$. However we know that $\alpha \equiv 0 \pmod{\mathfrak{P}}$ so $\alpha^n \equiv 0 \pmod{\mathfrak{P}^n}$, therefore $e + 1 > n \geq e$. Hence $e = n$ and $\mathfrak{p}$ is totally ramified. □

Proposition 1.2.33. *[39] Let F, L, M be algebraic number fields of finite degree such that $F \subset L \cap M$. Suppose that L and M are linearly disjoint over F, and $\mathcal{D}_{LM/L} = \mathcal{D}_{M/F}\mathcal{O}_{LM}$. Then $\mathcal{O}_{LM} = \mathcal{O}_L\mathcal{O}_M$.*

We end this section by describing the **ideal class group** of a number field K.

Definition 1.2.34. *Let K be a number field. Denote by I_K the group of fractional ideals of K and denote by P_K the group of all principal ideals of K. Clearly P_K is a subgroup of I_K and the quotient*

$$Cl_K := I_K/P_K$$

*is called the **ideal class group** of K. The order of the (finite) group Cl_K is called the **class number** of K.*

Clearly if the class number of a number field K is equal to 1, then the ring of integers $\mathcal{O}_K$ is a principal ideal domain. The class group therefore gives a measure of how much $\mathcal{O}_K$ fails to be a principal ideal domain.

Theorem 1.2.35. *[22] Let K be a number field of degree n with r_1 real embeddings and r_2 pairs of complex embeddings into $\mathbb{C}$. In every ideal class of $\mathcal{O}_K$ there is an integral ideal I such that*

$$\mathrm{N}_{K/\mathbb{Q}}(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|}. \tag{1.2}$$

The right hand side of the equality is often referred to as the **Minkowski bound** of K and denoted by M_K. Note that for a number field K, if $M_K < 2$ then $\mathcal{O}_K$ is necessarily a principal ideal domain.

1.2.4 The Decomposition Group

Definition 1.2.36. *Let L/K be a Galois extension with Galois group G and $\mathfrak{P} \subset \mathcal{O}_L$ a prime ideal above $\mathfrak{p} \subset \mathcal{O}_K$. The set of $g \in G$ such that $g\mathfrak{P} = \mathfrak{P}$ forms a subgroup $Z_\mathfrak{P}$ of G, called the **decomposition group** of $\mathfrak{P}$ over K.*

The decomposition group provides us with a way of explicitly computing the ramification index and the residue class degree of certain prime ideals.

Theorem 1.2.37. *[19] With the assumptions of above, the localization $L_\mathfrak{P}$ of L at $\mathfrak{P}$ is a Galois extension of $K_\mathfrak{p}$ with Galois group $Z_\mathfrak{P}$.*

Corollary 1.2.38. *[19] The order of the decomposition group $Z_{\mathfrak{P}}$ is equal to the product $e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}}$.*

Definition 1.2.39. *The m^{th}* ***ramification group*** *is defined to be the set*

$$G_m := \{g \in Z_{\mathfrak{P}} \mid g\alpha \equiv \alpha \pmod{\mathfrak{P}^{m+1}}, \quad \forall \alpha \in \mathcal{O}_L\}.$$

The **inertia group** is defined as the 0^{th} ramification group and one can show that the ramification groups form a decreasing sequence of normal subgroups of the decomposition group. We denote by $G_{\mathfrak{P}}$ the Galois group of the residue class field extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$, which we know to be cyclic since the residue class fields are finite.

Proposition 1.2.40. *[22] We have $Z_{\mathfrak{P}}/G_0 = G_{\mathfrak{P}}$. Furthermore $|G_0| = e_{\mathfrak{P}|\mathfrak{p}}$.*

The ramification groups also allow us to explicitly compute the different $\mathcal{D}_{L/K}$.

Proposition 1.2.41. *[22] Let v_n be the order of the ramification group G_n of $\mathfrak{P}$ with respect to L/K. Then $\mathfrak{P}$ divides the different $\mathcal{D}_{L/K}$ with exponent*

$$\sum_{n=0}^{\infty}(v_n - 1) = \sum_{n=0}^{\infty}(n+1)(v_n - v_{n+1}).$$

1.3 Central Simple Algebras

In the next chapter we will show how codes can be constructed from central simple algebras and that the fully diverse property can be linked to division algebras. We start by listing some definitions and general results on central simple algebras.

Definition 1.3.1. *The* ***centre*** *of a K-algebra A is defined as the set*

$$Z(A) = \{z \in A \mid az = za \text{ for all } a \in A\}.$$

It is a commutative K-subalgebra of A.

Definition 1.3.2. *Let A be a K-algebra and let B be a subset of A. The* ***centralizer of*** *B* ***in*** *A is defined as the set*

$$Z_A(B) := \{a \in A \mid ab = ba \text{ for all } b \in B\}.$$

Definition 1.3.3. *A K-algebra is called **central simple** if it has no non-trivial two sided ideals (**simple**) and its centre is equal to K (**central**).*

Definition 1.3.4. *Let A be a central simple K-algebra. The **(reduced) degree** of A is defined as $deg(A) = \sqrt{dim_K(A)}$.*

Proposition 1.3.5. *[10] Let A and B be central simple K-algebras. Then the tensor product $A \otimes_K B$ is also a central simple K-algebra.*

Theorem 1.3.6. *[10] Let A be a central simple K-algebra such that $dim_K(A)$ is finite and let B be a simple K-subalgebra of A such that $Z(B) = K$. Then*

$$A \simeq B \otimes_K Z_A(B).$$

Definition 1.3.7. *A central simple K-algebra is called **split** if it is isomorphic to a matrix algebra.*

Definition 1.3.8. *Given a central simple K-algebra A of degree n. We say that a field L is a **splitting field** of A if it contains K and $A \otimes_K L \simeq M_n(L)$. Moreover **every** central simple K-algebra has such a splitting field.*

Definition 1.3.9. *A **commutative subfield** of a K-algebra A is a commutative K-subalgebra L of A that is also a field.*

Proposition 1.3.10. *Let D be a division ring. The centre K of D is a commutative subfield and D is a central simple K-algebra.*

Proof. It is clear that the centre K of a division ring D is a commutative subfield of D. Furthermore any ring R with identity is a $Z(R)$-algebra. Hence D is a central K-algebra and is necessarily simple, since D has no non-trivial two sided ideals. □

Proposition 1.3.11. *[31] Let A be a central simple K-algebra with commutative subfield L. Then $[L : K] \mid deg(A)$.*

The above proposition shows us that for a central simple K-algebra A, there is an upper bound on the degree $[L : K]$ of a commutative subfield L of A. This leads to the following definition.

Definition 1.3.12. *Let A be a central simple K-algebra of degree n and let L be a commutative subfield of A such that $[L : K] = n$. Then L is called a* ***maximal commutative subfield*** *of A.*

Theorem 1.3.13. *[10] Let D be a central simple division K-algebra. Then D has a maximal commutative subfield L.*

Proposition 1.3.14. *[31] Let A be a central simple K-algebra and let L be a maximal commutative subfield of A. Then L is a splitting field of A.*

Theorem 1.3.15 (Primary Decomposition Theorem)**.** *[31] Let A be a central simple K-algebra of degree n, and let $n = p_1^{n_1} \cdots p_r^{n_r}$ be the decomposition of n into distinct prime powers. Then there exist r central simple K-algebras $A_1, \ldots, A_r$, uniquely determined up to isomorphism, such that*

1. *$deg(A_i) = p_i^{n_i}$, for all $i = 1, \ldots, r$.*
2. *$A \cong A_1 \otimes_K \cdots \otimes_K A_r$.*

Moreover, A is a division algebra if and only if $A_1, \ldots, A_r$ are division algebras.

We will finish this section by generalising Hamilton's notion of the quaternions over $\mathbb{R}$, to quaternion algebras over any field K with $char(K) \neq 2$ (quaternion algebras do exist over fields of characteristic equal to two but a slight modification of the definition is required, see [10]).

Definition 1.3.16. *Let K be a field and let a, b be non-zero elements of K. The* ***quaternion algebra*** *$(a, b)_K$ (sometimes $(\frac{a,b}{K})$) is the set of all expressions*

$$\alpha + \beta i + \gamma j + \delta k$$

where $\alpha, \beta, \gamma, \delta \in K$ and

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

The quaternion algebra $(a, b)_K$ is a central simple K-algebra and it has dimension 4 over K. The following results on quaternion algebras are well known, see for example [33].

Lemma 1.3.17. *For $a, b, y, z \in K^\times$ the following hold:*

1. $(a,b)_K \simeq (b,a)_K$.

2. $(a \cdot y^2, b \cdot z^2)_K \simeq (a,b)_K$.

3. $(1,b)_K \simeq M_2(K)$.

The Hamilton quaternions $\mathbb{H}$ would therefore be written as $(-1,-1)_{\mathbb{R}}$. It is well known that $\mathbb{H}$ is a division algebra, however this is not always the case for a general quaternion algebra $(a,b)_K$. Let $q = \alpha + \beta i + \gamma j + \delta k \in (a,b)_K$. We define the conjugate of q as $\bar{q} = \alpha - \beta i - \gamma j - \delta k \in (a,b)_K$ and the norm of q as $\mathrm{N}(q) = q \cdot \bar{q}$. We then have

$$N(q) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2.$$

Theorem 1.3.18. *The quaternion algebra $(a,b)_K$ is a division K-algebra if and only if $N(q) = 0 \Rightarrow q = 0$ for all $q \in (a,b)_K$.*

Remark If we regard the norm map N as a quadratic form on our quaternion algebra (viewed as a vector space) then $(a,b)_K$ is a division K-algebra if an only if our norm map N is anisotropic.

Furthermore if $(a,b)_K$ is not a division K-algebra then it must be isomorphic to $M_2(K)$. So in this case $(a,b)_K$ is split.

One way to see this is to note that $(a,b)_K$ is a central simple K-algebra and then using this result of Wedderburn's:

Proposition 1.3.19. *[10] Let K be a field and A a finite dimensional simple K-algebra. Then $A \simeq M_r(D)$ for some unique integer r and division algebra D over K (unique up to isomorphism).*

By then using the fact that $dim_K((a,b)_K) = 4$ and $dim_K(M_n(D)) = n^2 \cdot dim_K(D)$, we see that our only possibilities are that $n = 1$ and $(a,b)_K = D$ or that $n = 2$ and $D = K$. This result can be modified for any finite dimensional simple K-algebra A such that the degree of A over K is prime.

Definition 1.3.20. *Let A be a central simple K-algebra. The reduced degree of the unique division algebra associated to A by Proposition 1.3.19 is called the **index** of A, written $ind(A)$.*

Proposition 1.3.21. *[10] Let A be a central simple K-algebra. Then the index of A divides the reduced degree of A and we have equality if and only if A is a division K-algebra.*

Proposition 1.3.22. *[31] Let D be a central simple division K-algebra and assume that M/K is a field extension such that $[M : K]$ is a prime divisor of $deg(A)$. Then the following are equivalent.*

1. *M is isomorphic to a subfield of D.*
2. *$D_M := D \otimes_K M$ is not a division K-algebra.*
3. *$deg(D) = [M : K] \cdot ind(D_M)$.*

1.3.1 The Brauer Group

A very important object in the classification of division algebras over a field K is the **Brauer group**. The following results on the Brauer group are well known.

Definition 1.3.23. *Let A and B be central simple K-algebras. A and B are called **Brauer equivalent** (denoted $A \sim B$) if there exist natural numbers s and t such that*

$$A \otimes_K M_s(K) \simeq B \otimes_K M_t(K).$$

Brauer equivalence is an equivalence relation on the set of central simple K-algebras and we denote by $[A]$ the equivalence class of A. Let $Br(K)$ denote the set of these equivalence classes.

Lemma 1.3.24. *[10] If we define an addition on $Br(K)$ by $[A]+[B] := [A \otimes_K B]$ then $Br(K)$ has the structure of an abelian group with*

$$0 = [K] = [M_n(K)] \ \ and \ \ -[A] = [A^{op}].$$

Definition 1.3.25. *The abelian group $Br(K)$ is called the **Brauer group of K**.*

Lemma 1.3.26. *[10] Let A and B be central simple K-algebras. Then $A \simeq B$ if and only if $A \sim B$ and $[A : K] = [B : K]$.*

Definition 1.3.27. *Let $[A] \in Br(K)$. The order of $[A]$ in $Br(K)$ is called the **exponent** of A, written $exp(A)$.*

Proposition 1.3.28. *[10] Let $[A] \in Br(K)$. Then*

$$exp(A) \mid ind(A).$$

Furthermore, $exp(A)$ and $ind(A)$ have the same prime factors.

1.4 Crossed Product Algebras

In [34] it is shown that **cyclic division algebras** have some useful properties that lend themselves to constructing space-time codes. This section introduces the notion of a **crossed product algebra**. It then defines a **cyclic algebra** and talks about some of the properties that they exhibit.

For the rest of this thesis we set the following notation, $x^\tau = \tau^{-1}(x)$.

Definition 1.4.1. *Let A be an abelian group denoted multiplicatively and let G be a finite group that acts on the right of A by automorphisms, i.e.*

$$(a_1 \cdot a_2)^\sigma = a_1^\sigma \cdot a_2^\sigma \text{ for } \sigma \in G, a_1, a_2 \in A.$$

The set

$$Z^2(G,A) := \left\{ \xi : G \times G \to A : \begin{array}{ll} \xi_{1,\tau} = \xi_{\sigma,1} = 1 & \forall \sigma, \tau \in G \\ \xi_{\sigma,\tau\rho}\xi_{\tau,\rho} = \xi_{\sigma\tau,\rho}\xi_{\sigma,\tau}^\rho & \forall \sigma, \tau, \rho \in G \end{array} \right\}$$

*forms an abelian group called the 2-**cocycles** (of G with values in A).*

Definition 1.4.2. *Let L/K be a finite Galois extension of degree n with Galois group G and $\xi \in Z^2(G, L^\times)$. The set of all maps from G to L form a right L-vector space of dimension n with L-basis $(e_\sigma)_{\sigma \in G}$, where $e_\sigma \in \mathrm{Map}(G, L)$ is defined by*

$$e_\sigma(\tau) = \delta_{\sigma,\tau} \text{ for all } \tau \in G.$$

Let $\lambda, \lambda' \in L$. Define on the n^2 dimensional K-vector space

$$(\xi, L/K, G) := \bigoplus_{\sigma \in G} e_\sigma L$$

a multiplication by the following formulae:

$$\lambda e_\sigma = e_\sigma \lambda^\sigma$$

$$e_\sigma e_\tau = e_{\sigma\tau}\xi_{\sigma,\tau}$$

$$(\sum_{\sigma \in G} e_\sigma \lambda_\sigma)(\sum_{\tau \in G} e_\tau \lambda'_\tau) = \sum_{\sigma,\tau \in G} e_{\sigma\tau}\xi_{\sigma,\tau}\lambda_\sigma^\tau \lambda'_\tau.$$

*Then $(\xi, L/K, G)$ is called a **crossed product algebra** over K. One may check that the elements e_σ are invertible, $e_{\mathrm{Id}} = 1$, and $(\xi, L/K, G)$ is a central simple K-algebra with splitting field L, see [10] for more details.*

1.4.1 Cyclic Algebras

Definition 1.4.3. *Let L/K be a cyclic Galois extension of degree n with Galois group generated by σ and let γ be an element of L fixed by the action of G. We may form a 2-cocycle as above such that the elements of $Z^2(G, L^\times)$ satisfy*

$$\xi^{\sigma,\gamma}_{\sigma^i,\sigma^j} = \begin{cases} 1 & \text{if } i+j < n \\ \gamma & \text{if } i+j \geq n \end{cases}$$

Set $e = e_\sigma$. Then the crossed product algebra $A = (\gamma, L/K, \sigma) = (\xi^{\sigma,\gamma}, L/K, G)$ where

$$A = 1 \cdot L \oplus e \cdot L \oplus \cdots \oplus e^{n-1} \cdot L \tag{1.3}$$

and

$$\begin{aligned} \lambda e &= e\lambda^\sigma && \forall \lambda \in L \\ e^n &= \gamma && \gamma \in K^* = K \backslash \{0\} \end{aligned}$$

*is called a **cyclic algebra** of degree n corresponding to L/K.*

Theorem 1.4.4. *[16] Let L/K be a cyclic extension of degree n with Galois group generated by σ and let F be an extension field of K. Assume that $[LF : F] = m$ and denote by σ' the extension of $\sigma^{n/m}$ to LF/F. Then*

$$(\gamma, L/K, \sigma) \sim (\gamma, LF/F, \sigma').$$

We now state three useful properties of cyclic algebras [10]:

Lemma 1.4.5. *For cyclic algebras of degree n corresponding to L/K we have*

$$(\gamma_1, L/K, \sigma) \otimes_K (\gamma_2, L/K, \sigma) \simeq M_n((\gamma_1\gamma_2, L/K, \sigma)).$$

Lemma 1.4.6. *Let L/K be a cyclic extension of degree n with generating automorphism σ and let M be an intermediate field of degree m over K, then $\bar{\sigma} := \sigma_{|M}$ generates $Gal(M/K)$ and*

$$(\gamma^s, L/K, \sigma) \simeq M_s((\gamma, M/K, \bar{\sigma}))$$

where $s := n/m = [L : M]$.

Lemma 1.4.7. *We have $(a, L/K, \sigma) \simeq (b, L/K, \sigma)$ if and only if $\frac{b}{a} \in N_{L/K}(L^\times)$.*

1.5 Central Simple Algebras over Number Fields

For the bulk of this thesis we will be interested in division algebras over certain number fields. We would therefore like to introduce several definitions and results on this subject.

Definition 1.5.1. *Let K be a field. An **absolute value** on K is a map*

$$|\ |_w : K \to \mathbb{R}^+$$

satisfying

1. $|x|_w = 0$ *if and only if* $x = 0$
2. $|xy|_w = |x|_w|y|_w$ *for all* $x, y \in K$
3. $|x + y|_w \leq |x|_w + |y|_w$ *for all* $x, y \in K$

If instead of Condition 3 the absolute value satisfies the stronger condition

4. $|x + y|_w \leq \max(|x|_w, |y|_w)$

*then $|\ |_w$ is called **non-archimedean**.*

Definition 1.5.2. *Let $|\ |_1, |\ |_2$ be two absolute values on K with $|\ |_1$ non-trivial. The two absolute values are **equivalent** if $|\ |_2 = |\ |_1^a$ for some $a > 0$. An equivalence class of absolute values of K is called a **place** of K.*

Let K be a number field. A place w of K falls into one of three categories:

1. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. The $\mathfrak{p}$-**adic absolute value** is defined as

   $$|x|_{\mathfrak{p}} = |\mathcal{O}_K/\mathfrak{p}|^{-v_{\mathfrak{p}}(x)} \text{ for all } x \in K$$

   where $v_{\mathfrak{p}}(0)$ is defined as ∞. A place represented by such an absolute value is called a **finite** place.

2. Let σ be a real embedding of K into $\mathbb{C}$, i.e. σ is a $\mathbb{Q}$-embedding of K into $\mathbb{C}$ such that $\sigma(K) \subseteq \mathbb{R}$. We define an absolute value for σ by

   $$|x|_\sigma = |\sigma(x)| \text{ for all } x \in K$$

   where $|\cdot|$ denotes the classical absolute value on $\mathbb{R}$. A place represented by such an absolute value is called a **real** place.

3. Let σ be a complex embedding of K into $\mathbb{C}$, i.e. σ is a $\mathbb{Q}$-embedding of K into $\mathbb{C}$ such that $\sigma(K) \not\subseteq \mathbb{R}$. For each complex embedding σ there is a unique conjugate embedding $\bar{\sigma}$ constructed by composing σ with the complex conjugation map $\mathbb{C} \to \mathbb{C}$. We define an absolute value for σ by

$$|x|_\sigma = |\sigma(x)|^2 \text{ for all } x \in K$$

where $|\cdot|$ denotes the modulus of a complex number. Note that by the definition of $\bar{\sigma}$ we have $|x|_\sigma = |x|_{\bar{\sigma}}$. A place represented by such an absolute value is called a **complex** place.

We note that the completion K_w of a number field K at a place w is a local field. It is well known that for any element $a \in K_w^\times$ there is a unique integer $n_w(a)$ such that $a = \pi^{n_w(a)}u$, where u is a unit in the ring of integers of K_w and π is a uniformising element.

Lemma 1.5.3 (Hensel's Lemma (Trivial case))**.** *[23] Let K be a number field and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. Let $K_\mathfrak{p}$ be the completion of K at the place $\mathfrak{p}$ and denote the ring of integers of $K_\mathfrak{p}$ by $\mathcal{O}_\mathfrak{p}$. Let $f(X)$ be a polynomial with coefficients in $\mathcal{O}_\mathfrak{p}$ and assume there exists $\alpha_0 \in \mathcal{O}_\mathfrak{p}$ such that*

$$f(\alpha_0) \equiv 0 \pmod{\mathfrak{p}}, \quad f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{p}}.$$

Then there exists $\alpha \in K_\mathfrak{p}$ such that $f(\alpha) = 0$.

We now come to one of the most important results in the theory of central simple K-algebras. For more information on the theorem as well as its consequences, particularly in class field theory, see [32].

Theorem 1.5.4 (Brauer-Hasse-Noether)**.** *Let K be a number field and let A be a central simple K-algebra. Then we have the following:*

1. *A is isomorphic to a cyclic K-algebra.*
2. *A is split if and only if $A \otimes_K K_\upsilon$ is split for all places υ of K.*
3. *The number of places where $A \otimes_K K_\upsilon$ is not split is finite and even. In particular, if A splits at all places except maybe one, then A splits at all places and hence A splits.*

4. *The index of A is equal to the exponent of A and this value is equal to the least common multiple of $ind(A \otimes_K K_\upsilon)$, where υ runs through the set of places of K.*

Hence we can say that A is a division K-algebra if and only if $exp(A) = deg(A)$. We also have

Corollary 1.5.5. *Let K be a number field. A central simple K-algebra is a division K-algebra if and only if there exists a place υ of K such that $A \otimes_K K_\upsilon$ is a division algebra.*

Proof. Assume that there does not exist a place υ such that $A \otimes_K K_\upsilon$ is a division algebra. Then $ind(A)$ must be a strict divisor of $deg(A)$ and hence A is not a division K-algebra. Conversely if such a place does exist, then by a result of Hasse [15], we have $ind(A \otimes_K K_\upsilon)|ind(A)$ and so A must be a division algebra. □

Definition 1.5.6. *Let K be a local field and denote by $\kappa(\upsilon)$ the residue field of the place υ of K of order q. Assume that K contains a primitive n^{th} root of unity and that the characteristic of $\kappa(\upsilon)$ is prime to n. For $a, b \in K^\times$ the **(tame) Hasse symbol** is defined as*

$$(a,b)_{n,\upsilon} = (\overline{(-1)^{n_\upsilon(a)n_\upsilon(b)}a^{n_\upsilon(b)}b^{-n_\upsilon(a)}})^{\frac{q-1}{n}} \in \kappa(\upsilon)$$

which is a n^{th} root of 1.

Proposition 1.5.7. *[12] The (tame) Hasse symbol has the following properties for all $a, a', b, b' \in K$:*

1. $(aa', b)_{n,\upsilon} = (a,b)_{n,\upsilon}(a',b)_{n,\upsilon}$
2. $(a, bb')_{n,\upsilon} = (a,b)_{n,\upsilon}(a,b')_{n,\upsilon}$
3. $(a,b)_{n,\upsilon}(b,a)_{n,\upsilon} = 1$
4. $(a,b)_{n,\upsilon} = 1$ *if and only if a is a norm in $K(\sqrt[n]{b})/K$ if and only if $(a, K(\sqrt[n]{b})/K, \sigma)$ splits, where σ generates* $\mathrm{Gal}(K(\sqrt[n]{b})/K)$.

We will make use of this result in Chapter 3 where we will need to determine if certain cyclic K-algebras are division K-algebras.

Chapter 2

Code Construction

In this chapter we give an algebraic construction of codes based on crossed product algebras that satisfy the properties mentioned in the Introduction. We then show that certain coding constraints can be linked to the study of complex ideal lattices. Finally we provide bounds on the performance of codes based on crossed product algebras.

2.1 Algebra Based Codes

Recall from the Introduction that there is an upper bound on the pairwise probability of error

$$\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}}) \leq \Big(\prod_{i=1}^{r} \lambda_i\Big)^{-n_r} \cdot \Big(\frac{E_s}{4N_0}\Big)^{-rn_r}.$$

In the case of full rank codes this can be rewritten as

$$\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}}) \leq \frac{1}{|det(\mathbf{X} - \hat{\mathbf{X}})|^{2n_r}} \cdot \Big(\frac{E_s}{4N_0}\Big)^{-rn_r}.$$

We know that in order to reduce the probability of error in our code we must look to maximise the minimum determinant

$$\delta_{\min}(\mathcal{C}) = \inf\{|det(\mathbf{X} - \hat{\mathbf{X}})|^2 \ \mid \ \mathbf{X} \neq \hat{\mathbf{X}} \in \mathcal{C}\}.$$

This section will explain how we can go some way to achieving this by ensuring that the minimum determinant of our code is bounded away from zero.

Obviously the first step in this process is to ensure that $\delta_{\min}(\mathcal{C}) \neq 0$. Recall from Definition 1.3.8 that for every central simple K-algebra A there exists a field L/K

such that $A \otimes_K L \simeq M_n(L)$. We then have an injective K-algebra homomorphism

$$\phi : A \hookrightarrow M_n(L) \subset M_n(\mathbb{C}). \tag{2.1}$$

Proposition 2.1.1. *Let ϕ be as in Equation 2.1. If A is a division K-algebra, then ϕ will map A to a division subring of $M_n(L) \subset M_n(\mathbb{C})$.*

Proof. Clear, since ϕ is a ring homomorphism. □

The above result provides us with a way to ensure that $\delta_{\min}(\mathcal{C}) \neq 0$. We now need to give an explicit description of the injection ϕ.

Let A be a central simple K-algebra and assume that A has a maximal commutative subfield L. Therefore A is a right L-vector space. Recall the structure of a right L-vector space on $\mathrm{End}_L(A)$ is defined by

$$\mathrm{End}_L(A) \times L \to \mathrm{End}_L(A), \;\; (u, \lambda) \mapsto u\lambda$$

where

$$(u\lambda)(z) = u(z)\lambda, \text{ for all } z \in A.$$

We define for all $a \in A$ an endomorphism l_a on A by

$$l_a : A \to A, \;\; z \mapsto az.$$

To see that this is an endomorphism note that for all $z, z' \in A$ we have

$$l_a(z + z') = a(z + z') = az + az' = l_a(z) + l_a(z')$$

Furthermore for all $\lambda \in L$ we have

$$l_a(z\lambda) = a(z\lambda) = l_a(z)\lambda = (l_a\lambda)(z).$$

Proposition 2.1.2. *The map*

$$\phi : A \to End_L(A), \;\; a \mapsto l_a$$

is an injective K-algebra homomorphism.

Proof. We need to check that $\phi(a + a')(z) = \phi(a)(z) + \phi(a')(z)$, $\phi(aa')(z) = (\phi(a) \circ \phi(a'))(z)$ and $\phi(ak)(z) = \phi(a)(z)k$ for all $a, a', z \in A$ and $k \in K$. We

see that

$$l_{a+a'}(z) = (a+a')(z) = az + a'z = l_a(z) + l_{a'}(z)$$
$$l_{aa'}(z) = (aa')(z) = l_a(a'z) = (l_a \circ l_{a'})(z)$$
$$l_{ak}(z) = (ak)(z) = a(kz) = a(z)k = l_a(z)k$$

Now since A is simple we see that $ker(\phi) = (0)$ or A. However $\phi(1) = 1$ so $ker(\phi) = (0)$ and hence ϕ is injective. □

Now $n = dim_L(A) = dim_K(A)/[L : K]$[10] and we choose an L-basis $\{u_1, \ldots, u_n\}$ of A. We define M_a to be the matrix of left multiplication by a in the chosen L-basis of A, i.e. $M_a = (m_{ij})$ where $l_a(u_i) = \sum_{j=1}^{n} u_j m_{ij}$. Using this and the fact that $End_L(A) \simeq M_n(L)$, we now have an injective K-algebra homomorphism

$$\varphi_{A,L} : A \hookrightarrow M_n(L), \;\; a \mapsto M_a.$$

By Proposition 2.1.1 we know that if A is a division K-algebra then $\varphi_{A,L}$ will map A to a division subring of $M_n(L)$. This then allows us to construct codes that are fully diverse.

We take our codebook $\mathcal{C}$ to be a (large) finite subset of

$$\mathcal{C}_{A,L} := \{\mathbf{X} = \varphi_{A,L}(a), a \in A\}.$$

Let $\mathbf{X}', \mathbf{X}'' \in \mathcal{C}$ where $\mathbf{X}' \neq \mathbf{X}''$, so $\mathbf{X}' = \varphi_{A,L}(a'), \mathbf{X}'' = \varphi_{A,L}(a'')$ for $a' \neq a'' \in A$. If we consider the difference $\mathbf{X}' - \mathbf{X}''$ we see that

$$\mathbf{X}' - \mathbf{X}'' = \varphi_{A,L}(a') - \varphi_{A,L}(a'') = \varphi_{A,L}(a' - a'').$$

However $a' \neq a''$ and A is a division K-algebra, therefore $a' - a''$ is a unit of A. We then see that $\varphi_{A,L}(a' - a'') = \mathbf{X}' - \mathbf{X}''$ is a unit in $M_n(L) \subset M_n(\mathbb{C})$, since $\varphi_{A,L}$ is also a ring homomorphism. Therefore this choice of codebook $\mathcal{C}$ ensures that our code is fully diverse. This method of using division algebras to achieve fully diverse codes was first described in [34].

We now introduce an important concept in coding theory that will reinforce our interest in division algebras. The **rate** of a code measures how much useful information is sent by the code. More specifically the rate is the ratio of the number of information symbols sent and the total number of coefficients sent. It is clear

that codes with higher rates can be beneficial as they are able to transmit a higher number of information symbols in a given time.

Assume that A is a simple K-algebra and that L is a finite extension of K that is also a K-subalgebra of A with $dim_L(A) = r$. Consider a code $\mathcal{C} \subset \mathcal{C}_{A,L}$. The information symbols that we would like to transmit are elements of K that define elements of A. Any element $a \in A$ can therefore represent $dim_K(A)$ information symbols. Now since the elements of $\mathcal{C}$ belong to $M_r(\mathbb{C})$ the total number of coefficients sent will be equal to r^2. Hence the rate of a code $\mathcal{C} \subset \mathcal{C}_{A,L}$ is

$$R = \frac{dim_K(A)}{r^2}. \tag{2.2}$$

However $dim_K(A) = dim_L(A) \cdot [L : K] = r \cdot [L : K]$, so Equation 2.2 can be rewritten as

$$R = \frac{[L : K]^2}{dim_K(A)}.$$

Therefore to have a code with a higher rate we need to choose an extension L/K such that $[L : K]$ is as large as possible. By Proposition 1.3.11 if A is a central simple K-algebra then $[L : K] \leq deg(A)$. Furthermore, if A is also a division K-algebra then by Theorem 1.3.13 we can choose L to be a maximal commutative subfield of A. Then the rate of our code is $R = 1$, which is the maximum possible value in this case.

We have now shown how to choose a codebook $\mathcal{C}$ so that $\delta_{\min}(\mathcal{C}) \neq 0$. However another problem we must consider is that since our codebook could contain a large number of elements, $\delta_{\min}(\mathcal{C})$ could be very close to zero because $\mathcal{C}_{A,L}$ could contain matrices of arbitrarily small determinant. We therefore look to ensure that $\delta_{\min}(\mathcal{C}_{A,L})$ is bounded below by a positive constant. Such a codebook $\mathcal{C}_{A,L}$ is said to have **non-vanishing minimum determinant** [2]. In order to achieve a non-vanishing determinant we choose our elements $a \in A$ to be from an order Γ of A, which ensures the determinants are discrete.

This is where number fields come into play. Let K be a number field, A a central simple division K-algebra and L a maximal commutative subfield of A. For an L-basis $\{u_1, \ldots, u_n\}$ of A and any ideal $I \subseteq \mathcal{O}_L$ set

$$\Gamma_{A,I} = \bigoplus_{i=1}^{n} u_i I$$

and

$$\mathcal{C}_{A,I} = \{M_a | a \in \Gamma_{A,I}\}.$$

Since $\Gamma_{A,I}$ and $\mathcal{C}_{A,I}$ are additive groups we then have

$$\delta_{\min}(\mathcal{C}_{A,I}) = \inf\{|det(M_a)|^2 | a \in \Gamma_{A,I}, a \neq 0\}.$$

Furthermore if we take our codebook $\mathcal{C}$ to be a finite subset of $\mathcal{C}_{A,I}$ we see that $\delta_{\min}(\mathcal{C}) \geq \delta_{\min}(\mathcal{C}_{A,I})$.

We would now like to give a few more details on the transmission scheme, in order to justify our interest in number fields. In order to transmit our information symbols we need to transform them into a signal that is suitable for transmission through the channel. This process is known as **modulation** and is carried out by a **modulator**. The act of extracting the original information from a modulated carrier wave is called **demodulation**. This channel model is given in Figure 2.1.

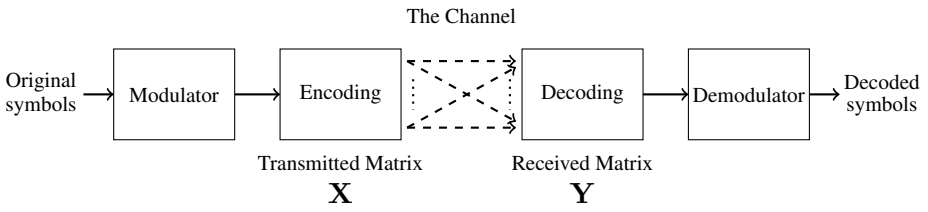
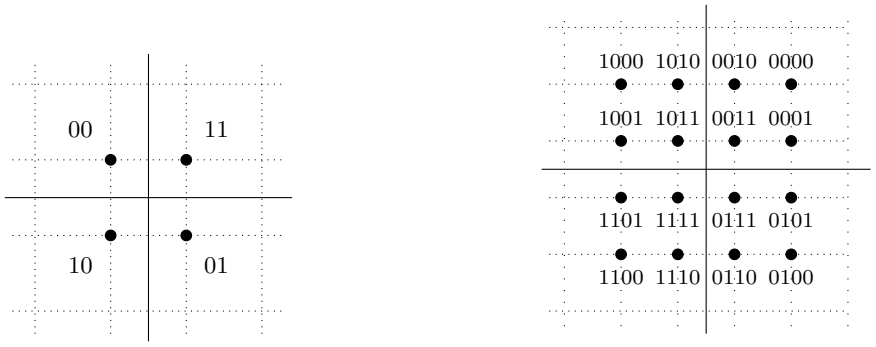


Figure 2.1: Transmission Scheme with Modulation

There are various modulation methods available, however in this thesis we will concentrate on q-QAM and q-HEX constellations. A constellation diagram is a graphical representation that makes it easier to visualise signals using complex modulation techniques.

Quadrature Amplitude Modulation (QAM) is a technique that transmits information by changing both the amplitude and the phase of the carrier wave. A q-QAM constellation can be seen as a subset of the Gaussian integers $\mathbb{Z}[i]$ [11]. It is well known that $\mathbb{Z}[i]$ is the ring of integers of the number field $\mathbb{Q}(\sqrt{-1})$. Three particular q-QAM constellations that we will consider are $q = 4, 16$ and 64. The constellation diagrams for $q = 4$ and 16 are given in Figure 2.2.



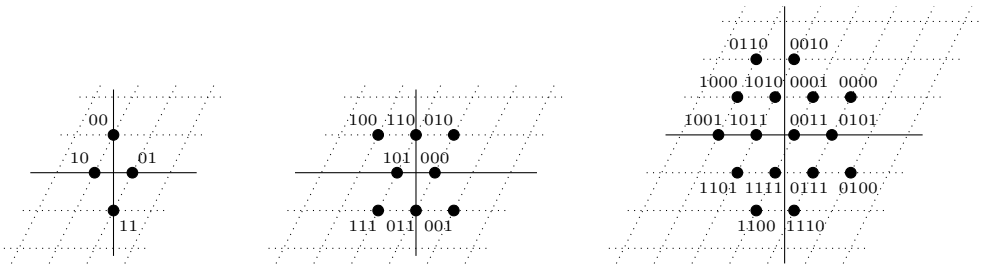
4-QAM 16-QAM

Figure 2.2: 4-QAM and 16-QAM Constellations

Hexadecimal constellations (q-HEX) are finite subsets of the hexagonal lattice A_2 with generator matrix

$$\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

The lattice A_2 is the densest lattice in dimension 2. Furthermore a q-HEX constellation can be seen as a subset of the Eisenstein integers $\mathbb{Z}[j]$ [11], where j is a primitive third root of unity. It is well known that $\mathbb{Z}[j]$ is the ring of integers of the number field $\mathbb{Q}(\sqrt{-3})$. Three particular q-HEX constellations that we will consider are $q = 4, 8$ and 16. The best hexagonal constellations for these sizes are presented in Figure 2.3.



4-HEX 8-HEX 16-HEX

Figure 2.3: 4-HEX, 8-HEX and 16-HEX Constellations

Proposition 2.1.3. *Let $K = \mathbb{Q}(\sqrt{-z})$ for some $z \in \mathbb{Z}^+$. Let A be a central simple division K-algebra with maximal commutative subfield L. Let I be an ideal of $\mathcal{O}_L$. Then there exists a positive integer c such that*

$$\delta_{min}(\mathcal{C}) \geq \frac{1}{c}$$

for all codebooks $\mathcal{C} \subseteq \mathcal{C}_{A,I}$.

Proof. Recall that $\Gamma_{A,I} := \bigoplus_{i=1}^{n} u_i I$ for an L-basis $\{u_1, \ldots, u_n\}$ of A and for any $a \in \Gamma_{A,I}$ we have $M_a \in M_n(L)$. Since every element of L may be written in the form α/β with $\alpha \in \mathcal{O}_L$ and $\beta \in \mathbb{Z}$, the set

$$\{m \in \mathbb{Z} \mid mM_{u_i} \in M_n(\mathcal{O}_L), \text{ for } i = 1, \ldots, n\}$$

is a non-zero ideal of $\mathbb{Z}$ and is therefore generated by a unique positive integer $r \geq 1$. Hence for any $a = u_1 a_1 + \cdots + u_n a_a \in \Gamma_{A,I}$, we have

$$rM_a = rM_{u_1} a_1 + \cdots + rM_{u_n} a_n \in M_n(\mathcal{O}_L).$$

Now $det(M_a)$ is the **reduced norm** of a and hence lies in K [10]. Therefore $det(rM_a) = r^n det(M_a) \in \mathcal{O}_L \cap K = \mathcal{O}_K$ and we obtain that

$$det(M_a) \in \frac{1}{r^n}\mathcal{O}_K.$$

Hence for all $a \in \Gamma_{A,I}$, there exists $x \in \mathcal{O}_K$ such that

$$det(M_a) = \frac{x}{r^n}.$$

Now $|x|^2 = x\bar{x} \in \mathcal{O}_K$ and the assumption that K is a totally imaginary quadratic number field implies that $|x|^2 \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$. Therefore

$$|det(M_a)|^2 = \frac{|x|^2}{|r|^{2n}} \in \frac{1}{r^{2n}}\mathbb{Z}, \text{ for all } a \in \Gamma_{A,I}.$$

If we set $c = r^{2n}$ we can then conclude that

$$\delta_{min}(\mathcal{C}) \geq \delta_{min}(\mathcal{C}_{A,I}) \geq \frac{1}{c}.$$

□

We have therefore described a way to ensure that $\delta_{min}(\mathcal{C})$ is not too close to zero. As mentioned above, in the sequel we will often assume that $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(j) \simeq \mathbb{Q}(\sqrt{-3})$. These two fields have the nice property that $\mathcal{O}_K$ is a PID and therefore any ideal $I \subset \mathcal{O}_L$ has an $\mathcal{O}_K$-basis $\omega_1, \ldots, \omega_n$.

We end this section with a brief description of a coding constraint called the **energy constraint**. Briefly this states that we should not increase the energy used in our system by encoding the information symbols.

Consider $\mathbf{X} \in \mathcal{C}$, which is a matrix representing some encoded information. Specifically we have

$$\mathbf{X} = M_a,\ a = e_1 a_1 + \cdots e_n a_n, a_i \in I$$

and the original information that is transmitted is represented by the elements $a_{ij} \in \mathcal{O}_K$ given by

$$a_i = \sum_{j=1}^{n} a_{ij} w_j, i = 1, \ldots, n.$$

The **energy cost** of transmitting the n^2 original information symbols is given by the sum

$$\sum_{i,j} |a_{ij}|^2.$$

Similarly the energy cost of transmitting the n^2 encoded symbols, where $\mathbf{X} = (x_{ij})_{i,j}$, is given by

$$\sum_{i,j} |x_{ij}|^2.$$

Therefore to satisfy the energy constraint we require that

$$\sum_{i,j} |a_{ij}|^2 = \sum_{i,j} |x_{ij}|^2.$$

In the next section we will consider a certain class of codes that employ crossed product algebras. The energy constraint will be looked at in detail with respect to these codes.

2.2 Codes Based on Crossed Product Algebras

In [37] the authors present constructions for codes based on crossed product algebras. Recall from Section 1.4 that a crossed product algebra is a central simple K-algebra

A such that $A = (\xi, L/K, G) = \bigoplus e_\sigma L$, where $\xi \in Z^2(G, L^\times)$ and A satisfies the following multiplication formulae:

$$\begin{aligned} \lambda e_\sigma &= e_\sigma \lambda^\sigma \\ e_\sigma e_\tau &= e_{\sigma\tau}\xi_{\sigma,\tau} \\ (\sum_{\sigma\in G} e_\sigma\lambda_\sigma)(\sum_{\tau\in G} e_\tau\lambda'_\tau) &= \sum_{\sigma,\tau\in G} e_{\sigma\tau}\xi_{\sigma,\tau}\lambda_\sigma^\tau\lambda'_\tau. \end{aligned}$$

Following the method of the previous section let us compute the matrix of left multiplication M_a. An element $a \in A$ is of the form $a = \sum_{\sigma\in G} e_\sigma a_\sigma$. We compute the multiplication for an arbitrary basis element e_τ:

$$\begin{aligned} ae_\tau &= \sum_{\sigma\in G} e_\sigma a_\sigma e_\tau \\ &= \sum_{\sigma\in G} e_\sigma e_\tau a_\sigma^\tau \\ &= \sum_{\sigma\in G} e_{\sigma\tau}\xi_{\sigma,\tau}a_\sigma^\tau \\ &= \sum_{\rho\in G} e_\rho \xi_{\rho\tau^{-1},\tau} a^\tau_{\rho\tau^{-1}}. \end{aligned}$$

We may now see that

$$(M_a)_{\rho,\tau} = \xi_{\rho\tau^{-1},\tau}a^\tau_{\rho\tau^{-1}}. \tag{2.3}$$

To see this more clearly let $G = \{\sigma_0 = \mathrm{Id}, \sigma_1, \ldots, \sigma_{n-1}\}$. Then

$$M_a = \begin{pmatrix} a_{\mathrm{Id}} & \xi_{\sigma_1^{-1},\sigma_1}a^{\sigma_1}_{\sigma_1^{-1}} & \cdots & \xi_{\sigma_{n-1}^{-1},\sigma_{n-1}}a^{\sigma_{n-1}}_{\sigma_{n-1}^{-1}} \\ a_{\sigma_1} & a^{\sigma_1}_{\mathrm{Id}} & \cdots & \xi_{\sigma_1\sigma_{n-1}^{-1},\sigma_{n-1}}a^{\sigma_{n-1}}_{\sigma_1\sigma_{n-1}^{-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\sigma_{n-1}} & \xi_{\sigma_{n-1}\sigma_1^{-1},\sigma_1}a^{\sigma_1}_{\sigma_{n-1}\sigma_1^{-1}} & \cdots & a^{\sigma_{n-1}}_{\mathrm{Id}} \end{pmatrix}$$

Now let I be an ideal of $\mathcal{O}_L$ and assume that $\mathcal{O}_K$ is a PID so that I has an $\mathcal{O}_K$-basis $(\omega_\sigma)_{\sigma\in G}$. Our n^2 original symbols denoted $a_{\sigma,\tau}$ for $\sigma, \tau \in G$ are encoded as the matrix $M_a \in \mathcal{C}_{A,I}$ with

$$a = \sum_{\sigma\in G} e_\sigma(\sum_{\tau\in G} a_{\sigma,\tau}\omega_\tau). \tag{2.4}$$

Proposition 2.2.1. *If we encode our information as described above, then the energy constraint is satisfied if and only if the following two conditions are satisfied:*

1. $|\xi_{\sigma,\tau}|^2 = 1$ *for all* $\sigma, \tau \in G$.
2. *The matrix* $W = (\omega_\tau^\sigma)_{\sigma,\tau}$ *is unitary.*

Proof. We require that

$$\sum_{\sigma,\tau} |a_{\sigma,\tau}|^2 = \sum_{\sigma,\tau} |\xi_{\sigma\tau^{-1},\tau} a_{\sigma\tau^{-1}}^\tau|^2 = \sum_{\sigma,\tau} |\xi_{\sigma,\tau} a_\sigma^\tau|^2$$

for all $a_{\sigma,\tau} \in \mathcal{O}_K$.

Consider the column vectors

$$X_\sigma = (\xi_{\sigma,\rho} a_\sigma^\rho)_{\rho \in G},\ A_\sigma = (a_{\sigma,\rho})_{\rho \in G} \in L^n.$$

Let $D_\sigma \in M_n(L)$ be the diagonal matrix, with non-zero entry in column ρ given by $\xi_{\sigma,\rho}$. Now

$$\xi_{\sigma,\tau} a_\sigma^\tau = \sum_{\rho \in G} \xi_{\sigma,\tau} a_{\sigma,\rho}^\tau \omega_\rho^\tau = \sum_{\rho \in G} \xi_{\sigma,\tau} a_{\sigma,\rho} \omega_\rho^\tau$$

since $a_{\sigma,\rho} \in K$ for $\sigma, \rho \in G$. Furthermore for $W = (\omega_\rho^\tau)_{\tau,\rho}$, we have $D_\sigma W = (\xi_{\sigma,\tau} \omega_\rho^\tau)_{\tau,\rho}$ and therefore

$$X_\sigma = D_\sigma \cdot W \cdot A_\sigma \text{ for all } \sigma \in G.$$

We now define the following block column vectors

$$\mathbf{x} = \begin{pmatrix} \vdots \\ X_\sigma \\ \vdots \end{pmatrix}, \mathbf{a} = \begin{pmatrix} \vdots \\ A_\sigma \\ \vdots \end{pmatrix}$$

and block diagonal matrix

$$M = \begin{pmatrix} \ddots & & \\ & D_\sigma W & \\ & & \ddots \end{pmatrix}.$$

We then have $\mathbf{x} = M \cdot \mathbf{a}$. Now $\mathbf{x}$ is just a vector of all the entries of M_a and similarly $\mathbf{a}$ is just a vector of all the information symbols. Therefore $\sum_{\sigma,\tau} |\xi_{\sigma,\tau} a_\sigma^\tau|^2 =$

$\bar{\mathbf{x}}^t \cdot \mathbf{x} = \overline{(M\mathbf{a})}^t \cdot (M\mathbf{a})$. Hence satisfying the energy constraint is equivalent to asking that M is a unitary matrix. This in turn is equivalent to $D_\sigma W$ being unitary for all $\sigma \in G$.

Now if M is a unitary matrix then W must be a unitary matrix since $D_{\mathrm{Id}} = I_n$. This then implies that D_σ must be unitary for all $\sigma \in G$ since $(D_\sigma W) \cdot \overline{(D_\sigma W)}^t = D_\sigma W \bar{W}^t \bar{D_\sigma}^t$, which is equivalent to condition (1) above by the definition of D_σ. Conversely if conditions (1) and (2) hold then $D_\sigma W$ is a product of unitary matrices and hence is unitary, for all $\sigma \in G$. □

We now have two criteria that allow us to construct codes from crossed product algebras that satisfy the energy constraint. However, in reality finding an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ satisfying Condition 2 of Proposition 2.2.1 is a difficult problem. Therefore we make the extra assumption that complex conjugation commutes with every element of $Gal(L/K)$. This assumption then allows us to make use of the theory of ideal lattices in our constructions. To see this note that if we assume $Gal(L/K)$ commutes with complex conjugation, then $\overline{W}^t W = (\mathrm{Tr}_{L/K}(\bar{\omega}_\sigma \omega_\tau))_{\sigma,\tau}$ and hence W is a generator matrix of the hermitian $\mathcal{O}_K$-lattice (I, h), where $h(x, y) = \mathrm{Tr}_{L/K}(\bar{x}y)$. Therefore Condition 2 of Proposition 2.2.1 is satisfied if and only if the lattice (I, h) is isomorphic to the cubic lattice.

2.3 Complex Ideal Lattices

The aim of this section is to introduce a few basic definitions on ideal lattices and develop some results that will allow us to construct codes from crossed product algebras that satisfy the conditions of Proposition 2.2.1.

Now by the remark at the end of Section 2.2 we need to find a hermitian $\mathcal{O}_K$-lattice (I, h) with hermitian form:

$$h : I \times I \to \mathcal{O}_K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(\bar{x}y)$$

that is isomorphic to the cubic lattice. In order to give ourselves more chances of finding such a lattice, we introduce a scaling element $\lambda \in L$ and consider hermitian $\mathcal{O}_K$-lattices $(I, h_{\lambda,I})$ where $h_{\lambda,I}(x, y) = \mathrm{Tr}_{L/K}(\lambda \bar{x} y)$. However it is clear that such a λ will need to be chosen carefully. Since $Gal(L/K)$ commutes with complex conjugation, we take λ such that $\lambda = \bar{\lambda}$ so that $h_{\lambda,I}$ is a hermitian form. We now need to consider under what circumstances $h_{\lambda,I}(x, y) \in \mathcal{O}_K$.

Proposition 2.3.1. *Let $\mathcal{O}_K$ be a PID and L/K a finite extension of number fields where L is closed under the action of $^-$. Let $\lambda \in L^\times$ such that $\bar{\lambda} = \lambda$ and I be an ideal of $\mathcal{O}_L$. Then $\mathrm{Tr}_{L/K}(\lambda \bar{x} y) \in \mathcal{O}_K$ for all $x, y \in I$ if and only if $\lambda \bar{I} I \subseteq \mathcal{D}_{L/K}^{-1}$.*

Proof. Assume that $\lambda \bar{I} I \subseteq \mathcal{D}_{L/K}^{-1}$. Then $\mathrm{Tr}_{L/K}(\lambda \bar{x} y \mathcal{O}_L) \subseteq \mathcal{O}_K$ for all $x, y \in I$ and $m \in \mathcal{O}_L$. Hence $\mathrm{Tr}_{L/K}(\lambda \bar{x} y) \in \mathcal{O}_K$ for all $x, y \in I$ since $\mathcal{O}_L$ contains 1. Conversely let $\mathrm{Tr}_{L/K}(\lambda \bar{x} y) \in \mathcal{O}_K$ for all $x, y \in I$. Now $\bar{I} I$ is additively generated by elements of the form $\bar{x} y$, $x, y \in I$. Hence $\mathrm{Tr}_{L/K}(\lambda \bar{I} I \mathcal{O}_L) \subset \mathcal{O}_K$ so $\lambda \bar{I} I \subseteq \mathcal{D}_{L/K}^{-1}$. □

By the assumption that $\mathcal{O}_K$ is a PID, every ideal I of $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $n = [L : K]$. In particular, the following definition makes sense:

Definition 2.3.2. *Let K be a totally imaginary quadratic field and let L, λ and I be as in Proposition 2.3.1 and assume $\lambda \bar{I} I \subseteq \mathcal{D}_{L/K}^{-1}$. A **complex ideal lattice on** L/K is a hermitian $\mathcal{O}_K$-lattice $(I, h_{\lambda,I})$, where*

$$h_{\lambda,I} : I \times I \to \mathcal{O}_K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(\lambda \bar{x} y) \in \mathcal{O}_K, \ \ \forall x, y \in I.$$

Hence we need to search for complex ideal lattices $(I, h_{\lambda,I})$ that are isomorphic to the cubic lattice. As an aside we now introduce the **relative discriminant** of an extension L/K. In Section 2.4 we will show that this is closely linked to the minimum determinant of our codes.

Definition 2.3.3. *Let $(\mathcal{O}_L, h)$ be the hermitian $\mathcal{O}_K$-lattice, $h(x, y) = \mathrm{Tr}_{L/K}(\bar{x} y)$. We define the **relative discriminant** $\mathbf{d_{L/K}}$ as $d_{L/K} = |det(\mathcal{O}_L, h)|$, that is the absolute value of the determinant of $(\mathrm{Tr}_{L/K}(\bar{\omega}_i \omega_j))_{i,j}$, where $\omega_1, \ldots, \omega_n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.*

Recall how we distinguish between notation that we use for the **norm** of an ideal. We define $\mathrm{N}_{L/\mathbb{Q}}(I) := |\mathcal{O}_L / I|$ and $\mathcal{N}_{L/\mathbb{Q}}(I) := \mathrm{N}_{L/\mathbb{Q}}(I)\mathbb{Z}$, i.e. the ideal generated by the integer $\mathrm{N}_{L/\mathbb{Q}}(I)$.

Lemma 2.3.4. *We have $\mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = (d_{L/K})^2$.*

Proof. Let $Aut(L/K) = \sigma_1, \ldots, \sigma_n$. Define the matrix M as

$$M := \begin{pmatrix} \omega_1^{\sigma_1} & \ldots & \omega_n^{\sigma_1} \\ \vdots & \ddots & \vdots \\ \omega_1^{\sigma_n} & \ldots & \omega_n^{\sigma_n} \end{pmatrix}$$

We then have $d_{L/K} = |det(\bar{M}^t M)| = \overline{det(M)} \cdot det(M)$.

Now let d be any generator of the (principal) ideal $\mathfrak{d}_{L/K} = \mathcal{N}_{L/K}(\mathcal{D}_{L/K})$, then $d = det(\mathrm{Tr}_{L/K}(\omega_i \omega_j)) = (det(M))^2$. Therefore

$$\mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = \mathrm{N}_{K/\mathbb{Q}}(\mathcal{N}_{L/K}(\mathcal{D}_{L/K})) = \overline{(det(M))}^2 \cdot (det(M))^2.$$

Hence $\mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = (d_{L/K})^2$. □

Proposition 2.3.5. *Let $K \subset L \subset M$ be a tower of fields. Then*

$$(d_{M/K})^2 = \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{d}_{M/L}) \cdot (d_{L/K})^{2 \cdot [M:L]}.$$

Proof. By Lemma 2.3.4 $(d_{M/K})^2 = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K})$ and by the tower of discriminants formula we know that $\mathfrak{d}_{M/K} = \mathcal{N}_{L/K}(\mathfrak{d}_{M/L}) \cdot \mathfrak{d}_{L/K}^{[M:L]}$. Putting this into our equation we get

$$(d_{M/K})^2 = \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{d}_{M/L}) \cdot \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})^{[M:L]}.$$

To complete the proof we note that $(d_{L/K})^2 = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$ by Lemma 2.3.4. □

We now return to our task of finding lattices $(I, h_{\lambda,I})$ that are isomorphic to the cubic lattice. The cubic lattice is a positive definite lattice with determinant equal to 1, we therefore consider the determinant of $(I, h_{\lambda,I})$. For the rest of this section we fix a Galois extension L/K such that $\bar{L} = L$.

Proposition 2.3.6. *Let $(I, h_{\lambda,I})$ be a complex ideal lattice on L/K. Then*

$$det(I, h_{\lambda,I}) = \mathrm{N}_{L/K}(\lambda)\mathrm{N}_{L/\mathbb{Q}}(I) d_{L/K}.$$

Proof. Since $\mathcal{O}_K$ is a PID and I is an ideal of $\mathcal{O}_L$, it is a free $\mathcal{O}_K$-submodule of $\mathcal{O}_L$ and there exists an $\mathcal{O}_K$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_L$ and elements $q_1, \ldots, q_n \in \mathcal{O}_K$, such that $q_1\omega_1, \ldots, q_n\omega_n$ is an $\mathcal{O}_K$-basis for I [40].

Now $det(I, h_{\lambda,I})$ is by definition the determinant of the matrix

$$H := (h_{\lambda,I}(q_i\omega_i, q_j\omega_j))_{i,j}$$

that is

$$H = \begin{pmatrix} \mathrm{Tr}_{L/K}(\lambda\overline{q_1 w_1} q_1 w_1) & \ldots & \mathrm{Tr}_{L/K}(\lambda\overline{q_n w_n} q_1 w_1) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{L/K}(\lambda\overline{q_1 w_1} q_n w_n) & \ldots & \mathrm{Tr}_{L/K}(\lambda\overline{q_n w_n} q_n w_n) \end{pmatrix}.$$

Define $\mathcal{L}$ as the diagonal matrix

$$\mathcal{L} = \begin{pmatrix} \lambda^{\sigma_1} & & \\ & \ddots & \\ & & \lambda^{\sigma_n} \end{pmatrix}.$$

With M defined as in the proof of Lemma 2.3.4 we may then compute that

$$det(I, h_{\lambda,I}) = det(H) = det(\bar{M}^t \cdot \mathcal{L} \cdot M) \cdot \overline{q_1} \cdots \overline{q_n} \cdot q_1 \cdots q_n$$

since $q_j^{\sigma_i} = q_j$, for all i, j. Now

$$det(\bar{M}^t \cdot M) = \overline{det(M)} det(M) = d_{L/K}$$

by Lemma 2.3.4. Hence $det(\bar{M}^t \cdot \mathcal{L} \cdot M) = d_{L/K} \cdot \mathrm{N}_{L/K}(\lambda)$. To deal with the rest of our equation we first need to note that $\mathcal{O}_L = \bigoplus_{i=1}^n w_i \mathcal{O}_K$ and $I = \bigoplus_{i=1}^n q_i w_i \mathcal{O}_K$ [24]. We have an isomorphism of groups

$$\mathcal{O}_L / I \cong w_1 \mathcal{O}_K / q_1 w_1 \mathcal{O}_K \times \cdots \times w_n \mathcal{O}_K / q_n w_n \mathcal{O}_K$$

so the order of $\mathcal{O}_L / I$ is equal to the product of the orders of the cyclic subgroups. Now $|(\omega_i \mathcal{O}_K)/(q_i \omega_i \mathcal{O}_K)| = \bar{q}_i \cdot q_i$, so we can see that

$$|\mathcal{O}_L / I| = \mathrm{N}_{L/\mathbb{Q}}(I) = \bar{q}_1 \cdots \bar{q}_n \cdot q_1 \cdots q_n.$$

Hence

$$det(I, h_{\lambda,I}) = \mathrm{N}_{L/K}(\lambda) \mathrm{N}_{L/\mathbb{Q}}(I) d_{L/K}.$$

□

Corollary 2.3.7. *Let $(I, h_{\lambda,I})$ be a positive definite complex ideal lattice. Then*

$$det(I, h_{\lambda,I}) = 1 \text{ if and only if } \lambda \bar{I} I = \mathcal{D}_{L/K}^{-1}.$$

Proof. We know that $\lambda \bar{I} I \subseteq \mathcal{D}_{L/K}^{-1}$, therefore by Proposition 1.2.21 we know they are equal if and only if $\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{I} I) = \mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}^{-1})$. By Lemma 2.3.4 we know $\mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}^{-1}) = (1/d_{L/K})^2$ and since $Gal(L/K)$ commutes with $^-$ and $K/\mathbb{Q}$ is a totally imaginary quadratic extension, we have $\mathrm{N}_{L/\mathbb{Q}}(\bar{I}) = \mathrm{N}_{L/\mathbb{Q}}(I)$. Therefore $\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{I} I) = (\mathrm{N}_{L/K}(\lambda) \mathrm{N}_{L/\mathbb{Q}}(I))^2$ and we see that $\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{I} I) = \mathrm{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/K}^{-1})$ if and only if $\mathrm{N}_{L/K}(\lambda) \mathrm{N}_{L/\mathbb{Q}}(I) = \pm d_{L/K}^{-1}$, which happens if and only if $det(I, h_{\lambda,I}) = \pm 1$ by Proposition 2.3.6. Since our lattice is assumed to be positive definite, we see that $\lambda \bar{I} I = \mathcal{D}_{L/K}^{-1}$ if and only if $det(I, h_{\lambda,I}) = 1$. □

2.3.1 The Signature

In this section we consider the restriction that our lattice must be positive definite. We will show that this property is linked to the **signature** of our hermitian $\mathcal{O}_K$-lattice. We then introduce the **minimal distance** of a hermitian $\mathcal{O}_K$-lattice and give a minimum bound on the minimal distance of our complex ideal lattice that is linked to the relative discriminant.

Consider a hermitian $\mathcal{O}_K$-lattice (M, h). We can extend by scalars to get a hermitian form on $V = M \otimes_{\mathcal{O}_K} K$ over K, which by abuse of notation we will also call h. By considering V as a $\mathbb{Q}$-vector space we get a quadratic form

$$q_h : V \to \mathbb{Q}, \;\; v \mapsto h(v, v).$$

It is well known that a hermitian form $h : V \times V \to K$ can be diagonalised, i.e.

$$h \simeq < a_1, \ldots, a_n >, \; a_i \in \mathbb{Q}^{\times}.$$

Therefore, for $K = \mathbb{Q}(\sqrt{-z})$, $z \in \mathbb{Z}^+$ we have

$$q_h \simeq < 1, z > \otimes < a_1, \ldots, a_n > .$$

The **signature** of the quadratic form q_h is equal to the difference of the number of positive entries and the number of negative entries in its diagonalisation. This is independent of the choice of diagonalisation.

Definition 2.3.8. *The **signature** of a hermitian $\mathcal{O}_K$-lattice (M, h) is defined as*

$$sign((M, h)) = \frac{1}{2} sign(q_h) \in \mathbb{Z}.$$

Notice that

$$\text{sign}(M, h) = \#\{i \mid a_i > 0\} - \#\{i \mid a_i < 0\},$$

for any diagonalisation

$$h \simeq < a_1, \ldots, a_n >, \; a_i \in \mathbb{Q}^{\times}.$$

Consider an extension $E/\mathbb{Q}$. For each real embedding $\sigma : E \to \mathbb{R}$ of E, we define an ordering on E extending the ordering on $\mathbb{Q}$ by $x \geq_\sigma 0$ if $\sigma(x) \geq 0$ for $x \in E$. Every ordering of E extending the ordering of $\mathbb{Q}$ may be obtained this way. In the following, the notation $< \lambda >$ will denote the one-dimensional bilinear space with matrix (λ).

Theorem 2.3.9. *[33] Let (K, P) be an ordered field and L/K a finite extension. Then for every quadratic form ϕ over L*

$$sign_P(\mathrm{Tr}\phi) = \sum_{R \supset P} sign_R(\phi)$$

where the sum is taken over all extensions R of P. In particular, the number of extensions equals $sign_P(\mathrm{Tr} < 1 >)$.

Proof. We can assume that $\phi =< \alpha >$, for some $\alpha \in L$. Let F be a real closure of (K, P) and $E = F(\sqrt{-1})$. Then

$$\mathrm{sign}_P(\mathrm{Tr} < \alpha >) = \mathrm{sign}(\mathrm{Tr} < \alpha >)_F.$$

The underlying vector space of $(\mathrm{Tr} < \alpha >)_F$ is

$$L \otimes_K F = F \times \cdots \times F \times E \times \cdots \times E$$

with r factors F. This is an orthogonal decomposition. The factors E are hyperbolic planes Each factor F is positive or negative definite depending on whether α is positive or negative in the corresponding ordering and the extensions of P correspond exactly to the factors F. This gives the result. □

Proposition 2.3.10. *Let (I, h_λ) be a complex ideal lattice on L/K, and let $X(L) = \mathrm{Hom}_K(L, \mathbb{C})$. Then we have*

$$\mathrm{sign}(I, h_\lambda) = \#\{\sigma \in X(L) \mid \sigma(\lambda) > 0\} - \#\{\sigma \in X(L) \mid \sigma(\lambda) < 0\}.$$

In particular, (I, h_λ) is positive definite if and only if $\sigma(\lambda) > 0$ for every K-embedding $\sigma : L \to \mathbb{C}$.

Proof. We define two quadratic forms q_{λ,L_0} and $q'_{\lambda,L}$ by

$$q_{\lambda,L_0} : \begin{array}{l} L_0 \longrightarrow \mathbb{Q} \\ x \longmapsto \mathrm{Tr}_{L_0/\mathbb{Q}}(\lambda x^2) \end{array}$$

and

$$q'_{\lambda,L} : \begin{array}{l} L \longrightarrow \mathbb{Q} \\ x \longmapsto \mathrm{Tr}_{L/\mathbb{Q}}(\lambda \bar{x} x). \end{array}$$

Since $\lambda \bar{x} x \in L_0$ for all $x \in L$, we have

$$\mathrm{Tr}_{L/K}(\lambda \bar{x} x) = \mathrm{Tr}_{L_0/\mathbb{Q}}(\lambda \bar{x} x) \in \mathbb{Q}$$

and therefore

$$q_{h_\lambda}(x) = \mathrm{Tr}_{L/K}(\lambda \bar{x} x) = \frac{1}{2}\mathrm{Tr}_{L/\mathbb{Q}}(\lambda \bar{x} x) = \frac{1}{2} q'_{\lambda,L}(x)$$

for all $x \in L$. Hence, we have

$$\mathrm{sign}(I, h_\lambda) = \frac{1}{2}\mathrm{sign}(q'_{\lambda,L}).$$

It is straightforward to compute that

$$q'_{\lambda,L} \simeq < 1, z > \otimes q_{\lambda,L_0},$$

where $K = \mathbb{Q}(\sqrt{-z})$ and therefore

$$\mathrm{sign}(I, h_\lambda) = \mathrm{sign}(q_{\lambda,L_0}).$$

Set $X'(L_0) = \mathrm{Hom}_{\mathbb{Q}}(L_0, \mathbb{C})$. By Theorem 2.3.9, we get

$$\mathrm{sign}(I, h_\lambda) = \#\{\tau \in X'(L_0) \mid \tau(\lambda) > 0\} - \#\{\tau \in X'(L_0) \mid \tau(\lambda) < 0\}.$$

Taking into account that every K-embedding of L into $\mathbb{C}$ is extended from a $\mathbb{Q}$-embedding of L_0 into $\mathbb{C}$, we have the desired result. □

We briefly return to our codebook $\delta_{\min}(\mathcal{C}_{A,I})$ and explain how the scaling element λ affects the encoding. Recall from Equation 2.3 that we encode our n^2 information symbols as $(M_a)_{\rho,\tau} = \xi_{\rho\tau^{-1},\tau} a^{\tau}_{\rho\tau^{-1}}$. However to give ourselves more chances to find the cubic lattice, we would like to include the scaling element λ. Denote by D_λ the diagonal matrix with non-zero entries given by the real numbers $\sqrt{\lambda^\tau}, \tau \in G$. We now encode our n^2 information symbols into the matrix

$$M_a D_\lambda = (\sqrt{\lambda^\tau}\xi_{\rho\tau^{-1},\tau} a^{\tau}_{\rho\tau^{-1}})_{\rho,\tau}. \tag{2.5}$$

It is straightforward to see that for this encoding we simply replace W by $W_\lambda := D_\lambda W$ in Proposition 2.2.1 and that $\overline{W_\lambda}^t W_\lambda = (\mathrm{Tr}_{L/K}(\lambda \bar{\omega_\sigma} \omega_\tau))_{\sigma,\tau}$. We then set

$$\mathcal{C}_{A,\lambda,I} = \{M_a D_\lambda | a \in \Gamma_{A,I}\}. \tag{2.6}$$

Now $\delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \mathrm{N}_{L/K}(\lambda) \cdot \delta_{\min}(\mathcal{C}_{A,I})$ and $\mathrm{N}_{L/K}(\lambda)$ is a positive real number. Hence $\delta_{\min}(\mathcal{C}_{A,\lambda,I})$ is bounded below by a positive constant as well. The rest of this section is concerned with providing a necessary condition for our lattice $(I, h_{\lambda,I})$ to be isomorphic to the cubic lattice.

Let (M, h) be a hermitian $\mathcal{O}_K$-lattice with K a quadratic imaginary field. Then for any $x \in M$ we see that $h(x, x) \in \mathbb{Z}$.

Definition 2.3.11. *Let (M, h) be as above. The **minimal distance** of (M, h) is defined as*

$$d(M, h) = \min_{x \in M \setminus \{0\}} |h(x, x)|.$$

Consider our complex ideal lattice $(I, h_{\lambda,I})$. It is clear that if $(I, h_{\lambda,I})$ is isomorphic to the cubic lattice, then $d(I, h_{\lambda,I}) = 1$. We therefore look to give a minimum bound on $h_{\lambda,I}(x, x)$ for a lattice $(I, h_{\lambda,I})$.

Lemma 2.3.12. *Let $(I, h_{\lambda,I})$ be a complex ideal lattice on L/K. Assume that $\sigma(\lambda)$ is real and positive for all embeddings σ of L_0. Define the hermitian form $h_{\lambda,I}$ by $h_{\lambda,I}(x, y) = \mathrm{Tr}_{L/K}(\lambda \bar{x} y)$. Then*

$$h_{\lambda,I}(x, x) \geq n \cdot (\mathrm{N}_{L/K}(\lambda)\mathrm{N}_{L/\mathbb{Q}}(I))^{1/n}$$

for all $x \in I$, $x \neq 0$.

Proof. We know that $\sigma_i(\lambda)$ is a positive real number for all i. Furthermore since σ commutes with complex conjugation we can say that $\sigma_i(\bar{x}x)$ is a positive real number for all $x \in I$. Hence we can use the inequality between the geometric and arithmetic mean to say

$$\mathrm{Tr}_{L/K}(\lambda \bar{x} x)/n \geq \mathrm{N}_{L/K}(\lambda \bar{x} x)^{1/n}.$$

Now if $\mathfrak{a} \subseteq \mathfrak{b}$ for any two non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$, then by Proposition 1.2.21 $\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{b})|\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{a})$. Since $(\lambda \bar{x} x) \subseteq \lambda \bar{I} I$ we have that $\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{I} I)|\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{x} x)$. By our assumptions on λ and $Gal(L/K)$ we see that

$$\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{x} x) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{L/K}(\lambda \bar{x} x)) = (\mathrm{N}_{L/K}(\lambda \bar{x} x))^2.$$

Furthermore we know that $\mathrm{N}_{L/\mathbb{Q}}(\lambda \bar{I} I) = (\mathrm{N}_{L/K}(\lambda)\mathrm{N}_{L/\mathbb{Q}}(I))^2$. Hence

$$(\mathrm{N}_{L/K}(\lambda)\mathrm{N}_{L/\mathbb{Q}}(I))^2 | (\mathrm{N}_{L/K}(\lambda \bar{x} x))^2$$

so

$$h_{\lambda,I}(x, x) \geq n \cdot \mathrm{N}_{L/K}(\lambda \bar{x} x)^{1/n} \geq n \cdot (\mathrm{N}_{L/K}(\lambda)\mathrm{N}_{L/\mathbb{Q}}(I))^{1/n}$$

for all $x \in I$, $x \neq 0$. □

Corollary 2.3.13. *Let $(I, h_{\lambda,I})$ be a positive definite complex ideal lattice on L/K of determinant* 1*. Then we have*

$$h_{\lambda,I}(x,x) \geq n \cdot d_{L/K}^{-1/n}$$

for all $x \in I$, $x \neq 0$.

Proof. Since the determinant of $(I, h_{\lambda,I})$ is equal to 1 we see by Corollary 2.3.7 that $\lambda \bar{I} I = \mathcal{D}_{L/K}^{-1}$. The result then follows by Lemma 2.3.4. □

Corollary 2.3.14. *Let $(I, h_{\lambda,I})$ be a positive definite complex ideal lattice on L/K. If $(I, h_{\lambda,I})$ is isomorphic to the cubic lattice then $d_{L/K} \geq n^n$.*

Proof. If it was possible to construct the cubic lattice then there must exist some element $x \in I$ such that $h_{\lambda,I}(x,x) = 1$. Rearranging the inequality in Corollary 2.3.13 then gives the result. □

2.4 Minimum Determinant

In [29] the authors derive certain bounds on the minimum determinant of perfect codes based on cyclic division algebras. We extend these results to the more general setting of crossed product algebras.

Let $(I, h_{\lambda,I})$ be a positive definite complex ideal lattice on L/K of determinant 1. We encode our n^2 information symbols $(a_{\sigma,\tau})_{\sigma,\tau \in G}$ into the matrix

$$X_a := M_a D_\lambda = (\sqrt{\lambda^\tau} \xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau}$$

where $a_\sigma = \sum_{\tau \in G} a_{\sigma,\tau} \omega_\tau$ for all $\sigma \in G$.

Definition 2.4.1. *Define an ideal of $\mathcal{O}_K$ as follows:*

$$\{x \in \mathcal{O}_K | x \cdot \xi_{\sigma,\tau} \in \mathcal{O}_L \quad for\ all\ \sigma, \tau \in G\}. \tag{2.7}$$

Let c be a generator of this (principal) ideal, which is in fact a common denominator of the cocycle values $\xi_{\sigma,\tau}$ and define $\mathbf{\Delta}_\xi := \mathrm{N}_{K/\mathbb{Q}}(c) = |c|^2$. This is independent of the choice of generator, since the norm of a unit is 1*. We also define $c^{(m)}$ to be the common denominator of the cocycle values $\xi_{\sigma,\tau}$ in the m^{th} row of the matrix M_a, with corresponding $\mathbf{\Delta}_\xi^{(\mathbf{m})}$.*

Proposition 2.4.2. *For the codebook $\mathcal{C}_{A,\lambda,I}$ we have*

$$\delta_{min}(\mathcal{C}_{A,\lambda,I}) \in \frac{1}{d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \mathbb{Z}^{+}.$$

Proof. Since $c^{(m)}$ is a common denominator of the cocycle values $\xi_{\sigma,\tau}$ in the m^{th} row of M_a we have

$$det(X_a) = \frac{1}{\prod_{m=1}^{n} c^{(m)}} \cdot det(M'_a) \cdot det(D_\lambda)$$

where the (σ,τ)th coefficient of M'_a is given by

$$\xi'_{\sigma\tau^{-1},\tau} \tau^{-1}(a_{\sigma\tau^{-1}}) \tag{2.8}$$

and $\xi'_{\sigma\tau^{-1},\tau} \in \mathcal{O}_L$ for all $\sigma, \tau \in G$. It is clear that $det(D_\lambda) = \sqrt{\mathrm{N}_{L/K}(\lambda)}$ so we must consider $det(M'_a)$. By (2.8) we can see that the (σ,τ)th coefficient of M'_a lies in I^{τ}, hence

$$det(M'_a) \in \prod_{\tau \in G} I^{\tau} = \mathcal{N}_{L/K}(I)\mathcal{O}_L.$$

However $det(M_a)$ is also the reduced norm of a and therefore $det(M'_a) \in \mathcal{O}_K$, which implies $det(M'_a) \in \mathcal{N}_{L/K}(I)\mathcal{O}_L \cap \mathcal{O}_K = \mathcal{N}_{L/K}(I)$. Therefore

$$det(X_a) \in \frac{\sqrt{\mathrm{N}_{L/K}(\lambda)}}{\prod_{m=1}^{n} c^{(m)}} \mathcal{N}_{L/K}(I).$$

By the assumption that $\lambda^{\sigma} > 0$ for all $\sigma \in G$ we see that

$$|det(X_a)|^2 \in \frac{\mathrm{N}_{K/\mathbb{Q}}(\mathcal{N}_{L/K}(I))}{\prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \cdot \mathrm{N}_{L/K}(\lambda)\mathbb{Z}^{+}.$$

and by the transitivity of the norm in a tower of fields we have

$$|det(X_a)|^2 \in \frac{\mathrm{N}_{L/\mathbb{Q}}(I)}{\prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \cdot \mathrm{N}_{L/K}(\lambda)\mathbb{Z}^{+}.$$

Then by the assumption that $\lambda \bar{I} I = \mathcal{D}_{L/K}^{-1}$ (since $det(I, h)$ is assumed to be 1) we may see that

$$\delta_{min}(\mathcal{C}_{A,\lambda,I}) \in \frac{1}{d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \mathbb{Z}^{+}. \tag{2.9}$$

□

Corollary 2.4.3. *We have the following bounds on the minimum determinant:*

$$\frac{1}{d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \leq \delta_{min}(\mathcal{C}_{A,\lambda,I}) \leq \min_{x \in I \setminus \{0\}} \mathrm{N}_{L/\mathbb{Q}}(x) \cdot \mathrm{N}_{L/K}(\lambda).$$

where the upper and lower bounds coincide if I is principal and $\prod_{m=1}^{n} \Delta_{\xi}^{(m)} = 1$.

Proof. As seen above our matrix $\mathbf{X}_a$ is given by

$$(\mathbf{X}_a)_{\rho,\tau} = (M_a D_\lambda)_{\rho,\tau} = \sqrt{\lambda^\tau} \xi_{\rho\tau^{-1},\tau} a^\tau_{\rho\tau^{-1}}.$$

The lower bound is clear from Proposition 2.4.2. Now if we take a defined by $a_{\mathrm{Id}} = x \in I$ and $a_\sigma = 0$ for $\sigma \neq \mathrm{Id} \in G$, then we may compute that $\mathrm{N}_{L/K}(x) \cdot \sqrt{\mathrm{N}_{L/K}(\lambda)}$ is the determinant of the matrix $\mathbf{X}_a$. Therefore

$$\delta_{min}(\mathcal{C}_{A,\lambda,I}) \not> \min_{x \in I \setminus \{0\}} |\mathrm{N}_{L/K}(x) \cdot \sqrt{\mathrm{N}_{L/K}(\lambda)}|^2 = \min_{x \in I \setminus \{0\}} \mathrm{N}_{L/\mathbb{Q}}(x) \cdot \mathrm{N}_{L/K}(\lambda).$$

In the case where $I = (\alpha)\mathcal{O}_L$ is a principal ideal of $\mathcal{O}_L$, any element $x \in I$ may be written $x = \alpha \cdot y$ for $y \in \mathcal{O}_L$. Hence, by taking $y = 1$ we see that $\min_{x \in I \setminus \{0\}} \mathrm{N}_{L/\mathbb{Q}}(x) = \mathrm{N}_{L/\mathbb{Q}}(\alpha)$. Now by the proof of Corollary 2.3.7 we know $\mathrm{N}_{L/\mathbb{Q}}(\alpha) \cdot \mathrm{N}_{L/K}(\lambda) = d_{L/K}^{-1}$, which gives us our equality when $\prod_{m=1}^{n} \Delta_{\xi}^{(m)} = 1$. $\square$

Consider the case of a non-principal ideal I and let $x \in I$ be some element of minimal norm. It is clear that the ideal $x\mathcal{O}_L \subset I$ and hence by the third isomorphism theorem we see

$$(\mathcal{O}_L / x\mathcal{O}_L)/(I/x\mathcal{O}_L) \simeq \mathcal{O}_L / I.$$

Therefore $\min_{x \in I \setminus \{0\}} \mathrm{N}_{L/\mathbb{Q}}(x) = \mathrm{N}_{L/\mathbb{Q}}(I) \cdot [I : x\mathcal{O}_L]$ and we can rewrite the inequality from Corollary 2.4.3 as

$$\frac{1}{d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}} \leq \delta_{min}(\mathcal{C}_{A,\lambda,I}) \leq \frac{[I : x\mathcal{O}_L]}{d_{L/K}}.$$

We therefore see that maximising $\delta_{\min}(\mathcal{C}_{A,\lambda,I})$ relies upon minimising $d_{L/K}$. The lower bound also tells us that taking $\xi_{\sigma,\tau} \in \mathcal{O}_L$ for all $\sigma, \tau \in G$ could increase our chances of having a code with good performance.

Chapter 3

Codes Based on Cyclic Algebras

A great deal of research has concentrated on constructing space-time block codes from cyclic division algebras. For example the well known Alamouti code was introduced in [1] and in [41] the authors consider a generalisation of the Alamouti code using orthogonal designs. In [35] it is shown that the Alamouti code can be viewed as a code based on a cyclic division algebra.

Cyclic division algebras were also investigated in [36] where the authors present constructions of STBCs using Brauer's division algebras. This work was extended in [34] and examples of STBCs based on cyclic division algebras constructed from n^{th} roots of transcendental elements were given. A family of 2×2 STBCs was introduced in [2] and further constructions of codes based on cyclic division algebras were presented in [38]. In [37] the authors give constructions based on crossed product algebras that include the codes from this paragraph as special cases.

The celebrated **golden code** [3] is a 2×2 STBC based on a cyclic division $\mathbb{Q}(i)$-algebra $(\gamma, L/\mathbb{Q}(i), \sigma)$ that satisfies the properties discussed in the previous chapters, i.e. fully diverse, a non-vanishing determinant and satisfying the energy constraint. It is the first example of a **perfect** STBC, see Section 3.1. A code equivalent to the golden code was presented independently in [9] and [47]. The algebraic construction in [3] was generalised to an infinite family of codes in the 2×2 case in [29]. The authors also gave a construction of a perfect STBC in the 3×3, 4×4 and 6×6 cases. In the 3×3 and 6×6 cases the base field in the cyclic division K-algebra $(\gamma, L/K, \sigma)$ was taken to be $\mathbb{Q}(j)$. An important assumption made in [29] is that we take γ to be a root of unity and it is shown in [5] that under

this assumption perfect STBCs can only exist in dimension $2, 3, 4$ and 6. However if this assumption is dropped and we take $\gamma \in K$, then perfect codes exist for any number n_t of transmit antennas and any number n_r of receive antennas [11].

In this thesis we will largely be interested in the perfect constructions given in [29]. Since cyclic algebras are also crossed product algebras, encoding our information can be done using the method explained in Section 2.2. Let us first compute the matrix of left multiplication for an arbitrary element $a \in A$, where A is a cyclic division K-algebra $(\gamma, L/K, \sigma)$. Recall a cyclic K-algebra is a crossed product K-algebra $(\xi^{\sigma,\gamma}, L/K, \sigma) = 1 \cdot L \oplus e \cdot L \oplus \cdots \oplus e^{n-1} \cdot L$, where the 2-cocycles satisfy

$$\xi^{\sigma,\gamma}_{\sigma^i,\sigma^j} = \begin{cases} 1 & if\ i+j < n \\ \gamma & if\ i+j \geq n \end{cases}$$

and $e^n = \gamma$. Our element $a \in A$ can be written as $a = a_0 + ea_1 + \cdots + e^{n-1}a_{n-1}$, $a_i \in L, i = 0, \ldots, n-1$. We then compute the matrix of left multiplication as

$$M_a = \begin{pmatrix} a_0 & \gamma a_{n-1}^{\sigma} & \gamma a_{n-2}^{\sigma^2} & \ldots & \gamma a_1^{\sigma^{n-1}} \\ a_1 & a_0^{\sigma} & \gamma a_{n-1}^{\sigma^2} & \ldots & \gamma a_2^{\sigma^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-2} & a_{n-3}^{\sigma} & a_{n-4}^{\sigma^2} & \ldots & \gamma a_{n-1}^{\sigma^{n-1}} \\ a_{n-1} & a_{n-2}^{\sigma} & a_{n-3}^{\sigma^2} & \ldots & a_0^{\sigma^{n-1}} \end{pmatrix} \tag{3.1}$$

where

$$a_i = \sum_{j=1}^{n} a_{ij} w_j, i = 1, \ldots, n.$$

Hence for a given cyclic division K-algebra A we would take as our codebook $\mathcal{C}$ a subset of the set $\{M_a | a \in A\}$.

Let us consider the bounds on the minimum determinant if we don't restrict to the case $\gamma \in \mathcal{O}_K$. In this case we can write γ as the reduced fraction γ_1/γ_2 with $\gamma_1, \gamma_2 \in \mathcal{O}_K$. The bound given in Corollary 2.4.3 then becomes

$$\frac{1}{d_{L/K} \cdot |\gamma_2|^{2(n-1)}} \leq \delta_{min}(\mathcal{C}_{A,\lambda,I}) \leq \min_{x \in I \setminus \{0\}} \mathrm{N}_{L/\mathbb{Q}}(x) \cdot \mathrm{N}_{L/K}(\lambda).$$

3.1 Perfect STBCs

In this thesis we will be concerned with **linear dispersion** STBCs. The basic idea of a linear dispersion code is to spread the information symbols linearly over space

and time. For more details see [17].

Definition 3.1.1. *A square $n \times n$ STBC is called **perfect** if and only if*

- *It is a full rate linear dispersion code using n^2 information symbols, either QAM of HEX.*
- *The minimum determinant of the infinite code is bounded away from zero.*
- *The energy required to send the linear combination of the information symbols on each layer is similar to the energy used for sending the symbols themselves, i.e. we do not increase the energy of the system by encoding the information symbols.*
- *It induces uniform average transmitted energy per antenna in all T time slots.*

Let us now summarise the approach taken in [29] to construct perfect STBCs. We can see from Equation 3.1 that by using a cyclic division K-algebra $(\gamma, L/K, \sigma)$ our code will be full rate, since there are n^2 information symbols a_{ij} in each codeword M_a. As seen in Section 2.1 the second criterion above can be achieved by restricting our elements $a \in A$ to some order Γ of A. The third property of a PSTBC is that the energy constraint must be satisfied. By Proposition 2.2.1 this is satisfied if and only if $|\gamma|^2 = 1$ and the complex ideal lattice $(I, h_{\lambda,I})$ is isomorphic to the cubic lattice. The authors in [29] also restrict to the case $\gamma \in \mathcal{O}_K$, which implies γ must be a unit in $\mathcal{O}_K$. We now come to the final criterion that our code induces uniform average power in all time slots. However, this is necessarily satisfied by the shaping constraint that is required for the third criterion, for details see [28].

3.1.1 2×2 case

In the 2×2 case we consider the transmission of QAM symbols so we take $K = \mathbb{Q}(i)$. Let $A = (\gamma, L/K, \sigma)$ be a cyclic K-algebra, where $L = K(\sqrt{p})$ for some prime number p. We will see in Section 3.2.1 that if we take $\gamma = i$ and $p \equiv 5 \pmod 8$ then A is a cyclic division K-algebra.

It is easy to show that for $L = K(\sqrt{p})$ with $p \equiv 1 \pmod 4$ the prime p decomposes as

$$(p)\mathcal{O}_L = \mathfrak{P}^2 \cdot \bar{\mathfrak{P}}^2.$$

for some prime ideal $\mathfrak{P} \subset \mathcal{O}_L$. This is because any such prime p splits in $K/\mathbb{Q}$ but must ramify in the quadratic extension $L_0/\mathbb{Q}$, where $L_0 := L \cap \mathbb{R}$. In [29] the authors show that in this case there always exists a hermitian $\mathcal{O}_K$-lattice $(\mathfrak{P}, h_{\lambda,\mathfrak{P}})$ that is isomorphic to the cubic lattice.

Consider the case when $p = 5$. Define $\theta = \frac{1+\sqrt{p}}{2}$, $\bar{\theta} = \frac{1-\sqrt{p}}{2}$, $\alpha = 1 + i - i\theta$ and $\bar{\alpha} = 1 + i - i\bar{\theta}$. The ideal $\mathfrak{P}$ is principal and generated by the element α. The codebook then has codewords of the form

$$\mathbf{X} = \frac{1}{\sqrt{p}} \begin{pmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ i\bar{\alpha}(c + d\theta) & \bar{\alpha}(a + b\bar{\theta}) \end{pmatrix}, \; a, b, c, d \in \mathbb{Z}[i].$$

The generator matrix of the lattice is then given by

$$R = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta \\ \bar{\alpha} & \overline{\alpha\theta} \end{pmatrix}.$$

This is a unitary matrix

It is then a straightforward computation to explicitly show that the minimum determinant of the code is given by

$$\delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{d_{L/K}} = \frac{1}{5}.$$

This example is known as the golden code. The name golden code relates to the appearance of the golden ratio as the element θ. It is shown in [27] that the golden code is the optimum perfect STBC in dimension 2.

3.1.2 3×3 case

In the 3×3 case we consider the transmission of HEX symbols so we take $K = \mathbb{Q}(j)$. Let $\theta = \zeta_7 + \zeta_7^{-1}$ and $L = K(\theta)$, we then have $[L : K] = 3$ and $d_{L/K} = 49$. This extension is cyclic with generator $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$ and the cyclic K-algebra $A = (j, L/K, \sigma)$ is a division K-algebra.

The prime ideal generated by 7 factors as

$$(7)\mathcal{O}_L = \mathfrak{P}^3 \cdot \bar{\mathfrak{P}}^3.$$

Furthermore $\mathfrak{P}$ is principal and generated by the element $\alpha = (1 + j) + \theta$. A $\mathbb{Z}[j]$-basis of $(\alpha)\mathcal{O}_L$ is computed as $\{\alpha\theta^k\}_{k=0}^2$. The authors perform a change of

basis using the matrix

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

to get a reduced $\mathbb{Z}[j]$-basis

$$\{v_k\}_{k=1}^3 = \{(1+j)+\theta, (-1-2j)+j\theta^2, (-1-2j)+(1+j)\theta+(1+j)\theta^2\}.$$

The generator matrix is given numerically as

$$R = \begin{pmatrix} 0.660+0.327i & 0.021+0.327i & -0.492+0.327i \\ -0.294-0.146i & -0.037-0.589i & -0.614+0.408i \\ 0.530+0.262i & -0.047-0.736i & 0.273-0.182i \end{pmatrix}.$$

This is a unitary matrix so the construction above gives a perfect STBC. Since the ideal $\mathfrak{P}$ is principal we see that

$$\delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{49}. \tag{3.2}$$

3.1.3 4×4 case

In the 4×4 case we consider the transmission of QAM symbols so we take $K = \mathbb{Q}(i)$. Let $\theta = \zeta_{15} + \zeta_{15}^{-1}$ and $L = K(\theta)$, we then have $[L : K] = 4$ and $d_{L/K} = 1125$. This extension is cyclic with generator $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$ and the cyclic K-algebra $A = (i, L/K, \sigma)$ is a division K-algebra.

The prime ideals generated by 3 and 5 have the factorisations

$$(3)\mathcal{O}_L = \mathfrak{P}_3^2 \cdot \overline{\mathfrak{P}_3}^2$$
$$(5)\mathcal{O}_L = \mathfrak{P}_5^4 \cdot \overline{\mathfrak{P}_5}^4$$

and the ideal $\mathfrak{P}_3 \cdot \mathfrak{P}_5$ is a principal ideal generated by $\alpha = (1-3i) + i\theta^2$.

A $\mathbb{Z}[i]$-basis of (α) is given by $\{\alpha\theta^k\}_{k=0}^3$. When we apply a change of basis using the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix}$$

we get a new $\mathbb{Z}[i]$-basis

$$\{v_k\}_{k=1}^4 = \{(1-3i) + i\theta^2, (1-3i) + i\theta^3, -i + (-3+4i)\theta + (1-i)\theta^3, \\ (-1+i) - 3\theta + \theta^2 + \theta^3\}.$$

The generator matrix is given numerically as

$$R = \begin{pmatrix} 0.258 - 0.312i & 0.345 - 0.481i & -0.418 + 0.505i & -0.214 + 0.258i \\ 0.258 + 0.087i & 0.472 + 0.160i & 0.160 + 0.054i & 0.764 + 0.258i \\ 0.258 + 0.214i & -0.505 - 0.418i & -0.418 - 0.345i & 0.312 + 0.258i \\ 0.258 - 0.763i & -0.054 + 0.160i & 0.160 - 0.472i & -0.087 + 0.258i \end{pmatrix}.$$

This is a unitary matrix so the construction above gives a perfect STBC. Since the ideal $\mathfrak{P}_3 \cdot \mathfrak{P}_5$ is principal we see that

$$\delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{1125}. \tag{3.3}$$

3.1.4 6×6 case

In the 6×6 case we again consider the transmission of HEX symbols so we take $K = \mathbb{Q}(j)$. Let $\theta = \zeta_{28} + \zeta_{28}^{-1}$ and $L = K(\theta)$, we then have $[L : K] = 6$ and $d_{L/K} = 2^6 \cdot 7^5$. This extension is cyclic and we can take as generator $\sigma : \zeta_{28} + \zeta_{28}^{-1} \mapsto \zeta_{28}^5 + \zeta_{28}^{-5}$ [45]. Furthermore the cyclic K-algebra $A = (-j, K(\zeta_{28} + \zeta_{28}^{-1})/K, \sigma)$ is a division K-algebra.

The prime ideal generated by 7 factors as

$$(7)\mathcal{O}_L = \mathfrak{P}_7^6 \overline{\mathfrak{P}_7}^6.$$

However the difference in this case is that the ideal $\mathfrak{P}$ is not principal, therefore we will only be able to give bounds on the minimum determinant. In order to show that perfect code can be constructed from A the authors needed to show that it was possible to have a unitary generator matrix. To do this they first computed a relative basis of $\mathfrak{P}$ and then used this to compute a Gram matrix of the lattice. In [26] a generalisation of the LLL algorithm [25] is given that works over $\mathbb{Z}[j]$. By employing this generalisation, the following change of basis matrix can be

computed

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1+j & 0 & 1 & 0 & 0 & 0 \\ -1-2j & 0 & -5 & 0 & 1 & 0 \\ 1+j & 0 & 4 & 0 & -1 & 0 \\ 0 & -3 & 0 & 1 & 0 & 0 \\ 0 & 5 & 0 & -5 & 0 & 1 \end{pmatrix}.$$

The generator matrix is then given numerically as

$$R = \frac{1}{\sqrt{14}} \begin{pmatrix} 1.950 & 1.302-0.866i & -0.055-0.866i & -1.747-0.866i & 1.564 & 0.868 \\ 0.868 & -1.747-0.866i & 1.302-0.866i & -0.055-0.866i & -1.950 & 1.564 \\ 1.564 & -0.055-0.866i & -1.747-0.866i & 1.302-0.866i & -0.868 & -1.950 \\ -1.950 & 1.302-0.866i & -0.055-0.866i & -1.747-0.866i & -1.564 & -0.868 \\ -0.868 & -1.747-0.866i & 1.302-0.866i & -0.055-0.866i & 1.950 & -1.564 \\ -1.564 & -0.055-0.866i & -1.747-0.866i & 1.302-0.866i & 0.868 & 1.950 \end{pmatrix}.$$

Finally bounds on the minimum determinant are given by

$$\frac{1}{2^6 \cdot 7^5} \leq \delta_{\min}(\mathcal{C}_{A,\lambda,I}) \leq \frac{1}{2^6 \cdot 7^4}. \tag{3.4}$$

3.2 Optimum Cyclic Constructions

In this Section we will look at the optimality of perfect STBCs in dimensions 4 and 6. We will always assume that our base field K is equal to $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$. First let us specify exactly what we mean by optimal. Recall that to reduce the pairwise probability of error we must look to maximise the minimum determinant $\delta_{\min}(\mathcal{C})$. Now for any $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ we have $\delta_{\min}(\mathcal{C}) \geq \delta_{\min}(\mathcal{C}_{A,\lambda,I})$ so by Corollary 2.4.3 we have

$$\frac{1}{\delta_{min}(\mathcal{C})} \leq d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}.$$

We can then say that a perfect STBC of dimension n is **optimal** if its value for $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)}$ is minimal within the class of perfect STBCs of dimension n. Note that we could assume that our ideal $I \subset \mathcal{O}$ for some order $\mathcal{O}$ of L that doesn't equal $\mathcal{O}_L$. However in this case a number of assumptions, such as the transitivity of the norm in towers, can no longer be taken. We will therefore always assume that our order is the ring of integers $\mathcal{O}_L$ and that $I \subset \mathcal{O}_L$.

Initially we will assume that $\gamma \in \mathcal{O}_K$ and therefore we need to find the minimal possible value for $d_{L/K}$. Our method for determining this is broken into 3 steps:

1. We give a necessary and sufficient condition for $A = (\gamma, L/K, \sigma)$ to be a division K-algebra.

2. We list all extensions that satisfy Step 1 above and for which $d_{L/K}$ is less than the value of $d_{L/K}$ for the best known extension.

3. We determine if it is possible to construct the cubic lattice from the remaining cyclic division K-algebras.

To complete our search for the optimal PSTBC we will then consider the case $\gamma \notin \mathcal{O}_K$.

We end this section with two results that will help us to complete Step 1 above. First note that our extension L is of the form $K(\sqrt[n]{d})$ for some $d \in K$, where $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$. We are able to assume that $d \in \mathcal{O}_K$ by multiplying by a suitable n^{th} power in K. Recall from Section 2.2 that we also assume that $Gal(L/K)$ commutes with complex conjugation. Note that both K and L are closed under complex conjugation.

Lemma 3.2.1. *Assume $\zeta_n \in K$ and let $L = K(\sqrt[n]{d})$. Let σ be a generator of the Galois group* $\mathrm{Gal}(L/K)$. *Then σ commutes with complex conjugation if and only if $\bar{d} \cdot d \in K^n$.*

Proof. The first thing to point out is that $\zeta_n = \bar{\zeta_n}^{-1}$. We now assume that σ commutes with complex conjugation and that $\alpha = \sqrt[n]{d}$. Direct computation then shows that $\sigma(\bar{\alpha}\alpha) = \overline{\zeta_n \alpha} \cdot \zeta_n \alpha = \zeta_n^{-1} \bar{\alpha} \zeta_n \alpha = \bar{\alpha}\alpha$. Therefore $\bar{\alpha}\alpha \in K$ and hence $(\bar{\alpha}\alpha)^n = \bar{d}d \in K^n$. The converse starts with the assumption that $\bar{d}d = (\bar{\alpha}\alpha)^n = x^n$, for some $x \in K$. So $\bar{\alpha} = x'/\alpha$ for some $x' \in \{\zeta_n^i x\}$. Direct computation gives $\sigma(\bar{\alpha}) = x'/\zeta_n \alpha = \bar{\alpha}/\zeta_n = \overline{\zeta_n \alpha} = \overline{\sigma(\alpha)}$, which completes the proof. □

For the rest of this chapter we will only consider cyclic algebras of degree 4 or 6 with base field $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$ respectively. We first describe the prime elements of the principal ideal domain $\mathcal{O}_K$ for $K = \mathbb{Q}(i)$ (respectively $K = \mathbb{Q}(j)$). In both cases there are four different types:

1. A special prime $\pi = 1 - i$ (respectively $\pi = 1 - j$). The conjugate $\bar{\pi}$ of such a prime π is associate to π and in fact

$$\pi = \bar{\pi} \cdot u_1$$

$$\bar{\pi} = \pi \cdot u_2$$

where u_1 and u_2 are primitive 4^{th} (respectively 6^{th}) roots of unity.

2. The inert primes of the form $p \equiv 3 \pmod 4$ (respectively $p \equiv 2 \pmod 3$), where p is a prime integer. We will denote this set by S_3 (respectively T_2).

3. Prime elements of the form $\pi = a + bi$ (respectively $\pi = a + bj$) with $0 < a < b$, where $a^2 + b^2 = p_\pi \equiv 1 \pmod 4$ (respectively $a^2 + b^2 - ab \equiv 1 \pmod 3$), where p_π is a prime integer. We will denote this set by S_1 (respectively T_1).

4. Conjugates of the prime elements π in S_1 (respectively T_1), namely $\bar{\pi} = a - bi$ (respectively $\bar{\pi} = a + bj^2$).

Proposition 3.2.2. *Let $d \in \mathcal{O}_K$ with $d \neq 0$ and assume that d is not divisible by any 4^{th} (respectively 6^{th}) power of $\mathcal{O}_K$. Then $\bar{d} \cdot d \in K^n$, where $n = 4$ (respectively $n = 6$), if and only if the following hold:*

1. *The valuation $v_\pi(d)$ at the special prime ideal (π) is 0.*

2. *The valuation $v_\pi(d)$ at a prime ideal (π) generated by a prime $\pi \in S_3$ (respectively T_2) is 0 or 2 (respectively 0 or 3).*

3. *The sum of the valuation $v_\pi(d)$ at a prime ideal (π) generated by a prime $\pi \in S_1$ (respectively T_1) and the valuation $v_{\bar{\pi}}(d)$ at its conjugate $\bar{\pi}$ is equal to 0 or 4 (respectively 0 or 6).*

Proof. Consider the prime decomposition $d = \pi_1^{l_1} \cdots \pi_r^{l_r} \cdot \mu$ for some unit $\mu \in \mathcal{O}_K$. Then $\bar{d} \cdot d \in K^n$ if and only if $(\pi_1^{l_1} \cdots \pi_r^{l_r}) \cdot \overline{(\pi_1^{l_1} \cdots \pi_r^{l_r})} \in K^n$. Note the disappearance of the units, since $\bar{\mu} \cdot \mu = 1$. Now $(\pi_1^{l_1} \cdots \pi_r^{l_r}) \cdot \overline{(\pi_1^{l_1} \cdots \pi_r^{l_r})} \in K^n$ if and only if $(\pi_1 \cdot \overline{\pi_1})^{l_1} \cdots (\pi_r \cdot \overline{\pi_r})^{l_r} \in K^n$

We first look at the special prime $\pi_k = 1 - i$ (respectively $\pi_k = 1 - j$). In this case $\pi_k \cdot \overline{\pi_k} = \pi_k^2 \cdot u$ where u is a primitive 4^{th} (respectively 6^{th}) root of unity. Therefore $(\pi_k \cdot \overline{\pi_k})^{l_k} = (\pi_k^2 \cdot u)^{l_k} \in K^n$ if and only if $l_k = n \cdot z$ for some non-negative integer z. This is the case since u is a primitive n^{th} root of unity. The assumption that d is not divisible by a n^{th} power tells us that l_k must equal 0. This then tells us that the valuation $v_{\pi_k}(d)$ at the special prime ideal (π_k) must be equal to 0, since the special prime element π_k does not divide d.

Now consider an inert prime p_k. In this case we have $(p_k \cdot \overline{p_k})^{l_k} = (p_k^2)^{l_k} \in K^n$ if and only if $2 \cdot l_k = 0$ or n. Hence $l_k = 0$ or 2 (respectively 0 or 3). This then tells us that the valuation $v_{p_k}(d)$ at an inert prime ideal (p_k) must be equal to 0 or 2 (respectively 0 or 3).

Finally we must consider a prime $\pi_k \in S_1$ (respectively T_1), in which case we get $(\pi_k \cdot \overline{\pi_k})^{l_k}$. By the assumption that d is not divisible by a n^{th} power we see that $(\pi_k \cdot \overline{\pi_k})^{l_k} \in K^n$ if and only if the sum of the exponent of π_k in d and the exponent of $\overline{\pi_k}$ in d is equal to 0 or n, i.e. 0 or 4 (respectively 0 or 6). This then tells us that the sum of the valuation $v_\pi(d)$ at a prime ideal (π) generated by a prime $\pi \in S_1$ (respectively T_1) and the valuation $v_{\bar{\pi}}(d)$ at its conjugate $\bar{\pi}$ must be equal to 0 or 4 (respectively 0 or 6). □

3.2.1 The 4×4 Case

Recall from Section 3.1.3 that for the best known PSTBC of degree 4 we have $A = (i, \mathbb{Q}(i)(\zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i), \sigma)$ and

$$\delta_{min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{d_{L/K}} = \frac{1}{1125}.$$

We now use the method explained in the previous section to determine the optimum code of degree 4. In this case we will also assume that $d \neq d'^2$ for some $d' \in \mathcal{O}_K$, so that $K(\sqrt[4]{d})/K$ is an extension of degree 4. Recall that we take $K = \mathbb{Q}(i)$ and we first assume that $\gamma \in \mathcal{O}_K$, in which case $\gamma \in \{\pm 1, \pm i\}$. Let us now determine when $A = (\gamma, K(\sqrt[4]{d})/K, \sigma)$ is a division K-algebra. Throughout this section we will assume that $\mathrm{Gal}(K(\sqrt[4]{d})/K)$ commutes with complex conjugation.

Proposition 3.2.3. *Let $A = (\gamma, K(\sqrt[4]{d})/K, \sigma)$. Then A is a cyclic division K-algebra if and only if*

- $\gamma = \pm i$
- *There exists a prime element $\pi = a + bi$ where $a^2 + b^2 = p \equiv 5 \pmod 8$ such that π divides d with odd exponent.*

Proof. Since K is a number field and A is a central simple K-algebra we know by the Brauer-Hasse-Noether Theorem that $exp(A) = ind(A)$. Assume that A is a division K-algebra, in which case $exp(A) = 4$ and therefore $2[A] \neq 0$. Conversely

assume A is not a division K-algebra then $ind(A)$ is a proper divisor of 4 so $ind(A)|2$ and therefore $exp(A)|2$, which implies that $2[A] = 0$. Hence A is a division K-algebra if and only if $2[A] \neq 0$.

By Lemma 1.4.5 we see that $2[A] = [A \otimes_K A] = M_4((\gamma^2, K(\sqrt[4]{d})/K, \sigma))$ and clearly $M_4((\gamma^2, K(\sqrt[4]{d})/K, \sigma)) \sim (\gamma^2, K(\sqrt[4]{d})/K, \sigma)$. Therefore $\gamma \neq \pm 1$, since $[(1, K(\sqrt[4]{d})/K, \sigma)] = [0]$, hence $\gamma = \pm i$. However it is clear that

$$2[(i, K(\sqrt[4]{d})/K, \sigma)] = 2[(-i, K(\sqrt[4]{d})/K, \sigma)]$$

therefore $(i, K(\sqrt[4]{d})/K, \gamma)$ is a division K-algebra if and only if $(-i, K(\sqrt[4]{d})/K, \gamma)$ is a division K-algebra. Without any loss of generality we can assume the former case. Therefore

$$2[A] = (\gamma^2, K(\sqrt[4]{d})/K, \sigma) = (-1, K(\sqrt[4]{d})/K, \sigma).$$

Now we see from Lemma 1.4.6 that

$$(-1, K(\sqrt[4]{d})/K, \sigma) \simeq M_2((i, K(\sqrt{d})/K, \bar{\sigma})) \sim (i, K(\sqrt{d})/K, \bar{\sigma})$$

where $\bar{\sigma}$ indicates the restriction of $\sigma \in Gal(K(\sqrt[4]{d})/K)$ to the extension $K(\sqrt{d})/K$. Hence $2[A] = [(i, K(\sqrt{d})/K, \bar{\sigma})]$, which tells us that A is a division K-algebra if and only if $[(i, K(\sqrt{d})/K, \bar{\sigma})] \neq 0$, or in other words A is a division K-algebra if and only if $A^{(2)} := (i, K(\sqrt{d})/K, \bar{\sigma})$ is a division K-algebra. Since $A^{(2)}$ is the quaternion algebra $Q := (i, d)_K$ there are only two possibilities: either Q is a division K-algebra or Q splits.

By Proposition 3.2.2 we know that if $p \in S_3$ and $p|d$ then $v_p(d) = 2$. Similarly if $\pi \in S_1$ and $\pi|d$ then $(v_\pi(d), v_{\bar{\pi}}(d)) = (1, 3)$, $(2, 2)$ or $(3, 1)$. Hence

$$(i, d)_K \simeq (i, u\pi_1\bar{\pi}_1 \cdots \pi_k\bar{\pi}_k)_K$$

for $u \in \mathcal{O}_K^\times$ and prime elements $\pi_i \in S_1$ such that $v_\pi(d)$ is odd.

We can then see that for primes $p \in S_3$ and $\pi \in S_1$ such that $v_\pi(d)$ is even, the Hasse symbols $(i, d)_{2,p}$, $(i, d)_{2,\pi}$ and $(i, d)_{2,\bar{\pi}}$ are trivial. Now for $\pi \in S_1$ and $v_\pi(d)$ odd, $(i, d)_{2,\pi}$ is the image of $i^{(p_\pi - 1)/2}$ in $\mathbb{F}_{p_\pi}$. If $p_\pi \equiv 1 \pmod 8$ then $i^{(p_\pi-1)/2} = 1$ and if $p_\pi \equiv 5 \pmod 8$ then $i^{(p_\pi-1)/2} = -1$.

Therefore if $\pi \in S_1$ such that $p_\pi \equiv 5 \pmod 8$ and $v_\pi(d)$ is odd, then $(i, d)_{2,\pi}$ is not trivial. This implies that $(i, d)_K$ is not split, which implies that A is a division

K-algebra. If there is no such divisor of d then $(i,d)_K \otimes_K K_v$ is split at all places, except maybe the place defined by $\pi' = 1 - i$. However by the Brauer-Hasse-Noether theorem, we know this implies that $(i,d)_K$ is split at all places v. Hence $(i,d)_K$ is split, which implies that A is split in this case.

□

Now that we have a necessary and sufficient condition for A to be a division K-algebra, we must study the ramification of ideals in $K(\sqrt[4]{d})/K$ to determine which extensions have $d_{L/K} < 1125$. In order to do this we first consider the ramification of a prime ideal (that doesn't lie above 2) generated by a prime element π where $v_\pi(d)$ is odd.

Proposition 3.2.4. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal not above 2 generated by π. If $v_\pi(d) = 1$ or 3 then $p^3 | d_{L/K}$, where p is the prime number lying below π.*

Proof. By Proposition 3.2.2 we know that $\pi \notin S_3$, i.e. $\pi \not\equiv 3 \pmod 4$. We also know that $v_\pi(d) + v_{\bar{\pi}}(d) = 4$. Since we assume that $v_\pi(d) = 1$ or 3, by Proposition 1.2.23 we see that both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ totally ramify in L/K. From the definition of the discriminant ideal we see that

$$\mathcal{N}_{L/K}(\mathfrak{P}^3) = \mathcal{N}_{L/K}(\mathfrak{P})^3 = \mathfrak{p}^3 | \mathfrak{d}_{L/K}.$$

Similarly we have $\bar{\mathfrak{p}}^3 | \mathfrak{d}_{L/K}$ and hence $(\mathfrak{p} \cdot \bar{\mathfrak{p}})^3 | \mathfrak{d}_{L/K}$. Using Lemma 2.3.4 we then see that $p^3 | d_{L/K}$. □

Corollary 3.2.5. *Let A be a cyclic division K-algebra. If $d_{L/K} \leq 1125$ then $v_\pi(d) = 1$ or 3 for a prime element π of $\mathcal{O}_K$ lying above the prime 5. Furthermore $125 | d_{L/K}$ and there is no other prime element π' (that doesn't lie above 5) such that $v_\pi(d) = 1$ or 3.*

Proof. Let $\pi = a + bi$, where $a^2 + b^2 = p \equiv 5 \pmod 8$ and $v_\pi(d) = 1$ or 3. If $p > 5$ (so $p \geq 13$) then by Proposition 3.2.4 we can calculate that $d_{L/K} \geq 2197$. Using the same proposition we can calculate that if $p = 5$ then $125 | d_{L/K}$.

Now assume that π' is a prime element not above 5 that divides d with odd exponent. By Proposition 3.2.2 we know that $\pi' \notin S_3$ and hence lies above a prime $p' \equiv 1 \pmod 4$. If $p' \neq 5$ then $p' \geq 13$, and as we have seen above, this would imply $d_{L/K} > 1125$. □

We now need to consider the case where a prime ideal $\mathfrak{p} = (\pi)$ is tamely ramified and $v_\pi(d) = 2$.

Proposition 3.2.6. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal not above 2 generated by a prime element $\pi \in \mathcal{O}_K$ lying above a prime p. If $v_\pi(d) = 2$ then $p^2 | d_{L/K}$.*

Proof. By results on Kummer extensions we know that $\mathfrak{p}$ must be ramified. It is also clear that it won't be totally ramified, hence $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^2$ or $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^2 \cdot \mathfrak{P}_2^2$.

In the first case we see that the residue class degree is equal to 2 and so $\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^2$, furthermore $\mathfrak{P} | \mathcal{D}_{L/K}$. Hence $\mathfrak{p}^2 | \mathfrak{d}_{L/K}$. If $p \equiv 3 \pmod 4$ then using Lemma 2.3.4 we see that $p^2 | d_{L/K}$. If $p \equiv 1 \pmod 4$ then $\bar{\mathfrak{p}}^2 | \mathfrak{d}_{L/K}$ as well and using Lemma 2.3.4 again we see that $p^2 | d_{L/K}$ in this case also.

In the second case we see that $\mathfrak{P}_1 \cdot \mathfrak{P}_2 | \mathcal{D}_{L/K}$. Hence $\mathcal{N}_{L/K}(\mathfrak{P}_1 \cdot \mathfrak{P}_2) = \mathfrak{p}^2 | \mathfrak{d}_{L/K}$. We then proceed as in the previous paragraph. □

Corollary 3.2.7. *Let A be a cyclic division K-algebra such that $d_{L/K} \leq 1125$. Assume that $v_\pi(d) = 2$ where π is a prime element not lying above 5. Then $\pi = 3$ and $1125 | d_{L/K}$.*

Proof. By Corollary 3.2.5 we know that $125 | d_{L/K}$ and $3^2 \cdot 125 = 1125$. □

The above results tell us that if A is a cyclic division K-algebra such that $d_{L/K} \leq 1125$ then the only possibilities for our field extension are $K(\alpha)/K$, where α is a root of one of the following polynomials:

1. $X^4 - (1+2i) \cdot (1-2i)^3$;
2. $X^4 - (1+2i) \cdot (1-2i)^3 \cdot (-1)$;
3. $X^4 - (1+2i) \cdot (1-2i)^3 \cdot (i)$;
4. $X^4 - (1+2i) \cdot (1-2i)^3 \cdot (-i)$.

We will give mathematical arguments to compute $d_{L/K}$ in the four cases above as well as computing whether the ideal class group of $\mathcal{O}_L$ is trivial or not.

The case $X^4 - (1+2i) \cdot (1-2i)^3$

Proposition 3.2.8. *Let α_1 be a root of the polynomial $f := X^4 - (1+2i) \cdot (1-2i)^3$. Then $K(\alpha_1) \simeq \mathbb{Q}(\zeta_{20})$.*

Proof. We know that $i \in \mathbb{Q}(\zeta_{20})$ and hence $K \subseteq \mathbb{Q}(\zeta_{20})$. Let $z = e^{2\pi i/20}$ then it can be computed that $z + z^{12} + z^{18} + z^{19}$ is a root of f. Therefore $K(\alpha_1) \subseteq \mathbb{Q}(\zeta_{20})$. Since

$$[\mathbb{Q}(\zeta_{20}) : \mathbb{Q}] = \phi(20) = 8 = [K(\alpha_1) : \mathbb{Q}]$$

we see that $K(\alpha_1) \simeq \mathbb{Q}(\zeta_{20})$. □

Remark The decomposition of prime ideals in cyclotomic extensions of $\mathbb{Q}$ is well understood, see for example [19].

Proposition 3.2.9. *Let $L = K(\alpha_1)$ then $d_{L/K} = 125$.*

Proof. It is well known (see for example [46]) that the absolute discriminant of a cyclotomic field $\mathbb{Q}(\zeta_n)$ is given by

$$d_{\mathbb{Q}(\zeta_n)} = (-1)^{\phi(n)/2} \cdot \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Hence $d_L = d_{\mathbb{Q}(\zeta_{20})} = 2^8 \cdot 5^6$ and we know that $d_K = -4$. By the tower of discriminants formula we have $d_L = N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) \cdot d_K^{[L:K]}$ and so

$$5^6 = N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) = N_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = (d_{L/K})^2.$$

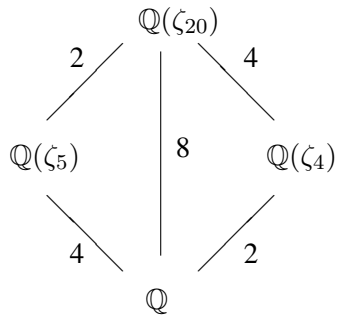
Therefore $d_{L/K} = 125$. □

Proposition 3.2.10. *Let $A = (i, K(\alpha_1)/K, \sigma)$. Then it is impossible to construct the cubic lattice from A.*

Proof. By Corollary 2.3.14 we know that if it was possible to construct the cubic lattice from A then $d_{L/K} \geq 4^4 = 256$. Since $d_{L/K} = 125$ the result follows. □

Proposition 3.2.11. *Let $L = K(\alpha_1)$ then the class group of $\mathcal{O}_L$ is trivial, or in other words $\mathcal{O}_L$ is a principal ideal domain.*

Proof. Since $L \simeq \mathbb{Q}(\zeta_{20})$ we will do our calculations in the cyclotomic case, in which case we have the following diagram:



We know that $\mathbb{Z}[\zeta_4]$ is a PID and the only prime that ramifies in $\mathbb{Q}(\zeta_4)/\mathbb{Q}$ is 2, which is totally ramified. Also we know that the only prime that ramifies in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is 5, which is totally ramified and the Minkowski bound is $M_{\mathbb{Q}(\zeta_5)} \approx 1.7$, therefore by Theorem 1.2.35 $\mathbb{Z}[\zeta_5]$ is a PID as well.

For the extension $\mathbb{Q}(\zeta_{20})/\mathbb{Q}$ we compute $M_{\mathbb{Q}(\zeta_{20})} \approx 12.63$, therefore we need to consider the decomposition of the primes $2, 3, 5, 7$ and 11. This gives us the following table:

$p\mathcal{O}_L$	Decomposition	$N_{L/\mathbb{Q}}(\mathfrak{p}_i)$
$2\mathbb{Z}[\zeta_{20}]$	$\mathfrak{p}_2^2$	16
$3\mathbb{Z}[\zeta_{20}]$	$\mathfrak{p}_3 \cdot \mathfrak{q}_3$	81
$5\mathbb{Z}[\zeta_{20}]$	$\mathfrak{p}_5^4 \cdot \mathfrak{q}_5^4$	5
$7\mathbb{Z}[\zeta_{20}]$	$\mathfrak{p}_7 \cdot \mathfrak{q}_7$	2401
$11\mathbb{Z}[\zeta_{20}]$	$\mathfrak{p}_{11} \cdot \mathfrak{q}_{11} \cdot \mathfrak{r}_{11} \cdot \mathfrak{s}_{11}$	121

The only prime ideals with norm less than $M_{\mathbb{Q}(\zeta_{20})}$ are $\mathfrak{p}_5$ and $\mathfrak{q}_5$. Without loss of generality we can assume that $\mathfrak{p}_5 \subset \mathbb{Z}[\zeta_4]$ and is therefore principal and generated by a prime element π_5. Now $\mathfrak{q}_5 = \bar{\mathfrak{p}_5}$, so it is generated by $\bar{\pi_5}$ and hence is principal as well. By Theorem 1.2.35 we therefore see that the class group is trivial. □

The case $X^4 - (1+2i) \cdot (1-2i)^3 \cdot (-1)$

Proposition 3.2.12. *Let α_2 be a root of the polynomial $g := X^4 - (1+2i) \cdot (1-2i)^3 \cdot (-1)$. Then $K(\alpha_2) \subset \mathbb{Q}(\zeta_{40})$ and $[\mathbb{Q}(\zeta_{40}) : K(\alpha_2)] = 2$.*

Proof. By Proposition 3.2.8 we know that $K(\alpha_1)(\zeta_8) \simeq \mathbb{Q}(\zeta_{40})$. Furthermore we can compute that $(\alpha_1 \cdot \zeta_8)^4 = -(1+2i) \cdot (1-2i)^3$, so we see that $\alpha_1 \cdot \zeta_8$ is a root

of the polynomial g. Hence $K(\alpha_2) \subset \mathbb{Q}(\zeta_{40})$. To complete the proof we note that $\phi(40) = 16$ and since $[K(\alpha_2) : \mathbb{Q}] = 8$, we have $[\mathbb{Q}(\zeta_{40}) : K(\alpha_2)] = 2$. □

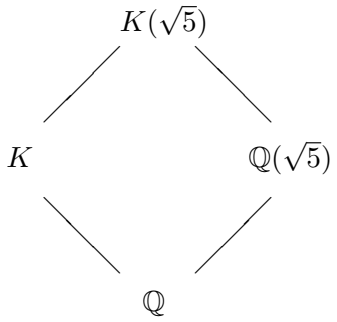
Remark The only primes that ramify in $\mathbb{Q}(\zeta_{40})/\mathbb{Q}$ are 2 and 5 and their decompositions are $2\mathbb{Z}[\zeta_{40}] = \mathfrak{P}_2^4$ and $5\mathbb{Z}[\zeta_{40}] = \mathfrak{P}_5^4 \cdot \mathfrak{Q}_5^4$.

Proposition 3.2.13. *We have $K(\sqrt{5})$ is an intermediate field of L/K. Furthermore the prime ideal $\mathfrak{p}_2 \in \mathcal{O}_K$ that lies above 2, remains inert in the extension $K(\sqrt{5})/K$.*

Proof. Since $\alpha_2 = \sqrt[4]{(1+2i)\cdot(1-2i)^3\cdot(-1)} = \sqrt{\sqrt{5}\cdot(1-2i)\cdot i}$ and $(1-2i)\cdot i \in K$ we see that $K \subset K(\sqrt{5}) \subset L$. Also $K(\sqrt{5})/K$ is a Kummer extension of degree 2 and it is easy to see that there exists some x in $\mathcal{O}_K$ such that Condition 2 of Theorem 1.2.25 is satisfied (e.g. $x = 1$), so $\mathfrak{p}_2$ is unramified in $K(\sqrt{5})/K$. Since $\mathfrak{p}_2$ cannot split by the remark above, this completes the proof. □

Proposition 3.2.14. *The ring of integers $\mathcal{O}_{K(\sqrt{5})}$ is equal to $\mathcal{O}_K\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, or in other words $\{1, i, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}i\}$ is an integral basis for $\mathcal{O}_{K(\sqrt{5})}$.*

Proof. Since $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ are linearly disjoint, we have the following diagram



where $K(\sqrt{5})$ is equal to the compositum of K and $\mathbb{Q}(\sqrt{5})$.

Now $\mathcal{D}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} = \mathfrak{p}_5\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. We saw in Proposition 3.2.13 that $\mathfrak{p}_2$ remains inert in $K(\sqrt{5})/K$ hence $\mathcal{D}_{K(\sqrt{5})/K} = \mathfrak{p}_5\mathcal{O}_{K(\sqrt{5})}$. We therefore see by Proposition 1.2.33 that $\mathcal{O}_{K(\sqrt{5})} = \mathcal{O}_K\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. □

Proposition 3.2.15. *The prime ideal $\mathfrak{p}_2$ is totally ramified in the extension $L/K(\sqrt{5})$.*

Proof. Let $j(X) := X^2 - \sqrt{5} \cdot (1-2i) \cdot i$ and let δ be a root of $j(X)$, so that $L = K(\sqrt{5})(\delta)$. Now $L \simeq K(\sqrt{5})(\delta - 1)$ and $\delta - 1$ is a root of the polynomial $j(X+1) = X^2 + 2X + (1 - 2\sqrt{5} - i\sqrt{5})$. Now $j(X+1)$ is an Eisenstein polynomial at $\mathfrak{p}_2$ in $\mathcal{O}_{K(\sqrt{5})}$. To see this consider $\mathfrak{p}_2 = (1-i)\mathcal{O}_{K(\sqrt{5})}$. Any element $z \in \mathcal{O}_{K(\sqrt{5})}$ has the form

$$z = z_1 + z_2 i + z_3 \frac{1+\sqrt{5}}{2} + z_4 \frac{1+\sqrt{5}}{2} i, \quad z_i \in \mathbb{Z}$$

By taking $z_1 = 2, z_2 = -1, z_3 = -3, z_4 = 1$ we can see that $(1 - 2\sqrt{5} - i\sqrt{5}) = z(1-i)i \equiv 0 \pmod{\mathfrak{p}_2}$. However $(1-2\sqrt{5}-i\sqrt{5}) \not\equiv 0 \pmod{\mathfrak{p}_2^2} = (2)\mathcal{O}_{K(\sqrt{5})}$. Applying Proposition 1.2.32 then completes the result. □

Proposition 3.2.16. *Let $L = K(\beta)$ then $d_{L/K} = 2000$.*

Proof. Consider the extension $\mathbb{Q}(\zeta_{40})/\mathbb{Q}$. By the remark above we have $2\mathbb{Z}[\zeta_{40}] = \mathfrak{P}_2^4$ and $5\mathbb{Z}[\zeta_{40}] = \mathfrak{P}_5^4 \cdot \mathfrak{Q}_5^4$. We now consider $L/\mathbb{Q}$. It is well known that $2\mathcal{O}_K = \mathfrak{p}_2^2$ and by Proposition 3.2.15 we know $\mathfrak{p}_2\mathcal{O}_L = \mathfrak{P}_2^2$, so $2\mathcal{O}_L = \mathfrak{P}_2^4$. Hence the prime ideal $\mathfrak{P}_2$ of $\mathcal{O}_L$ is unramified in the extension $\mathbb{Q}(\zeta_{40})/L$. Now $5\mathcal{O}_K = \mathfrak{p}_5 \cdot \mathfrak{q}_5$ and by Proposition 1.2.23 we see that $\mathfrak{p}_5\mathcal{O}_L = \mathfrak{P}_5^4$, so $5\mathcal{O}_L = \mathfrak{P}_5^4 \cdot \mathfrak{Q}_5^4$. Hence $\mathbb{Q}(\zeta_{40})/L$ is an unramified extension.

Now we can easily compute that $d_{\mathbb{Q}(\zeta_{40})} = 2^{32} \cdot 5^{12}$. The tower of discriminants formula tells us that

$$d_{\mathbb{Q}(\zeta_{40})} = N_{L/\mathbb{Q}}(\mathfrak{d}_{\mathbb{Q}(\zeta_{40})/L}) \cdot d_L^2.$$

However since $\mathbb{Q}(\zeta_{40})/L$ is unramified this simplifies to $d_{\mathbb{Q}(\zeta_{40})} = d_L^2$, hence $d_L = 2^{16} \cdot 5^6$. We then continue as in the proof of Proposition 3.2.9 to compute that

$$2^8 \cdot 5^6 = N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) = N_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = (d_{L/K})^2.$$

Therefore $d_{L/K} = 2^4 \cdot 5^3 = 2000$. □

The **Hilbert class field** E of a number field K is defined as the maximal abelian unramified extension of K. An important result on the Hilbert class field E is that the degree of E/K is equal to the class number of K [19]. Since $\mathbb{Q}(\zeta_{40})/L$ is an unramified extension of degree 2, the ideal class group of $\mathcal{O}_L$ is non-trivial and its class number is greater than or equal to 2.

The case $X^4 - (1+2i)\cdot(1-2i)^3\cdot(i)$

Proposition 3.2.17. *Let α_3 be a root of the polynomial $h(X) := X^4 - (1+2i)\cdot(1-2i)^3\cdot(i)$. Then $K(\alpha_3) \subset \mathbb{Q}(\zeta_{80})$ and $[\mathbb{Q}(\zeta_{80}) : K(\alpha_3)] = 4$.*

Proof. By Proposition 3.2.8 we know that $K(\alpha_1)(\zeta_{16}) \simeq \mathbb{Q}(\zeta_{80})$. Furthermore we can compute that $(\alpha_1\cdot\zeta_{16})^4 = (1+2i)\cdot(1-2i)^3\cdot(i)$, so we see that $\alpha_1\cdot\zeta_{16}$ is a root of the polynomial h. Hence $K(\alpha_3) \subset \mathbb{Q}(\zeta_{80})$. Since $\phi(80) = 32$ we see that $[\mathbb{Q}(\zeta_{80}) : K(\alpha_3)] = 4$. □

Remark The only primes that ramify in $\mathbb{Q}(\zeta_{80})/\mathbb{Q}$ are 2 and 5 and their decompositions are $2\mathbb{Z}[\zeta_{80}] = \mathfrak{P}_2^8$ and $5\mathbb{Z}[\zeta_{80}] = \mathfrak{P}_5^4\cdot\mathfrak{Q}_5^4$.

Proposition 3.2.18. *Let $L = K(\alpha_3)$ then the prime ideal $\mathfrak{p}_2$ is totally ramified in the extension L/K.*

Proof. We have $L \simeq K(\alpha_3 - 1)$ and $\alpha_3 - 1$ is a root of the polynomial $h(X+1) = X^4 + 4X^3 + 6X^2 + 4X - 19 + 15i$. Since $-19+15i = (-17-2i)(1-i)$ it is clear that $h(X+1)$ is an Eisenstein polynomial at $\mathfrak{p}_2$ in $\mathcal{O}_K$. By Proposition 1.2.32 we then see that $\mathfrak{p}_2$ is totally ramified in L/K. □

Proposition 3.2.19. *Let $L = K(\alpha_3)$ then $d_{L/K} = 32000$.*

Proof. We can easily compute that $d_{\mathbb{Q}(\zeta_{80})} = 2^{96}\cdot 5^{24}$. Consider the extension $L/\mathbb{Q}$. By Proposition 3.2.18 we know that $2\mathcal{O}_L = \mathfrak{P}_2^8$, so the prime ideal $\mathfrak{P}_2$ in $\mathcal{O}_L$ is unramified in $\mathbb{Q}(\zeta_{80})/L$. Following the proof of Proposition 3.2.16 we can also see that $5\mathcal{O}_L = \mathfrak{P}_5^4\cdot\mathfrak{Q}_5^4$. Using the remark above we therefore know that $\mathbb{Q}(\zeta_{80})/L$ is an unramified extension.

We know that

$$d_{\mathbb{Q}(\zeta_{80})} = N_{L/\mathbb{Q}}(\mathfrak{d}_{\mathbb{Q}(\zeta_{80})/L})\cdot d_L^4.$$

Since $\mathbb{Q}(\zeta_{80})/L$ is unramified this simplifies to $d_{\mathbb{Q}(\zeta_{80})} = d_L^4$, hence $d_L = 2^{24}\cdot 5^6$. We can then compute that

$$2^{16}\cdot 5^6 = N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) = N_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = (d_{L/K})^2.$$

Therefore $d_{L/K} = 2^8\cdot 5^3 = 32000$. □

Since $\mathbb{Q}(\zeta_{80})/L$ is an unramified extension of degree 4, the ideal class group of $\mathcal{O}_L$ is non-trivial and its class number is greater than or equal to 4.

Remark In the case $X^4 - (1+2i)\cdot(1-2i)^3\cdot(-i)$ we again get that $d_{L/K} = 32000$ and the proof follows in the same way as the case $X^4-(1+2i)\cdot(1-2i)^3\cdot(i)$.

Hence for $[L:K]=4$ we have shown that if $A=(\gamma, L/K, \sigma)$ is a cyclic division K-algebra with $\gamma \in \mathcal{O}_K$ and $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a code built on A that satisfies the energy constraint, then

$$d_{L/K}\cdot\prod_{m=1}^{n}\Delta_{\xi}^{(m)} \geq 1125.$$

However we must also consider the case $\gamma \notin \mathcal{O}_K$.

The case $\gamma \notin \mathbb{Z}[i]$

Let $\gamma \in K\backslash\mathcal{O}_K$ so that $\gamma = \frac{\gamma_1}{\gamma_2}$ with $\gamma_1, \gamma_2 \in \mathcal{O}_K$, $\gamma_2 \nmid \gamma_1$ and let $A=(\gamma, L/K, \sigma)$ be a cyclic division K-algebra of degree 4 with L-basis $\{1, e, e^2, e^3\}$. Let $a \in A$ be of the form $a = a_0 + ea_1 + e^2a_2 + e^3a_3$ where $a_i \in L$ for $i = 0, \ldots, 3$. The matrix M_a of left multiplication by a in our chosen L-basis is

$$M_a = \begin{pmatrix} a_0 & \frac{\gamma_1}{\gamma_2}a_3^{\sigma} & \frac{\gamma_1}{\gamma_2}a_2^{\sigma^2} & \frac{\gamma_1}{\gamma_2}a_1^{\sigma^3} \\ a_1 & a_0^{\sigma} & \frac{\gamma_1}{\gamma_2}a_3^{\sigma^2} & \frac{\gamma_1}{\gamma_2}a_2^{\sigma^3} \\ a_2 & a_1^{\sigma} & a_0^{\sigma^2} & \frac{\gamma_1}{\gamma_2}a_3^{\sigma^3} \\ a_3 & a_2^{\sigma} & a_1^{\sigma^2} & a_0^{\sigma^3} \end{pmatrix}.$$

By Corollary 2.3.14 we know that $d_{L/K} \geq 256$ and therefore

$$d_{L/K}\cdot\prod_{m=1}^{n}\Delta_{\xi}^{(m)} \geq 256\cdot(\gamma_2\cdot\bar{\gamma_2})^3.$$

Now since $\gamma_2 \neq 1$ we see that the right hand side of the above equation is greater than or equal to $256\cdot 2^3 = 2048 > 1125$. Therefore the price we pay in the coding gain by considering $\gamma \notin \mathcal{O}_K$ is too large to give a better performing code.

Corollary 3.2.20. *Let $[L:K]=4$ and let $A=(\gamma, L/K, \sigma)$ be a cyclic division K-algebra. If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a code built on A that satisfies the energy constraint, then*

$$d_{L/K}\cdot\prod_{m=1}^{n}\Delta_{\xi}^{(m)} \geq 1125.$$

Hence the PSTBC of dimension 4 presented in [29] is optimal.

3.2.2 The 6×6 Case

Recall for the best known PSTBC of degree 6 we have $K = \mathbb{Q}(j)$ and $A = (-j, K(\zeta_{28} + \zeta_{28}^{-1})/K, \sigma)$ and

$$\frac{1}{2^6 \cdot 7^5} \leq \delta_{\min}(\mathcal{C}_{A,\lambda,I}) \leq \frac{1}{2^6 \cdot 7^4}.$$

We now determine the optimum code of degree 6 where we assume that $K = \mathbb{Q}(j)$. Similar to the 4×4 case we will also assume that $d \neq d'^2$ and $d \neq d''^3$ for some $d', d'' \in \mathcal{O}_K$, so that $K(\sqrt[6]{d})/K$ is an extension of degree 6. Again we first assume that $\gamma \in \mathcal{O}_K$ and determine when $A = (\gamma, K(\sqrt[6]{d})/K, \sigma)$ is a division K-algebra. Similar to the previous section, we will assume throughout that $\mathrm{Gal}(K(\sqrt[6]{d})/K)$ commutes with complex conjugation.

Proposition 3.2.21. *Let $A = (\gamma, K(\sqrt[6]{d})/K, \sigma)$. Then A is a cyclic division K-algebra if and only if*

- $\gamma = -j$ *or* $-j^2$
- *There exist (not necessarily distinct) prime elements π and π' of $\mathbb{Z}[j]$ such that $v_\pi(d)$ is prime to 3, $v_{\pi'}(d)$ is odd and satisfying the following:*
  1. *$\pi' = a + bj$, where $l = a^2 + b^2 - ab$ is a prime number satisfying $l \equiv 7 \pmod{12}$.*
  2. *$\pi = a + bj$, where $l = a^2 + b^2 - ab$ is a prime number satisfying $l \equiv 4$ or $7 \pmod{9}$.*

Proof. Proceeding in a similar manner to the 4×4 case, we can use arguments involving the exponent of the Brauer group to give us the first condition. We can also show that $(-j, K(\sqrt[6]{d})/K, \sigma)$ is a division K-algebra if and only if $(-j^2, K(\sqrt[6]{d})/K, \sigma)$ is a division K-algebra and so without loss of generality we will assume that $A = (-j, K(\sqrt[6]{d})/K, \sigma)$.

By the Primary Decomposition Theorem $A \simeq A^{(2)} \otimes_K A^{(3)}$ and A is a division K-algebra if and only if $A^{(2)}$ and $A^{(3)}$ are division K-algebras. We first consider the quaternion algebra $A^{(2)} = (-j, K(\sqrt{d})/K, \bar{\sigma}) \simeq (-j, d)_K$.

We proceed as in the Proof of Proposition 3.2.3. By Proposition 3.2.2

$$(-j, d)_K \simeq (-j, up_1 \cdots p_k \pi_1 \bar{\pi}_1 \cdots \pi_l \bar{\pi}_l)_K$$

for $u \in \mathcal{O}_K^\times, p_i \in T_2, \pi_i \in T_1$ with $v_{p_i}(d)$ odd and $v_{\pi_i}(d)$ odd. Hence for $\pi = 1 - j$ or any $\pi \in T_1$ such that $v_\pi(d)$ is even, the Hilbert symbol $(-j, d)_{2,\pi}$ is trivial.

Consider a prime $p \in T_2$. then $(-j, d)_{2,\pi}$ is the image of $(-j)^{(p^2-1)/2}$ in $\mathbb{F}_{p^2}$. If $p \neq 2$ then $p \equiv 5 \pmod 6$ and therefore $6|\frac{p^2-1}{2}$. Hence the Hasse symbol $(-j, d)_{2,p}$ is trivial in this case.

Now consider $\pi \in T_1$ such that $v_p(d)$ is odd. In this case $(-j, d)_{2,\pi}$ is the image of $(-j)^{(p_\pi-1)/2}$ in $\mathbb{F}_{p_\pi}$. If $p_\pi \equiv 1 \pmod{12}$ then $(-j, d)_{2,\pi} = \bar{1}$ and if $p_\pi \equiv 7 \pmod{12}$ then $(-j, d)_{2,\pi} = \overline{-1}$.

Hence if $\pi \in T_1$ with $p_\pi \equiv 7 \pmod{12}$ and $\pi|d$ such that $v_\pi(d)$ is odd, then $(-j, d)_{2,\pi}$ is non-trivial and so $(-j, d)_K$ is a division K-algebra. If there is no such divisor of d, then the Hasse symbol is trivial at all places except maybe the place defined by 2. However by the Brauer-Hasse-Noether this implies that $(i, d)_K$ is split at all places v. Hence $(-j, d)_K$ is split in this case.

We now move to $A^{(3)} = (-j, K(\sqrt[3]{d})/K, \bar{\sigma}) \simeq (j, K(\sqrt[3]{d})/K, \bar{\sigma})$ by Lemma 1.4.7. Since $A^{(3)}$ is of degree 3 we see that $A^{(3)}$ is either split or a division K-algebra. By Proposition 3.2.2 we know that

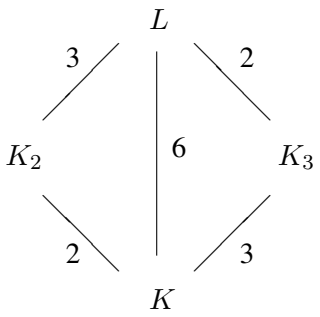
$$(j, K(\sqrt[3]{d})/K, \bar{\sigma}) \simeq (j, K(\sqrt[3]{u\pi_1\overline{\pi_1}^2 \cdots \pi_k\overline{\pi_k}'^2\pi_1^2\overline{\pi_1}' \cdots \pi_l'^2\overline{\pi_l}'})/K, \bar{\sigma})$$

where $u \in \mathcal{O}_K^\times$, $\pi, \pi' \in T_1$, $\pi|d$, $\pi'|d$ with $v_\pi(d) \neq 3$ and $v_{\bar{\pi}}(d) \neq 3$. We then immediately see that for any prime $p \in T_2$ or $\pi \in T_1$ such that $\pi|d$ and $v_\pi(d) = 3$ the Hasse symbols $(j, d)_{3,p}$, $(j, d)_{3,\pi}$ and $(j, d)_{3,\bar{\pi}}$ are trivial.

For any $\pi \in T_1$ such that $\pi|d$ and $v_\pi(d) \neq 3$ we see that $(j, d)_{3,\pi}$ will be the image of $j^{(p_\pi-1)/3}$ in $\mathbb{F}_{p_\pi}$. Now $p_\pi \equiv 1 \pmod 3$, which is equivalent to saying that $p_\pi \equiv 1, 4$ or $7 \pmod 9$. In this way we can see that $(j, d)_{3,\pi} = \bar{1}$ if and only if $p_\pi \equiv 1 \pmod 9$.

Therefore we can reason in a similar manner to above to show that $A^{(3)}$ is a division K-algebra if and only if there exists $\pi \in T_1$ with $p_\pi \equiv 4$ or $7 \pmod 9$ such that $\pi|d$ and $v_\pi(d) \neq 3$. This completes our proof. □

To consider the ramification of a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ in L/K we look at the two subextensions K_2 and K_3 of L, where $[K_2 : K] = 2$ and $[K_3 : 3]$, which gives us the following diagram:



As usual prime ideals above $\mathfrak{p}$ will be denoted by $\mathfrak{P}$ and $\mathfrak{P}_{(i)}$ will denote the prime ideal above $\mathfrak{p}$ lying in $\mathcal{O}_{K_i}$.

Since the ramification index of a prime ideal divides the degree of the extension we are able to deduce that there are three possibilities for a prime ideal $\mathfrak{p}$ that ramifies in L/K:

1. $\mathfrak{p}$ only ramifies in K_2/K.
2. $\mathfrak{p}$ only ramifies in K_3/K.
3. $\mathfrak{p}$ ramifies in K_2/K and K_3/K.

We will first consider the primes that ramify tamely in L/K before moving onto the wildly ramified primes.

Proposition 3.2.22. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal that doesn't lie above 2 or 3, generated by the prime element $\pi \in \mathcal{O}_K$. If $v_\pi(d) = 1$ or 5 then $p^5 | d_{L/K}$, where p is the prime number lying below π.*

Proof. We can see that $\mathfrak{p}$ ramifies in both K_2/K and K_3/K, so it must be totally ramified. Hence

$$\mathcal{N}_{L/K}(\mathfrak{P}^5) = \mathfrak{p}^5 | \mathfrak{d}_{L/K}.$$

Now by Proposition 3.2.2 we know that $v_\pi(d) + v_{\bar{\pi}}(d) = 6$. Hence $(\mathfrak{p} \cdot \bar{\mathfrak{p}})^5 | \mathfrak{d}_{L/K}$. Using Lemma 2.3.4 we then see that $p^5 | d_{L/K}$. □

Corollary 3.2.23. *Assume that $\mathfrak{p}$ lies above a prime $p \equiv 1 \pmod 3$ and that $v_\pi(d) = 1$ or 5. If $p > 13$ then $d_{L/K} > 2^6 \cdot 7^5$.*

Proof. First note that $13^5 = 371293 < 2^6 \cdot 7^5$. The next prime $p > 13$ such that $p \equiv 1 \pmod 3$ is 19. However $19^5 = 2476099 > 2^6 \cdot 7^5$. □

Proposition 3.2.24. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal that doesn't lie above 2 or 3, generated by the prime element $\pi \in \mathcal{O}_K$. If $v_\pi(d) = 2$ or 4 then $p^4 | d_{L/K}$, where p is the prime number lying below π.*

Proof. We can see that $\mathfrak{p}$ does not ramify in K_2/K and is totally ramified in K_3/K. Hence $\mathfrak{p}^2 | \mathfrak{d}_{K_3/K}$ and by the behaviour of the discriminant ideal in a tower of fields we see that $\mathfrak{p}^4 | \mathfrak{d}_{L/K}$. Then proceed as in the proof of Proposition 3.2.22 □

Corollary 3.2.25. *Assume that $\mathfrak{p}$ lies above a prime $p \equiv 1 \pmod 3$ and that $v_\pi(d) = 2$ or 4. If $p > 31$ then $d_{L/K} > 2^6 \cdot 7^5$.*

Proof. First note that $31^4 = 923521 < 2^6 \cdot 7^5$. The next prime $p > 31$ such that $p \equiv 1 \pmod 3$ is 37. However $37^4 = 1874161 > 2^6 \cdot 7^5$. □

Proposition 3.2.26. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal lying above a prime $p \neq 2$ or 3, generated by the prime element $\pi \in \mathcal{O}_K$. If $v_\pi(d) = 3$ then $p^3 | d_{L/K}$, where p is the prime number lying below π.*

Proof. We can see that $\mathfrak{p}$ does not ramify in K_3/K and is totally ramified in K_2/K. Hence $\mathfrak{p} | \mathfrak{d}_{K_2/K}$ and therefore $\mathfrak{p}^3 | \mathfrak{d}_{L/K}$. Then proceed as in the proof of Proposition 3.2.22. □

The above results allow us to produce a finite list of prime ideals that ramify tamely in an extension $K(\sqrt[6]{d})/K$ such that A satisfies the conditions of Proposition 3.2.21 and $d_{L/K} < 2^6 \cdot 7^5$.

We first consider a prime element $\pi = a + bj \in T_1$ that satisfies Condition 2 of Proposition 3.2.21. That is $\pi = a + bj$, where $l = a^2 + b^2 - ab$ is a prime number satisfying $l \equiv 4$ or $7 \pmod 9$. By Propositions 3.2.22 and 3.2.24 we know that if π satisfies Condition 2 of Proposition 3.2.21, then $l^4 | d_{L/K}$ or $l^5 | d_{L/K}$. The first three primes l that satisfy the congruence are 7, 13 and 31 and Corollaries 3.2.23 and 3.2.25 tell us that these are the only primes we need to consider. We are now left with five potential divisors of $d_{L/K}$ that must be checked, these are (in ascending order) $\{7^4, 7^5, 13^4, 13^5, 31^4\}$.

In order to check these divisors we must calculate the minimum possible value of $d_{L/K}$ for each divisor when Condition 1 of Proposition 3.2.21 is also satisfied.

If we consider this condition then Propositions 3.2.22 and 3.2.26 tell us that if $\pi' = a + bj$, where $l = a^2 + b^2 - ab$ is a prime number satisfying $l \equiv 7 \pmod{12}$, then $l^3 | d_{L/K}$ or $l^5 | d_{L/K}$. The first three primes l that satisfy the congruence are 7, 19 and 31.

We can now make our calculations for each of our five potential divisors. Firstly let π be a prime element above 7 such that $v_\pi(d) = 2$ or 4, in which case π satisfies Condition 2 of Proposition 3.2.21, so $7^4 | d_{L/K}$. If Condition 1 of Proposition 3.2.21 is also satisfied (by a prime element π' that does not lie above 7) then the remark above tells us that as a minimum $19^3 | d_{L/K}$ as well. However $7^4 \cdot 19^3 > 2^6 \cdot 7^5$, so this case can be dismissed.

The second case to consider is that π is a prime element above 7 such that $v_\pi(d) = 1$ or 5, so $7^5 | d_{L/K}$. In this instance Condition 1 of Proposition 3.2.21 is automatically satisfied by the prime element π.

Thirdly let π be a prime element above 13 such that $v_\pi(d) = 2$ or 4, so $13^4 | d_{L/K}$. If Condition 1 of Proposition 3.2.21 is also satisfied then we know from the remark above that as a minimum $7^3 | d_{L/K}$ as well. However $13^4 \cdot 7^3 > 2^6 \cdot 7^5$, so this case can be dismissed. The same logic allows us to dismiss the case π is a prime element above 13 such that $v_\pi(d) = 1$ or 5, so $13^5 | d_{L/K}$ and the case π is a prime element above 31 such that $v_\pi(d) = 2$ or 4, so $31^4 | d_{L/K}$.

Corollary 3.2.27. *If A is a cyclic division K-algebra and $d_{L/K} < 2^6 \cdot 7^5$ then there exists a prime element $\pi = a + bj$, where $l = a^2 + b^2 - ab = 7$, such that $v_\pi(d)$ is odd and prime to 3 (and therefore $7^5 | d_{L/K}$). Furthermore this is the only prime $p \neq 2$ or 3 that divides $d_{L/K}$.*

Proof. The first part comes from our work above. Now Propositions 3.2.22, 3.2.24 and 3.2.26 tell us that if another prime $p' \neq 2$ or 3 did divide $d_{L/K}$, then as a minimum $p'^3 | d_{L/K}$. The smallest prime $p' \neq 2$ or 3 is $p' = 5$. However $7^5 \cdot 5^3 > 2^6 \cdot 7^5$ and therefore 7 is the only prime (not equal to 2 or 3) that divides $d_{L/K}$. □

Now that we have considered the prime ideals that ramify tamely in our extension we must move our attention to the wildly ramified prime ideals. The only two ideals that would ramify wildly are the prime ideal $\mathfrak{p}$ generated by $(1 - j)$ in K_3/K and the prime ideal $\mathfrak{p}$ generated by 2 in K_2/K.

Proposition 3.2.28. *If the prime ideal* $\mathfrak{p}$ *generated by the prime element* $(1-j)$ *ramifies in* K_3/K *then* $3^2|d_{K_3/K}$.

Proof. If $\mathfrak{p}$ ramifies then it is totally and wildly ramified and hence $\mathfrak{P}^3|\mathcal{D}_{K_3/K}$. Taking absolute norms of both sides tells us that $3^3|(d_{K_3/K})^2$ and therefore it must be true that $3^2|d_{K_3/K}$. □

Proposition 3.2.29. *Let* A *be a cyclic division* K*-algebra. If the prime ideal* $\mathfrak{p}$ *generated by the prime element* $\pi = (1-j)$ *ramifies in* $K(\sqrt[6]{d})/K$ *then* $3^4|d_{L/K}$.

Proof. By Proposition 3.2.2 we know that $v_\pi(d) = 0$, therefore if $\mathfrak{p}$ ramifies then it will only be ramified in the subextension K_3/K, in which case $3^2|d_{K_3/K}$ by Proposition 3.2.28. Then using Proposition 2.3.5 we can see that $3^4|d_{L/K}$. □

Proposition 3.2.30. *If the prime ideal* $\mathfrak{p}$ *generated by the prime element* (2) *ramifies in* K_2/K *then* $2^2|d_{K_2/K}$.

Proof. If $\mathfrak{p}$ ramifies then it is totally and wildly ramified and hence $\mathfrak{P}^2|\mathcal{D}_{K_2/K}$. Taking absolute norms of both sides tells us that $2^4|(d_{K_2/K})^2$ and hence $2^2|d_{K_2/K}$. □

Proposition 3.2.31. *Let* A *be a cyclic division* K*-algebra. If the prime ideal* $\mathfrak{p}$ *generated by the prime element* $\pi = (2)$ *ramifies in* $K(\sqrt[6]{d})/K$ *then* $2^6|d_{L/K}$.

Proof. By Proposition 3.2.2 we know that $v_\pi(d) = 0$ or 3, therefore if $\mathfrak{p}$ ramifies then it will only be ramified in the subextension K_2/K, in which case $2^2|d_{K_2/K}$ by Proposition 3.2.30. Then using Proposition 2.3.5 we can see that this implies $2^6|d_{L/K}$. □

Corollary 3.2.32. *Let* A *be a cyclic division* K*-algebra such that* $d_{L/K} < 2^6 \cdot 7^5$. *Then the only prime ideals that ramify in* $K(\sqrt[6]{d})/K$ *are the prime ideals lying above* 7 *and we have* $d_{L/K} = 7^5$.

Proof. By Corollary 3.2.27 we need only consider the prime ideals lying above 2 and 3. If the prime ideal $\mathfrak{p}$ lying above 2 ramifies in $K(\sqrt[6]{d})/K$ then by Proposition 3.2.31 we know that $2^6|d_{L/K}$ and hence $2^6 \cdot 7^5|d_{L/K}$. If the prime ideal $\mathfrak{p}$ lying above 3 ramifies in $K(\sqrt[6]{d})/K$ then by Proposition 3.2.29 we know that $3^4|d_{L/K}$ and hence $3^4 \cdot 7^5|d_{L/K}$. However $3^4 \cdot 7^5 > 2^6 \cdot 7^5$, which completes the proof. □

Proposition 3.2.33. *Let A be a cyclic division K-algebra with $d_{L/K} = 7^5$. Then it is impossible to construct the cubic lattice from A.*

Proof. By Corollary 2.3.14 the cubic lattice cannot be constructed since $d_{L/K} < 6^6$. □

Hence for $[L : K] = 6$ we have shown that if $A = (\gamma, L/K, \sigma)$ is a cyclic division K-algebra with $\gamma \in \mathcal{O}_K$ and $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a code built on A that satisfies the energy constraint, then

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)} \geq 2^6 \cdot 7^5.$$

However we must also consider the case $\gamma \notin \mathcal{O}_K$.

The case $\gamma \notin \mathbb{Z}[j]$

In the degree 6 case we know that $d_{L/K} \geq 6^6$ and the price to pay in the coding gain by considering $\gamma \notin \mathcal{O}_K$ is a factor of $|\gamma_2|^{10} \geq 2^5$. Since $2^5 \cdot 6^6 > 2^6 \cdot 7^5$ we see that taking $\gamma \notin \mathcal{O}_K$ will not give rise to a better performing code.

Corollary 3.2.34. *Let $[L : K] = 6$ and let $A = (\gamma, L/K, \sigma)$ be a cyclic division K-algebra. If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a code built on A that satisfies the energy constraint, then*

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_{\xi}^{(m)} \geq 2^6 \cdot 7^5.$$

Hence the PSTBC of dimension 6 presented in [29] is optimal.

Chapter 4

Biquadratic Codes

4.1 Non-Cyclic Codes of Dimension four

4.1.1 Code Construction

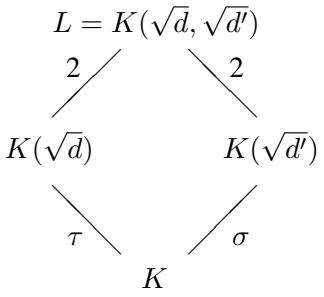
Having considered cyclic codes we now switch our attention to the case when the Galois group of L/K is non-cyclic. The obvious starting point for this is to consider codes when $Gal(L/K)$ is isomorphic to the Klein four-group $C_2 \times C_2$.

Codes based on crossed product algebras of degree 4 with non-cyclic Galois group have been studied in [4]. In [44] the authors consider constructions based on biquaternion algebras, which are included in the set of crossed product algebras with Galois group isomorphic to the Klein four-group. The constructions in [4] are also studied with regard to MIDO (multiple-input double-output) codes in [30], although we will not consider this here.

From now on we will assume that L/K is a non-cyclic Galois extension of degree four, i.e. $L = K(\sqrt{d}, \sqrt{d'})$, for some $d, d' \in K$. Note that the three distinct quadratic fields of L/K are $K(\sqrt{d})$, $K(\sqrt{d'})$ and $K(\sqrt{dd'})$. We have $Gal(L/K) = \{1, \sigma, \tau, \sigma\tau\}$, where σ and τ satisfy

$$\sigma(\sqrt{d}) = \sqrt{d}, \sigma(\sqrt{d'}) = -\sqrt{d'}$$
$$\tau(\sqrt{d}) = -\sqrt{d}, \tau(\sqrt{d'}) = \sqrt{d'}$$

so we have the following diagram:



Definition 4.1.1. *Let $a, b, u \in L^\times$ such that*

$$a^\sigma = a, b^\tau = b, uu^\sigma = \frac{a}{a^\tau}, uu^\tau = \frac{b^\sigma}{b}.$$

*Then the triple (a, b, u) is called (σ, τ)-**admissible**.*

Note that if (a, b, u) is (σ, τ)-admissible, then $(abu^\tau)^{\sigma\tau} = abu^\tau$. Therefore a, b and abu^τ are such that $a \in K(\sqrt{d})$, $b \in K(\sqrt{d'})$ and $abu^\tau \in K(\sqrt{dd'}) \simeq K(\sqrt{\frac{dd'}{(\gcd(d,d'))^2}})$.

Lemma 4.1.2. *Let $G = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\}$ and let (a, b, u) be (σ, τ)-admissible. Define a map $\xi^{a,b,u} : G \times G \to L^\times$ by*

$$\begin{gathered}
\xi^{a,b,u}_{\mathrm{Id},\tau} = \xi^{a,b,u}_{\sigma,\mathrm{Id}} = 1, \ \ \forall \sigma, \tau \in G \\
\xi^{a,b,u}_{\sigma,\sigma} = a, \xi^{a,b,u}_{\sigma,\tau} = 1, \xi^{a,b,u}_{\sigma,\sigma\tau} = a^\tau \\
\xi^{a,b,u}_{\tau,\sigma} = u, \xi^{a,b,u}_{\tau,\tau} = b, \xi^{a,b,u}_{\tau,\sigma\tau} = bu^\tau \\
\xi^{a,b,u}_{\sigma\tau,\sigma} = a^\tau u, \xi^{a,b,u}_{\sigma\tau,\tau} = b, \xi^{a,b,u}_{\sigma\tau,\sigma\tau} = abu^\tau
\end{gathered}$$

Then $\xi^{a,b,u}$ is a 2-cocycle.

Proof. By definition $\xi^{a,b,u}_{\mathrm{Id},\tau} = \xi^{a,b,u}_{\sigma,\mathrm{Id}} = 1$ for all $\sigma, \tau \in G$. Let (σ, τ, ρ) be a triple with entries in G. To check that $\xi^{a,b,u}$ is a 2-cocycle, we need to check that

$$\xi_{\sigma,\tau\rho}\xi_{\tau,\rho} = \xi_{\sigma\tau,\rho}\xi^\rho_{\sigma,\tau} \tag{4.1}$$

holds for all possible triples (σ, τ, ρ). It is not hard to check that Equation 4.1 holds if one of σ, ρ or τ is equal to Id, the remaining cases will be done individually.

(σ, σ, σ): The LHS of Equation 4.1 is equal to $\mathrm{Id} \cdot a$ and the RHS of Equation 4.1 is equal to $\mathrm{Id} \cdot a^\sigma = a$. Hence (σ, σ, σ) satisfies Equation 4.1.

(σ, σ, τ): The LHS is equal to $a^\tau \cdot \mathrm{Id}$ and the RHS is equal to $a^\tau \cdot \mathrm{Id}$.

$(\sigma, \sigma, \sigma\tau)$: The LHS is equal to $\mathrm{Id} \cdot a^\tau$ and the RHS is equal to $\mathrm{Id} \cdot a^{\sigma\tau} = a^\tau$.

(σ, τ, σ): The LHS is equal to $a^\tau \cdot u$ and the RHS is equal to $a^\tau u \cdot \mathrm{Id}$.

(σ, τ, τ): The LHS is equal to $\mathrm{Id} \cdot b$ and the RHS is equal to $b \cdot \mathrm{Id}$.

$(\sigma, \tau, \sigma\tau)$: The LHS is equal to $a \cdot bu^\tau$ and the RHS is equal to $abu^\tau \cdot \mathrm{Id}$.

$(\sigma, \sigma\tau, \sigma)$: The LHS is equal to $\mathrm{Id} \cdot a^\tau u$ and the RHS is equal to $u \cdot (a^\tau)^\sigma = a^\tau \cdot u$.

$(\sigma, \sigma\tau, \tau)$: The LHS is equal to $a \cdot b$ and the RHS is equal to $b \cdot (a^\tau)^\tau = a \cdot b$.

$(\sigma, \sigma\tau, \sigma\tau)$: The LHS is equal to $\mathrm{Id} \cdot abu^\tau$ and the RHS is equal to $bu^\tau \cdot (a^\tau)^{\sigma\tau} = a \cdot bu^\tau$.

(τ, σ, σ): The LHS is equal to $\mathrm{Id} \cdot a$ and the RHS is equal to $a^\tau u \cdot u^\sigma = a^\tau \cdot \frac{a}{a^\tau} = a$.

(τ, σ, τ): The LHS is equal to $bu^\tau \cdot \mathrm{Id}$ and the RHS is equal to $b \cdot u^\tau$.

$(\tau, \sigma, \sigma\tau)$: The LHS is equal to $b \cdot a^\tau$ and the RHS is equal to $abu^\tau \cdot u^{\sigma\tau} = ab \cdot (\frac{a}{a^\tau})^\tau = b \cdot a^\tau$.

(τ, τ, σ): The LHS is equal to $bu^\tau \cdot u = b \cdot \frac{b^\sigma}{b} = b^\sigma$ and the RHS is equal to $\mathrm{Id} \cdot b^{\sigma\tau} = b^\sigma$.

(τ, τ, τ): The LHS is equal to $\mathrm{Id} \cdot b$ and the RHS is equal to $\mathrm{Id} \cdot b^\tau = b$.

$(\tau, \tau, \sigma\tau)$:The LHS is equal to $u \cdot bu^\tau = b^\sigma$ and the RHS is equal to $\mathrm{Id} \cdot b^{\sigma\tau} = b^\sigma$.

$(\tau, \sigma\tau, \sigma)$: The LHS is equal to $b \cdot a^\tau u$ and the RHS is equal to $a \cdot (bu^\tau)^\sigma = ab^\sigma \cdot \frac{a^\tau}{au^\tau} = \frac{a^\tau b^\sigma}{u^\tau} = a^\tau bu$.

$(\tau, \sigma\tau, \tau)$: The LHS is equal to $u \cdot b$ and the RHS is equal to $\mathrm{Id} \cdot (bu^\tau)^\tau = b^\tau \cdot u = u \cdot b$.

$(\tau, \sigma\tau, \sigma\tau)$: The LHS is equal to $\mathrm{Id} \cdot abu^\tau$ and the RHS is equal to $a^\tau \cdot (bu^\tau)^{\sigma\tau} = (abu^\tau)^{\sigma\tau} = abu^\tau$

$(\sigma\tau, \sigma, \sigma)$: The LHS is equal to $\mathrm{Id} \cdot a$ and the RHS is equal to $u \cdot (a^\tau u)^\sigma = a^\tau u u^\sigma = a$.

$(\sigma\tau, \sigma, \tau)$: The LHS is equal to $\mathrm{Id} \cdot abu^\tau$ and the RHS is equal to $b \cdot (a^\tau u)^\tau = abu^\tau$.

$(\sigma\tau, \sigma, \sigma\tau)$: The LHS is equal to $b \cdot a^\tau$ and the RHS is equal to $bu^\tau \cdot (a^\tau u)^{\sigma\tau} = abu^\tau u^{\sigma\tau} = ab \cdot \frac{a^\tau}{a} = b \cdot a^\tau$.

$(\sigma\tau, \tau, \sigma)$: The LHS is equal to $abu^\tau \cdot u = ab \cdot \frac{b^\sigma}{b} = ab^\sigma$ and the RHS is equal to ab^σ.

$(\sigma\tau, \tau, \tau)$: The LHS is equal to $\mathrm{Id} \cdot b$ and the RHS is equal to $\mathrm{Id} \cdot b^\tau = b$.

$(\sigma\tau, \tau, \sigma\tau)$: The LHS is equal to $a^\tau u \cdot bu^\tau = a^\tau b \cdot \frac{b^\sigma}{b} = a^\tau b^\sigma$ and the RHS is equal to $a^\tau \cdot b^{\sigma\tau} = a^\tau b^\sigma$.

$(\sigma\tau, \sigma\tau, \sigma)$: The LHS is equal to $b \cdot a^\tau u$ and the RHS is equal to $\mathrm{Id} \cdot (abu^\tau)^\sigma = ab^\sigma u^{\sigma\tau} = a^\tau u u^\sigma b^\sigma u^{\sigma\tau} = a^\tau b^\sigma u \cdot \frac{b}{b^\sigma} = a^\tau bu$.

$(\sigma\tau, \sigma\tau, \tau)$: The LHS is equal to $a^\tau u \cdot b$ and the RHS is equal to $\mathrm{Id}(abu^\tau)^\tau = a^\tau bu$.

$(\sigma\tau, \sigma\tau, \sigma\tau)$: The LHS is equal to $\mathrm{Id} \cdot abu^\tau$ and the RHS is equal to $\mathrm{Id} \cdot (abu^\tau)^{\sigma\tau} = abu^\tau$. □

Definition 4.1.3. *[4] Given elements $a, b, u \in L^\times$ that satisfy the conditions of Lemma 4.1.2 a **biquadratic crossed product** K**-algebra** $A = (a, b, u, L/K, \sigma, \tau)$ is a crossed product K-algebra*

$$A = L \oplus eL \oplus fL \oplus efL$$

where

$$e^2 = a, f^2 = b, fe = efu, \lambda e = e\lambda^\sigma, \lambda f = f\lambda^\tau$$

for all $\lambda \in L$. Note that $A \simeq (\xi^{a,b,u}, L/K, Gal(L/K))$.

Lemma 4.1.4. *Let $(a, b, u, L/K, \sigma, \tau)$ be a biquadratic crossed product K-algebra, in particular (a, b, u) is (σ, τ)-admissible. Then (a, abu^τ, u) is $(\sigma, \sigma\tau)$-admissible and (abu^τ, b, u^τ) is $(\sigma\tau, \tau)$-admissible. Furthermore*

$$(a, b, u, L/K, \sigma, \tau) \simeq (a, abu^\tau, u, L/K, \sigma, \sigma\tau) \simeq (abu^\tau, b, u^\tau, L/K, \sigma\tau, \tau).$$

Proof. Assume that (a, b, u) is (σ, τ)-admissible and consider (a, abu^τ, u). Clearly $a^\sigma = a$ and by the remark after Definition 4.1.1 we have $(abu^\tau)^{\sigma\tau} = abu^\tau$. Since $a^\sigma = a$ we can also see that $uu^\sigma = \frac{a}{a^{\sigma\tau}}$. Finally we note that $\frac{(abu^\tau)^\sigma}{abu^\tau} = \frac{b^\sigma u^{\sigma\tau}}{bu^\tau} = uu^{\sigma\tau}$. Hence if (a, b, u) is (σ, τ)-admissible then (a, abu^τ, u) is $(\sigma, \sigma\tau)$-admissible. Similar arguments can be used to show that (abu^τ, b, u^τ) is $(\sigma\tau, \tau)$-admissible.

For the second part of the lemma, let e and f be generators of $(a, b, u, L/K, \sigma, \tau)$. Then the isomorphism

$$(a, b, u, L/K, \sigma, \tau) \simeq (a, abu^\tau, u, L/K, \sigma, \sigma\tau)$$

is obtained by taking e and ef as the new set of generators. Clearly we have $e^2 = a$ and $\lambda e = e\lambda^\sigma$ for al $\lambda \in L$. Furthermore

$$(ef)^2 = efef = e^2fuf = e^2f^2u^\tau = abu^\tau$$

and

$$\lambda(ef) = e\lambda^\sigma f = ef\lambda^{\sigma\tau}.$$

Similarly the isomorphism

$$(a, b, u, L/K, \sigma, \tau) \simeq (abu^\tau, b, u^\tau, L/K, \sigma\tau, \tau)$$

can be obtained by taking ef and f as the new set of generators. □

For the rest of this chapter we will only be concerned with codes constructed from biquadratic crossed product K-algebras. We will refer to such codes as **biquadratic codes** and as in the cyclic case we will require that our K-algebra is a division K-algebra so that our code is fully diverse. If $L = K(\sqrt{d}, \sqrt{d'})$ then as mentioned at the beginning of Section 4.1.1 we set

$$\sigma(\sqrt{d}) = \sqrt{d},\ \sigma(\sqrt{d'}) = -\sqrt{d'}$$
$$\tau(\sqrt{d}) = -\sqrt{d},\ \tau(\sqrt{d'}) = \sqrt{d'}.$$

We will also assume that our base field $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$. In order to construct biquadratic codes we need to compute the matrix of left multiplication M_x, for a given element $x \in A$.

Proposition 4.1.5. *Let $x = x_1 + x_\sigma e + x_\tau f + x_{\sigma\tau} ef \in A$. Its left multiplication matrix M_x is given by*

$$\begin{pmatrix} x_1 & a(x_\sigma)^\sigma & b(x_\tau)^\tau & abu^\tau(x_{\sigma\tau})^{\sigma\tau} \\ x_\sigma & (x_1)^\sigma & b(x_{\sigma\tau})^\tau & bu^\tau(x_\tau)^{\sigma\tau} \\ x_\tau & a^\tau u(x_{\sigma\tau})^\sigma & (x_1)^\tau & a^\tau(x_\sigma)^{\sigma\tau} \\ x_{\sigma\tau} & u(x_\tau)^\sigma & (x_\sigma)^\tau & (x_1)^{\sigma\tau} \end{pmatrix}.$$

Proof. Straightforward computation using Lemma 4.1.2. □

Recall we assume that $Gal(L/K)$ commutes with complex conjugation. In view of this, we have the following:

Proposition 4.1.6. *Let $A = (a, b, u, L/K, \sigma, \tau)$ be a biquadratic crossed product K-algebra as defined above. For a code constructed on A, the energy constraint is satisfied if and only if:*

1. $|a|^2 = |b|^2 = |u|^2 = 1$.

2. *The matrix*

$$W = \begin{pmatrix} \omega_1 & \omega_2 & \omega_3 & \omega_4 \\ \omega_1^\sigma & \omega_2^\sigma & \omega_3^\sigma & \omega_4^\sigma \\ \omega_1^\tau & \omega_2^\tau & \omega_3^\tau & \omega_4^\tau \\ \omega_1^{\sigma\tau} & \omega_2^{\sigma\tau} & \omega_3^{\sigma\tau} & \omega_4^{\sigma\tau} \end{pmatrix}$$

is unitary, where $\omega_1, \ldots, \omega_4$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Proof. By Proposition 2.2.1 we need $|\xi_{\rho,\gamma}|^2 = 1$ for all $\rho, \gamma \in Gal(L/K)$ and for $W = (\omega_\tau^\sigma)_{\sigma,\tau}$ to be unitary. By the definition of our 2-cocycle ξ and since $Gal(L/K)$ commutes with complex conjugation, the first part is equivalent to Condition 1 above. Condition 2 above is then clear. □

In view of Lemma 4.1.4 we remark here that the triple (a, b, u) satisfies Condition 1 of Proposition 4.1.6 if and only if $|a|^2 = |abu^\tau|^2 = |u|^2 = 1$ if and only if $|abu^\tau|^2 = |b|^2 = |u^\tau|^2 = 1$. Hence if a code constructed on $(a, b, u, L/K, \sigma, \tau)$ satisfies the energy constraint, then a code can also be constructed on $(a, abu^\tau, u, L/K, \sigma, \sigma\tau)$ and $(abu^\tau, b, u^\tau, L/K, \sigma\tau, \tau)$ that satisfies the energy constraint.

4.1.2 An Example

We end this section by describing the best known biquadratic code presented in [4]. Consider the biquadratic crossed product K-algebra

$$A = (a, b, u, L/K, \sigma, \tau) = (\zeta_8, \frac{\sqrt{5}}{1-2i}, i, \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i), \sigma, \tau).$$

In their paper the authors show that A is a division $\mathbb{Q}(i)$-algebra. Is also clear that

$$|a|^2 = |b|^2 = |u|^2 = 1.$$

In order to satisfy Condition 2 of Proposition 4.1.6 the authors restrict to an ideal $(\alpha)\mathcal{O}_L \subset L$. This ideal is defined as follows: let

$$\theta = \frac{1+\sqrt{5}}{2}, \text{ and } \alpha = 1 + i - i\theta$$

and define an $\mathcal{O}_K$-basis of $(\alpha)\mathcal{O}_L$ as

$$\{\omega_1, \ldots, \omega_4\} = \{\alpha, \alpha\theta, \alpha\zeta_8, \alpha\theta\zeta_8\}.$$

Furthermore define the scaling element as $\lambda = \frac{1}{\sqrt{10}}$. In this case the matrix $W_\lambda = D_\lambda W$ is unitary. Our codebook $\mathcal{C}$ is then taken as a subset of

$$\mathcal{C}_{A,\lambda,I} = \left\{ \begin{pmatrix} x_1 & a(x_\sigma)^\sigma & b(x_\tau)^\tau & ab(u)^\tau(x_{\sigma\tau})^{\sigma\tau} \\ x_\sigma & (x_1)^\sigma & b(x_{\sigma\tau})^\tau & b(u)^\tau(x_\tau)^{\sigma\tau} \\ x_\tau & (a)^\tau u(x_{\sigma\tau})^\sigma & (x_1)^\tau & (a)^\tau(x_\sigma)^{\sigma\tau} \\ x_{\sigma\tau} & u(x_\tau)^\sigma & (x_\sigma)^\tau & (x_1)^{\sigma\tau} \end{pmatrix} : x_1, x_\sigma, x_\tau, x_{\sigma\tau} \in (\alpha)\mathcal{O}_L \right\}.$$

We end this section by giving the minimum determinant $\delta_{\min}(\mathcal{C})$ of the code $\mathcal{C}$. By Corollary 2.4.3 we know that

$$\delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)}}$$

with $Gal(L/K)$ ordered as $\{\mathrm{Id}, \sigma, \tau, \sigma\tau\}$.

Let us first compute $d_{L/K}$. Since $\mathbb{Q}(i)(\sqrt{2}) \simeq \mathbb{Q}(\zeta_8)$ it is not difficult to compute that $d_{\mathbb{Q}(i)(\sqrt{2})/\mathbb{Q}(i)} = 4$. By Proposition 3.2.13 we know that $\mathfrak{p} = (1-i)$ is unramified in $\mathbb{Q}(i)(\sqrt{5})$ and so $d_{\mathbb{Q}(i)(\sqrt{5})/\mathbb{Q}(i)} = 5$. We can then use Proposition 2.3.5 to compute that $d_{L/K} = 400$.

We now need to consider the product $\prod_{m=1}^{n} \Delta_\xi^{(m)}$. Since $a = \zeta_8$, $b = \frac{\sqrt{5}}{1-2i}$ and $u = i$ we can compute that

$$\Delta_\xi^{(1)} = \Delta_\xi^{(2)} = 5$$
$$\Delta_\xi^{(3)} = \Delta_\xi^{(4)} = 1.$$

Hence, as the ideal $(\alpha)\mathcal{O}_L$ is principal, we have:

$$\delta_{\min}(\mathcal{C}) \geq \delta_{\min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{400 \cdot 5^2} = \frac{1}{10000}. \tag{4.2}$$

4.2 The Optimal Biquadratic Code

This section will be concerned with the optimality of the biquadratic code presented in [4]. In Section 3.2 we described the prime elements of $\mathbb{Z}[i]$ (respectively $\mathbb{Z}[j]$). We recall them here for ease:

1. A special prime $\pi = 1 - i$ (respectively $\pi = 1 - j$).

2. The inert primes of the form $p \equiv 3 \pmod 4$ (respectively $p \equiv 2 \pmod 3$), where p is a prime integer, denoted by S_3 (respectively T_2).

3. Prime elements of the form $\pi = a + bi$ (respectively $\pi = a + bj$) with $0 < a < b$, where $a^2 + b^2 = p \equiv 1 \pmod 4$ (respectively $a^2 + b^2 - ab \equiv 1 \pmod 3$), where p is a prime integer, denoted by S_1 (respectively T_1).

4. Conjugates of the prime elements $\pi \in S_1$ (respectively T_1), namely $\bar{\pi} = a - bi$ (respectively $\bar{\pi} = a + bj^2$).

Proposition 4.2.1. *Let $d \in \mathcal{O}_K^\times$ and assume that d is not divisible by any 2^{nd} power of $\mathcal{O}_K$. Then $d \cdot \bar{d} \in K^2$, if and only if the following hold:*

1. *The valuation $v_\pi(d)$ at the special prime ideal (π) is 0.*

2. *The valuation $v_\pi(d)$ at a prime ideal (π) generated by a prime $\pi \in S_3$ (respectively T_2) is 0 or 1.*

3. *The sum of the valuation $v_\pi(d)$ at a prime ideal (π) generated by a prime $\pi \in S_1$ (respectively T_1) and the valuation $v_{\bar{\pi}}(d)$ at its conjugate $\bar{\pi}$ is equal to 0 or 2.*

Proof. Follows the proof of Proposition 3.2.2 □

Lemma 4.2.2. *Assume $\zeta_n \in K$ and let $L = K(\sqrt{d}, \sqrt{d'})$. Then $Gal(L/K)$ commutes with complex conjugation if and only if $d.\bar{d} \in K^2$ and $d'.\bar{d'} \in K^2$.*

Proof. Very similar to the proof of Lemma 3.2.1. □

We will now split our argument into two cases. In the first case we will assume that our base field $K = \mathbb{Q}(i)$, we will then move on to consider the case $K = \mathbb{Q}(j)$.

4.2.1 The Case $K = \mathbb{Q}(i)$

Ramification in $\mathbb{Q}(i)(\sqrt{d}, \sqrt{d'})$

Proposition 4.2.1 tells us that $d, d' \in \mathbb{Z} \cdot u := \{z \cdot u | z \in Z, u \in \{\pm 1, \pm i\}\}$. Since -1 is a square in K we do not need to consider the cases $u = -1$ and $u = -i$. In particular the valuation on the special prime $1 - i$ tells us that the integer z must

be odd. However in this case we have $K(\sqrt{zi}) \simeq K(\sqrt{2z})$. Hence we can assume that $d, d' \in \mathbb{Z}^+$.

Let us first consider tame ramification in L/K.

Proposition 4.2.3. *Let π be a prime element of $\mathcal{O}_K$ lying above a prime $p_\pi \neq 2$. If $v_\pi(d) = 1$ or $v_\pi(d') = 1$, then $p_\pi^2 | d_{L/K}$.*

Proof. Assume that $\pi \in S_3$. Assume without loss of generality that $v_\pi(d) = 1$, in which case (π) totally ramifies in $K(\sqrt{d})/K$. Hence $p_\pi | d_{K(\sqrt{d})/K}$ and so by Proposition 2.3.5 we see that $p_\pi^2 | d_{L/K}$.

Now assume that $\pi \in S_1$. Again assume that $v_\pi(d) = 1$, which implies that $v_{\bar{\pi}}(d) = 1$. Hence (π) and $(\bar{\pi})$ are both totally ramified in $K(\sqrt{d})/K$ and so $p_\pi | d_{K(\sqrt{d})/K}$ and therefore $p_\pi^2 | d_{L/K}$ as above. □

We now consider the case of wild ramification, that is we consider the ramification of the prime ideal $\mathfrak{p} = (1 - i)$ in L/K.

By Proposition 1.2.14 we know that if $(1 - i)$ ramifies in L/K then it ramifies in $K(\sqrt{d})/K$ or $K(\sqrt{d'})/K$. Without loss of generality we will consider the ramification in $K(\sqrt{d})/K$. Recall that the element d is either an odd integer or the product of an odd integer and 2. We will refer to the former as Type I and the latter as Type II.

Proposition 4.2.4. *The prime ideal $\mathfrak{p} = (1 - i)$ ramifies in $K(\sqrt{d})/K$ if and only if d is of Type II, in which case an integral basis of $\mathcal{O}_{K(\sqrt{d})/\mathbb{Q}}$ is given by*

$$\{1, i, \sqrt{d}, \frac{i - i}{2}\sqrt{d}\}.$$

Proof. Assume that d is of Type I. By Theorem 1.2.25 we need to check if $x^2 \equiv d \pmod{(4)}$ has a solution in $\mathcal{O}_K$. If $d \equiv 1 \pmod 4$ then $x = 1$ satisfies the congruence and if $d \equiv -1 \pmod 4$ then $x = i$ satisfies the congruence. Hence $\mathfrak{p}$ is unramified in $K(\sqrt{d})/K$.

Now let d be of Type II and consider $x^2 \equiv d \pmod{(4)}$. Since $d \equiv 2 \pmod 4$ we consider $x^2 \equiv 2 \pmod{4\mathcal{O}_K}$. However, for any $x = a + bi \in \mathcal{O}_K$ we see that the real part of x^2 is equal to $a^2 - b^2$. Now $a^2 - b^2 \equiv 0 \text{ or } \pm 1 \pmod 4$. Hence $x^2 \equiv 2 \pmod{4\mathcal{O}_K}$ is insolvable and so $\mathfrak{p}$ ramifies in $K(\sqrt{d})/K$.

In order to compute the integral basis of $\mathcal{O}_{K(\sqrt{d})/\mathbb{Q}}$ we refer to Theorem 1 from [18], which gives an explicit description of the integral basis for any quartic field with a quadratic subfield. □

Recall from Section 1.2.4 that the m^{th} ramification group $G_m = G_m(L/K)$ of $\mathfrak{P}$ for $m = 0, 1, \ldots$ is defined as

$$G_m = \{g \in Z_{\mathfrak{P}} | g(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Corollary 4.2.5. *If $(1-i)$ ramifies in L/K then $2^4 | d_{L/K}$.*

Proof. By Proposition 4.2.4 we know that if $\mathfrak{p} = (1-i)$ ramifies in L/K then (without loss of generality) it ramifies in $K(\sqrt{d})/K$ where d is of Type II. Therefore the decomposition group of $K(\sqrt{d})/K$ is equal to $Gal(K(\sqrt{d})/K) = \{\mathrm{Id}, \sigma\}$, where $\sigma(\sqrt{d}) = -\sqrt{d}$. Denote by $\mathfrak{P}$ the prime ideal of $K(\sqrt{d})$ lying above $\mathfrak{p}$.

Now consider the 3^{rd} ramification group of $K(\sqrt{d})/K$:

$$\begin{aligned} G_3 &= \{g \in \{\mathrm{Id}, \sigma\} | g(\alpha) \equiv \alpha \pmod{\mathfrak{P}^4} \text{ for all } \alpha \in \mathcal{O}_{K(\sqrt{d})}\} \\ &= \{g \in \{\mathrm{Id}, \sigma\} | g(\alpha) \equiv \alpha \pmod{(2\mathcal{O}_{K(\sqrt{d})})} \text{ for all } \alpha \in \mathcal{O}_{K(\sqrt{d})}\}. \end{aligned}$$

Now any $\alpha \in \mathcal{O}_{K(\sqrt{d})}$ has the form $\alpha = \alpha_1 + \alpha_2 i + \alpha_3\sqrt{d} + \alpha_4 \frac{1-i}{2}\sqrt{d}$, where $\alpha_i \in \mathbb{Z}$. Hence $\sigma(\alpha) - \alpha = -2(\alpha_3\sqrt{d} + \alpha_4\frac{1-i}{2}\sqrt{d}) \in (2)\mathcal{O}_{K(\sqrt{d})}$. Therefore G_3 is non-trivial and by Proposition 1.2.41 we have $v_{\mathfrak{P}}(\mathcal{D}_{K(\sqrt{d})/K}) \geq 4$. This then gives $2^2 | d_{K(\sqrt{d})/K}$, which by Proposition 2.3.5 implies that $2^4 | d_{L/K}$. □

We end this section by remarking that in our extension L/K we must have at least two primes $p_1 \neq p_2$ such that $p_1 | d_{L/K}$ and $p_2 | d_{L/K}$. To see this consider the two subextensions $K(\sqrt{d})$ and $K(\sqrt{d'})$. Since $\mathbb{Q}(i)$ is its own Hilbert class field neither $K(\sqrt{d})/K$ nor $K(\sqrt{d'})/K$ can be unramified. Therefore, if there exists only a single prime p_1 such that $p_1 | d_{L/K}$ then $p_1 | d_{K(\sqrt{d})/K}$ and $p_1 | d_{K(\sqrt{d'})/K}$. However by our assumptions on d and d' this implies that $d = d'$ and we do not have a biquadratic extension of $\mathbb{Q}(i)$.

The Case A a Division Algebra

Proposition 4.2.6. *Let $A = (a, b, u, L/K, \sigma, \tau)$ be a division K-algebra. Then there exists a prime element $\pi \in S_1$ such that $v_\pi(d) = 1$ or $v_\pi(d') = 1$.*

Proof. Let M/K be a quadratic subextension of L/K (i.e. $M \simeq K(\sqrt{d}), K(\sqrt{d'})$ or $K(\sqrt{dd'})$) so that $A_M := A \otimes_K M$ is a quadratic K-subalgebra of A. In particular A_M is not a division K-algebra. If A is not a division K-algebra then this is clear and if A is a division K-algebra then this follows from Proposition 1.3.22.

Therefore $ind(A_M) \leq 2$ and $2[A]_M = 0 \in Br(M)$. Hence $2[A]$ is split by any such field M.

Now let K'/K be any extension in which d, d' or dd' is a square. Therefore $K \subset M \subset K'$ for at least one of the quadratic subextensions M. Hence K' splits $2[A]$, since M splits $2[A]$.

Assume that d and d' are not divisible by any prime element $\pi' \in S_1$. Let $\pi \neq 1 - i$ be any prime element of $\mathcal{O}_K$ and denote by $p_\pi \in \mathbb{Z}$ the prime number such that $\pi | p_\pi$. Note that by replacing d by $\frac{dd'}{p_\pi^2}$ if necessary, we can assume that $\pi \nmid d$.

We first consider the case $\pi \nmid d$ and $\pi \nmid d'$. If d (respectively d') is a square modulo $\pi\mathcal{O}_K$, then Hensel's lemma tells us that d (respectively d') is a square in K_π. If neither d nor d' is a square modulo $\pi\mathcal{O}_K$, then they both represent the unique non-trivial square class of $\mathcal{O}_K/\pi\mathcal{O}_K$. Therefore dd' is a non-zero square modulo $\pi\mathcal{O}_K$ and by Hensel's lemma is a square in K_π.

Now assume that $\pi \nmid d$ and $\pi | d'$. By assumption we then have $\pi = p \in S_3$. If d is a square modulo $p\mathbb{Z}$ then d is a square modulo $p\mathcal{O}_K$ and by Hensel's lemma is a square in K_p. Since $p \equiv 3 \pmod 4$, if d is not a square modulo $p\mathbb{Z}$ then d represents the class of -1 modulo $p\mathbb{Z}$. Therefore $-d$ is a square modulo $p\mathbb{Z}$ and hence modulo $p\mathcal{O}_K$. Since $d = (-d) \cdot i^2$, we see that d is also a square modulo $p\mathcal{O}_K$ and by Hensel's lemma is a square in K_π.

This tells us that if d and d' are not divisible by any prime $\pi \in S_1$ then $2[A]$ splits over K_π for all $\pi \neq 1 - i$. Therefore $2[A]$ splits over K_π for all π and hence $2[A] = 0$. Hence if A is a division K-algebra, then there must exist a prime element $\pi \in S_1$ such that $v_\pi(d) = 1$ or $v_\pi(d') = 1$. □

Proposition 4.2.7. *If a, b or $abu^\tau \in K$, then A is not a division K-algebra. Furthermore, if A satisfies the energy constraint then at most one of a, b, abu^τ lies in $\mathcal{O}_L$.*

Proof. First assume that $a \in K$. In this case e and $\sqrt{d'}$ generate a K-subalgebra $A_1 \simeq (a, d')_K$ of A. Now $deg(A_1) = 2$ and therefore the centralizer $Z_A(A_1)$ of A_1 in A also has degree 2. Since $Z(A_1) = K$, Theorem 1.3.6 tells us that $A \simeq A_1 \otimes_K Z_A(A_1)$. Therefore

$$2[A] = 2[A_1 \otimes_K Z_A(A_1)] = 2[A_1] + 2[Z_A(A_1)] = 0 \in Br(K)$$

and A is not a division K-algebra.

In the case $b \in K$ we can use a similar argument but replace e and $\sqrt{d'}$ by f and $\sqrt{d}$. In the case $abu^\tau \in K$ we can replace e and $\sqrt{d'}$ by ef and $\sqrt{dd'}$.

Recall that $a \in K(\sqrt{d})$, $b \in K(\sqrt{d'})$ and $abu^\tau \in K(\sqrt{dd'})$. Without loss of generality assume that $a \in \mathcal{O}_L$, so that $a \in \mathcal{O}_{K(\sqrt{d})}$. By Theorem 1.2.9 a must be a primitive root of unity and by above we know that $a \notin \{\pm 1, \pm i\}$. It is well known that for a primitive n^{th} root of unity ζ_n, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Since $[K(\sqrt{d}) : \mathbb{Q}] = 4$ we see that if $a = \zeta_n$, then $\varphi(n) \leq 4$. The only such n are $n = 2, 3, 4, 5, 6, 8, 10$ or 12. The cases $n = 5$ and $n = 10$ can be discarded since if $\zeta_5 \in K(\sqrt{d})$ then $\mathbb{Q}(i\zeta_5) \simeq \mathbb{Q}(\zeta_{20}) \subset K(\sqrt{d})$. However $[\mathbb{Q}(\zeta_{20}) : \mathbb{Q}] = 8$, which gives a contradiction.

Now if $a = \zeta_8$ then $\mathbb{Q}(\zeta_8) \subset K(\sqrt{d})$. Since $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$ we have $K(\sqrt{d}) \simeq \mathbb{Q}(\zeta_8)$. If $a = \zeta_3$ then $\mathbb{Q}(i\zeta_3) \simeq \mathbb{Q}(\zeta_{12}) \subset K(\sqrt{d})$ and so $K(\sqrt{d}) \simeq \mathbb{Q}(\zeta_{12})$. Similarly if $a = \zeta_6$ or ζ_{12} then $K(\sqrt{d}) \simeq \mathbb{Q}(\zeta_{12})$. We can argue in an analogous manner to show that if $b \in \mathcal{O}_L$ then $K(\sqrt{d'}) \simeq \mathbb{Q}(\zeta_8)$ or $\mathbb{Q}(\zeta_{12})$ and if $abu^\tau \in \mathcal{O}_L$ then $K(\sqrt{dd'}) \simeq \mathbb{Q}(\zeta_8)$ or $\mathbb{Q}(\zeta_{12})$.

Since $K(\sqrt{d})$, $K(\sqrt{d'})$ and $K(\sqrt{dd'})$ are distinct subfields of L we see that a, b and abu^τ cannot all lie in $\mathcal{O}_L$. Assume now that two of $\{a, b, abu^\tau\}$ lie in $\mathcal{O}_L$. In this case we see that L must be isomorphic to the compositum of $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\zeta_{12})$, i.e. $L \simeq \mathbb{Q}(\zeta_{24})$. However $d_{\mathbb{Q}(\zeta_{24})} = 2^{16} \cdot 3^4$. Since $d_K = -4$ we can then compute that

$$d_{L/K} = 2^4 \cdot 3^2 = 144 < 4^4.$$

By applying Corollary 2.3.14 we can then see that if A satisfies the energy constraint then at most one of a, b and abu^τ can lie in $\mathcal{O}_L$. □

Remark Since $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and our assumption that $d \in \mathbb{Z}^+$, we see that if $K(\sqrt{d}) \simeq \mathbb{Q}(\zeta_8)$ if and only if $d = 2$. Similarly, since $\sqrt{3} \in \mathbb{Q}(\zeta_{12})$ we have $K(\sqrt{d}) \simeq \mathbb{Q}(\zeta_{12})$ if and only if $d = 3$.

Proposition 4.2.8. *If* $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} < 10000$ *then* $256 \leq d_{L/K} < 2500$.

Proof. By Proposition 4.2.7 we can assume that $a \notin \mathcal{O}_L$ or $b \notin \mathcal{O}_L$. Consider first the case $a \notin \mathcal{O}_L$. By examining the multiplication matrix given in Proposition 4.1.5 we see that $\Delta_\xi^{(1)} \geq 2$ and $\Delta_\xi^{(3)} \geq 2$. Hence $\prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 4$, which immediately

gives the upper bound. If $b \notin \mathcal{O}_L$ then we can apply the same argument but we replace $\Delta_\xi^{(3)}$ by $\Delta_\xi^{(2)}$. The lower bound follows from Proposition 2.3.14. □

Proposition 4.2.9. *Assume that $A = (a, b, u, L/K, \sigma, \tau)$ is a division K-algebra. The only biquadratic extensions L/K that satisfy $256 \leq d_{L/K} < 2500$ are:*

$$K(\sqrt{2}, \sqrt{5}) : d_{L/K} = 400;$$
$$K(\sqrt{5}, \sqrt{7}) : d_{L/K} = 1225;$$
$$K(\sqrt{3}, \sqrt{13}) : d_{L/K} = 1521.$$

Proof. Note that if there exist three prime divisors $p_1 \neq p_2 \neq p_3$ of $d_{L/K}$ then $d_{L/K} \geq 2^4 \cdot 3^2 \cdot 5^2 = 3600$. Hence there must be exactly two prime divisors p_1 and p_2 of $d_{L/K}$.

Now by Propositions 4.2.6 and 4.2.3 we know that $p_1^2 | d_{L/K}$ for some prime $p_1 \equiv 1 \pmod 4$. By the previous results we also know that there exists a prime $p_2 \neq p_1$ such that $p_2^2 | d_{L/K}$ and in the special case that $p_2 = 2$ we have $2^4 | d_{L/K}$.

If $p_1 > 13$ then $d_{L/K} \geq 17^2 \cdot 3^2 = 2601$, so $p_1 = 5$ or 13. Let $p_1 = 13$ and assume that $p_2 \neq 3$ then $d_{L/K} \geq 13^2 \cdot 2^4 = 2704$. By the previous ramification results we see that if the only prime divisors of $d_{L/K}$ are 13 and 3 then $L \simeq K(\sqrt{3}, \sqrt{13})$ and $d_{L/K} = 3^2 \cdot 13^2 = 1521$.

Assume now that $p_1 = 5$ and $p_2 \geq 11$, then $d_{L/K} \geq 5^2 \cdot 11^2 = 3025$. Note if $p_1 = 5$ and $p_2 = 3$ then $d_{L/K} = 225 < 4^4$, so this case can also be discarded. Therefore it only remains to consider $p_2 = 2$ and $p_2 = 7$. As above we use the previous ramification results to see that if the only prime divisors of $d_{L/K}$ are 2 and 5 then $L \simeq K(\sqrt{2}, \sqrt{5})$ and as shown in Section 4.1.2 we have $d_{L/K} = 2^4 \cdot 5^2 = 400$. Similarly if the only prime divisors of $d_{L/K}$ are 5 and 7 then $L \simeq K(\sqrt{5}, \sqrt{7})$ and $d_{L/K} = 5^2 \cdot 7^2 = 1225$. This completes the proof. □

Lemma 4.2.10. *Let M/K be a quadratic extension such that complex conjugation is an automorphism of $M/\mathbb{Q}$ that commutes with $\mathrm{Gal}(M/K)$. Assume that there is only one prime ideal $\mathfrak{P}$ of $\mathcal{O}_M$ that lies above 2. Let $x \in M \backslash \mathcal{O}_M$ so that $x = x_1/x_2$ with $x_1 \in \mathcal{O}_M$ and x_2 in $\mathcal{O}_K$ satisfying $x_2 \nmid x_1$. If $|x|^2 = 1$ then $|x_2|^2 \geq 5$.*

Proof. We denote $M_0 := M \cap \mathbb{R}$, i.e. M_0 is a totally real quadratic field. As $x \notin \mathcal{O}_L$ we know that $x_2 \notin \mathcal{O}_K^\times$ so $|x_2|^2 \neq 1$. Furthermore there is no $a \in \mathcal{O}_K$ such that $|a|^2 = 3$. Therefore we need only show that $|x_2|^2 \neq 2$ or 4.

Assume to the contrary that $|x_2|^2 = 2$ or 4. Note that by the definition of M_0 this is equivalent to saying that $\mathrm{N}_{M/M_0}(x_2) = 2$ or 4. Write $y = x_2 \cdot x \in \mathcal{O}_M$. By the assumption that $|x|^2 = 1$, we then see that

$$\mathrm{N}_{M/M_0}(x_2) = \mathrm{N}_{M/M_0}(y) = 2 \text{ or } 4.$$

Therefore the prime ideals of $\mathcal{O}_M$ that divide $x_2\mathcal{O}_M$ and $y\mathcal{O}_M$ all lie above 2. By assumption $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_M$ that lies above 2, so $x_2\mathcal{O}_M = \mathfrak{P}^r$ and $y\mathcal{O}_M = \mathfrak{P}^s$ for some integers r and s. However $x_2\mathcal{O}_M$ and $y\mathcal{O}_M$ have the same absolute norms, which implies $r = s$ and hence $x_2\mathcal{O}_M = y\mathcal{O}_M$. This tells us that $y = x_2u$ for some unit $u \in \mathcal{O}_M^\times$. Therefore $y = x_2x = x_2u$ and so $x = u \in \mathcal{O}_M$, which is a contradiction. □

Proposition 4.2.11. *If $M = K(\sqrt{5})$, $K(\sqrt{10})$ or $K(\sqrt{13})$ then there is only one prime ideal $\mathfrak{P}$ of $\mathcal{O}_M$ that lies above 2.*

Proof. By Proposition 3.2.13 we know that $2\mathcal{O}_{K(\sqrt{5})} = \mathfrak{P}^2$. Now consider the field $K(\sqrt{10})$. By Proposition 4.2.4 we know that the prime ideal $(1-i)$ ramifies in $K(\sqrt{10})/K$ and hence $2\mathcal{O}_{K(\sqrt{10})} = \mathfrak{P}^4$.

Finally we consider $K(\sqrt{13})$. Clearly $K(\sqrt{13}) \cap \mathbb{R} = \mathbb{Q}(\sqrt{13})$, so let us consider the extension $\mathbb{Q}(\sqrt{13})/\mathbb{Q}$. Since the equation

$$x^2 \equiv 13 \pmod{(2)^3\mathbb{Z}}$$

is insolvable and the equation

$$x^2 \equiv 13 \pmod{(2)^2\mathbb{Z}}$$

is solvable, we see by Theorem 1.2.25 that $2\mathcal{O}_{K(\sqrt{13})} = \mathfrak{P}^2$. □

We now work through the three extensions L/K given in Proposition 4.2.9 and compute a lower bound for $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)}$ in each case.

Proposition 4.2.12. *If $L = K(\sqrt{2}, \sqrt{5})$ then $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 10000$.*

Proof. We know that one of $\{a, b, abu^\tau\}$ lies in $K(\sqrt{5})$ and by Theorem 1.2.9 and the remark following Proposition 4.2.7 we know that if it is of modulus 1 then it does

not lie in $\mathcal{O}_{K(\sqrt{5})}$. By examining the multiplication matrix given in Proposition 4.1.5 and applying Lemma 4.2.10, we see that $\Delta_\xi^{(1)} \geq 5$. If $a \in K(\sqrt{5})$ (respectively $b \in K(\sqrt{5})$) then $\Delta_\xi^{(3)} \geq 5$ (respectively $\Delta_\xi^{(2)} \geq 5$). Hence if $a \in K(\sqrt{5})$ or $b \in K(\sqrt{5})$ then

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 400 \cdot 5^2 = 10000.$$

If $a, b \notin K(\sqrt{5})$ then $a \in K(\sqrt{10})$ or $b \in K(\sqrt{10})$. Again we can apply Lemma 4.2.10 to see that in this case $\Delta_\xi^{(3)} \geq 5$ or $\Delta_\xi^{(2)} \geq 5$ respectively. We then conclude as above. □

Proposition 4.2.13. *If $L = K(\sqrt{5}, \sqrt{7})$ then $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} > 10000$.*

Proof. As above we know that $\Delta_\xi^{(1)} \geq 5$ and that if $a \in K(\sqrt{5})$ or $b \in K(\sqrt{5})$ then

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 1225 \cdot 5^2 > 10000.$$

Hence assume that $abu^\tau \in K(\sqrt{5})$. By Theorem 1.2.9 and the remark following Proposition 4.2.7 we see that if $|a|^2 = 1$ (respectively $|b|^2 = 1$) then $a \notin \mathcal{O}_L$ (respectively $b \notin \mathcal{O}_L$). Hence $\Delta_\xi^{(2)} \geq 2$ and $\Delta_\xi^{(3)} \geq 2$ and therefore

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 1225 \cdot 5 \cdot 2^2 > 10000.$$

□

Proposition 4.2.14. *If $L = K(\sqrt{3}, \sqrt{13})$ then $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} > 10000$.*

Proof. We know that one of $\{a, b, abu^\tau\}$ lies in $K(\sqrt{13})$ and by Theorem 1.2.9 and the remark following Proposition 4.2.7 we know that if it is of modulus 1 then it does not lie in $\mathcal{O}_{K(\sqrt{13})}$. Hence $\Delta_\xi^{(1)} \geq 5$ and if $a \in K(\sqrt{13})$ or $b \in K(\sqrt{13})$ then

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 1521 \cdot 5^2 > 10000.$$

Assume that $a, b \notin K(\sqrt{13})$. By Proposition 4.2.7 we know that (at least) one of a and b does not lie in $\mathcal{O}_L$. Hence $\Delta_\xi^{(2)} \geq 2$ or $\Delta_\xi^{(3)} \geq 2$ and therefore

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 1521 \cdot 5 \cdot 2 > 10000.$$

□

Hence if we restrict our base field to $K = \mathbb{Q}(i)$, then the code presented in [4] is optimal. However we also need to consider biquadratic codes with base field $K = \mathbb{Q}(j)$. This will be addressed in the next section.

4.2.2 The Case $K = \mathbb{Q}(j)$

Ramification in $\mathbb{Q}(j)(\sqrt{d}, \sqrt{d'})$

Similar to the case $K = \mathbb{Q}(i)$, we first present some ramification results. Proposition 4.2.1 tells us that $d, d' \in \mathbb{Z} \cdot u := \{z \cdot u | z \in Z, u \in \{\pm 1, \pm j, \pm j^2\}\}$. Since j is a square in K we see that

$$K(\sqrt{z}) \simeq K(\sqrt{zj}) \simeq K(\sqrt{zj^2}) \text{ and } K(\sqrt{-z}) \simeq K(\sqrt{-zj}) \simeq K(\sqrt{-zj^2}).$$

Therefore we will always assume that $d, d' \in \mathbb{Z}$. Furthermore the valuation on the special prime $1 - j$ tells us that the integer z cannot be divisible by 3 and hence $3 \nmid d_{L/K}$.

Let us consider ramification in L/K.

Proposition 4.2.15. *Let π be a prime element of $\mathcal{O}_K$ lying above a prime $p_\pi \neq 2$. If $v_\pi(d) = 1$ or $v_\pi(d') = 1$, then $p_\pi^2 | d_{L/K}$. If the prime ideal generated by the prime element $2 \in \mathcal{O}_K$ ramifies in $K(\sqrt{d})$ or $K(\sqrt{d'})$ then $2^4 | d_{L/K}$.*

Proof. The first part of the proof is identical to the proof of Proposition 4.2.3. Now if (2) ramifies in $K(\sqrt{d})$ then it is wildly ramified. By Proposition 1.2.30 we then see that $(2)^2 | \mathfrak{d}_{K(\sqrt{d})/K}$. We can then apply Proposition 2.3.5 to see that $2^4 | d_{L/K}$. □

Proposition 4.2.16. *Let M be a quadratic subextension of L/K. If $M = K(\sqrt{z})$, where $z = 2z_1$ for z_1 an odd integer, then (2) ramifies in M/K and hence $2^4 | d_{L/K}$. If $M = K(\sqrt{z})$ for some odd integer z, then (2) ramifies in M/K if and only if $z \equiv 3 \pmod 4$.*

Proof. In the first case $v_2(z) = 1$ by assumption. Hence (2) ramifies in M/K by Proposition 1.2.24. We then use Proposition 4.2.15 to complete the proof. In the second case we have $z \equiv 1$ or $3 \pmod 4$. If $z \equiv 1 \pmod 4$ then the equation $x^2 \equiv z \pmod{(4)\mathcal{O}_K}$ is clearly solvable. Hence by Theorem 1.2.25 (2)

is unramified in M/K. Now assume that $z \equiv 3 \pmod 4$. In this case the equation $x^2 \equiv z \pmod{(4)\mathcal{O}_K}$ is not solvable and therefore (2) ramifies in $K(\sqrt{z})$. $\square$

Note that the above proposition implies if (2) ramifies in $K(\sqrt{z})/K$ for some odd integer z, then (2) does not ramify in $K(\sqrt{-z})/K$. The converse also holds.

Proposition 4.2.17. *If $M = K(\sqrt{2})$ or $K(\sqrt{-2})$ then $d_{M/K} = 2^3$. If $M = K(\sqrt{-1})$ then $d_{M/K} = 2^2$.*

Proof. Recall that $d_K = -3$ and in all three cases we know that the only prime ideal that ramifies in M/K is (2). Assume $M = K(\sqrt{2})$, in which case it is clear that $M_0 := M \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$ and it is well known that $d_{\mathbb{Q}(\sqrt{2})} = 2^3$. By the tower of discriminants formula we have

$$d_M = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) \cdot (-3)^2 = \mathrm{N}_{M_0/\mathbb{Q}}(\mathfrak{d}_{M/M_0}) \cdot (2^3)^2.$$

We can therefore conclude that

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) = (d_{M/K})^2 = 2^6.$$

and so $d_{M/K} = 2^3$.

Now assume that $M = K(\sqrt{-2})$, in which case $M_0 = \mathbb{Q}(\sqrt{6})$ and it well known that $d_{M_0} = 2^3 \cdot 3$. However, since 2 and 3 both ramify in $M_0/\mathbb{Q}$ we see that M/M_0 is an unramified extension. The tower of discriminants formula then gives

$$d_M = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) \cdot (-3)^2 = (2^3 \cdot 3)^2.$$

Hence

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) = (d_{M/K})^2 = 2^6.$$

and so $d_{M/K} = 2^3$.

Finally assume that $M = K(\sqrt{-1})$, in which case $M_0 = \mathbb{Q}(\sqrt{3})$ and $d_{M_0} = 2^2 \cdot 3$. As above 2 and 3 both ramify in $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ and therefore

$$d_M = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) \cdot (-3)^2 = (2^2 \cdot 3)^2.$$

Hence

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{M/K}) = (d_{M/K})^2 = 2^4.$$

and so $d_{M/K} = 2^2$. $\square$

Corollary 4.2.18. *Let $M = K(\sqrt{2z})$ for some square-free odd integer z, which by assumption is not divisible by 3. Then $d_{M/K} = 2^3 \cdot z$.*

Proof. Assume z is positive. Then $M_0 = \mathbb{Q}(\sqrt{2z})$ and $d_{\mathbb{Q}(\sqrt{2z})} = 2^3 \cdot z$. If z is negative then $M_0 = \mathbb{Q}(\sqrt{6z})$ and $d_{\mathbb{Q}(\sqrt{6z})} = 2^3 \cdot 3 \cdot z$. In both cases we can proceed as in the proof of Proposition 4.2.17 and make use of Proposition 4.2.15 to conclude. □

Proposition 4.2.19. *Let $L = K(\sqrt{d}, \sqrt{d'})$ and let π be a prime element of $\mathcal{O}_K$ with $p_\pi \neq 2$. If $v_\pi(d) = 1$ or $v_\pi(d') = 1$ (i.e. if $p_\pi | d_{L/K}$) then there exists a prime $p_{\pi'} \neq p_\pi$ such that $p_\pi^2 \cdot p_{\pi'}^2 | d_{L/K}$ if $p_{\pi'}$ is odd and $p_\pi^2 \cdot 2^4 | d_{L/K}$ if $p_{\pi'} = 2$.*

Proof. By assumption π is a prime element of $\mathcal{O}_K$ with $p_\pi \neq 2$. Let π' be another prime element of $\mathcal{O}_K$ with $p_{\pi'} \neq p_\pi$. If $v_{\pi'}(d) = 1$ or $v_{\pi'}(d') = 1$ then we can use Propositions 4.2.15 and 4.2.16 to give us the result. Hence we can assume that the only prime that divides d and d' is p_π. However this implies that $L \simeq K(\sqrt{p_\pi}, \sqrt{-p_\pi})$ and by the remark after Proposition 4.2.16 we see that (2) must also ramify in L/K and so $2^4 | d_{L/K}$. □

The Case A a Division Algebra

Proposition 4.2.20. *If a, b or $abu^\tau \in K$, then $A = (a, b, u, L/K, \sigma, \tau)$ is not a division K-algebra. Furthermore, if A satisfies the energy constraint then at most one of a, b, abu^τ lies in $\mathcal{O}_L$.*

Proof. The first part of the proof is the same as Proposition 4.2.7.

For the second part let M be a quadratic subextension of L/K. Since $[M : \mathbb{Q}] = 4$ we see that if $\zeta_n \in M$ then $n = 2, 3, 4, 5, 6, 8, 10$ or 12. However the cases $n = 5$ and $n = 10$ can be discarded. Assume $\zeta_5 \in M$ then $\mathbb{Q}(j\zeta_5) \simeq \mathbb{Q}(\zeta_{15}) \subset M$. Since $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = 8$, we then get a contradiction. Similarly the case $n = 8$ can be discarded. In this case $\mathbb{Q}(j\zeta_8) \simeq \mathbb{Q}(\zeta_{24}) \subset M$. Since $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = 8$, we again get a contradiction.

Finally consider $n = 4$ (or similarly $n = 12$). If $\zeta_4 \in M$ then $\mathbb{Q}(ji) \simeq \mathbb{Q}(\zeta_{12}) \subset M$. Since $[\mathbb{Q}(\zeta_{12}) : \mathbb{Q}] = 4$ we see that $M \simeq \mathbb{Q}(\zeta_{12})$. Hence the only quadratic extension M/K that contains a primitive root of unity not contained in K is $M \simeq \mathbb{Q}(\zeta_{12}) \simeq K(\sqrt{-1})$.

Recall that $K(\sqrt{d})$, $K(\sqrt{d'})$ and $K(\sqrt{dd'})$ are distinct subfields of L. Furthermore $a \in K(\sqrt{d})$, $b \in K(\sqrt{d'})$ and $abu^\tau \in K(\sqrt{dd'})$. Therefore we can conclude that if A satisfies the energy constraint, then at most one of a, b, abu^τ lies in $\mathcal{O}_L$. □

Proposition 4.2.21. *If* $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} < 10000$ *then* $256 \leq d_{L/K} < 1112$.

Proof. Since Proposition 4.2.20 holds, we can mimic the proof of Proposition 4.2.8. However we note that the equation $|x|^2 = 2$ has no solutions for $x \in \mathcal{O}_K$. Hence in the case $a \notin \mathcal{O}_L$ we must have $\Delta_\xi^{(1)} \geq 3$ and $\Delta_\xi^{(3)} \geq 3$. Therefore $\prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 9$, which immediately gives the upper bound. If $b \notin \mathcal{O}_L$ then we can apply the same argument but we replace $\Delta_\xi^{(3)}$ by $\Delta_\xi^{(2)}$. The lower bound follows from Proposition 2.3.14. □

Proposition 4.2.22. *If* $(a, b, u, L/K, \sigma, \tau)$ *is a division* K*-algebra such that* $256 \leq d_{L/K} < 1112$ *then* $L \simeq K(\sqrt{-1}, \sqrt{7})$ *and* $d_{L/K} = 784$.

Proof. If p_1, p_2, p_3 are three distinct prime numbers that all divide $d_{L/K}$ then $d_{L/K} \geq 2^4 \cdot 5^2 \cdot 7^2 > 1112$. Hence there are at most two primes $p_1 \neq p_2$ such that $p_1 | d_{L/K}$ and $p_2 | d_{L/K}$. Assume (without loss of generality) that $p_1 \neq 2$. If $p_1 \geq 11$ then by Proposition 4.2.19 we have $d_{L/K} \geq 11^2 \cdot 2^4 > 1112$. Hence all the prime divisors of d and d' belong to $\{2, 5, 7\}$.

We now show that if A is a division K-algebra then 7 must divide d or d'. Assume on the contrary that d and d' are not divisible by 7. Let $\pi \neq 2$ be any prime element of $\mathcal{O}_K$. By replacing d by $\frac{dd'}{p_\pi^2}$ if necessary, we can assume that $\pi \nmid d$.

First consider the case $\pi \nmid d$ and $\pi \nmid d'$. As in the proof of Proposition 4.2.6, if d (respectively d') is a square modulo $\pi\mathcal{O}_K$ then d (respectively d') is a square in K_π. If neither d nor d' is a square modulo $\pi\mathcal{O}_K$, then dd' is a square modulo $\pi\mathcal{O}_K$ and hence a square in K_π.

Now assume $\pi \nmid d$ and $\pi | d'$. By assumption this implies that $\pi = 5$. If d is a square modulo $5\mathbb{Z}$, then d is a square modulo $5\mathcal{O}_K$ and by Hensel's lemma d is a square in K_π. If d is not a square modulo $5\mathbb{Z}$, then $d \equiv 2 \text{ or } 3 \pmod 5$. If $d \equiv 2 \pmod 5$ then $d \equiv (1 + 2j)^2 \pmod{5\mathcal{O}_K}$ and if $d \equiv 3 \pmod 5$ then $d \equiv (2 + 4j)^2 \pmod{5\mathcal{O}_K}$. In either case d is a square modulo $\pi\mathcal{O}_K$ and hence a square in K_π.

Therefore if $d_{L/K} < 1112$ and d and d' are not divisible by 7 then $2[A]$ splits over K_π for all $\pi \neq 2$. Hence $2[A]$ splits over K_π for all π and hence $2[A] = 0$ and A is not a division K-algebra.

We now note that if $v_5(d) = 1$ or $v_5(d') = 1$ then $d_{L/K} \geq 7^2 \cdot 5^2 = 1225$. Therefore the only prime divisors of d and d' are 2 and 7. However by Corollary 4.2.18 and Proposition 2.3.5 we see that if d or d' is divisible by 2, then $d_{L/K} \geq 2^6 \cdot 7^2 = 3136$. Hence the only possible case is $L \simeq K(\sqrt{-1}, \sqrt{7})$ and we can use Proposition 4.2.17 and Proposition 2.3.5 to see that $d_{L/K} = 2^4 \cdot 7^2 = 784$.

□

Proposition 4.2.23. *If $(a, b, u, K(\sqrt{7}, \sqrt{-1})/K, \sigma, \tau)$ is a division K-algebra then* $d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} > 10000$.

Proof. Consider the subfield $K(\sqrt{7}) \subset L$ and let $c \in K(\sqrt{7}) \backslash K$ such that $|c|^2 = 1$. Since the only roots of unity in $K(\sqrt{7})$ are $\{\pm 1, \pm j, \pm j^2\}$, we know that $c \notin \mathcal{O}_{K(\sqrt{7})}$, i.e. $c = c_1/c_2$ with $c_1 \in \mathcal{O}_{K(\sqrt{7})}$, $c_2 \in \mathcal{O}_K$ and $c_2 \nmid c_1$. Since $c \notin K$ we see that $c_1 \notin \mathcal{O}_K$. Note that as $|c|^2 = 1$ we have $|c_1|^2 = |c_2|^2$.

By [18] we can compute that $\{1, -j^2, \sqrt{7}, -j\sqrt{7}\}$ is an integral basis for $\mathcal{O}_{K(\sqrt{7})}$. Hence $c_1 = w + x(-j^2) + y\sqrt{7} + z(-j\sqrt{7})$ with $w, x, y, z \in \mathbb{Z}$. We can then calculate that

$$|c_1|^2 = w^2 + x^2 + wx + 7y^2 + 7z^2 + 7yz + 2wy\sqrt{7} + wz\sqrt{7} + xy\sqrt{7} - xz\sqrt{7}.$$

Now $|c_1|^2 = |c_2|^2$ and $|c_2|^2 \in \mathbb{Z}$, so for our purposes we need not consider the terms that include $\sqrt{7}$.

Since $c_1 \in \mathcal{O}_{K(\sqrt{7})} \backslash \mathcal{O}_K$, at least one of the terms y, z must be non-zero. Therefore we can compute that $|c_1|^2 \geq 7$ and hence $|c_2|^2 \geq 7$.

We know that one of a, b, abu^τ lies in $K(\sqrt{7})$, therefore we can see that $\Delta_\xi^{(1)} \geq 7$. If $a \in K(\sqrt{7})$ then $\Delta_\xi^{(3)} \geq 7$ and if $b \in K(\sqrt{7})$ then $\Delta_\xi^{(2)} \geq 7$. In either case we can conclude that

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 784 \cdot 7^2 = 38416.$$

We can therefore assume that $abu^\tau \in K(\sqrt{7})$. However by Proposition 4.2.20 we know that a or b does not lie in $\mathcal{O}_L$. If $a \notin \mathcal{O}_L$ then $\Delta_\xi^{(3)} \geq 3$ and if $b \notin$ then

$\Delta_\xi^{(2)} \geq 3$. In either case we can conclude that

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 784 \cdot 3 \cdot 7 = 16464.$$

This completes the proof. □

Corollary 4.2.24. *Let $A = (a, b, u, L/K, \sigma, \tau)$ be a biquadratic crossed product division K-algebra. If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a code built on A that satisfies the energy constraint, then*

$$d_{L/K} \cdot \prod_{m=1}^{n} \Delta_\xi^{(m)} \geq 10000.$$

Hence the biquadratic code presented in [4] is optimal.

Bibliography

[1] S.M. Alamouti. A simple transmit diversity technique for wireless communications. *Selected Areas in Communications, IEEE Journal on*, 16(8):1451 –1458, October 1998.

[2] J.-C. Belfiore and G. Rekaya. Quaternionic lattices for space-time coding. In *Information Theory Workshop, 2003. Proceedings. 2003 IEEE*, 2003.

[3] J.-C. Belfiore, G. Rekaya, and E. Viterbo. The Golden code: a 2×2 full-rate space-time code with nonvanishing determinants. *IEEE Trans. Inform. Theory*, 51(4):1432–1436, 2005.

[4] G. Berhuy and F. Oggier. Space-time codes from crossed product algebras of degree 4. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, pages 90–99. Springer, Berlin, 2007.

[5] G. Berhuy and F. Oggier. On the existence of perfect space-time codes. *IEEE Transactions on Information Theory*, 55(5):2078 – 2082, 2009.

[6] A.J. Berrick and ME Keating. *An introduction to rings and modules with K-theory in view*. Cambridge Univ Pr, 2000.

[7] E. Biglieri, J. Proakis, and S. Shamai. Fading channels: Information-theoretic and communications aspects. *Information Theory, IEEE Transactions on*, 44(6):2619–2692, 1998.

[8] R.C. Daileda. Algebraic integers on the unit circle. *Journal of Number Theory*, 118(2):189–191, 2006.

[9] P. Dayal and M.K. Varanasi. An optimal two transmit antenna space-time code and its stacked extensions. *Information Theory, IEEE Transactions on*, 51(12):4348 – 4355, 2005.

[10] P. K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[11] P. Elia, B. A. Sethuraman, and P. V. Kumar. Perfect space-time codes for any number of antennas. *IEEE Trans. Inform. Theory*, 53(11):3853–3868, 2007.

[12] I.B. Fesenko and S.V. Vostokov. *Local fields and their extensions*. American Mathematical Society, 2002.

[13] G.J. Foschini and M.J. Gans. On limits of wireless communications in a fading environment when using multiple antennas. *Wireless personal communications*, 6(3):311–335, 1998.

[14] J.-C. Guey, M.P. Fitz, M.R. Bell, and W.-Y. Kuo. Signal design for transmitter diversity wireless communication systems over rayleigh fading channels. *Communications, IEEE Transactions on*, 47(4):527 –537, apr. 1999.

[15] H. Hasse. Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. *Math. Ann.*, 104(1):495–534, 1931.

[16] H. Hasse. Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. *Math. Ann.*, 107(1):731–760, 1933.

[17] B. Hassibi and B.M. Hochwald. High-rate codes that are linear in space and time. *Information Theory, IEEE Transactions on*, 48(7):1804–1824, 2002.

[18] J. G. Huard, B. K. Spearman, and K. S. Williams. Integral bases for quartic fields with quadratic subfields. *J. Number Theory*, 51(1):87–102, 1995.

[19] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[20] A. W. Knapp. *Advanced algebra*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2007.

[21] H. Koch. *Algebraic number theory*. Springer-Verlag, Berlin, russian edition, 1997. Reprint of the 1992 translation.

[22] H. Koch. *Number Theory*, volume 24 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2000. Algebraic Numbers and Functions, Translated from the 1997 German original by David Kramer.

[23] S. Lang. *Algebraic Number Theory*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

[24] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[25] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[26] H. Napias. A generalization of the LLL-algorithm over Euclidean rings or orders. *J. Théor. Nombres Bordeaux*, 8(2):387–396, 1996.

[27] F. Oggier. On the optimality of the golden code. In *IEEE Information Theory Workshop (ITW'06)*, 2006.

[28] F. Oggier, J.-C. Belfiore, and E. Viterbo. Cyclic division algebras: A tool for space-time coding. *Found. Trends Commun. Inf. Theory*, 4(1):1–95, 2007.

[29] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo. Perfect space-time block codes. *IEEE Trans. Inform. Theory*, 52(9):3885–3902, 2006.

[30] F. Oggier, R. Vehkalahti, and C. Hollanti. Fast-decodable MIDO codes from crossed product algebras. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1080–1084. IEEE, 2010.

[31] R.S. Pierce. *Associative Algebras*. Springer Verlag, 1982.

[32] P. Roquette. The Brauer-Hasse-Noether Theorem in historical perspective., volume 15 of Schriftenreihe der Heidelberger Akademie der Wissenschaften, 2004.

[33] W. Scharlau. *Quadratic and Hermitian Forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[34] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Trans. Inform. Theory*, 49(10):2596–2616, 2003. Special issue on space-time transmission, reception, coding and signal processing.

[35] B.A. Sethuraman and B.S. Rajan. An algebraic description of orthogonal designs and the uniqueness of the alamouti code. In *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, volume 2, pages 1088 – 1092 vol.2, 2002.

[36] B.A. Sethuraman and B. Sundar Rajan. Full-rank, full-rate STBCs from division algebras. In *Information Theory Workshop, 2002. Proceedings of the 2002 IEEE*, pages 69 – 72, 2002.

[37] V. Shashidhar, B. Sundar Rajan, and B. A. Sethuraman. Information-lossless space-time block codes from crossed-product algebras. *IEEE Trans. Inform. Theory*, 52(9):3913–3935, 2006.

[38] V. Shashidhar, B.S. Rajan, and B.A. Sethuraman. STBCs using capacity achieving designs from cyclic division algebras. In *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, volume 4, pages 1957 – 1962 vol.4, 2003.

[39] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[40] I. Stewart and D. Tall. *Algebraic number theory*. Chapman and Hall Mathematics Series. Chapman & Hall, London, second edition, 1987.

[41] V. Tarokh, H. Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Inform. Theory*, 45:1456–1467, 1999.

[42] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communication: performance criterion and code construction. *IEEE Trans. Inform. Theory*, 44(2):744–765, 1998.

[43] E. Telatar. Capacity of multi-antenna gaussian channels. *European Transactions on Telecommunications*, 10:585–595, 1999.

[44] T. Unger and N. Markin. Quadratic forms and space-time block codes from generalized quaternion and biquaternion algebras. *Arxiv preprint arXiv:0807.0199*, 2008.

[45] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto. On the densest MIMO lattices from cyclic division algebras. *IEEE Trans. Inform. Theory*, 55(8):3751–3780, 2009.

[46] L.C. Washington. *Introduction to cyclotomic fields*. Springer Verlag, 1997.

[47] H. Yao and G.W. Wornell. Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes. In *Proceedings of the Annual Allerton Conference on Communication, Control and Computing*, volume 41, pages 400–409. The University; 1998, 2003.