Lattice theoretic approach to space-time codes from division algebras
Preface

I discovered coding theory for the first time while attending a class given by Professor Amin Shokrollahi at EPFL, entitled An introduction to coding theory. I started enjoying it immediately, and I began to consider the idea of studying this subject more closely in my master thesis. Professor Eva Bayer then told me about a book written by Grégory Berhuy and Frédérique Oggier, Introduction to central simple algebras and their applications to wireless communication [1], and placed me under the supervision of Dr. Roope Vehkilahiti.

One of the reasons I have chosen this subject is that it establishes a theory in an area where many different branches of mathematics merge. In that sense, throughout this master thesis the reader will be lead from an engineering problem and will arrive to an expression in terms of mathematical problems involving lattice theory, central simple algebras, algebraic number theory, and even some analysis.

J’aimerais remercier Eva Bayer sans qui je n’aurais pas fait un projet qui m’a tant motivé, et qui m’a placé dans des conditions de travail adéquates. J’aimerais spécialement remercier Roope qui a su à la fois être flexible et rigoureux dans son rôle d’assistant, et avec qui j’ai eu beaucoup de plaisir à travailler. Il m’a aussi permis de découvrir le domaine de recherche dans lequel il est actif. Je lui suis aussi reconnaissant pour les heures qu’il a passées à relire mon projet et à y apporter des corrections. Il comprendra, j’en suis sûr, ces quelques lignes de remerciements en français. Je remercie aussi David, Kate et Eeva de m’avoir si chaleureusement accueilli dans leur bureau, et qui ont toujours su contribuer à la bonne ambiance qui y régnait. Je profite aussi de ces remerciements pour exprimer ma gratitude envers toutes les personnes qui m’ont aidé et soutenu durant ce semestre qui met un terme à près de cinq années d’études en mathématiques à l’EPFL, une école que j’ai particulièrement appréciée. Un merci spécial va pour mes parents, le reste de ma famille et mes amis.
## Contents

### Preface

1 Introduction and motivation

1.1 Evolution of classical coding theory

1.2 Space-time codes

1.3 Designing codes

1.4 Thesis context and problem to study

2 Lattices

2.1 Basic definitions and results

2.2 Lattices in $M_n(C)$

2.3 Fundamental paralleloptopes of special lattices

3 Codes from number fields

3.1 Preliminaries

3.2 Construction of the codes and properties

4 Central simple algebras

4.1 Introduction to $K$-algebras

4.2 Introduction to central simple algebras

5 Splitting fields of central simple algebras

5.1 Preliminaries

5.2 Splitting fields

5.3 Galois splitting fields

5.4 The reduced characteristic polynomial

6 Codes from cyclic division algebras

6.1 Definitions and properties

6.2 Geometric structure

6.3 Construction of the codes and properties

7 Codes from crossed products

7.1 Definitions and properties

7.2 Geometric structure

7.3 Construction of the codes and properties
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conclusion</strong></td>
<td>81</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>83</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>85</td>
</tr>
</tbody>
</table>
1 Introduction and motivation

1.1 Evolution of classical coding theory

Coding theory is about transmitting a message, called a code, from a sender to a receiver, through a communication channel that is unreliable, in the sense that the code is changed when it reaches the receiver.

The goal of coding theory is twofold. It first aims at building models where the information sent can be recovered after going through the communication channel, this is referred to as the encoding, then, given a corrupted information the recovering part is called decoding. In this master thesis, very little attention is paid on decoding algorithms. Instead, we will focus on giving explicit code constructions, taking the decoding task in consideration.

I now want to quote what the authors of [1] have given as first sentence of their book: *Algebra has played a central role in coding theory since its early age*. Indeed, one of the first type of codes that appeared consisted of a set $C$ of vectors in $\mathbb{F}_q^n$ which forms a $k$-dimensional vector space over $\mathbb{F}_q$, the finite field with $q$ elements. The parameter $n$ is called the block length of $C$, the ratio $k/n$ gives the dimension rate, and the ratio $\log_q(|C|)/n$ gives the symbol rate of the code. Vectors of $C$ are called codewords. The minimum distance of a code is then the smallest Hamming distance between two distinct codewords, where the Hamming distance counts the number of entries in which the two codewords differ.

Classical coding theory involves one transmitter and one receiver. Say the transmitter sends a codeword from the aforementioned code. Then, we say that the communication channel is discrete and the channel model is given by

$$y = x + v,$$  \hspace{1cm} (1.1)

where $x, y, v$ are $n$-dimensional vectors over $\mathbb{F}_q$. The vector $x$ is the transmitted information, the vector $v$ symbolizes the unreliability of the channel and is called the noise. The vector $y$ is the noisy received vector. The decoding task is about recovering $x$ given $y$.

To better face with physical layer, continuous channels were introduced. There, the model is generalized by considering equation (1.1), but now with $x, y, v$ $n$-dimensional
vectors over the complex field $\mathbb{C}$, and the noise vector $v$ has random variable entries, typically Gaussian random variables with zero mean and unit variance.

Now, we are just one step before introducing the so called space-time codes in the next section. We talk about quasi-static fading channel when the channel model is described by

$$y = h \cdot x + v,$$

(1.2)

with $h$ a one-dimensional random variable and $y, x, v$ are as in the continuous channel (1.1). The variable $h$ is due to the obstacles in the environment that prevents the transmitted signal to take a simple line path, and is called the fading.

### 1.2 Space-time codes

Wireless communication motivated a further generalization. As it is explained in [1], suppose that the transmitter is equipped with $M$ transmit antennas and the receiver has $N$ receive antennas. At time $t$, the $M$ antennas each send one signal. We moreover assume that each signal faces independent fadings. Each signal will be sensed by all the receive antennas. Let us also suppose that the transmission is repeated $T$ times. Between each repetition, the channel is assumed to be constant. The model takes the form

$$Y_{N\times T} = H_{N\times M} X_{M\times T} + V_{N\times T},$$

where all matrices have coefficients in $\mathbb{C}$, and their dimensions are written in subscripts. The matrices $H$ and $V$ are random complex matrices and respectively model the fading and noise of the communication channel. The matrix $X$ is the sent codeword and the matrix $Y$ is the received message.

The data is encoded during time (we consider a time interval of $T$ slots) and space (since we have several antennas). This is why we talk about space-time codes. More precise definitions will be given hereafter.

Since rectangular matrices can be obtained from square ones by removing the appropriate number of rows or columns, we can suppose that $T = M = n$, obtaining

$$Y_{n\times n} = H_{n\times n} X_{n\times n} + V_{n\times n},$$

(1.3)

where the dimensions are still indicated.

In this context, a code $\mathcal{C}$ is a subset of $M_n(\mathbb{C})$, where $M_n(\mathbb{C})$ denotes $n \times n$ matrices with coefficients in $\mathbb{C}$. A codeword is a matrix in this set. We also sometimes call $\mathcal{C}$ the codebook.

Consider a received codeword $Y$. Decoding corresponds to choosing the codeword $X$ that minimizes

$$\min_{X \in \mathcal{C}} ||Y - HX||_F^2,$$

where $||\cdot||_F$ refers to the Frobenius norm defined for all $A \in M_n(\mathbb{C})$ by $||A||_F = (\text{Tr}(AA^*))^{1/2}$, with $A^*$ standing for the conjugate transpose of $A$.

In the sequel, by error probability we mean the probability that the receiver has
decoded a wrong codeword. An estimate of this error probability can be obtained using the union bound

\[ \Pr(e) \leq \frac{1}{|\mathcal{C}|} \sum_{X \in \mathcal{C}} \sum_{X \neq X} \Pr(X \to \hat{X}), \]

where \( \Pr(X \to \hat{X}) \) is the pairwise error probability, i.e., the probability that, when a codeword \( X \) is sent, the receiver decides erroneously in favor of another codeword \( \hat{X} \). Let us suppose that in the channel model (1.3), the coefficients of \( H \) and \( V \) are complex circular symmetric Gaussian random variables, with zero mean and unit variance. The reader can refer to [2, p. 8] which states in this case that

\[ \Pr(X \to \hat{X}) \leq \det \left( I_n + \frac{(X - \hat{X})(X - \hat{X})^*}{4} \right)^{-n} \tag{1.4} \]

Let \( r \) denote the rank of the codeword difference matrix

\[ A(X, \hat{X}) := (X - \hat{X})(X - \hat{X})^*. \]

If we denote by \( \lambda_j, j = 1, \ldots, r \) the nonzero eigenvalues of the codeword distance matrix, we can rewrite (1.4) as

\[ \Pr(X \to \hat{X}) \leq \prod_{j=1}^{r} \left( 1 + \frac{\lambda_j}{4} \right)^{-n}. \tag{1.5} \]

Obtaining the bound (1.5) as small as possible is a natural requirement. That is why we ask for \( r = n \). In other words, we want to find a family \( \mathcal{C} \) of matrices in \( M_n(\mathbb{C}) \) such that

\[ \det(X' - X'') \neq 0, \text{ for all } X' \neq X'' \in \mathcal{C}. \tag{1.6} \]

Relation (1.6) is referred to as the full-diversity property. The difficult task in designing codes with this property is that nothing much can be said about the determinant of the difference of two matrices. In particular, building large full-diversity codes is a hard goal to achieve. This motivates codes to be additive subgroups of \( M_n(\mathbb{C}) \). Indeed, relation (1.6) simplifies to

\[ \det(X) \neq 0, \text{ for all } X \in \mathcal{C}, X \neq 0, \tag{1.7} \]

which is a much more tractable constraint than (1.6).

So, from now on, we make the following assumption.

**Assumption 1.1.** Codes are equipped with an additive group structure.

Let us suppose that we work with codes having full-diversity property. Equation (1.5) makes sense to defining the coding gain of the code, namely

\[ \inf \{ \det((X - \hat{X})(X - \hat{X})^*) \}, \]

where the infimum is taken over all pairs of distinct codewords \( X, \hat{X} \in \mathcal{C} \).
Recall that we work with codes that are actually additive subgroups of $M_n(O)$. Therefore regarding the bound (1.5), the expression

$$\det(\mathcal{C}) := \inf\{|\det(X)|, X \in \mathcal{C}, X \neq 0\}$$

has to be maximized. Relation (1.8) defines what we call the minimum determinant of the code $\mathcal{C}$. As we will soon see, we will need to have a notion of "normalized" minimum determinant. In the case where there exists a constant $\epsilon > 0$ such that

$$\det(\mathcal{C}) \geq \epsilon,$$

we talk about codes having non-vanishing determinant (NVD) property. Let us remark that a code with NVD property is fully-diverse.

To make possible for the receiver to recover uniquely the codeword sent, it is natural to ask for the matrix codes to form a discrete set. Rigorous definitions of these intuitive concepts will be given in the proceeding chapters. This motivates to work with codes that are additive subgroups of $M_n(O)$, but which also have a lattice structure. So, we make the following additional assumption.

**Assumption 1.2.** Codes are equipped with a lattice structure.

To satisfy Assumptions 1.1 and 1.2, we will focus throughout the thesis on codes described in the following definition.

**Definition 1.3.** A space-time lattice code, that we will just call lattice code, is defined by

$$\mathcal{C} := \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k \subseteq M_n(O),$$

where matrices $M_1, \ldots, M_k$ are linearly independent over $\mathbb{R}$, and $k$ is called the dimension of the lattice.

**Remark 1.4.** The direct sum in Definition 1.3 is to be understood as a standard direct sum of abelian groups.

**Remark 1.5.** For actual transmission, the transmitter will only have a finite choice of codewords, so in Definition 1.3, what we call a code is actually the mathematical structure where the finite codes are chosen. To distinguish the practical point of view from the theoretical one, we will simply talk about finite codes to denote finite subsets of the general form (1.9).

**Remark 1.6.** To make things clearer, when we talk about code we will only mean a subset of $M_n(O)$, by lattice code we refer to the general form (1.9), and by finite code we understand a finite subset of (1.9). Furthermore, as it is the overwhelming context in which we work in this thesis, we forget about the "space-time" mention.

### 1.3 Designing codes

**1.3.1 Rates of a code**

As suggested by Remark 1.5, for the moment we will forget about the lattice structure and focus on finite codes. Armed with the coding gain of a code, we are now able to
compare two codes. We now want to have tools to characterize a given code. The space $M_n(C)$ is a vector space of dimension
\[ \dim_\mathbb{R}(M_n(C)) = 2n^2 \]
over the reals. Therefore, for every code $C \subseteq M_n(C)$, we can consider the subspace $\langle C \rangle$ spanned by the matrices of $C$. It has a $\mathbb{R}$-basis consisting of $k$ matrices, $1 \leq k \leq 2n^2$, so that each matrix $X$ in $C$ can be uniquely written as
\[ X = \sum_{i=1}^{k} g_i M_i, \]
where $M_i$ are some basis matrices and $g_i$ are real numbers. Once the matrices $M_1, \ldots, M_k$ are given, a finite code $C$ is defined by the values that $g_i$, $i = 1, \ldots, k$ can take. We write
\[ g := (g_1, \ldots, g_k) \]
and let $g$ take its values in
\[ G \subseteq \mathbb{R}^k, \quad (1.10) \]
so that
\[ C = \left\{ \sum_{i=1}^{k} g_i M_i \mid g = (g_1, \ldots, g_k) \in G \right\}. \quad (1.11) \]
Setting $G$ corresponds to what is usually called a choice of constellation points. For example, we can use what is called a $M$-pulse amplitude modulation ($M$-PAM) by taking $G$ to be the Cartesian product
\[ \{-M + 1, \ldots, -1, 1, \ldots, M - 1\} \times \ldots \times \{-M + 1, \ldots, -1, 1, \ldots, M - 1\}. \quad (1.12) \]
k times
It consequently makes sense to speak of the dimension of $\langle C \rangle$, which yields the following definition of rate.

**Definition 1.7.** The *dimension rate* $R_1$ for the code $C$ is given by
\[ R_1 = \frac{\dim_\mathbb{R}(\langle C \rangle)}{n} = \frac{k}{n}. \]

We immediately see that, since $1 \leq k \leq 2n^2$, the maximum rate achievable is $2n$. In Chapter 3, we will construct codes having rate 1, and in Chapters 6 and 7, we will give explicit examples of codes achieving the maximum rate.

One should note that this is not the common definition of rate, which we give below. Recall that in practice a code has only a finite number of codewords.

**Definition 1.8.** The *symbol rate* $R_2$ for the finite code $C$ is
\[ R_2 = \frac{\log_2(|C|)}{n}. \]
1.3.2 Normalized minimum determinant of a lattice code

Let us now discuss the question of how to compare two codes, and the necessity of defining the “normalized” minimum determinant of a lattice code.

To avoid the obvious trick consisting of multiplying each matrix code by a constant which would make the probability $O$ smaller, we have to scale the codes before comparing them. That is why for each finite code $C \subseteq M_n(\mathbb{C})$ we fix the maximum power

$$\max\{||A||_F^2 : A \in C\},$$

where we recall that $||X||_F = (\text{Tr}(XX^*))^{1/2}$ is the Frobenius norm, to a fixed constant.

*Remark 1.9.* Note that this can also be done by fixing the overall power constraint

$$\frac{1}{|C|} \cdot \sum_{X \in C} ||X||_F^2 = n^2,$$

(1.13)

Then, the problem is treated in another manner and we will not do it here.

The minimum determinant is a widely used concept to predict the performance of a finite code. If we want to compare two finite codes $C_1, C_2 \subseteq M_n(\mathbb{C})$ it is natural to expect that

1. $|C_1| = |C_2|$ and
2. $\max\{||A||_F^2 : A \in C_1\} = \max\{||B||_F^2 : B \in C_2\}$.

So we simply expect that both codebooks have equal number of elements and that the codes are scaled (multiplied by a real constant) so that the maximum power used is equal. In such case it is meaningful to compare the size of the absolute values of determinants of differences of codewords. Roughly speaking, looking again at (1.4), the code having larger minimum determinant probably performs better.

In the case of *infinite* lattice codes i.e. in the case described in Definition 1.3, the situation is not as simple. Indeed, with infinite lattice codes after energy normalization, the minimum determinant will decrease. Let us now give a short introduction to the concept before giving formal definitions in the next chapters. As we remember, a lattice code $C \subseteq M_n(\mathbb{C})$ has the form

$$\mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k,$$

where $M_1, \ldots, M_k$ are linearly independent over $\mathbb{R}$, and $k$ is called the dimension of the lattice. However, in practice, we would like to have the lattice itself but also a method to choose a given number of codewords (by making a choice for $\mathcal{G}$ in (1.10)). Let us suppose that we have a lattice code $L$ and a method to choose $R$ codewords, for any $R$. Let us suppose that we have a fixed power constraint, let say $\max\{||A||_F^2 | A \in C\} = 1$. Can we give a method that predicts whether the finite codes with $R$ elements, chosen from a lattice $L_1$ or a lattice $L_2$, have a larger minimum determinant just by considering the underlying lattices $L_1$ and $L_2$? It would be difficult. However, if we make the
agreement that the codewords are chosen by the same “method”, we might achieve something measurable.

One of the most energy efficient ways to choose codewords from a given lattice is to use spherical shaping, i.e. given a lattice code $L$, set a finite code to be

$$\{X \in L : ||X||_F \leq c\},$$

where $c \in \mathbb{R}$ is a fixed constant. Here, we simply choose the needed number of lowest energy codewords from the lattice and then scale the finite code to meet the power constraint. For large code sizes, this approach will roughly give us lattice points inside a sphere of dimension $k$, where $k$ is the dimension of the lattice.

Let us now consider subsets of the form

$$S(r)_L = \{A \in L : ||A||_F \leq r\}.$$

It is a result in lattice theory that

$$|S(r)_L| = M r^k + O(r^{k-1}), \quad (1.14)$$

where $M$ is a fixed constant and $O$ is the usual big $O$ symbol used in asymptotics. The reader can find the proof from [3, Theorem 1.7]. Roughly speaking, this equation tells us that if we are given a power limit $r$, the maximum number of points we can get from a given lattice depends only on the dimension $k$ and the constant $M$ (that at this point might depend on the chosen lattice).

Let us now introduce a notion that will be explained in details in Chapter 2. We have a geometric measure of any lattice, given by the volume of its fundamental parallelotope. For the moment, the fundamental parallelotope can be seen as one of the smallest pieces of the lattice that covers the whole space by translation.

Any lattice code can be scaled (i.e. multiplied by a real constant $r$) to have fundamental parallelotope of volume 1. Lattice theoretic results tell us that if we consider lattices having fundamental parallelotope of volume 1, the constant $M$ in equation (1.14) is the same for all lattices having the same dimension. In particular, if we consider lattice codes $L_1$ and $L_2$ that are normalized to have fundamental paralleloptopes of volume 1, we have that $S(r)_{L_1}$ and $S(r)_{L_2}$ have roughly the same number of elements. For both finite codes $S(r)_{L_1}$ and $S(r)_{L_2}$, the codeword with the greatest power has its power value close to $r$. Now we can see that we are able to compare the minimum determinants of the codes $S(r)_{L_1}$ and $S(r)_{L_2}$ without any scaling. Since the comparison is only possible when the underlying lattice have volume 1 fundamental parallelotope, this justifies the need of a ”normalized” minimum determinant.

Having normalized the lattice code to have a fundamental parallelotope of volume 1, the normalized minimum determinant is then defined to be the minimum determinant of the scaled lattice code. One should note that the notion of normalized minimum determinant only measures the ”potential” that the lattice code $L$ has. It predicts which lattice is likely to produce the finite codes with the biggest minimum determinants, if we are using spherical shaping. However, if we are using some other method than spherical shaping to choose codewords, the normalized minimum determinant might not predict well the minimum determinants of the finite codes chosen.
from the lattice. For example, if we are using a general M-PAM constellation, the value of the normalized minimum determinant might play a minor role when comparing lattice codes.

However, if we are comparing lattice codes where the underlying lattices have the same geometric structure, the normalized minimum determinant will work well. We give below an example of non-spherical shaped lattice codes having the same geometric property, that is being orthonormal.

Example 1.10. Let us suppose that we have two orthonormal lattice codes $L_1$ and $L_2$ having bases $A_1, \ldots, A_k$ and $B_1, \ldots, B_k$. Again, proper definitions will be given afterwards. For lattices to be orthonormal we mean that $||A_i|| = ||B_j|| = 1$, for all $1 \leq i, j \leq n$, and the $A_i$’s (respectively the $B_j$’s) are orthogonal to each other, with respect to the underlying real Frobenius inner product in $M_n(\mathbb{C})$ (see Proposition 2.18). Let us now consider finite codes

$$L_1(M) = \left\{ \sum_{i=1}^{k} g_i A_i \mid \mathbf{g} = (g_1, \ldots, g_k) \in \mathcal{G} \right\}$$

and

$$L_2(M) = \left\{ \sum_{i=1}^{k} g_i B_i \mid \mathbf{g} = (g_1, \ldots, g_k) \in \mathcal{G} \right\},$$

where $\mathcal{G} \subseteq \mathbb{R}^k$ is the Cartesian product of $k$ M-PAM constellations. If both of the lattices $L_1$ and $L_2$ are normalized to have fundamental parallelotopes of volume 1, we have that $||A_i||_F = ||B_j||_F = 1$, for all $1 \leq i, j \leq k$. This results that in both sets $L_1(M)$ and $L_2(M)$, the elements with the greatest power (greatest Frobenius norm) have equal value. Therefore the scaling to meet the given power constraint for $L_1(M)$ and $L_2(M)$ is the same. In this case, results of Chapter 2 will tell us that if $\delta(L_1) \geq \delta(L_2)$ we have that $\det_{\text{min}}(L_1(M)) \geq \det_{\text{min}}(L_2(M))$.

1.4 Thesis context and problem to study

Now that we have everything in hands, we can summarize the problem to study in this thesis.

Problem 1.11. Find the maximum $k$ such that

$$\mathcal{C} := \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k \subseteq M_n(\mathbb{C}),$$

with $\mathbb{R}$-linearly independent matrices $M_1, \ldots, M_k$, has NVD-property; and give explicit constructions.

Remark 1.12. Structures satisfying Problem 1.11 are actually very nice to work with. For example, adding matrices of $\mathcal{C}$ still gives an invertible matrix.

The plan of this thesis is as follows: as suggested, we will first introduce all the necessary material on lattices, then the remaining of the work will be devoted to code constructions satisfying Problem 1.11. The reader will surely find out that the lattice part is really interesting on its own. It can be independently read of the rest and does not deal with any kind of coding theoretic aspect. Code constructions will give
explicit solutions to Problem 1.11, and will be derived successively from number fields (Chapter 3), cyclic division algebras (Chapter 6), and crossed products (Chapter 7). The number field chapter can be seen as a training example to the cyclic division algebra code construction that achieve the maximal rate. Before working with division algebras, we will make two chapters (Chapters 4 and 5) on the theory of central simple algebras to set up the material as well as to introduce the needed notions. At the end, we will extend the cyclic division algebra case to more general codes built from crossed product algebras.

The purpose of this master thesis is also to clarify commonly used design criteria and to give a geometric treatment by means of lattices for codes from crossed products. This approach gives some extra insight to space-time coding theory in general.

We present below a dependency graph of the chapters in this master thesis.
Lattices

As explained in the previous introductory chapter, we give here an introduction to the lattice theory and set the ground for the coding theoretic chapters. This chapter can be read independently of the rest of the thesis.

2.1 Basic definitions and results

In all this section, we work with an $m$-dimensional $\mathbb{R}$-vector space $V$.

**Definition 2.1 (Lattice).** A $\mathbb{Z}$-lattice, or simply a lattice in $V$ is a subgroup of the form

$$L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k \subseteq V,$$

with $\mathbb{R}$-linearly independent vectors $v_1, \ldots, v_k$ of $V$.

**Remark 2.2.** As already pointed out in Chapter 1, the direct sum in Definition 2.1 is to be understood as a direct sum of abelian groups i.e. $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_k = L$ and for each $1 \leq i \leq k - 1$, $\mathbb{Z}v_{i+1} \cap (\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_i) = \{0\}$. Said differently, every element $x$ of $L$ has a unique representation as a linear expression

$$x = \sum_{i=1}^{k} a_i v_i,$$

with $a_i \in \mathbb{Z}$.

**Remark 2.3.** Note that a lattice is a finitely generated abelian subgroup of $V$. However, not every finitely generated subgroup of $V$ is a lattice. For example $\mathbb{Z}(1, 0) + \mathbb{Z}(\sqrt{2}, 0) \subseteq \mathbb{R}^2$ is clearly not.

As for now, let $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k \subseteq V$ be a lattice.

Let us introduce the *fundamental parallelootope* which is a central concept in lattice theory.

**Definition 2.4 (Fundamental parallelootope).** The $k$-tuple $(v_1, \ldots, v_k)$ is called a basis and the set

$$\mathcal{F}_L = \{x_1 v_1 + \cdots + x_k v_k : x_i \in \mathbb{R}, 0 \leq x_i < 1\},$$

a fundamental parallelootope of $L$. The lattice $L$ is called full if $k = m$. 
Let us intuitively explain what it means for a lattice to be full. It means that the fundamental parallelotope sort of "generates" the whole space $V$ by covering it by all the translates $F_L + x, x \in L$.

Note that for the case of non-full lattices, one can move from a $k$-dimensional lattice in $\mathbb{R}^m$ to a $k$-dimensional lattice in $\mathbb{R}^k$. Indeed, one can just take a matrix $A \in M_{k \times m}(\mathbb{C})$ such that $AL$ becomes a full lattice in $\mathbb{R}^k$.

Our next objective is to introduce notions of volume and distance in $V$.

**Definition 2.5 (Gram matrix).** Let $a_1, \ldots, a_k$ be vectors in $\mathbb{R}^m$. Their Gram matrix is defined by the $k \times k$ symmetric positive definite matrix $G(a_1, \ldots, a_k) = (a_i \cdot a_j)_{1 \leq i, j \leq k}$, where $\cdot$ is the natural inner product in $\mathbb{R}^m$.

Note that $G(a_1, \ldots, a_k) = AA^T$, where $A \in M_{k \times m}(\mathbb{R})$ is formed by the $a_i$'s as row vectors.

**Definition 2.6 (Fundamental volume).** Denote by $\eta : V \rightarrow \mathbb{R}^m$ a chosen $\mathbb{R}$-vector space isomorphism. It induces a natural inner product to the space $V$ defined as follows

$$\langle \cdot, \cdot \rangle_V : V \times V \rightarrow \mathbb{R}$$

$$(x, y) \mapsto \langle \eta(x), \eta(y) \rangle.$$

So, as for now, $V$ is a Euclidean space. On the other hand,

$$\eta(L) = \mathbb{Z}\eta(v_1) \oplus \cdots \oplus \mathbb{Z}\eta(v_k) \subseteq \mathbb{R}^m$$

becomes a $\mathbb{Z}$-lattice in $\mathbb{R}^m$.

The *volume of the fundamental parallelotope of $L$*, denoted by $\text{vol}(L)$ is then defined by

$$\text{vol}(L) := \text{vol}(\eta(L)) = \sqrt{\det(G(\eta(v_1), \ldots, \eta(v_k)))}.$$  \hspace{1cm} (2.1)

One can notice that here the Gram matrix satisfies

$$G(\eta(v_1), \ldots, \eta(v_k)) = MM^T,$$  \hspace{1cm} (2.2)

where $M \in M_{k \times m}(\mathbb{R})$ is formed by using the $\eta(v_i)$'s as row vectors.

From the previous definition, it seems that the volume depends on the chosen isomorphism $\eta$. However, the volume is the same inside a certain class of isomorphisms as the next proposition explains.

**Proposition 2.7.** Let $\eta, \mu : V \rightarrow \mathbb{R}^m$ be two chosen $\mathbb{R}$-vector space isomorphisms that are *inner-product preserving* i.e. satisfying

$$\langle \eta(x), \eta(y) \rangle = \langle \mu(x), \mu(y) \rangle = \langle x, y \rangle_V.$$

Then

$$\text{vol}(\eta(L)) = \text{vol}(\mu(L)) = \text{vol}(L).$$

**Proof.** This follows directly from the definitions. \qed
Remark 2.8. We often abuse the language by talking about the volume of a lattice \( L \) instead of the volume of its fundamental parallelotope \( F_L \).

As a subset of \( \mathbb{R}^m \), at least whenever \( L \) is a full lattice, we would expect the Lebesgue measure of \( \eta(F_L) \) to coincide with the volume of the fundamental parallelotope of \( L \). As a matter of fact, we have the following proposition.

**Proposition 2.9 (Link with the Lebesgue measure).** If \( L \) is a full lattice, then we have

\[
\int_{\eta(F_L)} dx = \sqrt{\det(G(\eta(v_1), \ldots, \eta(v_m)))}.
\]

**Proof.** Let us suppose that \( L \) is a full lattice. We denote by \((e_i)_{1 \leq i \leq m}\) the canonical \( \mathbb{R} \)-basis of \( \mathbb{R}^m \). Let

\[
g : \mathbb{R}^m \rightarrow \mathbb{R}^m \\
e_i \mapsto \eta(v_i), \quad 1 \leq i \leq m,
\]

which can also be written as

\[
g : \mathbb{R}^m \rightarrow \mathbb{R}^m \\
x \mapsto Mx,
\]

with \( M \) defined as in (2.2). In the case where \( L \) is a full lattice, as \( g \) is a bijective map (sending a basis to a basis), by a change of variables we get

\[
\int_{\eta(F_L)} dx = \int_{\eta([0,1]^m)} dx = \int_{[0,1]^m} |\det(J_g(x))| dx = \det(M),
\]

where \( J_g \) denotes the Jacobian matrix of the \( m \)-variable function \( g \). Then, relation (2.2) gives the result. \( \square \)

For non-full lattices, we also would like to use measure theoretic tools. Therefore, we are now left with discussing the relation between Lebesgue and lattice measures when we consider a non-full lattice \( L \) of dimension \( k < m \). Let

\[L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k \subseteq V,\]

where \( V \) is an \( m \)-dimensional \( \mathbb{R} \)-vector space. In this case

\[
\int_{\eta(F_L)} dx = 0.
\]

However we would like to recover the definition of the volume involving the Gram matrix, namely (2.1), which is obviously not zero. One way to overcome this obstacle is to choose an inner-product preserving isomorphism

\[
\beta : \mathbb{R}(L) = \mathbb{R}v_1 \oplus \cdots \oplus \mathbb{R}v_k \sim \mathbb{R}^k
\]

satisfying

\[(\eta(x), \eta(y)) = (\beta(x), \beta(y)),\]

for all \( x, y \in \mathbb{R}(L) \). Then we can make the following assumption.
Assumption 2.10. In the case of a non-full lattice $L$, we will integrate the fundamental parallelootope in $\beta(L)$, i.e. the subspace generated by the basis elements of the lattice $\beta(L)$.

With Assumption 2.10 we recover the definition of the volume involving the Gram matrix also for the non-full case. Finally, we have a complete characterization of the volume of the fundamental parallelootope of a lattice by the Lebesgue measure of the underlying subset.

Remark 2.11. As two bases of a full lattice in $\mathbb{R}^m$ are related to one another by some matrix in $GL_m(\mathbb{Z})$, the volume does not depend on the chosen basis (but the Gram matrix does). This result is also true for non-full lattices.

Now that we have a notion of volume in every lattice, we want to compare distances in this structure.

Definition 2.12. The shortest vector of a $k$-dimensional lattice $L$ is denoted by $sv(L)$, and is the smallest radius of a zero-centered ball containing one vector of $L$. The normalized shortest vector is then defined by

$$\frac{sv(L)}{\text{vol}(L)^{1/k}}$$

and is denoted by $Nsv(L)$. We also define the longest possible shortest vector by

$$Nsv(k) = \sup_{L}(Nsv(L)),$$

where the supremum is taken over all $k$-dimensional lattices $L$.

We conclude this section by giving a typical property of every lattice. As already pointed out, not every finitely generated subgroup of $V$ is a lattice, but every discrete subgroup of $V$ is, as we will see. Moreover, it turns out to be a necessary and sufficient condition.

Definition 2.13. We say that a subgroup $S$ of $V$ is discrete whenever for each $\gamma \in S$, there exists a neighborhood (in the topological sense) which contains no other points than $\gamma$.

Remark 2.14. Each lattice $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k$ has the special property of being a discrete subgroup of $V$. Indeed, for every point

$$\gamma = a_1v_1 + \ldots + a_kv_k \in L,$$

extending $v_1, \ldots, v_k$ to a basis $v_1, \ldots, v_m$ of $V$, the set

$$\{x_1v_1 + \ldots + x_mv_m : x_i \in \mathbb{R}, |a_i - x_i| < 1 \text{ for } i = 1, \ldots, k\}$$

clearly is such a neighborhood. The following proposition also takes the converse into account.

Proposition 2.15. A subgroup $L \subseteq V$ is a lattice if and only if it is discrete.

Proof. See [4, pp. 24-25].
2.2 Lattices in $M_n(\mathbb{C})$

Now we concentrate our attention to the case where $V = M_n(\mathbb{C})$ in Definition 2.4, i.e., lattices $L$ that are subgroups of the $2n^2$-dimensional $\mathbb{R}$-vector space $M_n(\mathbb{C})$.

We can flatten each $X \in M_n(\mathbb{C})$ to obtain a $2n^2$-dimensional real vector $X$ by first forming a vector of length $n^2$ out of the entries (say row by row) and then replacing each complex entry with the pair formed by its real and imaginary parts. This defines an isomorphism

$$\alpha : M_n(\mathbb{C}) \longrightarrow \mathbb{R}^{2n^2}$$

that plays the role of the isomorphism $\eta$ in Definition 2.6, where $V = M_n(\mathbb{C})$. As the general case applies, we know that $\alpha$ induces an inner product in the space $M_n(\mathbb{C})$, by setting

$$\langle X, Y \rangle := \langle \alpha(X), \alpha(Y) \rangle,$$

for all $X, Y \in M_n(\mathbb{C})$. Unless stated otherwise, this is the inner product in $M_n(\mathbb{C})$ that we will use by convention.

Remark 2.16. In particular, we get that if $L := \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k$ is a discrete subgroup of $V$, then $v_1, \ldots, v_k$ are linearly independent over $\mathbb{R}$. Indeed, by the previous proposition, we get that $L$ is a lattice. So there exist $v'_1, \ldots, v'_p$ $\mathbb{R}$-linearly independent vectors of $V$ such that $L := \mathbb{Z}v'_1 \oplus \cdots \oplus \mathbb{Z}v'_p$. Then, by the structure theorem on finitely generated abelian groups, we get that $p = k$, as it is uniquely determined. Thus,

$$\mathbb{R}(L) = \mathbb{R}v_1 \oplus \cdots \oplus \mathbb{R}v_k = \mathbb{R}v'_1 \oplus \cdots \oplus \mathbb{R}v'_k$$

is a vector space of dimension $k$. From which it follows that $v_1, \ldots, v_k$ are $\mathbb{R}$-linearly independent. As a result, $L$ cannot be generated by less than $k$ basis elements.

Remark 2.17. It has to be well understood that $M_n(\mathbb{C})$ is now equipped with the inner product $\alpha$ and as a consequence for every lattice $L \subseteq M_n(\mathbb{C})$, we have $\text{vol}(L) = \text{vol}((\alpha(L))$. However, in the case of a non-full lattice $L$ of dimension $k < n$, most of the time we will move from $L$ being a non-full lattice in $\mathbb{R}^n$ to $\beta(L)$ which is a full lattice in $\mathbb{R}^k$. We recall that the isomorphism $\beta$ used is the one described in Assumption 2.10. Nevertheless, by doing so, we assume that we have beforehand verify that

$$\langle \beta(x), \beta(y) \rangle = \langle \alpha(x), \alpha(y) \rangle,$$

for every $x, y \in L$. Then it will follow that $\text{vol}(L) = \text{vol}(\alpha(L)) = \text{vol}(\beta(L))$.

Let us now give a characterization of this particular inner product.

Proposition 2.18. Let $X, Y \in M_n(\mathbb{C})$, we have

$$\langle \alpha(X), \alpha(Y) \rangle = \Re(\text{Tr}(XY^*)),$$

where $X^*$ stands for the conjugate transpose of $X$. 
Proof. Recall that

\[
\alpha(X) := (\Re(X_{11}), \Im(X_{11}), \ldots, \Re(X_{1n}), \Im(X_{1n}),
\ldots, \\
\Re(X_{n,1}), \Im(X_{n,1}), \ldots, \Re(X_{nn}), \Im(X_{nn})).
\]

Then, it follows that

\[
\langle \alpha(X), \alpha(Y) \rangle = \sum_{s=1}^{2n^2} \alpha(X)_s \alpha(Y)_s
\]

\[
= \sum_{s=1}^{2n^2} \Re\left( X_{\lfloor s/2 \rfloor} \{ \frac{s}{2} \} \right) \Re\left( Y_{\lfloor s/2 \rfloor} \{ \frac{s}{2} \} \right)
\]

\[
+ \sum_{s=1}^{2n^2} \Im\left( X_{\lfloor s/2 \rfloor} \{ \frac{s}{2} \} \right) \Im\left( Y_{\lfloor s/2 \rfloor} \{ \frac{s}{2} \} \right)
\]

\[
= \sum_{l,t=1}^{n} \Re(\alpha(X_{l,t})\alpha(Y_{l,t})) + \Im(\alpha(X_{l,t})\alpha(Y_{l,t}))
\]

\[
= \Re(\text{Tr}(XY^*))
\]

The next corollary puts the stress on the fact that \(\alpha\) can be really thought of as an isometry.

**Corollary 2.19.** Let \(X \in M_n(\mathbb{C})\). Then the following equality holds

\[
||X||_F = ||\alpha(X)||_E,
\]

where \(||\cdot||_E\) denotes the Euclidean norm of a vector, and where we recall that \(||X||_F = (\text{Tr}(XX^*))^{1/2}\) is the Frobenius norm.

**Proof.** This follows directly from Proposition 2.18.

**Remark 2.20.** Unless stated otherwise, the Frobenius norm is the norm we will use by convention in \(M_n(\mathbb{C})\).

The following corollary will be useful for our calculations in the coding theoretic part of the thesis.

**Corollary 2.21.** Let \(X_1, \ldots, X_k \in M_n(\mathbb{C})\). Then, we have

\[
G(X_1, \ldots, X_k) := G(\alpha(X_1), \ldots, \alpha(X_k)) = (\Re(\text{Tr}(X_iX_j^*))_{1 \leq i, j \leq k}.
\]

**Proof.** This also directly follows from Proposition 2.18.
Remark 2.22. For a lattice \( L = \mathbb{Z}X_1 \oplus \ldots \oplus \mathbb{Z}X_k \subseteq M_n(\mathbb{C}) \), we denote by \( L^T \) the following lattice
\[
L = \mathbb{Z}X_1^T \oplus \cdots \oplus \mathbb{Z}X_k^T.
\]
Then, we can easily verify from Corollary 2.21, that \( \text{vol}(L) = \text{vol}(L^T) \).

The following result will later on play an important role.

**Lemma 2.23.** Let \( L_1 \) and \( L_2 \) be two lattices in \( M_n(\mathbb{C}) \) such that each vector in \( L_1 \) is orthogonal, with respect to the scalar product in \( M_n(\mathbb{C}) \) introduced above, to each vector in \( L_2 \). Then
\[
\text{vol}(L_1 \oplus L_2) = \text{vol}(L_1) \cdot \text{vol}(L_2).
\]

**Proof.** It suffices to note that
\[
G(L_1 \oplus L_2) = \begin{pmatrix} G(L_1) & 0 \\ 0 & G(L_2) \end{pmatrix},
\]
and then taking the square root of the determinant, we get the result. \( \square \)

Let us now give a proper definition for the minimum determinant that we discussed earlier in Chapter 1.

**Definition 2.24.** The **minimum determinant** of a \( k \)-dimensional lattice \( L \) in \( M_n(\mathbb{C}) \) is defined by
\[
\det(L) := \inf_{X \in L, X \neq 0} \{|\det(X)|\}.
\]
Moreover, we shall denote by \( \delta(L) \) the **normalized minimum determinant** of the lattice \( L \), i.e. here we first scale \( L \) to have a unit size fundamental parallelootope and then we take the minimum determinant of the resulting scaled lattice.

The following lemma gives us a way to effectively compute the normalized minimum determinant.

**Lemma 2.25.** Let us suppose that we have a \( k \)-dimensional lattice \( L \) in \( M_n(\mathbb{C}) \). We then have that
\[
\delta(L) = \frac{\det(L)}{\text{vol}(L)^n/k}.
\]

**Proof.** First write \( L \) as
\[
L = \mathbb{Z}X_1 \oplus \cdots \oplus \mathbb{Z}X_k.
\]
Let us then remark that for all \( \lambda \in \mathbb{C}, G(\lambda L) = |\lambda|^2 G(L) \). Indeed, for all \( i, j = 1, \ldots, k \) we have
\[
G(\lambda L)_{i,j} = \Re(\text{Tr}(\lambda X_i)(\lambda X_j)^*) = \Re(\text{Tr}(|\lambda|^2 X_i X_j^*)) = |\lambda|^2 \Re(\text{Tr}(X_i X_j^*)) = |\lambda|^2 G(L)_{i,j}.
\]
Now, set \( s := \frac{1}{\text{vol}(L)^{1/n}} \). Let us verify that \( \text{vol}(sL) = 1 \), so that \( sL \) will be the scaled version of the lattice \( L \). We have
\[
\text{vol}(sL) = \sqrt{\det(G(sL))} = \sqrt{\det \left( G \left( \frac{1}{\text{vol}(L)^{1/k}} L \right) \right)} = \sqrt{\det \left( \frac{1}{\text{vol}(L)^{2/k}} G(L) \right)}
\]
\[
= \sqrt{\frac{1}{\text{vol}(L)^2} \det(G(L))} = \frac{1}{\text{vol}(L)} \sqrt{\det(G(L))} = 1.
\]

So, \( \delta(L) = \text{det}_\min(sL) = \inf \{|\det(sX)| : X \in L, X \neq 0\} = s^n \text{det}_\min(L) \), i.e.
\[
\delta(L) = \frac{\text{det}(L)}{\text{vol}(L)^{n/k}}.
\]

\[\square\]

**Remark 2.26.** As the fundamental parallelootope of a lattice does not depend on the chosen basis of \( L \), we immediately get that the normalized minimum determinant depends only on the lattice itself and not on the chosen basis.

Our next step is to establish a relationship between the minimum determinant of a lattice in \( \mathbb{M}_n(\mathbb{C}) \) and its shortest vector. We begin with the Hadamard inequality.

**Lemma 2.27 (Hadamard inequality).** Let \( A = (a_{ij}) \in \mathbb{M}_n(\mathbb{C}) \), and denote by \( A_j \), \( j = 1, \ldots, n \) the columns of \( A \). Then,
\[
|\det(A)| \leq \prod_{j=1}^n \|A_j\|_E = \prod_{j=1}^n \left( \sum_{i=1}^n |a_{ij}|^2 \right)^{1/2},
\]
with equality if and only if both sides are zero or \( \sum_{i=1}^n a_{ij} \overline{a_{ik}} = 0 \) for \( j \neq k \).

**Proof.** [Sketch of the proof] If \( \det(A) = 0 \), we immediately get the result. For the case where \( A \) is an invertible matrix, the idea is to orthogonalize the columns of \( A \), using the standard Gram-Schmidt process. For details, see [5, pp. 233-234]. \( \square \)

The previous lemma states that the volume of a parallelepiped with given side lengths has maximal volume when the sides are orthogonal. Then, we need the following

**Lemma 2.28.** Let \( A \in \mathbb{M}_n(\mathbb{C}) \). Then,
\[
|\det(A)| \leq \frac{\|A\|_F^2}{n^{n/2}}.
\]

**Proof.** Let \( A_j, j = 1, \ldots, n \) be the rows of \( A \). By the Hadamard inequality, \( |\det(A)| \leq \prod_{j=1}^n \|A_j\|_E \). Squaring this inequality and using the fact that \( \|A\|_F^2 = \sum_{j=1}^n \|A_j\|_E^2 \) together with the well-known inequality between the geometric and arithmetic means of \( n \) positive numbers give the bound. Indeed, in short we have
\[
\|A\|_F^2 = \left( \sum_{j=1}^n \|A_j\|_E^2 \right)^{n/2} \geq \left( n \left( \prod_{j=1}^n \|A_j\|_E^2 \right)^{1/n} \right)^{n/2} \geq n^{n/2} |\det(A)|.
\]

\[\square\]
Proposition 2.29 (Relation between minimum determinant and shortest vector). Let $L$ be a $k$-dimensional lattice in $M_n(\mathbb{C})$. We then have that

$$\det_{\text{min}}(L) \leq \frac{\text{sv}(L)^n}{n^{n/2}},$$

or equivalently

$$\delta(L) \leq \frac{\text{Nsv}(L)^n}{n^{n/2}}.$$

From which we deduce

$$\delta(L) \leq \frac{\text{Nsv}(k)^n}{n^{n/2}}.$$

Proof. This follows directly from Lemma 2.28. \hfill \square

Example 2.30. Let us suppose that we have a 4-dimensional lattice

$$L = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \mathbb{Z}v_3 \oplus \mathbb{Z}v_4 \subseteq M_2(\mathbb{C}).$$

It is a known result in lattice theory that\(^1\) $\text{Nsv}(4) = 2^{1/4}$. The reader can find this result in [6, p. 20]. Then,

$$\delta(L) \leq \frac{1}{\sqrt{2}}.$$

Proposition 2.31. The bound in Example 2.30 is tight. Indeed, the following lattice in $M_2(\mathbb{C})$

$$L := \mathbb{Z}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} i & i \\ -i & -i \end{pmatrix} \subseteq \left\{ \begin{pmatrix} a & -b \\ b & \pi \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

satisfies $\delta(L) = 1/\sqrt{2}$.

Proof. It is just a matter of computation to show that $\delta(L) = 1/\sqrt{2}$. \hfill \square

2.3 Fundamental parallelotopes of special lattices

In the subsequent chapters, given a lattice code

$$C := \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k \subseteq M_n(\mathbb{C})$$

we will be interested in evaluating the normalized minimum determinant of $AC$, where $A \in M_n(\mathbb{C})$. So, the first step is to know how the volume of the fundamental parallelotope of a lattice in $M_n(\mathbb{C})$ behaves with respect to matrix multiplication. This is

\(^1\) In the literature, this is often referred to as the known values of the Hermite constant, which is actually the square of the normalized shortest vector.
the goal of this section. At the end we will derive a result which presents two cases where the normalized minimum determinant of a lattice stays unchanged by matrix multiplication.

First, we begin with computing the determinant of a special-type matrices, following [7]. Every complex number $a + ib$ can be represented by the $2 \times 2$ real matrix

$$
\begin{pmatrix}
a - b \\
b & a
\end{pmatrix}.
$$

In fact, this induces a ring embedding $\varphi : \mathbb{C} \rightarrow M_2(\mathbb{R})$. It is important to note that, since complex multiplication is commutative, multiplication of matrices of the above form is also commutative.

Note that, for all $z \in \mathbb{C}$,

$$
\det(\varphi(z)) = |z|^2. \tag{2.4}
$$

Although the latter fact seems meaningless, it is a first step toward the general results hereafter. We will extend the above idea by considering the following ring embedding

$$
\phi : M_n(\mathbb{C}) \rightarrow M_{2n}(\mathbb{R})
$$

$$
A = (a_{ij}) \rightarrow \begin{pmatrix}
\varphi(a_{11}) & \cdots & \varphi(a_{1n}) \\
\vdots & \ddots & \vdots \\
\varphi(a_{n1}) & \cdots & \varphi(a_{nn})
\end{pmatrix}. \tag{2.5}
$$

The following lemma is a generalization of equality (2.4).

**Lemma 2.32.** Let $A \in M_n(\mathbb{C})$. Then

$$
\det(\phi(A)) = |\det(A)|^2.
$$

To prove this lemma, we will have to study how the determinant behaves with commuting-block matrices.

**Theorem 2.33 (Sylvester).** Given a field $F$ and a commutative subring $S$ of $M_n(F)$, let $M \in M_k(S)$, i.e. $M \in M_{nk}(F)$, then

$$
\det_F(M) = \det_S(\det M).
$$

**Remark 2.34.** Let us first explain what $\det_S(M)$ is. As $M$ is a matrix of elements of $S$ which are themselves matrices in $M_n(F)$, taking the determinant of $M$ over $S$ just means that we consider each single block matrix of $M$ as a single element. Then, $\det_S(M)$ is a matrix in $M_n(F)$. What Theorem 2.33 says is that if $M$ has a block structure and if each block commutes under matrix multiplication, then taking the determinant of the matrix $\det_S(M)$ is equivalent to computing the determinant of the initial matrix considered in $M_{nk}(F)$. 
Proof. [Proof of Lemma 2.32] We apply Theorem 2.33 with the field of real numbers $F = \mathbb{R}$ and the commutative subring of $M_2(\mathbb{R})$

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$ 

Now, we have

$$\det(\phi(A)) = \det(\phi(A)) = \det(\det(\phi(A))) = \det \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_i B_{\sigma(i), i},$$

using the usual determinant formula, where each $\sigma$ is a permutation of the numbers $1, \ldots, n$, and each $B_{ji}$ is a $2 \times 2$ matrix in $S$ representing a complex number. Now, we let

$$\Delta := \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_i B_{\sigma(i), i},$$

which must be a matrix representation of a complex number, say $z$. Recalling (2.4), taking the determinant of $\Delta$ is equivalent to taking the square of the norm of the associated complex number $\det_{\mathbb{R}}(\Delta) = |z|^2$. We can then associate to each $B_{ji}$ its complex number by going from a matrix of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

to the complex number $a + ib$. And since by Theorem 2.33 we must get the same complex number, we have

$$\det(\phi(A)) = \det(\Delta) = |z|^2 = \left| \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_i A_{\sigma(i), i} \right|^2 = |\det(A)|^2,$$

which is the desired result. 

Remark 2.35. The result of this section expresses the relation between the complex and the real Jacobians, respectively denoted by $J_C$ and $J_R$, of a complex analytic map $f : \mathbb{C}^n \rightarrow \mathbb{C}^n$. Indeed, if we have an $n$-dimensional complex analytic map $f$, where we label the domain coordinates as $z_i = x_i + iy_i$ and range coordinates as $w_j = u_j + iv_j$, then the complex Jacobian $J_C$ is the matrix of partial derivatives ($\frac{\partial w_j}{\partial z_i}$). Then, using the Cauchy-Riemann conditions gives the association $J_C \rightarrow J_R$ by replacing each complex entry in the complex Jacobian with its corresponding real $2 \times 2$ matrix representation.

Let us now go back to the purpose this section. We are ready to present some cases where $\delta(AL) = \delta(L)$, for specific lattices $L \in M_n(\mathbb{C})$ and elements $A \in M_n(\mathbb{C})$. But first, let us set the ground with the following three lemmas.

Lemma 2.36. Let $A \in M_n(\mathbb{C})$ and let $L$ be a $2n$-dimensional lattice in $\mathbb{C}^n$. Then, we get

$$\text{vol}(AL) = |\det(A)|^2 \text{vol}(L).$$
Proof. Write
\[ L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_{2n} \subseteq \mathbb{C}^n, \]
which can be seen as a $\mathbb{Z}$-lattice in $\mathbb{R}^{2n}$. To do that, we flatten each basis vector $v_i$ to obtain a $2n$-dimensional real vector by replacing each complex entry with the pair formed by its real and imaginary parts. This defines a mapping
\[ \beta : \mathbb{C}^n \rightarrow \mathbb{R}^{2n}, \]
which is inner-product preserving and $\mathbb{R}$-linear. Then, the volume of $L$ is
\[ \text{vol}(L) := \int_{\mathcal{F}_\beta(L)} dx. \]
Note that $\beta(L) \subseteq \mathbb{R}^{2n}$ is a $\mathbb{Z}$-lattice of dimension $2n$, so it has nonzero Lebesgue measure.

One can check that $\beta(AL) = \phi(A)\beta(L)$, so that $\mathcal{F}_\beta(AL) = \phi(A)\mathcal{F}_\beta(L)$, where $\phi$ is the mapping introduced in \((2.5)\).

Now consider the following diagram
\[
\begin{array}{ccc}
L & \xrightarrow{f} & AL \\
\downarrow{\beta} & & \downarrow{\beta} \\
\alpha(L) & \xrightarrow{g} & \beta(AL) = \phi(A)\beta(L)
\end{array}
\]
where
\[ f : \mathbb{C}^n \rightarrow \mathbb{C}^n \]
\[ v \mapsto \phi(A)v, \]
and
\[ g : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{2n} \]
\[ v \mapsto \phi(A)v. \]

Then using a change of variables we get
\[
\text{vol}(AL) = \int_{\mathcal{F}_{\beta(AL)}} dx = \int_{\phi(A)\mathcal{F}_{\beta(L)}} dx = \int_{g(\mathcal{F}_{\beta(L)})} dx = \int_{\mathcal{F}_{\beta(L)}} |\det J_g(x)|dx
\]
\[ = |\det(\phi(A))| \int_{\mathcal{F}_{\beta(L)}} dx = |\det(A)|^2 \text{vol}(L), \]
where in the last inequality we have used Lemma 2.32. □

Lemma 2.37. Let $D \in M_n(\mathbb{C})$ be a diagonal matrix. Let $L$ be a $2n$-dimensional diagonal lattice in $M_n(\mathbb{C})$. Then, we get
\[ \text{vol}(DL) = |\det(D)|^2 \text{vol}(L). \]
Proof. First, note that we can flatten any diagonal matrix in $M_n(\mathbb{C})$ to obtain an $n$-dimensional complex vector by selecting the element in the $i$th row as $i$th component. This defines a bijective mapping

$$\gamma : \{ A \in M_n(\mathbb{C}) : A \text{ is diagonal} \} \rightarrow \mathbb{C}^n,$$

which is inner product-preserving and R-linear. Write

$$L = \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_{2n} \subseteq M_n(\mathbb{C}),$$

whose volume is

$$\text{vol}(L) = \text{vol}(\gamma(L)).$$

Further, noting that $\gamma(\mathbb{D}L) = D\gamma(L)$, we get

$$\text{vol}(DL) = \text{vol}(\gamma(DL)) = \text{vol}(D\gamma(L)) = |\det(D)|^2 \text{vol}(\gamma(L)) = |\det(D)|^2 \text{vol}(L),$$

where we have used Lemma 2.36. \qed

Lemma 2.38. Let $U \in M_n(\mathbb{C})$ be a unitary matrix and let $L$ be a $2n$-dimensional lattice in $M_n(\mathbb{C})$. Then, we get

$$\text{vol}(UL) = \text{vol}(L).$$

Proof. Let us write

$$L = \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_{2n} \subseteq M_n(\mathbb{C}).$$

Using the original definition of the volume of the fundamental parallelotope of a lattice involving the Gram matrix, it suffices to prove that

$$G(\alpha(UM_1), \ldots, \alpha(UM_{2n})) = G(\alpha(M_1), \ldots, \alpha(M_{2n})).$$

Indeed, as $UU^* = I_n$, $U$ is inner-product preserving and we get

$$\langle \alpha(UM_1), \alpha(UM_j) \rangle_{\mathbb{C}^{2n}^2} = \langle UM_1, UM_j \rangle_{M_n(\mathbb{C})} = \langle M_1, M_j \rangle_{M_n(\mathbb{C})} = \langle \alpha(M_1), \alpha(M_j) \rangle_{\mathbb{C}^{2n}^2},$$

where we specified which scalar product has been used. \qed

The next two propositions describe two specific cases where we have invariance of the normalized minimum determinant.

Proposition 2.39. Let $A \in M_n(\mathbb{C})$ such that $A = DP$ with $D \in M_n(\mathbb{C})$ a diagonal matrix, and $P \in M_n(\mathbb{C})$ a permutation matrix. Let $L$ be a $2n$-dimensional diagonal lattice in $M_n(\mathbb{C})$. Then, we get

$$\text{vol}(AL) = |\det(A)|^2 \text{vol}(L).$$

Proof. Using Lemmas 2.37 and 2.38, since $P$ is in particular a unitary matrix, we can write

$$\text{vol}(AL) = \text{vol}(DPL) = \text{vol}(PXL) = \text{vol}(XL) = |\det(X)|^2 \text{vol}(L),$$

where $X = P^{-1}DP$ is a diagonal matrix in $M_n(\mathbb{C})$. Further noting that $\det(X) = \det(A)$ gives the result. \qed
**Remark 2.40.** Let us show that in the context of the previous proposition, we actually have $\text{vol}(AL) = \text{vol}(LA)$. Using Remark 2.22, we can write

$$\text{vol}(AL) = |\det(A)|^2 \text{vol}(L) \text{vol}(L) = |\det(A^T)|^2 \text{vol}(L^T) = \text{vol}(A^T L^T) = \text{vol}((LA)^T) = \text{vol}(LA).$$

**Proposition 2.41.** Let $A \in M_n(\mathbb{C})$, and let $L$ be a $2n^2$-dimensional lattice in $M_n(\mathbb{C})$. Then,

$$\text{vol}(AL) = |\det(A)|^{2n} \text{vol}(L).$$

**Proof.** If $A$ is a singular matrix, then the result is trivial. Assume that $A$ is an invertible matrix. We will again make use of the $\alpha$ mapping which flattens any complex matrix in $M_n(\mathbb{C})$ to a $2n^2$-dimensional real vector in $\mathbb{R}^{2n^2}$. Now, write

$$L = \mathbb{Z} M_1 \oplus \cdots \oplus \mathbb{Z} M_{2n^2} \subseteq M_n(\mathbb{C}),$$

whose fundamental volume is

$$\text{vol}(L) = \text{vol}(\alpha(L)).$$

Note that by applying $\alpha$ to the multiplied lattice, every basis columns gets mapped with $\phi(A^T)$, in the sense that we have

$$\alpha(AL) = \begin{pmatrix} \phi(A^T) \\ \vdots \\ \phi(A^T) \end{pmatrix} \alpha(L),$$

where we are using the mapping $\phi$ defined in (2.5). Moreover, we note that both $\alpha(AL)$ and $\alpha(L)$ are $2n^2$-dimensional lattices in $\mathbb{R}^{2n^2}$, so their Lebesgue measure is nonzero. Finally, by a change of variables and using Lemma 2.32, we get

$$\text{vol}(AL) = \text{vol}(\alpha(AL)) = \text{vol}(R \alpha(L)) = |\det(R)| \text{vol}(\alpha(L)) = |\det(\phi(A^T))|^{n} \text{vol}(L) = |\det(A^T)|^{2n} \text{vol}(L) = |\det(A)|^{2n} \text{vol}(L).$$

$$\square$$

**Remark 2.42.** As in Remark 2.40, one can easily prove that in the context of the previous proposition, $\text{vol}(AL) = \text{vol}(LA)$.

We now present the result on the invariance of the normalized minimum determinant that we discussed earlier.

**Theorem 2.43.** Let $A$ be an invertible matrix in $M_n(\mathbb{C})$.

1. If $L$ is a $2n^2$-dimensional lattice in $M_n(\mathbb{C})$, then $\delta(AL) = \delta(L)$.

2. If $A = DP \in M_n(\mathbb{C})$, with $D \in M_n(\mathbb{C})$ diagonal, $P \in M_n(\mathbb{C})$ a permutation matrix, and $L$ is a $2n$-dimensional diagonal lattice in $M_n(\mathbb{C})$, then $\delta(AL) = \delta(L)$. 
2.3 Fundamental parallelotopes of special lattices

Proof. First note that
\[
\det(\text{min} L) = \inf \{|\det(X)| : X \in L, X \neq 0\} = |\det(A)| \inf \{|\det(X)| : X \in L, X \neq 0\}
\]
\[
= |\det(A)| \det(L).
\]

The results then follow from Lemma 2.25, Propositions 2.39 and 2.41.

Remarks 2.44. Theorem 2.43 is a generalization of [8, Lemma 10.1].

Remark 2.45. By Remarks 2.40 and 2.42, we directly get that \(\delta(\text{AL}) = \delta(\text{LA}) = \delta(L)\) in the two cases described in Theorem 2.43.
In this chapter, we give an explicit construction of lattice codes based on number fields. As we will see, those codes achieve a correct rate, but which can be improved. Improving the latter will be the object of the chapters about codes from division algebras. So, in the same time we are going to work on number fields, we will be trained to get through the generalization done by the division algebra-based codes, and then by the crossed product algebra-based codes.

3.1 Preliminaries

We suppose that the reader is acquainted with the basics of algebraic number theory. If the reader is not familiar with tools such as Galois extension, Galois group, trace, norm, etc., he is invited to consult [9]. However, to fix the notations, we recall some standard facts that will be used along the thesis. In this section, proofs are generally omitted, the reader will find some references to get further details.

In the sequel, all the fields considered are finite extensions of $\mathbb{Q}$. This assumption is not very restrictive in the coding theoretic point of view, since as it is explained in [1, Remark IV.3.9], in practice a signal is represented by an element of $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$, where $j = e^{2\pi i/3}$.

Let $E/F$ be a Galois extension of degree $n$. For short, if $E = F(\theta)$ is an extension of degree $n$, $E/F$ is said to be Galois if the minimal polynomial of $\theta$ over $F$ has all its roots in $E$.

If the Galois group of $E$ over $F$, that is the group of field automorphisms

$$\text{Gal}(E/F) := \{\sigma : E \rightarrow E \mid \sigma(x) = x, \forall x \in F\}$$

is cyclic, the extension is said to be a cyclic extension, or a cyclic field.

Let us now recall the concepts of trace and norm in a Galois extension. Note that these notions will be extended in Chapter 5 to each element of a central simple algebra, which is a structure we will work on later in the thesis.

**Definition 3.1.** Let $x \in E$ and $\text{Gal}(E/F) = \{\sigma_i\}_{i=1}^n$. The trace of $x$ over $F$ is defined as
\[
\text{Tr}_{E/F}(x) = \sum_{i=1}^{n} \sigma_i(x),
\]
while the norm of \(x\) is
\[
\text{Nr}_{E/F}(x) = \prod_{i=1}^{n} \sigma_i(x).
\]

We also have transitivity of traces and norms in the sense used in the following proposition.

**Proposition 3.2.** Let \(K \subseteq F \subseteq E\) be a finite Galois extensions tower. Then for \(x \in E\),

\[
\text{Nr}_{E/K}(x) = \text{Nr}_{F/K}(\text{Nr}_{E/F}(x))
\]
and
\[
\text{Tr}_{E/K}(x) = \text{Tr}_{F/K}(\text{Tr}_{E/F}(x)).
\]

**Definition 3.3.** Let \(E\) be a field, we denote by
\[
\mathcal{O}_E = \{x \in E \mid \exists \text{ a monic polynomial } f \in \mathbb{Z}[X] \text{ such that } f(x) = 0\}.
\]
the ring of integers of \(E\).

**Remark 3.4.** In Definition 3.3, the fact that \(\mathcal{O}_E\) is indeed a ring is not as straightforward as one can think. Have a look for example at [10, Corollaire 2, p.35].

Say we have an extension of fields \(E/F\). Since \(\mathcal{O}_E\) is a subring of \(E\), we can see \(E\) as a module over \(\mathcal{O}_E\). Now that we know the relationships between \(E\) and \(F\), \(E\) and \(\mathcal{O}_E\), and \(F\) and \(\mathcal{O}_F\), we would like to establish a relationship between \(\mathcal{O}_E\) and \(\mathcal{O}_F\). The next result, which is proved in [4], is aimed at filling this gap, in a particular situation.

**Proposition 3.5.** Let \(E/F\) be a separable extension, and suppose that \(\mathcal{O}_F\) is a principal ideal domain. Then, \(\mathcal{O}_E\) is a free \(\mathcal{O}_F\)-module of rank \([E : F]\). In other words, \(\mathcal{O}_E\) admits an integral basis over \(\mathcal{O}_F\).

**Proof.** See [4, p.12].

From Proposition 3.5, we deduce the two following corollaries, which will be intensively used in the construction of codes from number fields and also in the subsequent chapters.

**Corollary 3.6.** If \(F = \mathbb{Q}\), \(\mathcal{O}_E\) admits a \(\mathbb{Z}\)-basis, which is called an integral basis of \(E\) (or of \(\mathcal{O}_E\)).

**Proof.** This follows from Proposition 3.5.
Corollary 3.7. If \( F = \mathbb{Q}(i) \), \( \mathcal{O}_F \) admits a \( \mathbb{Z}[i] \)-basis.

Proof. This follows from Proposition 3.5. \( \square \)

We give below a generic result about the intersection of the base field and the ring of integers of the top field.

Lemma 3.8. Let \( E/F \) be a finite number field extension. Then \( \mathcal{O}_E \cap F = \mathcal{O}_F \).

Proof. This follows from the definitions. \( \square \)

Now, we want to describe the \( \mathcal{O}_E \)-submodules of \( E \) that are finitely generated, these are exactly the objects we are going to describe in the following definition.

Definition 3.9. A fractional ideal \( \mathcal{I} \) is an \( \mathcal{O}_E \)-submodule of \( E \) such that there exists \( d \in \mathcal{O}_E \setminus \{0\} \) with \( d\mathcal{I} \subseteq \mathcal{O}_E \). If we can take \( d = 1 \), a fractional ideal is said to be an integral ideal.

Remark 3.10. We will not establish it here but there is a situation where fractional ideals naturally appear. Indeed, in the same way that every rational number can be represented in a unique way as a product of prime numbers to some integer powers, such a decomposition also appears for fractional ideals of a ring of algebraic integers.

Armed with the notion of fractional ideal, Corollaries 3.6 and 3.7 extend as follows.

Corollary 3.11. If \( F = \mathbb{Q} \), every fractional ideal \( \mathcal{I} \) of \( \mathcal{O}_E \) admits a \( \mathbb{Z} \)-basis.

Proof. The reader can find the details in [4, p.12]. \( \square \)

Corollary 3.12. If \( F = \mathbb{Q}(i) \), every fractional ideal \( \mathcal{I} \) of \( \mathcal{O}_E \) admits a \( \mathbb{Z}[i] \)-basis.

Proof. The reader can find the details in [4, p.12]. \( \square \)

The concept given in the next definition will be used at some places in our results.

Definition 3.13. The discriminant of \( E/\mathbb{Q} \), denoted by \( d(E/\mathbb{Q}) \) is defined by

\[
d(E/\mathbb{Q}) = D(w_1, \ldots, w_n) = \det(\text{Tr}_{E/\mathbb{Q}}(w_iw_j)) \in \mathbb{Z},
\]

for any \( \mathbb{Z} \)-basis \( w_1, \ldots, w_n \) of \( \mathcal{O}_E \).

Note that the discriminant is independent of the choice of the basis. If \( \{w'_1, \ldots, w'_n\} \) is another basis, then the basis change matrix \( T = (a_{ij}) \) satisfying \( w'_i = \sum_j a_{ij}w_j \), as well as its inverse, has integral entries. It therefore has determinant \( \pm 1 \), so that indeed

\[
D(w'_1, \ldots, w'_n) = \det(T)^2 D(w_1, \ldots, w_n) = D(w_1, \ldots, w_n).
\]

3.2 Construction of the codes and properties

In this section we will show how to produce space-time codes from number fields. For the whole section, let us fix \( E/\mathbb{Q}(i) \) a Galois extension of degree \( n \), and let us assume that \( \text{Gal}(E/\mathbb{Q}(i)) = \{ \sigma_1, \ldots, \sigma_n \} \). The first step is to define a relative canonical embedding of \( E \) into \( M_n(E) \) by
\[ \psi : E \longrightarrow M_n(E) \]
\[ x \mapsto \begin{pmatrix} \sigma_1(x) & 0 & \ldots & 0 \\ 0 & \sigma_2(x) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \sigma_n(x) \end{pmatrix}. \]  
(3.1)

We immediately realize that for all \( x \in E \),
\[ \text{Tr}_{E/Q(i)}(x) = \text{Tr}(\psi(x)) \quad \text{and} \quad \text{Nr}_{E/Q(i)}(x) = \det(\psi(x)). \]  
(3.2)

One can also directly deduce from Proposition 2.15 that for all \( x \in E \),
\[ \text{Tr}_{E/Q}(x) = 2\Re \text{Tr}_{E/Q(i)}(x) \quad \text{and} \quad \text{Nr}_{E/Q}(x) = |\text{Nr}_{E/Q(i)}(x)|^2. \]  
(3.3)

Let us now give a lemma that will be widely used for determining normalized minimum determinants.

**Lemma 3.14.** Let us consider a number field extension \( E/Q(i) \). Then
\[ \text{for all} \quad x \in \mathcal{O}_E, \quad \text{Nr}_{E/Q(i)}(x) \in \mathbb{Z}[i]. \]
Moreover, if \( x \neq 0 \), \( \text{Nr}_{E/Q(i)}(x) \neq 0 \).

**Proof.** Let \( x \in \mathcal{O}_E \). Then as \( \sigma(\mathcal{O}_E) \subseteq \mathcal{O}_E \), we have \( \psi(x) \in M_n(\mathcal{O}_E) \), thus
\[ \text{Nr}_{E/Q(i)}(x) = \det(\psi(x)) \in \mathcal{O}_E. \]

Then, it is also a well-known fact that \( \text{Im}(\text{Nr}_{E/Q(i)}) \subseteq \mathbb{Q}(i) \). So, by Lemma 3.8, we get that
\[ \text{Nr}_{E/Q(i)}(x) \in \mathcal{O}_E \cap \mathbb{Q}(i) = \mathbb{Z}[i]. \]
The additional part of the lemma is clear. \( \square \)

Fractional ideals lie at the root of codes built from number field extensions, as the following proposition suggests.

**Proposition 3.15.** Let \( \mathcal{I} \subseteq d^{-1}\mathcal{O}_E \) be a fractional ideal of \( \mathcal{O}_E \). Then \( \psi(\mathcal{I}) \) is a lattice code of dimension \( 2n \) over \( \mathbb{R} \).

**Proof.** We immediately get that
\[ \psi(\mathcal{I}) = \mathbb{Z}\psi(w_1) \oplus \mathbb{Z}\psi(w_1) \oplus \cdots \oplus \mathbb{Z}\psi(w_n) \oplus \mathbb{Z}\overline{i}\psi(w_n), \]
where the existence of a \( \mathbb{Z}[i] \)-basis \( \{w_1, \ldots, w_n\} \subseteq E \) for \( \mathcal{I} \) is assured by Corollary 3.12, and where we have used the fact that \( \psi \) is \( \mathbb{Q}(i) \)-linear. We have to show that \( \psi(\mathcal{I}) \) is a \( 2n \)-dimensional lattice. We already have that \( \psi(\mathcal{I}) \) is a subgroup of the \( \mathbb{R} \)-vector space \( M_n(\mathbb{C}) \), and using Proposition 2.15, rather than directly proving that
3.2 Construction of the codes and properties

ψ(w_1), iψ(w_1), . . . , ψ(w_n), iψ(w_n) are \( \mathbb{R} \)-linearly independent, let us prove that \( \psi(I) \) is discrete by showing that \( ||\psi(x) - \psi(y)||_F \) stays above a constant strictly greater than 0, for all \( x \neq y \in I \).

So, let \( x, y \in \mathcal{I}, x \neq y \). Since \( \mathcal{I} \subseteq d^{-1}\mathcal{O}_E \), we have that \( x = d^{-1}x' \) and \( y = d^{-1}y' \), for some \( x', y' \in \mathcal{O}_E \). Using Lemma 2.28, we get that

\[
||\psi(x) - \psi(y)||_F = ||\psi(x - y)||_F = ||\psi(d^{-1}(x' - y'))||_F \\
\geq \sqrt{n} |\det(\psi(d^{-1}(x' - y')))|^{1/n} \\
= \sqrt{n} |\det(\psi(d^{-1}))|^{1/n} |\det(\psi(x' - y'))|^{1/n} \\
= \sqrt{n} |\det(\psi(d^{-1}))|^{1/n} |\operatorname{Nr}_{E/\mathbb{Q}(i)}(x' - y')|^{1/n} \\
\geq \sqrt{n} |\det(\psi(d^{-1}))|^{1/n} > 0,
\]

where in the last inequality we used Lemma 3.14 to get that \( |\operatorname{Nr}_{E/\mathbb{Q}(i)}(x' - y')| \geq 1 \). Looking back at Remark 2.16, we get that \( \psi(w_1), i\psi(w_1), . . . , \psi(w_n), i\psi(w_n) \) are linearly independent over the reals. \( \square \)

**Remark 3.16.** Note that in Proposition 3.15, \( \psi(I) \) is also a free \( \mathbb{Z}[i] \)-module. In many applications, it is very beneficial if the lattice has this extra structure. It will be a crucial point in Chapter 6.

As a particular case of Proposition 3.15, we state the following corollary.

**Corollary 3.17.** Let \( E/\mathbb{Q}(i) \) be a Galois extension of degree \( n \). Let \( a \in E, a \neq 0 \). Then

\[
\psi(a\mathcal{O}_E)
\]

is a \( 2n \)-dimensional lattice code in \( M_n(\mathbb{C}) \).

The following lemma gives us a way to compute the volume of the fundamental parallelootope of the lattice code \( \psi(a\mathcal{O}_E) \), \( a \in E, a \neq 0 \). In the final proposition we compute its normalized minimum determinant.

**Lemma 3.18.** Let \( E/\mathbb{Q}(i) \) be a Galois extension of degree \( n \). Let \( a \in E, a \neq 0 \). Then

\[
\operatorname{vol}(\psi(a\mathcal{O}_E)) = 2^{-n} \sqrt{|d(E/\mathbb{Q})|} \cdot \operatorname{Nr}_{E/\mathbb{Q}}(a).
\]

**Proof.** Let us first compute \( \operatorname{vol}(\psi(\mathcal{O}_E)) \). From Proposition 3.15 we know that \( \psi(\mathcal{O}_E) \) is a \( 2n \)-dimensional lattice that we write

\[
\psi(\mathcal{O}_E) = \mathbb{Z}\psi(w_1) \oplus \cdots \oplus \mathbb{Z}\psi(w_{2n}) \subseteq M_n(\mathbb{C}).
\]

But we also immediately realize that each \( \psi(w_i) \) is a diagonal matrix so that \( \psi(\mathcal{O}_E) \) becomes a \( 2n \)-dimensional diagonal lattice. Then, determining the volume of the fundamental parallelootope of \( \psi(a\mathcal{O}_E) \) amounts to computing \( \operatorname{vol}(\gamma(\psi(\mathcal{O}_E))) \), where

\[
\gamma : \{ A \in M_n(\mathbb{C}) : A \text{ is diagonal} \} \rightarrow \mathbb{C}^n
\]
simply maps the \(i\)th nonzero diagonal element of \(\psi(w_j)\) to the \(i\)th element of \(\gamma(\psi(w_j))\). So now \(\gamma(\psi(O_E))\) is a \(2n\)-dimensional lattice in \(\mathbb{C}^n\), and we need to embed it to the real vector space \(\mathbb{R}^{2n}\). We do it by the usual way i.e. splitting each element of a \(\gamma\)-vector into its real and imaginary parts, say this is done by a mapping \(\epsilon\). We finally set \(\eta := \epsilon \circ \gamma\), so that

\[
\text{vol}(\psi(O_E)) = \text{vol}(\eta(\psi(O_E))) = (\det(MM^T))^{1/2},
\]

where \(M \in M_{2n}(\mathbb{R})\) is formed by the \(\eta(\psi(w_i))\)'s as row vectors. Now set \(N := \overline{M}\) which is formed by the \(\eta(\psi(w_i))\)'s as column vectors. By similar arguments as in the proof of Proposition 2.18, we get that

\[
M\overline{N} = (\Re\text{Tr}(\psi(w_i)\psi(w_j)))_{1 \leq i, j \leq 2n}.
\]

Now, using relations (3.2) and (3.3), we have

\[
\det(M\overline{N}) = \det(\Re\text{Tr}_{E/\mathbb{Q}}(w_iw_j)) = 2^{-2n}d(E/\mathbb{Q}).
\]

Finally, as \(\text{vol}(\psi(O_E)) = |\det(M)| = |\det(N)|\), it follows that

\[
\text{vol}(\psi(O_E)) = \sqrt{|\det(M\overline{N})|} = 2^{-n}\sqrt{|d(E/\mathbb{Q})|}.
\]

As the final step of the proof, using Proposition 2.39 from the lattice theoretic part and relation (3.3), we have

\[
\text{vol}(\psi(aO_E)) = \text{vol}(\psi(a)\psi(O_E)) = |\det(\psi(a))|^2\text{vol}(\psi(O_E)) = 2^{-n}\sqrt{|d(E/\mathbb{Q})|N_r}_{E/\mathbb{Q}}(a).
\]

\[\square\]

**Proposition 3.19.** Let \(E/\mathbb{Q}(i)\) be a Galois extension of degree \(n\). Let \(a \in E, a \neq 0\). Then

\[
\delta(\psi(aO_E)) = 2^{n/2}|d(E/\mathbb{Q})|^{-1/4}.
\]

In particular, \(\psi(aO_E)\) has NVD property.

*Proof.* We first note that we can make use of Theorem 2.43 which implies in this case that

\[
\delta(\psi(aO_E)) = \delta(\psi(a)\psi(O_E)) = \delta(\psi(O_E)).
\]

Using Lemma 2.25, we get

\[
\delta(\psi(O_E)) = \frac{\det_{\min}(\psi(O_E))}{\text{vol}(\psi(O_E))^{1/2}}.
\]

Let us compute \(\det_{\min}(\psi(O_E))\). By the definition of the minimum determinant and using relation (3.2), we have that
\[ \det(\psi(\mathcal{O}_E)) = \inf_{x \in \mathcal{O}_E, x \neq 0} \{|\det(\psi(x))|\} = \inf_{x \in \mathcal{O}_E, x \neq 0} \{|\text{Nr}_{E/Q}(x)|\} \]

Then, using Lemma 3.14, we get that
\[ \det(\psi(\mathcal{O}_E)) \geq \inf_{y \in \mathbb{Z}[i], y \neq 0} |y| = 1. \]

On the other hand, \( \text{Nr}_{E/Q}(1) = 1 \). Therefore,
\[ \det(\psi(\mathcal{O}_E)) = \inf_{x \in \mathcal{O}_E, x \neq 0} \{|\text{Nr}_{E/Q}(x)|\} \leq 1. \]

Finally \( \det_{\min}(\psi(\mathcal{O}_E)) = 1 \). Putting everything together and using Lemma 3.18, we get the desired result. \( \square \)

**Remark 3.20.** Let us suppose that we have two cyclic Galois extensions of degree \( n \), \( E/Q(i) \) and \( E'/Q(i) \). Knowing the normalized minimum determinant of lattice codes of the type \( \psi(\alpha \mathcal{O}_E), \psi(\beta \mathcal{O}_E') \), with \( \alpha \in E \) and \( \beta \in E' \), we are now able to predict the efficiency of the codes and choose which one is better to be used.

We are now interested in finding lattice codes that are orthonormal in the natural sense introduced by the following definition. This characteristic will be one of the conditions of fundamental results derived in Chapter 6.

**Definition 3.21.** We say that a lattice
\[ L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k \subseteq V \]
is **orthogonal** if the vectors \( v_i \) are orthogonal to each other with respect to the inner product associated with \( V \) described in Definition 2.1. Moreover, we say that \( L \) is an **orthonormal** lattice if it is orthogonal and each basis vector has equal length.

**Remark 3.22.** Note that orthonormality is usually defined so that basis vectors have length 1.

**Example 3.23.** Consider the field extension \( E = Q(\sqrt{\frac{5}{2}})/Q(i) \). Our goal is to find an "orthonormal ideal," i.e., an ideal of the form \( \alpha \mathcal{O}_E \) such that, as a lattice code, \( \psi(\alpha \mathcal{O}_E) \) has an orthonormal basis.

Let \( \nu = \frac{1 + \sqrt{\frac{5}{2}}}{2} \), and \( \overline{\nu} = \frac{1 - \sqrt{\frac{5}{2}}}{2} \). We know that \( \mathcal{O}_E = \mathbb{Z}[i] \oplus \nu \cdot \mathbb{Z}[i] \) and that \( \text{Gal}(E/Q(i)) = (\sigma) \), defined by \( \sigma: \sqrt{\frac{5}{2}} \mapsto -\sqrt{\frac{5}{2}} \). Note that \( \sigma(\nu) = \overline{\nu} \). Then, keeping the notations of the chapter, we have the following relative canonical embedding of \( E \) into \( M_2(\mathbb{C}) \)
\[ \psi: E \rightarrow M_2(E) \]
\[ x \mapsto \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix}. \]

Let \( \alpha = 1 + i - iv \), then
\[ \alpha \mathcal{O}_E = \alpha \mathbb{Z}[i] \oplus \alpha \nu \mathbb{Z}[i], \]
and therefore \( \psi(\alpha \mathcal{O}_E) = \mathbb{Z}[i] \psi(\alpha) \oplus \mathbb{Z}[i] \psi(\alpha \nu) \). Now, it remains to check that \( \{ \psi(\alpha), i \psi(\alpha), \psi(\alpha \nu), i \psi(\alpha \nu) \} \) is an orthonormal set. We recall that we use the Frobenius norm and the real Frobenius inner product by default in \( M_n(\mathbb{C}) \).

We have

\[
\langle \psi(\alpha), \psi(\alpha) \rangle = \Re \left[ \text{Tr} \left( \begin{pmatrix} 1 + i - \nu & 0 \\ 0 & 1 + i - \nu \end{pmatrix} \right) \right] = 5,
\]

\[
\langle \psi(\alpha), \psi(\alpha \nu) \rangle = \Re \left[ \text{Tr} \left( \begin{pmatrix} 1 + i - \nu & 0 \\ 0 & 1 + i - \nu \end{pmatrix} \right) \begin{pmatrix} \nu + i \nu^2 & 0 \\ 0 & \nu + i \nu^2 \end{pmatrix} \right] = 0,
\]

\[
\langle \psi(\alpha \nu), \psi(\alpha \nu) \rangle = \Re \left[ \text{Tr} \left( \begin{pmatrix} \nu + i \nu^2 & 0 \\ 0 & \nu + i \nu^2 \end{pmatrix} \right) \begin{pmatrix} \nu - i \nu^2 & 0 \\ 0 & \nu - i \nu^2 \end{pmatrix} \right] = 5.
\]

The other conditions to make \( \{ \psi(\alpha), i \psi(\alpha), \psi(\alpha \nu), i \psi(\alpha \nu) \} \) an orthonormal set follow directly from the computations above. Thus, we have constructed our first example of a \( 2n \)-dimensional lattice code in \( M_n(\mathbb{C}) \), with an orthonormal basis. The code derived here will be the starting point of the construction of a more general code, as we will see in Chapter 6. We will there see how much the orthonormality property is relevant.

This chapter gives a first answer to Problem 1.11. Indeed, we have obtained a lattice code of dimension \( 2n \) with NVD property, which gives a dimension rate of value 1. In the following two chapters, we are going to see that the embedding (3.1) follows from the more general theory of splitting fields of central simple algebras.
Central simple algebras

In Chapter 1, we were looking for additive subgroups $D$ of $M_n(\mathbb{C})$ such that every nonzero element of $D$ is invertible. It turns out, as we will see in Chapter 6, that division algebras can be realized as a fully diverse additive group in $M_n(\mathbb{C})$. In a more general context, a division algebra is central simple algebra over its center. Defining these terms will be one of the goals of the following development.

We have assumed that the reader is familiar with groups, rings, fields, vector spaces, morphisms on them, etc., but the theory of central simple algebras is not as common in the general background of any graduate student in mathematics. This is one of the reasons why this chapter is devoted to presenting central simple algebras in detail. The reader who is already familiar with the basic theory can jump to Chapter 6 where we discuss splitting fields of central simple algebras. This chapter as well as Chapter 5 follows the presentation of 

4.1 Introduction to $K$-algebras

Let $K$ be an arbitrary field.

**Definition 4.1.** A $K$-algebra is a pair $(A, \mu)$, where $A$ is a $K$-vector space and $\mu : A \times A \rightarrow A$ is a $K$-bilinear map, called the product law of $A$. We write $aa'$ for $\mu(a, a')$, and call it the product of $a$ and $a'$. We will always assume that the product law is associative and has a unit element $1_A$.

A $K$-algebra is called commutative whenever the product law is commutative.

**Remark 4.2.** Another way to see a $K$-algebra is to consider it as a ring where we have an external action of the field $K$.

**Example 4.3.** (1) The ring of polynomials $K[X]$ is a commutative $K$-algebra.
(2) If $L/K$ is a field extension, then $L$ is a commutative $K$-algebra.
(3) The matrices of size $n$ with elements in $K$, $M_n(K)$, is a noncommutative $K$-algebra.

**Definition 4.4.** A $K$-algebra homomorphism is a $K$-linear map $f : A \rightarrow B$ satisfying $f(aa') = f(a)f(a')$, for all $a, a' \in A$, and $f(1_A) = 1_B$.

A $K$-algebra isomorphism is a $K$-algebra homomorphism which is bijective. In this case, it is easy to see that $f^{-1}$ is also a $K$-algebra homomorphism.
Remark 4.5. For short, a $K$-algebra homomorphism (resp. isomorphism) is a ring homomorphism (resp. isomorphism) that is also $K$-linear.

Definition 4.6. A subalgebra of a $K$-algebra $A$ is a linear subspace $B$ of $A$ which is closed under the product and such that $1_A \in B$. It is commutative whenever $A$ is.

Example 4.7. (1) The intersection of an arbitrary family of subalgebras of a $K$-algebra $A$ is again a subalgebra of $A$.
(2) The kernel (resp. the image) of a $K$-algebra homomorphism $f : A \to B$ is a subalgebra of $A$ (resp. of $B$).

We now deal with a particular subalgebra.

Definition 4.8. The center of a $K$-algebra $A$ is by definition the set
$$Z(A) = \{ z \in A \mid az = za \text{ for all } a \in A \}.$$ It is a commutative subalgebra of $A$.

Example 4.9. The matrix algebra $M_n(K)$ is a noncommutative $K$-algebra with center $K$, by identifying $K$ with the set of scalar matrices $K \cdot I_n$.

The next lemma gives some information on how $K$ is related to $A$.

Lemma 4.10. Let $A$ be a nonzero $K$-algebra. Then $K$ can be identified with a subalgebra of $Z(A)$, hence a subalgebra of $A$.

Proof. Let us consider the mapping
$$\varphi : K \to Z(A)$$
$$\lambda \mapsto \lambda \cdot 1_A.$$ Let us first check that $K \cdot 1_A \subseteq Z(A)$, so that $\varphi$ is well-defined. Let $\lambda \in K$, $a \in A$. The $K$-bilinearity and the properties of $1_A$ imply that we have
$$(\lambda \cdot 1_A)a = 1_A(\lambda \cdot a) = (\lambda \cdot a)1_A = a(\lambda \cdot 1_A).$$ One can then check that $K \cdot 1_A$ is a $K$-subalgebra of $Z(A)$ and that $\varphi$ is an injective $K$-algebra homomorphism. The map $\varphi$ is injective since $K$ is a field and $1_A \neq 0_A$ ($A$ is a nonzero $K$-algebra).

As for now, we make the following assumption.

Assumption 4.11. All $K$-algebras will implicitly be supposed to be finite-dimensional over $K$. Moreover, we will systematically identify $K$ and $K \cdot 1_A$ in the sequel, so that we have $K \subseteq Z(A)$ (and therefore $1_K = 1_A$).

Definition 4.12. A division $K$-algebra is a $K$-algebra which is also a division ring, that is, every non-zero element is invertible.

Let us now study more closely subalgebras generated by one element.
**Definition 4.13.** Let $D$ be a finite-dimensional division $K$-algebra, and let $d \in D^\times$. We denote by $K[d]$ the smallest subalgebra of $D$ containing $d$, and by $K(d)$ the smallest division subalgebra of $D$ containing $d$.

**Remark 4.14.** Clearly we have

$$K[d] = \{ P(d) | P \in K[X] \}.$$ 

Since $D$ is finite-dimensional over $K$, so is $K[d]$. Therefore, the successive powers of $d$ cannot be linearly independent, and the evaluation homomorphism

$$ev_d : K[X] \rightarrow D$$

$$P \mapsto P(d)$$

cannot be injective. Hence, since $K[X]$ is a principal ideal domain, its kernel is generated by a unique monic polynomial $\mu_d \in K[X]$, and we have an isomorphism of $K$-algebras

$$K[X]/(\mu_d) \cong K[d].$$

Since $D$ has no zero divisors, $K[d]$ is an integral domain and $(\mu_d)$ is a prime ideal, hence maximal. Thus $K[d]$ is a field, $K[d] = K(d)$ and moreover

$$[K(d) : K] = \deg(\mu_d).$$

This remark is just to make the link between the known standard results in algebra and this master thesis. We will use these facts without further reference.

**Definition 4.15.** Let $D$ be a division $K$-algebra, and let $d \in D$. The polynomial $\mu_d$ is called the *minimal polynomial* of $d \in D$ over $K$.

We give here the main properties of the tensor product of two $K$-algebras.

**Definition 4.16.** If $A$ and $B$ are $K$-algebras, their *tensor product* $A \otimes_K B$ may be viewed as the $K$-vector space spanned by the symbols $a \otimes b, a \in A, b \in B$ subject to the relations

$$(a + a') \otimes b = a \otimes b + a' \otimes b$$

$$a \otimes (b + b') = a \otimes b + a \otimes b'$$

$$(\lambda a) \otimes b = a \otimes (\lambda b) = \lambda(a \otimes b)$$

for all $a, a' \in A, b, b' \in B, \lambda \in K$. The symbols $a \otimes b$ are called *elementary tensors*.

**Proposition 4.17.** The product on $A \otimes_K B$ is the unique distributive law (with respect to addition) satisfying

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

for all $a, a' \in A, b, b' \in B$.

The $K$-algebra $A \otimes_K B$ is commutative whenever $A$ and $B$ are.

**Proof.** See [1, Appendix A].
Proposition 4.18. If \((e_i)_{i \in I}\) and \((e'_j)_{j \in J}\) are respectively \(K\)-bases of \(A\) and \(B\), then \((e_i \otimes e'_j)_{(i,j) \in I \times J}\) is a \(K\)-basis of \(A \otimes_K B\). In particular, \(A \otimes_K B\) is finite-dimensional as a \(K\)-vector space if and only if \(A\) and \(B\) are, and in this case we have
\[
\dim_K(A \otimes_K B) = \dim_K(A) \dim_K(B).
\]

Proof. See [1, Appendix A].

Lemma 4.19. If \(A\) and \(B\) are \(K\)-algebras, the \(K\)-algebra homomorphisms
\[
A \longrightarrow A \otimes_K B \quad \text{and} \quad B \longleftarrow A \otimes_K B
\]
\[a \longmapsto a \otimes 1_B \quad \text{and} \quad b \longmapsto 1_A \otimes b\]
are injective.

Proof. This is obvious.

Lemma 4.20. If \(\phi : A \longrightarrow C\) and \(\psi : B \longrightarrow C\) are two \(K\)-algebra homomorphisms with commuting images i.e. satisfying
\[
\phi(a)\psi(b) = \psi(b)\phi(a) \quad \text{for all} \quad a \in A, b \in B,
\]
then there exists a unique \(K\)-algebra homomorphism \(h : A \otimes_K B \longrightarrow C\) satisfying
\[
h(a \otimes 1_B) = \phi(a) \quad \text{and} \quad h(1_A \otimes b) = \psi(b), \quad \text{for all} \quad a \in A, b \in B.
\]
Moreover, the aforementioned homomorphism is given by
\[
h : A \otimes_K B \longrightarrow C
\]
\[a \otimes b \longmapsto \phi(a)\psi(b).
\]

Proof. For the existence of such an \(h\), see [1, Appendix A].

Corollary 4.21. If \(f : A \longrightarrow A'\) and \(g : B \longrightarrow B'\) are two \(K\)-algebra homomorphisms, then there exists a unique \(K\)-algebra homomorphism given by
\[
f \otimes g : A \otimes_K B \longrightarrow A' \otimes_K B'
\]
\[a \otimes b \longmapsto f(a) \otimes g(b).
\]
If \(f\) and \(g\) are isomorphisms, so is \(f \otimes g\).

Proof. This is a straightforward consequence of Lemma 4.20.

We give below a series of properties of the tensor product of algebras.

Lemma 4.22. Let \(L/K\) be a field extension. If \(A\) is a \(K\)-algebra and \(B\) is an \(L\)-algebra, then \(A \otimes_K B\) has a natural structure of \(L\)-algebra.

Proof. [Sketch] The structure of \(L\)-vector space is defined on elementary tensors by
\[
\lambda \cdot (a \otimes b) = a \otimes \lambda b, \quad \text{for all} \quad \lambda \in L, a \in A, b \in B.
\]
Corollary 4.23. Let $L/K$ be a field extension. If $A$ is a $K$-algebra then $A \otimes_K L$ has a natural structure of $L$-algebra. Moreover, $A \otimes_K L$ is finite-dimensional over $L$ if and only if $A$ is finite-dimensional over $K$. In this case, we have
\[ \dim_L(A \otimes_K L) = \dim_K(A). \]

Proof. This follows from the previous lemma. Elements for a proof of the additional part can be found in [1, Appendix A].

Lemma 4.24. Let $L/K$ be a field extension. If $A$ is a $K$-algebra and $B$ is an $L$-algebra, then we have the following natural isomorphism of $L$-algebras
\[ (A \otimes_K L) \otimes_L B \cong_L A \otimes_K B. \]

Proof. See [1, Appendix A].

Remark 4.25. Similarly, $B \otimes_K A$ and $L \otimes_K A$ have a natural structure of $L$-algebras, and we have an isomorphism of $L$-algebras
\[ B \otimes_L (L \otimes_K A) \cong_L B \otimes_K A. \]

Lemma 4.26. If now $A$ and $B$ are two $K$-algebras and $L/K$ is a field extension then we have a natural $L$-algebra isomorphism
\[ (A \otimes_K B) \otimes_K L \cong_L (A \otimes_K L) \otimes_L (B \otimes_K L). \]

Proof. See [1, Appendix A].

Lemma 4.27. If $K \subseteq E \subseteq F$ is a tower of field extensions, then we have
\[ (A \otimes_K E) \otimes_E F \cong_F A \otimes_K F. \]

Proof. See [1, Appendix A].

The following lemma will be used intensively in the next chapter.

Lemma 4.28. Let $A$ be a $K$-algebra, $n \geq 1$ an integer and $L/K$ a field extension. Then the following holds
(1) We have a natural $K$-algebra isomorphism $M_n(K) \otimes_K A \cong_K M_n(A)$;
(2) We have a natural $L$-algebra isomorphism $M_n(K) \otimes_K L \cong_L M_n(L)$.

Proof.
(1) Consider the following two $K$-algebra homomorphisms
\[
\phi : M_n(K) \rightarrow M_n(A) \quad \text{and} \quad \psi : A \rightarrow M_n(A),
\]
where $\phi$ maps $M \mapsto M$ and $a \mapsto aI_n$.

One can check that $\phi$ and $\psi$ have commuting images, so by Lemma 4.20, there exists a unique $K$-algebra homomorphism given by
\[
h : M_n(K) \otimes_K A \rightarrow M_n(A),
\]
where $M \otimes a \mapsto aM$.

Now, it suffices to show that $h$ is an isomorphism. Since
\[
\dim_K(M_n(K) \otimes_K A) = \dim_K(M_n(A)),
\]
we only need to prove that $h$ is surjective. Let $M = (M_{ij}) \in M_n(A)$. Then we have
\[
M = h \left( \sum_{i,j=1}^{n} E_{ij} \otimes m_{ij} \right).
\]
So, $h$ is surjective.

(2) By (1) we get that $M_n(K) \otimes_K L \cong_K M_n(L)$, so it remains to prove that the underlying isomorphism is an isomorphism of $L$-algebras. Let $\lambda, a \in L$, $M \in M_n(K)$. We have that
\[
h(\lambda(M \otimes a)) = h(M \otimes \lambda a) = \lambda aM = \lambda h(M \otimes a),
\]
which proves the $L$-linearity.

\[\square\]

Remark 4.29. In particular, we have a natural isomorphism
\[
M_n(K) \otimes M_n(K) \cong_K M_{mn}(K)
\]
which maps $M \otimes N$ onto the Kronecker product of $M$ and $N$.

4.2 Introduction to central simple algebras

We now define the main object on which codes will be based.

Definition 4.30. Let $K$ be a field. A $K$-algebra $A$ is simple if it has no non-trivial two-sided ideals.

The next lemma gives an elementary but very useful property of simple algebras.

Lemma 4.31. Let $K$ be a field, and let $\phi : A \rightarrow B$ be a $K$-algebra homomorphism. If $A$ is simple, then $\phi$ is injective. If moreover $A$ and $B$ are finite-dimensional over $K$ and $\dim_K(A) = \dim_K(B)$, then $\phi$ is an isomorphism.

Proof. Let us suppose that $A$ is simple. Then as $\ker(\phi)$ is an ideal of $A$, then it is either 0 or $A$. Recalling that $\phi(1) = 1$ we have that $\ker(\phi) = 0$, so $\phi$ is an injection. The additional part follows from linear algebra. \[\square\]
We now give some examples of simple algebras.

Example 4.32. (1) Any division ring $D$ is a simple algebra over its center. Indeed, $Z(D)$ is a field and the fact that $D$ is a $Z(D)$-algebra is easy to see. The simplicity part follows from the fact that any ideal of a division ring is either 0 or contains a unit so is $D$ itself.

(2) Let $K$ be an arbitrary field. Then $M_n(K)$ is a simple algebra. Indeed, let $J$ be a nonzero ideal of $M_n(K)$ generated by a matrix $M = (m_{ij}) \neq 0 \in M_n(K)$. We are going to show that $J$ contains a unit so that we will have $J = M_n(K)$.

Let $E_{ii} = m_{rs}^{-1} E_{ir} M E_{si} \in J$.

Finally, $I_n = \sum_{i=1}^{n} E_{ii} \in J$, which is the desired result.

(3) More generally, if $D$ is a division $K$-algebra, then $M_r(D)$ is a simple $K$-algebra for all $r \geq 1$.

Definition 4.33. A $K$-algebra $A$ is called central if $Z(A) = K$. A central simple $K$-algebra is a $K$-algebra which is central and simple.

Example 4.34. (1) Any division ring $D$ is a central simple algebra over its center. The fact that $D$ is a simple $Z(D)$-algebra was already pointed out in Example 4.32(1). The centrality part follows by construction.

(2) The $K$-algebra $M_n(K)$ is central simple.

(3) If $D$ is a central division $K$-algebra, then $M_r(D)$ is a central simple $K$-algebra for all $r \geq 1$. Indeed, the fact that $M_r(D)$ is simple was already pointed out in Example 4.32(3). Let $M = (m_{ij}) \in Z(M_r(D))$. Since $E_{ij} M = M E_{ij}$, for all $1 \leq i, j \leq r$ we get that $M$ is a diagonal matrix with $d := m_{11} = m_{22} = \ldots = m_{rr}$. The fact that $M \in Z(M_r(D))$ implies that $d \in Z(D) = K$. So, $M \in K I_n$, which is the desired result.

(4) If $L/K$ is a proper field extension, then $L$ is a simple $K$-algebra which is not central.

Definition 4.35. We say that a central simple algebra is split if it is isomorphic to a matrix algebra.

Remark 4.36. Even if not all simple algebras are split, they can be naturally viewed as subalgebras of matrix algebras, as it will be shown now. This property is particularly important for explicit computations and code constructions.

Definition 4.37. Let $A$ be a $K$-algebra. A subfield of $A$ is a commutative subalgebra $L$ of $A$ which is also a field. In particular, $A$ is a right $L$-vector space. Moreover, $L$ contains $K$ since it is a $K$-algebra. However, notice that $A$ is not an $L$-algebra (unless $L = K$), since $L$ does not necessarily commute with all the elements of $A$ (remember Assumption 4.11).
Remark 4.38. In the subsequent results, we will work with the set of $L$-linear applications over $A$, namely $\text{End}_L(A)$. One can realize that $\text{End}_L(A)$ has a structure of $L$-algebra, and in particular of $K$-algebra. The action of $L$ on the right is given by

$$\text{End}_L(A) \times L \rightarrow \text{End}_L(A) \quad (u, \lambda) \mapsto \left\{ u\lambda : A \rightarrow A \mid z \mapsto u(z)\lambda \right\},$$

while it is defined on the left by

$$L \times \text{End}_L(A) \rightarrow \text{End}_L(A) \quad (\lambda, u) \mapsto \left\{ \lambda u : A \rightarrow A \mid z \mapsto u(z\lambda) = u(z)\lambda \right\}.$$ 

Note that although $L$ is included in the center of $\text{End}_L(A)$, it is not necessarily contained in the center of $A$.

We may now state the next result.

**Lemma 4.39.** Let $A$ be a $K$-algebra, and let $L$ be a subfield of $A$. The following mapping

$$\Phi : A \rightarrow \text{End}_L(A) \quad a \mapsto \left\{ l_a : A \rightarrow A \mid z \mapsto az \right\}$$

is a well-defined $K$-algebra homomorphism. In particular, if $A$ is simple, $\phi$ is injective.

**Proof.** Let us check that $l_a$ is an endomorphism of the right $L$-vector space $A$. We have

$$l_a(z\lambda + z') = a(z\lambda + z') = az\lambda + az' = l_a(z)\lambda + l_a(z'),$$

for all $z, z' \in A$ and $\lambda \in L$. Hence, $l_a$ is an endomorphism of the right $L$-vector space $A$.

Let us now check that $\Phi$ is a $K$-algebra homomorphism. Clearly, we have $l_1 = \text{Id}_A$. Let $\mu \in K$ and $a, b \in A$. For all $z \in A$ we have

$$l_{\mu a + b}(z) = (\mu a + b)z = \mu az + bz = \mu l_a(z) + l_b(z).$$

We then get $\Phi(\mu a + b) = \mu \Phi(a) + \Phi(b)$. Let $a, a' \in A$. For all $z \in A$ we have

$$l_{aa'}(z) = aa'z = l_a \circ l_{a'}(z).$$

We then get $\Phi(aa') = \Phi(a)\Phi(a')$. The last part follows from Lemma 4.31. \qed

**Remark 4.40.** Let $A$ be a simple $K$-algebra. Let us choose a basis of the right $L$-vector space $A$, and set

$$m = \dim_L(A) = \frac{\dim_K(A)}{[L : K]}.$$
Then, composing the injective $K$-algebra homomorphism $\Phi$ defined in the previous lemma with the isomorphism $\text{End}_L(A) \cong_K M_m(L)$ gives rise to an injective $K$-algebra homomorphism

$$
\varphi_{A,L} : A \xleftarrow{\phi} \text{End}_L(A) \xrightarrow{\sim} K M_m(L) \xrightarrow{\phi} M_a,
$$

where $M_a$ is the matrix of left multiplication by $a$ in the chosen $L$-basis of $A$. For example, if $L = K$, we obtain an injection $\varphi_{A,K} : A \hookrightarrow M_d(K)$, where $d = \dim_K(A)$. So, each simple algebra can be embedded into a matrix algebra over a subfield. The embedding given in (4.1) will be crucial for the design of space-time codes done in the subsequent chapters.
The goal of this chapter is to prove the existence of central simple algebras splitting fields with good properties. We will then use the results obtained to extend the notion of characteristic polynomial to any element of a central simple algebra. This will lead to the concept of reduced norm, which will play a crucial role in coding theoretic Chapters 6 and 7. As the previous chapter, Chapter 5 follows [1].

5.1 Preliminaries

We start by introducing the notions which will be used in this chapter. For the sake of completeness, the reader can find the proofs in [1, Chapter III].

5.1.1 Some additional properties of the tensor product of $K$-algebras

**Proposition 5.1.** Let $A$ and $B$ be two $K$-algebras, and let $L/K$ be a field extension. Then the following holds

(1) $A \otimes_K B$ is central over $K$ if and only if $A$ and $B$ are central over $K$;
(2) $A \otimes_K L$ is central over $L$ if and only if $A$ is central over $K$.

*Proof.* See [1, Chapter III].

**Proposition 5.2.** If $A$ is a central simple $K$-algebra and $B$ is a simple $K$-algebra, then $A \otimes_K B$ is simple.

*Proof.* See [1, Chapter III].

**Proposition 5.3.** Let $A$ and $B$ be two $K$-algebras, and let $L/K$ be a field extension. Then the following holds

(1) If $A$ and $B$ are central simple, so is $A \otimes_K B$;
(2) $A$ is central simple over $K$ if and only if $A \otimes_K L$ is central simple over $L$.

*Proof.* See [1, Chapter III].
5.1.2 Wedderburn’s theorem

As pointed out in Example 4.34(3), $M_r(D)$ is central simple for all $r \geq 1$ and for every central division $K$-algebra $D$. We now state the converse, which is known as Wedderburn’s theorem.

**Theorem 5.4 (Wedderburn’s Theorem).** Any simple $K$-algebra $A$ is isomorphic to $M_r(D)$, for some integer $r \geq 1$ and some division $K$-algebra $D$ whose center is isomorphic to the center of $A$. In particular, a central simple $K$-algebra is isomorphic to a matrix algebra over a central division $K$-algebra. Moreover, the integer $r$ and the isomorphism class of $D$ only depend on the isomorphism class of $A$. In other words, if $M_n(D) \cong_K M_r(D')$, for some integers $n, r$ and some $K$-central division algebras $D$ and $D'$, then we get

$$D \cong_K D' \text{ and } n = r.$$  

**Proof.** See [1, Chapter III].

**Corollary 5.5.** Let $A$ and $B$ be two central simple $K$-algebras. For every integer $n \geq 1$, we have

$$M_n(A) \cong_K M_n(B) \iff A \cong_K B.$$  

**Proof.** See [1, Chapter III].

**Corollary 5.6.** If $K$ is algebraically closed, every central simple $K$-algebra is isomorphic to a matrix algebra over $K$.

**Proof.** See [1, Chapter III].

**Lemma 5.7.** Let $A$ be a central simple $K$-algebra, and let $\overline{K}$ be an algebraic closure of $K$. Then we have the following $\overline{K}$-algebra isomorphism

$$A \otimes_K \overline{K} \cong_{\overline{K}} M_n(\overline{K}),$$

for some $n \geq 1$.

**Proof.** Since $A \otimes_K \overline{K}$ is a central simple algebra over $\overline{K}$ this follows from the previous corollary.

**Corollary 5.8.** The dimension of a central simple $K$-algebra is the square of an integer.

**Proof.** Let $A$ be a $K$-algebra of degree $n$, and $\overline{K}$ an algebraic closure of $K$. By Lemma 5.7 we have that

$$\dim_K(A) = \dim_{\overline{K}}(A \otimes_K \overline{K}) = \dim_{\overline{K}}(M_n(\overline{K})) = n^2.$$  

□
Therefore the following definition makes sense.

**Definition 5.9.** Let $A$ be a central simple $K$-algebra. The *degree* of $A$ is the integer $\deg(A) = \sqrt{\dim_K(A)}$. The *index* of $A$ is the integer $\text{ind}(A) = \deg(D)$, where $D$ is the unique central division $K$-algebra associated to $A$ by Wedderburn’s theorem.

**Remark 5.10.** By definition, $\text{ind}(A) | \deg(A)$, and $\deg(A) = \text{ind}(A)$ if and only if $A$ is a central division $K$-algebra.

**Lemma 5.11.** Let $A$ be a $K$-algebra of degree $n$. Assume that $A \cong_K M_r(D)$ for some $r \geq 1$ and $D$ a $K$-division algebra of degree $s$. Then we have $n = rs$.

**Proof.** Note that

$$n^2 = \dim_K(A) = \dim_K(M_r(D)) = \dim_D(M_r(D)) \dim_K(D) = r^2 s^2.$$


### 5.2 Splitting fields

**Definition 5.12.** Let $A$ be a central simple $K$-algebra of degree $n$. A field $L$ is called a *splitting field* of $A$ if it contains $K$ and if we have an $L$-algebra isomorphism $A \otimes_K L \cong_L M_n(L)$. In this situation, we also say that $A$ splits over $L$, or that $L$ splits $A$.

**Remark 5.13.** Note that a splitting field may not be a subfield.

**Lemma 5.14.** Let $A$ be a central simple $K$-algebra. By Wedderburn’s theorem, we may write $A \cong_K M_r(D)$, for some central division $K$-algebra $D$ and some integer $r \geq 1$. Then for any field extension $L/K$, $L$ splits $A$ if and only if $L$ splits $D$.

**Proof.** Let $n := \deg_K(A)$ and $s := \deg_K(D)$ so that $n = rs$ (using Lemma 5.11). Let us first suppose that $L$ splits $A$ i.e. $A \otimes_K L \cong_L M_n(L)$. Then using Lemma 4.28 we have that

$$A \otimes_K L \cong_L M_r(D) \otimes_K L$$

$$\cong_L (M_r(K) \otimes_K D) \otimes_K L$$

$$\cong_L M_r(K) \otimes_K (D \otimes_K L)$$

$$\cong_L M_r(D \otimes_K L).$$

So, $M_r(M_s(L)) \cong_L M_r(D \otimes_K L)$. By Corollary 5.5, we get that $M_s(L) \cong_L D \otimes_K L$ and therefore $L$ splits $D$.

Conversely, if $L$ splits $D$ say $D \otimes_K L \cong_L M_s(L)$, similarly we get that

$$M_n(L) \cong_L M_r(M_s(L)) \cong_L M_r(D \otimes_K L) \cong_L A \otimes_K L,$$

so $L$ splits $A$. \qed
We are going to establish the existence of splitting fields with various properties. We first investigate under which conditions a subfield $L$ of a central simple $K$-algebra $A$ is a splitting field.

Before, we need new results.

### 5.2.1 The centralizer theorem

The proof of the centralizer theorem can be found in [1, Chapter III]. First, we need a definition.

**Definition 5.15.** Let $A$ be a $K$-algebra, and let $B \subseteq A$ be a subset of $A$. The centralizer of $B$ in $A$ is the set $C_A(B)$ defined by

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

Clearly, this is a subalgebra of $A$ and $C_A(A) = Z(A)$.

In the study of the centralizer of a simple subalgebra, the main theorem is the following.

**Theorem 5.16 (Centralizer theorem).** Let $K$ be a field. Let $A$ be a central simple $K$-algebra, and let $B$ be a simple subalgebra of $A$. Then the following properties hold

1. The centralizer $C_A(B)$ of $B$ in $A$ is a simple subalgebra of $A$ having same center as $B$. Moreover, we have

$$\dim_K(A) = \dim_K(B) \dim_K(C_A(B)).$$

    In particular, $\dim_K(B) | \dim_K(A)$;

2. We have $C_A(C_A(B)) = B$;

3. If $L = Z(B)$ and $r = [L : K]$, then $A \otimes_K L \cong_K M_r(B \otimes_L C_A(B))$. In particular, if $Z(B) = K$ we have $A \cong_K B \otimes_K C_A(B)$.

**Proof.** See [1, Chapter III].

**Corollary 5.17.** Let $A$ be a central simple $K$-algebra, and let $L$ be a subfield of $A$ of degree $r$ over $K$. We then have

$$A \otimes_K L \cong_L M_r(C_A(L)).$$

**Proof.** See [1, Chapter III].
The following lemma proves that there are some restrictions on the degree of a subfield of an algebra.

**Lemma 5.18.** Let $A$ be a central simple $K$-algebra, and let $L$ be a subfield of $A$. Then $[L : K] \mid \deg(A)$.

**Proof.** Since $L$ is a simple subalgebra of $A$, the centralizer theorem gives that

$$\dim_K(A) = \dim_K(L) \dim_K(C_A(L)).$$

Therefore, $\deg(A)^2 = [L : K] \dim_K(C_A(L))$.

Since $C_A(L)$ is a subalgebra of $A$ containing $L$, $C_A(L)$ can be seen as a right $L$-vector space. It follows that,

$$\dim_K(C_A(L)) = \dim_L(C_A(L))[L : K].$$

Finally, $\deg(A)^2 = [L : K]^2 \dim_L(C_A(L))$, i.e. $[L : K]^2 | \deg(A)^2$ leading to the desired result. \qed

### 5.2.2 Maximal subfields

In particular, Lemma 5.18 tells us that the maximal possible degree of a subfield of a central simple $K$-algebra of degree $n$ is $n$. Such subfields deserve a special name.

**Definition 5.19.** Let $A$ be a central simple $K$-algebra of degree $n$. A **maximal subfield** of $A$ is a subfield of degree $n$ over $K$.

The main interest in these particular subfields is given by the following proposition.

**Proposition 5.20.** Let $A$ be a $K$-algebra, and let $L$ be a subfield of $A$. Then there exists a unique $L$-algebra homomorphism

$$f : A \otimes_K L \longrightarrow \text{End}_L(A)$$

$$a \otimes \lambda \mapsto \begin{cases} f(a \otimes \lambda) : A \longrightarrow A \\ z \longmapsto az\lambda \end{cases}.$$

Moreover, if $A$ is central simple, and $[L : K] = \deg(A)$, then $f$ is an isomorphism. In other words, any maximal subfield is a splitting field of $A$.

**Proof.** Consider the $K$-algebra homomorphism $\Phi$ of Lemma 4.39

$$\Phi : A \longrightarrow \text{End}_L(A) \quad \text{and let} \quad \Psi : L \longrightarrow \text{End}_L(A)$$

$$a \longmapsto A \longmapsto A, \quad \lambda \longmapsto \text{Id}_A\lambda.$$

We let the reader check that $\Psi$ is also an homomorphism of $K$-algebras. Let us now verify that $\Phi$ and $\Psi$ have commuting images. Indeed, let $a \in A$ and $\lambda \in L$. Then for all $z \in A$ we have

$$\Phi(a) \circ \Psi(\lambda)(z) = \Phi(a)(z\lambda) = az\lambda = \Psi(\lambda)(az) = \Psi(\lambda) \circ \Phi(a)(z).$$
Then, applying Lemma 4.20, we get that there exists a unique $K$-algebra homomorphism  
$$ f : A \otimes_K L \longrightarrow \text{End}_L(A) $$ 
satisfying $f(a \otimes \lambda)(z) = az\lambda$, for all $z \in A$. Now, we just need to show that $f$ is an $L$-algebra homomorphism. Let $l \in L$, for all $z \in A$ we have 
$$ f((a \otimes \lambda)l)(z) = f(a \otimes \lambda l)(z) = az\lambda l = (f(a \otimes \lambda)(z))l. $$
It remains to prove that if $A$ is central simple and $[L : K] = \deg(A)$, then $f$ is an isomorphism. We know that 
$$ \dim_L(A) = \frac{\dim_K(A)}{[L : K]} = [L : K]. $$
So we get 
$$ \dim_L(A \otimes_K L) = \dim_K(A) = [L : K]^2 = \dim_L(A)^2 = \dim_L(\text{End}_L(A)). $$
Moreover, since $A$ is central simple, so is $A \otimes_K L$ by Proposition 5.1(2), and it suffices to apply Lemma 4.31 to conclude. 

Remark 5.21. A maximal subfield does not necessarily exist. For example, if $K$ is algebraically closed, there is no proper field extension of $K$, so $L$ does not exist if $A \neq K$. However, we are going to prove that such an $L$ always exists if $A$ is a division algebra.

Proposition 5.22. Let $D$ be a central division $K$-algebra of degree $n$, and let $L$ be a subfield of $D$ with $r = [L : K]$. Then the following properties are equivalent

1. $L$ is a splitting field of $D$;
2. $C_D(L) = L$;
3. $L$ is a maximal subfield of $D$.

Proof.
(1) $\implies$ (2)
Let us suppose that $L$ splits $D$. Then $D \otimes_K L \cong L M_n(L)$. Using Corollary 5.17 we then get that $M_r(C_D(L)) \cong L M_n(L)$. Recalling that $n = rs$ with $s := \deg(C_D(L))$, we have that 
$$ C_D(L) \cong L M_s(L). $$
But since $D$ is a division ring, so is $C_D(L)$, hence $s = 1$. As $L \subseteq C_D(L)$, we finally get that $C_D(L) = L$.

(2) $\implies$ (3)
If $C_D(L) = L$, by Theorem 5.16(3) we get that $\deg(D)^2 = [L : K]^2$. So $[L : K] = \deg(D)$ and $L$ becomes a maximal subfield of $D$.

(3) $\implies$ (1)
This is a particular case of Proposition 5.20. \qed
Corollary 5.23. Every central division algebra has a maximal subfield.

Proof. Let $L$ be a subfield of $D$ of maximal degree. Let us prove that in fact $L = C_D(L)$. Suppose the contrary and let $x \in C_D(L)$ such that $x \notin L$. Thus, as $D$ is a division ring, $L(x)$ is a subfield of $D$ which has strictly larger degree than $L$, contradicting the maximality of $[L : K]$. Thus $L = C_D(L)$ and by Proposition 5.22 $L$ is a maximal subfield of $D$. \qed

Corollary 5.24. Every central simple $K$-algebra $A$ has a subfield of degree $\text{ind}(A)$ over $K$ which splits $A$.

Proof. Write $A \cong_K M_r(D)$, for some integer $r \geq 1$ and $D$ a central division algebra over $K$. By the previous corollary, there exists a maximal subfield $L$ for $D$. As any maximal subfield of a central simple algebra is a splitting field, we get that $L$ splits $D$ and therefore $L$ splits $A$ by Lemma 5.14. Moreover, we have that
\[ \deg(L) = \deg(D) = \text{ind}(A), \]
as desired. \qed

Remark 5.25. (1) If $A$ is a central simple $K$-algebra and $L$ is a maximal subfield, then $C_A(L) = L$. Indeed, $L \subseteq C_A(L)$ and an application of the centralizer theorem shows that $[C_A(L) : K] = n = [L : K]$. Therefore $C_A(L) = L$.

(2) Let $D$ be a central division $K$-algebra, and let $L$ be a subfield of $D$. Then $L$ is a maximal subfield of $D$ if and only if it is maximal for the inclusion. Indeed, if $L$ is a maximal subfield, it has maximal degree by Proposition 5.20 and therefore is maximal for the inclusion. Conversely, if $L$ is maximal for the inclusion, it has the largest possible degree among the subfields of $D$ i.e. $\deg(D) = [L : K]$, which shows that $L$ is a maximal subfield.

(3) This result is not true anymore for arbitrary central simple $K$-algebras. For example, $\overline{K}$ is a subfield of $M_n(\overline{K})$ which is maximal for the inclusion, but is not a maximal subfield in the sense of Definition 5.19.

(4) The second remark also implies that every subfield $K$ of a central division $K$-algebra $D$ is contained in a maximal subfield, since it is contained in a subfield which is maximal for the inclusion. In particular, every element $d \in D$ is contained in a maximal subfield of $D$ (since $d \in K(d)$).

A central simple $K$-algebra $A$ may have splitting fields of degree larger than $\deg(A)$, and therefore not contained in $A$ by Lemma 5.18. However, we have the following result.
Proposition 5.26. Let $A$ be a central simple $K$-algebra of degree $n$, and let $L$ be a splitting field of $A$ of finite degree $m$ over $K$. Then there exists a central simple $K$-algebra $A'$ of degree $m$ such that

1. $M_m(A) \cong_K M_m(A')$;
2. $L$ is isomorphic to a maximal subfield of $A'$.

Proof. See [1, Proposition IV.1.12].

Corollary 5.27. Let $A$ be a central simple $K$-algebra, and let $L$ be a field extension satisfying $[L : K] = \deg(A)$. Then $L$ is a splitting field of $A$ if and only if it is isomorphic to a maximal subfield of $A$.

Proof. Let us first suppose that $L$ is a splitting field of $A$. Then by Proposition 5.26 there exists a $K$-algebra $A'$ of degree $m := \deg(A') = \deg(A)$ satisfying $M_m(A) \cong_K M_m(A')$ and such that $L$ is isomorphic to a maximal subfield of $A'$. By Corollary 5.5, this in particular implies that $A \cong_K A'$. Thus $L$ is isomorphic to a maximal subfield of $A$. Conversely, assume that $L$ is isomorphic to a maximal subfield of $A$. Then this directly implies that $L$ is a splitting field of $A$ by Proposition 5.20.

Corollary 5.28. Let $A$ be a central simple $K$-algebra. For any splitting field $L$ of finite degree over $K$, we have

$$\mathrm{ind}(A)[[L : K]].$$

Proof. Write $A \cong_K M_r(D)$, for some integer $r \geq 1$ and $D$ a central division algebra over $K$. Write $s := \deg(D) = \mathrm{ind}(A)$. Let $L$ be a splitting field of $A$. By Lemma 5.14, $L$ is also a splitting field of $D$. Denote by $m$ the degree of $L$ over $K$. By Proposition 5.26, there exists a $K$-central simple algebra $A'$ of degree $m$ such that $M_m(D) \cong_K M_s(A')$. Now, write $A' = M_p(D')$ for some integer $p \geq 1$ and $D'$ a central division algebra over $K$. We get that

$$M_m(D) \cong_K M_sp(D').$$

By the uniqueness part of Wedderburn’s theorem, it follows that $m = sp$, thus $s|m$. □

5.3 Galois splitting fields

We are now going to investigate the existence of Galois splitting fields. As for now, we only work with fields of characteristic 0.

Corollary 5.29. Every central simple $K$-algebra has a Galois splitting field of finite degree over $K$.

Proof. Let $A$ be a central simple algebra over $K$. Write $A \cong_K M_r(D)$ for some integer $r \geq 1$ and $D$ a central division algebra over $K$. We know that $D$ has a maximal subfield $L$ which splits $D$ and therefore $A$. Let $L'$ be the Galois closure of $L$ in $\overline{K}$. We have that

$$A \otimes_K L' \cong_{L'} (A \otimes_K L) \otimes_L L' \cong_{L'} M_n(L) \otimes_L L' \cong_{L'} M_n(L').$$

So, $L'$ is a Galois splitting field of $A$. □
Remark 5.30. One may wonder whether every central division $K$-algebra $D$ has a Galois maximal subfield. The answer is negative, but producing a counterexample would be beyond the scope of this project, as expressed in [1]. Central simple algebras having a Galois maximal subfield will be studied in Chapter 7 on crossed products.

At this stage, it is worth summarizing the various characterizations of central simple algebras we have seen.

**Theorem 5.31.** Let $K$ be a field and $\overline{K}$ a fixed algebraic closure of $K$. For any finite dimensional $K$-algebra $A$, the following properties are equivalent

1. $A$ is a central simple $K$-algebra;
2. $A \otimes_K \overline{K} \cong \overline{K} M_n(\overline{K})$;
3. There exists a field extension $L/K$ such that $A \otimes_K L \cong L M_n(L)$ for some $n \geq 1$.

In this case, $L/K$ may be chosen of finite degree over $K$, or finite Galois.

**Proof.** (1) $\Rightarrow$ (2) is Lemma 5.7, and (1) $\Rightarrow$ (3) is just a summary of the results seen before. Now (2) $\Rightarrow$ (1) and (3) $\Rightarrow$ (1) follow from Proposition 5.1(2). \qed

### 5.4 The reduced characteristic polynomial

If $K$ is a field and $M \in M_n(K)$, recall that the characteristic polynomial $\chi_M$ of $M$ is defined by

$$\chi_M = \text{det}(XI_n - M) \in K[X].$$

We would like to extend this notion to elements of arbitrary central simple algebras. A first natural idea would be to exploit (4.1), i.e. using the embedding of any central simple algebra into a matrix algebra. Doing so, if $A$ is a central simple $K$-algebra of degree $n$ and $a \in A$, let us define $P_a \in K[X]$ to be the characteristic polynomial of the $K$-algebra endomorphism

$$l_a : A \rightarrow A$$

$$z \mapsto az.$$

Let us compute $P_a$ in the split case when $A = M_n(K)$. Let $a = M \in M_n(K)$. Then it is not difficult to see that the matrix of $l_M$ in the canonical basis of $M_n(K)$ is given by

$$\begin{pmatrix}
M & & \\
& \ddots & \\
& & M
\end{pmatrix}.$$

Hence we get $P_M = \chi_M^a$. This definition is then not completely satisfactory since we do not recover the characteristic polynomial of a matrix. Instead of using this approach, we are going to exploit the existence of splitting fields. Let $A$ be a central simple $K$-algebra, $L$ a splitting field of $A$, and let

$$f : A \otimes_K L \xrightarrow{\sim} L M_n(L)$$

be an isomorphism of $L$-algebras.
Lemma 5.32. Keeping the notations above, for every \( a \in A \), the characteristic polynomial of \( f(a \otimes 1) \) does not depend on the choice of \( f \) or \( L \), and has coefficients in \( K \).

To prove the lemma above, we need Skolem-Noether’s theorem, which studies the automorphisms of a central simple \( K \)-algebra. Let us begin with a definition before stating the aforementioned theorem.

Definition 5.33. Let \( A \) be a central simple \( K \)-algebra. If \( a \in A^\times \) is an invertible element of \( A \), we denote by \( \text{Int}(a) \) the automorphism defined by
\[
\text{Int}(a) : A \rightarrow A \\
x \mapsto axa^{-1}.
\]
An automorphism of \( A \) of the form \( \text{Int}(a) \) is called an inner automorphism.

Theorem 5.34 (Skolem-Noether’s theorem). Let \( A \) be a central simple \( K \)-algebra and \( B \) a simple \( K \)-algebra. Let \( f_1, f_2 : B \rightarrow A \) be two \( K \)-algebra homomorphisms. Then there exists an inner automorphism \( \rho \) of \( A \) such that \( f_2 = \rho \circ f_1 \). In particular, every automorphism of \( A \) is inner.

Proof. See [1, Chapter III]. \( \square \)

We now introduce some notations that will be used in the following proof.

Notation 5.35. Let \( E/K \) and \( L/K \) be two field extensions. Let \( \phi : L \rightarrow E \) be a \( K \)-algebra homomorphism. Then, for \( P \in L[X] \), we denote by \( \phi \cdot P \) the polynomial of \( E[X] \) obtained by applying \( \phi \) to each coefficient of \( P \). Also, for \( M \in M_n(L) \), we denote by \( \phi(M) \) the matrix of \( M_n(E) \) obtained by applying \( \phi \) to each coefficient of \( M \).

One can easily prove that this defines a \( K \)-algebra homomorphism \( \tilde{\phi} : M_n(L) \rightarrow M_n(E) \) and that \( \chi_{\tilde{\phi}(M)} = \phi \cdot \chi_M \).

Now, we return to the proof of Lemma 5.32.

Proof. [Proof of Lemma 5.32] Let us first prove that the characteristic polynomial does not depend on the choice of \( f \). For that let \( a \in A \) and let
\[
f, g : A \otimes_K L \rightarrow L, M_n(L)
\]
be two \( L \)-algebra isomorphisms. We want to prove that \( \chi_{f(a \otimes 1)} = \chi_{g(a \otimes 1)} \). By Skolem-Noether’s theorem, we know that there exists \( \rho \in \text{Int}(M_n(L)) \) such that \( f = \rho \circ g \).

Say
\[
\rho : M_n(L) \rightarrow M_n(L) \\
M \mapsto MNM^{-1},
\]
for some invertible matrix \( N \in M_n(L) \). We then have that
\[
f(a \otimes 1) = Ng(a \otimes 1)N^{-1},
\]
from which we directly deduce that $\chi_{f(a \otimes 1)} = \chi_{g(a \otimes 1)}$.

From now on, for any central simple algebra over $K$ and any $a \in A$, if $L$ is a splitting field of $A$, we will let

$$\chi_a, L := \chi_{f(a \otimes 1)};$$

where $f : A \otimes_K L \to M_n(L)$ is an isomorphism of $L$-algebras.

The next step is to prove that the characteristic polynomial does not depend on the choice of $L$ and has coefficients in $K$. Let us first show that if $L$ is a splitting field of $A$, and if $\phi : L \to E$ is a $K$-algebra homomorphism, then $E$ splits $A$ and $\chi_a, E = \phi \cdot \chi_a, L$.

**First case**: if $\phi$ is an isomorphism of $K$-algebras.

Then consider $g := \phi \circ f \circ (\text{Id}_A \otimes \phi^{-1})$. One can check that the $K$-algebra isomorphism $g : A \otimes_K E \to M_n(E)$ is also $E$-linear so that $g$ becomes an isomorphism of $E$-algebras. So $E$ splits $A$. Noting that $g(a \otimes 1) = \phi(f(a \otimes 1))$, we get that

$$\chi_a, E = \chi_{g(a \otimes 1)} = \phi \cdot \chi_{f(a \otimes 1)} = \phi \cdot \chi_a, L.$$  

**Second case**: if $L \subseteq E$ and $\phi$ is the inclusion.

Consider the following $E$-algebra isomorphisms

$$A \otimes_K E \cong (A \otimes_K L) \otimes_L E \cong M_n(L) \otimes_L E \cong M_n(E).$$

Denote by $g : A \otimes_K E \simto E M_n(E)$ the resulting isomorphism sending $a \otimes 1$ to $f(a \otimes 1)$. Thus, $E$ splits $A$ and we have that

$$\chi_a, E = \det(XI_n - g(a \otimes 1)) = \det(XI_n - f(a \otimes 1)) = \chi_a, L.$$  

Back to the general case, we get that $\chi_{a, E} = \phi \cdot \chi_{a, L}$.

We will now prove that the polynomial in question has coefficients in the ground field $K$. Let $A$ be a central simple algebra over $K$. By Corollary 5.29, $A$ admits a Galois splitting field $L$. Then for every $\sigma \in \text{Gal}(L/K)$, by the previous result we get that

$$\chi_a, L = \sigma \cdot \chi_{a, L}.$$  

So each coefficient of the polynomial is fixed by the action of $\sigma$ and we deduce $\chi_{a, L} \in K[X]$.

Now, it remains to prove that the characteristic polynomial does not depend on the chosen splitting field. Let $L'$ be a splitting field of $A$, we are going to prove that $\chi_{a, L} = \chi_{a, L'}$. The desired result will then follow since $L'$ has been chosen arbitrarily. There exists a field $E$ and two $K$-algebra homomorphisms

$$\phi : L \to E \quad \text{and} \quad \phi' : L' \to E.$$  

For the details of this existence result, we refer the reader to [1]. By the previous results, we get that

$$\chi_{a, E} = \phi \cdot \chi_{a, L} = \phi' \cdot \chi_{a, L'}.$$  

Since $\chi_{a, L}$ has coefficients in $K$ and $\phi$ is $K$-linear, we get that $\chi_{a, L} = \phi' \cdot \chi_{a, L'}$. Therefore, by injectivity of $\phi'$ (as $\phi'$ is a nonzero field homomorphism) we have that $\chi_{a, L} = \chi_{a, L'}$. 

$\square$
Definition 5.36. Let $A$ be a central simple $K$-algebra of degree $n$, and let $a \in A$. The reduced characteristic polynomial of $a \in A$ is the polynomial $\text{Prd}_A(a)$ defined by

$$\text{Prd}_A(a) = \chi(f(a \otimes 1)) = \det(XI_n - f(a \otimes 1)),$$

where

$$f : A \otimes_K L \xrightarrow{\sim} L M_n(L)$$

is an isomorphism of $L$-algebras. By the previous lemma, $\text{Prd}_A(a) \in K[X]$ and does not depend on the choice of $L$ or $f$.

We now study briefly the properties of the reduced characteristic polynomial.

Lemma 5.37. Let $K$ be a field and let $A$ be a central simple $K$-algebra. Then we have the following properties

1. If $A = M_n(K)$, then $\text{Prd}_A(M) = \chi_M$ for all $M \in A$;
2. Let $L/K$ be an arbitrary field extension. Then we have

$$\text{Prd}_{A \otimes_K L}(a \otimes 1) = \text{Prd}_A(a)$$

for all $a \in A$;
3. If $\rho : A \xrightarrow{\sim} K A'$ is an isomorphism of central simple $K$-algebras, then we have

$$\text{Prd}_{A'}(\rho(a)) = \text{Prd}_A(a)$$

for all $a \in A$;
4. If $\deg(A) = n$, we have the equality

$$\chi_n = \text{Prd}_A(a)^n;$$
5. For all $a \in A$, we have $\text{Prd}_A(a)(a) = 0$.

Proof.

1. If $A = M_n(K)$,

$$f : A \otimes_K K \xrightarrow{\sim} K M_n(K)$$

is an isomorphism of $K$-algebras which makes $K$ a splitting field of $A$. Then

$$\text{Prd}_A(M) = \chi_{f(M \otimes 1)} = \chi_M,$$

as desired.

2. As a central simple algebra over $L$, $A \otimes_K L$ admits $\mathcal{L}$ as splitting field. We set

$$g : A \otimes_K \mathcal{L} \xrightarrow{\sim} \mathcal{L} (A \otimes_K L) \otimes \mathcal{L}.$$

We also have a canonical isomorphism

$$\text{Prd}_A(a) \in K[X].$$
satisfying $g(a \otimes 1) = a \otimes 1 \otimes 1$. So, the composite isomorphism

$$h := f \circ g : A \otimes_K \mathcal{L} \simto L M_n(\mathcal{L})$$

satisfies $h(a \otimes 1) = f(a \otimes 1 \otimes 1)$. We thus finally get that

$$\Prd_{A \otimes_K L}(a \otimes 1) = \chi_{f(a \otimes 1 \otimes 1)} = \chi_{h(a \otimes 1)} = \Prd_A(a).$$

(3) Let $L$ be a splitting field of $A$ and denote by $f$ the underlying isomorphism

$$f : A \otimes_K L \simto L M_n(L).$$

Now, denote by $g$ the following canonical isomorphism

$$g : A' \otimes_K L \simto L A \otimes_K L$$

$$a \otimes l \mapsto \rho^{-1}(a) \otimes l.$$

Then, letting $h$ to be the composite $L$-algebra isomorphism

$$h = f \circ g \simto L M_n(L)$$

$$a \otimes l \mapsto f(\rho^{-1}(a) \otimes l),$$

we notice that $h(\rho(a) \otimes 1) = f(a \otimes 1)$. Thus

$$\Prd_{A'}(\rho(a)) = \chi_{h(\rho(a) \otimes 1)} = \chi_{f(a \otimes 1)} = \Prd_A(a).$$

(4) Let us first consider the case where $A = M_n(K)$. Then as a direct consequence of the discussion we had in the beginning of the section, we have

$$\chi_{l_n} = \Prd_A(a)^n.$$  

Now back to the general case where $A$ is an arbitrary central simple algebra over $K$. Let $L$ be a splitting field of $A$ and set

$$f : A \otimes_K L \simto L M_n(L).$$

By the previous discussion, we have that

$$\chi_{f(a \otimes 1)} = \Prd_A(a)^n.$$  

But the isomorphism $f$ induces an isomorphism

$$\tilde{f} : \text{End}_L(A \otimes_K L) \simto \text{End}_L(M_n(L))$$

$$u \mapsto f \circ u \circ f^{-1}.$$  

It is easy to check that we have

$$\tilde{f}(l_z) = l_{f(z)},$$
for all $z \in A \otimes_K L$, so we get
\[ \chi_{f(a \otimes 1)} = \chi_{f(l_n \otimes 1)} = \chi_{l_n \otimes 1} \]
using the previous point. Now, the canonical isomorphism
\[ \eta : \text{End}_K(A) \otimes_K L \simto \text{End}_L(A \otimes_K L) \]
\[ f \otimes l' \mapsto A \otimes_K L \rightarrow A \otimes_K L \]
\[ a \otimes l \mapsto f(a) \otimes l' \]
sends $l_n \otimes 1$ to $l_{f(a \otimes 1)}$, so we finally get
\[ \chi_{f(a \otimes 1)} = \chi_{l_n \otimes 1} = \chi_{l_n}. \]

(5) Say the degree of $A$ over $K$ is $n$. As usual, let $L$ be a splitting field of $A$ and denote by $f$ the underlying isomorphism
\[ f : A \otimes_K L \simto L M_n(L). \]
By definition, $\text{Prd}(a) = \chi_{f(a \otimes 1)}$. By Cayley-Hamilton theorem we know that
\[ \chi_{f(a \otimes 1)}(f(a \otimes 1)) = 0. \]
Say
\[ \chi_{f(a \otimes 1)} = u_0 + u_1 X + \cdots + u_{n-1} X^{n-1} + X^n \in K[X], \]
Then we naturally get that
\[ 0 = \chi_{f(a \otimes 1)}(f(a \otimes 1)) = u_0 + u_1 f(a \otimes 1) + \cdots + u_{n-1} f(a \otimes 1)^{n-1} + f(a \otimes 1)^n \]
\[ = f((u_0 + u_1 a + \cdots + u_{n-1} a^{n-1} + a^n) \otimes 1). \]
The result follows from the injectivity of $f$. \hfill \Box

Let us now study more closely the reduced characteristic polynomial of a division algebra. Recall that if $D$ is a division $K$-algebra and $d \in D$, the $K$-subalgebra generated by $d$ is a subfield $K(d)$ of $D$ and $[K(d) : K] \cdot \deg(D)$ by Lemma 5.18. Hence the following statement makes sense.

**Lemma 5.38.** Let $D$ be a central division $K$-algebra of degree $n$. For all $d \in D$, we have
\[ \text{Prd}_D(d) = \mu_d^s, \]
where $\mu_d$ is the minimal polynomial of $d$ over $K$ and $s = \frac{\deg(D)}{[K(d) : K]}$.

**Proof.** Set $r := [K(d) : K]$ and write
\[ \mu_d = \mu_0 + \mu_1 X + \cdots + \mu_{r-1} X^{r-1} + X^r \in K[X]. \]
By the previous lemma, we know that \( \text{Pr}_{D}(d)^n = \mu_d^n \). We thus only prove that \( \chi_d = \mu_d^n \). Set \( m := n^2/r \). Let \( e_1, \ldots, e_m \) be a basis of \( D \) over \( K(d) \). Then \( e_1, e_1d, \ldots, e_1d^{r-1}, \ldots, e_md, \ldots, e_md^{r-1} \).

The representative matrix of \( l_d \) over \( K \) is then
\[
M := \begin{pmatrix}
C_{\mu_d} & \cdots \\
& \ddots \\
& & C_{\mu_d}
\end{pmatrix},
\]
while
\[
C_{\mu_d} = \begin{pmatrix}
0 & \cdots & 0 & -\mu_0 \\
1 & \cdots & 0 & -\mu_1 \\
0 & \cdots & 1 & -\mu_2 \\
& \ddots & \ddots & \ddots \\
0 & \cdots & 0 & 1 -\mu_{r-1}
\end{pmatrix}.
\]

Then, as \( \chi_M = \chi_{C_{\mu_d}}^n \) and \( \chi_{C_{\mu_d}} = \mu_d \), we get that
\[
\chi_d = \chi_M = \mu_d^n,
\]
as desired. \( \square \)

**Corollary 5.39.** Let \( D \) be a central division \( K \)-algebra. Then two elements of \( D \) are conjugate if and only if they have the same reduced characteristic polynomial.

**Proof.** Suppose first that \( d' = xd^{-1} \), for some \( x \in D^x \). Let \( L \) be a splitting field of \( D \) and denote by \( f \) the underlying isomorphism
\[
f := D \otimes_K L \xrightarrow{\sim} L M_n(L).
\]

We then have that
\[
f(d' \otimes 1) = f((xd^{-1}) \otimes 1) = f((x \otimes 1)(d \otimes 1)(x^{-1} \otimes 1)) = f(x \otimes 1)f(d \otimes 1)f(x \otimes 1)^{-1}.
\]
So we have an equality of the characteristic polynomials
\[
\text{Pr}_{D}(d) = \chi_{f(d \otimes 1)} = \chi_{f(d') \otimes 1} = \text{Pr}_{D}(d').
\]
Conversely, let us suppose that \( \text{Pr}_{D}(d) = \text{Pr}_{D}(d') \). Then by the previous result, we get that \( \mu_d = \mu_{d'} \). Then, there exists a unique homomorphism of \( K \)-algebras such that \( \rho(d) = d' \). Also consider the \( K \)-algebra homomorphism given by the inclusion
\[
i : K(d) \hookrightarrow D.
\]
Then by Skolem-Noether’s theorem, there exists \( x \in D^x \) satisfying \( \rho = \text{Int}(x) \circ i \), where we recall that
\[
\text{Int}(x) : D \rightarrow D \\
z \mapsto xzx^{-1}.
\]
In particular, we get that \( d' = xd^{-1} \), and we are done. \( \square \)
Remark 5.40. The previous lemma and its corollary might not be true for non-division central simple $K$-algebras, as the case of of a matrix algebra already suggests.

Thanks to the reduced characteristic polynomial, we are now able to generalize the notions of trace and determinant to central simple algebras.

**Definition 5.41.** Let $A$ be a central simple $K$-algebra, and let $a \in A$. Write

$$\Prd_A(a) = X^n - s_1X^{n-1} + s_2X^{n-2} + \ldots + (-1)^ns_n.$$  

The coefficients $s_1$ and $s_n$ are called respectively the reduced trace and the reduced norm of $a$. They are denoted respectively by $\Trd_A(a)$ and $\Nrd_A(a)$.

In other words, $\Trd_A(a) := \Tr(f(a \otimes 1))$ and $\Nrd_A(a) := \Nr(f(a \otimes 1))$, where

$$f : A \otimes_K L \xrightarrow{\sim} L M_n(L),$$

and $L$ is a splitting field of $A$.

**Lemma 5.42.** Let $A$ be a central simple $K$-algebra of degree $n$. Then the following properties hold

1. For all $n \geq 1$, $\Trd_{M_n(K)} = \Tr$ and $\Nrd_{M_n(K)} = \det$;
2. The map $\Trd_A : A \rightarrow K$

is a nonzero linear form;

3. For all $a, a' \in A$ and all $\lambda \in K$, we have

$$\Nrd_A(aa') = \Nrd_A(a)\Nrd_A(a')$$

and

$$\Nrd_A(\lambda) = \lambda^n.$$  

Moreover,

$$a \in A^\times \implies \Nrd_A(a) \neq 0;$$

4. Let $L/K$ be a field extension. For all $a \in A$, we have

$$\Trd_{A \otimes_K L}(a \otimes 1) = \Trd_A(a)$$

and

$$\Nrd_{A \otimes_K L}(a \otimes 1) = \Nrd_A(a);$$

5. Let $\rho : A \xrightarrow{\sim} A'$ be an isomorphism of central simple $K$-algebras. For all $a \in A$,

we have

$$\Trd_{A'}(\rho(a)) = \Trd_A(a)$$

and

$$\Nrd_{A'}(\rho(a)) = \Nrd_A(a).$$
5.4 The reduced characteristic polynomial 61

Proof. 

(1) As for all $M \in M_n(K)$, $\text{Prd}_{M_n(K)}(M) = \chi_M$, the result follows.

(2) As the reduced characteristic polynomial has coefficients in $K$, $\text{Trd}_A$ has image in $K$. Then, using the linearity of the trace of matrices we get that

$$\text{Trd}_A(\lambda a + b) = \text{Tr}(f((\lambda a + b) \otimes 1)) = \text{Tr}(\lambda f(a \otimes 1) + f(b \otimes 1))$$

$$= \lambda \text{Tr}(f(a \otimes 1)) + \text{Tr}(f(b \otimes 1)),$$

for all $\lambda \in K, a, b \in A$. Let us now prove by contradiction that $\text{Trd}_A$ is nonzero. Suppose the contrary. Then, as the elementary tensors $a \otimes 1, a \in A$ span $A \otimes_K L \cong_L M_n(L)$ as an $L$-vector space, using the definition which says

$$\text{Trd}_A(a) = \text{Tr}(f(a \otimes 1)),$$

we get that the trace on matrices is identically zero, which is not.

(3) Note that

$$\text{Nrd}(aa') = \text{Nrd}(f(aa') \otimes 1) = \text{Nrd}(f(a \otimes 1)f(a' \otimes 1)) = \text{Nrd}(f(a \otimes 1))\text{Nrd}(f(a' \otimes 1))$$

$$= \text{Nrd}(a)\text{Nrd}(a').$$

For $\lambda \in K$, we have that

$$\text{Nrd}(\lambda) = \text{Nrd}(f(\lambda \otimes 1)) = \text{Nrd}(\lambda f(1 \otimes 1)) = \text{Nrd}(\lambda I_n) = \lambda^n.$$

Now, if $a \in A^\times$, we get that

$$\text{Nrd}(a)\text{Nrd}(a') = \text{Nrd}(1) = 1.$$

Since $K$ is in particular an integral domain, it follows that $\text{Nrd}(a) \neq 0$.

(4) This follows from Lemma 5.37(2).

(5) This follows from Lemma 5.37(3).

\[\square\]

Remark 5.43. Let $A$ be a central simple $K$-algebra of degree $n$. Assume that $A$ has a maximal subfield $L$. In this case, there exists an $L$-algebra isomorphism

$$f : A \otimes_K L \simto_L \text{End}_L(A)$$

satisfying

$$f(a \otimes 1) = l_a$$

for all $a \in A$,

where $l_a \in \text{End}_L(A)$ is the endomorphism of left multiplication by $a$ in the right $L$-vector space $A$. After the choice of an $L$-basis of $A$, we get an $L$-algebra isomorphism

$$f' : A \otimes_K L \simto_L M_n(L)$$
satisfying

\[ f'(a \otimes 1) = M_a \text{ for all } a \in A, \]

where \( M_a \) is the representative matrix of \( l_a \) in the fixed \( L \)-basis of \( A \). By definition of the reduced characteristic polynomial, we then have

\[ \text{Prd}_A(a) = \chi_{M_a} \text{ for all } a \in A. \]

In particular, we get

\[ \text{Nrd}_A(a) = \det(M_a) \text{ and } \text{Trd}_A(a) = \text{Tr}(M_a) \text{ for all } a \in A. \] (5.1)
Codes from cyclic division algebras

Armed with the concepts of central simple algebra and splitting fields provided by the two previous chapters, we derive here a new type of codes constructed from cyclic division algebras.

6.1 Definitions and properties

Definition 6.1. Assume that $E/F$ is a cyclic field extension of degree $n$ with Galois group $\text{Gal}(E/F) = \langle \sigma \rangle$. We denote by $A = (E/F, \sigma, \gamma)$ the $F$-algebra defined by

$$A = E \oplus uE \oplus \ldots \oplus u^{n-1}E$$

as a right vector space over $E$, where $u \in A$ is an auxiliary generating element subject to the relations

$$xu = u\sigma(x) \text{ for all } x \in E \text{ and } u^n = \gamma \in F^\times.$$

We call the $F$-algebra $A$ a cyclic algebra.

The next proposition makes the link with the two previous algebraic chapters. The proof of this result is a particular case of a proposition on crossed products that we prove in Chapter 7.

Proposition 6.2. A cyclic algebra $A = (E/F, \sigma, \gamma)$ is a central simple algebra over $F$ and has degree $n$.

Proof. This follows from Theorem 7.5, where it will be proved that every crossed product algebra is a central simple algebra. Note that a proof of the particular case of the quaternion algebras is given in [1, Proposition I.2.5].

Remark 6.3. One can notice that $A$ admits $E$ as a maximal subfield. Therefore, by Proposition 5.20, $E$ is a splitting field of $A$, and we have an embedding

$$A \hookrightarrow A \otimes_F E \to \text{End}_E(A) \to M_n(E)$$

$$a \mapsto a \otimes 1 \mapsto \left\{ l_a : A \to A \left\{ \begin{array}{ccc} l_a & \to & A \\ z & \mapsto & az \end{array} \right\} \to M_n,\right.$$ 

where $M_n$ is the matrix representation of the endomorphism $l_a \in \text{End}(A)$ which consists of the multiplication by $a$ from the left. Putting everything together, we
consider the composite injection denoted by the relative canonical embedding which gives a matrix representation of every element \( a \in A \),

\[
\psi : A \longrightarrow M_n(E)
\]

\[
a = x_0 + u x_1 + \ldots + u^{n-1} x_{n-1} \longmapsto \begin{pmatrix}
  x_0 & \gamma \sigma(x_{n-1}) & \gamma \sigma^2(x_{n-2}) & \ldots & \gamma \sigma^{n-1}(x_1) \\
  x_1 & \sigma(x_0) & \gamma \sigma^2(x_{n-1}) & \ldots & \gamma \sigma^{n-1}(x_2) \\
  x_2 & \sigma(x_1) & \sigma^2(x_0) & \ldots & \gamma \sigma^{n-1}(x_3) \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \sigma^{n-1}(x_0)
\end{pmatrix}
\]

This gives an \( F \)-algebra homomorphism \( \psi : A \longrightarrow M_n(E) \). Looking back at \( (5.1) \), a direct consequence is that for all \( a \in A \), we have

\[
\det(\psi(a)) = \det(M_a) = \text{Nrd}_A(a).
\]

One can also note that for every \( a \in E \), \( \text{Nrd}_A(a) = \text{Nrd}_{E/F}(a) \), and that \( \psi(a) \) is a diagonal matrix in \( M_n(\mathbb{C}) \). Note that throughout this chapter, the embedding \( \psi \) is obtained with respect to the basis \( 1, u, \ldots, u^{n-1} \).

**Definition 6.4.** Let us consider a cyclic algebra \( A = (E/F, \sigma, \gamma) \), with \( \gamma \in \mathbb{F}^\times \). We then see that

\[
\Gamma_n := \mathcal{O}_E \oplus u \mathcal{O}_E \oplus u^2 \mathcal{O}_E \oplus \ldots \oplus u^{n-1} \mathcal{O}_E
\]

is a subgroup of \( A \). In the case where \( \gamma \in \mathcal{O}_F^\times \), \( \Gamma_n \) becomes a subring of \( A \) and is called the natural order of \( A \).

In the case of cyclic algebras, we also have a simple criterion to decide whenever it is a division ring.

**Proposition 6.5.** Let \( E/F \) be a cyclic field extension of degree \( n \) with Galois group \( \text{Gal}(E/F) = \langle \sigma \rangle \). If \( \gamma, \gamma^2, \ldots, \gamma^{n-1} \in \mathbb{F}^\times \) are not norms of any element of \( E \), then the cyclic algebra \( A = (E/F, \sigma, \gamma) \) is a division algebra.

*Proof.* See [11, p. 279]. Note that the particular case of the Hamilton quaternion algebra

\[
A = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1),
\]

where \( \sigma \) is given by the complex conjugation, is treated in [1, Proposition II.1.4]. □

**Remark 6.6.** Note that whenever we have a cyclic division algebra, the degree and the index of the algebra are identical. See Remark 5.10.

### 6.2 Geometric structure

From now on, we concentrate on the case where the center of the algebra \( A \) is \( \mathbb{Q}(i) \). In the following, we will see that this choice is very suitable from the coding theoretic point of view. The following lemma is a generalization of Lemma 3.14 for the case of cyclic division algebras.
Lemma 6.7. Let $A = (E/Q(i), \sigma, \gamma)$ be a cyclic division algebra of degree $n$ with $\gamma \in \mathbb{Z}[i]\{0\}$. Consider the natural order of $A$

$$
\Gamma_n = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E.
$$

Then for every $a \in \Gamma_n$, 

$$\text{Nrd}_A(a) \in \mathbb{Z}[i].$$

Moreover, if $a \neq 0$, then $\text{Nrd}_A(a) \neq 0$.

Proof. As $\sigma(\mathcal{O}_E) \subseteq \mathcal{O}_E$ and $\gamma \in \mathbb{Z}[i]$, using the fact that $\text{Nrd}_A(a) = \det(\psi(a))$, since $\psi(a)$ is a matrix having elements in the ring $\mathcal{O}_E$, we get that $\text{Nrd}_A(a) \in \mathcal{O}_E$. On the other hand, by Lemma 5.32, $\text{Nrd}_A(a) \in \mathbb{Q}(i)$. Therefore using Lemma 3.8, we get that $\text{Nrd}_A(a) \in \mathcal{O}_E \cap \mathbb{Q}(i) = \mathbb{Z}[i]$. The additional part follows from the property of the reduced norm described in Lemma 5.42(3).

We now prove three lemmas that will reveal the geometric structure of the codes. As previously, let us suppose that we have a cyclic algebra $A = (E/Q(i), \sigma, \gamma)$, $\Gamma_n = E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$, and the embedding $\psi$.

Lemma 6.8. For all $0 \leq s \leq n-1$, there exists a diagonal matrix $\Gamma_s \in M_n(\mathbb{C})$ and a permutation matrix $P_s \in M_n(\mathbb{C})$ such that 

$$\psi(u^s) = \Gamma_sP_s.$$

Proof. The case where $s = 0$ is obvious, so let us suppose that $s \geq 1$. This is just a matter of computation but to give a hint: the first $s$ diagonal elements of $\Gamma_s$ are $\gamma$’s and the remaining are one’s and the permutation matrix $P_s$ is just $\psi(u^s)$ where all the $\gamma$’s are replaced by one’s.

Lemma 6.9. Let $1 \leq t \leq n-1$. Then 

$$\psi(u^t)^* = \psi(\overline{\gamma}u^{n-t}).$$

Proof. This is an easy computation.

Lemma 6.10. For every diagonal matrix $Y \in M_n(\mathbb{C})$,

$$\text{Tr}(Y\psi(u^s)) = 0,$$

for all $1 \leq s \leq n-1$.

Proof. By the definition of $\psi$, we have that 

$$\text{Tr}(\psi(u^s)) = 0, \text{ for all } 1 \leq s \leq n-1.$$ 

Hence the result.
Let us recall that in $M_n(\mathbb{C})$ we work by convention with the Frobenius norm and that the inner product used is the one induced by the $\alpha$ mapping (2.3).

**Proposition 6.11.** Let $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ be a cyclic division algebra of degree $n$. Let $a \in E$, $a \neq 0$. Then the lattices $\psi(u^s a\mathcal{O}_E)$ and $\psi(u^t a\mathcal{O}_E)$ are orthogonal for every $0 \leq s \neq t \leq n - 1$.

**Proof.** Let $x, y \in \mathcal{O}_E$, and $0 \leq s \neq t \leq n - 1$. We have

$$\langle \psi(u^s ax), \psi(u^t ay) \rangle = \text{Re} \text{Tr}(\psi(u^s) \psi(a) \psi(x) \psi(y)^* \psi(a)^* \psi(u^t)^*).$$

As for all $A, B \in M_n(\mathbb{C})$, $\text{Tr}(AB) = \text{Tr}(BA)$, using Lemma 6.9 we get that

$$\langle \psi(u^s ax), \psi(u^t ay) \rangle = \text{Re} \text{Tr}(X \psi(u^s)^* \psi(u^s)) = \text{Re} \text{Tr}(X \psi(\gamma u^s) \psi(u^s) \psi(u^{s-t})).$$

Then, using Lemma 6.10 it follows that

$$\langle \psi(u^s ax), \psi(u^t ay) \rangle = \text{Re} \text{Tr}(Y \psi(u^{s-t})) = 0.$$

We can now conclude that the lattices $\psi(u^s \mathcal{O}_E)$ and $\psi(u^t \mathcal{O}_E)$ are orthogonal for all $s \neq t$. \hfill \Box

### 6.3 Construction of the codes and properties

#### 6.3.1 Volume and normalized minimum determinant of the codes

**Proposition 6.12.** Let $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ be a cyclic division algebra of degree $n$, with $\gamma \in \mathbb{Q}(i) \setminus \{0\}$. Let $a \in E$, $a \neq 0$. Then

$$\psi(I_n a)$$

is a $2n^2$-dimensional lattice code in $M_n(\mathbb{C})$.

**Proof.** By construction, $I_n a = a\mathcal{O}_E \oplus u a\mathcal{O}_E \oplus u^2 a\mathcal{O}_E \oplus \cdots \oplus u^{n-1} a\mathcal{O}_E$, so that

$$\psi(I_n a) = \psi(a\mathcal{O}_E) \oplus \psi(u) \psi(a\mathcal{O}_E) \oplus \psi(u^2) \psi(a\mathcal{O}_E) \oplus \cdots \oplus \psi(u^{n-1}) \psi(a\mathcal{O}_E).$$

From Proposition 3.15, we know that $\psi(a\mathcal{O}_E)$ is a lattice of dimension $2n$. So, once we will prove that, having fixed a $\mathbb{Z}$-basis of $a\mathcal{O}_E$, say $\{w_1, \ldots, w_n\} \subseteq E$, the set

$$\{\psi(w_1), \psi(u w_1), \ldots, \psi(u^{n-1} w_1), \ldots, \psi(w_n), \ldots, \psi(u^{n-1} w^n)\}$$

is linearly independent over $\mathbb{R}$, we will get that $\psi(I_n a)$ is indeed a lattice of dimension $2n^2$. To prove this, we use the same idea as in the proof of Proposition 3.15, namely we
show that the subgroup is discrete. So, let \( x, y \in \Gamma_\alpha, x \neq y \). For a certain \( z \in \Gamma_\alpha \setminus \{0\} \), using Lemma 2.28 we then have that
\[
||\psi(x) - \psi(y)||_F = ||\psi(a)\psi(z)||_F \geq \sqrt{n} |\det(\psi(a)\psi(z))|^{1/n}
\]
\[
= \sqrt{n} |\det(\psi(a))|^{1/n} |\det(\psi(z))|^{1/n}
\]
\[
= \sqrt{n} \det(\psi(a))^{1/n} |\det(\psi(v(\gamma)z))|^{1/n}
\]
\[
\geq \sqrt{n} \det(\psi(a))^{1/n} |v(\gamma)|,
\]
which is strictly bigger than zero. Indeed for the last inequality we used Lemma 6.7 as \( \Nrd_{\mathcal{A}}(v(\gamma)z) = \det(\psi(v(\gamma)z)) \), and \( \psi(v(\gamma)z) \) is a matrix of elements in \( \mathcal{O}_E \). As a discrete subgroup of \( M_n(\mathbb{C}) \), \( \psi(\Gamma_{\alpha}a) \) is indeed a \( 2n^2 \)-dimensional lattice in \( M_n(\mathbb{C}) \).

Let us now measure the normalized minimum determinant of the introduced codes.

**Proposition 6.13.** Let \( \mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma) \) be a cyclic division algebra of degree \( n \), with \( \gamma \in \mathbb{Z}[i], |\gamma| = 1 \). Let \( a \in E, a \neq 0 \). Then
\[
\operatorname{vol}(\psi(\Gamma_{\alpha}a)) = \operatorname{vol}(\psi(a\mathcal{O}_E))^n.
\]
Moreover,
\[
\delta(\psi(\Gamma_{\alpha}a)) = 2^{n/2} |d(E/\mathbb{Q})|^{-1/4}.
\]
In particular, \( \psi(\Gamma_{\alpha}a) \) has NVD property.

**Proof.** Let us first prove that \( \operatorname{vol}(\psi(\Gamma_{\alpha}a)) = \operatorname{vol}(\psi(a\mathcal{O}_E))^n \). According to the previous proposition, we have that the lattices \( \psi(a'\mathcal{O}_E) \) and \( \psi(a'\mathcal{O}_E) \) are orthogonal for \( s \neq t \). By Lemma 2.23 and Proposition 2.39 we have that
\[
\operatorname{vol}(\psi(\Gamma_{\alpha}a)) = \operatorname{vol}(\psi(a\mathcal{O}_E) \oplus \psi(ua\mathcal{O}_E) \oplus \cdots \oplus \psi(u^{n-1}a\mathcal{O}_E))
\]
\[
= \operatorname{vol}(\psi(a\mathcal{O}_E)) \operatorname{vol}(\psi(u)\mathcal{O}_E) \cdots \operatorname{vol}(\psi(u^{n-1})\mathcal{O}_E)
\]
\[
= \operatorname{vol}(\psi(a\mathcal{O}_E)) |\det(\psi(u))|^2 \operatorname{vol}(\psi(u\mathcal{O}_E)) \cdots |\det(\psi(u^{n-1}))|^2 \operatorname{vol}(\psi(u\mathcal{O}_E))
\]
\[
= \operatorname{vol}(\psi(a\mathcal{O}_E))^n.
\]
Now, concerning the normalized minimum determinant, making use of Theorem 2.43, we immediately get that
\[
\delta(\psi(\Gamma_{\alpha}a)) = \delta(\psi(\Gamma_{\alpha})).
\]
Now, let us compute \( \operatorname{det}_{\min}(\Gamma_{\alpha}) \). We have that
\[
\operatorname{det}(\psi(\Gamma_{\alpha})) = \inf_{x \in \Gamma_{\alpha}, x \neq 0} \{|\det(\psi(x))| \}
\]
\[
= \inf_{x \in \Gamma_{\alpha}, x \neq 0} \{|\Nrd_{\mathcal{A}}(x)| \}
\]
\[
\geq \inf_{x \in \mathbb{Z}[i], x \neq 0} |z| = 1,
\]
where Lemma 6.7 has been used for the last step. On the other hand,
\[
\operatorname{det}(\psi(\Gamma_{\alpha})) = \inf_{x \in \Gamma_{\alpha}, x \neq 0} \{|\Nrd_{\mathcal{A}}(x)| \} \leq \operatorname{Nrd}_{\mathcal{A}}(1, \mathcal{A}) = 1,
\]
so that finally \( \operatorname{det}_{\min}(\psi(\Gamma_{\alpha})) = 1 \). Finally, using Lemmas 2.25 and 3.18, we have that
\[
\delta(\psi(\Gamma_{\alpha}a)) = \frac{\operatorname{det}_{\min}(\psi(\Gamma_{\alpha}))}{\sqrt{\operatorname{vol}(\psi(a\mathcal{O}_E))}} = 2^{n/2} |d(E/\mathbb{Q})|^{-1/4}.
\]
Remark 6.14. Looking back at Proposition 3.19, we realize that whenever \( \gamma \in \mathbb{Z}[i] \) and \( |\gamma| = 1 \), \( \delta(\psi(a\mathcal{O}_E)) = \delta(\psi(I_n a)) \).

The following is a generalization of Proposition 6.13, in the sense that we now consider \( \gamma \in \mathbb{Q}(i) \). Note that in that case, the natural order \( I_n \) is not a subring of \( \mathcal{A} \) anymore but just a subgroup.

**Proposition 6.15.** Let \( \mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma) \) be a cyclic division algebra of degree \( n \), with \( \gamma \in \mathbb{Q}(i) \). Let \( a \in E \), \( a \neq 0 \). Then

\[
\text{vol}(\psi(I_n a)) = \text{vol}(\psi(a\mathcal{O}_E))^n |\gamma|^{n(n-1)}
\]

Moreover,

\[
\frac{1}{|v(\gamma)|^n \text{vol}( \psi(I_n) )} \leq \delta(\psi(I_n a)) \leq \frac{\text{Nsv}(2n)^n}{n^{n/2}},
\]

where, \( v(\gamma) = v(\frac{\gamma}{n} + \frac{1}{2} i) = bd \).

In particular, \( \psi(I_n a) \) has NVD property.

**Proof.** First denote by \( L \) the \( 2n^2 \)-dimensional lattice \( \psi(I_n a) \), and by \( L_i \) the \( 2n \)-dimensional lattice \( \psi(u^i a\mathcal{O}_E) \), for all \( i = 0, \ldots, n - 1 \). We then have that

\[
L = L_0 \oplus \cdots \oplus L_{n-1}.
\]

Proposition 6.11 implies that \( L \) is a direct sum of orthogonal lattices. Then, using Lemma 2.23 we get

\[
\text{vol}(L) = \prod_{i=0}^{n-1} \text{vol}(\psi(u^i a\mathcal{O}_E)).
\]

Now, by Proposition 2.39 and Lemma 6.8, we have

\[
\text{vol}(L) = \prod_{i=0}^{n-1} (\det(\psi(u^i)))^2 \text{vol}(\psi(a\mathcal{O}_E)) = \text{vol}(\psi(a\mathcal{O}_E))^n \prod_{i=0}^{n-1} |\gamma|^2i = \text{vol}(\psi(a\mathcal{O}_E))^n |\gamma|^{n(n-1)}.
\]

Let us now prove the lower bound on the normalized minimum determinant. We have that

\[
\det_{\text{min}}(\psi(I_n)) = \inf \{ |\det(\psi(x))| : x \in I_n, x \neq 0 \}
\]

\[
= \frac{1}{|v(\gamma)|^n} \inf \{ |\det(v(\gamma)\psi(x))| : x \in I_n, x \neq 0 \}
\]

\[
= \frac{1}{|v(\gamma)|^n} \inf \{ |\det(\psi(v(\gamma)x))| : x \in I_n, x \neq 0 \}.
\]

Using the same argument as in the proof of Proposition 6.13, the last infimum is greater or equal to 1. By Proposition 2.36, we therefore get that
\[
\delta(\psi(G_n)) = \delta(\psi(G_n)) = \frac{\det_{\text{min}}(\psi(G_n))}{\sqrt{\text{vol}(\psi(G_n))}} \geq \frac{1}{|\psi(\gamma)|^{n} \sqrt{\text{vol}(\psi(G_n))}}.
\]

Now, consider that \(L\) has unit-size fundamental parallelotope, so that

\[
\text{vol}(L) = \text{vol}(L_0) \cdots \text{vol}(L_{n-1}) = 1.
\]

Then, there exists at least one \(i\) such that \(\text{vol}(L_i) \leq 1\), implying that \(sv(L_i) \leq Nsv(L_i)\).
Then, as \(sv(L) \leq sv(L_i)\), we get that

\[
Nsv(L) = sv(L) \leq sv(L_i) \leq Nsv(L_i) \leq Nsv(2n).
\]

Finally, using Proposition 2.29, we get the desired upper bound, namely

\[
\delta(L) \leq \frac{Nsv(L)^n}{n^{n/2}} \leq \frac{Nsv(2n)^n}{n^{n/2}}.
\]

This concludes the proof.

\(\square\)

**Remark 6.16.** One can notice that the bound of Proposition 2.29 has been sharpened.

**Example 6.17.** We consider the cyclic division algebra \(\mathcal{A} = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1)\). The lattice code \(\psi(G_n)\) is referred to as the Alamouti code. We want to calculate \(\delta(\psi(G_n))\).

Here we have to be very careful as the center of \(\mathcal{A}\) is \(\mathbb{Q}\), for which case we have not proved so many results. However, as we will demonstrate, it turns out that what we have proved works also in this particular case. Let \(E = \mathbb{Q}(i)\), we then have \(\mathcal{O}_E = \mathbb{Z}[i]\), \(\mathcal{A} = E \oplus uE\), with \(\gamma = -1\) and \(u^2 = \gamma\), \(eu = u\sigma(e), \forall e \in E\). We also have, by construction, \(G_n = \mathcal{O}_E \oplus u\mathcal{O}_E\), and

\[
\psi : A \longrightarrow M_2(E) \\
x_0 + ux_1 \longmapsto \begin{pmatrix} x_0 \gamma \sigma(x_1) \\ x_1 \sigma(x_0) \end{pmatrix},
\]

so that

\[
\psi(G_n) = \mathbb{Z}_2 \oplus \mathbb{Z} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} : a, b \in \mathbb{Z} \right\}.
\]

By definition, \(\delta(\psi(G_n)) = \frac{\det_{\text{min}}(\psi(G_n))}{\sqrt{\text{vol}(\psi(G_n))}}\). The reader can check that the volume of the fundamental parallelotope is given by

\[
\text{vol}(\psi(G_n)) = \text{vol}(\psi(O_E))^2 = \det(\psi(O_E)) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 4.
\]

The minimum determinant being 1, we finally get \(\delta(\psi(G_n)) = 1/2\).

### 6.3.2 Perfect codes

Let us first define what a *perfect code* is. We first recall the following definition.
We therefore have that

Then as we already pointed out in Remark 3.16, it is beneficial if the code also has some extra structure.

**Definition 6.19.** If a lattice code $L \subseteq M_n(\mathbb{C})$ is also a free $\mathbb{Z}[i]$-module, i.e.

$$L = \mathbb{Z}[i]M_1 \oplus \cdots \oplus \mathbb{Z}[i]M_l,$$

with $M_1, iM_1, \ldots, M_l, iM_l$ linearly independent over $\mathbb{R}$, we call it a lattice code with $\mathbb{Z}[i]$-module structure.

**Definition 6.20.** Let us now suppose that we have a lattice code $L \subseteq M_n(\mathbb{C})$ with $\mathbb{Z}[i]$-module structure

$$L = \mathbb{Z}[i]M_1 \oplus \cdots \oplus \mathbb{Z}[i]M_{n^2},$$

and where $\{M_1, iM_1, \ldots, M_{n^2}, iM_{n^2}\}$ forms an orthonormal set. If $\delta(L) \neq 0$, we call $L$ a perfect code.

**Proposition 6.21.** Let $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ be a cyclic division algebra of degree $n$, with $\gamma \in \mathbb{Z}[i]$, $|\gamma| = 1$. Let us suppose that $\psi(a\mathcal{O}_E)$ is an orthonormal $\mathbb{Z}[i]$-lattice, with $a \in E, a \neq 0$. Then

$$\psi(I_n a)$$

is a perfect code.

**Proof.** The reader can easily verify that $\psi(I_n a)$ has a $\mathbb{Z}[i]$-module structure. On the other hand, as by definition $I_n = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$, we get that

$$\psi(I_n a) = \psi(a\mathcal{O}_E) \oplus \psi(u a\mathcal{O}_E) \oplus \cdots \oplus \psi(u^{n-1} a\mathcal{O}_E).$$

By Proposition 6.11, the components of $\psi(I_n a)$ in the expression above are orthogonal. Then, for $\psi(I_n a)$ to be an orthogonal lattice, it remains to prove that $\psi(u a\mathcal{O}_E)$ is an orthogonal lattice. Indeed, since for all $A, B \in M_n(\mathbb{C})$, $\text{Tr}(AB) = \text{Tr}(BA)$, we have that

$$\langle \psi(u^a x), \psi(u^a y) \rangle = \text{Re} \text{Tr}(\psi(u^a) \psi(x) \psi(y) \psi(u^a)^*) = \text{Re} \text{Tr}(\psi(y) \psi(u^a)^*) \psi(u^a) \psi(x)).$$

Then, as Lemma 6.8 implies that $\psi(u^a)$ is a unitary matrix it follows that

$$\langle \psi(u^a x), \psi(u^a y) \rangle = \text{Re} \text{Tr}(\psi(y)^* \psi(x)) = \text{Re} \text{Tr}(\psi(x) \psi(y)^*) = \langle \psi(x), \psi(y) \rangle. \quad (6.1)$$

Further, we therefore have that

$$\langle \psi(u^a x), \psi(u^a y) \rangle = 0,$$
whenever $\psi(x)$ and $\psi(y)$ are orthogonal. Now that we have showed that $\psi(\Gamma_\alpha)$ is an orthogonal lattice, we need to prove that it is orthonormal. Indeed, for all $x \in aO_E$ and for every $s = 0, \ldots, n - 1$, using (6.1), we have that

$$||\psi(u^sx)||_E = (\psi(u^sx), \psi(u^sx)) = (\psi(x), \psi(x)) = ||\psi(x)||_E.$$ 

Therefore, since $\psi(aO_E)$ is by assumption an orthonormal lattice, we get that $\psi(\Gamma_\alpha)$ is an orthonormal lattice.

Finally, using Proposition 6.13, since $a \neq 0$, we get that $\delta(\psi(\Gamma_\alpha)) \neq 0$, and thus we indeed have a perfect code.

The following example of a perfect code is taken from [12]. Our aim is to calculate its normalized minimum determinant, with our general methods.

**Example 6.22 (Golden code).** The Golden Code is inside the class of cyclic algebra based codes described above, it is called so because of the use of the Golden Number. We consider the cyclic division algebra $A = \left(\mathbb{E}/\mathbb{Q}(i), \sigma, \gamma\right)$, where $\mathbb{E} = \mathbb{Q}(i, \sqrt{5})$, $\gamma = i$, and the Galois group is generated by $\sigma : \sqrt{5} \mapsto -\sqrt{5}$. Now, write the natural order of $A$ as follows

$$\Gamma = O_E \oplus uO_E,$$

with $u \in E$ an auxiliary generating element associated to $A$. Write $\nu = \frac{1 + \sqrt{5}}{2}$, and $\sigma(\nu) = \frac{1 - \sqrt{5}}{2}$. We know that

$$O_E = \mathbb{Z}[i] \oplus \nu \mathbb{Z}[i].$$

Now, let $\alpha = 1 + i - i\nu$, and $\alpha^* = \sigma(\alpha) = 1 + i - i\nu$. We recall how the relative canonical embedding is defined

$$\psi : A \rightarrow M_2(\mathbb{E})$$

$$x_0 + ux_1 \mapsto \begin{pmatrix} x_0 \gamma \sigma(x_1) \\ x_1 \sigma(x_0) \end{pmatrix}.$$

Since $\psi(aO_E)$ has an orthonormal basis (see Example 3.23), using Proposition 6.21, we know that the following is a perfect code

$$\psi(\Gamma\alpha) = \mathbb{Z}[i] \psi(\alpha) \oplus \mathbb{Z}[i] \psi(\nu \alpha) \oplus \mathbb{Z}[i] \psi(u \alpha) \oplus \mathbb{Z}[i] \psi(u \nu \alpha),$$

so that a codeword $X$ belonging to the Golden Code has the form

$$X = \begin{pmatrix} \alpha(a + b\nu) & \gamma \alpha(c + d\nu) \\ \alpha(c + d\nu) & \nu \alpha(a + b\nu) \end{pmatrix},$$

with $a, b, c, d \in \mathbb{Z}[i]$ carefully chosen.

Now, we are interested to know what is the normalized minimum determinant of the Golden Code. We are making use of Proposition 6.13 which ensures $\delta(\psi(\Gamma\alpha)) = \frac{|\text{Nrd}_A(\alpha)|}{\sqrt{\text{vol}(\psi(aO_E))}}$. On the one hand, we find

$$\text{Nrd}_A(\alpha) = \det(\psi(\alpha)) = \alpha \alpha^* = 2 + i.$$ 

On the other hand, one can compute the Gram matrix associated to the considered lattice and find $\text{vol}(\psi(aO_E)) = 25$. Thus $\delta(\psi(\Gamma\alpha)) = \frac{1}{\sqrt{5}}$.

This chapter gives an answer to Problem 1.11 introduced at the beginning of the thesis. Indeed, we have constructed a lattice code of dimension $2n^2$ with NVD property, which corresponds to a dimension rate of $n$, which is the maximal rate reachable.
7

Codes from crossed products

Here we extend the results of the previous chapter on codes from cyclic division algebras to a more general structure called crossed product algebra. The reader will find out that the proofs and results of this chapter are generalizations of the ones in Chapter 6.

7.1 Definitions and properties

We give below the necessary material to define a crossed product algebra.

**Definition 7.1.** Let $E/F$ be a Galois extension of degree $n$ and $G$ the Galois group of $E/F$. We call a factor set from $G$ to $E^\times$ a map

$$f : G \times G \rightarrow E^\times$$

satisfying

$$f_{\sigma,\tau}f_{\rho,\tau} = \rho(f_{\sigma,\tau})f_{\rho,\sigma\tau}$$

$$f_{\text{Id},\sigma} = f_{\sigma,\text{Id}} = 1,$$

for every $\rho, \sigma, \tau \in G$.

**Remark 7.2.** Usually for a factor set $f : G \times G \rightarrow L^\times$, we denote by $f_{\sigma,\tau}$ the image of the pair $(\sigma, \tau)$ by $f$.

**Definition 7.3.** Let $E/F$ be a Galois extension of degree $n$ and denote its Galois group by $G$. Let us fix a factor set $f : G \times G \rightarrow E^\times$. We denote by $A = (E/F, f)$ the $F$-algebra defined by

$$\bigoplus_{\sigma \in G} u_{\sigma}E,$$

where $\{u_{\sigma}\}_{\sigma \in G}$ forms an $E$-basis and the multiplication is defined by the following rules
if $u_\sigma$ is a crossed product

$$xu_\sigma = u_\sigma^{-1}(x)$$

$$u_\sigma u_\tau = u_{\sigma_\tau} f_{\sigma,\tau},$$

for each $x \in E$, $\sigma, \tau \in G$. We call the $F$-algebra $A$ a crossed product algebra.

**Remark 7.4.** Note that we recover the definition of a cyclic division algebra in the particular case where the Galois group $G = \langle \tau \rangle = \{ \tau^i \}_{i=0}^{n-1}$ is cyclic. Let us now set $\sigma = \tau^{-1}$, then we also have that $G = \langle \sigma \rangle$. We also denote $u_\sigma$ by $u^i$. Let $\{ u_\sigma \}_{\sigma \in G} = \{ u_\sigma \}_{i=0}^{n-1} = \{ u_{\sigma} \}_{i=0}^{n-1}$ be generating elements of $E$. Introducing the following factor set

$$f : G \times G \to E^\times $$

$$(\sigma^i, \sigma^j) \mapsto \begin{cases} 1, & \text{if } i + j < n, \\ \gamma, & \text{if } i + j \geq n, \end{cases}$$

we get that

$$A = \bigoplus_{\sigma \in G} u_{\sigma} E = \bigoplus_{i=0}^{n-1} u^i E,$$

$$xu = xu^1 = xu_{\sigma^1} = u_{\sigma^1} (\sigma^1)^{-1}(x) = u\tau(x),$$

$$u^n = u^{n-1} u = \gamma,$$

for every $x \in E$.

From now on, we focus on number field extensions. Making the link with the algebraic material introduced in Chapters 4 and 5, we give the following theorem which comes from [13, Theorem 29.6, p. 243].

**Theorem 7.5.** $A = (E/F, f)$ is a central simple algebra over $F$ of degree $n$ and $E$ is its own centralizer in $A$.

**Proof.** We denote by $G = \{ \sigma_1, \ldots, \sigma_n \}$ the Galois group of $E/F$, with $\sigma_1 = \text{Id}$. Let us first prove the centrality. We are first going to prove that $Z(A) \subseteq u_{\sigma_1} E$. Let

$$a = u_{\sigma_1} x_1 + \cdots + u_{\sigma_n} x_n \in Z(A).$$

By contradiction, let us suppose that $x_j \neq 0$ for some $j \neq 1$. We know that there exists $x \in E$ such that $\sigma_j^{-1}(x) \neq x$. Now we have that

$$ax = u_{\sigma_1} x_1 + \cdots + u_{\sigma_n} x_n$$

$$xa = u_{\sigma_1} \sigma_1^{-1}(x)x_1 + \cdots + u_{\sigma_n} \sigma_n^{-1}(x)x_n.$$

Since $ax = xa$, we get that $x_j = 0$, which is a contradiction. Thus $Z(A) \subseteq u_{\sigma_1} E$.

Now, let $x \in E$, $x \neq 0$ such that $u_{\sigma_1} x \in Z(A)$. Then for all $i = 0, \ldots, n-1$ we get that

$$u_{\sigma_i} x = u_{\sigma_1} u_{\sigma_i} x = u_{\sigma_i} x u_{\sigma_1} = u_{\sigma_i} u_{\sigma_1} \sigma_i^{-1}(x) = u_{\sigma_i} \sigma_i^{-1}(x).$$
Therefore, \( x = \sigma^{-1}_i(x) \) for all \( i \) implying that \( x \in F \). Thus finally, \( Z(A) \subseteq u_{\sigma_i} F \). Then making the identification \( F \cong u_{\sigma_i} F \), we get that \( Z(A) \subseteq F \). The other inclusion being evident, we have proven that the center of \( A \) is \( F \). Proving that the centralizer of \( E \) in \( A \) is \( E \) itself can be done in the same way.

Let us now prove the simplicity part. Let \( I \) be a nonzero two-sided ideal of \( A \). Let

\[
a = u_{\sigma_i} x_1 + \cdots + u_{\sigma_i} x_r \in I, \ a \neq 0,
\]

with \( r \) minimal. If \( r > 1 \), then choose \( b \in E \) such that \( \sigma_1(b) \neq \sigma_2(b) \). Then \( a - ba_1(b) \) is a shorter nonzero element of \( I \). So, \( r = 1 \). Thus, \( a = u_{\sigma_i} x_1 \) which is a unit. Finally, \( I = A \).

**Remark 7.6.** One can note that \( E \) is by definition a maximal subfield of \( A \). In the case where \( A \) is a division algebra, one can also prove that \( E \) is a maximal subfield by using Theorem 7.5 and Proposition 5.22.

From now on, we will always consider crossed product algebras that are also division algebras.

**Notation 7.7.** We denote by \( \psi \) the relative canonical embedding which gives a matrix representation of every element in \( A \) with respect to the \( E \)-basis \( \{ u_{\sigma_i} \} \).

\[
\psi : A \hookrightarrow A \otimes E \xrightarrow{\sim} M_n(E).
\]

One can also note that in the case where \( G \) is a cyclic group, we get the following embedding

\[
\psi : A \rightarrow M_n(E)
\]

\[
\sum_{i=0}^{n-1} u_{\sigma_i} x_i \mapsto \begin{pmatrix}
    x_0 & f_{\sigma_{n-1},\sigma_1}^{-1}(x_{n-1}) & f_{\sigma_{n-2},\sigma_2}^{-1}(x_{n-2}) & \cdots & f_{\sigma_1,\sigma_{n-1}}^{-1}(x_1) \\
    x_1 & \sigma_1^{-1}(x_0) & f_{\sigma_{n-1},\sigma_1}^{-1}(x_{n-1}) & \cdots & f_{\sigma_2,\sigma_{n-1}}^{-1}(x_2) \\
    x_2 & f_{\sigma_1,\sigma_1}^{-1}(x_1) & \sigma_2^{-1}(x_0) & \cdots & f_{\sigma_3,\sigma_{n-1}}^{-1}(x_3) \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    x_{n-1} & f_{\sigma_{n-2},\sigma_1}^{-1}(x_{n-2}) & f_{\sigma_{n-2},\sigma_2}^{-1}(x_{n-2}) & \cdots & \sigma_{n-1}^{-1}(x_0)
\end{pmatrix}.
\]

More generally, as it is done in [1, Lemma VI.3.1], for a crossed product algebra \( A = (E/F, f) \) and \( a = \sum_{\sigma \in G} e_{\sigma} x_{\sigma} \in A \), one can compute the representative matrix \( M_a \) of the endomorphism consisting of left multiplication by \( a \) with respect to the basis \( \{ e_\sigma \}_{\sigma \in G} \). Indeed, as

\[
au_\tau = \sum_{\sigma \in G} u_{\sigma} x_{\sigma} u_\tau = \sum_{\sigma \in G} u_{\sigma} u_\sigma \tau^{-1}(x_\sigma) = \sum_{\sigma \in G} u_{\sigma} f_{\sigma \tau^{-1}}^{-1}(x_\sigma)
\]

\[
= \sum_{\sigma \in G} u_{\sigma} f_{\sigma^{-1} \tau^{-1}}^{-1}(x_{\sigma^{-1}}).
\]

Thus, \( \psi(a) = M_a = (f_{\sigma^{-1} \tau^{-1}}^{-1}(x_{\sigma^{-1}}))_{\sigma, \tau \in G} \).

**Definition 7.8.** We say that a factor set \( f \) is integral if for every \( \sigma, \tau \in G \) we have \( f_{\sigma \tau} \in \mathcal{O}_E \).
**Definition 7.9.** Let us suppose that we have a division algebra $A = (E/\mathbb{Q}(i), f)$. We will then denote the following subgroup of $A$

$$
\Gamma = \bigoplus_{\sigma \in G} u_\sigma \mathcal{O}_E
$$

by $\Gamma$. In the case where $f$ is an integral factor set, $\Gamma$ is a subring of $A$ and is called a **crossed product order**.

### 7.2 Geometric structure

Now we concentrate on crossed product algebras defined over number fields.

**Lemma 7.10.** Let $A = (E/\mathbb{Q}(i), f)$ be a crossed product algebra. Let us suppose we have a trivial factor set $f$ where $f_{\sigma, \tau} = 1$ for all $\sigma, \tau \in G$. For every $\sigma \in G$, we then have that $\psi(u_\sigma) = P_\sigma$ is a permutation matrix and

$$
P_\sigma P_\tau = P_{\sigma \tau}, \quad P_\sigma^T = P_{\sigma^{-1}}.
$$

Moreover, whenever $\sigma \neq \text{Id}$, we also have that $\text{Tr}(P_\sigma) = 0$.

**Proof.** We consider $A$ as a right vector space over $E$ with basis $\{u_\sigma\}_{\sigma \in G}$. By construction, $\psi(u_\sigma)$ is the matrix representation of the following endomorphism of vector spaces

$$
l_{u_\sigma} : A \rightarrow A
$$

\[a \mapsto u_\sigma a.\]

Then, it is not difficult to see that $\psi(u_\sigma)$ is a permutation matrix. Further, as the factor set is trivial, we naturally get that

$$
P_\sigma P_\tau = \psi(u_\sigma)\psi(u_\tau) = \psi(u_{\sigma \tau}) = P_{\sigma \tau}.
$$

Also, as

$$
P_\sigma P_{\sigma^{-1}} = \psi(u_\sigma)\psi(u_{\sigma^{-1}}) = \psi(1) = I_u,
$$

since the inverse of a permutation matrix is its transpose, we get that

$$
P_\sigma^T = P_{\sigma^{-1}} = P_{\sigma^{-1}}.
$$

Now, for the additional part of the lemma, for all $\sigma, \tau \in G$, $\sigma \neq \text{Id}$, we have that

$$
l_{u_\sigma}(u_\tau) = u_\sigma u_\tau = u_{\sigma \tau} \neq u_\tau.
$$

Thus, the diagonal elements of the matrix $P_\sigma$ are all zero, which leads to the fact that its trace is zero. \qed
Lemma 7.11. Let $\mathcal{A} = (E/\mathbb{Q}(i), f)$ be a crossed product algebra, with an arbitrary factor set $f$. For every $\sigma \in G$, we have that $\psi(u_\sigma) = \Gamma_\sigma P_\sigma$, where $\Gamma_\sigma$ has $f_{\sigma, \tau}, \tau \in G$ as diagonal elements, and $P_\sigma$ the permutation matrix of Lemma 7.10.

Proof. This follows from the definitions. \hfill $\square$

Lemma 7.12. Let $\mathcal{A} = (E/\mathbb{Q}(i), f)$ be a crossed product algebra, with an arbitrary factor set $f$. For every $x \in E$, $\psi(x)$ is a diagonal matrix.

Proof. This follows from the definitions. \hfill $\square$

Proposition 7.13. Let $\mathcal{A} = (E/\mathbb{Q}(i), f)$ be a crossed product algebra, with an arbitrary factor set $f$, and $a \in E, a \neq 0$. For every $x, y \in E$, we then have that

$$\langle \psi(u_\sigma ax), \psi(u_\sigma ay) \rangle = 0, \quad \forall \quad \sigma \neq \tau \in G.$$ 

Proof. We have that

$$\langle \psi(u_\sigma ax), \psi(u_\sigma ay) \rangle = \Re \text{Tr}(\psi(u_\sigma)\psi(ax)\psi(ay)^*\psi(u_\sigma)^*)$$

$$= \Re \text{Tr}(\psi(ay)^*\psi(u_\sigma)^*)\psi(u_\sigma)\psi(ax))$$

$$= \Re \text{Tr}(\psi(ay)^*P_\sigma^\top P_\sigma)$$

$$= \Re \text{Tr}(\psi(ax)\psi(ay)^*P_{\tau^{-1}\sigma})$$

$$= 0,$$

as $\psi(ax)\psi(ay)^*$ is a diagonal matrix in $M_n(\mathbb{C})$ and $\text{Tr}(P_{\tau^{-1}\sigma}) = 0$. \hfill $\square$

7.3 Construction of the codes and properties

7.3.1 Volume and normalized minimum determinant of the codes

Based on Proposition 6.12, the reader can make his own proof for the following result.

Proposition 7.14. Let $\mathcal{A} = (E/\mathbb{Q}(i), f)$ be a crossed product algebra of degree $n$. Let $\Gamma = \bigoplus_{\sigma \in G} u_\sigma \mathcal{O}_E \subseteq A$ and $a \in E, a \neq 0$. Then

$$\psi(\Gamma a)$$

is a $2n^2$-dimensional lattice code in $M_n(\mathbb{C})$. 
Proposition 7.15. Let $\mathcal{A} = (E/Q(i), f)$ be a crossed product algebra of degree $n$. Let $\Gamma = \bigoplus_{\sigma \in G} u_{\sigma} \mathcal{O}_{E} \subseteq A$ and $a \in E, a \neq 0$. Then

$$\text{vol}(\psi(\Gamma a)) = \text{vol}(\psi(a\mathcal{O}_{E}))^n \cdot \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2.$$

Proof. Let us first prove that

$$\text{vol}(\psi(\Gamma')) = \text{vol}(\psi(\mathcal{O}_{E}))^n \cdot \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2.$$

Write

$$\psi(\Gamma a) = \bigoplus_{\sigma \in G} \psi(u_{\sigma} a \mathcal{O}_{E}).$$

Then, using Lemma 2.23 and Proposition 7.13, we get that

$$\text{vol}(\psi(\Gamma')) = \prod_{\sigma \in G} \text{vol}(\psi(u_{\sigma})\psi(\mathcal{O}_{E})).$$

By Proposition 2.39, we then have that

$$\text{vol}(\psi(\Gamma)) = \prod_{\sigma \in G} |\det \psi(a_{\sigma})|^2 \text{vol}(\psi(\mathcal{O}_{E})) = \prod_{\sigma \in G} \prod_{\tau \in G} f_{\sigma, \tau}^2 \text{vol}(\psi(\mathcal{O}_{E})).$$

Therefore, using Propositions 2.36 and 2.39, we get that

$$\text{vol}(\psi(\Gamma a)) = |\det(\psi(a))|^2 n \text{vol}(\psi(\mathcal{O}_{E}))^n \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2$$

$$= (|\det(\psi(a))|^2 \text{vol}(\psi(\mathcal{O}_{E})))^n \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2$$

$$= \text{vol}(\psi(a\mathcal{O}_{E}))^n \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2.$$

□

Remark 7.16. We can now see how we recover the volume of the fundamental parallelootope of a lattice code built from a cyclic division algebra announced in Chapter 6. Indeed, we can deduce the first result of Proposition 6.15 from Proposition 7.15 above. To do that, let $\mathcal{A} = (E/Q(i), f)$ be a crossed product algebra which is a cyclic division algebra, and let $\Gamma$ be a crossed product order. Using Remark 7.4, we get that

$$\text{vol}(\psi(\Gamma a)) = \text{vol}(\psi(a\mathcal{O}_{E})) \prod_{\sigma, \tau \in G} f_{\sigma, \tau}^2 = \text{vol}(\psi(a\mathcal{O}_{E})) \left|\gamma^{n(n-1)/2}\right|^2$$

$$= \text{vol}(\psi(a\mathcal{O}_{E})) \left|\gamma^{n(n-1)}\right|.$$
Proposition 7.17. Let $\mathcal{A} = (E/Q(i), f)$ be a crossed product algebra of degree $n$, with $f$ integral. Let $\Gamma \subseteq A$ be a crossed product order and $a \in E$, $a \neq 0$. Then

$$\delta(\psi(\Gamma a)) = 2^{n/2} |d(E/Q)|^{-1/4} \left| \prod_{\sigma, \tau \in G} f_{\sigma, \tau} \right|^{-1/n}.$$

In particular, $\psi(\Gamma a)$ has NVD property.

Proof. By Theorem 2.43, we know that $\delta(\psi(\Gamma a)) = \delta(\psi(\Gamma))$. Let us now compute the minimum determinant of $\psi(\Gamma)$. By (5.1), we have that

$$\det_{\min}(\psi(\Gamma)) = \inf \{ |\psi(x)| : x \in \Gamma, x \neq 0 \} = \inf \{ |\text{Nrd}_A(x)| : x \in \Gamma, x \neq 0 \}.$$

In the same way as of the proof of Proposition 6.12, we get that the minimum determinant above is 1. Therefore, by the previous proposition we have that

$$\delta(\psi(\Gamma a)) = \delta(\psi(\Gamma)) = \frac{1}{(\text{vol}(\psi(\Gamma)))^{1/2n}} = \text{vol}(\psi(O_E))^{-1/2} \left| \prod_{\sigma, \tau \in G} f_{\sigma, \tau} \right|^2,$$

from which we derive the result, using Lemma 3.18. \qed

Remark 7.18. We now easily see how the second part of Proposition 6.13 can be deduced from Proposition 7.17 above. Indeed, let us take $\gamma \in \mathbb{Z}[i]$ with $|\gamma| = 1$. Then, using Remark 7.4 we get that

$$\delta(\psi(\Gamma a)) = 2^{n/2} |d(E/Q)|^{-1/4} \left| \gamma^{n(n-1)/2} \right|^{-1/n} = 2^{n^2} |d(E/Q)|^{-1/4}.$$

Proposition 7.19. Let $\mathcal{A} = (E/Q(i), f)$ be a crossed product division algebra of degree $n$, with an arbitrary factor set $f$. Let $\Gamma \subseteq A$ be a crossed product order and $a \in E$, $a \neq 0$. Then

$$\frac{1}{|V|^n \sqrt{\text{vol}(\psi(\Gamma))}} \leq \delta(\psi(\Gamma a)) \leq \frac{\text{Nsv}(2n)^n}{n^{n/2}},$$

where $V$ is a generator of the ideal $\psi(f) := \{ x \in \mathbb{Z}[i] : xf_{\sigma, \tau} \in O_E, \forall \sigma, \tau \in G \}$.

Proof. First, by Theorem 2.43 we get that $\delta(\psi(\Gamma a)) = \delta(\psi(\Gamma))$. We can write

$$\psi(\Gamma) = \bigoplus_{\sigma \in G} \psi(u_{\sigma} O_E).$$

Using the orthogonality result of Proposition 7.13, we obtain the upper bound exactly in the same way we obtained the upper bound of Proposition 6.15. Concerning the lower bound, we have that
\[
\det(\psi(\Gamma)) = \inf \{ |\det(\psi(x))| : x \in \Gamma, x \neq 0 \} \\
= \frac{1}{|V|^n} \inf \{ |\det(V\psi(x))| : x \in \Gamma, x \neq 0 \} \\
= \frac{1}{|V|^n} \inf \{ |\det(\psi(x))| : x \in \Gamma, x \neq 0 \} \\
\geq \frac{1}{|V|^n},
\]

where the last infimum is greater or equal than 1 since
\[
\det(\psi(y)) = \text{Nrd}_A(y) \in \mathbb{Z}[i],
\]
for every \( y \in \mathcal{O}_E \). Then it follows that
\[
\delta(\psi(\Gamma a)) = \frac{\det_{\min}(\psi(\Gamma))}{\sqrt{\text{vol}(\psi(\Gamma))}} = \frac{\det_{\min}(\psi(\Gamma))}{\sqrt{\text{vol}(\psi(\Gamma))}} \\
\geq \frac{1}{|V|^n \sqrt{\text{vol}(\psi(\Gamma))}}.
\]

Remark 7.20. We have obtained bounds for the normalized minimum determinant of crossed product algebra-based codes. The interesting thing is that we have used a geometric approach by means of lattices to obtain the aforementioned result. In [1], more algebraic methods were applied. In the case where \( f \) is an integral factor set, Proposition 7.19 is an extension to [1, Proposition VI.3.6]. The difference between these two results is that in [1], the authors assume that \(|f_{\sigma, \tau}| = 1\), for every \( \sigma, \tau \in \Gamma \).

### 7.3.2 Perfect codes

**Proposition 7.21.** Let \( \mathcal{A} = (E/\mathbb{Q}(i), f) \) be a crossed product algebra of degree \( n \), with \( f \) integral. Let \( \Gamma \subseteq \mathcal{A} \) be a crossed product order and \( a \in E, a \neq 0 \). Let us suppose that \( \psi(a\mathcal{O}_E) \) is an orthonormal \( \mathbb{Z}[i] \)-lattice. Then
\[
\psi(\Gamma a)
\]
is a perfect code.

**Proof.** We have that
\[
\psi(\Gamma a) = \bigoplus_{\sigma \in \Gamma} \psi(u_\sigma a\mathcal{O}_E).
\]
By Proposition 7.13, we get that the components of \( \psi(\Gamma a) \) as described above are orthogonal to each other. By using similar arguments as in the proof of Proposition 6.21, we let the reader verify the statement of the announced result.

Remark 7.22. We now see that Proposition 7.19 (respectively 7.21) are generalizations of Proposition 6.15 (respectively 6.21).

As a generalization of the previous chapter on codes constructed from cyclic division algebra, we obtain here too lattice codes of dimension \( 2n^2 \) with NVD property, which give the maximal reachable dimension rate, looking back at Problem 1.11.
Conclusion

In this master project, we have given a general geometric framework for the study of division algebra-based codes. In particular, we proved how these codes can be divided into orthogonal components and how the orthogonality can be used to analyze the codes. This geometric treatment gives a slightly different perspective to the results given by Grégory Berhuy and Frédérique Oggier in their book, *An introduction to central simple algebras and their applications to wireless communication* [1].

We began with an introduction to the engineering problem and then we carefully formulated it into mathematical form. We then slowly developed lattice theoretic and algebraic methods to study codes built from $\mathbb{Q}(i)$-central division algebras. Finally in Chapters 6 and 7 we applied all the previously developed tools in an analysis of codes from cyclic and more generally crossed product algebras. Finally in Proposition 7.19, we applied our methods to analyze the normalized minimum determinant of codes based on crossed product algebras. Here we gave a slight generalization to [1, Proposition VI.3.6]. This modest addition allows us to measure the normalized minimum determinant of crossed product algebra-based codes in the case where the factor set gets non unit absolute values.

The lattice theoretic methods we have given in this master project are finally quite similar to those in [1]. However, with our approach it might be easier to realize the limits of the given tools. Note that all the derived results heavily depend on the presentation we give for the algebra. Indeed, nothing *a priori* tells us that we still have the orthogonality requirement if we change the embedding of the algebra into $M_n(\mathbb{C})$. Seeing these limits also leads us to natural questions for further study. Motivated by the Alamouti code case, the most obvious one is, whether it is possible to extend our methods to analyze space-time codes from division algebras with centers that are not complex quadratic.
References

Index

algebra
  \( K \)-algebra, 35
  central simple algebra, 41
  crossed product algebra, \( A = (E/F, f) \), 74
  cyclic division algebra, \( A = (E/F, \sigma, \gamma) \), 63
  degree, deg, 47
  division algebra, 36
  index, ind, 47
  simple algebra, 40

center, \( Z(\cdot) \), 36
centralizer, 48
centralizer theorem, 48
channel
  communication channel, 1
  continuous channel, 1
  discrete channel, 1
  quasi-static fading channel, 2
characteristic polynomial
  characteristic polynomial, \( \chi_M \), 53
  reduced characteristic polynomial, \( \text{Prd}_A \), 56
code
  code, 2, 4
  codebook, 2
  codeword difference matrix, 3
  coding gain, 3
  finite code, 4
  lattice code, 4
  perfect code, 70
  with full-diversity property, 3
  with NVD property, 4
discriminant, \( d(\cdot) \), 29
error probability, 2

factor set, \( f_{\sigma, \tau} \), 73
fading, 2
  Frobenius norm, \( ||\cdot||_F \), 16
  fundamental parallelootope, \( F_L \), 11
  fundamental volume, \( \text{vol}(\cdot) \), 12

Galois
  Galois extension, 27
  Galois group, \( \text{Gal}(\cdot) \), 27
  Gram matrix, \( G(\cdot) \), 12

ideal
  fractional ideal, 29
  integral ideal, 29

lattice
  \( \mathbb{Z} \)-Lattice, 11
  \( \mathbb{Z}[i] \)-lattice, 70
  full lattice, 11
  orthogonal lattice, 33, 70
  orthonormal lattice, 8, 33, 70

minimum determinant
  \( \text{min}_{\text{det}}(\cdot) \), 4, 17
  normalized minimum determinant, \( \delta(\cdot) \), 7, 17

noise, 1, 2
norm
  norm, \( \text{Nr} \), 28
  reduced norm, \( \text{Nrd} \), 60

order
  crossed product order, \( \Gamma \), 76
  natural order, \( \Gamma_n \), 64

rate
  dimension rate, 5
  symbol rate, 5
ring of integers, \( O_K \), 28

shortest vector
  - longest possible shortest vector, 14
  - normalized shortest vector, Nsv, 14
  - shortest vector, sv, 14

Skolem-Noether’s theorem, 54

splitting field, 47

subfield
  - maximal subfield, 49

subfield of an algebra, 41

Sylvester’s theorem, 20

tensor product of algebras, \( A \otimes_K B \), 37

trace
  - reduced trace, Trd, 60
  - trace, Tr, 28

Wedderburn’s theorem, 46