N° d'ordre : 89/2022-C/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediène

Faculté de Mathématiques

THESE DE DOCTORAT

Présentée pour l'obtention du **grade** de **DOCTEUR**

En : Mathématiques

Spécialité : Mathématiques Fondamentales et Cryptographie

Par : BOUZARA Reguia Lamia

Sujet

Les réseaux arithmétiques et les codes sur les anneaux

Soutenue publiquement le / 02 Juillet 2022 / devant le jury composé de :

M S. Bouroubi	Professeur	à l'USTHB	Président
Mme K. Guenda	Professeur	à l'USTHB	Directrice de thèse
M E. Martinez-Moro	MCA	à U. Valladolid	Co- Directeur de thèse
Mme A. Batoul	MCA	à l'USTHB	Examinatrice
Mme F. Mamache	MCA	à l'USTHB	Examinatrice
M A. Senouci	MCA	à Col à U. Jijel	Examinateur

ACKNOWLEDGEMENT

My unalloyed appreciation goes to my amiable supervisor, Professor Kenza Guenda. I would like to express my sincere gratitude for her continuous support of my Ph.D study and research for her patience, motivation, enthusiasm and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis.
My sincere thanks also goes to my co-supervisor professor Edgar Martinez-Moro for his able guidance, valuable advices and support during my Ph.D.
I would like to thank the rest of my committee members, Pr. Sadek Bouroubi for accepting to be the president of the jury of my thesis, Dr. Aicha Batoul, Dr. Fatiha Mamache and Dr. Abdelkader Senouci for being the body of my thesis jury.
I extend my special thanks to my family for their love and support. All of this wouldn't be possible without them.
Finally, I would like to thank my colleagues and friends who in one way or another shared their help and support.

Résumé

La théorie des réseaux trouve des applications dans divers disciplines, ils sont étudiés en théorie des nombres et en géométrie. De nombreux problèmes sur la théorie des codes ont une relation avec des problèmes sur les réseaux. Cette thèse est consacrée à la construction des réseaux arithmétiques à partir des codes, le but est de construire des réseaux arithmétiques à partir des codes sur les anneaux à chaine finis en utilisant une construction A générale. On considère deux constructions A des réseaux arithmétiques: une construction A à partir des codes sur les corps finis, cette construction est généralisée en une construction A à partir des codes sur les anneaux à chaines finis en utilisant une méthode générale des lifted-codes basée sur la relation entre les anneaux à chaines finis et les corps p-adiques. Une construction particulière des réseaux arithmétiques à partir des codes sur les anneaux à chaines finis est proposée pour construire des codes auto-duaux sur les anneaux à chaines finis.

Abstract

Lattices theory is a research topic related to a broad range of subjects, they are studied in number theory and in geometry. Many problems about coding theory are related to problems about lattices. This thesis dedicated to the construction of lattices from codes.

The goal is to construct lattices from codes over finite chain rings using a generalized construction A. There are two construction considered: the construction A of lattices from codes over number fields, this construction is generalized to a construction A of lattices from codes over finite chain rings via a general treatment of lifted codes and using the connection between finite chain rings and p-adic fields. A particular construction of lattices from codes over finite chain rings is proposed to construct self-dual codes over finite chain rings.

Contents

Introduction

Brief introduction to Lattices Coding theory addresses the problem of reliable communication over noisy channels and is concerned with developing codes that can detect and correct errors in a digital communication. Coding theory is closely related to lattices in the setting of wiretap channel. Many problems about codes have their counterpart in problems about lattices.

Lattices theory is a research topic which is related to a different subjects, ranging from theoretical mathematics to real life. The connection between lattices and codes has been studied by many authors [34], [47], [48], [6], [10] and [16]. Early studies were focusing on unimodular lattices and their construction, for their relation with modular forms and sphere packings [44], [45]. The construction of lattices over number fields was introduced in [17], [12], [13], [3] and [16].

The focus of this thesis will be the algebraic construction of lattices from codes over number fields and more generally from codes over finite chain rings [5], we will give a general construction of lattices from codes over finite chain rings using the connection between finite chain rings and p-adic fields.

Brief introduction to p-adic fields In digital computer it is not possible to represent a rational number $\frac{a}{b}$ in terms of some radix. The set of numbers that are representable is a finite subset of the field of real numbers such as 2(binary), 8(octal) or 10(decimal). It is difficult to use a finite subset to simulate the infinite field of real numbers to solve problems using inexact arithmetic, as a consequence it is necessary to investigate finite number systems with exact arithmetic, that is

why attention was turned to p-adic numbers due to its possible applications in digital computer to get exact computations.
p-adic number fields were introduced by Kurt Hensel [21], [22] in 1897, recently, p-adic number systems for error-free computations was initiated by Krishnamurthy [32], [30], [31] and Alparslan [1]. The main idea was to put the infinite p-adic expansion into a fixed number of digits, r, for all numbers in a subset of $\mathbb{Q}$, we call this fixed-length representations Hensel codes.
The finite number system which contains these Hensel codes has been recently used and applied to many areas of research for example: design of algorithms for error-free computations [19], in matrix processors [32], [30], [31] and in digital signal processing. Recently, p-adic transformation have been introduced and are currently investigated [18], [33], [35], [37], [38], [39], [43].
At the same time, p-adic numbers became crucial in the development of arithmetic geometry, where methods from algebraic geometry are applied to arithmetic problems. One of the most significant achievements in this field is Deligne's proof of Weil's conjectures, we can also cite the proof of Fermat's big theorem, whose proof uses crucially the study of certain p-adic Galois representations. Since then, p-adic numbers have reached many other areas of mathematics, such as dynamical systems theory, Lie theory or cryptography.

Outline of the Thesis Chapter 2 introduces construction A of lattices over number fields. In Chapter 3 we present Construction A of lattices over number fields using linear codes over $\mathbb{F}_p$. Further we gave a generalization of the construction A to maximal real subfields of cyclotomic fields.

We propose a new construction A of lattices, a generalization of construction A from codes over finite chain rings using the fact that: a finite commutative chain ring is a finite local ring whose maximal ideals are principal. Any finite chain ring can be constructed from p-adic fields (see for example [26]) as follows: let K be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ with residue degree r and ramification index s, let $\mathcal{O}_K$ be the ring of integers of K and let π be a prime of K. Then $\mathcal{O}_K/\pi^{(n-1)s+t}$ is a finite commutative chain ring with invariants (p, n, r, s, t).

Further every finite commutative chain ring can be obtained in this way.
Using the definition of chain rings as non-trivial quotient of ring integers of p-adic fields we provide a general and a unified treatment of lifted codes for any finite chain ring. This definition allows to introduce a general construction of lifted cyclic codes that can be used to lift codes over finite fields $\mathbb{F}_{p^r}$ to codes over finite chain rings. Thus the lifted codes are used to give a general construction A of lattices from codes over finite chain rings that generalizes the construction of lattices in [28], we finish the work with a particular constructions of lattices that can be used to construct self-dual codes over finite chain rings.

Chapter 1

Lattices and Codes

In this chapter we will give the elementary definitions of lattices and linear codes and their relevant properties and parameters, then we will illustrate the connection between lattices and linear codes.

1.1 Lattices Fundamentals

We will start by the elementary definitions of lattices and some properties. The proofs and details of this section can be found in [16]

Definition .1. *A subset Λ of $\mathbb{R}^n$ with a basis $(e_1, \ldots, e_n)$ of $\mathbb{R}^n$ such that $\Lambda = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$ is called a lattice, it consists of all integral linear combinations of the vectors $e_1, \ldots, e_n$.*

Definition .2. *A generator matrix M_Λ for a lattice Λ in $\mathbb{R}^n$ is a full rank matrix* *whose rows generates Λ:*

$$M_\Lambda = \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \in \mathbb{R}^{n\times n} \text{ and } \Lambda = \{vM_\Lambda; v \in \mathbb{Z}^n\}.$$

Example .1. *1. The lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ is a standard example, we call it the cubic lattice or the integer lattice.*

2. The lattice $\mathbb{Z}^2$ (square lattice) is a lattice of rank 2 in $\mathbb{R}^2$ with basis $\{(1,0),(0,1)\}$

Definition .3. *Let Λ be a lattice such that $\Lambda \subseteq \mathbb{R}^n$ defined by:*

$$\Lambda := \{x \cdot M_\Lambda \ ; \ x \in \mathbb{Z}^n\}.$$

The matrix given by $G_\Lambda := M_\Lambda M_\Lambda^T$ is called a Gram matrix of Λ. Hence a lattice is a discrete additive subgroup of $\mathbb{R}^n$.

Definition .4. *Let Λ be a free $\mathbb{Z}$-module of rank n associated by a symmetric bilinear form*

$$b : \Lambda \times \Lambda \to \mathbb{Z}$$

The pair (Λ, b) is called an integral lattice over $\mathbb{R}$.

Definitions .1. *Let (Λ, b) be a lattice of dimension n with basis $(g_1, \dots, g_n)$ the rows of its generator matrix M_Λ.*

We define the fundamental parallelotope that is formed by the set of rows $\{g_1, \dots, g_n\}$, as follows:

$$P = \{\lambda_1 g_1 + \ldots + g_n \ ; 0 \leq \lambda_i < 1\} \ \textit{of} \ \Lambda.$$

The volume of Λ which is the volume of the fundamental parallelotope is given by:

$$vol(\Lambda) = vol(P) =\mid det(M_\Lambda) \mid .$$

The discriminant of Λ is the square of the volume of Λ:

$$disc(\Lambda) = det(G_\Lambda) = det(M_\Lambda)^2$$

Definition .5. ***The dual lattice***

The lattice (Λ^*, b) such that:

$$\Lambda^* = \{x \in \Lambda \ ; b(x,y) \in \mathbb{Z} \ , \forall y \in \Lambda\}$$

is called the dual lattice of the lattice (Λ, b) with generator matrix

$$M_\Lambda^* := (M_\Lambda^T)^{-1} \ \textit{where} \ M_\Lambda \ \textit{is the generator matrix of} \ \Lambda.$$

If $\Lambda \subseteq \Lambda^*$ we say that Λ is integral and:

$$vol(\Lambda) = vol(\Lambda^*) \mid \Lambda^*/\Lambda \mid$$

$$\text{and } disc(\Lambda) =\mid \Lambda^*/\Lambda \mid .$$

Definition .6. *Let (Λ_1, b_1) and (Λ_2, b_2) be two lattices we say that Λ_1 and Λ_2 are isometric if there exists a $\mathbb{Z}$-module isomorphism*

$$\varphi : \Lambda_1 \to \Lambda_2 \text{ satisfying}$$

$$b_2(\varphi(x), \varphi(y)) = b_1(x, y) \text{ for } x, y \in \Lambda_1$$

Definition .7. *[24] Let (Λ, b) be an integral lattice and l be a positive integer, if (Λ, lb) is isomorphic to (Λ, b) i.e., by applying the previous definition there exists a $\mathbb{Z}$-module isomorphism $\varphi^* \to \varphi$ such that $b(\varphi(x), \varphi(y)) = lb(x, y)$ for all $x, y \in \Lambda^*$, then Λ is called l-modular or modular of level l.*

When $l = 1$, we say that Λ is a unimodular lattice.

Definition .8. *Let (Λ, b) be an integral lattice then*

- *If $b(x, x) \in 2\mathbb{Z}$ for all $x \in \mathbb{Z}$ we say that (Λ, b) is even and odd otherwise.*

- *The minimal norm of* (Λ, b) *is*

$$\mu_\Lambda = min\{b(x,x)\ ;\ x \in \Lambda, x \neq 0\}$$

The cardinality of the set $\{x \in \Lambda\ ;\ b(x,x) = \mu_\Lambda\}$ *is called the kissing number of* Λ.

Next we propose another characterization of integral lattices:

Definition .9. *Let* R *be a unitary commutative ring, and* Λ *be a free* R*-module of rank* n. *We associate to* Λ *a symmetric bilinear form* $b : \Lambda \times \Lambda \to R$. *The pair* (Λ, b) *is called a symmetric bilinear form module over* R.

Proposition .1. *A lattice* Λ *is integral over* $\mathbb{R}^n$ *if* (Λ, b) *is a symmetric bilinear form module over the ring of integers* $\mathbb{Z}$, *where* $b : \Lambda \times \Lambda \to \mathbb{Z}$ *is a positive definite symmetric bilinear form.*

For a proof see [16]

Let (Λ, b) *and* (Λ', b') *be two symmetric bilinear form modules over* R, *we say that* (Λ, b) *and* (Λ', b') *are isomorphic if there is an* R*-linear bijection* $\phi : \Lambda \to \Lambda'$ *such that* $b'(\phi(x), \phi(y)) = b(x,y)$ *for all* $x, y \in \Lambda$.

Let Λ *be an integral lattice with a basis* $(e_1, \ldots, e_n)$. A *is a matrix with an* integer determinant det A. The determinant det A is independent of the choice of the basis.

Let $\tilde{e}_1, \ldots, \tilde{e}_2$ such that $\tilde{e}_i = \sum_{j=1}^{n} q_{ij} e_j$ be another basis of Λ with $\tilde{A} = ((e_i \tilde{\cdot} \tilde{e_j}))$. Let $Q = ((q_{ij}))$ be a matrix in $GL_n(\mathbb{Z})$ in particular det $Q = \pm 1$. We have that $\tilde{A} = QAQ^t$ then, $det\tilde{A} = detA$. Then det A is independent to the choice of the basis $(e_1, \ldots, e_n)$.

The number given by det A is called the discriminant of the lattice Λ and we write $disc(\Lambda)$.

The volume of Λ in this case is given by

$$vol(\mathbb{R}^n/\Lambda) = \sqrt{disc(\Lambda)},$$

$$vol(\mathbb{R}^n/\Lambda^*) = \frac{1}{\sqrt{disc(\Lambda)}}$$

Then we have $disc(\Lambda) = \mid \Lambda^*/\Lambda \mid$ since we have that

$$vol(\mathbb{R}^n/\Lambda) = vol(\mathbb{R}^n/\Lambda) \cdot \mid \Lambda^*/\Lambda \mid .$$

We say that a lattice $\Lambda \subset \mathbb{R}^n$ is unimodular if $\Lambda = \Lambda^*$ and we have that $vol(\Lambda) = 1$.

Theta function of a lattice *The theta series of the lattice Λ is the function :*

$$\theta_\Lambda(\tau) := \sum_{x\in\Lambda} q^{\|x\|^2} = \sum_{m\in\mathbb{Z}\geq 0} A_m q^m \ ; \tau \in \mathbb{H},$$

where $\mathbb{H} = \{\tau \in \mathbb{C} \ ; Im(\tau) > 0\}$. We can see that the kissing number of Λ is the coefficient of q in the second term of θ_Λ, and the minimum of Λ is giving by the power of q in the second term.

Lattices are lied with codes in wireless communication, they can achieve the capacity of additive white Gaussian noise channel with and without power construction. It is well known that lattices can be constructed from codes, they can provide a classical information theoretic way to obtain achievable rate. An applicable range of lattices in digital communications have been treated including the well known root lattices, Construction A and construction A'. In our work we are interesting in construction A.
Before introducing this construction we have to give some fundamental definitions of error-correcting codes.

1.2 Linear codes

Suppose that we have a message and we want to send it using a channel in such a way that it can be correctly recovered even if there is noise or transmission errors. Therefore the message is encoded with a certain redundancy such that errors can be detected and corrected. The design of such error correcting code is the main subject of coding theory, where error correcting codes are important for the transmission of information as an example: satellite, communication and in telephone.

By definition a message is a finite sequence of symbols such that for a finite field $\mathbb{F}_q$ the encoding is given by an injective mapping $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ $n > k > 0$
and the image $f(\mathbb{F}_q^k) := C \subset \mathbb{F}_q^n$ defines a code of length n.
We will start by giving some basic definitions.

Definition .10. *Let $x \in \mathbb{F}_q^n$ and $y \in \mathbb{F}_q^n$ with $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, the Hamming distance between x and y denoted by $d(x, y)$ is defined as follows:*

$$d(x, y) := w(x - y)$$

where $w(x)$ is the number of nonzero x_i.

Definition .11. *Let C be a nontrivial code over $\mathbb{F}_q$ of length n, the minimum distance of C denoted by d is defined by the minimum of distances $d(x, y)$, $x \neq y$ with $x \in C$ and $y \in C$.*

We have that an $[n, k]$-linear code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

- If $\mid C \mid= 1$ we say that C is trivial code,

- $q = 2$ we say that C is a binary code,

- $q = 3$ we say that C is a ternary code.
  The elements of a linear code C are called codewords.The codewords are of length n.

Remark 1. *The minimum weight of non-zero codewords in a code C is the minimum distance of C.*

Since C is a subspace, then there exists a basis $B = \{\beta_1, \dots \beta_k\}$, where k is the dimension of the subspace. We say that C is an $[n, k]$-code and every element w of C has a unique representation as a linear combination

$$w = \sum_{i=1}^{k} \alpha_i \beta_i \ ; \alpha_1, \dots, \alpha_k \in \mathbb{F}_q.$$

and the number of codewords in an $[n, k]$-linear code is q^k.
The corrective capacity of a code has an important link with the minimum distance of this code, a linear code C with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors and detect $d - 1$ errors.

Definition .12. *Let C be an $[n, k]$-linear code over $\mathbb{F}_q$.*

A generator matrix for C is given by:

$$G = \begin{pmatrix} g_1 \\ \\ g_2 \\ \\ \vdots \\ \\ g_k \end{pmatrix},$$

where $\{g_1, \dots, g_k\}$ is any basis of C and we write:

$$C = \left\{ uG; u \in \mathbb{F}_q^k \right\}.$$

We say that the matrix G is under systematic form if:

$G = \begin{pmatrix} I_k & A \end{pmatrix}$ where I_k is the $k \times k$ identity matrix, and A is some $k \times (n - k)$ matrix.

Let $x, y \in \mathbb{F}_q^n$, we may define an "inner product" in $\mathbb{F}_q^n$ as follows:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Let C be an $[n, k]$-code over $\mathbb{F}_q$. The Euclidean dual code $C^\perp$ of C is given by:

$$C^\perp = \left\{ v \in \mathbb{F}_q^n ; \forall c \in C, \langle v, c \rangle = 0 \right\}$$

and we say that a linear code C is self-orthogonal in the Euclidean sense if we have that $C \subset C^\perp$. Furthermore, if C satisfies $C = C^\perp$ then we say that C is self-dual and we have that:

$$dim\ C + dim\ C^\perp = n.$$

Hence, an $[n, k]$-linear code C is self-dual if and only if C is self-orthogonal and $k = n/2$.
The generator matrix of the dual code is given as follows:

Definition .13. *Let C be an $[n, k]$-code over $\mathbb{F}_q$, the parity check matrix for C is given as follows:*

$$H = \begin{pmatrix} -A^T & I_{n-k} \end{pmatrix}$$

such that H satisfies: $GH^T = 0^{k \times (n-k)}$ for every generator matrix G of C.

Equivalently, we have:

$$C = \left\{ c \in \mathbb{F}_q^n ; cH^T = 0 \right\}$$

Proposition .2. *The Euclidean dual code of a linear code C of rank k over $\mathbb{F}_q$ is an $[n, n-k]$-linear code and the parity check matrix H of C is a generator matrix* *for $C^{\perp}$, where H satisfies:*

$$GH^T = 0^{k\times(n-k)}$$

for every generator matrix G of C and we write:

$$C = \left\{c \in \mathbb{F}_q^n; cH^T = 0\right\}.$$

Remark 2. *The minimum distance of the dual code $C^{\perp}$ is denoted by $d^{\perp}$ and it is called the dual distance.*

The Hermitian dual: For a code over $\mathbb{F}_{p^2}$, we should consider the Hermitian inner product. The dual code with respect to this inner product is a linear code denoted by $C^{\perp h}$ and called Hermitian dual. It is given by:

$$C^{\perp h} = \left\{x \in \mathbb{F}_{q^2}^n \; ; \; \sum_{i=1}^{n} x_i y_i^q = 0, \forall y \in C\right\}.$$

A linear code is said to be self-orthogonal in the Hermitian sense if it satisfies $C \subset C^{\perp h}$. We say that C is self-dual in the Hermitian sense if $C = C^{\perp h}$.

1.2.1 Cyclic codes over finite fields $\mathbb{F}_q$

Cyclic codes are among the first codes used due to there rich algebraic structure.

Definition .14. *Let C be a linear code over $\mathbb{F}_q$ we say that C is a cyclic code if C is invariant under a cyclic shift:*

$$c = (c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1}) \in C$$

if and only if

$$\tilde{c} = (c_{n-1}, c_0, c_1, \ldots, c_{n-3}, c_{n-2}) \in C.$$

Since C is invariant under a single right cyclic shift then it is invariant under $n-1$ right cyclic shifts by iteration, hence we say that the linear code C is cyclic when it is invariant under all cyclic shifts.

Example .2. 1. *The repetition code is cyclic.*

2. *The binary parity check code is cyclic.*

Now let $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, since we can consider codewords of the code C as polynomials, then we can associate the polynomial of degree less then n to $a \in \mathbb{F}_q^n$ as follows:

$$a(x) = a_0 + a_1x + \ldots + a_ix^i + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$$

we say that $a(x)$ is the associated code polynomial.
The shifted codeword $\tilde{c}$ can also be associated by a code polynomial as follows:

$$\tilde{c} = c_{n-1} + c_0x + c_1x^2 + \ldots + c_ix^{i+1} + \ldots + c_{n-2}x^{n-1}$$

such that $\tilde{c} = x(c(x)) = xc(x)$, more precisely,

$$\tilde{(c)} = xc(x) - c_{n-1}(x^n) - 1$$

hence $\tilde{c}$ has degree less than n such that the degree of $(xc(x))$ is divided by $x^n - 1$, moreover $\tilde{c}(x)$ and $xc(x)$ are equal in the ring of polynomials $\mathbb{F}_q[x](mod\ x^n - 1)$ where arithmetic is done modulo the polynomial $x^n - 1$ and we will write $c(x) \in C$.
Let $f(c) \in C(mod\ x^n - 1)$, then the definition of cyclic codes using this notation $c(x) \in C$ will be:

$$c(x) \in C(mod\ x^n - 1) \textit{ if and only if}$$

$$c(x) \in C(mod\ x^n - 1),$$

moreover we have that $x^i c(x) \in C(mod\ x^n - 1)$ and by linearity we have that:

$$a_i x^i c(x) \in C(mod\ x^n - 1)\ for\ a_i \in \mathbb{F}_q.$$

Then:

$$\sum_{i=0}^{d} a_i x^i c(x) \in C(mod\ x^n - 1).$$

Therefore, the product of two polynomials $a(x) = \sum_{i=0}^{d} x^i \in \mathbb{F}_q[x]$ and $c(x)(mod\ x^n - 1)$ belongs to C.

Theorem .1. *Let C be a cyclic code over $\mathbb{F}_q$ of length n such that $C \neq 0$, then:*

1. *If $g(x)$ is a monic code polynomial of minimal degree r in C, then $g(x)$ can be uniquely determined in C and we have:*

   $$C = \{q(x)g(x)/q(x) \in \mathbb{F}_q[x]\}$$

   and we say that C has dimension $n - r$.

2. *The polynomial $g(x)$ divides $x^n - 1$ in $\mathbb{F}_q$.*

Now let $h(x) \in \mathbb{F}_q[x]$ such that:

$$g(x)h(x) = x^n - 1,$$

then the polynomial $h(x)$ is called the check polynomial of C.

Proposition .3. *Let C be a cyclic code over $\mathbb{F}_q$ of length n and let $h(x) \in \mathbb{F}_q$ be the check polynomial of C, then:*

$$C = \{c(x) \in \mathbb{F}_q[x]\ ;\ c(x)h(x) = 0(mod\ x^n - 1)\}$$

Proof. Let $c(x) \in C$ then there exists a polynomial $q(x)$ such that $c(x) = q(x)g(x)$, but we have:

$$c(x)h(x) = q(x)g(x)h(x) = q(x)(x^n - 1) = 0(mod\ x^n - 1)$$

for an arbitrary polynomial $c(x) \in \mathbb{F}_q$, where

$$c(x)h(x) = p(x)(x^n - 1),$$

we have that:

$c(x)h(x) = p(x)(x^n - 1) = p(x)g(x)h(x)$, then $(c(x) - p(x)g(x))h(x) = 0$ and we have

$c(x) - p(x)g(x) = 0$, because $g(x)h(x) = x^n - 1$ with $h(x) \neq 0$.

Therefore $c(x) = p(x)g(x)$. □

Definition .15. *Let C be a cyclic code over $\mathbb{F}_q$ of length n with a generator polynomial $g(x) = \sum_{j=0}^{r} g_j x^j$, then a generator matrix for C is given by*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & & \\ & & \ddots & & & \ddots & & \\ & & & g_0 & & g_1 & \cdots & g_{n-k} \end{pmatrix} \leftrightarrow \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$$

such that the matrix G is an $n(n-r)$ matrix, where each successive row is the cyclic shift of the previous row such that G is in echelon form and the $k = dim(C)$ rows of G are linearly independent.

1.2.2 Linear codes over finite chain rings

Finite chin rings are the most studied rings in coding theory. In this part we will extend the study of linear codes from finite fields to finite chain rings.
A finite chain ring R is a finite commutative local ring such that for a fixed generator π of the maximal ideal of R with nilpotency index s, the ideals of R form a chain given as follows:

$$0 = \langle \pi^s \rangle \subsetneq \left\langle \pi^{s-1} \right\rangle \subsetneq \ldots \subsetneq \left\langle \pi^1 \right\rangle \subsetneq \left\langle \pi^0 \right\rangle = R.$$

The elements of the residual field $\mathbb{F}_q = R/\langle \pi \rangle$ are units with $q = p^r$ for some integer r and prime p and we have that:

$$\mid R \mid = \mid \mathbb{F}_q \mid \cdot \mid \langle \pi \rangle \mid = p^{sr}$$

where $\mid \mathbb{F}_q \mid = \mid \mathbb{F}_{p^r} \mid = p^r$. For more details over finite chain rings see [4], [36], [8], [9].

A linear code $\mathcal{C} \subseteq R^m$ of length m over a finite chain ring R is a submodule of R^m. The length m is assumed to be not divisible by the characteristic of the residue field $R/M = \mathbb{F}_{p^r}$. A matrix G with entries in R is called a generator matrix for the code $\mathcal{C}$ if its rows span $\mathcal{C}$ and none of them can be written as an R-linear combination of other remaining rows of G. The generator matrix is in standard form if it is written as follows (see [41])

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,s-1} & A_{0,s} \\ 0 & \pi I_{k_1} & \pi A_{1,2} & \pi A_{1,3} & \cdots & \pi A_{1,s-1} & \pi A_{1,s} \\ 0 & 0 & \pi^2 I_{k_2} & \pi^2 A_{2,3} & \cdots & \pi^2 A_{2,s-1} & \pi^2 A_{2,s} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \pi^{s-1} I_{k_{s-1}} & \pi^{s-1} A_{s-1,s} \end{pmatrix} \tag{1.1}$$

where the columns are grouped into blocks of sizes $k_0, k_1, ..., k_{s-1}, m = \sum_{i=0}^{s-1} k_i$.

Definition .16. *Let $\mathcal{C}$ be a linear code with a generator matrix of the form given in equation 1.1. We say that $\mathcal{C}$ is of type $1^{k_0}\pi^{k_1}(\pi^2)^{k_2}\ldots(\pi^{s-1})^{k_{s-1}}$.*

It is clear that the size of the code is $|\mathcal{C}| = |M|^{\sum_{i=0}^{s-1}(s-i)k_i}$. The *rank* of the code $\mathcal{C}$ is defined to be $k(\mathcal{C}) = \sum_{i=0}^{s-1} k_i$. Both the type and the rank are invariants of the code. The linear code $\mathcal{C}$ is free if its rank is equal to the maximum of the ranks of the free submodules of $\mathcal{C}$. Then, the code $\mathcal{C}$ is a free R-submodule which is isomorphic as a module to $R^{k(\mathcal{C})}$.

The dual code

We attach the standard inner product to the ambient space, i.e., $x \cdot y = \sum x_i y_i$ where $x, y \in R^m$. The dual code $C^\perp$ of C is defined by $C^\perp = \{x \in R^m | x \cdot y = 0 \textit{ for all } y \in C\}$. If $C \subseteq C^\perp$ we say that the code is self-orthogonal, and if $C = C^\perp$ we say that the code is self-dual.

Theorem .2. *Let C be a code with generator matrix G in standard form. Then*

(i) If for $0 \leq i \leq v$, $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k}A^{tr}_{s-j,s-k} - A^{tr}_{s-j,v-i}$, then

$$H = \begin{pmatrix} B_{0,s} & B_{0,s-1} & \cdots & B_{0,1} & T_{n-k(C)} \\ \pi B_{1,s} & \pi B_{1,s-1} & \cdots & \pi I_{k_{s-1}(C)} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \pi^{s-1}B_{s-1,s} & \pi^{s-1}I_{k_1(C)} & \cdots & 0 & \end{pmatrix}$$

is a generator matrix for $C^\perp$ and a parity check matrix for C.

(ii) $|C^{\perp}| = |R^n|/|C|$ *and* $(C^{\perp})^{\perp} = C$.

For any code C and any $r \in R$, we define a sub-module quotient as follows:

$$(C : r) = \{x \in R^n | rx \in C\}.$$

Definition .17. *To any code C over R we associate the tower of codes*

$$C = (C : \pi) \subseteq \cdots \subseteq (C : \pi^i) \subseteq \cdots \subseteq (C : \pi^{s-1}).$$

over R, for $i = 1, 2, ..., s-1$ the projections of $(C : \pi^i)$ over the field M are denoted by $Tor_i(C) = \overline{(C : \pi^i)}$. We call this projections the torsion codes associated with the code C and we have:

$$|Tor_i(C)| = \prod_{j=0}^{i} q^{k_j},$$

such that

$$Tor_0(C) \subset Tor_1(C) \subset \cdots \subset Tor_{s-1}(C) \subset Tor_0(C)^{\perp}$$

Free codes

Definition .18. ***(Free codes)*** *a code C over R is said to be free if it is a free R-module.*

Obviously, over a field any code is free. the following characteristic of a free code are immediate:

Proposition .4. *Let C be a code over R. The following assertions are equivalent:*

(i) C *is a free code.*

(ii) *If* G *is a generator matrix for* C *in standard form, then* $G = (I \;\; N)$ *for some matrix* N.

(iii) $k(C) = k_0(C)$.

(iv) $\overline{C} = \overline{C : \pi} = \cdots = \overline{(C : \pi^{s-1})}$.

(v) $C^{\perp}$ *is a free code.*

(vi) $\overline{C}$ *has generator matrix* $\overline{G}$ *and parity check matrix* $\overline{H}$

For more details see [23].

1.2.3 Cyclic Codes over finite chain rings

Although this section n is a positive integer such that $p \nmid n$; wich implies that $x^n - 1$ is square free in $\overline{R}[x]$ where $\overline{R}$ is the residue field, and $x^n - 1$ has a unique decomposition as a product of basic irreducible pairwise coprime polynomials in $R[x]$ (a polynomial f is said to be basic irreducible in $R[x]$ if $\bar{f}$ is irreducible in $\overline{R}[x]$). As defined previously, a linear code C of length n over R is an R-submodule of R^n, we say that C is cyclic code if it is invariant under the cyclic shift i.e; if $c = (c_0, c_1, ..., c_{n-1})$ is a codeword of C then the cyclic shift of c defined as $(c_{n-1}, c_0, c_1, ..., c_{n-2})$ is also a codeword of C. We can associate to every codeword $c = (c_0, c_1, ..., c_{n-1})$ a polynomial $g(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in \dfrac{R[x]}{x^n - 1}$, we say that g is the polynomial representation of c.

Theorem .3. *[14] Let $x^n - 1 = \prod_{i=1}^{r} f_i$ where f_i for $i = 1, ..., r$ are basic irreducible pairwise-coprime polynomials in $R[x]$. Then the ideals of the quotient ring $\dfrac{R[x]}{x^n - 1}$ are sums of ideals of the form*

$$\langle a^j \widehat{f_i} + \langle x^n - 1 \rangle \rangle$$

where $\widehat{f_i} = \dfrac{x^n - 1}{f_i}$ and $0 \leq j \leq s, 1 \leq i \leq r$.

Corollary 1. *[14] If $x^n - 1 = f_1 f_2 ... f_t$ where f_i are monic basic irreducible coprime polynomials, then the number of cyclic codes over R of length n is $(s+1)^t$.*

The next theorem defines the structure of a cyclic code and its cardinality.

Theorem .4. *[14] If C is a cyclic code over R then there exists a unique family of pairwise coprime monic polynomials $F_0, F_1, ..., F_s \in R[x]$ such that $x^n - 1 = F_1 F_2 ... F_s$ and $C = \langle \widehat{F}_1, \pi \widehat{F}_2, ..., \pi^{s-1} \widehat{F}_s \rangle$. And we have*

$$|C| = (|\overline{R}|)^{\sum_{i=0}^{s-1} (s-i) deg\ F_{i+1}}$$

Theorem .5. *[14] Let C be a cyclic code over R such that $C = \langle \widehat{F}_1, \pi \widehat{F}_2, ..., \pi^{s-1} \widehat{F}_s \rangle$. Then*

$$|C^{\perp}| = (|\overline{R}|)^{\sum_{i=0}^{s} (s-i) deg\ F^*_{i+1}},$$

and

$$C^{\perp} = \langle \widehat{F}^*_0, \pi \widehat{F}^*_t, ..., \pi^{t-1} \widehat{F}^*_2 \rangle.$$

Cyclic dual codes

Proposition .5. *[14]*

Let $F_0, F_1, \ldots, F_t = x^n - 1$ and Â, C is said to be self-dual if and only if F_i is an associate of $F_j^* \forall i, j \in \{0, \ldots, t\}$ such that $i + j \equiv 1(mod\, t+1)$.

Lemma .1. *[14] If deg $f \geq$ deg g, then*

1. *$(f(x) + g(x))^* = f^*(x) + x^{deg\ f - deg\ g} g^*$.*

2. *$(f(x)g(x)) = f^*(x)g^*(x)$*

Theorem .6. *[14] For t an even integer, we have that non-trivial self-dual codes exists if and only if there exists $f \in R[x]$ where f is a basic irreducible factor of $x^n - 1$ such that f and f^* are not associate.*

The next theorem gives a necessary and sufficent condition for existence of non-trivial self-dual cyclic codes of length n over R for t even.

Theorem .7. *[14] Let R be a finite chain ring with maximal ideal $\langle \pi \rangle$, $\mid R \mid = p^{lt}$, where $\mid \bar{R} \mid = p^l$ and t is the nilpotency of π, then non-trivial self-dual cyclic codes of length n over R exist if and only if $p^i \neq -1(mod\, n)$ for all $i \geq 0$.*

1.3 Construction A of lattices

A natural way of constructing lattices is to associate a lattice in $\mathbb{R}^n$ to a linear code in $\mathbb{Z}_q^n$. This construction is called construction A of lattices and the obtained lattice is called q-ary lattice, this construction has several applications in information theory and cryptography for example in the development of good codes for the Gaussian channel, for some channels with side information and also for wiretap coding.
Let $q \geq 2$ be a positive integer, such that $q = m_1 m_2$, $m_1, m_2 \neq 0$ is a composite integer. For $q = p$ where p is a prime number we write $\mathbb{Z}_p^n = \mathbb{F}_p^n$.

Definition .19. *A linear code C in $\mathbb{Z}_q^n$ is an additive subgroup of $\mathbb{Z}_p^n$.*

Example .3. *[11] Let C be a code over $\mathbb{Z}_5^2$. Since $q = 5$ where $5 = p$ is a prime integer, then we write $\mathbb{Z}_5^2 = \mathbb{F}_5^2$.*

The code C is given by

$$C = \left\{a(1,2); a \in \mathbb{F}_5^2\right\} = \{(0,0),(1,2),(2,4),(3,1),(4,3)\}.$$

We have that C is a subspace of the vector space $\mathbb{F}_5^2$, generated by the vector $(1,2)$ so we write $C = \langle(\,1,2)\rangle$.

Next we will show the connection between lattices and linear codes in $\mathbb{Z}_q^n$.
We consider the map:

$$\psi : \mathbb{Z} \rightarrow \mathbb{Z}_q, x \mapsto x(\ mod\ q)$$

ψ is the reduction of x modulo q and the preimage of x by $\psi^{-1}(x)$ is the set of integers that are mapped to x by ψ such that:

$$\psi^{-1}(x) = \{x + bq\ ;\ b \in \mathbb{Z}\}.$$

The set of all ordered pairs (a, b), $a, b \in \{1, \dots, q-1\}$ given by

$$\mathbb{Z}_p \times \mathbb{Z}_p = \{(a, b)\ ;\ a, b\mathbb{Z}_q\}$$

is the Cartesian product of integers modulo q.
Let $\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_q \times \mathbb{Z}_q, (a, b) \mapsto (a(mod\ q), b(mod\ q))$ be the map of reduction modulo q component-wise. The preimage $\psi^{-1}((a, b))$ is the set of 2-dimensional vectors with entries in $\mathbb{Z}$.
For an arbitrary number n of copies of $\mathbb{Z}$, the map ψ can be defined as follows:

$$\psi : \mathbb{Z}^n \to \mathbb{Z}_q^n\ ,\ x \mapsto \psi(x)$$

such that we apply the reduction modulo q over the n components of x. The next result will establish the connection between linear codes and lattices:

Proposition .6. *[11] Let S be a subset of $\mathbb{Z}_q^n$, then $\psi^{-1}(S)$ is a lattice in $\mathbb{R}^n$ if and only if S is a linear code in $\mathbb{Z}_q^n$.*

For a proof see [11]

Definition .20. *Let C be a linear code in $\mathbb{Z}^n$, for $q \geq 2$ such that q is prime or composite integer. The component-wise reduction modulo q map is given by*

$$\psi : \mathbb{Z}^n \to \mathbb{Z}_q^n,$$

The preimage of C by ψ denoted by $\Gamma_C = \psi^{-1}(C)$ defined a lattice and we say that Γ_C is obtained via construction A. The lattice Γ_C is also called q-ary lattice or modulo q lattice.

Proposition .7. *[11]*

1. *If Γ_C is a q-ary lattice obtained via construction A from the code $C \subset \mathbb{Z}_q^n$, then:*

$$\left|\frac{\Gamma_C}{q\mathbb{Z}^n}\right| = \frac{q^n}{vol(\Gamma_C)} =\mid C \mid$$

where $\mid C \mid$ is the number of codewords of C.

2. *Any full rank integer lattice $\Gamma \subset \mathbb{Z}^n$ is q-ary for $q = vol(\Gamma)$.*

Proof.

1. Since there is an isomorphism between $\Gamma_C/q\mathbb{Z}$ and C then the first property is verified.

2. Since $\Gamma \subset \mathbb{Z}^n$, then $vol(\Gamma) \in \mathbb{Z}$. If we take a generator matrix B for Γ, then $vol(\Gamma) =\mid det(B) \mid= q$, therefore $Bx = qz$ is a linear system with an integer solution for any $z \in \mathbb{Z}^n$, it follows that $q\mathbb{Z}^n \subset \Gamma$ then Γ is a q-ary lattice.

□

Now we consider the case of q is a prime number, hence a linear code C over $\mathbb{Z}_p = \mathbb{F}_p$ is a subspace moreover C has a basis formed by k vector such that the k vectors form a generator matrix. For a linear code C we can write any element a of C using a set of generators as follows:

$$a = \sum_{i=1}^{l} a_i v_i, \;\; v_i = (v_{i1}, \ldots, v_{in}) \;\; \textit{i=1,\ldots, l.}$$

$(l = k)$ for the case of an $[n, k]$-linear code over $\mathbb{F}_p$.
Now for $h_1, \dots, h_n \in \mathbb{Z}$ we have that:

$$a = \sum_{i=1}^{l} a_i v_i \in C \Leftrightarrow \psi^{-1}(a) = \sum_{i=1}^{l} a_i v_i + \sum_{1}^{n} q h_i l_i \in \mathbb{R}$$

with $0 \leq a_i,\ v_{ij} \leq m - 1$ such that for all $i, j\ e_i, i = 1, \dots, n$ form the canonical basis of $\mathbb{R}^n$. Moreover we have that $\psi^{-1}(a)$ is an integral linear combination of $v_1, \dots, v_l, qe_1, \dots, qe_n$. An expanded generator matrix B can be obtained using the next proposition:

Proposition .8. *[11]*

1. *Let Γ_C be a modulo-p lattice then: $p\mathbb{Z}^n \subseteq \Gamma_C \subseteq \mathbb{Z}^n$.*

2. *Let C be an $[n, k]$-linear code over $\mathbb{F}_p$ with generator matrix G. Then the determinant of Γ_C is: $det(\Gamma_C) = p^{n-k}$.*

3. *A generator matrix of Γ_C is:*

$$G_{\Gamma_C} = \begin{pmatrix} G \\ \\ pI_n \end{pmatrix}$$

4. *When the generator matrix G is of the systematic form such that*

$$G = \begin{pmatrix} I_k & A_{k\times(n-k)} \end{pmatrix},$$

then the generator matrix G_{Γ_C} of Γ_C can be reduced to a standard $n \times n$

generator matrix for Γ_C:

$$G_{\Gamma_C} = \begin{pmatrix} I_k & A_{k\times(n-k)} \\ & \\ 0 & pI_{n-k} \end{pmatrix}$$

To obtain an expanded generator matrix B we will proceed as follows:
Put all the column vectors in an $n \times (n+l)$ matrix, then we have to get a row echelon of this matrix. But we are working over lattices and only $\mathbb{Z}$-linear combinations are allowed and only elementary operations on the columns (Addition and subtractions) can be applied. Hence we will replace the notion of reduced echelon form by the notion of Hermite normal form (HNF).
An integer matrix of full row rank is in column Hermite normal form if it is of the form $\begin{pmatrix} H & 0 \end{pmatrix}$ where $H = \begin{pmatrix} h_ij \end{pmatrix}$ is a square matrix such that it satisfies the two next conditions:

1. $h_ij = 0$ for $i < j$
2. $0 \leq h_{ij} < h_{ii}$ for $i > j$

The first condition means that H will be a lower triangle matrix.
The second condition means that its entries are nonnegative and each row has a maximum entry on the diagonal. Note that we can reduce any matrix A with integer entries to a column Hermite normal form, $A = \begin{pmatrix} H & 0 \end{pmatrix} U$, where U is a square unimodular matrix.

Proposition .9. *[11] Let C be a linear code over $\mathbb{Z}_q$ with generators $v_1, \ldots, v_l$*

and let $e_1, \ldots, e_n$ be the canonical basis of $\mathbb{R}$.

A generator matrix for the lattice $\Gamma_C = \psi^{-1}(C)$ is given by

$$\begin{pmatrix} I_k & 0_{l\times(n-l)} \\ & \\ A & qI_{(n-l)} \end{pmatrix}$$

where $\begin{pmatrix} I_k \\ \\ A \end{pmatrix}$ *is the generator matrix of C under systematic from.*

Note that for the case $\mathbb{Z}_p = \mathbb{F}_p$, $l = k$.

Proof. A generator matrix for the lattice $\Gamma_C = \psi^{-1}(C)$ is obtained by the Hermite normal form $\begin{pmatrix} H & 0 \end{pmatrix}$ of $[v_1, \ldots, v_l, qe_1, \ldots, qe_n]$ where $v_1, \ldots, v_l, qe_1, \ldots, qe_n$ generates the lattice.

Now, we have to extract a basis by computing the Hermite normal form from the next matrix:

$$\begin{pmatrix} I_l & qI_k & 0_{l\times(n-l)} \\ \\ A & 0_{(n-l)\times l} & qI_{n-l} \end{pmatrix}$$

If we multiply the first l columns by $-q$ and we add them to the next l columns we get:

$$\begin{pmatrix} I_k & 0_l & 0_{l\times(n-l)} \\ \\ A & -qA & qI_{n-l} \end{pmatrix}$$

Then we multiply the column containing the *ith* 1 of I_{n-l} in turn by a_ij, with $j = 1, \ldots, n-1$ then we will add it to the corresponding column in $-qA$, Hence we will get the desired result. □

Example .4. *[11] Let C be a linear code over $\mathbb{F}_2$ such that:*

$C = \left\{(a_1, \dots, a_{n-1}, \sum_{i=1}^{n-1} a_i); a_1, \dots, a_{n-1} \in \mathbb{F}_2\right\}$

with length n and dimension $n-1$. A systematic generator matrix for Γ_C is given by:

$$\begin{pmatrix} I_{n-1} \\ \\ 1 \dots 1 \end{pmatrix}$$

and a generator matrix for Γ_C is given by:

$$\begin{pmatrix} I_{n-1} & 0_{(n-1)\times 1} \\ \\ 1 \dots 1 & 2 \end{pmatrix}$$

Conclusion

In this chapter, we initiate the construction A of lattices from codes over finite fields. In the next chapter we will give a more general construction A of lattices from codes over number fields.

Chapter 2

Construction A of lattices over number fields

The importance of construction A is due to a series of dualities between theoretical properties of lattices obtained via Construction A and linear codes, for example the theta series of the lattice and the weight enumerator of the code. In this chapter we consider a generalized construction A of lattices over number fields from linear codes. We will show the connection between lattices and codes using number fields that have a prime that totally ramifies and cyclotomic fields. The proofs of this chapter can be found in [28] and [16].

2.1 Number fields

Let K be a finite extension of the field of rational numbers $\mathbb{Q}$. The field K is a number field, let $\{e_1, \ldots, e_n\}$ be a basis that generates K over $\mathbb{Q}$, we say that K

is an extension of degree n over $\mathbb{Q}$ and we write $[K:\mathbb{Q}]=n$.
The element of the basis $\{e_1,\dots,e_n\}$ can be chosen from the ring of integers of K, denoted by $\mathcal{O}_K$ and given as follows:

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

The set $\mathcal{O}_K$ is a commutative ring.
In general, a notion of ideals is studied: fractional ideals which are finitely generated $\mathcal{O}_K$-submodules of K.
The ideals form a commutative group on the set of nonzero prime ideals of $\mathcal{O}_K$ such that each ideal $\mathfrak{a}$ admit a unique representation as a product:

$$\mathfrak{a}=\prod\nolimits_{\pi}\pi^{v_\pi(\mathfrak{a})}$$

where π denotes a prime ideal of $\mathcal{O}_K$ and $v_\pi(\pi)\in\mathbb{Z}$ and $v_\pi(\mathfrak{a})=0$ for almost all π.
We have that since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, fractional ideals are also free $\mathbb{Z}$-modules with rank n; for a prime integer $p\in\mathbb{Z}$, the ideal generated by p in $\mathcal{O}_K$ satisfies:

$$p\mathcal{O}_K=\prod_{i=1}^{g}\pi_i^{e_i},$$

the exponent e_i is the ramification index, and the degree

$$f_i\equiv[\mathcal{O}_K/\pi:\mathbb{Z}_p]$$

is called the inertia degree of π over p.
Moreover, we have:

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

If $e_1=n$ we say that p is totally ramified.
The number field K has exactly n $\mathbb{Q}$-embeddings of K into $\mathbb{C}$. Let $\sigma_1,\dots,\sigma_n$ be this embeddings such that $\sigma_i:K\to\mathbb{C}$ is a field homomorphism that becomes the identity map on $\mathbb{Q}$.

1. We say that K is totally real if $\sigma_i(K)\subseteq\mathbb{R}$ for all i.

2. The field K is said to be a CM field, if there exists $T \subseteq K$, a totally real number field such that $[K:T]=2$ and $\sigma_i(K) \nsubseteq \mathbb{R}\ \forall\ 1 \leq i \leq n$.

3. The field K is a Galois extension of $\mathbb{Q}$, if $\sigma_i(K)=K$ for all i, in this case we have:

$$e_1 = e_2 = \ldots = e_g.$$

We denote this integers e and we say that e is the ramification index of p, similarly we have $f_1 = \ldots = f_n$. we denote this integer f, f is called the inertia degree of p.

The trace map and the norm map of any element $x \in K$ are given as follows:
The trace map:

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

The norm map:

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

Let $\{e_1,\ldots,e_n\}$ be a basis of K over $\mathbb{Q}$. The integer $d_K = det(Tr(e_ie_j))_{i,j=1}^{n}$ is called the discriminant of K.

2.2 A general lattice construction

Let K be a number field and $\pi \in \mathcal{O}_K$ a prime (π is a prime above p).
$\mathbb{F}_{p^f} = \mathcal{O}_K/\pi$ is the residual field. Let C be a linear code over $\mathbb{F}_{p^f}$ of length m and rank k.

Definition .21. *[28] Let $\psi : \mathcal{O}_K^m \rightarrow \mathbb{F}_{p^f}^m$ be the reduction modulo π in each coordinate map. We define a lattice from the code C as follows:*

$$\Gamma_{\mathcal{C}} := \psi^{-1}(\mathcal{C}) \in \mathcal{O}_K^m$$

Now let $\psi^{-1}(\mathcal{C}) \subset \mathcal{O}_K^m$.
We have that C is a subgroup of $\mathbb{F}_{p^f}^m$, then $\psi^{-1}(\mathcal{C})$ is a subgroup of $\mathcal{O}_K^m$. Furthermore, $\psi^{-1}(\mathcal{C})$ is a free $\mathbb{Z}$-module since $\mathcal{O}_K^m$ is a free $\mathbb{Z}$-module of rank nm.

2.3 The case of totally ramified prime

In this section we will give a generator matrix for the lattice Γ_C and its discriminant.
We will focus on the case where K is a Galois extension and the prime π totally ramified. Therefore, we have $p\mathcal{O}_K = \pi^n$, $e = n$ and $f = 1$.
A generator matrix for the lattice Γ_C can be computed using a generator matrix for the lattice formed by $(\mathcal{O}_K, \langle w, z\rangle)$, where $\langle w, z\rangle = \mathrm{Tr}(wz); w, z \in \mathcal{O}_K$ is the standard trace from.

The matrix

$$M = \begin{pmatrix} \sigma_1(v_1) & \sigma_2(v_1) & \dots & \sigma_n(v_1) \\ \vdots & \vdots & & \vdots \\ \sigma_1(v_n) & \sigma_2(v_n) & \dots & \sigma_n(v_n) \end{pmatrix} \tag{2.1}$$

is a generator matrix for the lattice $\mathcal{O}_K$. We know that $MM^T = \mathrm{Tr}_{K/\mathbb{Q}}(v_iv_j)$. Let w be a vector of the lattice $\mathcal{O}_K$ then w is a combination of the rows of M such that $w = \sum_{i=1}^n w_iv_i$, w is embedded in $\mathbb{R}^n$ as $(\sigma_1(\sum_{j=1}^n w_jv_j), \dots, \sigma_n(\sum_{i=j}^n w_jv_j))$, and

$$\langle w, z\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$$

as it should be (when $m = 1$ and $\alpha = 1$ in the bilinear form defined before

Next we derive a generator matrix for the lattice Γ_C. The prime ideal π is a $\mathbb{Z}$-module of rank n. It has a $\mathbb{Z}$-basis $\{u_1, \dots, u_n\}$, where $u_i = \sum_{j=1}^n u_{ij}v_j$, $u_{ij} \in \mathbb{Z}$. The next matrix which is the last step to get a generator matrix for the lattice Γ_C, is the matrix of embeddings of a $\mathbb{Z}$-basis of π:

$$\begin{pmatrix} \sigma_1(u_1) & \dots & \sigma_n(u_n) \\ \vdots & & \vdots \\ \sigma_1(u_n) & \dots & \sigma_n(u_n) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n u_{1j}\sigma_1(v_j) & \dots & \sum_{j=1}^n u_{1j}\sigma_n(v_j) \\ \vdots & & \vdots \\ \sum_{j=1}^n u_{nj}\sigma_1(v_j) & \dots & \sum_{j=1}^n u_{nj}\sigma_n(v_j) \end{pmatrix} = DM$$

where $D = (u_{ij})_{i,j=1}^n$

Proposition .10. *[28] The lattice Γ_C is a sublattice of $\mathcal{O}_K^N$ with discriminant*

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

where $d_K = (det(\sigma_i(w_j))_{i,j=1}^n)^2$ is the discriminant of K.

Proof. Since by definition the bilinear form $\langle u, v\rangle = Tr_{K/\mathbb{Q}}(uv)$, $u, v \in \mathcal{O}_K$ has determinant:

$$d_K = det(MM^T)$$

then the bilinear form $\langle x, y\rangle = \sum_{i=1}^m Tr(x_i y_i)$ has determinant d_K^m over $\mathcal{O}_K^m$.

The map ψ defined above is sutrjective and $\psi^{-1}(C)$ has $(p^r)^{m-k}$ as index, thus

$$disc(\Gamma_C) = d_K^m (p^r)^{2m-2k}$$

is the discriminant of Γ_C. □

Proposition .11. *; [28] Let $\begin{pmatrix} I_k & A \end{pmatrix}$ be a generator matrix of the code C, and M be the matrix of embeddings of $\mathbb{Z}$-basis of $\mathcal{O}_K$. A generator matrix for the lattice*

Γ_C *is given by*

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

Where $\otimes$ is the tensor product of matrices, the matrix DM is the matrix of embeddings of a $\mathbb{Z}$-basis of π.

Proof. From the generator matrix M_C it is clear that this lattice has the right rank.

The embedding of a basis of C correspond to the first nk rows of M_C and the embedding of a basis of π correspond to the last $n(m-k)$ rows of M_C. To make this more precise:

Let $u_i = (u_{i_1}, \ldots, u_{i_n}) \in \mathbb{Z}^n$ where

$$x_i = \sum_{l=1}^{n} u_{il} v_l, i = 1, \ldots, m$$

and we define the canonical embedding of K as follows: $\sigma = (\sigma_1, \ldots, \sigma_n) : \mathcal{O}_K \to \mathbb{R}^n$.

We have that

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

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

where $x_{k+1}^{'}, \ldots, x_m^{'} \in \pi$. Then the above vector is an element of Γ_C.

If we define

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

then applying ρ and ψ componentwise in order gives:

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

we have that $x_i^{'} \equiv 0(mod\ \pi)$, the codeword c of C is given by

$$c = (\psi(\rho(\sigma(x_1))), \ldots, \psi(\rho(\sigma(x_k)))) \cdot \begin{pmatrix} I_k & M \end{pmatrix}$$

by computing the absolute value of the determinant of M_C we get

$$\mid det(M_C) \mid = \sqrt{d_K}^{m} (p^r)^{m-k},$$

This shows that M_C generates a lattice with the same volume as Γ_C. Which complete the proof. □

Next, we propose the case of a totally ramified prime. In this case the matrix A can be easily lifted, because it has coefficient in $\mathbb{F}_p$.

Let $x=(x_1,\dots,x_m)\in\Gamma_C\subset\mathcal{O}_K^m$ for $i=1,\dots,k$, $\sum_{j=1}$, $x_i=\sum_{j=1}^n x_{ij}v_j$.
The above results tell us that x is embedded to $\mathbb{R}^{nm}$ as

$$x=(\sigma(x_1),\dots,\sigma(x_k),\sum_{j=1}^k a_{j,1}\sigma(x_j)+\sigma(x^{'}_{k+1},\dots,\sum_{j=1}^k a_{j,m-k}\sigma(x_j)+\sigma(x^{'}_m))$$

$$=(\sigma_1(x_1),\dots,\sigma_n(x_1),\dots,\sigma_1(x_m),\dots,\sigma_n(x_m))$$

where $x_{k+1}=\sum_{j=1}^k a_{j,1}x_j+x^{'}_{k+1},\dots,x_m=\sum_{j=1}^k a_{j,m-k}x_j+x^{'}_m$. Then,

$$\langle x,y\rangle=\sum_{i=1}^m Tr_{K/\mathbb{Q}}(x_iy_i).$$

Corollary 2. *[28] The matrix*

$$\begin{pmatrix} GG^T\otimes Tr(v_iv_j) & A\otimes Tr(u_iv_j)\\ \\ A^T\otimes Tr(u_iv_j) & I_{m-k}\otimes Tr(u_iu_j)\end{pmatrix}$$

is the Gram matrix of the integral lattice Γ_C, where $u_1,\dots,u_n$ is a $\mathbb{Z}$-basis of π and $G=\begin{pmatrix} I_k & A\end{pmatrix}$.

2.3.1 The case of a totally ramified prime and self-orthogonal codes

Let K be a totally real extension of $\mathbb{Q}$. We have that $\bar{y_i}=y_i$, then we can treat the real and CM-fields at the same time.
Let Γ_C be a lattice defined as in the previous subsection. We have that Γ_C is an integral lattice of rank nm with respect to the bilinear form

$$\langle x,y\rangle=\sum_{i=1}^m Tr_{K/\mathbb{Q}}(\alpha x_iy_i)$$

where α is a totally positive element such that $\alpha \in \mathcal{O}_K \cap \mathbb{R}$. Let C be a self-orthogonal code, i.e. $C \subset C^{\perp}$.

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

Next, we will derive some proposition of the lattice Γ_C when C is self-orthogonal. Let C be an $[m, k]$-linear code over $\mathbb{F}_p$ such that $C \subset C^{\perp}$. Since $\sum_{i=1}^m Tr_{K/\mathbb{Q}}(x_i\bar{y}_i) \in p\mathbb{Z}$, then we can normalize the symmetric bilinear form by choosing α to be $1/p$. The next lemma characterize the case of $\alpha = 1/p$.

Lemma .2. *[28] Let C be an $[m, k]$-self-orthogonal code over $\mathbb{F}_p$. We have that the lattice Γ_C is an integral lattice with respect to the bilinear form $\langle x, y\rangle = \sum_{i=1}^m Tr_{K/\mathbb{Q}}(x_i\bar{y}_i/p)$*

Proof. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ such that $x, y \in \Gamma_C = \psi^{-1}(C)$.

We have that:

$$\psi(x \cdot y) = \psi(\sum_{i=1}^m x_i y_i) = \sum_{i=1}^m \psi(x_i)\psi(y_i) = \psi(x) \cdot \psi(y) = 0 \in \mathbb{F}_p.$$

Thus $\langle x, y\rangle$ is an integer for all $x, y \in \Gamma_C$. and since $\psi(x), \psi(y) \in C$ and $C \subset C^{\perp}$.

It follows that

$$x \cdot y \equiv 0 (mod\ \pi)$$

. Next we have to show that $\bar{y}_i \equiv y_i (mod\ \pi)$ for all $i = 1, \ldots, m$.

Since $\mathcal{O}_K/\pi \simeq \mathbb{F}_p$ and $y_i \in \mathcal{O}_K$, then $y_i = y_i^{'} + y_i^{"}$ for each i, where $y_i^{'} \in \mathbb{Z}$ and $y_i^{"} \in \pi$.

($\bar{\cdot}$ is the automorphism of K induces by complex conjugation).

We have that π is the only prime above p and $y_i^" \in \pi$, then $\bar{y}_i = y_i^{'} + \bar{y}_i^{'} \equiv y_i^{'} + y_i^" \equiv y_i(mod\,\pi)$ as desired. Thus $\sum_{i=1}^m x_iy_i \equiv \sum_{i=1}^m x_i\bar{y}_i \equiv 0(mod\pi)$ and all of conjugates of $\sum_{i=1}^m x_i\bar{y}_i$ must lie in π, therefore $Tr_{K/\mathbb{Q}}(\sum_{i=1}^m x_i\bar{y}_i) \in \pi$, implying that $Tr_{K/\mathbb{Q}}(\sum_{i=1}^m x_i\bar{y}_i) \in \pi \cap \mathbb{Z} = p\mathbb{Z}$, since the trace map is linear, then

$$\langle x, y\rangle = \sum_{i=1}^m Tr_{K/\mathbb{Q}}(x_i\bar{y}_i)/p = \frac{1}{p}Tr_{K/\mathbb{Q}}(\sum_{i=1}^m x_i\bar{y}_i).$$

□

as a result of this lemma, instead of considering the lattice $\psi^{-1}(C)$ with $\langle x, y\rangle = \sum_{i=1}^m Tr_{K/\mathbb{Q}}\frac{x_i\bar{y}_i}{p}$, we can consider the lattice $\psi^{-1}(C)/\sqrt{p}$ with $\langle x, y\rangle = \sum_{i=1}^m Tr_{K/\mathbb{Q}}(x_i\bar{y}_i)$.

The generator matrix for Γ_C in this case is

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

The discriminant of Γ_C is then

$$disc(\Gamma_C) = d_K^m p^{2m-2k-nm}$$

It can be computed directly from the determinant of M_C:

$$disc(\Gamma_C) = (\frac{1}{p})^{nm} d_K^m (p^r)^{2(m-k)} = d_K^m \frac{p^{2(m-k)}}{p^{nm}}.$$

The Gram matrix is:

$$\frac{1}{p}\begin{pmatrix} GG^T \otimes Tr(v_iv_j) & A \otimes Tr(u_iv_j) \\ A^T \otimes Tr(u_iv_j) & I_{m-k} \otimes Tr(u_iu_j) \end{pmatrix}.$$

for more details see [28]

2.3.2 Maximal totally real subfields of cyclotomic fields

In this subsection we will consider the case of cyclotomic fields and their subfields. Then we will consider the case where π is a prime above p.
The prime p is an odd prime such that p totally ramifies in K. Let ζ_{p^r} be a primitive p^rth root of unity and let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, $r \geq 1$ be the maximal totally real subfield of the cyclotomic field $K = \mathbb{Q}(\zeta_{p^r})$, such that:
$\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ is the ring of integers and $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$ is the ring of integers of K and $[K^+ : \mathbb{Q}_p] = \frac{p^{r-1}(p-1)}{2}$.
The ideal $\beta = \langle 1 - \zeta_{p^r} \rangle$ is a principal prime ideal, thus:

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

and $\mathcal{O}_K/\pi \simeq \mathbb{F}$ is the residue field and we write:

$$e(\beta \mid p) = p^{r-1}(p-1)$$

by transitivity of ramification indices.
Now for π the prime above p in K^+ we conclude that
$e(\pi \mid p) = p^{r-1}(p-1)/2$ and $p\mathcal{O}_{K^+} = \pi^{\frac{p^{r-1}(p-1)}{2}}$

Lemma .3. *[28] Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ and let C be an $[m, k]$-code over $\mathbb{F}_p$ such that C is self-orthogonal.*

The lattice Γ_C given by $\psi^{-1}(C)$ together with the bilinear form

$$\langle x, y \rangle = \sum_{i=1}^{m} Tr_{K/\mathbb{Q}}(\alpha x_i y_i)$$

is an integral lattice of rank $mp^{r-1}(p-1)/2$.

The matrix

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

is a generator matrix of the lattice $\Gamma_C = \psi^{-1}(C)$, *where* $G = \begin{pmatrix} I_k & A \end{pmatrix}$ *is a generator matrix of* C.

The ideal $\pi = \left\langle (2 - \zeta_{p^r} - \zeta_{p^r}^{-1}) \right\rangle$ is principal and $\left\{ \zeta_{p^r}^i + \zeta_{p^r}^{-i} \right\}_{i=0}^{n-1}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{K^+}$.
By applying the n embeddings of K $\zeta_{p^r} + \zeta_{p^r}^{-1} \mapsto \zeta_{p^r}^i + \zeta_{p^r}^{-i}$, with i coprime to p, we obtain the matrix M from the Z-basis of $\mathcal{O}_{K^+}$.

Lemma .4. *[28] Consider the field* $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, *and let* C *be an* $[m, k]$*-code over* $\mathbb{F}_p$ *such that* C *is self-orthogonal, then:*

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

Proof. For $x \in \Gamma_C$, $y \in \Gamma_{C^\perp}$. By definition new have that $\psi(x) \in C$ and $\psi(y) \in C^\perp$, it follows that

$\psi(x) \cdot \psi(y) \equiv 0 (mod\ p)$. Then $(x, y) \in \mathbb{Z}$, therefore $\Gamma_{C^\perp} \subset \Gamma_C^*$.

The discriminant of the lattice Γ_C is given by

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

Since $d_{K^+} = p^{(p-1)/2-1}$, then

$$vol(\mathbb{R}^{nm}/\Gamma_C) = (p^{m-2k})^{1/2} = p^{\frac{m}{2}-k}$$

and

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

Since the dimension of $C^{\perp}$ is $m-k$, then

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

Which imply

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

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

Corollary 3. *[28] Let K^+ be a field such that $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let C be an $[m,k]$-code over $\mathbb{F}_p$ such that C is self-orthogonal.Then the lattice $\Gamma_C = \psi^{-1}(C)$ together with the bilinear form $\langle x, y\rangle = \sum_{i=1}^{m} Tr_{K/\mathbb{Q}}(\alpha x_i y_i)$ is an integral lattice of rank $mp^{r-1}(p-1)/2$. In addition, Γ_C is an odd unimodular lattice for C self-dual.*

Proof. Let Γ be a lattice such that Γ contains a vector x with $\langle x \cdot x\rangle$ is an odd integer, then we say that the lattice is an odd integral lattice.

If we take $x = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1}, 0, \dots, 0) \in \Gamma$, we have that

$$\langle x \cdot x\rangle = Tr_{K^+/\mathbb{Q}}((2 - \zeta_{p^r} - \zeta_{p^r}^{-1})^2/p) = \frac{1}{p} Tr_{K^+}/\mathbb{Q}(6 - 4(\zeta_p + \zeta_p^{-1}) + (\zeta_p^2 + \zeta_p^{-2}))$$

Since $\zeta_p + \zeta_p^{-1}$ and $\zeta_p^2 + \zeta_p^{-2}$ are conjugate and

$$Tr_{K+/\mathbb{Q}}(\zeta_p + \zeta_p^{-1}) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)} = 1$$

Then we have $\langle x \cdot x \rangle = \dfrac{6(p-1)}{2p} + \dfrac{3}{p} = 3.$ □

2.4 Construction of Lattices from Codes over $\mathbb{F}_p$

In this section we propose the study of the case $r = 1$ to show the connection between lattices and self-dual codes.

Let C be an $[m, k]$-code over $\mathbb{F}_p$ (p is an odd prime), such that C is self-orthogonal ($C \subset C^{\perp}$). Let $\mathcal{O}_K$ be the ring of integers of the cyclotomic field $K = [\zeta]$.

Definition .22. *The map $\psi : \mathcal{O}_K^m \to \mathbb{F}_p^m$ is the map defined by the reduction modulo the principal ideal $\beta = (1 - \zeta)$ in each coordinate. The preimage of the code C by the map ψ:*

$$\Gamma_C := \psi^{-1}(C) \subset \mathcal{O}_K^m$$

is a lattice.

Let $x, y \in \mathcal{O}_K$ such that $x = (x_1, \ldots, x_n)$ and $y = y_1, \ldots, y_n$ with $x_i, y_i \in \mathcal{O}_K$ for $i = 1, \ldots, n$.

Using the symmetric bilinear form $(x_i, y_i) \mapsto Tr(\dfrac{x_i \bar{y}_i}{p})$ we can define a symmetric bilinear form over $\mathcal{O}_K^m$ as follows:

$$\langle x_i, y_i \rangle = \sum_{i=1}^{m} Tr(\frac{x_i \bar{y}_i}{p}).$$

Since for any $a \in \mathcal{O}_K$, we have $a \equiv \bar{a}(\text{mod } \beta)$, then $x \cdot \bar{y} \equiv x \cdot y(mod\ \beta)$.
by assuming that $\psi(x), \psi(y) \in C$, we have $0 \equiv x \cdot y \equiv x \cdot \bar{y}(mod\ \beta)$. This implies that the lattice Γ_C is an even integral lattice of rank $m(p-1)$, because we have that $\langle x, y\rangle \in \mathbb{Z}$ and $\langle x, x\rangle \in 2\mathbb{Z}$ for all $x, y \in \Gamma_C \subset \mathcal{O}_K^m$.

Proposition .12. *[16] The discriminant of the lattice Γ_C is:*

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

Proof. We have that the map ψ is surjective and $\psi^{-1}(C)$ has index p^{m-k} in $\mathcal{O}_K^m$, with $m = dimC$, moreover the bilinear form $\langle\ ,\ \rangle$ on $\mathcal{O}_K^m$ has determinant $(\frac{1}{p})^n$ then the discriminant of C is p^{m-2k}. □

Lemma .5. *[16]*

Let C be an $[m, k]$-code over $\mathbb{F}_p$ such that $C \subset C^\perp$. Then

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

Proof. For a proof see [16]. □

Proposition .13. *[16] Let C be an $[m, k]$-linear code over $\mathbb{F}_q$ such that C is self-orthogonal, then the lattice formed by the preimage of C by ψ together with the symmetric bilinear form $\langle x, y\rangle = \sum_{i=1}^m Tr(\frac{x_i \bar{y}_i}{p})$ is an even integral lattice of discriminant p^{m-2k} and rank $m(p-1)$. Moreover if C is self-dual then Γ_C is unimodular.*

2.4.1 Theta Function over Number Fields

A theta function is a function from the product of $\frac{p-1}{2}$ upper half planes $\mathbb{H}$ to $\mathbb{C}$. We shall associate a theta function to the lattice Γ_C, for one variable the theta function is given by:

$$v_{\rho+\Gamma}(z) := \sum_{x\in\rho+\Gamma} e^{\pi i z x^2}, z \in \mathbb{H}.$$

For more details see [16].

For our purposes we shall consider a generalized theta function of several variables. Let $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ and let $\mathbf{k} = \mathbb{Q}(\zeta + \zeta^{-1})$ be the real subfield of K, the ring of integers of K is denoted by $\mathcal{O}_K$ and the principal ideal of $\mathcal{O}_K$ is denoted by β such that $\beta = \langle 1 - \zeta\rangle$.

If we identify the lattice Γ_C with the lattice β with symmetric bilinear form $\langle x, y\rangle = Tr_{K/\mathbb{Q}}(\frac{x\bar{y}}{p})$ and we identify the dual lattice with $\mathcal{O}_K$ we get:

$$v_j = \sum_{x\in\beta+j} e^{\pi i z Tr_{K/\mathbb{Q}}(\frac{x\bar{x}}{p})} = \sum_{x\in\beta+j} e^{2\pi i z Tr_{\mathbf{k}/\mathbb{Q}}(\frac{x\bar{x}}{p})}$$

for $i = 0, \ldots, \frac{p-1}{2}$, since we have that $[\mathbf{k} : \mathbb{Q}] = \frac{p-1}{2}$, then there exist exactly $\frac{p-1}{2}$ distinct real embeddings $\sigma_l = \mathbf{k} \to \mathbb{R}$, $l = 1, \ldots, \frac{p-1}{2}$. The embeddings are of the form $\zeta + \zeta^{-1} \mapsto \zeta^a + \zeta^{-a}$, such that $\sigma_l(\mathbf{k}) = \mathbf{k}$.

σ_l form a group called the Galois group of $\mathbf{k}$ over $\mathbb{Q}$ and it is denoted by $Gal(\mathbf{k}, \mathbb{Q})$.

Now we consider the product of $\frac{p-1}{2}$ upper half planes

$$\mathbb{H}^{\frac{p-1}{2}} = \mathbb{H} \times \mathbb{H} \times \ldots \times \mathbb{H}\ (p-1)/2 \textit{ times.}$$

The next step is to define a theta function depending on $\frac{p-1}{2}$ variables $z_l \in \mathbb{H}$ by:

$$\theta_j(z) := \sum_{x\in\beta+j} e^{2\pi i Tr_{\mathbf{k}/\mathbb{Q}}(z\frac{x\bar{x}}{p})},$$

where

$$Tr_{\mathbf{k}/\mathbb{Q}}(z\frac{x\bar{x}}{p}) := \sum_{l=1} z_l \cdot \frac{\sigma_l(x\bar{x})}{p}$$

(The function θ_j is holomorphic in $z \in \mathbb{H}^{(p-1)/2}$)
The group $SL_2(\mathcal{O}_K)$ is the group of all 2×2 matrices:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

where $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$.
The determinant is given by:

$$\alpha\gamma - \beta\gamma = 1.$$

By the definition of the norm given before

$$N_{\mathbf{k}/\mathbb{Q}}(\gamma z + \delta) := \prod_{l=1}^{(p-1)/2} (\sigma_l(\gamma) z_l + \sigma_l(\delta))$$

where $\sigma \in Gal(K, \mathbb{Q})$ we set

$$\sigma(z) = (z_{\varepsilon(1)}, \ldots, z_{\varepsilon(\frac{p-1}{2})})$$

the ε are the permutation of indices $1, \ldots, \frac{p-1}{2}$ such that $\sigma_l \circ \sigma = \sigma_{\varepsilon(l)}$ with $1 \leq l \leq \frac{p-1}{2}$.
for more details see [16] Let Γ be a subgroup of $SL_2(\mathcal{O}_K)$, then we have the next definition:

Definition .23. *[16] We call a holomorphic function $f : \mathbb{H}^{\frac{p-1}{2}} \to \mathbb{C}$ a Hilbert modular form of weight m for Γ, if it is given by:*

$$f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = f(z) \cdot N_{\mathbf{k}/\mathbb{Q}}(\gamma z + \delta)^m$$

for all $\begin{pmatrix} \alpha & \beta \\ \\ \gamma & \delta \end{pmatrix} \in \Gamma$. We say that f is symmetric if we have that

$$f(\sigma(z)) = f(z) \text{ for all } \sigma \in Gal(\mathbf{k}, \mathbb{Q}).$$

See [16]

As we have seen in the previous section that:

$$\pi := \beta \cap \mathcal{O}_K, \textit{ then } \pi = (\zeta + \zeta^{-1} - 2) = ((\zeta - 1)(\zeta^{-1} - 1)$$

and also we have $\pi^{\frac{p-1}{2}} = p$. Now we define:

$$\Gamma(\pi) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathcal{O}_K) \ ; \gamma \equiv (mod\ \pi) \right\}.$$

Then the next theorem hold:

Theorem .8. *[16] The Hilbert modular form $\theta_j, j = 0, 1, \ldots, \frac{p-1}{2}$ is of weight* 1

for the group $\Gamma(\pi)$. Further we have:

$$\theta_0 \left(\frac{\alpha z + \beta}{\gamma z + \delta} \right) = \theta_0(z) \cdot \left(\frac{\delta}{p} \right) \cdot N_{\mathbf{k}/\mathbb{Q}}(\gamma z + \delta) \textit{ for all } \begin{pmatrix} \alpha & \beta \\ \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(\pi).$$

Let C be a self-dual code over $\mathbb{F}_p$ and let Γ_C be the lattice constructed from the code $C \subset \mathbb{F}_p^m$ together with symmetric bilinear form given by $\langle x, y \rangle = \sum_{x \in \Gamma} Tr_{\mathbf{k}/\mathbb{Q}}(\frac{x\bar{x}}{p})$. The lattice Γ is an even unimodular lattice of rank $m(p-1)$, furthermore the theta function of one variable of the lattice Γ_C is given by:

$$v_C = \sum_{x \in \Gamma_C} e^{2\pi i z Tr_{\mathbf{k}/\mathbb{Q}}(\frac{x\bar{x}}{p})}, \textit{ where } z \in \mathbb{H}.$$

Since Γ_C is an $\mathbb{Z}$-module and also an $\mathcal{O}_{\mathbf{k}}$, then we can define a theta function in several variables as follows:

$$\theta_C(z) := \sum_{x \in \Gamma_C} e^{2\pi i Tr_{\mathbf{k}/\mathbb{Q}}(z\frac{x\bar{x}}{p})}.$$

Definition .24. *The Lee weight enumerator of a code $C \subset \mathbb{F}_p^n$ is given by: the*

homogeneous polynomial of degree n:

$$W_C(X_0, X_1, \ldots, X_{\frac{p-1}{2}}) := \sum_{u \in C} X_0^{l_0(u)} X_1^{l_1(u)} \ldots X_{\frac{p-1}{2}}^{l_{(p-1)/2}(u)}$$

with u is the number of zeros in u, and $l_i(u)$, $i = 1, \ldots, \frac{p-1}{2}$ is the number of $+i$ or $-i$ occurring in the codewords u.

Theorem .9. *[16] The theta function θ_C is a Hilbert modular form of weight n for the whole group $SL_2(\mathcal{O}_{\mathbf{k}})$.*

Theorem .10. *Let C be an $[m, k]$-code over $\mathbb{F}_p$ such that $C \subset C^{\perp}$, then:*

$$\theta_C = W_C(\theta_0, \theta_1, \ldots, \theta_{\frac{p-1}{2}}).$$

For a proof see [16].

Example .5. *[16] Let as consider the case of $n = 12$. Let $C \subset \mathbb{F}_3^{12}$ be a self-dual code of length 12, the weight enumerator of C has the form $(\theta_0^4 + 8\theta_0\theta_1^3)3 + a(\theta_1^4 - \theta_1^4 - \theta_0^3\theta_1)^3$.*

Since C is self-dual code, then the weight of every codeword is divisible by 3. We now look for a code C with no codewords of weight 3, to have such a code the coefficient $\theta_0^9\theta_1^3$ must be zero. Therefore we have that:

$$3 \cdot 8 - a = 0,$$

then $a = 24$. Thus the weight enumerator of such a code is the polynomial

$$W_C = (X_0, X_1) = X_0^{12} + 26X_0^6X_1^6 + 440X_0^3X_1^9 + 24X^{12}.$$

This code is the ternary Golay code.

Conclusion

Given a linear code C over $\mathbb{F}_p$, then C can be lifted to a linear code $\tilde{C}$ over a finite chain ring R. Using lifted codes it is possible to construct lattices. In the next chapter we will give a generalized construction A of lattices using lifted codes over finite chain rings.

Chapter 3

Lattices from codes over finite chain rings

Finite chain rings can be defined as non-trivial quotient of ring integers of p-adic fields, this allows us to give a unified treatment valid for all finite chain rings which can be used to construct new lattices from codes over finite chain rings. In this chapter we start by preliminaries over p-adic fields and we conclude this chapter by a lattices construction that can be used to construct self-dual codes over finite chain rings.

3.1 p-adic Fields

In this section we will give some basic definitions on p-adic fields for the proofs and more details see [2] and [27]. Starting by p-adic absolute value and valuation:

3.1.1 Absolute Value:

Definition .25. *Let K be a field. An absolute value over K is an application $|\cdot| : K \to \mathbb{R}^+$ that associate to an element a of K, an element $|a|$ in $\mathbb{R}^+$, such that:*

1) $\forall a \in K, |a| = 0 \Leftrightarrow a = 0;$

2) $\forall a, b \in K, |ab| = |a||b|;$

3) $\forall a, b \in K, |a + b| \leq |a| + |b|.$

And we say that K is an valued field.

Definition .26. *If the absolute value over K satisfies the following condition:*

3') $\forall a, b \in K, |a + b| \leq Max(|a|, |b|)$ *(which stronger then conditon 3 in .25), we say that $|\cdot|$ is an ultrametric absolute value and that K is an ultrametric valued field.*

Definition .27. *Let K be a field. An application $v : K \to \mathbb{R} \cup \{+\infty\}$ is a valuation if it satisfies the next conditions:*

1) $\forall a \in K, v(a) = +\infty \Leftrightarrow a = 0;$

2) $\forall a, b \in K, v(ab) = v(a) + v(b)$;

3) $\forall a, b \in K, v(a+b) \geq Min(v(a), v(b))$,

Proposition .14. *Let K be a field and $w \in]0,1[$.*

1) If v is a valuation over K, then the application $|\cdot|$ defined by $|0| = 0$ and $\forall a \in K - \{0\}$, $|a| = w^{v(a)}$ is an ultrametric absolute value over K.

2) Reciprocally, if $|\cdot|$ is an ultrametric absolute value over K, then the application defined by $v(0) = +\infty$ and $\forall a \in K - \{0\}$, $v(a) = \dfrac{Log|a|}{Log\ w}$ is a valuation over K.

Example .6. *Let*

$$v_0(0) = +\infty,\ v_0(x) = 0 \textit{ for all } x \neq 0 \textit{ in } K.$$

Then v_0 is a valuation of K. It is called the trivial valuation of K.

Example .7. *Let p be a prime number. Each non-zero rational number x can be uniquely written in the form $x = p^e y$, where e is an integer and y is a rational number whose numerator and denominator are not divisible by p. We define a function v_p on the rational field $\mathbb{Q}$ by*

$$v_p(0) = +\infty;\ v_p(x) = e,\ \textit{if } x \neq 0 \textit{ and } x = p^e y \textit{ as above.}$$

Then v_p is a valuation of $\mathbb{Q}$; it is the well-known $p-$adic valuation of the rational field. v_p is the unique valuation on $\mathbb{Q}$ satisfying $v(p) = 1$.

Proposition .15. *Let w fixed in $]0,1[$, v a valuation over a field K and $|\cdot|$ the corespondant absolute value (ie $\forall a \in K - \{0\}, |a| = w^{v(a)}$).*

1) *The set $\mathcal{O}_K = \{a \in K; v(a) \geq 0\} = \{a \in K; |a| \leq 1\}$ is a unitary ring of K called the valuation ring of K.*

2) *If $a \in K$, we have that $a \in \mathcal{O}_K$ or $a^{-1} \in \mathcal{O}_K$.*

3) *$K = \mathcal{F}(\mathcal{O}_K)$ (ie K is the field of fractions of $\mathcal{O}_K$).*

4) *$\mathfrak{m} = \{a \in K; v(a) > 0\} = \{a \in K; |a| < 1\}$ is the unique maximal ideal of the ring $\mathcal{O}_K$. We say that $\mathfrak{m}$ is the ideal of the valuation v and that $\mathcal{O}_K$ is a local ring.*

5) *The set of units of the ring $\mathcal{O}_K$ is:*

   $U(\mathcal{O}_K) = \{a \in K; v(a) = 0\} = \{a \in K; |a| = 1\}$.

Definition .28. *The quotient ring $\mathcal{O}_K/\mathfrak{m}$ is a field. We call this field the residual field of the valuation v. we call residual degree, the dimension of the $\mathbb{F}_p-$vector space $\mathcal{O}/\mathfrak{m}$ is called residual degree and we denote by k with $f_\mathfrak{m} = dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{m})$*

Example .8. *The ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}_p$ is $\mathbb{Z}_p$ and $\mathfrak{m} = p\mathbb{Z}_p$, the residue field for $\mathfrak{m}$ is $\mathbb{F}_p$.*

Hensel's way of writing: Let π be in $\mathfrak{m}$ such that $ord_{\mathfrak{m}}\pi = 1$. Then π is called a uniformizer of $\mathfrak{m}$ or of $\mathcal{O}_K$. For example, for the ring of p-adic integers $\mathbb{Z}_p$, $\pi = p$.
Let $\Xi = \{r_0 = 0, r_1, ..., r_{q-1}\}; q = \mathbb{N}(\pi) = |\mathcal{O}/\mathfrak{m}|$ be a system of representatives of $\mathcal{O}_K/\mathfrak{m}$, in the case of $\mathcal{O}_K = \mathbb{Z}_p$ we have that $\Xi = \{0, 1, 2, ..., p-1\}$ and the set

$$\{\pi^k r_0, \pi^k r_1, ..., \pi^k r_{q-1}\},$$

is a system of representatives for $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ the next lemma show the way of writing for the ring of valuation.

Lemma .6. 1. *Let $\alpha \in \mathcal{O}_K$ then it can be written in a unique way as*

$$\alpha = a_0 + a_1\pi + a_2\pi^2 + ...$$

with $a_i \in \Xi$.

2. *An element of $\alpha \in K$ can be written as*

$$\alpha = a_{-k}\pi^{-k} + a_{-k+1}\pi^{-k+1} + ...$$

3. *The uniformizer generates the ideal $\mathfrak{m}$, such that*

$$\pi^k \mathcal{O}_K = \mathfrak{m}^k.$$

Properties of ultrametric valued fields:

(P1): $\forall n \in \mathbb{N} - \{0,1\}, \forall a_1, ..., a_n \in K$,
$\sum_{i=1}^{n} a_i = 0 \Rightarrow \exists i, j \in \{1, ..., n\}, i \neq j, ; |a_i| = |a_j|$; and
$\sum_{i=1}^{n} a_i = 0 \Rightarrow \exists i, j \in \{1, ..., n\}, i \neq j, ; v(a_i) = v(a_j)$.

(P2): a_n Cauchy's sequence $\Leftrightarrow |a_{n+1} - a_n| \to 0 \Leftrightarrow v(a_{n+1} - a_n) \to \infty$.

(P3): If K is complet, then the series $\sum a_n$ converges if and only if it general term a_n tends to zero.

(P4): If a_n converges, then a_n is a Cauchys sequence.

Remark 3. *Let v be a valuation over K and $|.|$ an ultrametric absolute value over K, then $v(K^*)$ is a subgroup of the group $(\mathbb{R}, +)$ (said the valuation group) and $|K^*|$ is a subgroup of the group $(\mathbb{R}^*, +)$.*

3.1.2 Irreducible polynomial:

We have a criterion of irreducibility (Eisenstein) and a criterion of reducibility (Hensel): obviously, this two criterion are not sufficient to determine the all irreducible polynomials. However, they are valuable for many applications.

Theorem .11. *(Eisenstein criterion) Let K be a valued field, $\mathcal{O}_K$ the valuation ring, $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$ and let P be a monic polynomial with coefficient in $\mathcal{O}_K$:*

$$P(X) = X^n + a_1 X^{n-1} + ... + a_n.$$

If $a_i \in \mathcal{O}_K$ for $i = 1, ..., n$ end $a_n \notin \mathcal{O}_K^2$, the polynomial P is irreducible in $K[X]$.

The polynomials satisfying this criterion is called an Eisenstein polynomial.

Theorem .12. *(Hensel's lemma) Let K be a complete valued field and $P \in \mathcal{O}_K$ a non-zero polynomial, $d =$ degree (P).*

We suppose that there is two monic polynomials g and h in $\mathcal{O}_K[X]$ such as:

$$\bar{P} = \bar{g}\bar{h},\ dg\ g + dg\ h \leq d \text{ and } (\bar{g}, \bar{h}) = 1.$$

Then there exist G and H in $\mathcal{O}_K[X]$ such that:

$$\bar{G} = \bar{g},\ \bar{H} = \bar{h},\ dg\ G = dg\ g \text{ and } P = GH.$$

Recall that $\bar{P}$ means the image of P in $\mathcal{O}_K/\mathfrak{m}[X]$.

Next we will show the existence of the roots of unity over the ring of integers $\mathcal{O}_K$

Corollary 4. *Let K be a valued field, and $q = |\mathcal{O}_K/\mathfrak{m}|$. Then the set U_{q-1} of $(q-1)$th roots of unity belongs to $\mathcal{O}_K$.*

Proof. Let $X^{q-1} - 1$ be a polynomial over the finite field $\mathcal{O}_K/\mathfrak{m}$ with q elements, this polynomial is a product of linear factors, and its roots are exactly the invertible elements of $\mathcal{O}_K/\mathfrak{m}$. By Hensel's lemma, $f \in \mathcal{O}_K[X]$ can be completely factorized and it has $q-1$ roots in $\mathcal{O}_K$. More precisely, we can write

$$X^{q-1}-1=\prod_{\zeta\in\mathcal{O}_K}(X-\zeta)\in\mathcal{O}_K[X].$$

□

3.1.3 Finite algebraic extension of an ultrametric field:

Let K be an ultrametric valued field and L a finite algebraic extension of K, $n=[L:K]$. We denote $\mathcal{O}_L$ the set of element of $x\in L$ satisfying the equation $P(x)=0$ where P is a minimal polynomial, $P\in\mathcal{O}_K[x]$. We also call $\mathcal{O}_L$ the ring of valuation (integer) of L. Let $x\in L$, we denote $N_{L/K}(x)$ (or simply $N(x)$) the determinant of the endomorphism of the $K-$vector space L defined by the multiplication by x. the caracteristic polynomial of this endomorphism is:

$$X^n+...+(-1)^nN(x)$$

is annulled by x in L. It is equivalent to say that x is un integer of L (ie. an element of B) or its normal polynomial is coefficient in $\mathcal{O}_K$. We have also that $\mathcal{O}_K=\mathcal{O}_L\cap K$ we call also the integer of K the element of $\mathcal{O}_K$. The next proposition define the valuation of L.

Proposition .16. *Let K be a complete ultrametric valued field and L an extension of K with degree n, the expression:*

$$w(x)=1/nv(N_{L/K}(x))$$

define the unique valuation w of L extending the valuation v of K.

Lemma .7. *The function $w(x) = 1/nv(N(x))$ is a valuation over L.*

We will now note v the only extension of v to L. by definition, $v(L^*) = 1/nv(K^*)$. If $\Gamma = v(K^*)$ is discrete, $\Gamma \subseteq v(L^*) \subseteq 1/n\Gamma$ trains that Γ is a subgroup of $v(L^*)$, of finite index. Let e be this index, then e divides n.

Definition .29. *The index e of $v(K^*)$ in $v(L^*)$ is called index of ramification of L over K. We call residuel degree of L over K the quotient $f = n/e$. We say that L is totally ramified if $e = n$ and unramified if $e = 1$.*

The totally ramified extensions are described by the next proposition:

Proposition .17. *Let K be a complete ultrametric field with discrete valuation.*

(i) Let P be an Eisenstein polynomial of $K[X]$, P define a totally ramified extension L of K and a root x of P in L is an uniformizer of L.

(ii) Let L be a totally ramified extension of degree n of K and x be an uniformizer of L, the normal polynomial of x in L is an Eseinstein polynomial, and x is of degree n.

Now let L be an extension of K of degree n, then we have:

(i) $\mathcal{O}_L/\mathfrak{m}_L = \mathbb{F}_{p^f}$ we say that f is the inertial degree.

(ii) Let π_K be a uniformizer of K, and π_L a uniformizer of L. Then

$$|\pi_K|_p = |\pi_L|_p^e$$

where e is the ramification index.

(iii) $[L : K] = n = ef$

Theorem .13. *The $\mathcal{O}_K-$module $\mathcal{O}_L$ is free of rank*

$$n = [L : K] = ef.$$

such that if $\alpha_1, ..., \alpha_f \subset \mathcal{O}_K$ is a set where the reductions $\{\overline{\alpha}_i\}$ generates $\mathbb{F}_{p^f}$ as an $\mathbb{F}_p-$vector space, and the set

$$\{\alpha_j \pi_L^k\}_{0 \leq k \leq e, 1 \leq j \leq f}$$

is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Definition .30. *We say that an extension is totally ramified if $f = 1$ i.e.; $n = e$. And is non-ramified if $e = 1$ i.e.; $n = f$.*

3.1.4 Lattices over Integers of p-adic Fields

Let L be a vector space of dimension n over $\mathbb{Q}_p$ and let Λ be a $\mathbb{Z}_p$-submodule of L of finite rank associated by a non-degenerate bilinear form $b : \Lambda \times \Lambda \to \mathbb{Z}_p$. The pair (Λ, b) is called *an integral lattice over L*. The dual lattice of Λ over L is given by

$$\Lambda^* = \{y \in L \ ; b(y, x) \in \mathbb{Z}_p, \forall x \in \Lambda\}.$$

The lattice Λ is a unimodular lattice if $\Lambda = \Lambda^*$. If Λ is a free lattice with a $\mathbb{Z}_p$-basis $\{x_1, \cdots, x_n\}$, then the matrix given by $G = ((x_i, x_j))_{i,j}$ is the generator matrix corresponding to the lattice Λ. For an integral lattice Λ, the discriminant group is $d_\Lambda = \Lambda^*/\Lambda$. If Λ is free, then the discriminant of Λ denoted by $\mathrm{disc}(\Lambda)$ is

$$\mathrm{disc}(\Lambda) = \det(G) = \det((x_i, x_j))_{i,j}.$$

The norm ideal of Λ is the $\mathbb{Z}_p$-ideal generated by $\{b(x,x); x \in \Lambda\}$.

Now, let K be a Galois extension over $\mathbb{Q}_p$ of degree n, K can be seen as a $\mathbb{Q}_p$-vector space of dimension n. Let Ω be an algebraic closure of $\mathbb{Q}_p$. Since K is a separable extension of $\mathbb{Q}_p$, there are n distinct $\mathbb{Q}_p$-embeddings $\sigma_1, \ldots, \sigma_n$ from K into Ω. For an element $\alpha \in K$ the norm and the trace maps are given by

$$\mathrm{N}_{K|\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Tr}_{K|\mathbb{Q}_p}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Note that the $\mathbb{Q}_p$-bilinear symmetric form that associates $(x,y) \in K \times K$ to the element $\mathrm{Tr}_{K|\mathbb{Q}_p}(xy) \in \mathbb{Q}_p$ is non-degenerate.

The ring of integers $\mathcal{O}_K$ of the field K can be considered as the set of those elements in K which are integral over $\mathbb{Z}_p$, then $\mathcal{O}_K$ can be written as

$$\mathcal{O}_K = \mathbb{Z}_p e_1 \oplus \cdots \oplus \mathbb{Z}_p e_n,$$

where $\{e_1, \ldots, e_n\}$ is a free basis of the $\mathbb{Z}_p$-module $\mathcal{O}_K$. Since for $\alpha \in \mathcal{O}_K$ we can write $\alpha e_i = \sum_{j=1}^{n} \alpha_{ij} e_j$, where $\alpha_{ij} \in \mathbb{Z}_p$, then $\mathrm{Tr}_{K|\mathbb{Q}_p}(\alpha)$ is the trace of the $n \times n$ matrix α_{ij} and $\mathrm{Tr}_{K|\mathbb{Q}_p}(x) \in \mathbb{Z}_p$.

As $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank n, with a basis $\{e_1, \ldots, e_n\}$ over $\mathbb{Z}_p$, then a generator matrix of the lattice is written as follows:

$$M = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \vdots & & \vdots \\ \sigma_1(e_n) & \sigma_2(e_2) & \cdots & \sigma_n(e_n) \end{pmatrix}.$$

The discriminant of K over $\mathbb{Q}_p$ is denoted by D_K and it is the discriminant of the lattice $\Lambda_b = (\mathcal{O}_K, b)$, $D_K = \det\left(\mathrm{Tr}_{K|\mathbb{Q}_p}(e_i e_j)_{i,j=1}^{n}\right)$ (see [46]). If I is an ideal of $\mathcal{O}_K$, then I is a $\mathbb{Z}_p$-submodule. The following section considers the ideals of $\mathcal{O}_K$ as lattices by defining ideal lattices which are the general framework for the construction A of lattices [5]. Before that we will introduce one further notion.

Definition .31. *[5] A lattice $\Lambda \in \mathcal{O}_K$ is cyclic if* $\operatorname{rot}(x_1, \cdots, x_{n-1}, x_n) = (x_n, x_1, \cdots, x_{n-1})$ *for every $(x_1, \cdots, x_{n-1}, x_n) \in \Lambda$, where* $\operatorname{rot}(x)$ *is the rotational shift operator in $\mathcal{O}_K$.*

3.1.5 $\mathbb{Z}_p^n$-Ideal Lattices

Let I be an ideal of $\mathcal{O}_K$, note that I is also an $\mathcal{O}_K$-submodule of K different from $\{0\}$. The norm $\mathrm{N}_{K|\mathbb{Q}_p}(I)$ of I is defined as the $\mathbb{Z}_p$-submodule generated by $\mathrm{N}_{K|\mathbb{Q}_p}(x)$ for all $x \in I$.

Lemma .8. *[5] Let I be an ideal of $\mathcal{O}_K$, then $\mathrm{N}_{K|\mathbb{Q}_p}(I) = p^{ri}$ for some $i > 0$.*

Proof. Since $\mathcal{O}_K$ is a principal ideal domain, then every ideal I of $\mathcal{O}_K$ is of the form $I = \langle \pi^i \rangle$; $i > 0$, and $\mathrm{N}_{K|\mathbb{Q}_p}(\langle \pi \rangle) = p$, then $\mathrm{N}_{K|\mathbb{Q}_p}(\langle \pi^i \rangle) = (p^r)^i = p^{ri}$. □

The lattice (I, b_I) associated to the ideal $I \subseteq \mathcal{O}_K$ is called an *ideal lattice*. We have an associated symmetric bilinear form $b_I : I \times I \to \mathbb{Z}_p$ by

$$b_I(x, y) = \mathrm{Tr}_{K|\mathbb{Q}_p}(\alpha x \bar{y}), \ \forall x, y \in I,$$

where α is an element in K such that $\sigma_i(\alpha) > 0$ for all i. A generator matrix of (I, b_I) is given by

$$G_I = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(u_1) & \sqrt{\alpha_2}\sigma_2(u_1) & \cdots & \sqrt{\alpha_n}\sigma_n(u_1) \\ \vdots & \vdots & \cdots & \vdots \\ \sqrt{\alpha_1}\sigma_1(u_n) & \sqrt{\alpha_2}\sigma_2(u_n) & \cdots & \sqrt{\alpha_n}\sigma_n(u_n) \end{pmatrix}$$

Its discriminant is (see [46]) $\operatorname{disc}(\Lambda_I) = \mathrm{N}_{K|\mathbb{Q}_p}(\alpha) \cdot \mathrm{N}_{K|\mathbb{Q}_p}(I)^2 \cdot D_K$.

Ideal lattices for cryptography

Let Γ be a lattice of dimension n in $\mathcal{O}_K^n$. Then we have the property that for every $x = (x_1, \ldots, x_n) \in \Gamma$ the shift $(x_n, x_1, \ldots, x_{n_1})$ belongs to Γ which means that all shifts of $(x_1, \ldots, x_n)$ must be in Γ.

Lemma .9. *[5] A lattice Γ in $\mathcal{O}_K^n$ is cyclic if Γ is an ideal of $\mathcal{O}_K/(x^n - 1)$.*

Proof. Let $a = (a_1, \ldots, a_n)$, we associate to a a polynomial in $\mathcal{O}_K[x]$ as follows:

$$p(x) = a_1 + a_2x + a_3x^2 + \ldots + a_nx^{n-1}$$

Since the degree of $p(x)$ is less than n, then $p(x)$ to $\mathcal{O}_K[x]/(x^n - 1)$. Moreover we have that Γ is an ideal, then it is closed under multiplication. Therefore, by multiplying $p(x)$ by x we get:

$$(a_1 + a_2x + a_3x^2 + \ldots + a_nx^{n-1})x = a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n,$$

but we have that $x^n \equiv 1$ in $\mathcal{O}_K[x]/(x^n - 1)$, then

$$(a_1 + a_2x + a_3x^2 + \ldots + a_nx^{n-1})x \equiv a_1x + a_2x^2 + a_3x^3 + \ldots + a_n.$$

Therefore, $(a_{n-1}, a_1, \ldots, a_n) \in \Gamma$ as desired. □

Cyclic ideal lattices have been considered to build efficient cryptographic primitives and homomorphic encryption schemes. To give a generalization, we will consider a polynomial $p(x) \in \mathcal{O}_K[x]$ different then $x^n - 1$. In the literature the family that has been considered is that of cyclotomic polynomials.
The q-th cyclotomic polynomial is given by:

$$\phi_q(x) = \prod_{\zeta \in \mathcal{O}_K} (x - \zeta) \in \mathcal{O}_K[x]$$

where the roots of ϕ_q are exactly the invertible elements of $\mathcal{O}/\pi$. If q is prime, then

$$\phi_p(x) = \frac{x^p - 1}{x - 1}$$

if q is a power of 2, then we have that $\phi_q(x) = x^{q/2} + 1$, Hence:

$$\mathcal{O}_K[x]/(\phi_p(x)) \simeq \mathcal{O}_K[\zeta_q] \subset \mathbb{Q}_p(\zeta_q) \simeq \mathcal{O}_K(x)/(\phi_p(x))$$

where ζ_p is the q-th primitive root of unity, such that:

$$\mathbb{Q}_q(\zeta_q) = \{a_1 + a_2\zeta + \ldots + a_{d-1}, a_1, \ldots, a_{d-1} \in \mathbb{Q}_p\}$$

with $d = \varphi(n)$ is the Euler totient of n.

Remark 4. *The notions of cyclotomic polynomials and "ideal lattices" coincide in the quotient $\mathcal{O}_K[x]/(x^n - 1)$.*

3.2 p-adic fields and finite chain rings

3.2.1 Construction of finite chain rings using p-adic fields

A commutative ring with identity is called a chain ring if its ideals form a chain under inclusion. A finite chain ring, roughly speaking, is an extension over a

Galois ring of characteristic p^n using an Eisenstein polynomial. Let R be a finite commutative chain ring with maximal ideal M. The residue field R/M is a finite field $GF(p^r)$. The characteristic of R is a power of p, say, p^n. All the ideals of R are powers of M. Let s be the nilpotency of M and we write $pR = M^e$ $(e \leq s)$ and $s = (n-1)e + t$, where $t = e$ when $n = 1$ and $1 \leq t \leq e$ when $n > 1$. The integers (p, n, r, e, t) are called the invariant of R. Let $GR(p^n, r)$ be the Galois ring of characteristic p^n and rank r, i.e., $GR(p^n, r) = \mathbb{Z}_{p^n}[X]/(f)$, where $f \in \mathbb{Z}_{p^n}[X]$ is a monic polynomial of degree r whose image in $\mathbb{Z}_{p^n}[X]$ is irreductible. Then every finite commutative chain ring is of the form

$$R = GR(p^n, r)[X]/(g, p^{n-1}x^t),$$

where $g \in GR(p^n, r)[X]$ is an Eisensein polynomial of degree e, i.e.,

$$g = x^e - p(a_{e-1}x^{e-1} + ... + a_0), \;\; a_i \in GR(p^n, r), a_0 \in GR(p^n, r)^{\times}.$$

Finite commutative chain rings can be also constructed from the $p-$adic fields. Choose a prime p, positive integers n, f, and a monic polynomial $\phi \in (\mathbb{Z}/p^n\mathbb{Z})[X]/(\phi)$ (the Galois ring of characteristic p^n and rank f) it is determind up to isomorphism by p, n, and f. Every finite commutative chain ring is isomorphic to a ring of the form $R[X]/(\Psi, p^{n-1}X^t)$, where $R = GR(p^n, f)$ is a Galois ring, $\Psi \in R[X]$ is an Eisenstein polynomial of degree e, and

$$t = e \;\; if \; n = 1,$$

$$1 \leq t \leq e \;\; if \; n \geq 2.$$

The integers p, n, f, e, t are called the invariants of the commutative chain ring. The following proposition summarize the connections between finite commutative chain rings and $p-$adic fields.

Proposition .18. *[26], [25] Let $K/\mathbb{Q}_p$ be a finite extension with residue degree r and ramification index s. Let $\mathcal{O}_K$ the ring of integer of K and π be an uniformizer* *of K, then $R = \mathcal{O}_K/\pi^{(n-1)e+t}\mathcal{O}_K$ is a finite chain ring, and we have $|R| = p^n$ and $|\overline{R}| = p^r$ where*

p^n is the characteristic of R

$p^r = |R/\langle\pi\rangle|$

e is the degree of the Eisenstein polynomial h such that $h(\pi) = 0$

$s = (n-1)e + t$, $1 \leq t \leq e$. nilpotency index of π.

The proof of this proposition follows immediately from the next well-known results

(i) Let $a \in \mathcal{O}_k$ be such that $\bar{k} = (\mathbb{Z}/p\mathbb{Z})[\bar{a}]$, where $\bar{a}$ is the image of a in $\bar{k}$, and let $\Phi \in \mathbb{Z}_p[X]$ be the minimal polynomial of a over $\mathbb{Q}_p$. Then the image $\tilde{\Phi}$ of Φ in $(\mathbb{Z}/p\mathbb{Z})[X]$ is monic of degree $f$and the image $\bar{\Phi}$ of $\tilde{\Phi}$ in $(\mathbb{Z}/p^n\mathbb{Z})[X]$ is irreductible.
Therefore
$$\mathcal{O}_k/p^n\mathcal{O}_k \cong GR(p^n, f).$$

(ii) The minimal polynomial of π_K over k is an Eisenstein polynomial $\Psi \in \mathcal{O}_k[X]$ of degree e such that
$$\mathcal{O}_K/\pi_K^s\mathcal{O}_K \cong (\mathcal{O}_k/p^n\mathcal{O}_k)[X]/(\tilde{\Psi}, p^{n-1}X^t) \cong GR(p^n, f)[X]/(\Psi, p^{n-1}X^t),$$
where
$$\tilde{\Psi} \in (\mathcal{O}_k/p^n\mathcal{O}_k)[X] \cong GR(p^n, f)[X]$$
is an Eisenstein polynomial over $GR(p^n, f)$
Thus $\mathcal{O}_K/\pi_K^s$ is a finite commutative chain ring with invariants
$$(p, 1, f, t, t) \text{ } \textit{if } n = 1,$$

$$(p, n, f, e, t) \textit{ if } n > 1.$$

Moreover, every finite chain commutative chain ring is isomorphic to $\mathcal{O}_K/\pi_K^s\mathcal{O}_K$ for some finite extension $K/\mathbb{Q}_p$ and some $s \geq 1$.

the integers p, n, r, e and t are called the invariant of R. And the ideals of R form the following chain:

$$\langle 0\rangle = \langle \pi^s\rangle \subsetneq \langle \pi^{s-1}\rangle \subsetneq ... \subsetneq \langle \pi\rangle \subsetneq \langle \pi^0\rangle = R$$

The next conditions are equivalent for any finite chain ring:

Proposition .19. *(i) R is a local ring and and the maximal ideal M is principal.*

(ii) R is a local principal ideal ring.

(iii) R is a chain ring.

Definition .32. *The quotient $R/\langle\pi\rangle$ is called the residue field of R and we denote it by $\overline{R}$.*

We define the natural ring homomorphism from $R[x]$ into $\overline{R}[x]$ as follow:

$$\mu : R[x] \to \overline{R}[x] \tag{3.1}$$

$$\sum_{i=0}^{n-1} a_i x^i \mapsto \overline{f} = \sum_{i=0}^{n-1} \overline{a}_i x^i. \tag{3.2}$$

$$\tag{3.3}$$

where $a_i \in R$. The ideals of R are of the form $\langle \pi^i \rangle$, we can compute the cardinality of $\langle \pi^i \rangle$ from the cardinality of $\overline{R}$: $|\langle \pi^i \rangle| = |\overline{R}|^{s-i}$, and so the cardinality of R;

$$\begin{aligned} |R| =& |\overline{R}| \cdot |\langle \pi \rangle| \\ =& |\overline{R}| \cdot |\overline{R}|^{s-1} \\ =& |\overline{R}|^{s} = p^{sr} \end{aligned}$$

The next definition collect the definitions of coprime polynomials, basic irreductible polynomial, and regular polynomial.

Definition .33. *i) Two polynomials $f, g \in R[x]$ are coprime if there exist $u, v \in R[x]$ such that $uf + vg = 1$.*

ii) We say that a polynomial $f \in R[x]$ is basic irreducible if its image in $\overline{R}[x]$ i.e.; μf is irreducible.

iii) $f \in R[x]$ is regular if $\mu f \neq 0$ i.e.; f is not a divisor of zero.

Let T be the set of $f \in R[x]$ that has distinct zeros in the algebraic closure of $\overline{R}[x]$. the following proposition gives the relation between irrducibility and basic irreducibility of regular polynomials.

Proposition .20. *Let $f \in R[x]$ be a regular polynomial, the next conditions are equivalent:*

i) f is basic irreducible then $\overline{f}$ is irreducible.

ii) If f is irreducible then $\overline{f} = ug^k$, where $u \in \overline{R}$ and g is a monic irreducible in $\overline{R}[x]$.

iii) If f is in T then f is irreducible if and only if f is basic irreducible.

3.3 Lifted codes over finite chain rings

Let π be a uniformizer of the valuation ring $\mathcal{O}_K$. For each $i \leq n$ we define

$$R_i = \mathcal{O}_K/\pi^i\mathcal{O}_K = \{a_0 + a_1\pi^1 + \ldots + a_{i-1}\pi^{i-1} \mid a_i \in E'\},$$

where E' is a complete set of representatives of the residue field $\mathbb{F}_{p^r} = \mathcal{O}_K/\pi\mathcal{O}_K$ in $\mathcal{O}_K$ containing 0.
Since every finite chain ring is isomophic to a nontrivial quotient of rings of integers of p-adic fields, then the ring R_i is a finite chain ring with maximal ideal $\langle\pi\rangle$. The *ring of formal power series in π* with coefficient in a finite chain ring R is defined to be

$$R[[\pi]] = \left\{ a(x) = \sum_{i=0}^{\infty} a_i\pi^i \mid a_i \in R \textit{ for all } i \in \mathbb{N} \right\},$$

where addition and multiplication operators are defined as usual. We have that the uniformizer of the valuation ring $\mathcal{O}_K$ is the generator of the maximal ideal of the finite chain ring R_i, then:

Theorem .14. *[5] The ring of formal power series in π with coefficients in a nontrivial quotient rings of integers of K is the ring of integers of K, that is $R_\infty = \mathcal{O}_K$.*

Proof. Every element $\alpha \in \mathcal{O}_K$ can be written in a unique way as $\alpha = \sum_{j=0}^{\infty} b_j \pi^j$ where $b_j \in E'$, then:

$$R_\infty = \left\{ \sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} b_j \pi^j \right) \pi^i \right\} = \left\{ \sum_{s=0}^{\infty} \left(\sum_{i+j=s} b_{ij} \right) \pi^s ; b_{ij} \in E' \right\}.$$

Consider $a_s = \sum_{i+j=s} b_{ij}$ with $b_{ij} \in E'$, then $\sum_{i+j=s} b_{ij}$ with $b_{ij} \in E'$ is a finite sum. Therefore:

$$R_\infty = \left\{ \sum_{s}^{\infty} a_s \pi^s ; a_s \in E' \right\} = \mathcal{O}_K.$$

□

The chain of ideals of $\mathcal{O}_K$ is given as (see [27]) $\{0\} \subset \cdots \langle \pi^n \rangle \subset \cdots \subset \langle \pi^2 \rangle \subset \langle \pi \rangle \subset \langle \pi^0 \rangle = \mathcal{O}_K$. Thus R_∞ satisfies the ascending chain condition, which means that $R_\infty = \mathcal{O}_K$ is a Noetherian ring. Moreover, it is an Euclidean domain (and therefore is a Dedekind domain). Indeed, if a and $b \neq 0$ are in R_∞, then there are q and r in R_∞ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$, where f is a function from R_∞ to $\mathbb{Z}^+$. Moreover, $V : R_\infty \to \mathbb{Z}^+$ is the function defined by $V(0) = 0$ and $V(r) = v(r)$ if $r \neq 0$.
If $v(a) \geq v(b)$, then $v(a/b) = v(a)_v(b) \geq 0$ and if $q = a/b \in R_\infty$, then $r = 0$. Thus, if $v(a) < v(b)$, then $q = 0$ and $r = a$.

A submodule $\mathcal{C}$ of rank k over R_∞^m is called *π-adic code of length m* and rank k. Let $\mathcal{C}$ be a nonzero linear code over R_∞ of length m, then any generator matrix of $\mathcal{C}$ is permutation-equivalent to a matrix of the following form

$$G = \begin{pmatrix} \pi^{m_0} I_{k_0} & \pi^{m_0} A_{0,1} & \pi^{m_0} A_{0,2} & \pi^{m_0} A_{0,3} & & & \pi^{m_0} A_{0,z} \\ & \pi^{m_1} I_{k_1} & \pi^{m_1} A_{1,2} & \pi^{m_1} A_{1,3} & & & \pi^{m_1} A_{1,z} \\ & & \pi^{m_2} I_{k_2} & \pi^{m_2} A_{2,3} & & & \pi^{m_2} A_{2,z} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \pi^{m_{z-1}} I_{k_{z-1}} & \pi^{m_{z-1}} A_{z-1,z} \end{pmatrix} \tag{3.4}$$

The code $\mathcal{C}$ with generator matrix of this form is said to be of type $(\pi^{m_0})^{k_0}(\pi^{m_1})^{k_1}\cdots(\pi^{m_{z-1}})^{k_{z-1}}$, where $k = k_0 + k_1 + \cdots + k_{z-1}$ is called its rank and $k_z = m - k$.

For two integers $i < j$, we define a map as in [15]:

$$\begin{array}{cccc} \Psi_i^j : & R_j & \to & R_i \\ & \sum_{l=0}^{j-1} a_l \pi^l & \mapsto & \sum_{l=0}^{i-1} a_l \pi^l. \end{array} \tag{3.5}$$

If R_j is replaced with R_∞, then Ψ_i^∞ is denoted by Ψ_i. For any two elements $a, b \in R_\infty$ we have that $\Psi_i(a + b) = \Psi_i(a) + \Psi_i(b)$, $\Psi_i(ab) = \Psi_i(a)\Psi_i(b)$. The two maps Ψ_i and Ψ_i^j can be extended naturally from R_∞^m to R_i^m and R_j^m to R_i^m respectively.

Remark 5. *based on the above construction in (3.5) the following series of chain rings is obtained:*

$$R_\infty \to \cdots \to R_s \cdots \to R_{s-1} \to R_l \to \cdots \to R_1$$

Note that $R_1 = \mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{F}_{p^r}$, $R_l = \mathcal{O}_K/\pi^l\mathcal{O}_K$, $R_{s-1} = \mathcal{O}_K/\pi^{s-1}\mathcal{O}_K$ *and* $R_s = \mathcal{O}_K/\pi^s\mathcal{O}_K$.

The following definition gives the lifts of a code $\mathcal{C}$ over a finite chain ring which are defined in a similar way as described in [15] but using this more general setting.

Definition .34. *[5] Let i, j be two integers such that $1 \le i \le j < \infty$. An $[m, k]$-code C_1 over R_i lifts to an $[m, k]$ code C_2 over R_j, denoted by $\mathcal{C}_1 \le \mathcal{C}_2$, if $\mathcal{C}_2$ has a generator matrix G_2 where $\Psi_i^j(G_2)$ is a generator matrix of $\mathcal{C}_1$.*

It can be proven (the proof in [15] can be followed in our general setting) that $\mathcal{C}_1 = \Psi_i^j(\mathcal{C}_2)$. If $\mathcal{C}$ is an $[m, k]$-π-adic code, then for any $i < \infty$, $\Psi_i(\mathcal{C})$ will be called *the projection* of $\mathcal{C}$. The image $\Psi_i(\mathcal{C})$ is denoted by C^i and we have the following result:

Lemma .10. *[5] Let $\mathcal{C}$ be a linear code over R_i and $\tilde{\mathcal{C}}$ be the lifted code of $\mathcal{C}$ over R_j, where $i < j \leqslant \infty$. Hence if $\mathcal{C}$ is free over R_i, then $\tilde{\mathcal{C}}$ is free over R_j.*

3.4 Lattices and Codes over Finite Chain Rings

3.4.1 Construction A of Lattices

Let $R = \mathcal{O}_K/\pi^s\mathcal{O}_K$ be a finite chain ring defined as in Section 3.2 and let $\mathcal{C}$ be a code over the ring R of length m. We consider the map $\Psi : \mathcal{O}_K \to R$ the reduction modulo the prime π^s such that the preimage of $\mathcal{C}$ by Ψ is the lifted code of $\mathcal{C}$ over $\mathcal{O}_K$. Then, $\Psi^{-1}(\mathcal{C})$ is an $\mathcal{O}_K$-module of finite rank and since $\Psi^{-1}(\mathcal{C})$ is a $\mathbb{Z}_p$-submodule, then a lattice can be described as follows:

Definition .35. *[5] Given a code $\mathcal{C}$ over the finite chain ring $R = \mathcal{O}_K/\pi^s\mathcal{O}_K$ and the symmetric bilinear form $b_{\mathcal{C}} = \sum_{i=1}^m \mathrm{Tr}_{K|\mathbb{Q}_p}(\alpha x_i \bar{y}_i)$ where $\alpha \in \mathcal{O}_K$ the lattice $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ is defined as the preimage $\Psi^{-1}(\mathcal{C})$ of $\mathcal{C}$ in $\mathcal{O}_K^m$ together with the symmetric bilinear form $b_{\mathcal{C}}$.*

Lemma .11. *[5] The lattice $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ is an integral lattice.*

Proof. Let $x, y \in \mathcal{O}_K^m$, then $Tr_{K/\mathbb{Q}_p}(x_i\bar{y}_i) \in \mathbb{Z}_p$ for all $i = 1, \ldots, m$. Since $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}(\alpha x_i y_i)$ belongs to $\mathbb{Z}_p$, thus, $b_{\mathcal{C}}(x, y) \in \mathbb{Z}_p$ and therefore, $\Lambda_{\mathcal{C}}$ is an integral lattice. □

The dual lattice of $(\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ is the pair $\Lambda^*_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C})^*, b_{\mathcal{C}})$ defined as follows:

$$\Psi^{-1}(\mathcal{C})^* = \{x \in K^m \ ; b_{\mathcal{C}}(x, y) \in \mathbb{Z}_p, \forall y \in \Psi^{-1}(\mathcal{C})\}.$$

Let A and B be two finite $\mathcal{O}_K$-modules such that $B \subset A$, then the quotient A/B is a module of finite rank. The invariant of A/B denoted by $\chi(A/B)$(see [46]) is a non-zero ideal of A. The following statement is straightforward.

Proposition .21. *[5] Let $\Lambda_{\mathcal{C}}$ be the integral lattice defined above. The discriminant of $\Lambda_{\mathcal{C}}$ is*

$$\mathrm{disc}(\Lambda_{\mathcal{C}}) = \mathrm{N}_{K/\mathbb{Q}_p}(\alpha)^m \cdot D_K^m \cdot \mathrm{N}_{K/\mathbb{Q}_p}(\chi(\mathcal{O}_K^m/\mathcal{C}))^2.$$

If $\mathcal{C}$ is a free code, then the lifted code given as the preimage of $\mathcal{C}$ by Ψ is also free, thus $\Psi^{-1}(\mathcal{C})$ is isomorphic as a module to $\mathcal{O}_K^k$, where $k = k(\Psi^{-1}(\mathcal{C}))$ is the rank of the lifted code of $\mathcal{C}$. Then, the following result follows.

Corollary 5. *[5] For a free code $\mathcal{C}$ the discriminant of $\Lambda_{\mathcal{C}}$ is*

$$\mathrm{disc}(\Lambda_{\mathcal{C}}) = D_K^m (p^r)^{2(m-k)}.$$

If we let $K|\mathbb{Q}_p$ be a Galois extension and the prime π is chosen so that π is totally ramified, therefore, we have $n = e$, $f = 1$, and $\pi^n = p$, and let $\mathcal{C}_i$ be a self-orthogonal code of length m over a finite chain ring $R_i = \mathcal{O}_K/\pi^s\mathcal{O}_K$. Then, we have the following result.

Lemma .12. *[5] The lattice formed by the lifted code of a self-orthogonal code $\mathcal{C}_i$*

over $R_i = \mathcal{O}_K/\pi^i\mathcal{O}_K$ is integral with respect to the bilinear form given by

$$b_{\mathcal{C}_i} = \sum_{i=1}^{m} \mathrm{Tr}_{K|\mathbb{Q}_p}(x_i\bar{y_i}/p).$$

Proof. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ in $\Lambda_{\mathcal{C}}$, then:

$$\Psi(x \cdot y) = \Psi\left(\sum_{i=1}^{m} x_i y_i\right) = \sum_{i=1}^{m} \Psi(x_i)\Psi(y_i) = \Psi(x) \cdot \Psi(y) = 0.$$

Since $\Psi(x) \cdot \Psi(y) \in \mathcal{C}$ and $\mathcal{C} \subset \mathcal{C}^{\perp}$, then:

$$\sum_{i=1}^{m} x_i y_i = x \cdot y \equiv 0 \mod \pi^s.$$

Since π is the only prime above p, all conjugates of $\sum_{i=1}^{m} x_i y_i$ must lie in π and thus this is also true for its trace. In other words, $\mathrm{Tr}_{K|\mathbb{Q}_p}(x_i\bar{y_i}) \in \pi^s$, thus $\mathrm{Tr}_{K|\mathbb{Q}_p}(x_i\bar{y_i}) \in p\mathbb{Z}_p$. Therefore, by the linearity of the trace we have:

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

and $\Lambda_{\mathcal{C}}$ is integral. □

Example .9. *Let us consider lattices over integers of p-adic cyclotomic fields as follows. Let L be the field obtained from $\mathbb{Q}_p$ by adjoining a pth root of unity ζ, where $[L : \mathbb{Q}_p] = p - 1$. The ring of integers of L is given by the set*

$$\mathcal{O}_L = \left\{\alpha = \sum_{i=0}^{p-2} a_i\zeta^i \ ; \ \alpha_i \in \mathbb{Z}_p \text{ for } i = 0, 1, \cdots, p-2\right\}.$$

Note that the principal ideal of $\mathcal{O}_L$ is $\mathfrak{m}_L = \langle 1-\zeta \rangle$. There exist $p-1$ distinct embeddings $\sigma_i : L \to \mathbb{C}_p$, the trace of an element $\alpha \in L$ over $\mathbb{Q}_p$ is $\mathrm{Tr}_{L|\mathbb{Q}_p}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha)$. Therefore, $\mathrm{Tr}_{L|\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$.

For $x \in \mathbb{Q}_p(\zeta)$ $\bar{x}$ denotes the complex conjugate. We consider the symmetric bilinear form $(x,y) \mapsto \mathrm{Tr}_{L|\mathbb{Q}_p}(x\bar{y})$.

Now, let l be the subfield of L such that $l = \mathbb{Q}_p(\zeta + \zeta^{-1})$ then $[L : l] = 2$ and $[l : \mathbb{Q}_p] = \dfrac{p-1}{2}$. Moreover, $\mathrm{Tr}_{L|\mathbb{Q}_p}(x\bar{x}) = 2\mathrm{Tr}_{l|\mathbb{Q}_p}(x\bar{x})$. This shows that the bilinear form above is even.

Finally, consider $\mathcal{C}$ a code over the finite chain ring $R \simeq \mathcal{O}_L/(1-\zeta)^s\mathcal{O}_L$. The lattice formed by the preimage of $\mathcal{C}$ over $\mathcal{O}_L$ associated with the bilinear form $\mathrm{Tr}_{L|\mathbb{Q}_p}$ is integral, because $\mathrm{Tr}_{L|\mathbb{Q}_p}(x) \in \mathbb{Z}_p$ then is also even. Therefore, the lattice is unimodular.

3.4.2 The case of cyclic codes

A cyclic code of length m over the ring of integers $\mathcal{O}_K$ is a linear code $\mathcal{C}$ such that if $(c_0, c_1, \cdots, c_{m-1}) \in \mathcal{C}$, then $(c_{m-1}, c_0, \cdots, c_{m-2}) \in \mathcal{C}$. The codewords of a cyclic code over $\mathcal{O}_K$ are represented as usual by polynomials, more precisely they are the ideals of the ring $\mathcal{O}_K/\langle x^n - 1\rangle$. We propose in this subsection a general construction of lifting cyclic codes which generalizes the construction given in [42]. This general construction allows to lift cyclic codes over finite fields $\mathbb{F}_{p^r}$ to finite chain rings and to the ring of integers $\mathcal{O}_K$ and the case of cyclic lattices will be treated. We will need the Hensel's lemma for the construction. Its proof can be found in [40].

Theorem .15. *(Hensel's Lemma) [5] Let K be a finite extension of $\mathbb{Q}_p$ of degree n, and let $\mathcal{O}_K$ be the ring of integers of K with maximal ideal $M = \langle \pi \rangle$ and residue field $k := \mathcal{O}_K/\langle \pi \rangle$. Let $f \in \mathcal{O}_K[x]$ and let $\overline{f}$ be its image in $k[X]$. Let $\overline{g}$, $\overline{h}$ be two coprime polynomials of $k[x]$ such that $\overline{f} = \overline{g}\overline{h}$, then there exist g, $h \in \mathcal{O}_K[x]$ for which $f = gh$ and $g \equiv \overline{g}[\pi]$ and $\overline{h} \equiv h[\pi]$ with deg $g =$ deg $\overline{g}$.*

It is well known that if $\mathcal{C}$ is a cyclic code of length m over the finite field $\mathbb{F}_{p^r} = \mathcal{O}_K/\langle \pi \rangle$ then, $\mathcal{C}$ is generated by a monic factor $g(x)$ of $x^m - 1 = \overline{g}(x)\overline{h}(x)$. Taking into account Hensel's Lemma, any decomposition modulo π can be generalized to a decomposition modulo π^s by $x^n - 1 = g_s(x)h_s(x)[\pi^s]$ and therefore to $\mathcal{O}_K$ as $x^m - 1 = g(x)h(x)$. If we consider now $\mathcal{C}$ a cyclic code over a finite chain ring R we have the following result.

Theorem .16. *[5] Let $\mathcal{C}$ be a cyclic code over R. The lattice $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ is a cyclic lattice of $\mathcal{O}_K$.*

Proof. We have that a lattice Λ in $\mathcal{O}_K^m$ is cyclic if Λ is an ideal of $\mathcal{O}_K[x]/(x^m - 1)$, and since $\Psi^{-1}(\mathcal{C})$ is a cyclic code of $\mathcal{O}_K$, it means that $\Psi^{-1}(\mathcal{C})$ is an ideal of $\mathcal{O}_K[x]/(x^m - 1)$ then the lattice $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ is cyclic. □

Corollary 6. *[5] Let $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b_{\mathcal{C}})$ be a cyclic lattice in $\mathcal{O}_K$, then $\mathcal{C}$ is a cyclic code.*

Thus we can construct cyclic codes over finite chain rings easily using cyclic lattices over $\mathcal{O}_K$.

Example .10. *Let $L = \mathbb{Q}_{p^r}$ be the unramified extension of $\mathbb{Q}_p$ of degree r obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^r - 1)$st root of unity. The ring of integers of L is denoted by $\mathcal{O}_L$, the maximal ideal is given by $\mathfrak{m} = \langle p \rangle$ and the residue field is $\mathbb{F}_{p^r}$. Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{p^r} = \mathcal{O}_L/(p)$, then $\mathcal{C}$ is generated by a monic factor $g_r(x)$ such that $x^m - 1 = g_r(x)h_r(x)$. Using the Hensel's Lemma any class of cyclic codes can be generalized from $\mathbb{F}_{p^r}$ to $\mathcal{O}_L$ by $x^m - 1 = g(x)h(x)$. Then, the lattice formed by the lifted code of $\mathcal{C}$ is a cyclic lattice over $\mathcal{O}_L$.*

3.4.3 Lattices over p-adic Cyclotomic Fields

Now, we propose the construction A from codes over finite chain rings to p-adic cyclotomic fields and their subfields using the same steps in Lemma 2 and Lemma 3 from [28]. This construction can be used to construct self-dual codes over finite chain rings.

Let p be an odd prime and let ζ_{p^r} be the p^rth primitive root of unity. We consider $l = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1})$ the subfield of the cyclotomic field $L = \mathbb{Q}_p(\zeta_{p^r})$. Hence the rings $\mathcal{O}_l = \mathbb{Z}_p[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ and $\mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^r}]$ are respectively their rings of integers. The prime p totally ramifies in l and the degree of l over $\mathbb{Q}_p$ is $[l : \mathbb{Q}_p] = \dfrac{p^{r-1}(p-1)}{2}$. Therefore $p\mathcal{O}_L = \beta^{p^{r-1}(p-1)}$ and β is a principal prime ideal with generator $(1 - \zeta_{p^r})$

with residue field $\mathcal{O}_L/\pi \simeq \mathbb{F}_p$, with

$$\pi = \beta \cap \mathcal{O}_l = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1})) = (2-\zeta_{p^r}-\zeta_{p^r}^{-1}).$$

Using the preceding facts and notations we can generalize the results on codes over finite fields in Corollary 2 from [28] to codes over finite chain rings.

Lemma .13. *[5]*

Let $l = \mathbb{Q}_p(\zeta_{p^r}+\zeta_{p^r}^{-1})$ and let $\mathcal{C}$ be a k-dimensional code over R^m such that $\mathcal{C} \subset \mathcal{C}^{\perp}$. The lattice $(\Psi^{-1}(\mathcal{C}), b)$, where $b = \Sigma_{i=1}^{m} \mathrm{Tr}_{L/\mathbb{Q}_p}(\alpha x_i y_i)$ is integral of rank $mp^{r-1}(p-1)/2$. Using the same steps in [28], we get the same results over finite chain rings. A generator matrix of the lattice $\Lambda_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b)$ is

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

where $G = \begin{pmatrix} I_k & A \end{pmatrix}$ is a generator matrix of $\mathcal{C}$. The ring of integers $\mathcal{O}_l = \mathbb{Z}_p[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ has $\left\{\zeta_{p^r}+\zeta_{p^r}^{-1}\right\}_{i=0}^{n-1}$ as a $\mathbb{Z}_p$-basis and the principal ideal π is generated by $2-\zeta_{p^r}-\zeta_{p^r}^{-1}$.

Lemma .14. *[5] Let $l = \mathbb{Q}_p(\zeta_{p^r}+\zeta_{p^r}^{-1})$ and let $\mathcal{C}$ be a k-dimensional code over R^m such that $\mathcal{C} \subset \mathcal{C}^{\perp}$. Then:*

$$\Lambda_{\mathcal{C}}^{*} = \Lambda_{\mathcal{C}^{\perp}}.$$

Corollary 7. *[5] Let $l = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1})$ and let $\mathcal{C}$ be a k-dimensional code over R^m such that $\mathcal{C} \subset \mathcal{C}^\perp$ then the lattice $(\Lambda_\mathcal{C}, b)$ where b is the bilinear form $b = \Sigma_{i=1}^m \mathrm{Tr}_{l/\mathbb{Q}_p}(\alpha x_i y_i)$ is an integral lattice of rank $mp^{r-1}(p-1)/2$. We have that the lattice $\Lambda_\mathcal{C}$ is an odd unimodular if the code $\mathcal{C}$ is self-dual code.*

Note that, using this corollary we can construct self-dual codes over finite chain rings from odd unimodular lattices over $\mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1})$.

Conclusion

The thesis was dedicated to construction A of lattices over number fields from codes over $\mathbb{F}_q$, then we propose a new construction A of lattices from codes over finite chain rings, a general construction of lattices from codes over finite chain rings using p-adic fields. The connection between finite chain rings and p-adic fields was highlighted and based on this connection, the lifting of codes over finite chain rings was generalized. Also lattices were defined over p-adic integers with allow us to deal with lattices over the ring of integers of a Galois extension of $\mathbb{Q}_p$ from lifted codes over finite chain rings were constructed.

Appendix

A.1 Rings

Definition .36. *Let R be a non-empty set such that $+$ and $\cdot$ are the binary operations given by:*

$$+ : R \times R \to R \ , \ (a, b) \mapsto a + b$$

$$\cdot : R \times R \to R \ , \ (a, b) \mapsto a \cdot b$$

We say that the structure $(R, +, \cdot)$ define a ring if:

1. *R is an abelian group with respect to $+$, so that:*

2. *For any $a, b, c \in R$ we have: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of $\cdot$).*

3. *For any $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributivity of $\cdot$).*

4. *There exists* $0 \in R$.

5. *For any* $a \in R$ *there exists the inverse element* $-a \in R$ *such that* $a+(-a) = 0$

If the ring R has a neutral element for the law $(\cdot)$ then we say that the ring R is a unitary ring. The ring R is said to be commutative if the law $(\cdot)$ is commutative. An element $a \in R$ is a unit if there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1$, moreover a is said to be invertible with inverse b (and vice versa. We call the set of units of R the group of units of R and we denote it by $R^{\times}$.
An nonzero element $a \in R$ is a zerodivisor if for any element $b \in R$, with $b \neq 0$ we have: $a \cdot b = b \cdot a = 0$. The element a is nilpotent if $a^k = 0$ for some $k \in \mathbb{N}$ and idempotent if $a^2 = a$.

A.2 Product of rings

The product of two rings R and S is called the direct product denoted by $R \times S$ is given by:

$$\{(r, s) \ ; r \in R, s \in S\} .$$

The set $R \times S$ defined a ring with respect to addition and a multiplication componentwise: $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2, s_1 + s_2)$
$(r_1 + s_1) \cdot (r_2 + s_2) = (r_1 r_2, s_1 s_2)$.
The zero element is $(0, 0)$ and the multiplication identity is $(1, 1)$.

A.3 Homomorphism

Let R, S be two rings. The function $\phi : R \to S$ is a ring homomorphism if:

1. $\phi(a + b) = \phi(a) + \phi(b)$

2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

3. $\phi(1) = 1$
   The homomorphism ϕ is injective if it is injective as a map and surjective if it is surjective as a map.
   We denote the set of all homomorphism from R to S by $Hom(R, S)$.

Definition .37. *A bijective homomorphism from a ring R to another ring S is called an isomorphism, if ther is an isomorphism between R and S and we say that R and S are isomorphism and we write $R \simeq S$*

A.4 Ideals

Definition .38. *We call a subset I of a commutative ring R an ideal, if I satisfies the next conditions:*

1. *For any $r \in R$ and for any $i \in I$ we have $r \cdot i \in I$*

2. *$(I, +)$ is an additive subgroup of $(R, +)$.*

Let $X = (x_1, \ldots, x_k)$ be a subset of R. The ideal generated by (X) is the smallest ideal containing all elements of X, we call the element $x_1, \ldots, x_k$ generators of the ideal.

Definition .39. *Let I be an ideal of the ring R such that I is generated by one element: $I = (x)$, then the ideal $I = (x)$ is called principal.*

A.5 Fields, Integral domain, Euclidean domain

A.5.1 Fields

Let $(R, +, \cdot)$ be a ring such that:

1. $(R, +)$ is an abelian group.

2. $(R\{0\}, \cdot)$ is an abelian group.

3. The distributive law hold.

Then we say that R defines a field.

Example .11. *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.*

A.5.2 Integral domain

Let R be a commutative ring with identity in which $0 \neq 1$, we say that R is an integral domain (ID) if R has no zero divisors. Moreover if R is an integral domain such that every ideal in it is principal which mean that every ideal can be generated by a single element then we say that R is a principal ideal domain (PID).

Definition .40. *A norm on R is a function N defined from $R\ \ \{0\}$ to $\mathbb{N}$, such that:*

1. *If $f, g \in R$ with $g \neq 0$, there exist $q, r \in R$ so that,*

   $f = qg + r$, with either $r = 0$ or $N(r) < N(g)$.

2. *If $g, f \in R$ such that $g \neq 0$ and $f \neq 0$, then $N(f) \leq N(fg)$*

Definition .41. *An Euclidean domain is an integral domain R such that there is a norm on it.*

A.5.3 Polynomial rings

Let R be a ring. A polynomial $f(x)$ over R is given by:

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

with $n \geq 0$ and $a_0, a_1, \ldots, a_n \in R$.
The degree of $f(x)$ is n if $a_n \neq 0$ and we write $deg f(x) = n$, undefined if $f(x) = 0$.
The set of all polynomials in the indeterminate x with coefficients in the ring R is denoted by $R[x]$ and it is called a polynomial ring.

Proprieties .1.

1. *$R[x]$ is a ring with respect to the operations of polynomial addition and multiplication.*

2. *The ring $R[x]$ is commutative if R is a commutative ring.*

3. *If R is with unity 1, then the ring $R[x]$ is a ring with unity.*

4. *$R[x]$ is an integral domain if R is an integral domain.*

5. *In the case where $\mathbb{F}$ is a field, then $F[x]$ is an integral domain.*

A.6 Quotient rings

Let R be a ring and let I be an ideal of R, we define an equivalence relation $\sim$ on R as follows:

$x \sim y$ if and only if $x - y \in I$ and we say that $x \sim y$ are congruent modulo I ($\sim$ is a congruence relation) and

$$[x] = x + I := \{x + r \ ; r \in I\}$$

is the congruence class of x in R and we write $x \ mod \, I$, it is called the residue class of x modulo I.

The set of all equivalence classes is a ring denoted by R/I and we say that R/I is the quotient ring of R modulo I.

The map given by $\varphi : R \to R/I$, $\varphi(x) = x + I$

is a surjective ring homomorphism.

Proprieties .2. *1. If R is a commutative ring then R/I is also commutative (the converse it is not true in general).*

2. For a commutative ring R, R/I is a field if and only if I is a maximal ideal.

3. R/I is an integral domain if and only if I is a prime ideal.

A.7 Finite fileds

A field with finite number of elements is called a finite field or a Galois field so that the operations the operations of addition, subtraction, multiplication and division are defined with certain basic rules.

The order of a field is given by its number of elements, it is either a prime number

or a prime power.
The characteristic of a finite field is the least positive $n \in \mathbb{N}$ such that $n \cdot 1 = 0$.
Generally fields are denoted $\mathbb{F}_q$ with $q = p^k$ or $GF(q)$.

Example .12. *The field of order p, denoted by $\mathbb{F}_p$ is the field constructed as the integers modulo p, $\mathbb{Z}/p\mathbb{Z}$.*

A.7.1 Finite extension

Let K and F be two fields such that $K \subset F$, then:

Theorem .17. *The multiplicative group F^* is a cyclic group and we call any generator of this group a primitive element of F.*

Proposition .22. *Any finite field with characteristic p is a simple algebraic extension of $GF(p)$.*

Proprieties .3.

1. *The identity given by $(x + y)^p = x^p + y^p$ is true in a field of characteristic p.*

2. *For a prime number p and $x \in GF(p)$ then $x^p = x$ by the Fermat's little theorem. The next equality holds:*

$$x^p - x = \prod_{a \in GF(p)} x - a)$$

And every $x \in GF(p^n)$ satisfies the equation $x^{p^n} - x = 0$

A.8 Vector spaces

Let F be a commutative field a vector space over F is a set whose elements are called vectors and in which we can make linear combinations, such that:

1. $(E, +)$ is an abelian group.

2. $\forall(x, y) \in E^2$, $(\lambda, \mu) \in F^2$:

    - $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
    - $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
    - $\lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
    - $1 \cdot x = x$

A non-empty part $E^{'}$ of E is a vector subspace if it is stable by linear combination. Let $E^{'}$ and $E^{"}$ be two subspaces of E, then the intersection of $E^{'}$ and $E^{"}$ is also a subspace of E.

Definition .42. *Let K be a commutative field and let E, J be two vector spaces over K, an application ψ from E to J is called a linear map or a morphism if:*

$$\forall(x, y) \in E^2, (\alpha, \beta) \in K^2, f(\alpha x + \alpha y) = \alpha f(x) + \beta f(y).$$

The set of all linear maps from the vector space E to the vector space J is also a vector space over K.

Proposition .23. *The sum of two subspaces E_1 and E_2 of the vector space E is a vector subspace generated by $E_1 \cup E_2$ and we denote it by $E_1 + E_2$, such that:*

$$E_1 + E_2 = \{x_1 + x_2; x_1 \in E \text{ and } x_2 \in E_2\}.$$

Definition .43. *Let E_1 and E_2 be two subspaces of E. The vector space E is a direct sum of E_1 and E_2 if we have that:*

1. $E = E_1 + E_2,$

2. $E_1 \cap E_2 = \{0\},$

and we write $E = E_1 \oplus E_2$.

Theorem .18. *Let $E_1, \dots, E_2$, $n\mathbb{N}^*$ be n vector subspaces of E, we have that:*

1. *If $x \in E$, then x can be written in a unique way $x = x_1 + x_2 + \dots + x_n$ with $x_i \in E_i, i \in \{1, \dots, n\}$*

2. *$E = E_1 + E_2 + \dots + E_n$, where $i \in \{1, \dots, n\}$ and $E_i \cap (\sum_{j \neq i} E_j) = \{0\}$ We say that E is the direct sum of E_i if one of this two conditions is true, and we write:*

$$E = E_1 \oplus E_2 \oplus \dots \oplus E_n = \oplus_{i=1}^{n} E_i.$$

A.9 Modules

Let R be a unitary commutative ring.

Definition .44. *A module over R is an abelian group $(M, +)$ with a map $\mu : R \times M \to M$ so that:*

1. $a(x + y) = ax + ay$
2. $(a + b)x = ax + bx$
3. $(ab)x = a(bx)$
4. $1x = x$

   for all $a, b \in R$ and $x, y \in M$.

   We call a module over R an R-module.

Proprieties .4. *Let M be an R-module (we distinguish the zero vector 0_M from the zero scalar 0_R). We have that:*

1. $r0_M = 0_M$
2. $0_r x = 0_M$
3. $(-r)x = r(-x)$
4. *In the case where R is a field, then $rx = 0_M$ implies that either $r = 0_R$ or $x = 0_M$.*

Definition .45. *Let M be an R-module. A subgroup N of M such that $ax \in N$ for $a \in R$ and $x \in N$ is called a submodule of M.*

and we have that a subset N of M is a submodule of M if and only if $x, y \in N$ and $a, b \in R$ imply $ax + by \in N$, in other words if and only if N is stable by linear combination.

Free modules

Definition .46. *Let M be an R-module, a subset T of M form a basis of M if:*

1. *for all $x \in M$, x can be written as follows:*

   $$x = \Sigma_{i=1}^{n} a_i b_i$$

   where $n \in \mathbb{N}^*$, $b_i \in T$ and $a_i \in R$.

   We say that T generates M.

2. *T is a free part of M if the elements of T are linearly independent on R.*

Definition .47. *An R-module M is free if it has a basis.*

Example .13. *For a finite commutative ring R, the R-module given by*

$$R^n \left\{(a_1, \ldots, a_n)\ ;\ a_i \in A\right\}$$

is a free R-module with basis $\beta = (e_1, \ldots, e_n)$.

Bibliography

[1] E. Alparslan."Finite p-adic Computing Systems with Possible Applications". Ph.D. Dissertation, Dept, of Elec. Eng., University of Maryland, College Park, 1975.

[2] Y. Amice, Les nombres p-adiques, Presse universitaire de France, 1975.

[3] E. Bayer-Fluckiger, “Definite unimodular lattices having an automorphism of given characteristic polynomial”, Commentarii Mathematici Helvetici,vol 59, 509–538, 1984.

[4] G. Bini and F. Flamini, Finite Commutative Rings and Their Applications, Kluwer Academic Publishers, Massachusetts, 2002.

[5] R. L. Bouzara, K. Guenda and E. Martinez-Moro, Lifted codes and lattices from codes over finite chain rings, Cryptography and Communications, 2022.

[6] M. Broué and M. Enguehard. Polynomes des poids de certains codes et fonctions theta de certains réseaux. Ann. scient. Ec. Norm. Sup., 5:157–181, 1972.

[7] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, Des. Codes Cryptogr., 6(1), pp. 21-35, 1995.

[8] W-E. Clark and D-A. Drake, Finite chain rings, Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, (39), pp. 147153, 1973.

[9] W-E. Clark and J-J. Liang, Enumeration of finite commutative chain rings, Journal of Algebra, (27), pp. 445453, 1973.

[10] J. H. Conway and N. J. A. Sloane. Sphere Packings, Lattices and Groups. Springer, New York etc., 1988.

[11] S. I. R. Costa, F. Oggier, A. Campello, J-C. Belfiore, and E. Viterbo. Lattices applied to coding for reliable and secure communications, SpringerBriefs in Mathematics. Springer, Cham, 2017.

[12] M. Craig, “A cyclotomic construction for Leech’s lattice”, Mathematika,vol 25, 236–241, 1978.

[13] M. Craig, “Extreme forms and cyclotomy”, Mathematika, vol 25 , 44–56, 1978.

[14] H.Q. Dinh and S.R. Lopez-Permouth, Cyclic and Negacyclic Codes over Finite Chain Rings, IEE. Trans. Inform. Theory, vol. 50, 1728-1744, 2004.

[15] S.T. Dougherty, H. Liu, and Y. H. Park, Lifted codes over finite chain rings, Mathematical Journal of Okayama University, pp. 39-53, Volume 53, 2010.

[16] W. Ebeling. Lattices and codes: A course Partially Based on Lecture by F. Hirzebruch, originally published by Vieweg, reedited by Springer, 2013.

[17] W. Feit, “Some lattices over $\mathbb{Q}\sqrt{-3}$”, Journal of Algebra, vol 52, 248–263, 1978.

[18] R.N. Gorgui-Naguib and A. Leboyer. "Comment on ’Determination of p-adic Transform Bases and Lengths’". Electronics Letters, vol. 21, No.20, pp. 905-906, 1985.

[19] R.T. Gregory and E.V. Krishnamurthy. "Methods and Applications of Error-Free Computation". Texts and Monographs in Computer Science, Springer-Verlag, 1984.

[20] K. Guenda and T.A. Gulliver, MDS and self-dual codes over rings, Finite Fields and Their Applications, pp. 1061-1075, (18), 2012.

[21] K. Hensel. "Theorie der Algebraischen Zahlen".Teubner, Leipzig, 1908.

[22] K. Hensel."Zahlentheorie".Goschen, Berlin and Leipzig, 1913.

[23] T. Honold and I. Landjev, Linear Codes over Finite Chain Rings, The Electronic Journal of Combinations, vol 7, 2000.

[24] X. Hou and F. Oggier, Algebraic constructions of modular lattices, A thesis submitted to the Nanyang Technological University in partial fulfillment of the requirement for the degree of Doctor of Philosophy of Mathematics, 2017.

[25] X. Hou and K. Keating. Enumeration of isomorphism classes of extensions of p-adic fields. J. Number Theory, pp. 14-61, 104(1), 2004.

[26] X. Hou, K. H. Leung, and S. L. Ma, On the groups of units of finite commutative chain rings. Finite Fields appl., , pp.20-38,9(1), 2003.

[27] K. Iwasawa. Local class field theory, Oxford university Publications. The Clarendon Press, Oxford University Press, New York, Oxford Mathematical Monographs, 1986.

[28] W. Kositwattanarerk. S. S. Ong, and F. Oggier, Construction A of Lattices over Number Fields and Block Fading (Wiretap) Coding, IEE Trans. Inform. Theory, 61(5), pp. 2273-2282, 2015.

[29] E.V. Krishnamurthy, T. Mahadeva Rao and K. Subramanian. "Finite-Segment p-adic Number Systems with Applications to Exact Computation" Proc. Indian Acad. Sci., vol. 81A, No.vol 2, pp. 58-79, 1975.

[30] E.V. Krishnamurthy, T. Mahadeva Rao and K. Subramanian. "p-adic Arithmetic Procedures for Exact Matrix Computations". Proc. Indian Acad. Sci., vol. 82A, No. vol 5, pp. 165-175, 1975.

[31] E.V. Krishnamurthy "Matrix Processors Using p-adic Arithmetic for Exact Linear Computations". IEEE Trans, on Computers, vol. C-26, No. vol 7, pp.633-639, 1977.

[32] E.V. Krishnamurthy, T. Mahadeva Rao and K. Subramanian. "Finite-Segment p-adic Number Systems with Applications to Exact Computation". Proc. Indian Acad. Sci., vol. 81A, No. vol 2, pp. 58-79, 1975.

[33] A. Leboyer. "p-adic Numbers-p-adic Transform". MSc. Ccmmunications Report, Imperial College, June 1985.

[34] J. Leech and N. J. A. Sloane. Sphere packings and error-correcting codes. Canad. J. Math., vol 23,pp. 718– 745, 1971.

[35] V. Loahakosol and W. Surakampontorn. "p-adic Transforms". Electronics Letters, vol. 20, No. vol 18, pp. 726-727, 1984.

[36] B. R. McDonald. Finite Rings with Identity, Marcel Dekker, New York, Inc., Pure and applied Mathematics, Vol 28, New York, 1974.

[37] N.M. Nasrabadi. "Orthogonal Transforms and their Applications to Image Coding". Ph.D. Thesis, Imperial College, London, 1984.

[38] N.M. Nasrabadi and R.A. King. "Fast Digital Convolution Using p-adic Transforms". Electronics Letters, vol 19, pp. 266-267, 1983.

[39] N.M. Nasrabadi and R.A. King. "Complex Number Theoretic Transform in p-adic Field". Proc. of IEEE-ICASSP 84, pp.28A.4.1-28A.4.3, 1984.

[40] J. Neurkish. Algebraic nulber theory, volume 322 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer Verlag. Berlin, Translated from the 1992 German original and with a note by Nobert Schappacher, with a foreword by G. Harder, 1999.

[41] G. H. Norton and A. *Sălăgan*. On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Engrg. Comm. Comput., pp. 489-506, 10(6), 2000.

[42] Y. H. Park. The q-adic liftings of codes over finite fields.Korean J. Math., 26(3), pp. 53744, 2018.

[43] S.-C. Pei and J.-L. Wu. "Determination of p-adic Transform Bases and Lengths". Electronics Letters, vol. 21, 1985, pp. 431-432.

[44] H.-G. Quebbemann, “A construction of integral lattices”, Mathematika, vol 31, 137–140, 1984.

[45] H.-G. Quebbemann, “Modular lattices in Euclidean Spaces”, Journal of Number Theory, vol 54, 190–202, 1995.

[46] J-P Serre. Local Fields, Springer-Verlag New York-Berlin, volume 67 of Graduate Texts in Mathematics, Translated from the French by Marvin Jay Greenberg, 1979.

[47] N. J. A. Sloane. Binary codes, lattices and sphere packings. In P. J. Cameron, editor, Combinatorial Surveys, pages 117–164, New York, Academic Press, 1977.

[48] N. J. A. Sloane. Self-dual codes and lattices. In Proc. Symp. Pure Math. Vol. 34, 273–308, 1979.

[49] J. A. Wood. Mr27789905-review of: Lifted codes over finite chain rings. AMS Reviews, 2012.