UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"

Constelações Ciclotômicas

Autora: Tatiane da Silva Evangelista

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação de Mestrado apresentada ao Departamento de Matemática IBILCE-UNESP, como parte dos requisitos para obtenção do título de Mestre em Matemática. Área de concentração: **Matemática**.

São José do Rio Preto - SP

Fevereiro/2006

Constelações Ciclotômicas

Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

BANCA EXAMINADORA

- Prof. Dr. Antonio Aparecido de Andrade
  IBILCE - UNESP - São José do Rio Preto - SP
  Orientador

- Prof. Dr. Edson Donizete de Carvalho
  FEIS - UNESP - Ilha Solteira - SP
  1º Examinador

- Prof. Dr. João Roberto Gerônimo
  UEM - Maringá - PR
  2º Examinador

A meus pais Ademir e Marta
e às minhas irmãs Katiane e Tays,
dedico

Agradecimentos

Ao concluir este trabalho, agradeço:

Primeiramente, a Deus por mais uma etapa concluída.

Aos meus pais Ademir e Marta, pelo amor, estímulo, carinho e compreensão, foram a alma desta vitória, que através de um sorriso sincero, sempre me fizeram lembrar que os sonhos são possíveis.

Às minhas irmãs Katiane e Tays, pelo carinho e de compartilhar todos os momentos alegres e, principalmente, de me apoiarem nos momentos difícies.

Ao meu cunhado Guilherme, que também acompanhou essa jornada com grande incentivo e carinho, meu sincero agradecimento.

Ao Prof. Dr. Antonio Aparecido de Andrade, pela amizade, oportunidade e honra de trabalharmos juntos. Sem a sua paciência, dedicação e competência, este trabalho não estaria concluído.

Aos professores do Departamento de Matemática da UNESP - São José do Rio Preto - SP, pela formação acadêmica.

Aos professores da banca examinadora: Prof. Dr. Ali Messaoudi (IBILCE - UNESP - São José do Rio Preto - SP), Prof. Edson Donizete de Carvalho (FEIS - UNESP - Ilha Solteira - SP) e Prof. João Roberto Gerônimo (UEM - Maringá - PR).

A TODOS os meus colegas da pós-graduação pelas experiências trocadas, convívio e amizades tão sinceras, em especial às minhas amigas Cátia e Elen.

A todos que direta ou indiretamente contribuiram para a realização deste trabalho.

À FAPESP pelo auxílio financeiro.

"O valor das coisas não está no tempo que elas duram, mas na intensidade com que acontecem. Por isso, existem momentos inesquecíveis, coisas inexplicáveis e pessoas incomparáveis..."

Fernando Pessoa

Sumário

Lista de Símbolos

$\mathbb{N}$: Conjunto dos números naturais

$\mathbb{Z}$: Conjunto dos números inteiros

$\mathbb{Q}$: Conjunto dos números racionais

$\mathbb{R}$: Conjunto dos números reais

$\mathbb{C}$: Conjunto dos números complexos

$\prod$: Produtório

$\sum$: Somatório

$\det A$: Determinante de A

$mdc(a, b)$: Máximo divisor comum entre a e b

$\mathcal{O}_{\mathbb{K}}$: Anel de inteiros de $\mathbb{K}$

$\#X$: Cardinalidade do conjunto X

$\frac{A}{X}$: Quociente de A por X

$\bar{a}$: Conjugado complexo do elemento a

$\langle a \rangle$: Ideal gerado por a

$D(\alpha_1, \ldots, \alpha_n)$: Discriminante de uma n-upla

$D_{B/A}$: Discriminante B em relação a A

$[\mathbb{L} : \mathbb{K}]$: Grau de $\mathbb{L}$ sobre $\mathbb{K}$

$a \mid b$: a divide b

$a \nmid b$: a não divide b

$w_{\mathcal{M}}$: Peso de Manhattan

$w_{\bar{\mathcal{M}}}$: Peso de Mannheim

$d_{\mathcal{M}}$: Distância de Manhattan

$d_{\bar{\mathcal{M}}}$: Distância de Mannheim

d_{min}: Distância mínima

$min\{X\}$: Mínimo do conjunto X

$max\{X\}$: Máximo do conjunto X

$[a]$: O inteiro mais próximo de a

$Gal_{\mathbb{K}}\mathbb{L}$: Grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$

$V_S(a)$: Região de Voronoi de a em S

$GF(p^m)$: Grupo de Galois de cardinalidade p^m

G_{p^m}: p-grupo aditivo de cardinalidade p^m

Resumo

O principal objetivo do presente trabalho foi o estudo da construção de constelações de sinais casadas a grupos quocientes aditivos, via corpos quadráticos e corpos ciclotômicos. E por meio dessas constelações de sinais, construímos códigos corretores de erros. Também vimos a região de Voronoi via o anel de inteiros de Eisenstein-Jacobi e o anel de inteiros de Gauss.

Palavras-chave: constelações de sinais, distância de Mannheim, rotulamento casado, corpos quadráticos, corpos ciclotômicos, região de Voronoi, codificação e decodificação.

Abstract

The principal work was the study of construct cyclotomic signal constellations matched additive quotient group over quadratic fields and cyclotomic fields. It is by means of the signal constellations to construct codes to correct on error. From this Voronoi regions over Eisenstein-Jacobi integer ring and Gauss integer ring.

Keywords: signal constellations, Mannheim distance, matched labeling, quadratic fields, cyclotomic fields, Voronoi regions, coding and decoding.

Introdução

A demanda por sistemas de comunicação que operem com altas taxas de transmissão e capacidade de armazenamento requer que a confiabilidade também seja alta. Isto pode ser alcançado através da geração de novas estruturas de códigos corretores de erros.

Deste modo, utilizando o anel de inteiros de Eisenstein-Jacobi e o anel de inteiros de Gauss, Huber [1] e [2], propôs uma construção de códigos mediante a métrica de Mannheim. Nóbrega et.al [3], estenderam os trabalhos de Huber para os anéis de inteiros de Eisenstein-Jacobi. Interlando et.al [4], melhorou o procedimento de Nóbrega para constelações de sinais rotulados por elementos de $GF(p^m)$. Recentemente, Carvalho et.al [5] e [6] adaptou este trabalho para p-grupos aditivos G_{p^m}. Por sua vez, Fan et.al [7] e Dong et.al [8] e [9] estenderam os trabalhos de Huber via corpos ciclotômicos.

Assim, a partir desses resultados, um dos principais enfoques deste trabalho, consiste em realçar a diferença em relação à estrutura algébrica e geométrica das constelações de sinais via corpos quadráticos e corpos ciclotômicos. Além disso, analisar a codificação/decodificação de códigos corretores de erros nestes corpos.

O Capítulo 1, refere-se aos conceitos básicos de teoria algébrica dos números que serão referência para os demais capítulos. Sendo assim, introduzimos os conceitos de módulo, elementos inteiros, anéis notherianos e anéis de Dedekind, norma de elementos, norma de ideais, corpos quadráticos, corpos ciclotômicos e decomposições de ideais nestes corpos.

O Capítulo 2, refere-se aos trabalhos de Huber [1] e [2] e Carvalho et.al [5] e [6],

que se caracterizam nos estudos das constelações de sinais no $\mathbb{R}^2$ casadas a grupos quocientes aditivos $GF(p)$ ou $GF(p^m)$ e a p-grupos aditivos G_{p^m}, que não fazem parte de um corpo de Galois via corpos quadráticos. Neste casos, as identificações dos pontos de sinais são dados por elementos dos correspondentes anéis de inteiros $\mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = w = \frac{1+\sqrt{-3}}{2}$.

O Capítulo 3, refere-se a teoria de decodificação de códigos e constelações de sinais via corpos ciclotômicos, baseados nos trabalhos de Fan et.al [7] e Dong et.al [8] e [9].

O Capítulo 4, refere-se aos trabalhos de Interlando et.al [4] e Nóbrega et.al [3]. Nestes trabalhos vimos o estudo de rotulamento de reticulados, no qual consiste em encontrar uma forma explícita do isomorfismo entre o grupo de Galois $GF(p)$ e o quociente $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}$, em que $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de um corpo de número $\mathbb{K}$ e $\mathcal{P}$ é um ideal primo em $\mathcal{O}_{\mathbb{K}}$ e determinar a região de Voronoi da origem em S, na qual S é um reticulado de $\mathbb{Z}[\rho]$, gerado por $\{\pi, \rho\pi\}$, onde $\pi = a + b\rho$, para $a, b \in \mathbb{Z}$, $\rho = i$ ou $\rho = w$.

O estudo dos Capítulos 2 e 3, proporcionou-nos ferramentas necessárias para o estudo do Capítulo 5, no qual finaliza nosso trabalho. Neste capítulo, apresentamos códigos corretores de erros via corpos quadráticos e corpos ciclotômicos.

Os exemplos ilustrados neste trabalho, que não tiver referência são de minha própria autoria. O uso do software Maple 7 foi indispensável para alguns cálculos aqui desenvolvidos.

Capítulo 1

Teoria algébrica dos números

1.1 Introdução

Este capítulo tem por objetivo introduzir conceitos importantes da teoria algébrica dos números, que serão utilizados nos capítulos posteriores, como: módulo, elementos inteiros sobre um anel, norma de elementos. Sobre um corpo de números, veremos as principais propriedades dos anéis noetherianos, dos anéis de Dedekind, fatoração de ideais em uma extensão e para finalizar veremos os corpos quadráticos e os corpos ciclotômicos, também suas decomposições em ideais.

1.2 Módulo, elementos inteiros e discriminante

Nesta seção, apresentamos o conceito de módulo, elementos inteiros sobre um anel, na qual veremos que o conjunto desses elementos é um anel chamado anel de inteiros. Também apresentamos um estudo sobre as suas principais propriedades e a definição de discriminante.

Definição 1.2.1. *Seja A um anel. Um A-módulo M é um grupo abeliano (aditivo) munido de uma aplicação $A \times M \longrightarrow M$, denotada por $(a, m) \mapsto am$, tal que para quaisquer $a, b \in A$ e $x, y \in M$, tem-se:*

1. $a(x + y) = ax + ay$;

2. $(a+b)x = ax + bx$;

3. $(ab)x = a(bx)$;

4. $1x = x$.

Definição 1.2.2. *Sejam A um anel e M um A-módulo. Um subconjunto $N \subset M$ não vazio é um A-submódulo de M se, com as operações herdadas de M, também é um A-módulo.*

Definição 1.2.3. *Seja M um A-módulo, dizemos que M é um A-módulo finitamente gerado se existem elementos $x_1, \ldots, x_n$ em M tais que $M = x_1A + \ldots + x_nA$.*

Definição 1.2.4. *Sejam A, B anéis tais que $A \subseteq B$. Dizemos que um elemento $\alpha \in B$ é inteiro sobre A, se α é uma raiz de um polinômio mônico com coeficientes em A, ou seja, se existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$. Essa equação é chamada de equação de dependência integral de α.*

Exemplo 1.2.1. *Se $\alpha = \sqrt{5} + \sqrt{7} \in \mathbb{R}$, então α é inteiro sobre $\mathbb{Z}$, pois α é raiz do polinômio $x^4 - 24x^2 + 4 \in \mathbb{Z}[x]$.*

Teorema 1.2.1. *([10], p. 27) Sejam $A \subset B$ anéis e $\alpha \in B$. São equivalentes as seguintes afirmações:*

1. *α é inteiro sobre A.*

2. *O anel $A[\alpha]$ é um A-módulo finitamente gerado.*

3. *Existe um subanel R do anel B tal que R é um A-módulo finitamente gerado que contém A e α.*

Demonstração: 1. $\Rightarrow$ 2. Seja $A[\alpha] = \{\sum_i a_i\alpha^i : a_i \in A\}$. Por hipótese, temos que α é um inteiro sobre A. Então, existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$. Seja $M = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$ um A-módulo finitamente gerado. Vamos mostrar que $A[\alpha] = M$. Temos que $\alpha^n = -(a_{n-1}\alpha^{n-1} +$

$\ldots + a_1\alpha + a_0$), ou seja, $\alpha^n \in \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$. Agora, vamos provar por indução que $\alpha^j \in \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$, para todo $j \in \mathbb{N}$. Suponhamos, por hipótese de indução que $\alpha^j \in \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$ e mostremos que $\alpha^{j+1} \in \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$. Pela hipótese de indução, segue que existem elementos $b_0, \ldots, b_{n-1} \in A$ tal que $\alpha^j = b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0$. Assim,

$$\begin{aligned}\alpha^{j+1} &= \alpha^j\alpha = (b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0)\alpha \\ &= b_{n-1}\alpha^n + \ldots + b_1\alpha^2 + b_0\alpha \\ &= b_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots a_1\alpha - a_0) + \ldots + b_1\alpha^2 + b_0\alpha \\ &= -a_0b_{n-1} + (b_0 - b_{n-1}a_1)\alpha + \ldots + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1},\end{aligned}$$

ou seja, $\alpha^{j+1} \in \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$, para todo $j \in \mathbb{N}$. Por outro lado, temos que $\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle \subset A[\alpha]$. Logo, $\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle = A[\alpha]$. Portanto, $A[\alpha]$ é um A-módulo finitamente gerado por $1, \alpha, \ldots, \alpha^{n-1}$.

2. $\Rightarrow$ 3. Como $\alpha \in A[\alpha]$ e $A \subset A[\alpha]$ é suficiente tomar $R = A[\alpha]$.

3. $\Rightarrow$ 1. Se $R = \langle y_1, \ldots, y_n\rangle$ um A-módulo finitamente gerado tal que $A \subset R \subset B$ e $\alpha \in R$, então $R = Ay_1 + \ldots + Ay_n$. Como $\alpha \in R$, segue que $\alpha y_i \in R$, para todo $i = 1, \ldots, n$. Logo, existem $a_{ij} \in A$ com $1 \leq i, j \leq n$, de modo que

$$\begin{cases} \alpha y_1 = a_{11}y_1 + \ldots + a_{1n}y_n \\ \alpha y_2 = a_{21}y_1 + \ldots + a_{2n}y_n \\ \vdots \\ \alpha y_n = a_{n1}y_1 + \ldots + a_{nn}y_n. \end{cases}$$

Assim,

$$\begin{cases} (\alpha - a_{11})y_1 - a_{12}y_2 - \ldots - a_{1n}y_n = 0 \\ -a_{21}y_1 + (\alpha - a_{22})y_2 - \ldots - a_{2n}y_n = 0 \\ \vdots \\ -a_{n1}y_1 - a_{n2}y_2 - \ldots + (\alpha - a_{nn})y_n = 0. \end{cases}$$

Expressando na forma matricial, temos

$$\begin{pmatrix} \alpha - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & \alpha - a_{22} & \ldots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \ldots & \alpha - a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Seja d o determinante da matriz dos coeficientes deste sistema linear. Aplicando a Regra de Cramer, temos que $dy_j = 0$, para todo $j = 1, \ldots, n$. Como $1 \in R$, segue que $1 = \sum_{j=1}^{n} e_j y_j$, com $e_j \in A$. Assim, $d = d.1 = d\sum_{j=1}^{n} e_j y_j = \sum_{j=1}^{n} e_j dy_j = 0$. Logo, d é uma equação de dependência integral de α, uma vez que $d = \alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0$, onde cada $b_i \in A$. Portanto, α é inteiro sobre A. ■

Corolário 1.2.1. *([10], p. 28) Sejam $A \subset B$ anéis e $\alpha_1, \ldots, \alpha_n \in B$. Se α_1 é inteiro sobre A, α_2 é inteiro sobre $A[\alpha_1]$ e α_n é inteiro sobre $A[\alpha_1, \ldots, \alpha_{n-1}]$, então $A[\alpha_1, \ldots, \alpha_n]$ é um A-módulo finitamente gerado.*

Demonstração: Faremos a prova por indução sobre n. Se α_1 é inteiro sobre A, então pelo Teorema 1.2.1, temos que $A[\alpha_1]$ é um A-módulo finitamente gerado. Assim, suponhamos por hipótese de indução que $R = A[\alpha_1, \ldots, \alpha_{n-1}]$. Seja um A-módulo finitamente gerado por $\{v_1, v_2, \ldots, v_n\}$ e que α_n seja inteiro sobre $R = A[\alpha_1, \ldots, \alpha_{n-1}]$. Novamente, pelo Teorema 1.2.1, temos que $R[\alpha_n]$ é um R-módulo finitamente gerado. Assim, existe $\{w_1, \ldots, w_s\} \subset R[\alpha_n]$ tal que

$$R[\alpha_n] = A[\alpha_1, \ldots, \alpha_n] = \sum_{i=1}^{s} Rw_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{n} a_j v_j \right) w_i = \sum_{j,i} a_j v_j w_i.$$

Logo, $\{v_j w_i\}$, para $i = 1, \ldots, s$ e $j = 1, \ldots, n$, gera $R[\alpha_n]$ como um A-módulo. Portanto, $A[\alpha_1, \ldots, \alpha_n]$ é um A-módulo finitamente gerado. ■

Corolário 1.2.2. *([10], p. 29) Sejam $A \subset B$ anéis. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha \pm \beta$ e $\alpha\beta$ são inteiros sobre A.*

Demonstração: Temos que $\alpha \pm \beta$ e $\alpha\beta$ pertencem a $A[\alpha, \beta]$. Pelo Corolário 1.2.1, temos que $A[\alpha, \beta]$ é um A-módulo finitamente gerado e pelo Teorema 1.2.1, segue que $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A. ■

Definição 1.2.5. *Sejam $A \subset B$ anéis. Dizemos que B é inteiro sobre A, se todo elemento de B é inteiro sobre A.*

Definição 1.2.6. *Sejam $A \subset B$ anéis.*

1. *$\mathcal{O}_B = \{\alpha \in B : \alpha$ é inteiro sobre $A\}$ é chamado fecho inteiro de A em B (ou anel de inteiro de B).*

2. *Se A é um domínio e $B = \mathbb{K}$ é o corpo de frações de A, dizemos que $\mathcal{O}_B$ é o fecho inteiro de A em $\mathbb{K}$. Além disso, se $A = \mathcal{O}_B$ dizemos que A é um anel integralmente fechado.*

Proposição 1.2.1. *([10], p. 29) Se $A \subset B$ são anéis, então $A \subseteq \mathcal{O}_B \subseteq B$.*

Demonstração: Pelo Corolário 1.2.2, temos que $\mathcal{O}_B$ é um subanel de B. Se $\alpha \in A$, então α é raiz do polinômio $p(x) = x - \alpha$, o qual tem coeficientes em A. Logo, $\alpha \in \mathcal{O}_B$. Portanto, $A \subseteq \mathcal{O}_B \subseteq B$. ■

Proposição 1.2.2. *([10], p. 29) Sejam $A \subset B \subset R$ anéis. Então, R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

Demonstração: Suponhamos que R é inteiro sobre A. Se $\alpha \in R$, então existem $a_i \in A$ para $i = 0, \ldots, n-1$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Como $A \subset B$, segue que $a_i \in B$, $i = 0, 1, \ldots, n-1$, ou seja, α é inteiro sobre B. Portanto, R é inteiro sobre B. Se $\alpha \in B$ tal que $B \subset R$, então $\alpha \in R$. Pela hipótese, α é inteiro sobre A. Portanto, B é inteiro sobre A. Reciprocamente, seja $\alpha \in R$. Como R é inteiro sobre B, segue que existem $b_0, \ldots, b_{n-1} \in B$, não todos nulos, tal que $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0$. Seja $C = A[b_0, \ldots, b_{n-1}]$. Logo, α é inteiro sobre C. Como B é inteiro sobre A, segue que os $b_i's$ são inteiros sobre A. Pelo Corolário 1.2.1, temos que $C[\alpha] = A[b_0, \ldots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado e pelo Teorema 1.2.1, tem-se que α é inteiro sobre A. Portanto, R é inteiro sobre A. ■

Observação 1.2.1. *Sejam $A \subseteq B$ anéis.*

1. *Se A é um domínio, então $\mathcal{O}_B$ é um anel integralmente fechado.*

2. *Se A é um anel principal, então A é um anel integralmente fechado.*

3. *$\mathcal{O}_B$ é um A-submódulo de um A-módulo livre.*

Definição 1.2.7. *Seja $\mathbb{K}$ um corpo qualquer. Uma extensão $\mathbb{L} \supset \mathbb{K}$ diz-se finita se $[\mathbb{L} : \mathbb{K}] = n < \infty$. Caso contrário, $\mathbb{L} \supset \mathbb{K}$ diz-se extensão infinita.*

Definição 1.2.8. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão finita de corpos de grau n e $\alpha \in \mathbb{L}$. Definimos a norma de α sobre $\mathbb{K}$ como $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ e o traço de α como $Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$, na qual $\sigma_i : \mathbb{L} \to \mathbb{C}$, para $i = 1, 2, \ldots, n$, são $\mathbb{K}$-homomorfismos.*

Definição 1.2.9. *Sejam B um anel, A um subanel de B tal que A é um A-módulo livre de posto finito n e $\{\alpha_1, \ldots, \alpha_n\} \in B^n$. Definimos o seu discriminante dado por*

$$D_{B/A}(\alpha_1, \ldots, \alpha_n) = \det(Tr(\alpha_i \alpha_j)).$$

Proposição 1.2.3. *Sejam B um anel, A um subanel de B tal que A é um A-módulo livre de posto finito n e $(\alpha_1, \ldots, \alpha_n) \in B^n$. Se $(\beta_1, \ldots, \beta_n) \in B^n$ é um conjunto de elementos de B tais que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in A$, então*

$$D_{B/A}(\beta_1, \ldots, \beta_n) = (\det(a_{ij}))^2 D_{B/A}(\alpha_1, \ldots, \alpha_n).$$

Demonstração: Sejam $\beta_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^{n} a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in A$. Sendo $\beta_p\beta_q = \sum_{i=1}^{n} a_{pi}\alpha_i \sum_{j=1}^{n} a_{qj}\alpha_j$, temos

$$Tr(\beta_p\beta_q) = Tr(\sum_{i,j}^{n} a_{pi}a_{qj}\alpha_i\alpha_j) = \sum_{i,j}^{n} a_{pi}a_{qj}Tr(\alpha_i\alpha_j).$$

Colocando na forma matricial, temos que $(Tr(\beta_p\beta_q)) = (a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t$. Pela Definição 1.2.9, tem-se que $D_{B/A}(\beta_1, \ldots, \beta_n) = \det(Tr(\beta_p\beta_q))$. Logo,

$$\begin{aligned} D_{B/A}(\beta_1, \ldots, \beta_n) &= \det((a_{pi})Tr(\alpha_i\alpha_j)(a_{qj})^t) \\ &= \det(a_{pi}) \det(Tr(\alpha_i\alpha_j)) \det(a_{qj})^t \\ &= \det(a_{ij})^2 D_{B/A}(\alpha_1, \ldots, \alpha_n). \quad \blacksquare \end{aligned}$$

1.3 Anéis noetherianos e anéis de Dedekind

Nesta seção, veremos os conceitos de anéis noetherianos e de anéis de Dedekind, enfocando suas principais propriedades.

Definição 1.3.1. *Sejam A um anel e M um A-módulo. Dizemos que M é um A-módulo noetheriano se satisfaz uma das seguintes condições:*

1. *Toda família não vazia de A-submódulos de M tem um elemento maximal.*
2. *Toda sequência crescente de A-submódulos de M é estacionária.*
3. *Todo A-submódulo de M é finitamente gerado.*

Dizemos que um anel A é noetheriano se A considerado como um A-módulo for noetheriano.

Proposição 1.3.1. *([10]) Todo anel principal A é noetheriano.*

Demonstração Sejam A um anel principal e uma sequência crescente de A-submódulos de A dada por $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$. Como A é principal, segue que todos os ideais de A são principais e como os submódulos de A são exatamente os ideais de A, temos que os submódulos de A são principais. Logo, $I = \bigcup_{n\in N} I_n$ é um ideal de A. Agora, notemos que $I_n \subset I = \langle a\rangle$, para todo $n \in \mathbb{N}$ e $a \in I_{n_0}$, para algum $n_0 \in \mathbb{N}$, pois $a \in \langle a\rangle = I = \bigcup_{n\in\mathbb{N}} I_n$. Se $a \in I_{n_0}$ tal que $a \in \langle a\rangle$, então $I = \langle a\rangle \subset I_{n_0}$. Portanto, $I = I_{n_0}$. Assim, existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$ tem-se que $I_n = I_{n_0}$. ■

Proposição 1.3.2. *([10], p. 46) Sejam A um anel, M um A-módulo e N um submódulo de M. Então, M é noetheriano se, e somente se, $\frac{M}{N}$ e N são noetherianos.*

Demonstração: Suponhamos que M é noetheriano. Se $(M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos de N, então $(M_n)_{n\geq 0}$ também é uma sequência crescente de A-submódulos de M. Como M é noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária. Portanto, N é noetheriano. Para mostrar que $\frac{M}{N}$ é noetheriano, sejam $S = \{\text{submódulos de } M \text{ que contém } N\}$ e $T = \{\text{submódulos de } \frac{M}{N}\}$. A aplicação $\varphi : S \longrightarrow T$ definida por $\varphi(E) = \frac{E}{N}$, onde $E \in S$, é uma bijeção de S em T. Assim, se $(M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos de $\frac{M}{N}$, então $(\varphi^{-1}(M_n))_{n\geq 0}$

também é uma sequência crescente de A-submódulos de M. Como M é noetheriano, segue que $(\varphi^{-1}(M_n))_{n\geq 0}$ é estacionária e portanto, $(M_n)_{n\geq 0}$ é estacionária. Assim, $\frac{M}{N}$ é noetheriano. Reciprocamente, suponhamos que $\frac{M}{N}$ e N são noetherianos. Se $(M_n)_{n\geq 0}$ uma sequência crescente de A-submódulos de M, então $(N \cap M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos N. Como N é noetheriano, segue que $(N \cap M_n)_{n\geq 0}$ é estacionária, ou seja, existe $k \in \mathbb{N}$ tal que $M_n \cap N = M_{n+1} \cap N$ e $\frac{M_n}{N} = \frac{M_{n+1}}{N}$, para todo $n \geq k$. Dessa forma, $M_n \subseteq M_{n+1}$, para todo $n \geq k$. Agora, se $x \in M_{n+1}$, então existe $y \in M_n$ tal que $x + N = y + N$. Assim, $x - y \in N \cap M_{n+1} = N \cap M_n$. Logo, $x - y \in M_n$ e como $y \in M_n$, segue que $x \in M_n$. Portanto, $M_n = M_{n+1}$, para todo $n \geq k$. Assim, M é noetheriano. ■

Corolário 1.3.1. *([10], p. 47) Se $M_1, \ldots, M_n$ são A-módulos noetherianos, então o produto $M_1 \times \ldots \times M_n$ é um A-módulo noetheriano.*

Demonstração: Faremos a prova por indução sobre n. Para $n = 2$, identificamos $M_1 \simeq M_1 \times \{0\} \subset M_1 \times M_2$ e definimos a função $\varphi : M_1 \times M_2 \longrightarrow M_2$ tal que $\varphi(0, y) = y$. Como φ é um homomorfismo sobrejetor, segue que $\frac{M_1 \times M_2}{\ker \varphi} \simeq M_2$, na qual $\ker \varphi = M_1 \times \{0\}$. Também como M_2 é noetheriano, segue que $\frac{M_1 \times M_2}{M_1 \times \{0\}} \simeq M_2$ é noetheriano e pela Proposição 1.3.2, tem-se que $M_1 \times M_2$ é noetheriano. Suponhamos agora, por hipótese de indução que $M = M_1 \times \ldots \times M_{n-1}$ é noetheriano. Como M_n é noetheriano, segue que do caso $n = 2$, que $M = M_1 \times \ldots \times M_n$ é um A-módulo noetheriano. ■

Corolário 1.3.2. *([10], p. 47) Sejam A é um anel noetheriano e M é um A-módulo finitamente gerado. Então, M é um A-módulo noetheriano.*

Demonstração: Seja $\{e_1, \ldots, e_n\}$ um conjunto de geradores do A-módulo M. A aplicação $\varphi : A^n \longrightarrow M$ definida por $\varphi(a_1, \ldots, a_n) = a_1e_1 + \ldots + a_ne_n$ é um homomorfismo sobrejetor. Assim, $\frac{A^n}{\ker \varphi} \simeq M$. Como A é noetheriano, pelo Corolário 1.3.1, segue que A^n é noetheriano. Pela Proposição 1.3.2, temos que M é um A-módulo noetheriano. ■

Proposição 1.3.3. *([10], p. 47) Seja A um anel noetheriano e integralmente fechado. Sejam $\mathbb{K}$ é o corpo de frações de A, $\mathbb{K} \subset \mathbb{L}$ é uma extensão finita de grau n e $\mathcal{O}_B$ é o fecho inteiro de A em $\mathbb{L}$. Então, $\mathcal{O}_B$ é um A-módulo finitamente gerado e $\mathcal{O}_B$ é um anel noetheriano.*

Demonstração: Pela Observação 1.2.1, temos que $\mathcal{O}_B$ é um submódulo de um A-módulo livre de posto n. Pelo Corolário 1.3.2, tem-se que $\mathcal{O}_B$ é um A-módulo noetheriano e portanto, finitamente gerado. Como os ideais de $\mathcal{O}_B$ são os A- submódulos de $\mathcal{O}_B$, segue que $\mathcal{O}_B$ é um anel noetheriano. ■

Proposição 1.3.4. *([10], p. 47) Sejam $A \subset B$ anéis. Se $\mathcal{P} \subset B$ é um ideal primo, então $\mathcal{P} \cap A$ é um ideal primo de A.*

Demonstração: Seja a aplicação $\varphi : A \xrightarrow{i} B \xrightarrow{\pi} \dfrac{B}{\mathcal{P}}$, em que i é a inclusão e π é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo, pois π e i são homomorfismo e $\ker(\varphi) = A \cap \mathcal{P}$, pois $\varphi(x) = \pi \circ i(x) = \pi(x) = x + \mathcal{P}$ e $\varphi(x) = \bar{0}$ se, e somente se, $x \in \mathcal{P} \cap A$. Portanto, $\dfrac{A}{\mathcal{P} \cap A} \simeq Im(\varphi) \subset \dfrac{B}{\mathcal{P}}$. Como $\dfrac{B}{\mathcal{P}}$ é um domínio, segue que $\dfrac{A}{\mathcal{P} \cap A}$ é um domínio. Portanto, $\mathcal{P} \cap A$ é um ideal primo de A. ■

Proposição 1.3.5. *([10], p. 48) Sejam A um anel e $\mathcal{P}$ um ideal primo de A. Se $\mathcal{P}$ contém um produto de ideais $\mathcal{A}_1, \ldots, \mathcal{A}_n$ de A, então $\mathcal{P}$ contém $\mathcal{A}_j$, para algum $j = 1, 2, \ldots, n$.*

Demonstração: Se $\mathcal{A}_j \not\subset \mathcal{P}$, para todo $j = 1, \ldots, n$, então existe $\alpha_j \in \mathcal{A}_j$ tal que $\alpha_j \notin \mathcal{P}$, para algum $j = 1, 2, \ldots, n$. Como $\mathcal{P}$ é primo, segue que $\alpha_1 \ldots \alpha_n \notin \mathcal{P}$. Por hipótese de indução, $\mathcal{P}$ contém um produto de ideais primos $\mathcal{A}_1 \ldots \mathcal{A}_n$, então $\mathcal{P} \supset \alpha_1 \ldots \alpha_n \in \mathcal{A}_1 \ldots \mathcal{A}_n$, o que é um absurdo. Portanto, $\mathcal{P}$ contém $\mathcal{A}_j$ para algum $j = 1, \ldots, n$. ■

Observação 1.3.1.

1. *Em um anel noetheriano A, todo ideal contém um produto de ideais primos.*
2. *Em um domínio noetheriano, todo ideal não nulo contém um produto de ideais primos não nulos.*

Definição 1.3.2. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Um ideal fracionário de A (ou de $\mathbb{K}$ em relação a A) é um A-módulo $\mathcal{I} \subset \mathbb{K}$ tal que existe $d \in A - \{0\}$ na qual $d\mathcal{I} \subset A$. Em particular, os ideais inteiros de A são ideais fracionários com $d = 1$.*

Observação 1.3.2. *Se A é um domínio noetheriano, então todo ideal fracionário $\mathcal{I}$ de A é um A-módulo finitamente gerado.*

Definição 1.3.3. *Dizemos que um anel A é um anel de Dedekind se satisfaz as seguintes condições:*

1. *A é integralmente fechado.*
2. *A é noetheriano.*
3. *Todo ideal primo não nulo de A é maximal.*

Teorema 1.3.1. *([10], p. 49) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subset \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_B$ o fecho inteiro de A em $\mathbb{L}$. Então, $\mathcal{O}_B$ é um anel de Dedekind.*

Demonstração: Pela Observação 1.2.1 e Proposição 1.3.3, temos que $\mathcal{O}_B$ é integralmente fechado e noetheriano, respectivamente. Assim, falta mostrar que todo ideal primo não nulo de $\mathcal{O}_B$ é maximal. Seja $\mathcal{P} \subset \mathcal{O}_B$ um ideal primo não nulo. Como $A \subset \mathcal{O}_B$, pela Proposição 1.3.4, segue que $\mathcal{P} \cap A$ é um ideal primo de A. Vamos mostrar que $\mathcal{P} \cap A$ é não nulo. Seja $\alpha \in \mathcal{P}$ e $\alpha \neq 0$. Como $\mathcal{P} \subset \mathcal{O}_B$, segue que $\alpha \in \mathcal{O}_B$. Assim, existem $a_i \in A$, para $i = 0, \ldots, n-1$, não todos nulos, tais que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$ e que n seja mínimo. Logo, $a_0 \neq 0$, pois caso contrário, obteríamos uma equação de grau menor. Assim, $a_0 = \alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \ldots - a_1) \in \alpha\mathcal{O}_B \cap A \subset \mathcal{P} \cap A$. Portanto, $\mathcal{P} \cap A \neq 0$. Como $\mathcal{P} \cap A$ é um ideal primo de A e A é Dedekind, segue que $\mathcal{P} \cap A$ é um ideal maximal de A e assim, $\dfrac{A}{\mathcal{P} \cap A}$ é corpo. Seja a aplicação $\varphi : A \xrightarrow{i} \mathcal{O}_B \xrightarrow{\pi} \dfrac{\mathcal{O}_B}{\mathcal{P}}$, em que i é a inclusão e π é a projeção. Assim, $\dfrac{A}{\mathcal{P} \cap A} \simeq Im(\varphi) \subset \dfrac{\mathcal{O}_B}{\mathcal{P}}$. Como $\mathcal{O}_B$

é inteiro sobre A, segue que $\frac{\mathcal{O}_B}{\mathcal{P}}$ é inteiro sobre $\frac{A}{\mathcal{P}\cap A}$. Logo, $\frac{\mathcal{O}_B}{\mathcal{P}}$ é um corpo. Portanto, $\mathcal{P}$ é maximal. ■

Observação 1.3.3. *Seja A um anel de Dedekind que não é um corpo e seja $\mathbb{K}$ o seu corpo de frações. Então, todo ideal maximal $\mathcal{M}$ de A é inversível.*

Teorema 1.3.2. *([10], p. 50) Se F é o conjunto dos ideais primos de A tal que A é um anel de Dedekind, que não é um corpo, então todo ideal fracionário $\mathcal{B}$ não nulo de A é um produto de ideais primos de A de modo único, isto é, $\mathcal{B}=\prod_{i=1}^{n}\mathcal{P}_i^{e_i}$, em que $e_1,\ldots,e_n$ são inteiros positivos.*

Demonstração: Se $\mathcal{B}$ é um ideal fracionário de A, então existe $d\in A-\{0\}$ tal que $d\mathcal{B}\subset A$. Notemos que $\mathcal{B}=(d\mathcal{B})(d^{-1}A)$ assim, é suficiente mostrar o resultado para ideais inteiros. Seja F a família dos ideais inteiros de A, não nulos, que não são um produto de ideais primos de A. Suponhamos $F\neq\emptyset$. Como A é noetheriano, segue que F tem um elemento maximal M. Logo $M\neq A$, pois A é o produto da coleção vazia de ideias primos. Assim, $M\subset\mathcal{P}$ para algum ideal maximal $\mathcal{P}$ de A. Pela Observação 1.3.3, temos que $\mathcal{I}=\{x\in\mathbb{K}: x\mathcal{P}\subset A\}$ é tal que $\mathcal{P}\mathcal{I}=A$. Como $M\subset\mathcal{P}$, segue que $M\mathcal{I}\subset\mathcal{P}\mathcal{I}=A$. Além disso, como $A\subset\mathcal{I}$, segue que $M=MA\subset M\mathcal{I}\subset A$. Temos que $M\subset M\mathcal{I}$, pois se $M=M\mathcal{I}$ tal que $\alpha\in\mathcal{I}$, então $\alpha M\subset M$, $\alpha^2M\subset\alpha M\subset M$. Assim $\alpha^nM\subset M$, para todo $n\in\mathbb{N}$. Se $d\in M-\{0\}$, então $d\alpha^n\in M\subset A$. Portanto, $A[\alpha]$ é um ideal fracionário de A. Como A é noetheriano, segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema 1.2.1, tem-se que α é inteiro sobre A e sendo A integralmente fechado, segue que $\alpha\in A$. Portanto, $\mathcal{I}\subset A$ e assim, $\mathcal{I}=A$. Mas isto é impossível, pois se $\mathcal{I}=A$, então $\mathcal{P}=\mathcal{P}A=\mathcal{P}\mathcal{I}=A$, o que é um absurdo, uma vez que $\mathcal{P}$ é um ideal primo. Pela maximilidade de M e como $M\not\subset M\mathcal{I}$, segue que $M\mathcal{I}\notin F$. Logo, $M\mathcal{I}=\mathcal{P}_1\ldots\mathcal{P}_n$, na qual $\mathcal{P}_i$ são ideais primos de A, para $i=1,\ldots,n$. Multiplicando por $\mathcal{P}$ ambos os lados, temos que $M=\mathcal{P}_1\ldots\mathcal{P}_n\mathcal{P}$, o que é um absurdo, pois $M\in F$. Portanto, $F=\emptyset$. ■

Definição 1.3.4. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Sejam $\mathcal{A}$ e $\mathcal{B}$*

ideais fracionários de A. Dizemos que $\mathcal{A}$ divide $\mathcal{B}$ se existe $\mathcal{D}$ ideal inteiro de A tal que $\mathcal{B} = \mathcal{A}\mathcal{D}$.

Proposição 1.3.6. *([12], p. 120) Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e $\mathcal{A}$, $\mathcal{B}$ ideais fracionários de A. Então, $\mathcal{A}$ divide $\mathcal{B}$ se, e somente se, $\mathcal{B} \subset \mathcal{A}$.*

Demonstração: Se $\mathcal{A}$ divide $\mathcal{B}$, então existe um ideal $\mathcal{D} \subseteq A$ tal que $\mathcal{B} = \mathcal{A}\mathcal{D} \subset \mathcal{A}$. Por outro lado, se $\mathcal{B} \subset \mathcal{A}$, então $\mathcal{B}\mathcal{A}^{-1} \subset \mathcal{A}\mathcal{A}^{-1} = A$. Assim, $\mathcal{B}\mathcal{A}^{-1}$ é um ideal inteiro tal que $(\mathcal{B}\mathcal{A}^{-1})\mathcal{A} = \mathcal{B}$. Portanto, $\mathcal{A}$ divide $\mathcal{B}$. ■

1.4 Norma de um ideal

Nesta seção, apresentamos o conceito de norma de um ideal do anel de inteiros de um corpo de números, na qual consideramos $\mathbb{K}$ um corpo de números de grau finito n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Também, veremos algumas propriedades da norma, dentre elas que a norma é multiplicativa.

Definição 1.4.1. *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Definimos a norma do ideal $\mathcal{A}$ como $N(\mathcal{A}) = \#\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$.*

Teorema 1.4.1. *([10], p. 52) Se $\mathcal{A} = \langle\alpha\rangle$ tal que $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{A}) = \#\dfrac{\mathcal{O}_{\mathbb{K}}}{\langle\alpha\rangle}$.*

Demonstração: Pela Observação 1.2.1, temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Como a aplicação $\phi : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}$ definida por $\phi(a) = a\alpha$, para $\alpha \in \mathcal{O}_{\mathbb{K}}$ é um isomorfismo, segue que $\langle\alpha\rangle$ é um $\mathbb{Z}$-módulo livre de posto n e também como $\mathbb{Z}$ é um anel principal e $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre, segue que existem uma base $\{e_1, \ldots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e $c_1, \ldots, c_n \in \mathbb{Z}$ tal que $\{c_1e_1, \ldots, c_ne_n\}$ é uma base de $\langle\alpha\rangle$. A aplicação $\Psi : \mathcal{O}_{\mathbb{K}} \to \dfrac{\mathbb{Z}}{c_1\mathbb{Z}} \times \ldots \times \dfrac{\mathbb{Z}}{c_n\mathbb{Z}}$ definida por $\Psi(\sum a_ie_i) = (\bar{a}_1, \ldots, \bar{a}_n)$ é um homomorfismo sobrejetor e $ker(\Psi) = \langle\alpha\rangle$ se, e somente se, $\Psi(a) = \bar{0}$ se, e somente se, $\bar{a}_i = \bar{0}$, para $i = 1, \ldots, n$ se, e somente se, $a_i \in c_i\mathbb{Z}$, para $i = 1, \ldots, n$ se, e somente se, c_i divide a_i, para $i = 1, \ldots, n$ se, e somente se, $a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i$. Como $b_i \in \mathbb{Z}$, segue que $a \in \langle\alpha\rangle$. Portanto,

$$\frac{\mathcal{O}_{\mathbb{Z}}}{\langle\alpha\rangle} \simeq \frac{\mathbb{Z}}{c_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{c_n\mathbb{Z}}.$$

Assim, $\#\dfrac{\mathcal{O}_{\mathbb{K}}}{\langle\alpha\rangle} = c_1 \dots c_n$. Seja a aplicação $\mathbb{Z}$-linear $\mu : \mathcal{O}_{\mathbb{K}} \to \langle\alpha\rangle$, definida por $\mu(e_i) = c_i e_i$, para $i = 1, \dots, n$. Logo, $\mu(e_1) = c_1 e_1 + 0e_2 + \dots + 0e_n, \dots, \mu(e_n) = 0e_1 + 0e_2 + \dots + c_n e_n$ e $\det(\mu) = c_1 \dots c_n$. Por outro lado, temos que $\{c_1 e_1, \dots, c_n e_n\}$ e $\{\alpha_1 e_1, \dots, \alpha_n e_n\}$ são bases de $\langle\alpha\rangle$. Portanto, existe um automorfismo $\Upsilon : \langle\alpha\rangle \to \langle\alpha\rangle$ tal que $\Upsilon(c_i e_i) = \alpha e_i$, para $i = 1, \dots, n$. Como a matriz mudança de base é inversível, segue que $\det(\Upsilon)$ é inversível em $\mathbb{Z}$ e portanto, $\det(\Upsilon) = \pm 1$. Também, $(\Upsilon \circ \mu)(e_i) = \Upsilon(\mu(e_i)) = \Upsilon(c_i e_i) = \alpha e_i$, para $i = 1, \dots, n$. Assim, $(\Upsilon \circ \mu)(a) = \alpha a$. Finalmente, $N(\alpha) = \det(\Upsilon \circ \mu) = \det(\Upsilon)\det(\mu) = \pm 1 c_1 \dots c_n = \pm\dfrac{\mathcal{O}_{\mathbb{K}}}{\langle\alpha\rangle}$. Portanto, $|N(\alpha)| = \#\dfrac{\mathcal{O}_{\mathbb{K}}}{\langle\alpha\rangle}$. ■

Proposição 1.4.1. *([10], p. 52) Se $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{A})$ é finita.*

Demonstração: Se $\alpha \in \mathcal{A}$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathcal{A}$ e $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$ pode ser visto como um quociente de $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}$. Assim, $\#\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} = \#\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}\#\dfrac{\mathcal{A}}{\mathcal{O}_{\mathbb{K}}\alpha}$. Pelo Teorema 1.4.1, temos que $\#\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}$ é finito. Portanto, $\#\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$ é finito. ■

Proposição 1.4.2. *([10], p. 52) Se $\mathcal{A}$ e $\mathcal{B}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$.*

Demonstração: Pelo Teorema 1.3.2, temos que $\mathcal{B} = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$, na qual $\mathcal{P}_i \subset \mathcal{O}_{\mathbb{K}}$ são ideais primos para $i = 1, \dots, n$. Como todo ideal primo é maximal, é suficiente mostrar que $N(\mathcal{AM}) = N(\mathcal{A})N(\mathcal{M})$, ou seja,

$$\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{AM}} = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}, \tag{1.1}$$

em que $\mathcal{M}$ é um ideal maximal de $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{AM} \subset \mathcal{A}$, segue que o homomorfismo sobrejetor $\phi : \dfrac{\mathcal{A}}{\mathcal{AM}} \longrightarrow \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$, definido por $\phi(x + \mathcal{AM}) = x + \mathcal{A}$ para $x \in \mathcal{O}_{\mathbb{K}}$, possui $\ker(\phi) = \dfrac{\mathcal{A}}{\mathcal{AM}}$. Assim, $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}} \simeq \dfrac{\mathcal{O}_{\mathbb{K}}/\mathcal{AM}}{\mathcal{A}/\mathcal{AM}}$ e isto implica que

$$\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{AM}} = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}\#\frac{\mathcal{A}}{\mathcal{AM}}. \tag{1.2}$$

Por (1.1) e (1.2) é suficiente mostrar que $\#\frac{\mathcal{A}}{\mathcal{AM}} = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$. Temos que $\frac{\mathcal{A}}{\mathcal{AM}}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo. Logo, $\frac{\mathcal{A}}{\mathcal{AM}}$ é um $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$-módulo. Como $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$ é corpo, segue que $\frac{\mathcal{A}}{\mathcal{AM}}$ é um espaço vetorial sobre $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$. Seus subespaços são ideais da forma $\frac{\mathcal{I}}{\mathcal{AM}}$, em que $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{AM} \subset \mathcal{I} \subset \mathcal{A}$. Assim, pela Proposição 1.3.6, existem ideais $\mathcal{D}, \mathcal{E} \in \mathcal{O}_{\mathbb{K}}$ tais que $\mathcal{AM} = \mathcal{ID}$ e $\mathcal{I} = \mathcal{AE}$. Assim, $\mathcal{AM} = \mathcal{AED}$ e portanto, $\mathcal{M} = \mathcal{ED}$. Assim, $\mathcal{M} \subset \mathcal{D} \subset \mathcal{O}_{\mathbb{K}}$ e $\mathcal{M} \subset \mathcal{E} \subset \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{M}$ é maximal, segue que $\mathcal{E} = \mathcal{M}$ ou $\mathcal{E} = \mathcal{O}_{\mathbb{K}}$. Logo, $\mathcal{I} = \mathcal{AM}$ ou $\mathcal{I} = \mathcal{A}$. Deste modo, os únicos subespaços de $\frac{\mathcal{A}}{\mathcal{AM}}$ são os triviais e assim, $dim_{\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}}(\frac{\mathcal{A}}{\mathcal{AM}}) = 1$. Portanto, $\#\frac{\mathcal{A}}{\mathcal{AM}} = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$. ■

Proposição 1.4.3. *([12], p. 129) Se o anel $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal primo não nulo, então*

1. *$N(\mathcal{A}) \in \mathcal{A}$.*
2. *$N(\mathcal{A}) = 1$ se, e somente se, $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$.*
3. *Se $N(\mathcal{A})$ é um número primo, então $\mathcal{A}$ é um ideal primo.*

Demonstração:

1. Como $N(\mathcal{A}) = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$, segue que o grupo aditivo de $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$ tem ordem $m = N(\mathcal{A})$. Assim, $m\bar{1} = \bar{0}$, sendo $\bar{1}$ e $\bar{0}$, respectivamente, a unidade e o zero do anel $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}}$. Como $\bar{m} = m\bar{1} = \bar{0}$, segue que $m + \mathcal{A} = 0 + \mathcal{A}$. Portanto, $m = N(\mathcal{A}) \in \mathcal{A}$ e assim, $N(\mathcal{A}) \in \mathcal{A}$.
2. Temos que $N(\mathcal{A}) = 1$ se, e somente se, $\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}} = 1$ se, e somente se, $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$.
3. Seja p um número primo tal que $N(\mathcal{A}) = p$. Consideremos o ideal $\mathcal{A}$ como o produto de ideais primos, ou seja, $\mathcal{A} = \mathcal{P}_1 \dots \mathcal{P}_n$. Calculando a norma, tem-se que $p = N(\mathcal{A}) = N(\mathcal{P}_1) \dots N(\mathcal{P}_n)$, isto implica que, $N(\mathcal{P}_1) = p$, pois $N(\mathcal{P}_j) = 1$, para todo j se, e somente se, $\mathcal{P}_j = \mathcal{O}_{\mathbb{K}}$, o que é uma contradição. Portanto, $\mathcal{A} = \mathcal{P}_1$ e assim, $\mathcal{A}$ é um ideal primo. ■

Observação 1.4.1.

1. *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $N(\alpha) = \pm 1$ se, e somente se, α é uma unidade.*

2. *Sejam $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$. Se $\alpha = \mu\beta$ na qual μ é uma unidade de $\mathcal{O}_{\mathbb{K}}$, então $N(\alpha) = \pm N(\beta)$.*

Definição 1.4.2. *Sejam $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$. Dizemos que α e β são associados se $\alpha \mid \beta$ e $\beta \mid \alpha$.*

Observação 1.4.2. *Se $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$, então*

1. *α divide β se, e somente se, $\langle\alpha\rangle \subseteq \langle\beta\rangle$.*

2. *α é associado a β se, e somente se, $\langle\alpha\rangle = \langle\beta\rangle$.*

3. *α é unidade em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $\langle\alpha\rangle = \mathcal{O}_{\mathbb{K}}$.*

4. *α é irredutível em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $\langle\alpha\rangle$ é um ideal maximal de $\mathcal{O}_{\mathbb{K}}$.*

1.5 Fatoração de ideais em uma extensão

Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$. Nesta seção, veremos a decomposição de ideais primos não nulos $\mathcal{P}$ de A na extensão $\mathbb{L}$, ou seja, o ideal estendido $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ de $\mathcal{O}_{\mathbb{L}}$, que é expresso de modo único na forma $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, na qual os $\mathcal{Q}_i$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e os e_i são elementos de $\mathbb{Z}$, para $i = 1, \ldots, g$.

Proposição 1.5.1. *([10], p. 71) Os ideais primos $\mathcal{Q}_i$ da fatoração $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{Q}_i \cap A = \mathcal{P}$, para $i = 1, \ldots, g$.*

Demonstração: Seja $\mathcal{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Então, $\mathcal{Q} \cap A = \mathcal{P}$ se, e somente se, $\mathcal{Q} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}}$. De fato, se $\mathcal{Q} \cap A = \mathcal{P}$, então $\mathcal{P} \subset \mathcal{Q}$ e portanto, $\mathcal{P}\mathcal{O}_{\mathbb{L}} \subset \mathcal{Q}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}$. Por outro lado, se $\mathcal{Q} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} {\mathcal{Q}_i}^{e_i}$, então pela Proposição 1.3.5, segue que $\mathcal{Q} \supset \mathcal{Q}_i$, para algum i. Como $\mathcal{Q}_i$ é maximal, pois $\mathcal{O}_{\mathbb{L}}$ é Dedekind, segue que $\mathcal{Q}_i = \mathcal{Q}$. Como $\mathcal{Q} \subset \mathcal{O}_{\mathbb{L}}$ e $A \subset \mathcal{O}_{\mathbb{L}}$, pela Proposição 1.3.4, segue que $\mathcal{Q} \cap A$ é um ideal primo de

A e também $\mathcal{Q} \cap A \subsetneq A$, pois $1 \notin \mathcal{Q}$. Agora, como $\mathcal{P} \subset \mathcal{Q}$ e $\mathcal{P} \subset A$, segue que $\mathcal{P} \subset A \cap \mathcal{Q}$. Sendo A Dedekind, temos que $\mathcal{P} = A \cap \mathcal{Q}$, pois $\mathcal{P}$ é maximal. Assim, $\mathcal{Q}$ está na fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{Q} \cap A = \mathcal{P}$. ∎

Definição 1.5.1. *Se $\mathcal{P} \subset A$ e $\mathcal{Q} \subset \mathcal{O}_{\mathbb{L}}$ são ideais primos tal que $\mathcal{P} = A \cap \mathcal{Q}$, dizemos que $\mathcal{Q}$ está acima de $\mathcal{P}$.*

Observação 1.5.1. *Com as notações anteriores temos que*

1. *$\dfrac{A}{\mathcal{P}}$ e $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$ são corpos e que $\dfrac{A}{\mathcal{P}}$ pode ser identificado como um subcorpo de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$, para $i = 1, 2, \ldots, g$.*
2. *$\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$ é um espaço vetorial de dimensão finita sobre $\dfrac{A}{\mathcal{P}}$, para $i = 1, \ldots, g$.*

Segue diretamente da Observação 1.5.1 que se $\mathbb{K}$ é um corpo de números, $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$ e $\mathcal{P} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal primo, então $\mathcal{P} \cap \mathbb{Z} = \langle p \rangle$, em que $p \in \mathbb{Z}$, $[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}} : \mathbb{Z}_p] = f \leq n$ e $N(\mathcal{P}) = p^f$.

Definição 1.5.2. *Para $i = 1, 2, \ldots, g$ o grau $f_i = f(\mathcal{Q}_i|\mathcal{P})$ da extensão $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$ sobre $\dfrac{A}{\mathcal{P}}$ é chamado de grau de inércia de $\mathcal{O}_{\mathbb{L}}$ sobre A e o expoente $e_i = e(\mathcal{Q}_i|\mathcal{P})$ é chamado de índice de ramificação de $\mathcal{Q}_i$ sobre A.*

Definição 1.5.3. *Dizemos que $\mathcal{P}$ é:*

1. *totalmente decomposto em $\mathbb{L}$ (ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = f(\mathcal{Q}|\mathcal{P}) = 1$, para todo ideal primo $\mathcal{Q}$ que está acima de $\mathcal{P}$.*
2. *inerte em $\mathbb{L}$ (ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = 1$ e $f(\mathcal{Q}|\mathcal{P}) = n$, para todo ideal primo $\mathcal{Q}$ que está acima de $\mathcal{P}$.*
3. *totalmente ramificado em $\mathbb{L}$ (ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = n$ e $f(\mathcal{Q}|\mathcal{P}) = 1$, para todo ideal primo $\mathcal{Q}$ que está acima de $\mathcal{P}$.*
4. *ramificado em $\mathbb{L}$ (ou em $\mathcal{O}_{\mathbb{L}}$) se existir um ideal primo $\mathcal{Q}_i$ de $\mathcal{O}_{\mathbb{L}}$ que está acima de $\mathcal{P}$ tal que $e_i > 1$ para algum i.*

Observação 1.5.2. *Com as notações acima temos que*

1. $\mathcal{P}\mathcal{O}_{\mathbb{L}} \cap A = \mathcal{P}$.
2. $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}}$ *é um espaço vetorial de dimensão finita sobre* $\dfrac{A}{\mathcal{P}}$.

Proposição 1.5.2. *([10], p. 71) A sequência de ideais*

$$\mathcal{O}_{\mathbb{L}} \supset \mathcal{Q}_1 \supset \mathcal{Q}_1^2 \supset \ldots \supset \mathcal{Q}_1^{e_1} \supset \mathcal{Q}_1^{e_1}\mathcal{Q}_2 \supset \ldots \supset \mathcal{Q}_1^{e_1}\mathcal{Q}_2^{e_2} \supset \ldots \supset \mathcal{Q}_1^{e_1} \ldots \mathcal{Q}_g^{e_g} = \mathcal{P}\mathcal{O}_{\mathbb{L}}$$

é maximal.

Demonstração: Dois elementos desta sequência são da forma $\mathcal{Q}$ e $\mathcal{Q}\mathcal{Q}_i$, em que $\mathcal{Q}$ é o produto de ideais $\mathcal{Q}_j$. Se existir $\mathcal{D}$ tal que $\mathcal{Q}\mathcal{Q}_i \subset \mathcal{D} \subset \mathcal{Q}$, então pela Proposição 1.3.6 segue que $\mathcal{D}$ divide $\mathcal{Q}\mathcal{Q}_i$ e $\mathcal{Q}$ divide $\mathcal{D}$. Assim, existem $\mathcal{C}_1, \mathcal{C}_2 \subset \mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q}\mathcal{Q}_i = \mathcal{D}\mathcal{C}_1$ e $\mathcal{D} = \mathcal{Q}\mathcal{C}_2$. Logo, $\mathcal{Q}\mathcal{Q}_i = \mathcal{Q}\mathcal{C}_1\mathcal{C}_2$ e portanto, $\mathcal{Q}_i = \mathcal{C}_1\mathcal{C}_2$. Como $\mathcal{Q}_i$ é primo, segue que $\mathcal{C}_1 = A$ ou $\mathcal{C}_2 = A$. Assim, $\mathcal{Q}\mathcal{Q}_i = \mathcal{D}$ ou $\mathcal{D} = \mathcal{Q}$. Portanto, não existe ideal não trivial entre $\mathcal{Q}\mathcal{Q}_i$ e $\mathcal{Q}$. ∎

Teorema 1.5.1. *([10], p. 71)* **(Teorema da Igualdade Fundamental)**

$$\sum_{i=1}^{g} e_i f_i = [\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathcal{P}}] = n.$$

Demonstração: Primeiramente, vamos provar a primeira igualdade. Pela Observação 1.5.1, temos que $\dfrac{\mathcal{Q}}{\mathcal{Q}\mathcal{Q}_i}$ é um espaço vetorial sobre $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$, para $i = 1, 2, \ldots, g$ e pela Observação 1.5.2, tem-se que seus subespaços são os triviais. Assim, $dim_{\mathcal{O}_{\mathbb{L}}}\dfrac{\mathcal{Q}}{\mathcal{Q}\mathcal{Q}_i} = 1$ e $\#\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} = \#\dfrac{\mathcal{Q}}{\mathcal{Q}\mathcal{Q}_i}$. Como $[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} : \dfrac{A}{\mathcal{P}}] = f_i$ e $[\dfrac{\mathcal{Q}}{\mathcal{Q}\mathcal{Q}_i} : \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}] = 1$, segue que $[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} : \dfrac{A}{\mathcal{P}}] = f_i$. Dado um índice i, observemos que existem exatamente e_i elementos consecutivos na sequência dos ideais com o quociente da forma $\dfrac{\mathcal{Q}}{\mathcal{Q}\mathcal{Q}_i}$, ou seja, de dimensão f_i sobre $\dfrac{A}{\mathcal{P}}$. Assim, a dimensão total de $[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} : \dfrac{A}{\mathcal{P}}]$ é igual a soma das dimensões dos quocientes, ou seja,

$$[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathcal{P}}] = e_1 f_1 + \ldots + e_g f_g = \sum_{i=1}^{g} e_i f_i.$$

Agora, vamos provar a segunda igualdade. Como A é principal, pela Observação 1.2.1, segue que $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n. Se $\{x_1, \ldots, x_n\}$ é uma base

de $\mathcal{O}_{\mathbb{L}}$ sobre A, então $\{x_1+\mathcal{P}\mathcal{O}_{\mathbb{L}},\ldots,x_n+\mathcal{P}\mathcal{O}_{\mathbb{L}}\}$ é uma base de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}}$ sobre $\dfrac{A}{\mathcal{P}}$. De fato, se $\bar{b}\in\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}}$ tal que $\bar{b}=b+\mathcal{P}\mathcal{O}_{\mathbb{L}}$, então

$$\begin{aligned}(a_1x_1+\ldots+a_nx_n)+\mathcal{P}\mathcal{O}_{\mathbb{L}} &= (a_1x_1+\mathcal{P}\mathcal{O}_{\mathbb{L}})+\ldots+(a_nx_n+\mathcal{P}\mathcal{O}_{\mathbb{L}})\\ &= (a_1+\mathcal{P})(x_1+\mathcal{P}\mathcal{O}_{\mathbb{L}})+\ldots+(a_n+\mathcal{P})(x_n+\mathcal{P}\mathcal{O}_{\mathbb{L}})\\ &= \bar{a_1}\bar{x_1}+\ldots+\bar{a_n}\bar{x_n},\end{aligned}$$

com $\bar{a_i}\in\dfrac{A}{\mathcal{P}}$, para $i=1,\ldots,n$. Agora, se $\bar{a_1}\bar{x_1}+\ldots+\bar{a_n}\bar{x_n}=\bar{0}$, então $a_1x_1+\ldots+a_nx_n=\displaystyle\sum_{j=1}^{s}b_jp_j$, com $b_j\in\mathcal{O}_{\mathbb{L}}$ e $p_j\in\mathcal{P}$, para $j=1,\ldots,s$. Se $\{x_1,\ldots,x_n\}$ gera $\mathcal{O}_{\mathbb{L}}$ sobre A, então $b_j=\displaystyle\sum_{i=1}^{n}c_{ij}x_i$, com $c_{ij}\in A$, para $j=1,\ldots,n$. Logo, $\displaystyle\sum_{i=1}^{n}a_ix_i=\sum_{j=1}^{s}\left(\sum_{i=1}^{n}c_{ij}x_i\right)p_j=\sum_{i=1}^{n}\left(\sum_{j=1}^{s}c_{ij}p_j\right)x_i$. Como $\{x_1,\ldots,x_n\}$ é linearmente independente, segue que $a_i=\displaystyle\sum_{j=1}^{s}c_{ij}p_j\in\mathcal{P}$, ou seja, $\bar{a}_i=\bar{0}$, para $i=1,\ldots,n$. A demonstração para o caso geral é feita por redução ao caso anterior. Temos que A é um anel de Dedekind. Se $\mathcal{P}$ é um ideal primo não nulo de A tal que $S=A-\mathcal{P}$, então o anel de fração $S^{-1}A$ é um anel principal. Logo, $S^{-1}\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros de $\mathbb{L}$ sobre $S^{-1}A$ e $S^{-1}\mathcal{O}_{\mathbb{L}}$ é um $S^{-1}A$-módulo livre. Pelo caso anterior, segue que $\left[\dfrac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{P}}:\dfrac{S^{-1}A}{S^{-1}A\mathcal{P}}\right]=n$. Considerando a fatoração do ideal $\mathcal{P}S^{-1}\mathcal{O}_{\mathbb{L}}=\displaystyle\prod_{i=1}^{g}(S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i)^{e_i}$. Desde que, $\mathcal{Q}_i\cap A=\mathcal{P}$, $\mathcal{Q}_i\cap S=\emptyset$ e $S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i$ são ideais primos não nulos de $S^{-1}\mathcal{O}_{\mathbb{L}}$, temos pela primeira parte que

$$\left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{\mathcal{P}S^{-1}\mathcal{O}_{\mathbb{L}}}:\frac{S^{-1}A}{\mathcal{P}S^{-1}A}\right]=\sum_{i=1}^{g}e_i\left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i}:\frac{S^{-1}A}{\mathcal{P}S^{-1}A}\right].$$

Assim, $\dfrac{S^{-1}A}{\mathcal{P}S^{-1}A}\simeq\dfrac{A}{\mathcal{P}}$ e $\dfrac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i}\simeq\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$. Portanto, segue que

$$n=\left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i}:\frac{S^{-1}A}{\mathcal{P}S^{-1}A}\right]=\sum_{i=1}^{g}e_if_i.$$

■

Proposição 1.5.3. *([12], p. 125) Se $\mathcal{A}_1,\mathcal{A}_2$ são ideais de um anel A e $\mathcal{A}_1+\mathcal{A}_2=A$, então $\mathcal{A}_1\mathcal{A}_2=\mathcal{A}_1\cap\mathcal{A}_2$.*

Demonstração: Como $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1$ e $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_2$, segue que $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1 \cap \mathcal{A}_2$. Agora, suponhamos que $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Se $\mathcal{A}_1 + \mathcal{A}_2 = A$, então existem elementos $a_1 \in \mathcal{A}_1$ e $a_2 \in \mathcal{A}_2$ tais que $1 = a_1 + a_2$. Logo, $x = a_1x + a_2x$ é a soma de dois elementos de $\mathcal{A}_1\mathcal{A}_2$. Assim, $\mathcal{A}_1 \cap \mathcal{A}_2 \subset \mathcal{A}_1\mathcal{A}_2$. Portanto, $\mathcal{A}_1\mathcal{A}_2 = \mathcal{A}_1 \cap \mathcal{A}_2$. ■

Proposição 1.5.4. *([10], p. 18) Seja A um anel. Se $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ é um conjunto finito de ideais de A, tais que $\mathcal{A}_i + \mathcal{A}_j = A$ para $i \neq j$, então* $\dfrac{A}{\prod_{i=1}^{n} \mathcal{A}_i} \simeq \prod_{i=1}^{n} \dfrac{A}{\mathcal{A}_i}$.

Demonstração: Faremos a prova por indução sobre n. Para o caso $n = 2$, seja a aplicação $\varphi : A \longrightarrow \dfrac{A}{\mathcal{A}_1} \times \dfrac{A}{\mathcal{A}_2}$, definida por $\varphi(x) = (x+\mathcal{A}_1, x+\mathcal{A}_2)$ com $x \in A$. Assim $\ker(\varphi) = \mathcal{A}_1 \cap \mathcal{A}_2$, uma vez que, $\varphi(x) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $(x + \mathcal{A}_1, x + \mathcal{A}_2) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $x + \mathcal{A}_1 = \bar{0}$ e $x + \mathcal{A}_2 = \bar{\bar{0}}$ se, e somente se, $x \in \mathcal{A}_1$ e $x \in \mathcal{A}_2$ se, e somente se, $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Para a sobrejetora dado $y, z \in A$, devemos encontrar $x \in A$ tal que $(y + \mathcal{A}_1, z + \mathcal{A}_2) = (x + \mathcal{A}_1, x + \mathcal{A}_2) = \varphi(x)$. Como $\mathcal{A}_1 + \mathcal{A}_2 = A$, existem elementos $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$ tais que $1 = a_1 + a_2$. Seja, $x = a_1z + a_2y$. Como $a_2 \equiv 1(mod\ \mathcal{A}_1)$ e $a_1 \equiv 1(mod\ \mathcal{A}_2)$, segue que $x \equiv y(mod\ \mathcal{A}_1)$ e $x \equiv z(mod\ \mathcal{A}_2)$ o que implica, $x + \mathcal{A}_1 = y + \mathcal{A}_1$ e $x + \mathcal{A}_2 = z + \mathcal{A}_2$, ou seja, φ é sobrejetora. Portanto, $\dfrac{A}{\mathcal{A}_1 \cap \mathcal{A}_2} \simeq \dfrac{A}{\mathcal{A}_1} \times \dfrac{A}{\mathcal{A}_2}$ e pela Proposição 1.5.3, temos que $\dfrac{A}{\mathcal{A}_1\mathcal{A}_2} \simeq \dfrac{A}{\mathcal{A}_1} \times \dfrac{A}{\mathcal{A}_2}$. Agora, suponhamos que o resultado é verdadeiro para $n - 1$. Seja $\mathcal{B} = \mathcal{A}_2 \ldots \mathcal{A}_n$. Como $\mathcal{A}_1 + \mathcal{A}_i = A$, para $i \geq 2$, segue que existem elementos $c_i \in \mathcal{A}_1$ e $a_i \in \mathcal{A}_i$ tais que $c_i + a_i = 1$. Assim, $1 = \prod_{i=2}^{n} (c_i + a_i) = c + a_2 + \ldots + a_n$, em que c é a soma dos termos que contém no mínimo um c_i como fator. Logo, $c \in \mathcal{A}_1$. Como $a_2 \ldots a_n \in \mathcal{B}$, segue que $\mathcal{A}_1 + \mathcal{B} = A$. Pelo caso $n = 2$, segue que $\dfrac{A}{\mathcal{A}_1\mathcal{B}} \simeq \dfrac{A}{\mathcal{A}_1} \times \dfrac{A}{\mathcal{B}}$ e por hipótese de indução temos que $\dfrac{A}{\prod_{i=1}^{n} \mathcal{A}_i} \simeq \prod_{i=1}^{n} \dfrac{A}{\mathcal{A}_i}$. ■

Proposição 1.5.5. *([10]) Com as notações anteriores, temos que* $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} \simeq \prod_{i=1}^{g} \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i^{e_i}}$.

Demonstração: O único ideal maximal de $\mathcal{O}_{\mathbb{L}}$ que contém $\mathcal{Q}_i^{e_i}$ é $\mathcal{Q}_i$, pois se existir $\mathcal{M}$ um ideal maximal tal que $\mathcal{M} \supset \mathcal{Q}_i^{e_i}$, pela Proposição 1.3.5, tem-se que $\mathcal{M} \supset \mathcal{Q}_i$,

para algum i. Como $\mathcal{Q}_i$ é um ideal maximal, segue que $\mathcal{M} = \mathcal{Q}_i$. Vamos mostrar que $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$, para $i \neq j$. Se $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} \not\subseteq \mathcal{O}_{\mathbb{L}}$, então existe um ideal maximal $\mathcal{M}$ de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} \subset \mathcal{M} \subset \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{Q}_i^{e_i} \subset \mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j}$, segue que $\mathcal{Q}_i^{e_i} \subset \mathcal{M}$, ou seja, $\mathcal{Q}_i \subset \mathcal{M}$ e como $\mathcal{Q}_i$ é maximal, temos que $\mathcal{Q}_i = \mathcal{M}$. De modo análogo, como $\mathcal{Q}_j^{e_j} \subset \mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j}$, segue que $\mathcal{Q}_j^{e_j} \subset \mathcal{M}$, ou seja, $\mathcal{Q}_j \subset \mathcal{M}$ e tendo $\mathcal{Q}_j$ maximal, segue que $\mathcal{Q}_j = \mathcal{M}$. Assim, $\mathcal{Q}_i = \mathcal{Q}_j$, o que é um absurdo. Logo, $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$. Portanto, aplicando a Proposição 1.5.4, temos que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} \simeq \prod_{i=1}^{g} \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i^{e_i}}$. ■

Lema 1.5.1. *([10]) Seja A um domínio de Dedekind. Sejam $\mathcal{P}_1, \ldots, \mathcal{P}_r$ ideais primos distintos e não nulos de A, $x_1, \ldots, x_r \in A$ e $e_1, \ldots, e_r$ inteiros positivos. Então, existe um elemento $x \in A$ tal que $x - x_i \in \mathcal{P}_i^{e_i}$ e $x - x_i \notin \mathcal{P}_i^{e_i+1}$, para $i = 1, \ldots, r$.*

Demonstração: Para $i = 1, \ldots, r$ temos que $\mathcal{P}_i^{e_i} \not\supset \mathcal{P}_i^{e_i+1}$. Então, existe um elemento $a_i \in \mathcal{P}_i^{e_i}$, tal que $a_i \notin \mathcal{P}_i^{e_i+1}$. Pela Proposição 1.5.5, existe $x \in A$ tal que $x - (x_i + a_i) \in \mathcal{P}_i^{e_i+1}$, para $i = 1, \ldots, r$. Logo, $x - x_i = (x - (x_i + a_i)) + a_i \in \mathcal{P}_i^{e_i}$, mas $x - x_i \notin \mathcal{P}_i^{e_i+1}$, pois $a_i \notin \mathcal{P}_i^{e_i+1}$. ■

Proposição 1.5.6. *([10]) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de números, $\mathbb{K} \subset \mathbb{L}$ uma extensão de Galois finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$. Se $\mathcal{Q}_1$ e $\mathcal{Q}_2$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{Q}_1 \cap A = \mathcal{Q}_2 \cap A \neq 0$, então existe um $\mathbb{K}$-automorfismo σ de $\mathbb{L}$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_2$.*

Demonstração: Seja $G = \{\sigma_1, \ldots, \sigma_n\}$ o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\sigma_i(\mathcal{Q}_1) \neq \mathcal{Q}_2$, para todo $i = 1, \ldots, n$, pelo Lema 1.5.1, existe $x \in \mathcal{O}_{\mathbb{L}}$ tal que $x \notin \sigma_i(\mathcal{Q}_1)$, para $i = 1, \ldots, n$ e $x \in \mathcal{Q}_2$. Seja $a = \prod_{i=1}^{n} \sigma_i(x)$. Assim, $a \in \mathcal{Q}_2 \cap A$ e $a \notin \mathcal{Q}_1$, pois $\sigma_i(x) \notin \mathcal{Q}_1$, para $i = 1, \ldots, n$, o que é uma contradição. Portanto, existe $\sigma \in G$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_2$. ■

Teorema 1.5.2. *([10]) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subset \mathbb{L}$ uma extensão de Galois finita de grau n, $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$ e $\mathcal{P}$ um ideal primo de A. Se $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ e $[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} : \dfrac{A}{\mathcal{P}}] = f_i$, então $e_1 = e_2 = \ldots = e_g$, $f_1 = f_2 = \ldots = f_g$ e os corpos $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$, $i = 1, \ldots, g$, são isomorfos.*

Demonstração: Pela Proposição 1.5.6, para cada $i = 1, \ldots, g$, existe $\sigma \in G$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_i$. Assim, temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \sigma(\mathcal{P}\mathcal{O}_{\mathbb{L}}) = \prod_{i=1}^{g} \sigma(\mathcal{Q}_i)^{e_i}$. Pela unicidade da fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$, segue que $e_i = e$ para cada $i = 1, \ldots, g$. Finalmente, como $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} = \frac{\mathcal{O}_{\mathbb{L}}}{\sigma(\mathcal{Q}_1)} \simeq \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_1}$ segue que $f_1 = f_i$ para $i = 1, \ldots, g$. ■

Observação 1.5.3. *Com as hipóteses do Teorema 1.5.2, temos que $efg = n$.*

1.6 Corpos quadráticos

Esta seção, tem por objetivo introduzir o conceito de corpos quadráticos, bem como suas principais proprieddes.

Definição 1.6.1. *Um número inteiro racional é dito livre de quadrados se ele não é divisível por um quadrado de um número primo.*

Definição 1.6.2. *Um corpo quadrático é uma extensão de grau 2 de $\mathbb{Q}$ da forma $\mathbb{Q}(\sqrt{d})$, em que d é um inteiro livre de quadrados.*

Observação 1.6.1. *O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $x^2 - d$. O conjugado de $\sqrt{d}$ é -$\sqrt{d}$, ou seja, existe um automorfismo $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ tal que $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.*

Proposição 1.6.1. *([10], p. 35) Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados sobre $\mathbb{Z}$. Se $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$, então $2a \in \mathbb{Z}$ e $2b \in \mathbb{Z}$.*

Demonstração: Pela Observação 1.6.1, existe um automorfismo σ de $\mathbb{K}$ tal que $\sigma(\alpha) = \sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Como $\sigma(\alpha)$ também é raiz da mesma equação de dependência integral de α, segue que $\sigma(\alpha) \in \mathcal{O}_{\mathbb{K}}$. Como α e $\sigma(\alpha) \in \mathcal{O}_{\mathbb{K}}$, pelo Corolário 1.2.2, segue que $\alpha + \sigma(\alpha) \in \mathcal{O}_{\mathbb{K}}$ e $\alpha\sigma(\alpha) \in \mathcal{O}_{\mathbb{K}}$. Além disso, $\alpha + \sigma(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Z}$ e $\alpha\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}$. Como $\mathbb{Z}$ é um anel de ideais principais, segue que $\mathbb{Z}$ é integralmente fechado. Logo, se

$$2a \in \mathbb{Z} \quad \text{e} \quad a^2 - db^2 \in \mathbb{Z}, \tag{1.3}$$

então $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Como $2a \in \mathbb{Z}$, segue que $(2a)^2 \in \mathbb{Z}$. Por outro lado, $2b \notin \mathbb{Z}$ e o seu denominador tem um fator primo p e este fator aparece como p^2 no denominador de $d(2b)^2$. Sendo d livre de quadrados, segue que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Portanto, $2b \in \mathbb{Z}$. ■

Teorema 1.6.1. *([10], p. 35) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, tal que $d \not\equiv 0(mod\ 4)$.*

1. *Se $d \equiv 2$ ou $d \equiv 3(mod\ 4)$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$, consiste de todos os elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$.*

2. *Se $d \equiv 1(mod\ 4)$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$, consiste de todos os elementos da forma $\frac{1}{2}(a + b\sqrt{d})$, com $a, b \in \mathbb{Z}$ e de mesma paridade.*

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$. Pela Proposição 1.6.1, temos que $a = \frac{u}{2}$ e $b = \frac{v}{2}$, com $u, v \in \mathbb{Z}$. De (1.3) tem-se que $u^2 - dv^2 \in 4\,\mathbb{Z}$.

1. Se $d \equiv 2$ ou $d \equiv 3(mod\ 4)$, então u, v são pares, pois se v fosse ímpar, teríamos $v^2 \equiv 1\ (mod\ 4)$. Como $u^2 - dv^2 \in 4\mathbb{Z}$, segue que $u^2 - d(4k+1) \in 4\mathbb{Z}$ o que implica $u^2 - d \in 4\mathbb{Z}$, ou seja, $u^2 \equiv d(mod\ 4)$. Portanto, $d \equiv 1(mod\ 4)$ ou $d \equiv 0(mod\ 4)$, o que contradiz a hipótese. Sendo v par, temos que $v^2 \equiv 0(mod\ 4)$, portanto $u^2 \in 4\mathbb{Z}$. Assim, u também é par. Então $a, b \in \mathbb{Z}$ e $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$. Portanto, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{K}}$. Assim, $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_{\mathbb{K}}$.

2. Se $d \equiv 1\ (mod\ 4)$, então u, v tem a mesma paridade, uma vez que se v é par, pelo item 1 tem-se que u é par. Assim, $a, b \in \mathbb{Z}$ e portanto, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se v é ímpar, então $v^2 \equiv 1\ (mod\ 4)$ e sendo $d \equiv 1\ (mod\ 4)$, segue que $u^2 - 1 \in 4\mathbb{Z}$, ou seja, $u^2 \equiv 1\ (mod\ 4)$. Logo, u é ímpar. Assim, $\alpha = \frac{u}{2} + \frac{v\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Por outro lado, se $\alpha = a + b(\frac{1+\sqrt{d}}{2}) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, com $a, b \in \mathbb{Z}$, então α é raiz do polinômio $x^2 - (2a+b)x + (a^2 + ab - \frac{(1-d)b^2}{4}) \in \mathbb{Z}[x]$, pois $d \equiv 1(mod\ 4)$. Assim, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathcal{O}_{\mathbb{K}}$. ■

Observação 1.6.2. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático.*

1. *Se $d \not\equiv 1 \ (mod\ 4)$, então seu discriminante é $4d$.*

2. *Se $d \equiv 1 \ (mod\ 4)$, então seu discriminante é d.*

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Não temos, em geral, para $\mathcal{O}_{\mathbb{K}}$ um teorema de fatoração única em elementos primos como temos para $\mathbb{Z}$.

Proposição 1.6.2. *([12], p. 88) Sejam $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ e $\pi \in \mathcal{O}_{\mathbb{K}}$. Se $N(\pi) = p \in \mathbb{Z}$, em que $\pi \in \mathcal{O}_{\mathbb{K}}$ é um número primo, então π é elemento irredutível em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Temos que $\pi \neq 0$ e não é um elemento inversível, pois $N(\pi) = p$ é um número primo. Agora se $\pi = \alpha\beta$, com $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$, então $p = N(\pi) = N(\alpha)N(\beta)$. Assim, $N(\alpha) = \pm 1$ ou $N(\beta) = \pm 1$. Logo, α é inversível ou β é inversível. Como $\pi \neq 0$ e não é inversível, segue que π é um elemento irredutível. ∎

O próximo teorema mostra que toda não unidade em $\mathcal{O}_{\mathbb{K}}$ tem uma decomposição em elementos irredutíveis de $\mathcal{O}_{\mathbb{K}}$. Em geral, essa decomposição não é única e assim os anéis $\mathcal{O}_{\mathbb{K}}$ em geral não são fatoriais. Vejamos inicialmente como os inteiros primos se fatoram em $\mathcal{O}_{\mathbb{K}}$.

Proposição 1.6.3. *([12], p. 88) Seja $p \in \mathbb{Z}$ um número primo.*

1. *Se existir $\pi \in \mathcal{O}_{\mathbb{K}}$ tal que $N(\pi) = p$, então $p = \pi\bar{\pi}$ é uma fatoração de p em elementos irredutíveis de $\mathcal{O}_{\mathbb{K}}$.*

2. *Caso contrário, p é irredutível em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: A afirmação 1 é verdadeira pela Proposição 1.6.2. Agora, suponhamos que o item 1 não ocorre. Se $p = \alpha\beta$ com $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$, então $p^2 = N(p) = N(\alpha)N(\beta)$. Como $N(\alpha), N(\beta) \in \mathbb{Z}$ e $N(\alpha) = p = N(\beta)$ não ocorre, pois estamos excluindo o item 1, segue que $N(\alpha) = \pm 1$ e $N(\beta) = \pm p^2$ ou $N(\alpha) = \pm p^2$

e $N(\beta) = \pm 1$. Logo, $\alpha \in \mathcal{O}_{\mathbb{K}}^*$ ou $\beta \in \beta_{\mathbb{K}}^*$ e assim, p é um elemento irredutível em $\mathcal{O}_{\mathbb{K}}$. ■

Observação 1.6.3. *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, onde $\alpha \neq 0$ e α não é inversível, então α é um produto de elementos irredutíveis.*

A Observação 1.6.3 tem uma falha, uma vez que não se pode assegurar sua unicidade. Por exemplo: $2.3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Temos assim uma decomposição de 6 de duas maneiras que são claramente distintas. Para termos fatoração única devemos exigir um pouco mais dos fatores.

A seguir veremos que se existir uma fatoração em elementos primos, temos que essa fatoração é necessariamente única.

Proposição 1.6.4. *([12], p. 87)*

1. *Todo primo em $\mathcal{O}_{\mathbb{K}}$ é um elemento irredutível.*

2. *Sejam $\pi_1, \pi_2, \ldots, \pi_r$ e $\rho_1, \rho_2, \ldots, \rho_s$ com $r, s \geq 1$, são elementos primos de $\mathcal{O}_{\mathbb{K}}$ tais que $\pi_1\pi_2 \ldots \pi_r = \rho_1\rho_2 \ldots \rho_s$. Então, $r = s$ e para cada $1 \leq i \leq r$ existe um único $1 \leq j \leq s$ tal que π_i e ρ_j são associados em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração:

1. Seja π um elemento primo de $\mathcal{O}_{\mathbb{K}}$. Assim, $\pi \neq 0$ e não é inversível. Agora, sejam $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tais que $\pi = \alpha\beta$. Logo, se π divide $\alpha\beta$, então π divide α ou π divide β. Se π divide α, então existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\alpha = \pi\gamma$. Assim, $\pi = \pi\gamma\beta$ e portanto, $1 = \gamma\beta$ e $\beta \in \mathcal{O}_{\mathbb{K}}^*$. Analogamente, se π divide β, então $\alpha \in \mathcal{O}_{\mathbb{K}}^*$.

2. Faremos a prova por indução sobre r. Se $r = 1$, então $\pi_1 = \rho_1 \ldots \rho_s$. Pela definição de elemento primo, segue que existe $1 \leq j \leq s$ tal que $\pi_1 \mid \rho_j$. Pelo item 1 concluímos que π_1 e ρ_j são associados pois nenhum dos dois é uma unidade. Assim, se $\pi_1 = \mu\rho_j$, em que $\mu \in \mathcal{O}_{\mathbb{K}}^*$, então $\mu\rho_j = \rho_1 \ldots \rho_s$. Cancelando ρ_j de ambos os lados da igualdade obtemos uma contradição se

$s > 1$ e portanto $\pi_1 = \rho_1$. Assumimos agora o resultado para todo $1 \leq r < n$ e suponhamos que $\pi_1\pi_2 \ldots \pi_r = \rho_1\rho_2 \ldots \rho_s$ onde $\pi_i = \rho_j$, para $i = 1, 2, \ldots, r$ e $j = 1, 2, \ldots, s$, são elementos primos. Suponhamos que $r < s$. Da igualdade acima, segue que π_1 divide $\rho_1 \ldots \rho_s$. Como π_1 é primo, segue que π_1 divide ρ_j, para algum $j = 1, 2, \ldots, s$. Sem perda de generalidade, podemos supor que $j = 1$. Como todo primo é irredutível, segue que π_1 e ρ_1 são associados. Assim, existe $\mu_1 \in A^*$ tal que $\rho_1 = \mu_1\pi_1$. ■

Definição 1.6.3. *Um domínio de integridade $\mathcal{D}$ é chamado de domínio de fatoração única se toda não unidade $a \in \mathcal{D}$, $a \neq 0$ é um produto de elementos irredutíveis e todo irredutível é primo.*

Agora, examinamos uma condição necessária para que todo irredutível seja primo e exibimos alguns valores de d para os quais isso acontece. Primeiramente, recordamos a definição de domínio euclidiano.

Definição 1.6.4. *Dizemos que um domínio $\mathcal{D}$ é euclidiano se existir uma função $\psi : \mathcal{D} - \{0\} \to \mathbb{N}$ tal que*

1. *Se $a, b \in \mathcal{D} - \{0\}$ tal que $a|b$, então $\psi(a) \leq \psi(b)$.*

2. *Se $a, b \in \mathcal{D} - \{0\}$, então existe $q, r, \in \mathcal{D}$ tal que $a = bq + r$ em que $\psi(r) < \psi(b)$.*

A função ψ é chamada de norma euclidiana.

Teorema 1.6.2. *([13], p. 54) Seja $\mathcal{D}$ um domínio euclidiano com norma euclidiana ψ.*

1. *Para todo par $a, b \in \mathcal{D}$ existem $m, n \in \mathcal{D}$ tais que $d = am + bn = mdc(a, b)$.*

2. *Todo irredutível é primo.*

Demonstração:

1. Se a divide b, então o $mdc(a, b) = a = a.1 + b.0$. Igualmente, se b divide a, então a afirmação é verdadeira. Suponhamos que a não divide b e que b não divide a.

Consideremos o conjunto $J = \{\psi(ax+by) : x, y \in \mathcal{D}, ax+by \neq 0\}$. Temos que, J não é vazio e portanto, tem um menor elemento. Sejam $d \in \mathcal{D}$ tal que $\psi(d)$ é um mínimo de J e $m, n \in \mathcal{D}$ tais que $d = am + bn$. Agora, verificamos que $d = mdc(a, b)$. Como $\mathcal{D}$ é euclidiano, segue que $q, r \in \mathcal{D}$ tais que $a = dq + r$, com $r = 0$ ou $\psi(r) < \psi(d)$. Se $r \neq 0$, com $r = a(1 - qm) + b(-qn)$, então $\psi(r) \in J$. Como $\psi(r) < \psi(d)$, segue que isso contradiz a escolha de d. Logo, $r = 0$ e d divide a. Igualmente d divide b. Seja agora, $\bar{d}$ um divisor comum de a e b. Como d é combinação linear de a e b, segue que $\bar{d}$ divide d.

2. Seja $\pi \in \mathcal{D}$ irredutível e suponhamos que π divide ab, com $a, b \in \mathcal{D}$. Suponhamos que π não divide a e seja $d = \pi m + an = mdc(\pi, a)$. Como d divide π, segue que $d \in \mathcal{D}$ ou d é associado a π. Se d é associado a π, então π divide a, que é contra nossa suposição. Como $d \in \mathcal{D}^*$, segue que d é associado a 1. Logo, 1 também é um $mdc(a, b)$. Sem perda de generalidade, assumimos que $d = 1$. Como π divide ab, segue que existe $c \in \mathcal{D}$ tal que $ab = \pi c$. Assim, $b = b\pi m + ban = \pi(bm + cn)$ e portanto, π divide b. ■

1.6.1 Decomposição de ideais em corpos quadráticos

Nesta seção, apresentamos especificamente a decomposição nos corpos quadráticos.

Sejam $d \in \mathbb{Z}$ livre de quadrados, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$ e p um número primo. Seja $p\mathcal{O}_\mathbb{K} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ a decomposição em $\mathbb{K}$ do ideal $p\mathcal{O}_\mathbb{K}$ como um produto de ideais primos de $\mathcal{O}_\mathbb{K}$. Pelo Teorema da Igualdade Fundamental, segue que $\sum_{i=1}^{g} e_i f_i = 2$. Assim, $g \leq 2$ e temos os seguintes casos:

1. Se $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, então p se decompõe em $\mathbb{K}$, ou seja, $p\mathcal{O}_\mathbb{K} = \mathcal{Q}_1\mathcal{Q}_2$, em que $\mathcal{Q}_1, \mathcal{Q}_2$ são ideais primos distintos de $\mathcal{O}_\mathbb{K}$ acima de $p\mathbb{Z}$.

2. Se $g = 1$, $e_1 = 1$, $f_1 = 2$, então p é inerte em $\mathbb{K}$, ou seja, $p\mathcal{O}_\mathbb{K} = \mathcal{Q}$, em que $\mathcal{Q}$ é um ideal primo de $\mathcal{O}_\mathbb{K}$ acima de $p\mathbb{Z}$.

3. Se $g = 1$, $e_1 = 2$, $f_1 = 1$, então p ramifica em $\mathbb{K}$, ou seja, $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^2$, em que $\mathcal{Q}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$.

Definição 1.6.5. *Dado um número primo ímpar p e um inteiro d relativamente primo com p, dizemos que d é um resíduo quadrático módulo p, se existir $a \in \mathbb{Z}$ tal que $d \equiv a^2 (mod\ p)$, isto é, se a classe de restos de d módulo p for um quadrado em $\mathbb{Z}_p$, caso contrário, d não é resíduo quadrático módulo p.*

Exemplo 1.6.1. *Se $p = 5$, então $d = 19$ é um resíduo quadrático módulo 5, pois existe $a = 2$ tal que $19 \equiv 2^2 (mod\ 5)$. Se $p = 7$, então $d = 19$ não é resíduo quadrático módulo 7, pois não existe a tal que $19 \equiv a^2 (mod\ 7)$.*

Teorema 1.6.3. *([10], p. 77) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, em que d é um inteiro livre de quadrados.*

1. *Os primos ímpares p, em que d é um resíduo quadrático módulo p, decompõem em $\mathcal{O}_{\mathbb{K}}$.*

2. *Os primos ímpares p, em que d não é um resíduo quadrático módulo p, são inertes em $\mathcal{O}_{\mathbb{K}}$.*

3. *Os primos ímpares divisores de d ramificam em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Se p é ímpar, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ ou $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Agora, se $\alpha = a + \left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ com b ímpar, então $\alpha \equiv a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right)$ $(mod\ p)$. Assim, $\alpha' = a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\sqrt{d}]$ e $\alpha \equiv \alpha' (mod\ p)$. Portanto, $\frac{\mathcal{O}_{\mathbb{K}}}{p\mathcal{O}_{\mathbb{K}}}$ é isomorfo a $\frac{\mathbb{Z}[\sqrt{d}]}{p\mathcal{O}_{\mathbb{K}}}$. Por outro lado, temos que $\frac{\mathbb{Z}[x]}{\langle x^2 - d\rangle}$ é isomorfo a $\mathbb{Z}[\sqrt{d}]$ e portanto, $\frac{\mathcal{O}_{\mathbb{K}}}{p\mathcal{O}_{\mathbb{K}}} \simeq \frac{\mathbb{Z}[x]}{\langle p, x^2 - \bar{d}\rangle} \simeq \frac{\mathbb{Z}_p[x]}{\langle x^2 - \bar{d}\rangle}$, na qual $\bar{d}$ é a classe de resíduo de d módulo p.

1. Se $d \equiv x^2 (mod\ p)$, então $x^2 - \bar{d} \in \mathbb{Z}_p[x]$. Portanto, $x^2 - \bar{d} = (x - \sqrt{d})(x + \sqrt{d})$, na qual $h_1(x) = x - \sqrt{d}$ e $h_2(x) = x + \sqrt{d}$ são polinômios irredutíveis distintos

tais que $\langle h_1 h_2\rangle = \langle h_1\rangle \cap \langle h_2\rangle$ e $\langle h_1 + h_2\rangle = \mathbb{Z}_p[x]$. Assim, $\dfrac{\mathcal{O}_{\mathbb{K}}}{p\mathcal{O}_{\mathbb{K}}} = \dfrac{\mathbb{Z}_p[x]}{\langle x^2 - d\rangle} \simeq \dfrac{\mathbb{Z}_p[x]}{\langle x - \sqrt{d}\rangle} \times \dfrac{\mathbb{Z}_p[x]}{\langle x + \sqrt{d}\rangle}$. Como $\dfrac{\mathbb{Z}_p[x]}{\langle x - \sqrt{d}\rangle}$ e $\dfrac{\mathbb{Z}_p[x]}{< x + \sqrt{d} >}$ são corpos, segue que $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2$, com $\mathcal{Q}_1$ e $\mathcal{Q}_2$ primos distintos, ou seja, p se decompõe em $\mathcal{O}_{\mathbb{K}}$.

2. Se $d \not\equiv x^2 (mod\ p)$, então $x^2 - \bar{d}$ é irredutível em $\mathbb{Z}_p[x]$ e $\dfrac{\mathcal{O}_{\mathbb{K}}}{p\mathcal{O}_{\mathbb{K}}}$ é isomorfo a um corpo. Assim, $p\mathcal{O}_{\mathbb{K}}$ permanece primo, ou seja, p é inerte em $\mathcal{O}_{\mathbb{K}}$.

3. Se p é um divisor de d temos que $x^2 - \bar{d}$ é um quadrado de um polinômio irredutível. Assim, $\dfrac{\mathcal{O}_{\mathbb{K}}}{p\ \mathcal{O}_{\mathbb{K}}} \simeq \dfrac{\mathbb{Z}_p[x]}{\langle h^2\rangle}$ e o elemento $h + \langle h^2\rangle$ é não nulo e nilpotente. Então, p ramifica em $\mathcal{O}_{\mathbb{K}}$. ■

Exemplo 1.6.2. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{10})$. *Como* 5 *divide* 10, *temos pelo Teorema 1.6.3, que* 5 *ramifica em* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{10}]$ *com* $e = 2$ *e* $f = 1$. *Se* $p = 3$, *então* 10 *é resíduo quadrático módulo* 3. *Logo,* 3 *decompõe com* $e = 1$ *e* $f = 1$. *Se* $p = 7$, *então* 10 *não é resíduo quadrático módulo* 7 *e assim,* 7 *é inerte.*

Teorema 1.6.4. *([10], p. 77) Se* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *é um corpo quadrático, em que* d *é um inteiro livre de quadrados, então*

1. *Se* $d \equiv 1 (mod\ 8)$, *então* 2 *se decompõe em* $\mathcal{O}_{\mathbb{K}}$.

2. *Se* $d \equiv 5 (mod\ 8)$, *então* 2 *é inerte em* $\mathcal{O}_{\mathbb{K}}$.

3. *Se* $d \equiv 2 (mod\ 4)$ *ou* $d \equiv 3 (mod\ 4)$, *então* 2 *ramifica em* $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Se $d \equiv 1 (mod\ 4)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$ e o polinômio minimal de $\dfrac{1+\sqrt{d}}{2}$ é $x^2 - x - \dfrac{d-1}{4}$. Assim, $\mathcal{O}_{\mathbb{K}}$ é isomorfo a $\dfrac{\mathbb{Z}[x]}{\langle x^2 - x - a\rangle}$, na qual $a = \dfrac{d-1}{4}$ e portanto, $\dfrac{\mathbb{Z}}{2\mathcal{O}_{\mathbb{K}}} \simeq \dfrac{\mathbb{Z}_2[x]}{\langle x^2 - x - \bar{a}\rangle}$.

1. Se $d \equiv 1 (mod\ 8)$, então $2k = \dfrac{d-1}{4}, k \in \mathbb{Z}$. Assim, $a \equiv 0 (mod\ 2)$ e $x^2 - x - \bar{a} \equiv x^2 + x \equiv x(x+1) (mod\ 2)$. Portanto, $\dfrac{\mathcal{O}_{\mathbb{K}}}{2\mathcal{O}_{\mathbb{K}}}$ é um produto de dois corpos, ou seja, 2 decompõe em $\mathcal{O}_{\mathbb{K}}$.

2. Se $d \equiv 5(mod\ 8)$, então $2k = \dfrac{d-1-4}{4}$, para $k \in \mathbb{Z}$. Assim, $a \equiv 1(mod\ 2)$ e $x^2 - x - \bar{a} \equiv x^2 + x + \bar{1}(mod\ 2)$. Como $x^2 + x + \bar{1}$ é irredutível, segue que 2 permanece primo em $\mathcal{O}_{\mathbb{K}}$.

3. Se $d \equiv 2$ ou $d \equiv 3(mod\ 4)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ e $\dfrac{\mathcal{O}_{\mathbb{K}}}{2\mathcal{O}_{\mathbb{K}}}$ é isomorfo a $\dfrac{\mathbb{Z}_p[x]}{\langle x^2 - \bar{d}\rangle}$. Neste caso, $x^2 - \bar{d} = x^2$ ou $x^2 - \bar{1} = (x^2-1)^2$ e ambos os casos é um quadrado. Assim, $\dfrac{\mathbb{Z}_p[x]}{\langle x^2 - \bar{d}\rangle}$ possui um elemento nilpotente não nulo. Logo, 2 ramifica em $\mathcal{O}_{\mathbb{K}}$. ■

Um método prático para determinar o tipo de decomposição em $\mathcal{O}_{\mathbb{K}}$ de cada número primo p é através da Lei da Reciprocidade Quadrática de Gauss, devido a Legendre e Gauss. Para isso, vamos introduzir o símbolo de Legendre $\left(\dfrac{d}{p}\right)$.

Definição 1.6.6. *Sejam p um número inteiro primo e d um inteiro primo com p. O símbolo de Legendre é dada por*

$$\begin{cases} \left(\dfrac{d}{p}\right) = 1 \quad se \quad d \quad é\ um\ resíduo\ quadrático\ módulo \quad p, \\ \left(\dfrac{d}{p}\right) = -1 \quad se \quad d \quad não\ é\ um\ resíduo\ quadrático\ módulo \quad p. \end{cases}$$

Observação 1.6.4.

1. *(Critério de Euler) Se p é um primo ímpar e $a \in \mathbb{Z}$, então $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ $(mod\ p)$. Em particular, $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.*

2. *(Lei da Reciprocidade Quadrática de Gauss) Se p e q são números primos ímpares, então*
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proposição 1.6.5. *([14]) Seja p um primo ímpar, para $d = -1, -3$ temos que*

1. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ tal que $p \equiv 1\ (mod\ 4)$, então p se decompõe em $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$.*

2. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ tal que $p \equiv 1\ (mod\ 6)$, então p se decompõe em $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.*

Demonstração:

1. Se $p \equiv 1 \ (mod\ 4)$, então $p = 4t + 1$, para algum t. Pelo Critério de Euler, temos que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4t+1-1}{2}} = (-1)^{\frac{4t}{2}} = 1$. Logo, $d = -1$ é um resíduo quadrático módulo p. Assim, pela Proposição 1.6.3, segue que p se decompõe em $\mathcal{O}_{\mathbb{K}}$.

2. Se $p \equiv 1 \ (mod\ 6)$, então $p = 6t + 1$, para algum t. Pela Lei da Reciprocidade Quadrática de Gauss, tomando $q = d = -3$ tem-se que $\left(\frac{-3}{p}\right)\left(\frac{p}{-3}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \frac{(6t+1-1)(-3-1)}{4} = (-1)^{6t} = 1$. Logo, $d = -3$ é um resíduo quadrático. Assim, pela Proposição 1.6.3, segue que p se decompõe em $\mathcal{O}_{\mathbb{K}}$. ■

1.7 Corpos ciclotômicos

Nesta seção, apresentamos os corpos ciclotômicos. Esses corpos tem um papel fundamental na teoria álgebrica dos números, uma vez que é possível caracterizar o anel de inteiros algébricos de um corpo ciclotômico.

Definição 1.7.1. *Seja $\mathbb{L}$ um corpo. Um elemento $\xi \in \mathbb{L}$ tal que $\xi^n = 1$ é chamado uma raiz n-ésima da unidade. Dizemos que ξ é uma raiz n-ésima primitiva da unidade se $\xi^n = 1$ e $\xi^m \neq 1$, para todo $0 < m < n$.*

Uma raiz n-ésima primitiva da unidade ξ_n pode ser escrito como $\xi_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\text{sen}(\frac{2\pi}{n})$, em que $n \in \mathbb{N}$. Neste capítulo, ξ_n será sempre uma raiz n-ésima primitiva da unidade.

Definição 1.7.2. *Um corpo ciclotômico é um corpo gerado por uma raiz n-ésima da unidade.*

Definição 1.7.3. *O polinômio $\phi_n(x) = \prod_{j=1}^{n}(x - \xi_n^j)$, na qual $mdc(j, n) = 1$ é chamado de n-ésimo polinômio ciclotômico.*

Proposição 1.7.1. *([15], p. 206) Se n é um inteiro positivo, então $x^n - 1 = \prod_{h|n} \phi_h(x)$.*

Demonstração: Seja $f(x) = x^n - 1$ tal que $1, w, w^2, \ldots, w^{n-1}$ são as raízes. Logo, podemos escrever $f(x)$ como $f(x) = (x-1)(x-w)\ldots(x-w^{n-1})$. Assim, analisando as ordens de cada raiz de $f(x)$ e escrevendo todas as raízes de mesma ordem como um polinômio da forma $\phi_n(x) = \prod_{\text{ordem } w=h}(x-w)$, tem-se que $x^n - 1 = \prod_{h|n} \phi_h(x)$. ■

Da Proposição 1.7.1, obtemos que $\phi_n(x) = \dfrac{x^n-1}{\prod_{h|n}\phi_h(x)}$. Logo, $\phi_1(x) = x - 1$, $\phi_2(x) = \dfrac{x^2-1}{\phi_1(x)} = x + 1$, $\phi_3(x) = \dfrac{x^3-1}{\phi_1(x)} = x^2 + x + 1, \ldots$, etc. Quando $n = p$, em que p é um número primo, temos que

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

é chamado de p-ésimo polinômio ciclotômico. E quando $n = p^r$, na qual $r \in \mathbb{Z}$ tal que $r > 1$ e p é um número primo, temos que $x^{p^r} - 1 = \phi_1(x)\phi_p(x)\ldots\phi_{p^{r-1}}(x)\phi_{p^r}(x)$ e $x^{p^{r-1}} - 1 = \phi_1(x)\phi_p(x)\ldots\phi_{p^{r-1}}(x)$. Logo,

$$\phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \ldots + x^{p^{r-1}} + 1 \tag{1.4}$$

é o p^r-ésimo polinômio ciclotômico.

Observação 1.7.1. *Seja ξ_n é uma raiz n-ésima primitiva da unidade.*

1. $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$, *na qual φ é a função de Euler.*

2. *O n-ésimo polinômio ciclotômico é irredutível sobre $\mathbb{Q}$.*

3. *O anel de inteiros de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$ e $\{1, \xi_n, \ldots, \xi_n^{\varphi(n)-1}\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}[\xi_n]$.*

4. *Se $mdc(m, n) = 1$, então $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{mn})$.*

5. *O discriminante absoluto de $\mathbb{K} = \mathbb{Q}(\xi_n)$ sobre $\mathbb{Q}$ é*

$$D_{\mathbb{K}} = D_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1, \xi_n, \ldots, \xi_n^{\varphi(n)-1}) = \pm\frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

1.7.1 Decomposição de ideais em corpos ciclotômicos

Nesta seção, apresentamos especificamente a decomposição de ideais em corpos ciclotômicos.

Teorema 1.7.1. *([12], p. 186)***(Lema de Kummer)** *Sejam $\mathbb{K}$ um corpo de números de grau n com ordem maximal $\mathcal{D}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$, $\alpha \in \mathcal{O}_{\mathbb{K}}$ e p um número primo. Se $\overline{m(x)} = \overline{m_1(x)^{e_1}} \dots \overline{m_r(x)^{e_r}}$ é a fatoração do polinômio minimal $m(x)$ de α em $\mathbb{Z}[x]$, como um produto de polinômios irredutíveis de grau d_i, para $i = 1, \dots, r$, sobre $\mathbb{Z}_p[x]$, em que $\bar{\cdot}$ denota a aplicação $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, então o ideal $\langle p \rangle$ de $\mathbb{Z}$ decompõe-se de modo único da forma*

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r},$$

como um produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$, na qual $\mathcal{P}_i = \langle p, m_i(\alpha) \rangle$ e $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_i} \cong GF(p^{d_i})$, para $i = 1, \dots, r$.

Demonstração: Sejam $\bar{\mu}(x)$ um fator irredutível de $\bar{m}(x)$, $\bar{\alpha}$ uma raiz de $\bar{\mu}(x)$ e $\mathcal{P}$ o ideal primo de $\mathcal{O}_{\mathbb{K}}$ que é o Kernel da função $\phi : \mathbb{Z}[\alpha] \to \bar{\mathbb{Z}}[\bar{\alpha}]$. Temos que $p\mathcal{O}_{\mathbb{K}} + \mu(\alpha)\mathcal{O}_{\mathbb{K}}$ está contido em $\mathcal{P}$. Por outro lado, se $g(\alpha) \in \mathcal{P}$, onde $g(\alpha) \in \mathbb{Z}[x]$, então $\bar{g}(x) = \overline{\mu(x)h(x)}$, para algum $\bar{h}(x) \in \bar{A}[x]$ e portanto, $g(x) - \mu(x)h(x)$, que é um polinômio com coeficientes em $\mathbb{Z}$, uma vez que tem coeficientes em $p\mathcal{O}_{\mathbb{K}}$. Logo, $\mathcal{P}_i = p\mathcal{O}_{\mathbb{K}} + \mu_i(\alpha)\mathcal{O}_{\mathbb{K}}$. Agora, sejam $e_i^{'}$ o índice de ramificação de $\mathcal{P}_i$ tal que

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_1^{'}} \dots \mathcal{P}_r^{e_r^{'}}$$

e d_i o grau de $\bar{\mu}_i$. Como $m(\alpha) = 0$ e $m(x) - \mu_1(x)^{e_1} \dots \mu_r(x)^{e_r} \in pZ[x]$, segue que

$$\mu_1(\alpha)^{e_1} \dots \mu_r(\alpha)^{e_r} \in p\mathcal{O}_{\mathbb{K}}. \tag{1.5}$$

Por outro lado, temos que $\mathcal{P}_i^{e_i} \subset p\mathcal{O}_{\mathbb{K}} + \mu_i(\alpha)^{e_i}\mathcal{O}_{\mathbb{K}}$, consequentemente usando a equação (1.5), temos que

$$\mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} \subset p\mathcal{O}_{\mathbb{K}} + \mu_1(\alpha)^{e_1} \dots \mu_r(\alpha)^{e_r}\mathcal{O}_{\mathbb{K}} \subset p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_1^{'}} \dots \mathcal{P}_r^{e_r^{'}}.$$

Isso prova que $e_i \geq e_i^{'}$, para todo i. Mas sabemos que $\sum_i e_i d_i = gr(m) = [\mathbb{L} : \mathbb{K}] = \sum_i e_i^{'} d_i$. Assim, $e_i = e_i^{'}$, para todo i, o que prova $p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$. ■

Teorema 1.7.2. *([10], p. 74) Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números tal que $\mathbb{K} \subseteq \mathbb{L}$. Um ideal primo p de $\mathcal{O}_{\mathbb{K}}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $D_{\mathbb{L}/\mathbb{K}} \subseteq p\mathcal{O}_{\mathbb{K}}$, em que $D_{\mathbb{L}/\mathbb{K}}$ é o discriminante de $\mathbb{L}$ sobre $\mathbb{K}$.*

Demonstração: Pelo Teorema 1.3.2, temos que $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$, na qual e_i são inteiros positivos. A afirmação p se ramifica em $\mathcal{O}_{\mathbb{K}}$, é equivalente a dizer, que $p\mathcal{O}_{\mathbb{K}}$ não se decompõe. Por [[10], p. 73, Lemma 3], segue que $D_{p\mathcal{O}_{\mathbb{K}}/p\mathbb{L}} = \langle 0 \rangle$, tomando $\mathbb{S} = \mathbb{L} - p\mathbb{L}$, $\mathbb{L}' = \mathbb{S}^{-1}\mathbb{K}$, $\mathbb{K}' = \mathbb{S}^{-1}\mathbb{K}$ e $p' = p\mathbb{L}'$ tal que $\mathbb{L}'$ é um ideal principal, $\mathbb{K}'$ é um $\mathbb{L}'$-módulo livre, $p\mathbb{L} \simeq p'\mathbb{L}'$ e $p \simeq p'\mathcal{O}_{\mathbb{K}'}$. Como $D_{p\mathcal{O}_{\mathbb{K}}/p\mathbb{L}} = \langle 0 \rangle$, por [[10], p. 73, Lemma 2], segue que $D(e_1, \ldots, e_n) \in p'$. Logo, podemos escrever $(e_1, \ldots, e_n)$ como uma base $\mathbb{L}'$-módulo de $\mathbb{K}'$. Consideremos $(x_1, \ldots, x_n)$ base de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $x_i = \sum a'_{ij} e_j$, com $a'_{ij} \in \mathbb{L}'$, tem-se que $D_{\mathbb{L}/\mathbb{K}} = D(x_1, \ldots, x_n) = \det(a'_{ij})^2 D(e_1, \ldots, e_n) \in p\mathcal{O}_{\mathbb{K}'}$. Pela Proposição 1.3.4, temos que $p\mathcal{O}_{\mathbb{K}'} \cap \mathbb{L} = p\mathcal{O}_{\mathbb{K}}$. Logo, $D(x_1, \ldots, x_n) \in p\mathcal{O}_{\mathbb{K}}$ e portanto, $D_{\mathbb{L}/\mathbb{K}} \subseteq p\mathcal{O}_{\mathbb{K}}$. Reciprocamente, seja $D_{\mathbb{L}/\mathbb{K}} \subseteq p\mathcal{O}_{\mathbb{K}}$ tomando $e_i = y_i s^{-1}$ com $y_i \in \mathbb{K}$ e $s \in \mathbb{S}$, para $i = 1, \ldots, n$, tem-se que $D(e_1, \ldots, e_n) = s^{-2n} D(y_1, \ldots, y_n) \in \mathbb{L}' D_{\mathbb{L}/\mathbb{K}} \subseteq p\mathbb{L}' = p'$, ou seja, $D(e_1, \ldots, e_n) \in p'$, isto implica que, $D_{\mathbb{L}/\mathbb{K}} \neq \langle 0 \rangle$. Novamente, por [[10], p. 73, Lemma 3], concluímos que p se ramifica em $\mathcal{O}_{\mathbb{K}}$. ■

Decorre deste resultado que existe apenas um número finito de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathbb{K}$.

Exemplo 1.7.1. *Sejam $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_{15}]$ o anel de inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\xi_{15})$ e $m(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ o polinômio minimal de ξ_{15} sobre $\mathbb{Q}$. Tomando $m(x)$ módulo 3, obtemos que $m(x) \equiv (x^4 + x^3 + x^2 + x + 1)^2$ $(mod\ \mathbb{Z}_3[x])$. Assim, pelo Lema de Kummer, temos que $3\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^2$, na qual $\mathcal{P}_1 = \langle 3, \xi_{15}^4 + \xi_{15}^3 + \xi_{15}^2 + \xi_{15} + 1 \rangle$. Portanto, $3\mathcal{O}_{\mathbb{K}}$ se ramifica em $\mathcal{O}_{\mathbb{K}}$.*

Definição 1.7.4. *Sejam $\mathbb{L}$ um corpo e $f(x)$um polinômio não constante de $\mathbb{K}[x]$, dizemos que $\mathbb{L}$ é um corpo de raízes de $f(x)$ sobre $\mathbb{K}$ se $\mathbb{K}$ é um subconjunto de $\mathbb{L}$ e $f(x)$ se fatora sobre $\mathbb{L}$ como produto de polinômios irredutíveis.*

Definição 1.7.5. *Sejam $\mathbb{K}$ um corpo e G um conjunto de automorfismos em $\mathbb{K}$. O conjunto dos elementos de $\mathbb{K}$ que são fixados por todos os elementos de G é um subcorpo de $\mathbb{K}$ chamado corpo fixo de G.*

Teorema 1.7.3. *[19] Sejam $\mathbb{K}$ um corpo de característica zero e $\mathbb{L}$ uma extensão de grau finito n sobre $\mathbb{K}$. São equivalentes:*

1. *$\mathbb{K}$ é o corpo fixo do grupo $\mathcal{G}$ dos $\mathbb{K}$-automorfismos de $\mathbb{L}$.*

2. *Para todo $\alpha \in \mathbb{L}$, o polinômio minimal de α sobre $\mathbb{K}$ tem todas suas raízes em $\mathbb{L}$.*

3. *$\mathbb{L}$ é um corpo de raízes de um polinômio em $\mathbb{K}[x]$.*

Se as condições do Teorema 1.7.3 são satisfeitas, $\mathbb{L}$ é chamado de extensão galoisiana de $\mathbb{K}$ e $\mathcal{G}$ é chamado de grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ e denotado por $Gal_{\mathbb{K}}(\mathbb{L})$.

Lema 1.7.1. *([9], p. 107)Se $\alpha \in \mathbb{Q}(\xi_n)$, então $N(\alpha) \geq 0$.*

Demonstração: Seja $\sigma \in Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$ tal que $\sigma(\xi_n) = \xi_n^a$, em que ξ_n^a é uma raiz n-ésima primitiva do polinômio ciclotômico $\phi_n(x)$, com $mdc(n,a) = 1$. Temos que o conjugado complexo $\bar{\xi_n^a}$ de ξ_n^a é uma raiz n-ésima primitiva da unidade de $\phi_n(x)$. Logo, existe um automorfismo τ em $Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$ tal que $\tau(\xi_n) = \bar{\xi_n^a}$. Assim, para qualquer elemento $\alpha \in \mathbb{Q}(\xi_n)$, dado por $\alpha = x_0 + x_1\xi_n + \ldots + x_{\varphi(n)-1}\xi_n^{\varphi(n)-1}$ em $\mathbb{Q}(\xi_n)$ tem-se que $\sigma(\alpha)\tau(\sigma) = \sigma(x_0 + x_1\xi_n + \ldots + x_{\varphi(n)-1}\xi_n^{\varphi(n)-1})\tau(x_0 + x_1\xi_n + \ldots + x_{\varphi(n)-1}\xi_n^{\varphi(n)-1}) = (x_0 + x_1\sigma(\xi_n) + \ldots + x_{\varphi(n)-1}\sigma(\xi_n^{\varphi(n)-1}))(x_0 + x_1\tau(\xi_n) + \ldots + x_{\varphi(n)-1}\tau(\xi_n^{\varphi(n)-1})) = (x_0 + x_1\xi_n^a + \ldots + x_{\varphi(n)-1}(\xi_n^{\varphi(n)-1})^a)(x_0 + x_1\bar{\xi_n^a} + \ldots + x_{\varphi(n)-1}\overline{(\xi_n^{\varphi(n)-1})^a}) = x_0^2 + x_1^2 + \ldots x_{\varphi(n)-1}^2 + 2\Re(\xi_n^a) + \ldots + 2\Re((\xi_n^{\varphi(n)-1})^a) + 2\Re((\xi_n^a)(\xi_n^{\varphi(n)-1})^a) \geq x_0^2 + x_1^2 + \ldots x_{\varphi(n)-1}^2 \geq 0$, em que $\Re(z)$ denota a parte real do número complexo z. Como $N(\alpha)$ é definida como o produto dos $\varphi(n)$ automorfismos de $Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$, segue que podemos expressá-la como sendo o produto de $\frac{\varphi(n)}{2}$ números complexos e seus conjugados. Portanto, $N(\alpha) \geq 0$. ∎

Se $n \equiv 2 \ (mod\ 4)$ temos que $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{\frac{n}{2}})$. Assim, sem perda de generalidade, podemos supor $n \not\equiv 2 \ (mod\ 4)$. Por [[17], p. 204, Theorem 11.1], tem-se que $\mathbb{Z}[\xi_n]$ é um domínio de ideais principais se, e somente se, $n = \{1\} \cup A$, onde $A = \{3, 2, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$. Nos próximos resultados, consideramos sempre $n \in A$ que será muito importante para a construção/decodificação dos códigos via corpos ciclotômicos.

Lema 1.7.2. *([17], p. 14) Sejam p um primo e $\mathcal{P}$ um ideal primo de $\mathbb{Z}[\xi_n]$ acima de p. Se $p \nmid n$, então as n-ésimas raízes da unidade são distintas módulo $\mathcal{P}$.*

Demonstração: Sabemos que $n = \prod_{j=1}^{n-1}(1 - \xi_n^j)$. Se $\xi_n^j \equiv \xi_n^k \ (mod\ \mathcal{P})$, com $0 \leq j < k \leq n-1$, então $\xi_n^j - \xi_n^k \in \mathcal{P}$. Assim, $\xi_n^j(1 - \xi_n^k) \in \mathcal{P}$. Como $\mathcal{P}$ é primo, segue que $\xi_n^j \in \mathcal{P}$ ou $1 - \xi_n^{k-j} \in \mathcal{P}$, o que é um absurdo, uma vez que se $\xi_n^j \in \mathcal{P}$, então $\xi_n^j = 1 \in \mathcal{P}$ e se $1 - \xi_n^{k-j} \in \mathcal{P}$, então $n \in \mathcal{P} \cap \mathbb{Z} = \langle p \rangle$. ■

Teorema 1.7.4. *([17], p. 14) Sejam p um número primo e f o menor inteiro positivo tal que $p^f \equiv 1 \ (mod\ n)$. Se $p \nmid n$, então p se decompõe em $g = \frac{\varphi(n)}{f}$ primos distintos $\mathcal{P}$ em $\mathbb{Z}[\xi_n]$, na qual $[\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}} : \mathbb{Z}_p] = f$.*

Demonstração: Seja $\mathcal{P}$ um ideal primo de $\mathbb{Z}[\xi_n]$ acima de p. O automorfismo de Frobenius de $\mathbb{Z}[\xi_n]$ é definido por $\sigma_p(x) \equiv x^p \ (mod\ \mathcal{P})$, para todo $x \in \mathbb{Z}[\xi_n]$. Como $\sigma_p(\xi_n)$ é uma raiz n-ésima da unidade, segue que pelo Lema 1.7.2 que $\sigma_p(\xi_n) = \xi_n^p$. A ordem de σ_p é $[\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}} : \mathbb{Z}_p]$, uma vez que σ_p é o gerador do grupo de Galois de $\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}}$. Agora, $\sigma_p^f = 1$ se, e somente se, $\sigma_p^f(\xi_n) = \xi_n$ se, e somente se, $\xi_n^{p^f} = \xi_n$ se, e somente se, $p^f \equiv 1 \ (mod\ n)$. Como p não é ramificado em $\mathbb{Z}[\xi_n]$, segue que $e = 1$ e portanto, pela Observação 1.5.3 temos que $fg = [\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$. ■

Corolário 1.7.1. *([9], p. 108) Se p é um número primo da forma $p = nk + 1$, na qual $n \in A$, então $p\mathbb{Z}[\xi_n] = \prod_{j=1}^{\varphi(n)} \mathcal{P}_j$, em que $\mathcal{P}_j$ são ideais primos distintos de $\mathbb{Z}[\xi_n]$. Além disso, cada $\mathcal{P}_j$ é gerado por um elemento irredutível que tem norma p e $\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}_j}$ é isomorfo ao corpo $GF(p)$, para $j = 1, \ldots, \varphi(n)$.*

Demonstração: Se $p = nk + 1$, em que $n \in A$, então $p \nmid n$, pelo Teorema 1.7.4, temos que $p\mathbb{Z}[\xi_n]$ é expresso como um produto de primos $\mathcal{P}_j$ distintos de $\mathbb{Z}[\xi_n]$, para $j = 1, 2, \ldots, \varphi(n)$, ou seja, $p\mathbb{Z}[\xi_n] = \prod_{j=1}^{\varphi(n)} \mathcal{P}_j$. Como $\mathbb{Z}[\xi_n]$ é um domínio de ideais principais, segue que cada ideal $\mathcal{P}_j$ é gerado por um elemento irredutível, isto é, $\mathcal{P}_j = \langle \alpha_j \rangle$, para $j = 1, \ldots, \varphi(n)$. Como $\mathbb{Z}[\xi_n]$ é um domínio fatorial, uma vez que $\mathbb{Z}[\xi_n]$ é domínio de ideais principais, segue que p se decompõem em um produto de elementos irredutíveis a menos de uma unidade em $\mathbb{Z}[\xi_n]$, ou seja, $p = \alpha_1 \ldots \alpha_{\varphi(n)}\mu$, onde μ é uma unidade de $\mathbb{Z}[\xi_n]$. Aplicando a norma nesta igualdade, temos que $p^{\varphi(n)} = N(p) = N(\alpha_1 \ldots \alpha_{\varphi(n)}\mu) = N(\alpha_1) \ldots N(\alpha_{\varphi(n)})N(\mu)$. Se μ é uma unidade em $\mathbb{Z}[\xi_n]$, pela Observação 1.4.1, então $N(\mu) = \pm 1$. Como os α_j não são unidades em $\mathbb{Z}[\xi_n]$ e pelo Lema 1.7.1, segue que $N(\alpha_j) > 1$, para $j = 1, \ldots, \varphi(n)$. Como p é primo, segue que $N(\alpha_j) = p$, para $j = 1, \ldots, \varphi(n)$. Logo, $\mathcal{P}_j = \langle \alpha_j \rangle$ e $N(\mathcal{P}_j) = N(\langle \alpha_j \rangle) = N(\alpha_j) = p$, para $j = 1, 2, \ldots, \varphi(n)$. Portanto, os ideais primos $\mathcal{P}_j$ são gerados por elementos irredutíveis e tem norma p prima. Agora, como α_j é irredutível e $\mathcal{P}_j = \langle \alpha_j \rangle$, pela Observação 1.4.2, segue que $\mathcal{P}_j = \langle \alpha_j \rangle$ é um ideal maximal. Assim, $\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{P}_j}$ é um corpo com p elementos, uma vez que $\#\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{P}_j} = N(\mathcal{P}_j) = p$. Como $GF(p)$ também tem p elementos, segue que $\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{P}_j}$ é isomorfo a $GF(p)$, para $j = 1, 2, \ldots, \varphi(n)$ ■

Corolário 1.7.2. *([9], p. 108) Seja p um número primo tal que $p = nk + 1$, com $n \in A$. Se $\varphi(n)$ é o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$, então $p\mathbb{Z}[\xi_n]$ é um ideal primo de $\mathbb{Z}[\xi_n]$. Além disso, $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ é isomorfo a $GF(p^{\varphi(n)})$.*

Demonstração: Tomando $s = \varphi(n)$ tal que $p^s \equiv 1 \ (mod\ n)$ e aplicando o Teorema 1.7.4, segue o resultado. ■

Capítulo 2

Constelações de sinais via corpos quadráticos

2.1 Introdução

O problema da construção de sinais que possuam boas propriedades geométricas e boas estruturas algébricas é fundamental e relevante, tanto no aspecto da geração de constelações, como na implementação prática dos moduladores e demoduladores. Neste capítulo, veremos o conceito de constelações de sinais, na qual estabelecemos as condições necessárias para a construção de constelações de sinais casadas a grupos quocientes aditivos. Tais constelações fazem parte do espaço de sinais no $\mathbb{R}^2$ cuja identificação dos pontos de sinais são dados por elementos dos correspondentes anéis de inteiros $\mathbb{Z}[\rho]$, em que $\rho = i$ ou $\rho = w = \frac{1+\sqrt{-3}}{2}$. A rotulagem casada decorrerá da ação transitiva de grupos aditivos do corpo de Galois $GF(p^m)$ ou dos p-grupos aditivos G_{p^m}, como fez [5] e [6]. Também veremos a distância de Mannheim, sobre os anéis de inteiros $\mathbb{Z}[\rho]$, que é uma distância apropriada quando se usa modulações do tipo QAM, onde nem a distância de Hamming e nem a distância de Lee são apropriadas.

2.2 Constelações de sinais

Nesta seção, apresentamos a estrutura algébrica e geométrica das constelações de sinais via corpos quadráticos, também veremos a distância de Mannheim nestes corpos. Além disso, exibimos a aplicação casada que leva os elementos da constelações de sinais a um certo grupo aditivo.

Definição 2.2.1. *Uma constelação de sinais é um subconjunto finito de pontos do* $\mathbb{R}^n$*. Os pontos da constelação são chamados de pontos de sinais.*

Neste trabalho, veremos as constelações de sinais como sendo um subconjunto finito de pontos do plano.

Definição 2.2.2. *Uma constelação de sinais* S *é dita casada com um grupo* $(G, *)$*, mediante a uma distância* d*, se existe uma aplicação* μ *de* G *sobre* S *tal que*

$$d(\mu(g_1), \mu(g_2)) = d(\mu(e), \mu(g_1^{-1} * g_2)), \tag{2.1}$$

para todo g_1 *e* g_2 *pertencentes a* G*, em que* e *é o elemento neutro de* G *e* $d(.,.)$ *é uma distância em* S*. Neste caso, a aplicação* μ *é chamada de aplicação casada. Além disso, se* μ *for injetora chamamos* μ^{-1} *de rotulamento casado.*

Sejam $\mathbb{Q}(\sqrt{d})$ um extensão quadrática, com d livre de quadrados e $\mathbb{Z}[\rho]$ o anel de inteiros de $\mathbb{Q}(\sqrt{d})$. Analisaremos dois casos particulares $d = -1$ e $d = -3$. Assim, pelo Teorema 1.6.1, se $d = -1$, então $\mathbb{Z}[\rho] = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ é chamado anel de inteiros de Gauss e se $d = -3$, então $\mathbb{Z}[\rho] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[w]$ é chamado anel de inteiros de Eisenstein-Jacobi. Além disso, temos que $\mathbb{Z}[\rho]$, em que $\rho = i$ ou $\rho = w$ é um domínio de ideais principais. Assim, todo ideal primo $\mathcal{I}$ de $\mathbb{Z}[\rho]$ é escrito na forma

$$\mathcal{I} = \langle \pi \rangle = \pi\mathbb{Z}[\rho] = \{\pi\alpha : \alpha \in \mathbb{Z}[\rho]\},$$

na qual $\pi = a + b\rho \in \mathbb{Z}[\rho]$ é um elemento primo. Temos que i é uma raiz quarta primitiva da unidade e w é uma raiz sexta primitiva da unidade.

Observação 2.2.1. *Se $\pi = a + b\rho \in \mathbb{Z}[\rho]$, então a norma de π é dada por:*

$$N(\pi) = N(a+b\rho) = (a+b\rho)(\overline{a+b\rho}) = \pi\bar{\pi} = \begin{cases} a^2 - db^2 \text{ se } d \equiv 2,3 \ (mod\ 4) \\ a^2 + ab + \dfrac{1-d}{4}b^2 se\ d \equiv 1 \ (mod\ 4), \end{cases}$$

em que $\overline{a+b\rho}$ denota a conjugação complexa de $a+b\rho$. Assim, temos que se $d = -1$, então $N(\pi) = a^2 + b^2$ e se $d = -3$, então $N(\pi) = a^2 + ab + b^2$.

Definição 2.2.3. *Definimos o peso de Manhattan de um elemento $\alpha = a+b\rho \in \mathbb{Z}[\rho]$, na qual $\rho = i$ ou $\rho = w$, como $w_{\mathcal{M}}(\alpha) = |a| + |b|$. Além disso, se $\alpha = a + b\rho$ e $\beta = c + d\rho$ são elementos de $\mathbb{Z}[\rho]$, definimos a distância de Manhattan entre os elementos α e β como $d_{\mathcal{M}}(\alpha, \beta) = w_{\mathcal{M}}(\alpha - \beta) = |a - c| + |b - d|$.*

Se p é um número ímpar tal que

$$\begin{cases} p \equiv 1(mod\ 4) & \text{se } d = -1 \\ p \equiv 1(mod\ 6) & \text{se } d = -3, \end{cases}$$

então pela Proposição 1.6.5, p se decompõe totalmente em $\mathbb{Z}[\rho]$. Nosso objetivo é determinar um rotulamento casado entre o grupo aditivo de $GF(p)$ e um subconjunto conveniente do $\mathbb{R}^2$. Em ambos os casos temos que p fatora-se como $p = \pi\bar{\pi}$, em que $N(\pi) = \pi\bar{\pi} = p$ e que o ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ fatora-se completamente em $\mathbb{Z}[\rho]$, isto é, $p\mathbb{Z}[\rho] = \mathcal{I}\bar{\mathcal{I}}$, na qual $\mathcal{I} = \langle\pi\rangle$ e $\bar{\mathcal{I}} = \langle\bar{\pi}\rangle$ são dois ideais primos distintos de $\mathbb{Z}[\rho]$. Como $\mathbb{Z}[\rho]$ é um domínio principal, segue que seus ideais primos $\mathcal{I}$ não nulos são maximais. Portanto, o quociente $\dfrac{\mathbb{Z}[\rho]}{\mathcal{I}}$ é um corpo de ordem p, uma vez que $\#\dfrac{\mathbb{Z}[\rho]}{\mathcal{I}} = N(\mathcal{I}) = N(\langle\pi\rangle) = p$, que denotamos por $A_p[\rho]$, na qual $A_p[\rho]$ são as constelações de sinais S. As unidades de $\mathbb{Z}[\rho]$ formam um grupo ciclíco que denotamos por $\mathbb{Z}[\rho]^*$. Assim, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ se $d = -1$ e $\mathbb{Z}[w]^* = \{\pm 1, \pm w, \pm w^2\}$ se $d = -3$. Os elementos $0, 1, \ldots, p-1$ formam um conjunto completo de representantes das classes laterais de $\mathcal{I}$ em $\mathbb{Z}[\rho]$. Assim, como $\rho \in \mathbb{Z}[\rho]$, segue que ρ pertence a alguma classe lateral $\bar{s} \in \dfrac{\mathbb{Z}[\rho]}{\mathcal{I}}$, em que $0 \leq s \leq p-1$. Logo, $\overline{x+y\rho} = \bar{x}+\bar{y}\bar{\rho} = \bar{x}+\bar{y}\bar{s} = \overline{x+ys} = \bar{l}$, na qual $l \in \{0, 1, \ldots, p-1\}$. Agora, $\overline{x+ys} = \bar{l}$ se, e somente se, $x+ys-l \in \mathcal{I} \bigcap \mathbb{Z} = p\mathbb{Z}$, em que $x, y, s, l \in \mathbb{Z}$. Portanto, $x + y\rho \equiv l(mod\ \mathcal{I})$ se, e somente se, $x + ys \equiv l(mod\ p)$, na qual s é um representante da classe lateral contedo ρ.

Teorema 2.2.1. *([3], p. 5) Se $p \in \mathbb{Z}$ é um número primo ímpar tal que $p = \pi\bar{\pi}$, em que $\pi = a + b\rho \in \mathbb{Z}[\rho]$, então em cada classe lateral $l + \mathcal{I}$, onde $\mathcal{I} = \langle\pi\rangle$ e $l = 0, 1, \ldots, p-1$, existe um único elemento $\alpha_l = l + \mu\pi$ com norma euclidiana mínima.*

Demonstração: Seja $N_l^* = min\{N(\alpha) : \alpha \in l+\mathcal{I}\}$, o valor mínimo das normas dos elementos de $l + \mathcal{I}$. Como $\{-\frac{(p-1)}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$ é um conjunto completo de representantes de $\mathcal{I}$ em $\mathbb{Z}[\rho]$, segue que a distância euclidiana entre quaisquer dois representantes das classes de norma mínima é sempre menor que p. Para a unicidade, suponhamos que $\alpha_{l_1} = l + \mu_1\pi = \alpha_{l_2} = l + \mu_2\pi$ são dois elementos de $l + \mathcal{I}$ tendo a mesma norma mínima, isto é, $N(\alpha_{l_1}) = N(\alpha_{l_2}) = N_l^*$. Assim,

$$l^2 + l(\mu_1\pi + \bar{\mu_1}\bar{\pi}) + \mu_1\bar{\mu_1}\pi\bar{\pi} = l^2 + l(\mu_2\pi + \bar{\mu_2}\pi) + \mu_2\bar{\mu_2}\pi\bar{\pi}$$

e portanto,

$$l((\bar{\mu_1} - \bar{\mu_2})\bar{\pi} + (\mu_1 - \mu_2)\pi) = (\mu_1\bar{\mu_1} - \mu_2\bar{\mu_2})\pi\bar{\pi}.$$

Como $l, \pi, \bar{\pi}$ são coprimos e $\langle\pi\rangle$, $\langle\bar{\pi}\rangle$ são ideais principais primos, segue que $\mu_1 - \mu_2 \in \langle\bar{\pi}\rangle$, isto é, $\alpha_{l_1} - \alpha_{l_2} = pt$, para algum $t \in \mathbb{Z}[\rho]$. Como α_{l_1} e α_{l_2} pertencem ao círculo com raio $\frac{p-1}{2}$ e centro na origem, segue que $t = 0$ e portanto, $\alpha_{l_1} = \alpha_{l_2}$. ■

Pelo Teorema 2.2.1, podemos considerar $A_p[\rho] = \{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\} \subset \mathbb{C}$ como um conjunto de representantes de $\mathcal{I}$ em $\mathbb{Z}[\rho]$, satisfazendo $\alpha_l \equiv l(mod\ \mathcal{I})$ e $N(\alpha_l)$ mínima, munido das seguintes operações de adição e multiplicação, definidas por:

$$\begin{cases} \alpha_i + \alpha_j = \alpha_k & \text{tal que } k \equiv i + j\ (mod\ p),\ \text{ para }\ i, j = 0, 1, \ldots, p-1, \\ \alpha_i\alpha_j = \alpha_k & \text{tal que } k \equiv ij\ (mod\ p),\ \text{ para }\ i, j = 0, 1, \ldots, p-1. \end{cases} \tag{2.2}$$

Assim, $A_p[\rho]$ com essas operações é um corpo com p elementos isomorfo a $GF(p)$.

Definição 2.2.4. *Dado $\gamma = a + b\rho \in A_p[\rho]$, definimos o peso de Mannheim de γ como $w_{\bar{\mathcal{M}}}(\gamma) = |a| + |b|$.*

Proposição 2.2.1. *A aplicação $d_{\bar{\mathcal{M}}} : A_p[\rho] \times A_p[\rho] \to \mathbb{R}$ definida por $d_{\bar{\mathcal{M}}}(\alpha, \beta) = w_{\bar{\mathcal{M}}}(\gamma)$, em que $\alpha, \beta \in A_p[\rho]$ e $\alpha - \beta \equiv \gamma\ (mod\ \mathcal{I})$, com $\gamma \in A_p[\rho]$ é uma métrica.*

Demonstração: Sejam $\alpha, \beta \in A_p[\rho]$ tal que $\alpha - \beta \equiv \gamma \ (mod\ \mathcal{I})$, com $\gamma \in A_p[\rho]$, isto é, $\gamma = a + b\rho$, com $a, b \in \mathbb{Z}$.

1. Temos que $d_{\bar{\mathcal{M}}}(\alpha, \beta) = w_{\bar{\mathcal{M}}}(\gamma) = |a| + |b| \geq 0$, pois $|a|, |b| \geq 0$ e $d_{\bar{\mathcal{M}}}(\alpha, \beta) = 0 \Leftrightarrow w_{\bar{\mathcal{M}}}(\gamma) = 0 \Leftrightarrow |a| + |b| = 0 \Leftrightarrow a = b = 0 \Leftrightarrow \gamma = 0 \Leftrightarrow \alpha = \beta$.

2. Temos que $d_{\bar{\mathcal{M}}}(\alpha, \beta) = w_{\bar{\mathcal{M}}}(\gamma)$, com $\alpha - \beta \equiv \gamma \ (mod\ \mathcal{I})$. Como $-(\alpha - \beta) \equiv -\gamma \ (mod\ \mathcal{I})$, segue que $\beta - \alpha \equiv -\gamma \ (mod\ \mathcal{I})$. Assim, $-\gamma = -a - b\rho$ e $w_{\bar{\mathcal{M}}}(-\gamma) = |a| + |b| = w_{\bar{\mathcal{M}}}(\gamma)$. Portanto, $d_{\bar{\mathcal{M}}}(\alpha, \beta) = d_{\bar{\mathcal{M}}}(\beta, \alpha)$.

3. Sejam $\alpha, \beta, \delta \in A_p[\rho]$ tal que

   - $d_{\bar{\mathcal{M}}}(\alpha, \beta) = w_{\bar{\mathcal{M}}}(\gamma)$ com $\alpha - \beta \equiv \gamma_1 \ (mod\ \mathcal{I})$, $\gamma_1 \in A_p[\rho]$ e $N(\gamma_1)$ mínimo.
   - $d_{\bar{\mathcal{M}}}(\alpha, \delta) = w_{\bar{\mathcal{M}}}(\gamma_2)$ com $\alpha - \delta \equiv \gamma_2 \ (mod\ \mathcal{I})$, $\gamma_2 \in A_p[\rho]$ e $N(\gamma_2)$ mínimo.
   - $d_{\bar{\mathcal{M}}}(\delta, \beta) = w_{\bar{\mathcal{M}}}(\gamma_3)$ com $\delta - \beta \equiv \gamma_3 \ (mod\ \mathcal{I})$, $\gamma_3 \in A_p[\rho]$ e $N(\gamma_3)$ mínimo.

   Temos que $\alpha - \beta \equiv \gamma_2 + \gamma_3 \ (mod\ \mathcal{I})$ e $N(\gamma_1) \leq N(\gamma_2 + \gamma_3)$, pois $N(\gamma_1)$ é mínima. Portanto, $d_{\bar{\mathcal{M}}}(\alpha, \beta) \leq d_{\bar{\mathcal{M}}}(\alpha, \delta) + d_{\bar{\mathcal{M}}}(\delta, \beta)$. ■

Definição 2.2.5. *Sejam $\alpha, \beta \in A_p[\rho]$ tal que $\alpha - \beta \equiv \gamma \ (mod\ \mathcal{I})$, com $\gamma \in A_p[\rho]$. Definimos a distância de Mannheim entre α e β como $d_{\bar{\mathcal{M}}}(\alpha, \beta) = w_{\bar{\mathcal{M}}}(\gamma)$.*

Teorema 2.2.2. *([3], p. 9) Se $\pi = a + bw \in \mathbb{Z}[w]$ é tal que $N(\pi) = a^2 + ab + b^2 = p$, em que p é um primo tal que $p \equiv 1 \ (mod\ 6)$, então a distância máxima de Mannheim entre os elementos de $A_p[w]$ é dado por*

$$d_{\mathcal{M},max}(A_p[w]) = max\{|a|, |b|, |a + b|\} - 1.$$

Teorema 2.2.3. *([1], p. 208) Se $\pi = a + bi \in \mathbb{Z}[i]$ é tal que $N(\pi) = a^2 + b^2 = p$, em que p é primo tal que $p \equiv 1 \ (mod\ 4)$, então a distância máxima de Mannheim entre os elementos de $A_p[i]$ é dada por*

$$d_{\mathcal{M},max}(A_p[i]) = max\{|a|, |b|\} - 1.$$

Assim, temos que $d_{\bar{\mathcal{M}}}(.,.)$ é uma métrica em $A_p[\rho]$ e portanto, podemos definir de modo natural um rotulamento casado do conjunto de sinais $A_p[\rho] = \{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\} \subset \mathbb{Z}[\rho]$ com o grupo aditivo de $GF(p)$.

Definição 2.2.6. *O rotulamento casado μ do grupo aditivo de $GF(p)$ sobre $A_p[\rho]$ é definida por $\mu(\bar{l}) = \alpha_l$, para $l = 0, 1, \ldots, p-1$.*

Para determinar o rótulo de cada elemento do conjunto de sinais $A_p[\rho] = \{\alpha_0, \ldots, \alpha_{p-1}\} \subset \mathbb{Z}[\rho]$ por um elemento do corpo $GF(p)$, usamos o procedimento dado na Seção 2.3.

Figura 2.1: Mapa da rua de Mannheim

A Figura 2.1 mostra o mapa da rua de Mannheim que deu origem a distância de Mannheim, na qual vem o formato de ziguezague das constelações. Além disso, a distância de Mannheim garante a simetria dos pontos das constelações de sinais em relação ao primo p considerado.

2.3 Algoritmo para rotular os elementos de $A_p[\rho]$

Nesta seção, apresentamos os passos do algoritmo para rotular os elementos de $A_p[\rho]$ por elementos de $GF(p)$ e damos exemplos via os anéis de inteiros de Eisenstein-Jacobi e de Gauss. O algoritmo para rotular os elementos de $A_p[\rho]$ consiste dos seguintes passos:

1. Tome um número primo p que decompõe-se completamente em $\mathbb{Z}[\rho]$ e seja $\pi = a + b\rho$ tal que $N(\pi) = p$, $\pi \in \mathbb{Z}[\rho]$.

2. Tome $s \in \mathbb{Z}$ a única solução na variável r da equação $a + br \equiv 0 \ (mod\ p)$, em que $0 \leq r \leq p - 1$.

3. O elemento $l \in GF(p)$ é o rótulo do ponto $\alpha_l = x + y\rho \in \mathbb{Z}[\rho]$ se $x + ys \equiv l \ (mod\ p)$ e $N(\alpha_l)$ for mínima.

Garantimos a unicidadade do ponto α_l pelo Teorema 2.2.1. Para melhorar o processo de rotulamento devemos ordenar os valores de l em ordem crescente e em seguida, para cada ponto $\alpha_l = x+y\rho \in A_p[\rho]$ atribuímos o rótulo l, na qual $l \equiv x+ys \ (mod\ p)$, sendo $N(\alpha_l)$ mínima.

2.3.1 Exemplos no anel de inteiros de Eisenstein-Jacobi

Se $\alpha = a + bw \in A_p[w]$, em que $w = \frac{1+\sqrt{-3}}{2}$, então $N(\alpha) = a^2 + ab + b^2$ e os valores assumidos são $0, 1, 3, 4, 7, 9, 12, \ldots$. Sejam os primos p que se decompõem completamente em $\mathbb{Z}[w]$, isto é, os primos p tais que $p \equiv 1 \ (mod\ 6)$.

Exemplo 2.3.1. *Sejam $d = -3$ e $p = 7 \equiv 1 \ (mod\ 6)$. Usando o algoritmo temos:*

1. *Uma solução da equação $N(\pi) = a^2 + ab + b^2 = p = 7$ é dada por $(a, b) = (-3, 1)$. Assim, podemos tomar $\pi = -3 + w \in \mathbb{Z}[w]$.*

2. *A única solução da equação $a + br = -3 + r \equiv 0 \ (mod\ 7)$, em que $0 \leq r \leq 6$ é $r = 3$.*

3. *Assim,* $l \in GF(7)$ *será o rótulo do ponto* $\alpha_l = x + yw$ *de* $A_7[w]$*, se* $x + 3y \equiv l \ (mod\ 7)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_7[w]$ *são dados pela Tabela 2.1, assim como sua representação geométrica pela Figura* 2.2*.*

(x, y)	$N(\alpha_l)$	$x + 3y \equiv l \ (mod\ 7)$	(x, y)	$N(\alpha_l)$	$x + 3y \equiv l \ (mod\ 7)$
$(0, 0)$	0	0	$(1, 1)$	3	4
$(1, 0)$	1	1	$(1, -1)$	1	5
$(-1, 1)$	1	2	$(-1, 0)$	1	6
$(-1, -1)$	3	3			

Tabela 2.1: Constelação com 7 sinais rotulados por $GF(7)$, com $d = -3$

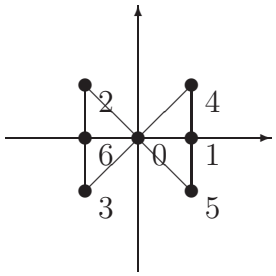

Figura 2.2

Exemplo 2.3.2. *([13], p. 74) Sejam* $d = -3$ *e* $p = 13 \equiv 1 \ (mod\ 6)$*. Aplicando o algoritmo temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + ab + b^2 = p = 13$ *é dada por* $(a, b) = (-1, 4)$*. Assim, podemos tomar* $\pi = -1 + 4w \in \mathbb{Z}[w]$*.*

2. *A única solução da equação* $a+br = -1+4r \equiv 0 \ (mod\ 13)$*, em que* $0 \leq r \leq 12$ *é* $r = 10$*.*

3. *Assim,* $l \in GF(13)$ *será o rótulo do ponto* $\alpha_l = x+yw$ *de* $A_{13}[w]$*, se* $x+10y \equiv l \ (mod\ 13)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{13}[w]$ *são dados pela Tabela 2.2, assim como sua representação geométrica pela Figura* 2.3*.*

(x,y)	$N(\alpha_l)$	$x+10y \equiv l \ (mod\ 13)$	(x,y)	$N(\alpha_l)$	$x+10y \equiv l \ (mod\ 13)$
$(0,0)$	0	0	$(0,-2)$	4	7
$(1,0)$	1	1	$(-2,1)$	3	8
$(-2,-1)$	3	2	$(-1,1)$	1	9
$(-1,-1)$	3	3	$(1,1)$	3	10
$(1,-1)$	1	4	$(2,1)$	7	11
$(2,-1)$	3	5	$(-1,0)$	1	12
$(0,2)$	4	6			

Tabela 2.2: Constelação com 13 sinais rotulados por $GF(13)$, com $d=-3$

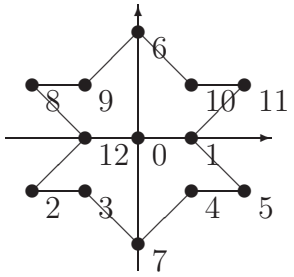

Figura 2.3

Exemplo 2.3.3. *Sejam* $d=-3$ *e* $p=19\equiv 1\ (mod\ 6)$. *Aplicando o algoritmo, temos:*

1. *Uma solução da equação* $N(\pi)=a^2+ab+b^2=p=19$ *é dada por* $(a,b)=(-5,2)$. *Assim, podemos tomar* $\pi=-5+2w\in\mathbb{Z}[w]$.

2. *A única solução da equação* $a+br=-5+2r\equiv 0\ (mod\ 19)$, *em que* $0\leq r\leq 18$, *é* $r=12$.

3. *Assim,* $l\in GF(19)$ *será o rótulo do ponto* $\alpha_l=x+yw$ *de* $A_{19}[w]$, *se* $x+12y\equiv l\ (mod\ 19)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{19}[w]$ *são dados pela Tabela 2.3, assim como sua representação geométrica pela Figura* 2.4.

(x,y)	$N(\alpha_l)$	$x+12y \equiv l \ (mod\ 19)$	(x,y)	$N(\alpha_l)$	$x+12y \equiv (mod\ 19)$
$(0,0)$	0	0	$(-2,1)$	3	10
$(1,0)$	1	1	$(-1,1)$	1	11
$(2,0)$	4	2	$(0,1)$	1	12
$(3,0)$	9	3	$(-1,-2)$	7	13
$(-1,2)$	3	4	$(0,-2)$	4	14
$(0,2)$	4	5	$(1,-2)$	3	15
$(1,2)$	7	6	$(-3,0)$	9	16
$(0,-1)$	1	7	$(-2,0)$	4	17
$(1,-1)$	1	8	$(-1,0)$	1	18
$(2,-1)$	3	9			

Tabela 2.3: Constelação com 19 sinais rotulados por $GF(19)$, com $d=-3$

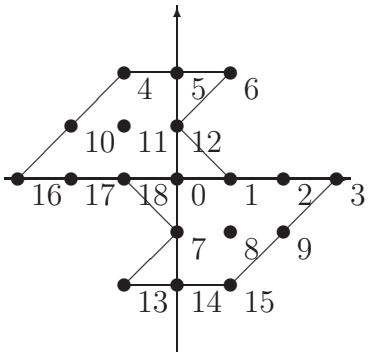

Figura 2.4

Exemplo 2.3.4. *Sejam $d=-3$ e $p=31\equiv 1\ (mod\ 6)$. Aplicando o algoritmo, temos:*

1. *Uma solução da equação $N(\alpha)=a^2+ab+b^2=p=31$ é dada por $(a,b)=(-5,6)$. Assim, podemos tomar $\pi=-5+6w\in\mathbb{Z}[w]$.*

2. *A única solução da equação $a+br=-5+6r\equiv 0\ (mod\ 31)$, em que $0\leq r\leq 30$ é $r=6$.*

3. *Assim, $l\in GF(31)$ será o rótulo do ponto $\alpha_l=x+yw$ de $A_{31}[w]$, se $x+6y\equiv l\ (mod\ 31)$ e $N(\alpha_l)$ for mínima.*

Os elementos de $A_{31}[w]$ são dados pela Tabela 2.4, assim como sua representação geométrica pela Figura 2.5.

(x,y)	$N(\alpha_l)$	$x+6y \equiv l \ (mod\ 31)$	(x,y)	$N(\alpha_l)$	$x+6y \equiv l \ (mod\ 31)$
$(0,0)$	0	0	$(-3,-2)$	19	16
$(1,0)$	1	1	$(-2,-2)$	12	17
$(2,0)$	4	2	$(-1,-2)$	7	18
$(-3,1)$	7	3	$(0,-2)$	4	19
$(-2,1)$	3	4	$(1,-2)$	3	20
$(-1,1)$	1	5	$(2,-2)$	4	21
$(0,1)$	1	6	$(3,-2)$	7	22
$(1,1)$	3	7	$(-2,-1)$	7	23
$(2,1)$	7	8	$(-1,-1)$	3	24
$(-3,2)$	7	9	$(0,-1)$	1	25
$(-2,2)$	4	10	$(1,-1)$	1	26
$(-1,2)$	3	11	$(2,-1)$	3	27
$(0,2)$	4	12	$(3,-1)$	7	28
$(1,2)$	7	13	$(-2,0)$	4	29
$(2,2)$	12	14	$(-1,0)$	1	30
$(3,2)$	19	15			

Tabela 2.4: Constelação com 31 sinais rotulados por $GF(31)$, com $d=-3$

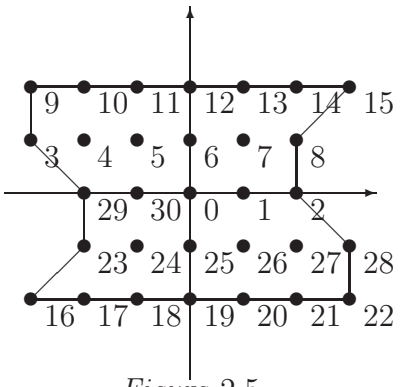

Figura 2.5

Exemplo 2.3.5. *([13], p. 75) Sejam $d=-3$ e $p=37\equiv 1\ (mod\ 6)$. Aplicando o algoritmo, temos:*

1. *Uma solução da equação $N(\pi)=a^2+ab+b^2=p=37$ é dada por $(a,b)=(3,4)$. Assim, podemos tomar $\pi=3+4w\in\mathbb{Z}[w]$.*

2. *A única solução da equação $a+br=3+4r\equiv 0\ (mod\ 37)$, em que $0\leq r\leq 36$ é $r=27$.*

3. *Assim, $l\in GF(37)$ será o rótulo do ponto $\alpha_l=x+yw$ de $A_{37}[w]$, se $x+27y\equiv l\ (mod\ 37)$ e $N(\alpha_l)$ for mínima.*

Os elementos de $A_{37}[w]$ são dados pela Tabela 2.5, assim como sua representação geométrica pela Figura 2.6.

(x,y)	$N(\alpha_l)$	$x+27y \equiv l \ (mod\ 37)$	(x,y)	$N(\alpha_l)$	$x+27y \equiv l \ (mod\ 37)$
$(0,0)$	0	0	$(0,-2)$	4	20
$(1,0)$	1	1	$(1,-2)$	3	21
$(2,0)$	4	2	$(2,-2)$	4	22
$(3,0)$	9	3	$(3,-2)$	7	23
$(-3,3)$	9	4	$(-3,1)$	7	24
$(-2,3)$	7	5	$(-2,1)$	3	25
$(1,-3)$	7	6	$(-1,1)$	1	26
$(0,3)$	9	7	$(0,1)$	1	27
$(-2,-1)$	7	8	$(1,1)$	3	28
$(-1,-1)$	3	9	$(2,1)$	7	29
$(0,-1)$	1	10	$(0,-3)$	9	30
$(1,-1)$	1	11	$(1,-3)$	7	31
$(2,-1)$	3	12	$(2,-3)$	7	32
$(3,-1)$	7	13	$(3,-3)$	9	33
$(-3,2)$	7	14	$(-3,0)$	9	34
$(-2,2)$	4	15	$(-2,0)$	4	35
$(-1,2)$	3	16	$(-1,0)$	1	36
$(0,2)$	4	17			
$(1,2)$	7	18			
$(-1,-2)$	7	19			

Tabela 2.5: Constelação com 37 sinais rotulados de $GF(37)$, com $d=-3$

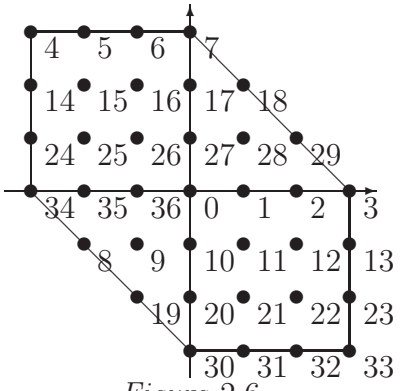

Figura 2.6

Exemplo 2.3.6. *([13], p. 77) Sejam $d=-3$ e $p=43\equiv 1\ (mod\ 6)$. Aplicando o algoritmo, temos:*

1. *Uma solução da equação $N(\pi)=a^2+ab+b^2=p=43$ é dada por $(a,b)=(6,1)$. Assim, podemos tomar $\pi=6+w\in\mathbb{Z}[w]$.*

2. *A única solução da equação* $a + br = 6 + r \equiv 0 \ (mod\ 43)$, *em que* $0 \leq r \leq 42$ *é* $r = 37$.

3. *Assim,* $l \in GF(43)$ *será o rótulo do ponto* $\alpha_l = x+yw$ *de* $A_{43}[w]$, *se* $x+37y \equiv l \ (mod\ 43)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{43}[w]$ *são dados pela Tabela 2.6, assim como sua representação geométrica pela Figura* 2.7.

(x, y)	$N(\alpha_l)$	$x + 37y \equiv l \ (mod\ 43)$	(x, y)	$N(\alpha_l)$	$x + 37y \equiv l \ (mod\ 43)$
$(0, 0)$	0	0	$(-3, 3)$	9	22
$(1, 0)$	1	1	$(-2, 3)$	7	23
$(2, 0)$	4	2	$(-1, 3)$	7	24
$(3, 0)$	9	3	$(0, 3)$	9	25
$(-2, -1)$	7	4	$(2, -4)$	12	26
$(-1, -1)$	3	5	$(-4, 2)$	12	27
$(0, -1)$	1	6	$(-3, 2)$	7	28
$(1, -1)$	1	7	$(-2, 2)$	4	29
$(2, -1)$	3	8	$(-1, 2)$	3	30
$(3, -1)$	7	9	$(0, 2)$	4	31
$(-2, -2)$	12	10	$(1, 2)$	7	32
$(-1, -2)$	7	11	$(2, 2)$	12	33
$(0, -2)$	4	12	$(-3, 1)$	7	34
$(1, -2)$	3	13	$(-2, 1)$	3	35
$(2, -2)$	4	14	$(-1, 1)$	1	36
$(3, -2)$	7	15	$(0, 1)$	1	37
$(4, -2)$	12	16	$(1, 1)$	3	38
$(-2, 4)$	12	17	$(2, 1)$	7	39
$(0, -3)$	9	18	$(-3, 0)$	9	40
$(1, -3)$	7	19	$(-2, 0)$	4	41
$(2, -3)$	7	20	$(-1, 0)$	1	42
$(3, -3)$	9	21			

Tabela 2.6: Constelação com 43 sinais rotulados por $GF(43)$, com $d = -3$

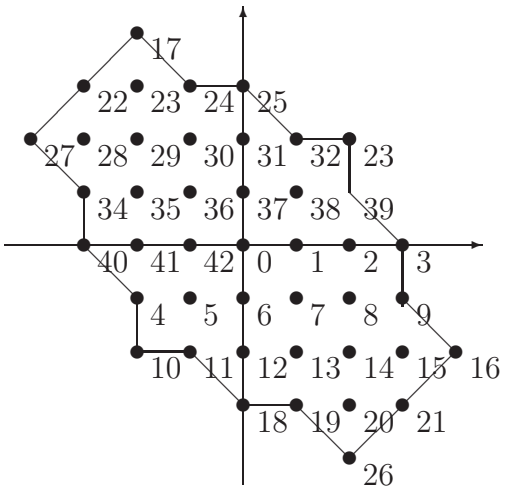

Figura 2.7

2.3.2 Exemplos no anel de inteiros de Gauss

Se $\alpha = a+bi \in A_p[i]$, então $N(\alpha) = a^2+b^2$ e os valores assumidos são $0, 1, 2, 4, 5, 8, \ldots$. Sejam os primos p que se decompõem completamente em $\mathbb{Z}[i]$, isto é, os primos p tais que $p \equiv 1 \ (mod\ 4)$.

Exemplo 2.3.7. *Sejam* $d = -1$ *e* $p = 5 \equiv 1 \ (mod\ 4)$. *Aplicando o algoritmo, temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p = 5$ *é dada por* $(a, b) = (2, 1)$. *Assim, podemos tomar* $\pi = 2 + i \in \mathbb{Z}[i]$.

2. *A única solução da equação* $a + br = 2 + r \equiv 0 \ (mod\ 5)$, *em que* $0 \leq r \leq 4$ *é* $r = 3$.

3. *Assim,* $l \in GF(5)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *de* $A_5[i]$, *se* $x + 3y \equiv l \ (mod\ 5)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_5[i]$ *são dados pela Tabela 2.7, assim como sua representação geométrica pela Figura* 2.8.

(x,y)	$N(\alpha_l)$	$x+3y \equiv l \ (mod\ 5)$	(x,y)	$N(\alpha_l)$	$x+3y \equiv l \ (mod\ 5)$
$(0,0)$	0	0	$(0,1)$	1	3
$(1,0)$	1	1	$(-1,0)$	1	4
$(0,-1)$	1	2			

Tabela 2.7: Constelação com 5 sinais rotulados por $GF(5)$, com $d=-1$

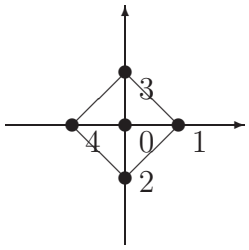

Figura 2.8

Exemplo 2.3.8. *Sejam $d=-1$ e $p=13\equiv 1\ (mod\ 4)$. Aplicando o algoritmo, temos:*

1. *Uma solução da equação $N(\pi)=a^2+b^2=p=13$ é dada por $(a,b)=(3,2)$. Assim, podemos tomar $\pi=3+2i\in\mathbb{Z}[i]$.*

2. *A única solução da equação $a+br=3+2r\equiv 0\ (mod\ 13)$, em que $0\leq r\leq 12$ é $r=5$.*

3. *Assim, $l\in GF(13)$ será o rótulo do ponto $\alpha_l=x+yi$ de $A_{13}[i]$, se $\alpha=x+5y\equiv l\ (mod\ 13)$ e $N(\alpha_l)$ for mínima.*

Os elementos de $A_{13}[i]$ são dados pela Tabela 2.8, assim como sua representação geométrica pela Figura 2.9.

(x,y)	$N(\alpha_l)$	$x+5y \equiv l \ (mod\ 13)$	(x,y)	$N(\alpha_l)$	$x+5y \equiv l \ (mod\ 13)$
$(0,0)$	0	0	$(-1,-1)$	2	7
$(1,0)$	1	1	$(0,-1)$	1	8
$(2,0)$	4	2	$(1,-1)$	2	9
$(0,-2)$	4	3	$(0,2)$	4	10
$(-1,1)$	2	4	$(-2,0)$	4	11
$(0,1)$	1	5	$(-1,0)$	1	12
$(1,1)$	2	6			

Tabela 2.8: Constelação com 13 sinais rotulados por $GF(13)$, com $d=-1$

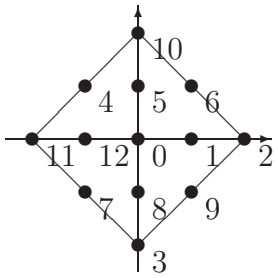

Figura 2.9

Exemplo 2.3.9. *([13], p. 71) Sejam* $d = -1$ *e* $p = 17 \equiv 1 \ (mod\ 4)$. *Aplicando o algoritmo, temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p = 17$ *é dada por* $(a, b) = (4, 1)$. *Assim, podemos tomar* $\pi = 4 + i \in \mathbb{Z}[i]$.

2. *A única solução da equação* $a + br = 4 + r \equiv 0 \ (mod\ 17)$, *em que* $0 \leq r \leq 16$ *é* $r = 13$.

3. *Assim,* $l \in GF(17)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *de* $A_{17}[i]$, *se* $x + 13y \equiv l \ (mod\ 17)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{17}[i]$ *são dados pela Tabela 2.9, como sua representação geométrica pela Figura* 2.10.

(x, y)	$N(\alpha_l)$	$x + 13y \equiv l \ (mod\ 17)$	(x, y)	$N(\alpha_l)$	$x + 13y \equiv l \ (mod\ 17)$
$(0, 0)$	0	0	$(0, 2)$	4	9
$(1, 0)$	1	1	$(1, 2)$	5	10
$(2, 0)$	4	2	$(-2, 1)$	5	11
$(-1, -1)$	2	3	$(-1, 1)$	2	12
$(0, -1)$	1	4	$(0, 1)$	1	13
$(1, -1)$	2	5	$(1, 1)$	2	14
$(2, -1)$	5	6	$(-2, 0)$	4	15
$(-1, -2)$	5	7	$(-1, 0)$	1	16
$(0, -2)$	4	8			

Tabela 2.9: Constelação com 17 sinais rotulados por $GF(17)$, com $d = -1$

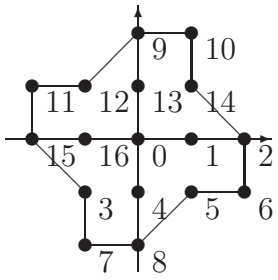

Figura 2.10

Exemplo 2.3.10. *([13], p. 73) Sejam* $d = -1$ *e* $p = 29 \equiv 1 \ (mod\ 4)$. *Aplicando o algoritmo, temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p = 29$ *é dada por* $(a, b) = (5, 2)$. *Assim, podemos tomar* $\pi = 5 + 2i \in \mathbb{Z}[i]$.

2. *A única solução da equação* $a + br = 5 + 2r \equiv 0 \ (mod\ 29)$, *em que* $0 \leq r \leq 28$ *é* $r = 12$.

3. *Assim,* $l \in GF(29)$ *será o rótulo do ponto* $\alpha_l = x + iy$ *de* $A_{29}[i]$, *se* $x + 12y \equiv l \ (mod\ 29)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{29}[i]$ *são dados pela Tabela 2.10, assim como sua representação geométrica pela Figura* 2.11.

(x,y)	$N(\alpha_l)$	$x+12y \equiv l \ (mod\ 29)$	(x,y)	$N(\alpha_l)$	$x+12y \equiv l \ (mod\ 29)$
$(0,0)$	0	0	$(-2,-1)$	5	15
$(1,0)$	1	1	$(-1,-1)$	2	16
$(2,0)$	4	2	$(0,-1)$	1	17
$(-2,-2)$	8	3	$(1,-1)$	2	18
$(-1,-2)$	5	4	$(2,-1)$	5	19
$(0,-2)$	4	5	$(3,-1)$	10	20
$(1,-2)$	5	6	$(-1,-3)$	10	21
$(2,-2)$	8	7	$(-2,2)$	8	22
$(1,3)$	10	8	$(-1,2)$	5	23
$(-3,1)$	10	9	$(0,2)$	4	24
$(-2,1)$	5	10	$(1,2)$	5	25
$(-1,1)$	2	11	$(2,2)$	8	26
$(0,1)$	1	12	$(-2,0)$	4	27
$(1,1)$	2	13	$(-1,0)$	1	28
$(2,1)$	5	14			

Tabela 2.10: Constelação com 29 sinais rotulados por $GF(29)$, com $d=-1$

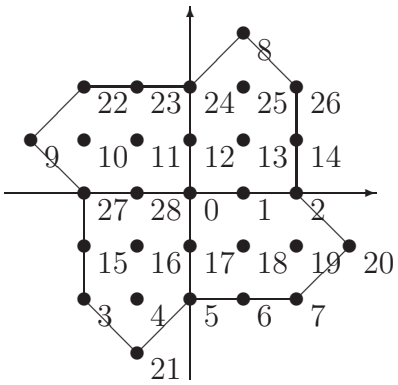

Figura 2.11

Exemplo 2.3.11. *Sejam $d=-1$ e $p=37\equiv 1\ (mod\ 4)$. Aplicando o algoritmo, temos que:*

1. *Uma solução da equação $N(\pi)=a^2+b^2=p=37$ é dada por $(a,b)=(6,1)$. Assim, podemos tomar $\pi=6+i\in\mathbb{Z}[i]$.*

2. *A única solução da equação $a+br=6+r\equiv 0\ (mod\ 37)$, em que $0\leq r\leq 36$ é $r=31$.*

3. *Assim, $l\in GF(37)$ será o rótulo do ponto $\alpha_l=x+yi$ de $A_{37}[i]$, se $x+31y\equiv l\ (mod\ 37)$ e $N(\alpha_l)$ for mínima.*

Os elementos de $A_{37}[i]$ são dados pela Tabela 2.11, assim como sua representação geométrica pela Figura 2.12.

(x,y)	$N(\alpha_l)$	$x+31y \equiv l \ (mod\ 37)$	(x,y)	$N(\alpha_l)$	$x+31y \equiv l \ (mod\ 37)$
$(0,0)$	0	0	$(0,3)$	9	19
$(1,0)$	1	1	$(1,3)$	10	20
$(2,0)$	4	2	$(2,3)$	13	21
$(3,0)$	9	3	$(-3,2)$	13	22
$(-2,-1)$	5	4	$(-2,2)$	8	23
$(-1,-1)$	2	5	$(-1,2)$	5	24
$(0,-1)$	1	6	$(0,2)$	4	25
$(1,-1)$	2	7	$(1,2)$	5	26
$(2,-1)$	5	8	$(2,2)$	8	27
$(3,-1)$	10	9	$(-3,1)$	10	28
$(-2,-2)$	8	10	$(-2,1)$	5	29
$(-1,-2)$	5	11	$(-1,1)$	2	30
$(0,-2)$	4	12	$(0,1)$	1	31
$(1,-2)$	5	13	$(1,1)$	2	32
$(2,-2)$	8	14	$(2,1)$	5	33
$(3,-2)$	13	15	$(-3,0)$	9	34
$(-2,-3)$	13	16	$(-2,0)$	4	35
$(-1,-3)$	10	17	$(-1,0)$	1	36
$(0,-3)$	9	18			

Tabela 2.11: Constelação com 37 sinais rotulados por $GF(37)$, com $d=-1$

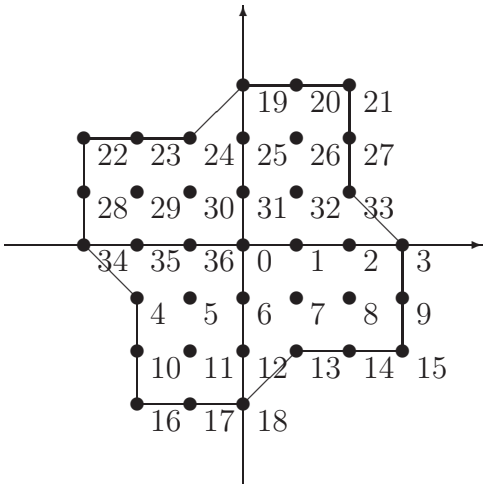

Figura 2.12

Exemplo 2.3.12. *Sejam* $d = -1$ *e* $p = 41 \equiv 1 \ (mod\ 4)$. *Aplicando o algoritmo, temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p = 41$ *é dada por* $(a, b) = (5, 3)$. *Assim, podemos tomar* $\pi = 5 + 3i \in \mathbb{Z}[i]$.

2. *A única solução da equação* $a + br = 5 + 4r \equiv 0 \ (mod\ 41)$, *em que* $0 \leq r \leq 40$ *é* $r = 9$.

3. *Assim,* $l \in GF(41)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *de* $A_{41}[i]$, *se* $x + 9y \equiv l \ (mod\ 41)$ *e* $N(\alpha_l)$ *for mínima.*

Os elementos de $A_{41}[i]$ *são dados pela Tabela 2.12, assim com sua representação geométrica pela Figura* 2.13.

(x, y)	$N(\alpha_l)$	$x + 9y \equiv l \ (mod\ 41)$	(x, y)	$N(\alpha_l)$	$x + 9y \equiv l \ (mod\ 41)$
$(0, 0)$	0	0	$(-2, -2)$	8	21
$(1, 0)$	1	1	$(-1, -2)$	5	22
$(2, 0)$	4	2	$(0, -2)$	4	23
$(3, 0)$	9	3	$(1, -2)$	5	24
$(4, 0)$	16	4	$(2, -2)$	8	25
$(0, -4)$	16	5	$(-1, 3)$	10	26
$(-3, 1)$	10	6	$(0, 3)$	9	27
$(-2, 1)$	5	7	$(1, 3)$	10	28
$(-1, 1)$	2	8	$(-3, -1)$	10	29
$(0, 1)$	1	9	$(-2, -1)$	5	30
$(1, 1)$	2	10	$(-1, -1)$	2	31
$(2, 1)$	5	11	$(0, -1)$	1	32
$(3, 1)$	10	12	$(1, -1)$	2	33
$(-1, -3)$	10	13	$(2, -1)$	5	34
$(0, -3)$	9	14	$(3, -1)$	10	35
$(1, -3)$	10	15	$(0, 4)$	16	36
$(-2, 2)$	8	16	$(-4, 0)$	16	37
$(-1, 2)$	5	17	$(-3, 0)$	9	38
$(0, 2)$	4	18	$(-2, 0)$	4	39
$(1, 2)$	5	19	$(-1, 0)$	1	40
$(2, 2)$	8	20			

Tabela 2.12: Constelação com 41 sinais rotulados por $GF(41)$, com $d = -1$

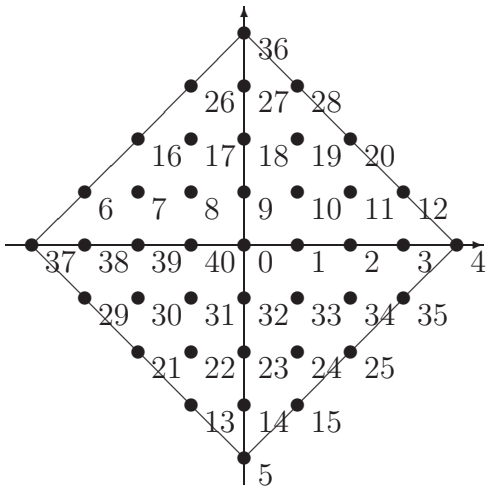

Figura 2.13

Observação 2.3.1. *A importância do primo p se fatorar completamente em $\mathbb{Z}[\rho]$, isto é, $p\mathbb{Z}[\rho] = \mathcal{I}\bar{\mathcal{I}}$, na qual $\mathcal{I} = \langle\pi\rangle$ e $\bar{\mathcal{I}} = \langle\bar{\pi}\rangle$ são dois ideais primos distintos de $\mathbb{Z}[\rho]$ com $\pi = a + b\rho \in \mathbb{Z}[\rho]$ tal que $\rho = i$ se $d = -1$ e $\rho = w = \frac{1+\sqrt{-3}}{2}$ se $d = -3$, garante que o quociente $\dfrac{\mathbb{Z}[\rho]}{\mathcal{I}} = A_p[\rho]$ é isomorfo ao corpo de Galois $GF(p)$. A seguir, veremos dois contra-exemplos no anel de inteiros de Gauss $\mathbb{Z}[i]$, para um primo p inerte e para um primo p que se ramifica totalmente, respectivamente.*

Exemplo 2.3.13. *Se $d = -1$ e $p = 3$, então aplicando o algoritmo, temos que a equação $N(\pi) = a^2 + b^2 = p = 3$, não tem solução inteira. Portanto, o algoritmo não se aplica.*

Exemplo 2.3.14. *Sejam $d = -1$ e $p = 2$. Aplicando o algoritmo, temos:*

1. *Uma solução da equação $N(\pi) = a^2 + b^2 = p = 2$ é dada por $(a, b) = (1, 1)$. Assim, podemos tomar $\pi = 1 + i \in \mathbb{Z}[i]$.*

2. *A única solução da equação $a + br = 1 + r \equiv 0 \ (mod\ 2)$, em que $0 \leq r \leq 1$, é $r = 1$.*

3. *Assim, $l \in GF(2)$ será o rótulo do ponto $\alpha_l = x + yi$ de $A_2[i]$, se $x + y \equiv l \ (mod\ 2)$ e $N(\alpha_l)$ for mínima.*

Note pela Tabela 2.13, temos $(0, 1)$ e $(1, 0)$ são representantes para α_1, o que é uma contradição devido ao Teorema 2.2.1.

(x, y)	$N(\alpha_l)$	$x + y \equiv l \ (mod\ 2)$
$(0, 0)$	0	0
$(0, 1)$	1	1
$(1, 0)$	1	1

Tabela 2.13: $p = 2$ ramifica totalmente em $\mathbb{Z}[i]$

2.4 Construção e rotulamento de constelações com p^m sinais no $\mathbb{R}^2$

Nesta seção, apresentamos procedimentos de construção de constelações de sinais no $\mathbb{R}^2$ casadas a grupos aditivos de $GF(p^m)$ e a p-grupos aditivos G_{p^m} que não fazem parte de um corpo de Galois. Veremos que este fato ocorre de maneira similar no $\mathbb{R}^n$ com uma única ressalva de que os grupos aditivos de $GF(p^k)$ ocorram para $k \leq n$.

As constelações com p^m sinais no $\mathbb{R}^2$, cuja construção é descrita nesta seção, são constituídas por representantes de classes laterais provenientes de ideais $\mathcal{I}$ de norma relativa p^m nos anéis de inteiros $\mathbb{Z}[\rho]$, para $\rho = i$ e $\rho = w = \frac{1+\sqrt{-3}}{2}$. Em [1], [2] Huber e [3] Nóbrega et.al, foram estabelecidas as condições de quando é possível construir constelações com p sinais, cada uma casada ao correspondente grupo aditivo de $GF(p)$. Para isso é analisado se p é um número primo que se decompõe totalmente no anel de inteiros $\mathbb{Z}[\rho]$. Assim, é suficiente tomar o ideal primo em $\mathbb{Z}[\rho]$ gerado por π. Deste modo, indiretamente fica estabelecido um procedimento de se encontrar ideais primos $\mathcal{I}$ em $\mathbb{Z}[\rho]$ gerado por π. Por outro lado, observarmos que neste processo existe um elemento $\pi = a + b\rho$ tal que $N(\pi) = p$ em $\mathbb{Z}[\rho]$. Através do estudo da representatividade de potências de primo p^m associada a norma relativa de um anel de inteiro $\mathbb{Z}[\rho]$, veremos as condições necessárias para construir constelações de sinais com p^m sinais cuja identificação dos pontos de sinais são dadas por elementos dos correspondentes anéis de inteiros $\mathbb{Z}[\rho]$. No caso em que é possível tal construção, é suficiente tomar π como sendo o gerador de um ideal $\mathcal{I}$ em $\mathbb{Z}[\rho]$. Através do quociente $G_{p^m} \cong \dfrac{\mathbb{Z}[\rho]}{\mathcal{I}}$, obtemos o grupo quociente aditivo casado a constelação com p^m sinais

identificados pelos elementos dos correspondentes anéis de inteiros $\mathbb{Z}[\rho]$. A estrutura algébrica de tais grupos quocientes aditivos, G_{p^m}, depende das congruências de p módulo 4 ou de p módulo 6 para os elementos identificados por $\mathbb{Z}[i]$ ou por $\mathbb{Z}[w]$ e do valor de m. Nos trabalhos de Huber [1], [2] e Nóbrega et.al [3] foi mostrado que é possível construir constelações com p sinais identificadas por $\mathbb{Z}[i]$, somente no caso em que $p \equiv 1 \ (mod\ 4)$ e identificadas por $\mathbb{Z}[w]$, no caso em que $p \equiv 1 \ (mod\ 6)$. Em todos esses casos, as constelações de sinais são casadas a grupos aditivos de $GF(p)$. As proposições a seguir, fornecem respostas gerais de quando é possível construir constelações com p^m sinais casadas a grupos, identificadas por $\mathbb{Z}[i]$ e por $\mathbb{Z}[w]$ e fica bem explícito quem são os grupos aditivos.

Proposição 2.4.1. *([6], p. 17) Seja o anel $\mathbb{Z}[i]$.*

1. *Se $p \equiv 1 \ (mod\ 4)$, então é possível construir constelações com p^2 sinais casadas a p-grupos aditivos G_{p^2} que não fazem parte de $GF(p^2)$.*

2. *Se $p \equiv 3 \ (mod\ 4)$, então é possível construir constelações com p^2 sinais casadas a grupos aditivos de $GF(p^2)$.*

Demonstração:

1. Se $p \equiv 1 \ (mod\ 4)$, então pela Proposição 1.6.5, p se decompõe, isto é, $p = \pi\bar{\pi}$, com $\pi \in \mathbb{Z}[i]$. Logo, por definição, $N(\pi) = \pi\bar{\pi} = a^2 + b^2 = p$. Assim, tomando $\pi^2 = (a + bi)^2 = a^2 + b^2 + 2abi$, temos que $N(\pi^2) = N(\pi)N(\pi) = pp = p^2$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[i]$ é dado por $\mathcal{I} = \langle \pi^2 \rangle$.

2. Se $p \equiv 3 \ (mod\ 4)$, então p é um elemento irredutível, pois se $p \equiv 3 \ (mod\ 4)$, então p é da forma $p = 3 + 4t$. Pelo Critério de Euler, temos que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{3+4t-1}{2}} = (-1)^{2t+1} = -1$. Assim, $d = -1$ não é resíduo quadrático módulo p. Pelo Teorema 1.6.3, tem-se que p é inerte em $\mathbb{Z}[i]$, ou seja, $p\mathbb{Z}[i] = \langle p \rangle$. Como $\langle p \rangle$ é um ideal primo, segue que p é um número primo e isto implica, que p é irredutível. Logo, $\langle p \rangle$ é um ideal maximal. Assim, é suficiente tomar $\pi = p$ tal que $N(\pi) = N(p) = pp = p^2$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[i]$ é dado por $\mathcal{I} = \langle \pi \rangle$. ■

Proposição 2.4.2. *([6], p. 17) Seja o anel* $\mathbb{Z}[w]$.

1. *Se* $p \equiv 1 \ (mod\ 6)$, *então é possível construir constelações com* p^2 *sinais casadas a p-grupos aditivos que não fazem parte de* $GF(p^2)$.

2. *Se* $p \not\equiv 1 \ (mod\ 6)$, *então é possível construir constelações com* p^2 *sinais casadas a grupos aditivos de* $GF(p^2)$.

Demonstração:

1. Se $p \equiv 1 \ (mod\ 6)$, então p se decompõe, isto é, $p = \pi\bar{\pi}$, com $\pi \in \mathbb{Z}[w]$. Logo por definição, $N(\pi) = \pi\bar{\pi} = a^2 + ab + b^2 = p$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[w]$ é dado por $\mathcal{I} = \langle \pi^2 \rangle$.

2. Se $p \not\equiv 1 \ (mod\ 6)$, então de maneira análoga a Proposição 2.4.1 é suficiente tomar $\pi = p$ tal que $N(\pi) = N(p) = pp = p^2$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[w]$ é dado por $\mathcal{I} = \langle \pi \rangle$. ■

Deste modo, pelas Proposições 2.4.1 e 2.4.2, temos que para qualquer primo p é possível construir constelações com p^2 sinais. Estendendo para o caso geral, temos as seguintes proposições.

Proposição 2.4.3. *([6], p. 18) Seja o anel* $\mathbb{Z}[i]$.

1. *Se o número primo p é da forma* $p \equiv 1 \ (mod\ 4)$, *então é possível construir constelações com* p^m *sinais casadas a* p^m*-grupos aditivos* G_{p^m} *que não fazem parte de* $GF(p^m)$.

2. *Se o número primo p é da forma* $p \equiv 3 \ (mod\ 4)$, *então é possível construir constelações com* p^m *sinais casadas a grupos aditivos de* $GF(p^m)$, *para o casos em que m é par.*

Demonstração:

1. Se $p \equiv 1 \ (mod\ 4)$, então pela Proposição 1.6.5, p se decompõe, isto é, $p = \pi\bar{\pi}$, com $\pi \in \mathbb{Z}[w]$. Logo, por definição, $N(\pi) = a^2 + b^2 = p$. Tomando $\gamma = \pi^m$, temos que $N(\gamma) = N(\pi^m) = \pi^m$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[i]$ é dado por $\mathcal{I} = \langle \pi^m \rangle$.

2. Se $p \equiv 3 \ (mod\ 4)$, então pela Proposição 2.4.1 tomando $\pi = p$, temos que $N(\pi) = N(p) = pp = p^2$. Assim, tomando $\gamma = \pi^k$, segue que $N(\gamma) = N(\pi^k) = (p^2)^k$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[i]$ é dado por $\mathcal{I} = \langle \pi^k \rangle$, com $k \leq m$. ■

Proposição 2.4.4. *([6], p. 18) Seja o anel $\mathbb{Z}[w]$.*

1. *Se o número primo p é da forma $p \equiv 1 \ (mod\ 6)$, então é possível construir constelações com p^m sinais casadas a p^m-grupos aditivos G_{p^m} que não fazem parte de $GF(p^m)$.*

2. *Se o número primo p é da forma $p \not\equiv 1 \ (mod\ 6)$, então é possível construir constelações com p^m sinais casadas a grupos aditivos de $GF(p^m)$, para o caso em que m é par.*

Demonstração:

1. Se p é fatorável em $\mathbb{Z}[w]$, então existe $\pi \in \mathbb{Z}[w]$ tal que $p = \pi\bar{\pi}$. Neste caso, $N(\pi) = p$. Assim, tomando $\gamma = \pi^m$, segue que $N(\gamma) = N(\pi^m) = p^m$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[w]$ é dado por $\mathcal{I} = \langle \gamma \rangle = \langle \pi^m \rangle$.

2. Se p não é fatorável em $\mathbb{Z}[w]$, então para os valores de $m = 2k$, com k inteiro, é suficiente tomar $\pi = p^k(1 - w)$, uma vez que $N(\pi) = N(p^k)N(1 - w) = p^{2k}1 = p^m$. Neste caso, o ideal $\mathcal{I} \subset \mathbb{Z}[w]$ é dado por $\mathcal{I} = \langle \pi \rangle$. ■

O rotulamento casado para a construção de constelações de p^m sinais no $\mathbb{R}^2$ é definido igual a Definição 2.2.6. Assim, o algoritmo para rotular os elementos dos pontos de sinais das constelações aos elementos de um grupo aditivo G_{p^m} ou de grupos aditivos de $GF(p^m)$ é dada por: Um elemento $l \in G_{p^m}$ ou $l \in GF(p^m)$ é um rótulo para um ponto $a + b\rho \in \mathbb{Z}[\rho]$ se $x + ys \equiv l \ (mod\ p^m)$, na qual $s \in \mathbb{Z}$ é a única solução (em r) da equação $a + br \equiv 0 \ (mod\ p^m)$, em que $0 \leq r \leq p^m - 1$, sendo $\pi = a + b\rho \in \mathbb{Z}[\rho]$ tal que $N(\pi) = p^m$.

Exemplo 2.4.1. *([6], p. 19) Sejam $p = 5$, $m = 2$, $\mathbb{Z}[w]$ e $\pi = a + bw \in \mathbb{Z}[w]$.*

1. *Uma solução da equação* $N(\pi) = a^2 + ab + b^2 = p^m = 25$ *é dada por* $(a, b) = (5, -5)$. *Assim, podemos tomar* $\pi = 5 - 5w$.

2. *A única solução da equação* $a + br = 5 - 5r \equiv 0 \ (mod\ 25)$, *em que* $0 \leq r \leq 24$ *é* $r = -4$.

3. *Com isso, o rótulo do ponto* $a + bw$ *em* $\mathbb{Z}[w]$ *é obtido se* $x - 4y \equiv l \ (mod\ 25)$. *Como* $p = 5 \not\equiv 1 \ (mod\ 6)$, *segue que tais constelações estão casadas a grupos aditivos de* $GF(p^2) = GF(25)$. *Assim, obtemos a Tabela 2.14 e a Figura* 2.14.

(x, y)	$x - 4y \equiv l \ (mod\ 25)$	(x, y)	$x - 4y \equiv l \ (mod\ 25)$	(x, y)	$x - 4y \equiv l \ (mod\ 25)$
$(0, 0)$	0	$(1, -2)$	9	$(-3, 1)$	18
$(1, 0)$	1	$(2, -2)$	10	$(-2, 1)$	19
$(2, 0)$	2	$(-2, 3)$	11	$(-1, 1)$	20
$(-1, -1)$	3	$(-1, 3)$	12	$(0, 1)$	21
$(0, -1)$	4	$(1, -3)$	13	$(1, 1)$	22
$(1, -1)$	5	$(2, -3)$	14	$(-2, 0)$	23
$(2, -1)$	6	$(-2, 2)$	15	$(-1, 0)$	24
$(3, -1)$	7	$(-1, 2)$	16		
$(0, -2)$	8	$(0, 2)$	17		

Tabela 2.14: Constelação com 25 sinais casada a $GF(25)$ em $\mathbb{Z}[w]$

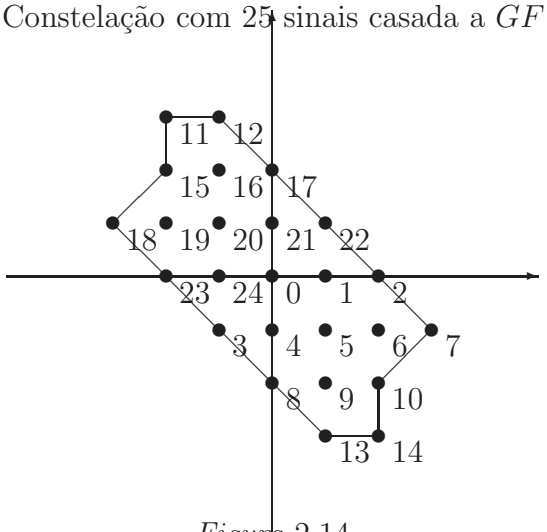

Figura 2.14

Exemplo 2.4.2. *([6], p. 19) Sejam* $p = 5$, $m = 2$, $\mathbb{Z}[i]$ *e* $\pi = a + bi \in \mathbb{Z}[i]$.

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p^m = 25$ *é dada por* $(a, b) = (4, -3)$. *Assim, podemos tomar* $\pi = 4 - 3i$.

2. *A única solução da equação* $a + br = 4 - 3r \equiv 0 \ (mod\ 25)$, *em que* $0 \leq r \leq 24$ *é* $r = -7$.

3. *Com isso, o rótulo do ponto* $a + bi$ *em* $\mathbb{Z}[i]$ *é obtido se* $x - 7y \equiv l \ (mod\ 25)$. *Como* $p = 5 \equiv 1 \ (mod\ 4)$, *segue que tais constelações estão casadas a 5-grupos aditivos* $G_{p^2} = G_{25}$ *que não fazem parte de* $GF(p^2) = GF(25)$. *Assim, obtemos a Tabela 2.15 e a Figura* 2.15.

(x, y)	$x - 7y \equiv l \ (mod\ 25)$	(x, y)	$x - 7y \equiv l \ (mod\ 25)$	(x, y)	$x - y \equiv l \ (mod\ 25)$
$(0, 0)$	0	$(2, -1)$	9	$(-1, 1)$	17
$(1, 0)$	1	$(-1, 2)$	10	$(0, 1)$	18
$(2, 0)$	2	$(0, 2)$	11	$(1, 1)$	19
$(3, 0)$	3	$(1, 2)$	12	$(2, 1)$	20
$(0, 3)$	4	$(-1, -2)$	13	$(0, -3)$	21
$(-2, -1)$	5	$(0, -2)$	14	$(-3, 0)$	22
$(-1, -1)$	6	$(1, -2)$	15	$(-2, 0)$	23
$(0, -1)$	7	$(-2, 1)$		$(-1, 0)$	24
$(1, -1)$	8				

Tabela 2.15: Constelação com 25 sinais casada a G_{25} em $\mathbb{Z}[i]$

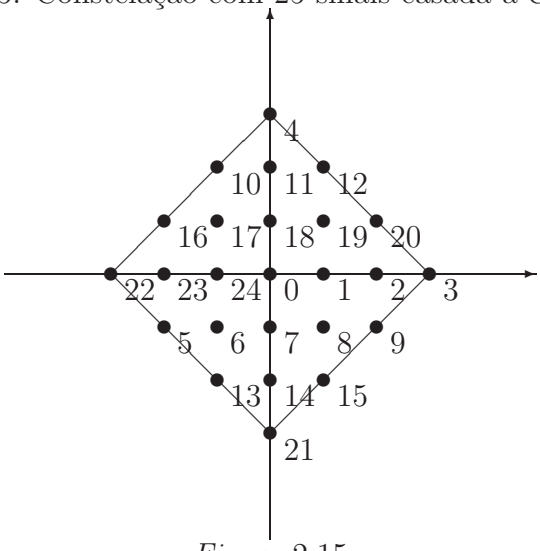

Figura 2.15

Exemplo 2.4.3. *Sejam* $p = 7$, $m = 2$, $\mathbb{Z}[w]$ *e* $\pi = a + bw \in \mathbb{Z}[w]$. *Sob estas condições temos:*

1. *Uma solução da equação* $N(\pi) = a^2 + ab + b^2 = p^m = 49$ *é dada por* $(a, b) = (7, -7)$. *Assim, podemos tomar* $\pi = 7 - 7w$.

2. *A única solução da equação* $a + br = 7 - 7r \equiv 0 \ (mod\ 49)$*, em que* $0 \leq r \leq 48$ *é* $r = -6$.

3. *Com isso, o rótulo do ponto* $a + bw$ *em* $\mathbb{Z}[w]$ *é obtido se* $x - 6y \equiv l \ (mod\ 49)$. *Como* $p = 7 \equiv 1 \ (mod\ 6)$*, tais constelações estão casadas a 7-grupos aditivos* $G_{p^2} = G_{49}$ *que não fazem parte de* $GF(p^2) = GF(49)$. *Assim, temos a Tabela 2.16 e a Figura* 2.16.

(x, y)	$x - 6y \equiv l \ (mod\ 49)$	(x, y)	$x - 6y \equiv l \ (mod\ 49)$	(x, y)	$x - 6y \equiv l \ (mod\ 49)$
$(0, 0)$	0	$(-1, -3)$	17	$(-4, 2)$	33
$(1, 0)$	1	$(0, -3)$	18	$(-3, 2)$	34
$(2, 0)$	2	$(1, -3)$	19	$(-2, 2)$	35
$(3, 0)$	3	$(2, -3)$	20	$(-1, 2)$	36
$(-2, -1)$	4	$(3, -3)$	21	$(0, 2)$	37
$(-1, -1)$	5	$(4, -3)$	22	$(1, 2)$	38
$(0, -1)$	6	$(-1, -4)$	23	$(2, 2)$	39
$(1, -1)$	7	$(0, -4)$	24	$(-3, 1)$	40
$(2, -1)$	8	$(0, 4)$	25	$(-2, 1)$	41
$(3, -1)$	9	$(1, 4)$	26	$(-1, 1)$	42
$(-2, -2)$	10	$(-4, 3)$	27	$(0, 1)$	43
$(-1, -2)$	11	$(-3, 3)$	28	$(1, 1)$	44
$(0, -2)$	12	$(-2, 3)$	29	$(2, 1)$	45
$(1, -2)$	13	$(-1, 3)$	30	$(-3, 0)$	46
$(2, -2)$	14	$(0, 3)$	31	$(-2, 0)$	47
$(3, -2)$	15	$(1, 3)$	32	$(-1, 0)$	48
$(4, -2)$	16				

Tabela 2.16: Constelação com 49 sinais casada a G_{49} em $\mathbb{Z}[w]$

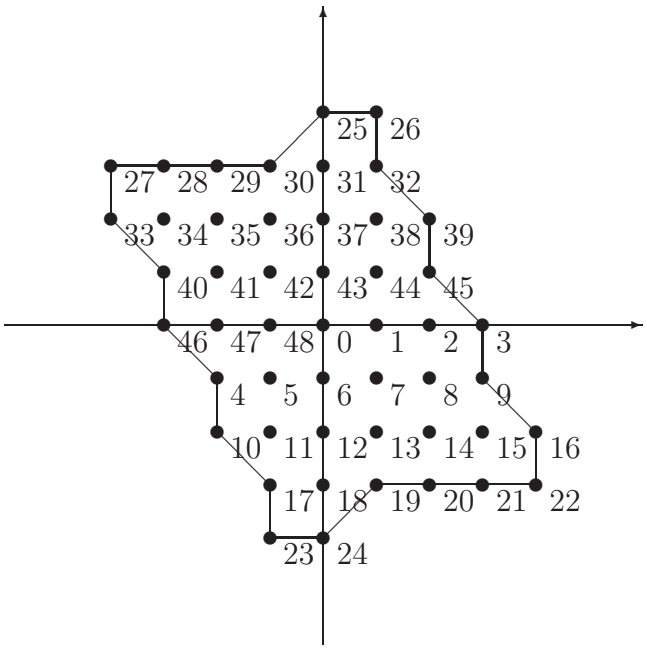

Figura 2.16

Exemplo 2.4.4. *Sejam* $p = 7$, $m = 2$, $\mathbb{Z}[i]$ *e* $\pi = a + bi \in \mathbb{Z}[i]$.

1. *Uma solução da equação* $N(\pi) = a^2 + b^2 = p^m = 49$ *é dada por* $(a, b) = (0, -7)$.

2. *A única solução da equação* $a + br = -7r \equiv 0 \ (mod\ 49)$, *em que* $0 \leq r \leq 48$ *é* $r = -7$.

3. *Com isso, o rótulo do ponto* $a + bi$ *em* $\mathbb{Z}[i]$ *é obtido se* $x - 7y \equiv l \ (mod\ 49)$. *Como* $p = 7 \equiv 3 \ (mod\ 4)$ *segue que tais constelações estão casadas a grupos aditivos de* $GF(p^2) = GF(49)$. *Assim, obtemos a Tabela 2.17 e a Figura* 2.17.

(x,y)	$x-7y \equiv l \ (mod\ 49)$	(x,y)	$x-7y \equiv l \ (mod\ 49)$	(x,y)	$x-7y \equiv l \ (mod\ 49)$
$(0,0)$	0	$(3,-2)$	17	$(-2,2)$	33
$(1,0)$	1	$(-3,-3)$	18	$(-1,2)$	34
$(2,0)$	2	$(-2,-3)$	19	$(0,2)$	35
$(3,0)$	3	$(-1,-3)$	20	$(1,2)$	36
$(-3,-1)$	4	$(0,-3)$	21	$(2,2)$	37
$(-2,-1)$	5	$(1,-3)$	22	$(3,2)$	38
$(-1,-1)$	6	$(2,-3)$	23	$(-3,1)$	39
$(0,-1)$	7	$(3,-3)$	24	$(-2,1)$	40
$(1,-1)$	8	$(-3,3)$	25	$(-1,1)$	41
$(2,-1)$	9	$(-2,3)$	26	$(0,1)$	42
$(3,-1)$	10	$(-1,3)$	27	$(1,1)$	43
$(-3,-2)$	11	$(0,3)$	28	$(2,1)$	44
$(-2,-2)$	12	$(1,3)$	29	$(3,1)$	45
$(-1,-2)$	13	$(2,3)$	30	$(-3,0)$	46
$(0,-2)$	14	$(3,3)$	31	$(-2,0)$	47
$(1,-2)$	15	$(-3,2)$	32	$(-1,0)$	48
$(2,-2)$	16				

Tabela 2.17: Constelação com 49 sinais casada a $GF(49)$ em $\mathbb{Z}[i]$

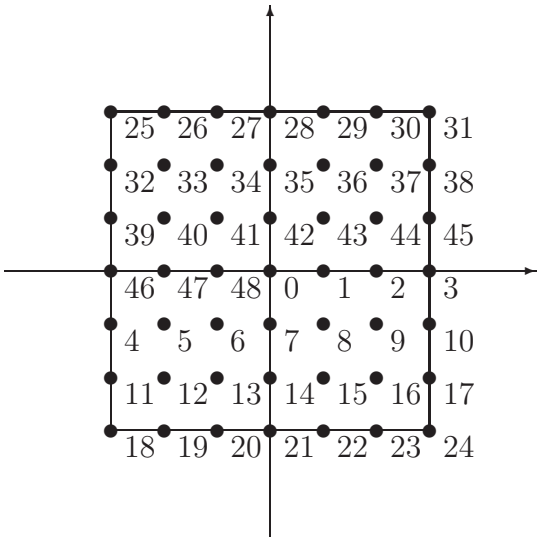

Figura 2.17

Observação 2.4.1. *Convém observar, que nos Exemplos 2.4.1 e 2.4.2, 2.4.3 e 2.4.4, considerando o mesmo primo p, identificado via anéis de inteiros Eisenstein-Jacobi e de Gauss, obtemos constelações de sinais de grupos de rótulos distintos. Além disso, o arranjo geométrico destas constelações de sinais são diferentes.*

Capítulo 3

Constelações de sinais via corpos ciclotômicos

3.1 Introdução

Neste capítulo, veremos resultados para a construção e decodificação dos códigos via corpos ciclotômicos. Estudaremos um novo conceito da distância de Mannheim via corpos ciclotômicos e também condições necessárias para a construção de constelações de sinais no $\mathbb{R}^2$ que sejam casadas ao grupo aditivo de $GF(p)$. Os elementos das constelações de sinais são identificados por elementos dos correspondentes anéis de inteiros $\mathbb{Z}[\xi_n]$, em que ξ_n é uma raiz n-ésima primitiva da unidade.

3.2 Fatos sobre corpos ciclotômicos

Nesta seção, veremos resultados importantes que serão fundamentais para a construção, codificação/decodificação de códigos via corpos ciclotômicos, que veremos no Capítulo 5 baseados nos trabalhos de [8] e [9].

Definição 3.2.1. *Seja $\alpha \in \mathbb{Q}(\xi_n)$ definimos a norma de $\alpha \in \mathbb{Q}(\xi_n)$ como $N(\alpha) = \prod_{\sigma \in Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))} \sigma(\alpha) = \prod_{i=1}^{\varphi(n)} \sigma_i(\alpha)$, na qual $\varphi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$.*

Observação 3.2.1. *Seja p um número primo. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ é tal que $N(\alpha) = p$, então $N(\sigma(\alpha)) = p$, para $\alpha \in Gal_{\mathbb{Q}}(\mathbb{K})$.*

Proposição 3.2.1. *([9], p. 108) Se $\alpha, \beta \in \mathbb{Z}[\xi_n]$ são elementos irredutíveis, então $\langle\alpha\beta\rangle = \langle\alpha\rangle\langle\beta\rangle$.*

Demonstração: Se $x \in \langle\alpha\beta\rangle$, então $x = \alpha\beta t$, para algum t em $\mathbb{Z}[\xi_n]$. Logo, $x = (\alpha 1)(\beta t) \in \langle\alpha\rangle\langle\beta\rangle$ e assim, $\langle\alpha\beta\rangle \subseteq \langle\alpha\rangle\langle\beta\rangle$. Reciprocamente, se $x \in \langle\alpha\rangle\langle\beta\rangle$, então $x = (\alpha t_1)(\beta t_2) = (\alpha\beta)(t_1 t_2) \in \langle\alpha\beta\rangle$. Assim, $\langle\alpha\rangle\langle\beta\rangle \subseteq \langle\alpha\beta\rangle$ e portanto, $\langle\alpha\beta\rangle = \langle\alpha\rangle\langle\beta\rangle$. ■

Para os resultados a seguir, consideremos $n \in \{1\} \cup A$, onde $A = \{3, 2, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$.

Teorema 3.2.1. *([9], p. 108) Sejam $\alpha \in \mathbb{Z}[\xi_n]$ e p um número primo tal que $p \nmid n$. Se $N(\alpha) = p$, então α é um elemento irredutível em $\mathbb{Z}[\xi_n]$ e $p = nk + 1$. Além disso, $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ é um corpo com p elementos.*

Demonstração: Se $\alpha \in \mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p$, então pela Proposição 1.4.3, temos que $\langle\alpha\rangle$ é um ideal primo de $\mathbb{Z}[\xi_n]$. Como $\mathbb{Z}[\xi_n]$ é um anel principal, segue pela Observação 1.4.2, que α é um elemento irredutível, uma vez que $\langle\alpha\rangle$ é um ideal maximal em $\mathbb{Z}[\xi_n]$. Agora, se $\sigma \in Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$, então pela Observação 3.2.1, temos que $N(\sigma(\alpha)) = p$. Assim, novamente pela Proposição 1.4.3 e pela Observação 3.2.1, tem-se que $\sigma(\alpha)$ é um elemento irredutível para todo $\sigma \in Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$. Considerando $\sigma_i(\alpha) = \alpha_i$, para $i = 1, 2, \ldots, \varphi(n)$, temos que $p = N(\alpha) = \prod_{i=1}^{\varphi(n)} \sigma_i(\alpha) = \prod_{i=1}^{\varphi(n)} \alpha_i$. Expressando a decomposição de p em $\mathbb{Z}[\xi_n]$, temos que $p\mathbb{Z}[\xi_n] = \prod_{i=1}^{\varphi(n)} \langle\alpha_i\rangle$. Como $\mathbb{Z}[\xi_n]$ é um anel de Dedekind, segue pelo Teorema 1.3.2, que essa fatoração é única. Pelo Teorema 1.7.4, tem-se que $p \equiv 1 \ (mod\ n)$. Finalmente, como $N(\alpha) = p = \#\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$, segue que $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ é um corpo com p elementos. ■

Exemplo 3.2.1. *Os elementos irredutíveis em $\mathbb{Z}[\xi_{16}]$ e $\mathbb{Z}[\xi_7]$ são dados pelas seguintes tabelas.*

elemento irredutível	norma
$-2-\xi_{16}+2\xi_{16}^2+\xi_{16}^3-\xi_{16}^4$	17
$1+2\xi_{16}+\xi_{16}^2+\xi_{16}^4$	97
$-2-2\xi_{16}-\xi_{16}^4$	113
$-2-\xi_{16}+\xi_{16}^3+\xi_{16}^4$	193
$2+\xi_{16}+2\xi_{16}^2+\xi_{16}^3+\xi_{16}^4$	241
$-2-2\xi_{16}$	257
$2+\xi_{16}+\xi_{16}^2+\xi_{16}^3$	337
$-2-2\xi_{16}+\xi_{16}^3$	353

Tabela 3.1: Elementos irredutíveis em $\mathbb{Z}[\xi_{16}]$

elemento irredutível	norma	elemento irredutível	norma
$1+\xi_7+2\xi_7^2$	29	$1+2\xi_7+\xi_7^2+\xi_7^3$	2^3
$2+\xi_7^2$	43	$2+3\xi_7+\xi_7^2-2\xi_7^3$	11^3
$1-\xi_7+2\xi_7^2$	71	$2+5\xi_7+3\xi_7^2-2\xi_7^3$	23^3
$1-2\xi_7+2\xi_7^2$	113	$2-\xi_7+2\xi_7^2$	13^2
$-2\xi_7+\xi_7^2$	127	$4+3\xi_7+4\xi_7^2$	41^2
$2+2\xi_7+\xi_7^3$	197	17	17^6
$2+\xi_7-\xi_7^2+\xi_7^3$	211	19	19^6
$2+\xi_7-\xi_7^2+2\xi_7^3$	239	31	31^6

Tabela 3.2: Elementos irredutíveis em $\mathbb{Z}[\xi_7]$

Observação 3.2.2.

1. *Em [12], p.76, Exercício* 3.8 *fornece um processo para se obter a norma de um elemento irredutível, no caso em que n é um número ímpar.*

2. *Note que, as normas dos elementos irredutíveis dados nas Tabelas 3.1 e 3.2, são da forma $p = nk + 1$, em que $n = 16$ ou $n = 7$, para algum k em $\mathbb{Z}$, respectivamente.*

Proposição 3.2.2. *([9], p. 109) Seja $(G, .)$ um grupo cíclico multiplicativo com*

$p-1$ elementos, em que $p = nk+1$ é um número primo ímpar para $k \in \mathbb{Z}$. Se n é ímpar, então existe um único subgrupo cíclico de G com $2n$ elementos.

Demonstração: Seja n ímpar. Se $p = nk+1$, então $n \mid p-1$. Como $2 \mid p-1$ e $mdc(n,2) = 1$, segue que $2n \mid p-1$, ou seja, $p-1 = 2nk$, para algum k em $\mathbb{Z}$. Consideremos $G = \langle\gamma\rangle$ um grupo multiplicativo cíclico tal que $o(G) = p-1$. Vamos provar que existe um único subgrupo H de G tal que $o(H) = 2n$. Tomando $H = \langle\gamma^k\rangle$, temos que:

- H é um subgrupo de G.
- H é um subgrupo cíclico, uma vez que é um subgrupo de um grupo cíclico.
- A ordem de H é $2n$, pois $(\gamma^k)^{2n} = \gamma^{2nk} = \gamma^{p-1} = 1$ e se existir $0 < j < 2n$ tal que $(\gamma^k)^j = 1$, ou seja, $\gamma^{kj} = 1$. Como $o(\gamma) = o(G) = p-1$, segue que $p-1 \mid kj$. Assim, $kj = (p-1)l$ para algum l em $\mathbb{Z}$. Como $2nk = p-1$, segue que $kj = 2nkl$. Logo, $j = 2nl$ e isto implica que $2n \mid j$. Assim, $2n \leq j$, o que contradiz a escolha de j. Portanto, $o(H) = 2n$.
- H é único: suponhamos que existem H e K subgrupos cíclicos de G tal que $o(H) = o(K)$, na qual $H = \langle\alpha\rangle$ e $K = \langle\beta\rangle$. Como aplicação $\Psi : H \to K$ definida por $\Psi(\alpha) = \beta$ é um isomorfismo, segue que $H = K$.

Portanto, existe um único subgrupo cíclico H de G tal que $o(H) = 2n$, onde n ímpar. ■

Proposição 3.2.3. *([9], p. 109) Seja $(G,.)$ um grupo cíclico multiplicativo com $p-1$ elementos, em que $p = nk+1$ é um número primo ímpar para $k \in \mathbb{Z}$. Se n é par, então existe um único subgrupo cíclico de G com n elementos.*

Demonstração: Seja n par. Se $p = nk+1$, então $n \mid p-1$, ou seja, $p-1 = nk$ para algum k em $\mathbb{Z}$. Consideremos $G = \langle\gamma\rangle$ um grupo multiplicativo cíclico tal que $o(G) = p-1$. Tomando $H = \langle\gamma^k\rangle$, temos que:

- H é um subgrupo de G.

- H é um subgrupo cíclico, uma vez que é um subgrupo de um grupo cíclico.

- A ordem de H é n, pois $(\gamma^k)^n = \gamma^{nk} = \gamma^{p-1} = 1$ e se existir $0 < j < n$ tal que $(\gamma^k)^j = 1$, ou seja, $\gamma^{kj} = 1$. Como $o(\gamma) = o(G) = p-1$, segue que $p-1 \mid kj$. Assim, $kj = (p-1)l$, para algum l em $\mathbb{Z}$. Como $nk = p-1$, segue que $kj = nkl$. Assim, $j = nl$ e isto implica que $n \mid j$. Logo, $n \leq j$, o que contradiz a escolha de j.

- H é único: suponhamos que existam H e K subgrupos cíclicos de G tal que $o(H) = o(K)$, na qual $H = \langle\alpha\rangle$ e $K = \langle\beta\rangle$. Como a aplicação $\Psi : H \to K$ definida por $\Psi(\alpha) = \beta$ é um isomorfismo. Logo, $H = K$.

Portanto, existe um único subgrupo cíclico H de G tal que $o(H) = n$, em que n é par. ■

Teorema 3.2.2. *([9], p. 109) Sejam p um número primo ímpar e α um elemento irredutível em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk + 1$.*

1. *Se n é ímpar, então o grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ contém um único subgrupo cíclico com $2n$ elementos.*

2. *Se n é par, então o grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ contém um único subgrupo cíclico com n elementos.*

Demonstração:

1. Sejam n ímpar e α um elemento irredutível de $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk+1$. Como α é um elemento irredutível de $\mathbb{Z}[\xi_n]$, pela Observação 1.4.2, segue que $\langle\alpha\rangle$ é um ideal maximal em $\mathbb{Z}[\xi_n]$. Assim, $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ é um corpo e tem p elementos, uma vez que $\#\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle} = N(\langle\alpha\rangle) = N(\alpha) = p$. Logo, o grupo multiplicativo maximal G de $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ tem $p-1$ elementos, ou seja, $o(G) = p-1$. Além disso, G é um grupo cíclico. Pela Proposição 3.2.2, temos que existe um único subgrupo cíclico do grupo multiplicativo G do corpo $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ com $2n$ elementos.

2. Sejam n par e α um elemento irredutível de $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk + 1$. De maneira ánaloga, ao item 1, concluímos que $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ é um corpo com p elementos. Logo, o grupo multiplicativo maximal G de $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ tem $p-1$ elementos. Pela Proposição 3.2.3, temos que existe um único subgrupo cíclico do grupo multiplicativo G do corpo $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ com n elementos. ■

Lema 3.2.1. *([9], p. 109) Sejam n ímpar, p um número primo ímpar e $d = \frac{n}{mdc(n,j)}$. Se ξ_n^j, para $j = 1, 2, \ldots, n$ é uma raiz d-ésima primitiva da unidade com $d > 1$, então $N(1+\xi_n^j)$ para $j = 1, 2, \ldots, n$ e $N(1-\xi_n^j)$ para $j = 1, 2, \ldots, n-1$, não possuem p como um divisor.*

Demonstração: Denotando ξ_n^j por ϵ_d, temos que

$$N(1+\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1+\xi_n^j) = N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(N_{\mathbb{Q}(\xi_n)|\mathbb{Q}(\epsilon_d)}(1+\xi_n^j)) = [N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(1+\epsilon_d)]^{\frac{\varphi(n)}{\varphi(d)}},$$

para $j = 1, 2, \ldots, n$. Como

$$\begin{aligned} N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(1+\epsilon_d) &= \prod_{i=1}^{\varphi(d)} \sigma_i(1+\epsilon_d) = \prod_{i=1}^{\varphi(d)} \sigma_i(1+\xi_n^j) \\ &= (1+\sigma_1(\xi_n^j))(1+\sigma_2(\xi_n^j)) \ldots (1+\sigma_{\varphi(d)}(\xi_n^j)) \\ &= (1+\xi_n^j)(1+\xi_n^{2j}) \ldots (1+\xi_n^{\varphi(d)j}) \\ &= (1+\epsilon_1)(1+\epsilon_2) \ldots (1+\epsilon_{\varphi(d)}) \\ &= (-1)(-1-\epsilon_1)(-1)(-1-\epsilon_2) \ldots (-1)(-1-\epsilon_{\varphi(d)}) \\ &= (-1)^{\varphi(d)}(-1-\epsilon_1) \ldots (-1-\epsilon_{\varphi(d)}) \\ &= (-1)^{\varphi(d)}\Phi_d(-1), \end{aligned} \tag{3.1}$$

em que $\phi_d(x)$ é o d-ésimo polinômio ciclotômico e ϵ_i são todas as raízes d-ésimas distintas primitivas da unidade, segue que

$$N(1+\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1+\xi_n^j) = [(-1)^{\varphi(d)}\phi_d(-1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.2}$$

para $j = 1, 2, \ldots, n$ e

$$N(1-\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1-\xi_n^j) = N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(N_{\mathbb{Q}(\xi_n)|\mathbb{Q}(\epsilon_d)}(1-\xi_n^j)) = [N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(1-\epsilon_d)]^{\frac{\varphi(n)}{\varphi(d)}},$$

para $j = 1, 2, \ldots, n-1$. De maneira análoga ao raciocínio usado na Equação (3.1), obtemos que $N_{\mathbb{Q}(\epsilon_d)|\mathbb{Q}}(1-\epsilon_d) = \phi_d(1)$, na qual ϕ_d é o d-ésimo polinômio ciclotômico. Assim,

$$N(1-\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.3}$$

para $j = 1, 2, \ldots, n-1$. Por outro lado, como $x^d - 1 = \prod_{h|d} \phi_h(x)$, com $d > 1$, segue que $mdc((x-1), \phi_d(x)) = 1$, uma vez que os polinômios $(x-1)$ e $\phi_d(x) = (x-\epsilon_1)\ldots(x-\epsilon_{\varphi_d})$, em que $\epsilon_i \neq 1$ para todo i são raízes d-ésimas distintas primitivas da unidade e assim não possuem fatores comuns. Agora, como $x^d - 1 = \prod_{h|d} \phi_h(x) = \phi_1(x)\phi_{s_1}(x)\ldots\phi_{s_r}(x)\phi_d(x)$, onde $s_i \mid d$, para todo $i = 1, \ldots, r$, segue que $\phi_1(x) = x-1$ e $\phi_d(x)$ são co-primo. Tomando $a(x) = \phi_{s_1}(x)\ldots\phi_{s_r}(x)$, temos que $x^d - 1 = (x-1)(\phi_{s_1}(x)\ldots\phi_{s_r}(x))\phi_d(x)$, ou seja, $\dfrac{x^d-1}{x-1} = a(x)\phi_d(x)$. Logo

$$x^{d-1} + x^{d-2} + \ldots + x + 1 = a(x)\phi_d(x). \tag{3.4}$$

Pelo Lema de Gauss, temos que $a(x) \in \mathbb{Z}[x]$. Observamos que d é ímpar, uma vez que, se d fosse par teríamos $d = \dfrac{n}{mdc(n,j)}$, ou seja, $d = mdc(n,j) = n$ o que é um absurdo, pois n é ímpar. Assim, tomando $x = -1$ na Equação (3.4) e usando o fato que d é ímpar temos que,

$$a(-1)\phi_d(-1) = (-1)^{d-1} + \ldots - 1 + 1 = 1.$$

Logo, $\phi_d(-1) = 1$ ou $\phi_d(-1) = -1$. Se $\phi_d(-1) = 1$, pela equação (3.2), então $N(1+\xi_n^j) = (-1)^{\varphi(n)} = 1$, que não tem p como um divisor primo. Se $\phi_d(-1) = -1$, pela Equação (3.3), então $N(1+\xi_n^j) = (-1)^{\frac{\varphi(n)}{\varphi(d)}} = -1$, o que é um absurdo, pois contraria o Lema 1.7.1. Agora, tomando $x = 1$, na Equação (3.4), temos que

$$a(1)\phi_d(1) = \underbrace{1 + \ldots + 1}_{d \text{ vezes}} = d.$$

Como $N(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}$ e $a(1)\phi(1) = d$, segue que $N(1-\xi_n^j)$ é um divisor de $d^{\frac{\varphi(n)}{\varphi(d)}}$, para $j = 1, 2, \ldots, n-1$. Agora, como $d \mid n$, segue que $N(1-\xi_n^j)$ divide $n^{\frac{\varphi(n)}{\varphi(d)}}$, para $j = 1, 2, \ldots, n-1$. Se $p = nk+1$ divide $N(1-\xi_n^j)$, para $j = 1, 2, \ldots, n-1$, então p divide n e portanto, p divide 1, o que é um absurdo. Assim, $N(1-\xi_n^j)$ não possui p como um divisor primo, o que completa a demonstração. ■

Proposição 3.2.4. *([9], p. 109) Sejam p um número primo ímpar, n um número ímpar e α um elemento irredutível em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk+1$. Se α é irredutível, então quaisquer dois elementos distintos do conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ estão em classes laterais distintas módulo o ideal $\langle\alpha\rangle$.*

Demonstração: Seja n ímpar. Se $(-\xi_n)^h$ e $(-\xi_n)^k$ estão na mesma classe lateral módulo o ideal $\langle\alpha\rangle$ em que $1 \leq h < k \leq 2n$, então $\overline{(-\xi_n)^h} = \overline{(-\xi_n)^k}$ se, e somente se, $(-\xi_n)^h + \langle\alpha\rangle = (-\xi_n)^k + \langle\alpha\rangle$ se, e somente se, $(-\xi_n)^h - (-\xi_n)^k \in \langle\alpha\rangle$. Logo, $(-\xi_n)^h - (-\xi_n)^k = \alpha\beta$, para algum $\beta \in \mathbb{Z}$. Calculando a norma, temos que

$$N((-\xi_n)^h - (-\xi_n)^k) = N(1 - (-\xi_n)^{k-h}) = N(\alpha)N(\beta) = pN(\beta).$$

Tomando $j = k - h$ tem-se que $N(1 - \xi_n^j) = pN(\beta)$, para $j = 1, 2, \ldots, n-1$. Logo, $N(1 - \xi_n^j)$ possuem como divisor o primo p. Agora, como ξ_n^j é uma raiz $d = \dfrac{n}{mdc(n,j)}$-ésima primitiva da unidade, para n e j fixos, temos que:

1. Se $d = 1$, então $mdc(n, j) = n$ e assim, $n = j$, o que não ocorre.

2. Se $d > 1$, pelo Lema 3.2.1, temos que $N(1 \pm \xi_n^j)$ não possui p como um divisor.

Portanto, $(-\xi_n)^h$ e $(-\xi_n)^k$, para $1 \leq h < k \leq 2n$ estão em classes laterais distintas módulo $\langle\alpha\rangle$. De modo análogo, temos que ξ_n^h e ξ_n^k, $(-\xi_n)^h$ e ξ_n^k e ξ_n^h e $(-\xi_n)^k$, para $1 \leq h < k \leq 2n$, estão em classe laterais distintas módulo $\langle\alpha\rangle$. ■

Teorema 3.2.3. *([9], p. 109) Sejam p um número primo ímpar, n um número ímpar e α um elemento em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk+1$. Se α é irredutível, então podemos tomar o conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ como sendo um conjunto completo das classes laterais do subgrupo cíclico com $2n$ elementos do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$.*

Demonstração: Pela Proposição 3.2.4 temos que quaisquer dois elementos distintos de $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$, estão em classes laterais distintas módulo o ideal $\langle\alpha\rangle$. Como o conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ é um subgrupo cíclico com $2n$ elementos gerado por $-\xi_n$ e é único pelo Teorema 3.2.2, segue que podemos tomar o conjunto

$\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$, como sendo um conjunto completo das classes laterais do subgrupo cíclico com $2n$ elementos do grupo multiplicativo do corpo $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$. ■

Lema 3.2.2. *([9], p. 109) Sejam n um número par, p um número primo ímpar e $d = 2^k$ para $k \in \mathbb{Z}$ com $k \geq 2$. Se ξ_n^j para $j = 1, 2, \ldots, n$ é uma raiz d-ésima primitiva da unidade, então $N(1+\xi_n^j)$ para $1 \leq j < \frac{n}{2}$ e $N(1-\xi_n^j)$ para $1 \leq j \leq \frac{n}{2}$, não possuem p como um divisor.*

Demonstração: Denotando ξ_n^j por ϵ_d, de modo análogo ao Lema 3.2.1, temos que

$$N(1+\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1+\xi_n^j) = [(-1)^{\varphi(d)}\phi_d(-1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.5}$$

para $1 \leq j < \frac{n}{2}$ e

$$N(1-\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.6}$$

para $1 \leq j \leq \frac{n}{2}$, na qual $\phi_d(x)$ é o d-ésimo polinômio ciclotômico. Temos que $x^{\frac{d}{2}} - 1$ e $\phi_d(x)$ são co-primos, uma vez que as raízes de $\phi_d(x) = (x-\eta_1)\ldots(x-\eta_{\varphi(d)})$ são todas as raízes d-ésima primitivas da unidade e não tem fator comum com $x^{\frac{d}{2}} - 1$. Como $(x^{\frac{d}{2}} - 1)(x^{\frac{d}{2}} + 1) = x^d - 1 = \prod_{h|d}\phi_h(x) = \phi_1(x)\phi_{s_1}(x)\ldots\phi_{s_r}(x)\phi_d(x)$, em que $s_i \mid d$, para todo $i = 1, 2, \ldots, r$ e $mdc((x^{\frac{d}{2}} - 1), \phi_d(x)) = 1$, segue que

$$x^{\frac{d}{2}} + 1 = \frac{\phi_1(x)\phi_{s_1}(x)\ldots\phi_{s_r}(x)}{x^{\frac{d}{2}} - 1}\phi_d(x) = b(x)\phi_d(x), \tag{3.7}$$

na qual $b(x) = \frac{\phi_1(x)\phi_{s_1}(x)\ldots\phi_{s_r}(x)}{x^{\frac{d}{2}} - 1}$. Pelo fato de $x^{\frac{d}{2}} + 1$ e $\phi_d(x)$ serem polinômios primitivos em $\mathbb{Z}[x]$, pelo Lema de Gauss tem-se que $b(x) \in \mathbb{Z}[x]$. Tomando $x = -1$ na Equação (3.7) e do fato de d ser uma potência de 2, temos que $b(-1)\phi_d(-1) = 2$. Logo, $\phi_d(-1) = \pm 1$ ou $\phi_d(-1) = \pm 2$. Se $\phi_d(-1) = \pm 1$, então o resultado segue de modo ánalogo ao Lema 3.2.1. Se $\phi_d(-1) = \pm 2$, então pela Equação (3.5), tem-se que $N(1+\xi_n^j) = [(-1)^{\varphi(n)}(-2)]^{\frac{\varphi(n)}{\varphi(d)}} = (\pm 2)^{\frac{\varphi(n)}{\varphi(d)}} < 0$ e portanto, $N(1+\xi_n^j)$, para $1 \leq j < \frac{n}{2}$ não possui um divisor primo ímpar p. Tomando $x = 1$ na Equação (3.7), segue que $b(1)\phi_d(1) = 2$. De modo análogo ao caso anterior, concluímos que $N(1-\xi_n^j)$ não possui um divisor primo p, o que completa a demonstração. ■

Lema 3.2.3. *([9], p. 109) Sejam n um número par, p um número primo ímpar e $d = 2^k m$, em que $m, k \in \mathbb{Z}$, $k \geq 1$ e $mdc(2, m) = 1$. Se ξ_n^j, para $j = 1, 2, \ldots, n$, é uma raiz d-ésima primitiva da unidade, então $N(1+\xi_n^j)$ para $1 \leq j < \frac{n}{2}$ e $N(1-\xi_n^j)$ para $1 \leq j \leq \frac{n}{2}$ não possuem p como um divisor.*

Demonstração: Denotando ξ_n^j por ϵ_d, temos de modo análogo ao Lema 3.2.1 que

$$N(1+\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1+\xi_n^j) = [(-1)^{\varphi(d)}\phi_d(-1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.8}$$

para $1 \leq j < \frac{n}{2}$ e

$$N(1-\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.9}$$

para $1 \leq j \leq \frac{n}{2}$, na qual $\phi_d(x)$ é o d-ésimo polinômio ciclotômico. Como

$$\frac{x^{2^k m}-1}{x^{2^k}-1} = x^{2^k(m-1)} + x^{2^k(m-2)} + \ldots + x^{2^k} + 1,$$

segue que

$$(x^{2^k}-1)(x^{2^k(m-1)} + x^{2^k(m-2)} + \ldots + x^{2^k} + 1) = \prod_{h|d} \phi_h(x),$$

e de modo análogo ao Lema 3.2.2, temos que $mdc(x^{2^k}-1, \phi_d(x)) = 1$. Pelo Lema de Gauss, existe $c(x) \in \mathbb{Z}[x]$ tal que

$$x^{2^k(m-1)} + x^{2^k(m-2)} + \ldots + x^{2^k} + 1 = c(x)\phi_d(x). \tag{3.10}$$

Tomando $x = -1$ na Equação (3.10) e usando o fato que $2^k(m-i)$, para todo $i = 1, 2, \ldots, m$ são potências pares, temos que $c(-1)\phi_d(-1) = m$. Assim, $N(1+\xi_n^j) = (-1)^{\varphi(n)} m^{\frac{\varphi(n)}{\varphi(d)}} = m^{\frac{\varphi(n)}{\varphi(d)}}$, para $1 \leq j < \frac{n}{2}$. Como $m \mid n$, segue que $N(1+\xi_n^j) = m^{\frac{\varphi(n)}{\varphi(d)}}$, para $1 \leq j < \frac{n}{2}$ divide $n^{\frac{\varphi(n)}{\varphi(d)}}$. Agora, se $x = 1$ na Equação (3.10), então $c(1)\phi_d(1) = m$. De modo análogo, $N(1-\xi_n^j) = m^{\frac{\varphi(n)}{\varphi(d)}}$ divide $n^{\frac{\varphi(n)}{\varphi(d)}}$, para $1 \leq j \leq \frac{n}{2}$. Finalmente, se $p = nk+1$ divide $N(1 \pm \xi_n^j)$, então p divide $n^{\frac{\varphi(n)}{\varphi(d)}}$ e portanto, $p \mid n$ o que é um absurdo, uma vez que neste caso p dividiria 1, o que conclui a demonstração. ∎

Lema 3.2.4. *([9], p. 109) Sejam n um número par, p um número primo ímpar e $d = \frac{n}{mdc(n,j)}$, para $j = 1, 2, \ldots, n$. Se ξ_n^j, para $j = 1, 2, \ldots, \frac{n}{2}$ é uma raiz d-ésima primitiva da unidade, em que d é um número ímpar, então $N(1+\xi_n^j)$, para $1 \leq j < \frac{n}{2}$ e $N(1-\xi_n^j)$, para $1 \leq j \leq \frac{n}{2}$, não possuem p como um divisor.*

Demonstração: Denotando ξ_n^j por ϵ_d, temos de modo análogo ao Lema 3.2.1 que

$$N(1+\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1+\xi_n^j) = [(-1)^{\varphi(d)}\phi_d(-1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.11}$$

para $1 \leq j < \frac{n}{2}$ e

$$N(1-\xi_n^j) = N_{\mathbb{Q}(\xi_n)|\mathbb{Q}}(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}, \tag{3.12}$$

para $1 \leq j \leq \frac{n}{2}$, na qual $\phi_d(x)$ é o d-ésimo polinômio ciclotômico. Pelo Lema de Gauss, existe $a(x) \in \mathbb{Z}[x]$ tal que

$$x^{d-1} + x^{d-2} + \ldots + x + 1 = a(x)\phi_d(x). \tag{3.13}$$

Tomando $x = -1$ na Equação (3.13) e como d ímpar, segue que $a(-1)\phi_d(-1) = 1$ e portanto, $\phi_d(-1) = \pm 1$. Se $\phi_d(-1) = \pm 1$, então pela Equação (3.11), tem-se que $N(1+\xi_n^j) = \pm 1$, para $1 \leq j < \frac{n}{2}$. Portanto, $N(1+\xi_n^j)$, para $1 \leq j < \frac{n}{2}$, não possui um divisor primo p. Agora, tomando $x = 1$ na Equação (3.13), temos que $a(1)\phi_d(1) = d$. Assim, pela Equação (3.12), tem-se que $N(1-\xi_n^j) = [\phi_d(1)]^{\frac{\varphi(n)}{\varphi(d)}}$, para $1 \leq j \leq \frac{n}{2}$ é um divisor de $d^{\frac{\varphi(n)}{\varphi(d)}}$. Se $p = nk+1$ é um divisor de $N(1-\xi_n^j)$, para $1 \leq j \leq \frac{n}{2}$, então p divide d. Logo, p divide n e portanto, p divide 1, o que é um absurdo, o que completa a demonstração. ∎

Proposição 3.2.5. *([9], p. 109) Sejam p um número primo ímpar, n um número par e α um elemento em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk+1$. Se α é irredutível, então quaisquer dois elementos distintos do conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ estão em classes laterais distintas módulo o ideal $\langle\alpha\rangle$.*

Demonstração: Se $(\xi_n)^h$ e $(\xi_n)^k$ estão na mesma classe lateral módulo o ideal $\langle\alpha\rangle$, na qual $1 \leq h < k \leq n$, então $\overline{(\xi_n)^h} = \overline{(\xi_n)^k}$ se, e somente se, $(\xi_n)^h + \langle\alpha\rangle = (\xi_n)^k + \langle\alpha\rangle$

se, e somente se, $(\xi_n)^h - (\xi_n)^k \in \langle\alpha\rangle$. Logo, para algum $\beta \in \mathbb{Z}[\xi_n]$, tem-se que $(\xi_n)^h - (\xi_n)^k = \alpha\beta$. Calculando a norma, temos que

$$N((\xi_n)^h - (\xi_n)^k) = N(1 - (\xi_n)^{k-h}) = N(\alpha)N(\beta) = pN(\beta).$$

Tomando $j = h - k$ temos que $1 \leq j < n$ e assim,

$$\begin{cases} N(1 + \xi_n^j) = pN(\beta) \text{ para } \quad 1 \leq j < \frac{n}{2} \\ N(1 - \xi_n^j) = pN(\beta) \text{ para } \quad 1 \leq j \leq \frac{n}{2}. \end{cases} \tag{3.14}$$

Vamos provar que isto é uma contradição. Se ξ_n^j a raiz $d = \dfrac{n}{mdc(n,j)}$-ésima primitiva da unidade, para j e n fixos, então $d \neq 1$, uma vez que $mdc(j,n) \leq j < n$. Assim,

1. Se d é par, temos que

   - se $d = 2$, então $mdc(n,j) = \frac{n}{2}$. Assim, $j = \frac{n}{2}$. Pela Equação (3.14), tem-se que $N(1 - \xi_n^j) = N(1 - \xi_n^{\frac{n}{2}}) = N(1 - (\xi_n^n)^{\frac{1}{2}}) = N(-1 - (-1)) = N(2) = 2^{\varphi(n)}$. Como $pN(\beta) = N(1 - \xi_n^j) = 2^{\varphi(n)}$, segue que $p \mid 2^{\varphi(n)}$ e portanto, $p \mid 2$ o que é um absurdo, uma vez que p é um número primo ímpar.

   - se $d = 2^k$, para $k \geq 2$, então pelo Lema 3.2.2 temos que, $N(1 + \xi_n^j)$ e $N(1 - \xi_n^j)$ não possuem p como divisor.

   - se $d = 2^k m$, para $k \geq 1$ e $mdc(2,m) = 1$, então pelo Lema 3.2.3, temos que $N(1 + \xi_n^j)$ e $N(1 - \xi_n^j)$ não possuem p como divisor.

2. Se d é ímpar, então pelo Lema 3.2.4 temos que $N(1 + \xi_n^j)$ e $N(1 - \xi_n^j)$ não possuem p como um divisor.

Portanto, quaisquer dois elementos distintos do conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ estão em classes laterais distintas módulo o ideal $\langle\alpha\rangle$. ■

Teorema 3.2.4. *([9], p. 110) Sejam p um número primo ímpar e $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$.*

1. *Se n é ímpar, então o grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ contém um único subgrupo cíclico com $2n$ elementos.*

2. *Se n é par, então o grupo multiplicativo do corpo $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ contém um único subgrupo cíclico com n elementos.*

Demonstração: Se p é um número primo ímpar e $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$, então pelo Corolário 1.7.2, segue que $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ é um corpo com $p^{\varphi(n)}$ elementos, uma vez que $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ é isomorfo a $GF(p^{\varphi(n)})$. Assim, o grupo cíclico multiplicativo G do corpo $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ tem $p^{\varphi(n)} - 1$ elementos.

1. Se n é ímpar, então pela Proposição 3.2.2, temos que existe um único subgrupo cíclico do grupo multiplicativo G com $2n$ elementos.

2. Se n é par, então pela Proposição 3.2.3, temos que existe um único subgrupo cíclico do grupo multiplicativo G com n elementos. ■

Lema 3.2.5. *([9], p. 110) Sejam p um número primo ímpar, n um número ímpar e $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$. Se ξ_n^j é uma raiz n-ésima primitiva da unidade, então*

$$N(1-\xi_n^j) = 2^{\varphi(n)} sen^2(\frac{\pi j j_1}{n}) \dots sen^2(\frac{\pi j j_{\varphi(n)}}{n}),$$

para $1 \leq j < 2n$.

Demonstração: Seja $\sigma_i \in Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$ definido por $\sigma_i(\xi_n^j) = (\xi_n^j)^{j_i}$, para $i = 1, 2, \dots, \varphi(n)$, pela demonstração do Lema 1.7.1, podemos expressar $N(1-\xi_n^j)$ como um produto de $\frac{\varphi(n)}{2}$ números complexos e seus conjugados, ou seja,

$$\begin{aligned} N(1-\xi_n^j) &= (1-\sigma_1(\xi_n^j))(1-\overline{\sigma_1(\xi_n^j)}) \dots (1-\sigma_{\frac{\varphi(n)}{2}}(\xi_n^j))(1-\overline{\sigma_{\frac{\varphi(n)}{2}}(\xi_n^j)}) \\ &= (1-\xi_n^{jj_1})(1-\overline{\xi_n^{jj_1}}) \dots (1-\xi_n^{jj_{\frac{\varphi(n)}{2}}})(1-\overline{\xi_n^{jj_{\frac{\varphi(n)}{2}}}}), \end{aligned} \tag{3.15}$$

na qual $1 \leq j_1, \dots, j_{\frac{\varphi(n)}{2}} < n$, $mdc(j_1, n) = \dots mdc(j_{\frac{\varphi(n)}{2}}, n) = 1$ e $j_1, \dots, j_{\frac{\varphi(n)}{2}}$ são dois a dois distintos. Por outro lado, para $1 \leq m \leq \frac{\varphi(n)}{2}$, temos que

$$\begin{aligned} (1-\xi_n^{jj_m})(\overline{1-\xi_n^{jj_m}}) &= (1-\xi_n^{jj_m})(1-\overline{\xi_n^{jj_m}}) \\ &= 1 - 2\cos(\tfrac{2\pi jj_m}{n}) + \cos^2(\tfrac{2\pi jj_m}{n}) + \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}) \\ &= (1-\cos(\tfrac{2\pi jj_m}{n}))^2 + \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}). \end{aligned} \tag{3.16}$$

Como

$$\begin{aligned}\cos(\tfrac{2\pi jj_m}{n}) &= \cos(\tfrac{\pi jj_m}{n}+\tfrac{\pi jj_m}{n})\\ &= \cos^2(\tfrac{\pi jj_m}{n})-\operatorname{sen}^2(\tfrac{2\pi jj_m}{n})\\ &= (1-\operatorname{sen}^2(\tfrac{\pi jj_m}{n}))-\operatorname{sen}^2(\tfrac{\pi jj_m}{n}) = 1-2\operatorname{sen}^2(\tfrac{\pi jj_m}{n})\end{aligned}$$

e

$$\operatorname{sen}(\frac{2\pi jj_m}{n}) = \operatorname{sen}(\frac{\pi jj_m}{n}+\frac{\pi jj_m}{n}) = 2\cos(\frac{\pi jj_m}{n})\operatorname{sen}(\frac{\pi jj_m}{n}),$$

segue que $\operatorname{sen}^2(\frac{2\pi jj_m}{n}) = 2^2\cos^2(\frac{\pi jj_m}{n})\operatorname{sen}^2(\frac{\pi jj_m}{n})$. Assim, substituindo na equação (3.16), tem-se que

$$\begin{aligned}(1-\xi_n^{jj_m})(1-\overline{\xi_n^{jj_m}}) &= (1-\cos(\tfrac{2\pi jj_m}{n}))^2+\operatorname{sen}^2(\tfrac{2\pi jj_m}{n})\\ &= (1-(1-2\operatorname{sen}^2(\tfrac{\pi jj_m}{n})))^2+2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n})\\ &= (2\operatorname{sen}^2(\tfrac{\pi jj_m}{n}))^2+2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n})\\ &= 2^2\operatorname{sen}^4(\tfrac{\pi jj_m}{n})+2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n})\\ &= 2^2\operatorname{sen}^2(\tfrac{\pi jj_m}{n})(\operatorname{sen}^2(\tfrac{\pi jj_m}{n})+\cos^2(\tfrac{\pi jj_m}{n}))\\ &= 2^2\operatorname{sen}^2(\tfrac{\pi jj_m}{n}).\end{aligned}$$

Finalmente, pela Equação (3.15), temos que

$$\begin{aligned}N(1-\xi_n^j) &= \underbrace{2^2\operatorname{sen}^2(\frac{\pi jj_1}{n})\ldots 2^2\operatorname{sen}^2(\frac{\pi jj_{\frac{\varphi(n)}{2}}}{n})}_{\frac{\varphi(n)}{2}\text{ vezes}}\\ &= (2^2)^{\frac{\varphi(n)}{2}}\operatorname{sen}^2(\tfrac{\pi jj_1}{n})\ldots\operatorname{sen}^2(\tfrac{\pi jj_{\frac{\varphi(n)}{2}}}{n})\\ &= 2^{\varphi(n)}sen^2(\tfrac{\pi jj_1}{n})\ldots\operatorname{sen}^2(\tfrac{\pi jj_{\frac{\varphi(n)}{2}}}{n}).\ \blacksquare\end{aligned}$$

Lema 3.2.6. *([9], p. 110) Sejam p um número primo ímpar, n um número ímpar e $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1\ (mod\ n)$. Se ξ_n^j é uma raiz n-ésima primitiva da unidade, então*

$$N(1+\xi_n^j) = 2^{\varphi(n)}\cos^2(\frac{\pi jj_1}{n})\ldots\cos^2(\frac{\pi jj_{\varphi(n)}}{n}),$$

para $1 \le j < 2n$.

Demonstração: Analogamente ao Lema 3.2.5 tem-se que

$$\begin{aligned}N(1+\xi_n^j) &= (1+\sigma_1(\xi_n^j))(1+\overline{\sigma_1(\xi_n^j)})\ldots(1+\sigma_{\frac{\varphi(n)}{2}}(\xi_n^j))(1+\overline{\sigma_{\frac{\varphi(n)}{2}}(\xi_n^j)})\\ &= (1+\xi_n^{jj_1})(1+\overline{\xi_n^{jj_1}})\ldots(1+\xi_n^{jj_{\frac{\varphi(n)}{2}}})(1+\overline{\xi_n^{jj_{\frac{\varphi(n)}{2}}}}),\end{aligned} \tag{3.17}$$

na qual $1 \leq j_1, \ldots, j_{\frac{\varphi(n)}{2}} < n$, $mdc(j_1, n) = \ldots mdc(j_{\frac{\varphi(n)}{2}}, n) = 1$ e $j_1, \ldots, j_{\frac{\varphi(n)}{2}}$ são dois a dois distintos. Por outro lado, para $1 \leq m \leq \frac{\varphi(n)}{2}$, temos que

$$\begin{aligned}(1+\xi_n^{jj_m})(\overline{1+\xi_n^{jj_m}}) &= (1+\xi_n^{jj_m})(1+\overline{\xi_n^{jj_m}}) \\ &= 1 + 2\cos(\tfrac{2\pi jj_m}{n}) + \cos^2(\tfrac{2\pi jj_m}{n}) + \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}) \\ &= (1+\cos(\tfrac{2\pi jj_m}{n}))^2 + \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}).\end{aligned} \tag{3.18}$$

Como

$$\begin{aligned}\cos(\tfrac{2\pi jj_m}{n}) &= \cos(\tfrac{\pi jj_m}{n} + \tfrac{\pi jj_m}{n}) \\ &= \cos^2(\tfrac{\pi jj_m}{n}) - \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}) \\ &= \cos^2(\tfrac{\pi jj_m}{n}) - (1-\cos^2(\tfrac{\pi jj_m}{n})) = -1 + 2\cos^2(\tfrac{\pi jj_m}{n})\end{aligned}$$

e

$$\operatorname{sen}(\frac{2\pi jj_m}{n}) = \operatorname{sen}(\frac{\pi jj_m}{n} + \frac{\pi jj_m}{n}) = 2\cos(\frac{\pi jj_m}{n})\operatorname{sen}(\frac{\pi jj_m}{n}),$$

segue que $\operatorname{sen}^2(\frac{2\pi jj_m}{n}) = 2^2\cos^2(\frac{\pi jj_m}{n})\operatorname{sen}^2(\frac{\pi jj_m}{n})$. Assim, substituindo na Equação (3.18), tem-se que

$$\begin{aligned}(1+\xi_n^{jj_m})(1+\overline{\xi_n^{jj_m}}) &= (1+\cos(\tfrac{2\pi jj_m}{n}))^2 + \operatorname{sen}^2(\tfrac{2\pi jj_m}{n}) \\ &= (1+(-1+2\cos^2(\tfrac{\pi jj_m}{n})))^2 + 2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n}) \\ &= (2\cos^2(\tfrac{\pi jj_m}{n}))^2 + 2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n}) \\ &= 2^2\cos^4(\tfrac{\pi jj_m}{n}) + 2^2\cos^2(\tfrac{\pi jj_m}{n})\operatorname{sen}^2(\tfrac{\pi jj_m}{n}) \\ &= 2^2\cos^2(\tfrac{\pi jj_m}{n})(\cos^2(\tfrac{\pi jj_m}{n}) + \operatorname{sen}^2(\tfrac{\pi jj_m}{n})) = 2^2\cos^2(\tfrac{\pi jj_m}{n}).\end{aligned}$$

Finalmente, pela Equação (3.17), temos que

$$\begin{aligned}N(1+\xi_n^j) &= \underbrace{2^2\cos^2(\frac{\pi jj_1}{n})\ldots 2^2\cos^2(\frac{\pi jj_{\frac{\varphi(n)}{2}}}{n})}_{\frac{\varphi(n)}{2}\text{ vezes}} \\ &= (2^2)^{\frac{\varphi(n)}{2}}\cos^2(\tfrac{\pi jj_1}{n})\ldots\cos^2(\tfrac{\pi jj_{\frac{\varphi(n)}{2}}}{n}) \\ &= 2^{\varphi(n)}\cos^2(\tfrac{\pi jj_1}{n})\ldots\cos^2(\tfrac{\pi jj_{\frac{\varphi(n)}{2}}}{n}). \ \blacksquare\end{aligned}$$

Proposição 3.2.6. *([9], p. 110) Sejam p um número primo ímpar e n um número ímpar. Se $\varphi(n)$ é o menor inteiro positivio tal que $p^{\varphi(n)} \equiv 1\ (mod\ n)$, então quaisquer dois elementos distintos do conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ estão em classes laterais distintas módulo o ideal $\langle p\rangle$ em $\mathbb{Z}[\xi_n]$.*

Demonstração: Se $(-\xi_n)^h$ e $(-\xi_n)^k$ estão na mesma classe lateral módulo o ideal $\langle p\rangle$, na qual $1 \leq h < k \leq 2n$, então $\overline{(-\xi_n)^h} = \overline{(-\xi_n)^k}$ se, e somente se, $(-\xi_n)^h + \langle p\rangle = (-\xi_n)^k + \langle p\rangle$ se, e somente se, $(-\xi_n)^h - (-\xi_n)^k \in \langle p\rangle$. Logo, para algum $\beta \in \mathbb{Z}[\xi_n]$, temos que $(-\xi_n)^h - (-\xi_n)^k = p\beta$. Calculando a norma, obtemos que

$$N((-\xi_n)^h - (-\xi_n)^k) = N(1 - (-\xi_n)^{k-h}) = N(p)N(\beta) = p^{\varphi(n)}N(\beta).$$

Tomando $j = k - h$ tem-se que $1 \leq j < 2n$ e deste modo,

$$N(1 - \xi_n^j) = p^{\varphi(n)}N(\beta) \text{ se } 1 \leq j < n. \tag{3.19}$$

Vamos provar que isto é uma contradição. Pelo Lema 3.2.5, temos que

$$N(1 - \xi_n^j) = 2^{\varphi(n)}\text{sen}^2(\frac{\pi j j_1}{n}) \ldots \text{sen}^2(\frac{\pi j j_{\varphi(n)}}{n}). \tag{3.20}$$

Substituindo (3.20) na Equação (3.19), tem-se que

$$p^{\varphi(n)}N(\beta) = 2^{\varphi(n)}\text{sen}^2(\frac{\pi j j_1}{n}) \ldots \text{sen}^2(\frac{\pi j j_{\varphi(n)}}{n}) \leq 2^{\varphi(n)}.$$

Isto implica que, $p^{\varphi(n)}N(\beta) \leq 2^{\varphi(n)}$, uma vez que a função seno é limitada, mas isto é uma contradição, pois $2^{\varphi(n)} \leq p^{\varphi(n)}N(\beta)$. Portanto, $(-\xi_n)^h$ e $(-\xi_n)^k$, na qual $1 \leq h < k \leq 2n$, estão em classes laterais distintas módulo o ideal $p\mathbb{Z}[\xi_n]$. De modo análogo, temos que $(-\xi_n)^h$ e ξ_n^k, ξ_n^h e $(-\xi_n)^k$, em que $1 \leq h < k \leq 2n$, estão em classes laterais distintas módulo o ideal $p\mathbb{Z}[\xi_n]$. ∎

Teorema 3.2.5. *([9], p. 110) Sejam p um número primo ímpar e $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1\ (mod\ n)$. Se n é ímpar, então $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ pode ser tomado como sendo um conjunto completo das classes laterais do subgrupo cíclico com $2n$ elementos do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$.*

Demonstração: Pela Proposição 3.2.6, temos que quaisquer dois elementos distintos do conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$, estão em classes laterais distintas módulo o ideal $\langle p\rangle$ em $\mathbb{Z}[\xi_n]$. Como $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ é um subgrupo cíclico com $2n$ elementos gerado por $-\xi_n$ e é único pelo Teorema 3.2.2, segue que podemos tomar o conjunto $\{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$, como sendo um conjunto completo das classes laterais do subgrupo cíclico com $2n$ elementos do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$. ∎

Observação 3.2.3. *Se n for par, os Lemas 3.2.5, 3.2.6 e a Proposição 3.2.6 também são válidas, com a ressalva de que j varia de* 1 *a n, para* $N(1 \pm \xi_n^j)$*, onde* ξ_n^j *é uma raiz n-ésima primitiva da unidade.*

Teorema 3.2.6. *([9], p. 110) Sejam p um número primo ímpar e* $\varphi(n)$ *o menor inteiro positivo tal que* $p^{\varphi(n)} \equiv 1 \ (mod\ n)$*. Se n é par, então podemos tomar o conjunto* $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ *como sendo o conjunto completo das classes laterais do subgrupo cíclico com n elementos do grupo multiplicativo do corpo* $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$.

Demonstração: Pela Observação 3.2.3, tem-se que a Proposição 3.2.6 vale para n par. Assim, quaisquer dois elementos distintos no conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ estão em classes laterais distintas módulo o ideal $\langle p \rangle$ em $\mathbb{Z}[\xi_n]$. Como o conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ é um subgrupo cíclico com n elementos gerado por ξ_n e é único pelo Teorema 3.2.2, segue que podemos tomar o conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$, como sendo um conjunto completo das classes laterais do subgrupo cíclico com n elementos do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$. ■

Teorema 3.2.7. *([9], p. 110) Se* $\varphi(n)$ *é o menor inteiro positivo tal que* $2^{\varphi(n)} \equiv 1$ $(mod\ n)$*, então o grupo multiplicativo do corpo* $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ *possui um único subgrupo cíclico com n elementos. Além disso, o conjunto* $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$ *é um conjunto completo das classes laterais do subgrupo cíclico do grupo multiplicativo do corpo* $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$.

Demonstração: Se $\varphi(n)$ é o menor inteiro positivo tal que $2^{\varphi(n)} \equiv 1 \ (mod\ n)$, então pelo Corolário 1.7.2, temos que $2\mathbb{Z}[\xi_n]$ é um ideal primo de $\mathbb{Z}[\xi_n]$. Como $\mathbb{Z}[\xi_n]$ é um domínio de ideais principais, segue que $2\mathbb{Z}[\xi_n]$ é um ideal maximal. Logo, $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ é um corpo com $2^{\varphi(n)}$ elementos, uma vez que $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ é isomorfo a $GF(2^{\varphi(n)})$. Assim, o grupo cíclico multiplicativo G do corpo $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ tem $2^{\varphi(n)} - 1$ elementos. Pela Proposição 3.2.3, existe um único subgrupo cíclico com n elementos do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$. Se ξ_n^h e ξ_n^k estão na mesma classe lateral módulo o ideal $\langle 2 \rangle$, onde $1 \leq h < k \leq n$, então $\overline{\xi_n^h} = \overline{\xi_n^k}$ se, e somente se, $\xi_n^h + \langle 2 \rangle = \xi_n^k + \langle 2 \rangle$ se, e somente se, $\xi_n^h - \xi_n^k \in \langle 2 \rangle$. Logo, para algum $\beta \in \mathbb{Z}[[\xi_n]$, tem-se que $\xi_n^h - \xi_n^k = 2\beta$.

Calculando a norma, temos que

$$N(\xi_n^h - \xi_n^k) = N(1 - (\xi_n)^{k-h}) = N(2)N(\beta) = 2^{\varphi(n)}N(\beta).$$

Tomando $j = k - h$, temos que $1 \leq j < n$ e deste modo,

$$N(1 - \xi_n^j) = 2^{\varphi(n)}N(\beta). \tag{3.21}$$

Pelo Lema 3.2.5, tem-se que

$$N(1 - \xi_n^j) = 2^{\varphi(n)}\text{sen}^2(\frac{\pi jj_1}{n}) \dots \text{sen}^2(\frac{\pi jj_{\varphi(n)}}{n}).$$

Substituindo na Equação (3.21), temos que $2^{\varphi(n)}N(\beta) = 2^{\varphi(n)}\text{sen}^2(\frac{\pi jj_1}{n}) \dots \text{sen}^2(\frac{\pi jj_{\varphi(n)}}{n})$. Logo, $N(\beta) = \text{sen}^2(\frac{\pi jj_1}{n}) \dots \text{sen}^2(\frac{\pi jj_{\varphi(n)}}{n})$. Como a função seno é limitada, segue pelo Lema 1.7.1 que $N(\beta) = 1$, ou seja, $\text{sen}^2(\frac{\pi jj_1}{n}) \dots \text{sen}^2(\frac{\pi jj_{\varphi(n)}}{n}) = 1$. Assim, $\frac{\pi jj_m}{n} = \frac{\pi}{2} + l_m\pi$, onde $l_m \in \mathbb{Z}$, para $1 \leq m \leq \frac{\varphi(n)}{2}$. Logo n é um número par, uma vez que se n fosse ímpar, então $\frac{\pi jj_m}{2k+1} = \frac{\pi}{2} + l_m\pi$, ou seja, $jj_m = (2k+1)(\frac{1}{2} + l_m) = l_m(2k+1) + k + \frac{1}{2} \in \mathbb{Q}$, e isto implica que $jj_m \in \mathbb{Q}$, o que é um absurdo pois $jj_m \in \mathbb{Z}$. Como $2^{\varphi(n)} \equiv 1 \ (mod\ n)$, segue que $n \mid 2^{\varphi(n)} - 1$, isto é, $2^{\varphi(n)} - 1 = nk$, para algum k. Do fato de n ser par, tem-se que $2 \mid 2^{\varphi(n)} - 1$ e como $2 \mid 2^{\varphi(n)}$, segue que 2 divide a diferença, ou seja, $2 \mid 1$, o que é um absurdo. Dessa forma, 2 não divide $N(1 - \xi_n^j)$. Logo, quaisquer dois elementos distintos estão em classes laterais distintas. Portanto, $\langle \xi_n \rangle = \{1, \xi_n, \dots, \xi_n^{n-1}\}$ é um conjunto completo das classes laterais do subgrupo cíclico do grupo multiplicativo do corpo $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$. ■

3.3 Distância de Mannheim

Nesta seção, veremos o conceito da distância de Mannheim e do peso de Mannheim via corpos ciclotômicos, na qual observamos que existe uma sutil diferença da distância de Mannheim via corpos quadráticos e estudamos algumas propriedades dessa distância.

Definição 3.3.1. *Seja G um grupo abeliano. Uma função $w : G \to \mathbb{R}$ é chamada uma função peso se:*

1. $w(g) \geq 0$, *para todo* $g \in G$.

2. $w(g) = 0$ *se, e somente se,* $g = 0$.

3. $w(g) = w(-g)$, *para todo* $g \in G$.

4. $w(g+h) \leq w(g) + w(h)$, *para todo* $g, h \in G$.

A função peso pode ser estendida a n cópias do grupo G como

$$w(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} w(a_i),$$

em que $(a_1, a_2, \ldots, a_n) \in G^n$.

Uma função peso w sobre G induz uma distância $d : G \times G \to \mathbb{R}$ definida por $d(g,h) = w(g-h)$, na qual $g, h \in G$ satisfazendo as seguintes propriedades:

1. $d(g,h) \geq 0$, para todo $g, h \in G$.

2. $d(g,h) = 0$ se, e somente se, $g = h$, para todo $g, h \in G$.

3. $d(g,h) = d(h,g)$, para todo $g, h \in G$.

4. $d(g,h) \leq d(g,k) + d(k,h)$, para todo $g, h, k \in G$.

A função distância pode ser estendida a n cópias do grupo G como

$$d((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)) = \sum_{i=1}^{n} w(a_i - b_i),$$

em que $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ são elementos de G^n.

Definição 3.3.2. *Definimos o peso de Manhattan de um elemento* $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i \in \mathbb{Z}[\xi_n]$, *como* $w_{\mathcal{M}}(\alpha) = \sum_{i=0}^{\varphi(n)-1} |a_i|$. *Além disso, se* $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i$ *e* $\beta = \sum_{i=0}^{\varphi(n)-1} b_i \xi_n^i$ *são elementos de* $\mathbb{Z}[\xi_n]$. *Definimos a distância de Manhattan entre os elementos* α *e* β *como* $d_{\mathcal{M}}(\alpha, \beta) = \sum_{i=0}^{\varphi(n)-1} w_{\mathcal{M}}(a_i - b_i) = \sum_{i=0}^{\varphi(n)-1} |a_i - b_i|$.

Observação 3.3.1. *Notemos que, a distância de Manhattan definida via corpos ciclotômicos é igual a distância de Mannheim via corpos quadráticos.*

Seja $GF(p^h)$ um corpo finito onde p é um número primo e h um inteiro positivo. Como $o(GF(p^h)^*) = p^h - 1$, segue que para todo divisor m de $p^h - 1$ existem $\varphi(m)$ raízes m-ésimas primitivas da unidade em $GF(p^h)^*$.

Definição 3.3.3. *Sejam p um número primo e m um inteiro positivo. Dizemos que a ordem de p módulo m é n se $p^n \equiv 1 \ (mod\ m)$ e $p^k \not\equiv 1 \ (mod\ m)$, para todo $k = 1, 2, \ldots, n-1$.*

Observação 3.3.2. *Sejam m, n números inteiros positivos e p um número primo ímpar.*

1. *$m \mid n$ se, e somente se, $p^m - 1 \mid p^n - 1$.*

2. *A ordem de p módulo m é h se, e somente se, $GF(p^h) = \mathbb{Z}_p(\xi_m)$.*

Seja $\mathbb{Z}_p(\xi_m)$, na qual ξ_m é uma raiz m-ésima primitiva da unidade. Seja $n = p^e m$, em que $e \geq 0$ é um inteiro. Seja ξ_n uma raiz n-ésima primitiva sobre $\mathbb{Q}$. Pela Observação 1.7.1, temos que o anel de inteiros de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$ e $\{1, \xi_n, \ldots, \xi_n^{\varphi(n)-1}\}$ é uma base de $\mathbb{Z}[\xi_n]$ sobre $\mathbb{Z}$. Assim,

$$\mathbb{Z}[\xi_n] = \{ \sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i : a_i \in \mathbb{Z}\}$$

e portanto, $\mathbb{Z}[\xi_n]$ está em bijeção com $\mathbb{Z}^{\varphi(n)}$, na qual $\sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i \leftrightarrow (a_0, a_1, \ldots, a_{\varphi(n)-1})$. Pelo Teorema 1.5.2, temos que $p\mathbb{Z}[\xi_n] = (\mathcal{I}_1 \ldots \mathcal{I}_r)^{\varphi(e)}$, em que $\mathcal{I}_i \subseteq \mathbb{Z}[\xi_n]$ são ideais primos tais que $\mathcal{I}_i \cap \mathbb{Z} = \langle p \rangle$, para $i = 1, 2, \ldots, r$ e $\varphi(m) = hr$. Além disso, $\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{I}_i}$ é isomorfo a $\mathbb{Z}_p(\xi_m)$, na qual o isomorfismo envia ξ_n em $\bar{\xi_n} = \xi_m$. Deste modo, os elementos de $\mathbb{Z}_p(\xi_m)$ são classes laterais do tipo $\alpha + \mathcal{I}_i$, para $i = 1, 2, \ldots, r$, em que $\alpha \in \mathbb{Z}[\xi_n]$.

Se $\mathcal{I} \subset \mathbb{Z}[\xi_n]$ é um ideal primo tal que $\mathcal{I} \cap \mathbb{Z} = \langle p \rangle$, então $\mathbb{Z}_p(\xi_m)$ é isomorfo a $\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{I}}$ e portanto, todo elemento $\alpha + \mathcal{I} \subseteq \mathbb{Z}[\xi_n]$ estão em correspondência um a um com os elementos $\bar{\alpha} \in \mathbb{Z}_p(\xi_m)$.

Seja a aplicação $\bar{w}_{\bar{\mathcal{M}}} : \mathbb{Z}_p(\xi_m) \to \mathbb{Z}$ definida por $\bar{w}_{\bar{\mathcal{M}}}(\bar{\alpha}) = min_{x\in\alpha+\mathcal{I}} w_{\mathcal{M}}(x)$. Agora, para cada $\bar{\alpha} \in \mathbb{Z}_p(\xi_m)$ seja $\alpha \in \mathbb{Z}[\xi_n]$ tal que $w_{\mathcal{M}}(\alpha) = w_{\bar{\mathcal{M}}}(\bar{\alpha})$. Observamos que o elemento α, em geral, não é único. Mas, se $n = 4$ e p for ímpar temos a unicidade. Deste modo, acabamos de provar a seguinte proposição.

Proposição 3.3.1. *([7], p. 4) Existe um subconjunto $R \subseteq \mathbb{Z}[\xi_n]$, formado pelo representante das classes laterais tal que*

1. *$\mathbb{Z}[\xi_n] = \cup_{\alpha\in R}(\alpha + I)$ e a união é disjunta.*
2. *Para todo $\alpha \in R$ tem-se que $w_{\bar{\mathcal{M}}}(\bar{\alpha}) = w_{\mathcal{M}}(\alpha) \leq w_{\mathcal{M}}(x)$, para qualquer $x \in \alpha + \mathcal{I}$.*

Proposição 3.3.2. *([7], p. 5) A aplicação $w_{\bar{\mathcal{M}}}(\bar{\alpha}) = min_{x\in\alpha+\mathcal{I}} w_{\mathcal{M}}(x)$ é uma função peso sobre corpo finito $\mathbb{Z}_p(\xi_m)$.*

Demonstração:

1. Temos que $w_{\bar{\mathcal{M}}}(\bar{\alpha}) \geq 0$, uma vez que $w_{\mathcal{M}}(x) \geq 0$, para todo $x \in \alpha+\mathcal{I} \subset \mathbb{Z}[\xi_n]$. Além disso, $\bar{w}_{\mathcal{M}}(\bar{\alpha}) = 0$ se, e somente se, $min_{x\in\alpha+\mathcal{I}} w_{\mathcal{M}}(x) = 0$ se, e somente se, $w_{\mathcal{M}}(x) = 0$, para algum x se, e somente se, $x = 0$, se e somente se, $\bar{\alpha} = \bar{0}$.

2. Se $\alpha+\mathcal{I}$ é uma classe lateral, então $-\alpha+\mathcal{I} = -(\alpha+\mathcal{I})$ é a classe lateral e assim, $-\bar{\alpha} = \overline{(-\alpha)}$. Logo $w_{\bar{\mathcal{M}}}(-\bar{\alpha}) = min_{x\in-\alpha+\mathcal{I}} w_{\mathcal{M}}(x) = min_{x\in\alpha+\mathcal{I}} w_{\mathcal{M}}(-x) = min_{x\in\alpha+\mathcal{I}} w_{\mathcal{M}}(x) = w_{\bar{\mathcal{M}}}(\bar{\alpha})$.

3. Sejam R como na Proposição 3.3.1 e $a, b \in R$. Se $a + b \in R$, então pela desigualdade triangular do peso de Manhattan $w_{\mathcal{M}}(-)$ em $\mathbb{Z}[\xi_n]$, tem-se que

   $$w_{\bar{\mathcal{M}}}(\bar{a} + \bar{b}) = w_{\mathcal{M}}(\overline{a + b}) = w_{\mathcal{M}}(a + b) \leq w_{\mathcal{M}}(a) + w_{\mathcal{M}}(b) = w_{\bar{\mathcal{M}}}(\bar{a}) + w_{\bar{\mathcal{M}}}(\bar{b}).$$

   Se $a+b \notin R$, então existe $c \in R$ tal que $\bar{a}+\bar{b} = \bar{c}$, isto é, $(a+b)+\mathcal{I} = c+\mathcal{I}$. Logo $w_{\mathcal{M}}(c) \leq w_{\mathcal{M}}(a + b)$. Portanto, $w_{\bar{\mathcal{M}}}(\bar{a} + \bar{b}) = w_{\bar{\mathcal{M}}}(\bar{c}) = w_{\mathcal{M}}(c) \leq w_{\mathcal{M}}(a + b) \leq w_{\mathcal{M}}(a) + w_{\mathcal{M}}(b) = w_{\bar{\mathcal{M}}}(\bar{a}) + w_{\bar{\mathcal{M}}}(\bar{b})$. ∎

Definição 3.3.4. *O subconjunto R de $\mathbb{Z}[\xi_n]$ da Proposição 3.3.1 é chamado de sistema de representante do peso de Mannheim do corpo $\dfrac{\mathbb{Z}[\xi_n]}{\mathcal{I}} \simeq \mathbb{Z}_p(\xi_m)$.*

Definição 3.3.5. *O peso de Mannheim de um elemento $\bar{\alpha} \in \mathbb{Z}_p(\xi_m)$ é definido como*

$$w_{\bar{\mathcal{M}}}(\bar{\alpha}) = min_{x \in \alpha + \mathcal{I}} w_{\mathcal{M}}(x).$$

O peso de Mannheim de uma n-upla $\bar{\alpha} = (\bar{\alpha_1}, \ldots, \bar{\alpha_n})$ sobre $\mathbb{Z}_p(\xi_m)$ é definido como

$$w_{\bar{\mathcal{M}}}(\bar{\alpha}) = \sum_{i=1}^{n} w_{\bar{\mathcal{M}}}(\bar{\alpha_i}).$$

Definição 3.3.6. *Seja G um grupo abeliano. Uma função peso $w : G \to \mathbb{R}$ é chamada consecutiva se para todo $g \in G$ existe uma sequência $g_0 = 0, g_1, \ldots, g_{w(g)} = g \in G$ de elementos de G de comprimento $w(g)$ tal que $w(g_j - g_{j-1}) = 1$, para todo $j = 1, 2, \ldots, w(g)$.*

Proposição 3.3.3. *([7], p. 6) Sejam G um grupo abeliano, $w : G \to \mathbb{R}$ uma função peso e $g \in G$. Se existe uma sequência $g_0 = 0, g_1, \ldots, g_{w(g)} = g$ de elementos de G tal que $w(g_j - g_{j-1}) = 1$, para $j = 1, 2, \ldots, w(g)$, então $w(g_j) = j$, para $j = 1, \ldots, w(g) - 1$.*

Demonstração: Seja $g \in G$ tal que $w(g) > 0$. Pela desigualdade triangular, temos que

$$\begin{aligned} w(g_{w(g)-1}) &= w(g_1 - g_1 + g_2 - g_2 + \ldots + g_{w(g)-2} - g_{w(g)-2} + g_{w(g)-1}) \\ &\leq w(g_1) + w(g_2 - g_1) + \ldots + w(g_{w(g)-1} - g_{w(g)-2}) \\ &= \underbrace{1 + \ldots + 1}_{(w(g)-1) \text{ vezes}} = 1(w(g) - 1) = w(g) - 1, \end{aligned}$$

ou seja, $w(g_{w(g)-1}) \leq w(g) - 1$. Por outro lado, novamente pela desigualdade triangular, temos que $w(g) = w(g - g_{w(g)-1} + g_{w(g)-1}) \leq w(g - g_{w(g)-1}) + w(g_{w(g)-1}) \leq 1 + w(g) - 1 = w(g)$, e assim, $w(g_{w(g)-1}) = w(g) - 1$. Agora,

$$\begin{aligned} w(g_{w(g)-2}) &= w(g_1 - g_1 + g_2 - g_2 + \ldots + g_{d-3} - g_{w(g)-3} + g_{w(g)-2}) \\ &\leq w(g_1) + w(g_2 - g_1) + \ldots + w(g_{w(g)-2} - g_{w(g)-3}) \\ &= \underbrace{1 + \ldots + 1}_{(w(g)-2) \text{ vezes}} \\ &= 1(w(g) - 2) = w(g) - 2. \end{aligned}$$

Por outro lado, novamente pela desigualdade triangular, temos que

$$\begin{aligned} w(g)-1 &= w(g_{w(g)-1}) = w(g_{w(g)-1}+g_{w(g)-2}-g_{w(g)-2}) \\ &\leq w(g_{w(g)-1}-g_{w(g)-2})+w(g_{w(g)-2}) \\ &\leq 1+w(g)-2 = w(g)-1. \end{aligned}$$

Logo, $w(g_{w(g)-2}) = w(g)-2$. De modo análogo, $w(g_j) = j$, para $1 \leq j \leq w(g)-3$.■

Proposição 3.3.4. *([7], p. 6) Sejam G um grupo abeliano e $w : G \to \mathbb{R}$ uma função peso. Então, $w(-)$ é consecutiva se, e somente se, para todo $g \in G$ tal que $w(g) \geq 0$, existe um elemento $h \in G$ tal que $w(g-h) = 1$ e $w(h) = w(g)-1$.*

Demonstração: Suponhamos que $w(-)$ é consecutiva. Seja $g \in G$ tal que $w(g) > 0$. Como $w(-)$ é uma função consecutiva, segue que existe uma sequência $0 = g_0, g_1, \ldots, g_{w(g)} = g$ de elementos de G e de comprimento $w(g)$ tal que $w(g_j - g_{j-1}) = 1$ para $j = 1, \ldots, w(g)$. Pela Proposição 3.3.3, temos que $w(g_{w(g)-1}) = w(g)-1$. Tomando $h = g_{w(g)-1} \in G$ tem-se que $w(g-h) = 1$ e $w(h) = w(g_{w(g)-1}) = w(g)-1$. Reciprocamente, se $g \in G$ é tal que $w(g) = 1$, então existe $h = 0 \in G$ com $w(g-h) = 1$ e $w(h) = w(g)-1 = 0$. Neste caso, existe a sequência $g_0 = h = 0, g_1 = g$ tal que $w(g_1 - g_0) = w(g-h) = 1$. Se $g \in G$ com $w(g) = 2$, então existe $h \in G$ tal que $w(g-h) = 1$ e $w(h) = w(g)-1 = 1$. Neste caso, existe a sequência $g_0 = 0, g_1 = g-h, g_2 = g$ com $w(g_1 - g_0) = w(g_2 - g_1) = 1$. Por indução, suponhamos que o resultado é válido para $g \in G$ com $w(g) > 0$, ou seja, que existe uma sequência $g_0 = 0, g_1, \ldots, g_{w(g)} = g$ de elementos de G e de comprimento $w(g)$ tal que $w(g_j - g_{j-1}) = 1$, para $j = 1, \ldots, w(g)$. Agora, seja $\tilde{g} \in G$ com $w(\tilde{g}) = w(g)+1$. Por hipótese, existe $h \in G$ tal que $w(\tilde{g}-h) = 1$ e $w(h) = w(\tilde{g})-1 = w(g)$. Mas pela hipótese de indução, existe uma sequência $h_0 = 0, h_1, \ldots, h_{w(g)} = h$ de elementos de G e comprimento $w(g)$ tal que $w(h_j - h_{j-1}) = 1$, para $j = 1, \ldots, w(g)$. Assim, a sequência $h_0 = 0, h_1, \ldots, h_{w(g)} = h$ de elementos de G e comprimento $w(g)$ com $w(h_j - h_{j-1}) = 1$, para $j = 1, 2, \ldots, w(g)$. Assim, a sequência $h_0 = 0, h_1, \ldots, h_{w(g)}, h_{w(g)+1} = \tilde{g}$ são elementos de G e de comprimento $w(g)+1$ tal que $w(h_j - h_{j-1}) = 1$, para $j = 1, 2, \ldots, w(g)+1$. Portanto, $w(-)$ é uma função consecutiva. ■

Proposição 3.3.5. *([7], p. 6) Sejam G um grupo abeliano e $w : G \to \mathbb{R}$ uma função peso. Então, $w(-)$ é consecutiva se, e somente se, para todo $g, h \in G$ tal que $w(g-h) > 0$, existe uma sequência $g_0 = g, g_1, \ldots, g_{w(g-h)}$ de elementos de G com $w(g_j - g_{j-1}) = 1$, para $j = 1, 2, \ldots, w(g-h)$.*

Demonstração: Suponhamos que $w(-)$ é consecutiva. Seja $w(g-h) > 0$, com $g, h \in G$. Por hipótese, existe uma sequência $h_0 = 0, h_1, \ldots, h_{w(g-h)} = g - h$ de elementos de G e comprimento $w(g-h)$ tal que $w(h_j - h_{j-1}) = 1$, para $j = 1, \ldots, w(g-h)$. A sequência $g_j = h_j + g$, para $j = 0, 1, \ldots, w(g-h)$ é de elementos de G e de comprimento $w(g-h)$ com $w(g_j - g_{j-1}) = w(h_j + g - (h_{j-1} + g)) = w(h_j - h_{j-1}) = 1$. Reciprocamente, tomando $h \in G$ e $g = 0$ temos, por hipótese, que existe uma sequência $g_0 = g = 0, g_1, \ldots, g_{w(h)}$ de elementos de G e de comprimento $w(h)$ tal que $w(g_j - g_{j-1}) = 1$, para $j = 1, 2, \ldots, w(h)$. Portanto, $w(-)$ é consecutiva. ■

Proposição 3.3.6. *([7], p. 6) Sejam G um grupo abeliano e $w : G \to \mathbb{R}$ uma função peso. Então, são equivalentes*

1. *Para todo $g, h \in G$ tal que $w(g-h) > 0$ existe uma sequência $g_0 = g_1, \ldots, g_{w(g-h)}$ de elementos de G com $w(g_j - g_{j-1}) = 1$, para $j = 1, 2, \ldots, w(g-h)$.*

2. *Para todo $g, h \in G$ tal que $w(g-h) > 0$ e para todo $n \in \mathbb{N}$ com $0 \leq m \leq w(g-h)$, existe um elemento $k \in G$ tal que $w(g-k) = m$ e $w(k-h) = w(g-h) = m$.*

3. *Para todo $g \in G$ tal que $w(g) > 0$, existe um elemento $h \in G$ tal que $w(g-h) = 1$ e $w(h) = w(g) - 1$.*

Demonstração: Pelas Proposições 3.3.4 e 3.3.5 é suficiente provar que 1) $\Rightarrow$ 2) e 2) $\Rightarrow$ 3). Para o primeiro caso, sejam $g, h \in G$ tal que $w(g-h) > 0$ e $m \in \mathbb{Z}$ com $0 \leq m \leq w(g-h)$. Por hipótese, existe uma sequência $g = g_0, g_1, \ldots, g_d = h \in G$ tal que $w(g_j - g_{j-1}) = 1$, para $j = 1, \ldots, w(g-h)$. Tomando $k = g_m$, pela desigualdade

triangular, obtemos que

$$\begin{aligned} w(g-k) &= w(g-g_m) = w(g-g_1+g_1-g_2+g_2+\ldots+g_{m-1}-g_m) \\ &\leq w(g-g_1)+w(g_1-g_2)+\ldots+w(g_{m-1}-g_m) \\ &= \underbrace{1+\ldots+1}_{m \text{ vezes}} = m, \end{aligned}$$

ou seja, $w(g-k) \leq m$. Por outro lado, aplicando novamente, a desigualdade triangular, tomando $h = k$, tem-se que

$$\begin{aligned} m &= \underbrace{1+\ldots+1}_{m \text{ vezes}} \\ &= w(g_0-g_1)+\ldots+w(g_{w(g-h)}-g_{w(g-h)-1}) \\ &\leq w(g_0-g_1+g_1+\ldots-g_d) = w(g_0-g_d) = w(g-h) = w(g-k). \end{aligned}$$

Portanto, $w(g-k) = m$. Agora, $w(k-h) = w(k+g-g-h) \leq w(g-h)+w(-g+k) = w(g-h)-w(g-k) = w(g-h)-m$ e $w(g-h)-m = w(g-h)-w(g-k) \geq w(g-h-g+k) = w(k-h)$. Para o segundo caso, tomando $h = 0$, $m = 1$ e $g \in G$ tal que $w(g) > 0$, temos que existe $k \in G$ tal que $w(g-k) = 1$ e $w(k) = w(g)-1$.■

Corolário 3.3.1. *([7], p. 6) Se $w(-)$ é uma função peso consecutiva sobre um grupo abeliano G, então a função peso $w(-)$ induzida sobre G^n é consecutiva.*

Demonstração: Seja $g = (g_1, \ldots, g_n) \in G^n$ tal que $w(g) = \sum_{j=1}^{n} w(g_j) > 0$. Sem perda de generalidade, assumimos que $w(g_1) > 0$. Pela Proposição 3.3.4, existe $h_1 \in G$ com $w(h_1) = w(g_1)-1$ e $w(g_1-h_1) = 1$. Assim, se $h = (h_1, h_2, \ldots, h_n) \in G^n$, então $w(g-h) = w(g_1-h_1) = 1$ e $w(h) = w(h_1)+\sum_{j=2}^{n} w(g_j) = w(g_1)-1+\sum_{j=2}^{n} w(g_j) = \sum_{j=1}^{n} w(g_j)-1 = w(g)-1$. Novamente, pela Proposição 3.3.4, temos que a função peso $w(-)$ sobre G^n é consecutiva. ■

Proposição 3.3.7. *([7], p. 7) Sejam $w(-)$ uma função peso sobre o corpo $GF(p^h)$, $d(.,.)$ a distância sobre $GF(p^h)^l$ induzida pela função peso e $t = [\frac{d_w-1}{2}]$. Se $C \subset GF(p^h)^l$ é um código com distância mínima $d_w > 0$, então C é capaz de corrigir todo padrão de t-erros mas não corrige todos os padrões de $(t+1)$-erros.*

Demonstração: Pela desigualdade do triângulo, segue que C é um código capaz de corrigir todo padrão de t-erros. Por outro lado, existem $x, y \in C$ tal que $d(x,y) = d_w$. Pelo Corolário 3.3.1 e pelas Proposições 3.3.4 e 3.3.6, segue que existe $z \in GF(p^h)^l$ com $d(x,z) = t+1$ e $d(z,y) = d_w - (t+1)$. Como $d_w \leq 2t+1$, segue que $d(z,y) = d_w - (t+1) \leq 2t+1-(t+1) = t$. Assim, se x é a palavra-transmitida, z é a palavra recebida e ocorreram $t+1$ erros, então usando a decodificação através da distância mínima o vetor recebido será y e não pode obter a palavra-código x. Portanto, o código C não corrige padrões de $t+1$ erros. ■

Lema 3.3.1. *([7], p. 7) Seja $\alpha \in \mathbb{Z}[\xi_n]$. Então,*

1. *$w_{\mathcal{M}}(\alpha) = 1$ se, e somente se, $\alpha = \pm 1, \pm\xi_n, \ldots, \pm\xi_n^{\varphi(n)-1}$. Neste caso, $w_{\bar{\mathcal{M}}}(\bar{a}) = w_{\mathcal{M}}(a) = min_{x \in a+\mathcal{I}} w_{\mathcal{M}}(x)$.*

2. *Se p e m são ímpares, então $\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{\varphi(n)-1}$ são elementos em $\mathbb{Z}_p(\xi_m) \simeq \frac{\mathbb{Z}[\xi_n]}{\mathcal{I}}$ de peso de Mannheim 1. Por outro lado, $1, \xi_m, \ldots, \xi_m^{\varphi(m)-1}$ são todos os elementos em $\mathbb{Z}_p(\xi_m) \simeq \frac{\mathbb{Z}[\xi_n]}{\mathcal{I}}$ de peso de Mannheim 1.*

Demonstração:

1. Seja $\alpha = \sum_{k=0}^{\varphi(n)-1} a_k \xi_n^k \in \mathbb{Z}[\xi_n]$ tal que $w_{\mathcal{M}}(\alpha) = 1$. Assim, $w_{\bar{\mathcal{M}}}(\bar{\alpha}) = w_{\mathcal{M}}(\alpha) = 1$ se, e somente se, $\sum_{k=0}^{\varphi(n)-1} |a_k| = 1$ se, e somente se, $a_k = \pm 1$, para algum $k = 0, 1, \ldots, \varphi(n)-1$ se, e somente se, $\alpha = \pm 1, \pm\xi_n, \ldots, \xi_n^{\varphi(n)-1}$.

2. Seja $n = p^e m$ tal que p não divide m. Através do isomorfismo, $\mathbb{Z}_p(\xi_m) \simeq \frac{\mathbb{Z}[\xi_n]}{\mathcal{P}_i}$, para $i = 1, 2, \ldots, r$, temos que $\bar{\xi_n} = \xi_m$ é uma raiz m-ésima primitiva da unidade. Sendo p e m ímpares, segue que $(-\bar{\xi_n})^m = -1 \neq 1$ e caso contrário, $(\bar{\xi_n})^m = 1$. ■

Proposição 3.3.8. *([7], p. 7) O peso de Mannheim $w_{\bar{\mathcal{M}}}(\bar{a}) = min_{x \in a+\mathcal{I}} w_{\mathcal{M}}(x)$, para $\bar{a} \in \mathbb{Z}_p(\xi_m)$ é consecutivo.*

Demonstração: Seja $\bar{a} \in \mathbb{Z}_p(\xi_m)$ com $a = \sum_{k=0}^{\varphi(n)-1} a_k \xi_n^k \in \mathbb{Z}[\xi_n]$ tal que $w_{\bar{\mathcal{M}}}(\bar{a}) = w_{\mathcal{M}}(a) = min_{x \in a+\mathcal{I}} w_{\mathcal{M}}(x) > 0$. Pela Proposição 3.3.4 e pelo Lema 3.3.1 é suficiente encontrar um elemento $b \in \mathbb{Z}[\xi_n]$ com $w_{\bar{\mathcal{M}}}(\bar{b}) = w_{\mathcal{M}}(b) = w_{\mathcal{M}}(a) - 1$ e $w_{\mathcal{M}}(a-b) = 1$. Seja $a = (a_0, \ldots, a_{\varphi(n)-1})$ a sequência de inteiros tal que $w_{\mathcal{M}}(a) = min_{x \in a+\mathcal{I}} w_{\mathcal{M}}(x)$. Sem perda de generalidade, assumimos que $a_0 \neq 0$. Suponhamos que $a_0 > 0$. Se $b = (a_0 - 1, a_1, \ldots, a_{\varphi(n)-1})$, então $w_{\mathcal{M}}(a-b) = 1$ e $w_{\mathcal{M}}(b) = w_{\mathcal{M}}(a) - 1$. Devemos provar que $w_{\bar{\mathcal{M}}}(\bar{b}) = w_{\mathcal{M}}(b)$. Se $w_{\bar{\mathcal{M}}}(\bar{b}) \neq w_{\mathcal{M}}(b)$, então existe $u = (u_0, u_1, \ldots, u_{\varphi(n)-1}) \in \mathcal{I}$, na qual $\mathcal{I}$ é o ideal primo com $\frac{\mathbb{Z}[\xi_n]}{\mathcal{I}} \simeq \mathbb{Z}_p(\xi_m)$, com $w_{\bar{\mathcal{M}}}(\bar{b}) = w_{\mathcal{M}}(b+u) < w_{\mathcal{M}}(b)$, ou seja,

$$\begin{aligned} w_{\mathcal{M}}(b+u) &= w(a_0 - 1 + u_0, a_1 + u_1, \ldots, a_{\varphi(n)-1}) + u_{\varphi(n)-1}) \\ &= |a_0 - 1 + u_0| + \ldots + |a_{\varphi(n)-1} + u_{\varphi(n)-1}| < w_{\mathcal{M}}(b) \\ &= |a_0 - 1| + |a_1| + \ldots + |a_{\varphi(n)-1}|. \end{aligned}$$

Assim,

$$|a_0 - 1 + u_0| - |a_0 - 1| < |a_1| + \ldots + |a_{\varphi(n)-1}| - |a_1 - u_1| - \ldots - |a_{\varphi(n)-1} - u_{\varphi(n)-1}|. \quad (3.22)$$

Pela desigualdade triangular, temos que

$$|a_0 + u_0| = |(a_0 - 1 + u_0) + 1| \leq |a_0 - 1 + u_0| + 1.$$

Como $a_0 - 1 \geq 0$, segue que

$$|a_0 + u_0| + a_0 - 1 \leq |a_0 - 1 + u_0| + 1 + a_0 - 1 = |a_0 - 1 + u_0| + a_0,$$

ou seja, $|a_0 + u_0| + |a_0 - 1| \leq |a_0 - 1 + u_0| + |a_0|$. Assim, $|a_0 + u_0| - |a_0| \leq |a_0 - 1 + u_0| - |a_0 - 1|$. Combinando esta última desigualdade com a Equação (3.22) obtemos que

$$|a_0 + u_0| - |a_0| < |a_1| + \ldots + |a_{\varphi(n)-1}| - |a_1 - u_1| - \ldots - |a_{\varphi(n)-1} - u_{\varphi(n)-1}|,$$

ou seja, $w(a+u) = |a_0 + u_0| + |a_1 + u_1| + \ldots + |a_{\varphi(n)-1} + u_{\varphi(n)-1}| < |a_0| + |a_1| + \ldots + |a_{\varphi(n)-1}| = w_{\mathcal{M}}(a)$, o que é uma contradição, pois escolhemos a tal que $w_{\mathcal{M}}(a) = min_{x \in a+\mathcal{I}} w_{\mathcal{M}}(x)$. Assim, $w_{\bar{\mathcal{M}}}(\bar{b}) = w_{\mathcal{M}}(b)$ e portanto, $w_{\bar{\mathcal{M}}}(-)$ é consecutivo. De

modo análogo, o resultado também vale para $a_0 < 0$, uma vez que neste caso considere $-a$ temos, pelo caso anterior, que existe uma sequência $0, \bar{c_1}, \ldots, \bar{c}_{w_{\mathcal{M}}(a)-1}, -\bar{a}$ de comprimento $w_{\mathcal{M}}(a)$ tal que $w(\bar{c_j} - \bar{c_{j-1}}) = 1$ para $j = 1, 2, \ldots, w(-\bar{a})$ e deste modo, $0, -\bar{c_1}, \ldots, -\bar{c}_{w_{\mathcal{M}}(a)-1}, \bar{a}$ é uma cadeia satisfazendo o resultado. ■

Definição 3.3.7. *Sejam $\bar{\alpha}$, $\bar{\beta} \in \mathbb{Z}_p(\xi_m)$. Definimos a distância de Mannheim entre $\bar{\alpha}, \bar{\beta}$, como*

$$d_{\bar{\mathcal{M}}}(\bar{\alpha}, \bar{\beta}) = w_{\bar{\mathcal{M}}}(\bar{\alpha} - \bar{\beta}) = min_{x \in (\alpha-\beta)+\mathcal{I}} w_{\mathcal{M}}(x).$$

Corolário 3.3.2. *([7], p. 7) Se a distância de Mannheim mínima de um código C é $d_{\bar{w}}$, então sua capacidade de correção é $[\frac{d_{\bar{w}} - 1}{2}]$.*

Demonstração: Consequência da Proposição 3.3.8. ■

Proposição 3.3.9. *([7], p. 8) Sejam α um gerador do grupo multiplicativo $GF(p^h)^*$ e $p^h - 1 = lk$. Se C é um código linear com matriz controle de paridade*

$$H = \begin{pmatrix} 1 & \beta & \ldots & \beta^{n-1} \end{pmatrix},$$

então C corrige um erro que pertence ao conjunto $\{1, \alpha^l, \alpha^{2l}, \ldots, \alpha^{(k-1)l}\}$.

Demonstração: Sejam $c \in C$ e $r = (0, \ldots, 0, \alpha^{jl}, 0, \ldots, 0)$ com α^{jl} sendo a única componente não nula na posição L. Assim, a síndrome do vetor recebido $c + r$ é $(c + r)H^T = \alpha^L \alpha^{jl} = \alpha^{L+jl} = \alpha^e$. Como a potência e é conhecida pela síndrome, segue que a posição do erro $L \equiv e \ (mod\ l)$, é o resto da divisão de e por l, em que o índice do erro $j = [\frac{e}{l}]$ é o quociente de e dividido por l. ■

Teorema 3.3.1. *([7], p. 9) Sejam α um gerador do grupo multiplicativo $GF(p^h)^*$ e $p^h - 1 = lk$, na qual*

$$l = \begin{cases} \frac{p^h - 1}{2m} & \text{se } p \text{ é primo ímpar e } m \text{ ímpar} \\ \frac{p^h - 1}{m} & \text{caso contrário.} \end{cases}$$

Se C é um código linear com matriz controle de paridade dada por $H = \begin{pmatrix} 1 & \alpha & \ldots & \alpha^{l-1} \end{pmatrix}$, então C corrige um erro de Mannheim, ou seja, $d_{\bar{\mathcal{M}}}(C) \geq 3$.

Demonstração: Sabemos que $m \mid (p^h - 1)$. Agora, se p e m são primos ímpares, então $mdc(p, m) = 1$ e portanto, $pm \mid (p^h - 1)$. Assim, em ambos os casos temos que $l \in \mathbb{Z}$. Pelo Lema 3.3.1, temos que $\pm 1, \pm\xi_m, \ldots, \pm\xi_m^{\varphi(m)-1}$ são todos os elementos de $GF(p^h)$ de peso de Mannheim 1. Se $k = \dfrac{p^h - 1}{l}$, então em ambos os casos tem-se que $-\xi_m$ tem ordem k. Assim, $-\xi_m$ pertence ao subgrupo de ordem k gerado por α^l, uma vez que o subgrupo de ordem k em $GF(p^h)^*$ é único. Deste modo, todos os elementos em $GF(p^h)$ de peso de Mannheim 1 pertence ao subgrupo de ordem k gerado por α^l. Pela Proposição 3.3.9, segue que o código pode corrigir um erro de Mannheim. ■

Observação 3.3.3. *Se $n = m = 4$ e $p \equiv 1$ $(mod\ 4)$ no Teorema 3.3.1, então obtemos um código sobre o anel de inteiros gaussianos que é um código corretor de um erro de Mannheim e a distância de Mannheim via corpos ciclotômicos torna-se a distância de Manhattan como visto na Definição 3.3.2.*

3.4 Comparação entre Huber e Fan

Nesta seção, veremos uma comparação entre as constelações de sinais de Huber [1] e de Fan [7] via o anel de inteiros Gaussianos e um processo de rotulamento para determimar o sistema de representantes $R \subset \mathbb{Z}[i]$ via o peso de Mannheim de Fan.

Para isso consideremos $\mathbb{Z}[\xi_4] = \mathbb{Z}[i]$ o anel de inteiros Gaussianos. Como $p = 2$, pelo Lema de Kummer, temos que $p\mathbb{Z}[i] = (1 + i)(1 - i)$ e assim, $\dfrac{\mathbb{Z}[i]}{\langle 1 + i \rangle} \simeq \mathbb{Z}_2$. Se p é ímpar, então $GF(p^h) \simeq \mathbb{Z}_p(\xi_m)$, em que

$$h = \begin{cases} 1 \text{ se } p \equiv 1 \pmod 4, \\ 2 \text{ se } p \equiv 3 \pmod 4. \end{cases}$$

Se $h = 2$, então o sistema de representantes R é um quadrado como fez Carvalho em [5] e [6]. Deste modo, consideremos $h = 1$, ou seja, $p \equiv 1$ $(mod\ 4)$ tal como fez Huber [1]. Temos que, o ideal primo $\mathcal{I}$ tal que $\dfrac{\mathbb{Z}[i]}{\mathcal{I}} \simeq \mathbb{Z}_p$ é um ideal principal gerado por $\pi = a + bi \in \mathbb{Z}[i]$ com $N(\pi) = a^2 + b^2 = p$.

Se $\mathcal{I} = \langle \pi \rangle$ em $\mathbb{Z}[i]$ é um ideal primo com $N(\pi) = a^2 + b^2 = p$, então $a+b$ é ímpar, a e b são não nulos e $a \neq b$. Sem perda de generalidade, assumimos que $a > b > 0$. O conjunto dos pontos do ideal $\mathcal{I} = \langle \pi \rangle$ em $\mathbb{Z}[i]$ é o conjunto dos pontos no plano complexo gerado pelos vetores $\pi = a + bi$ e $i\pi = i(a + bi) = -b + ai$, conforme a Figura I.

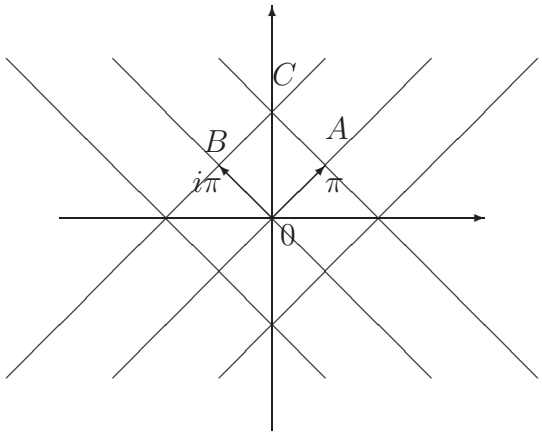

Figura I

Fazendo uma translação, temos que cada ponto de $\mathbb{Z}[i]$ pode ser movido dentro do quadrado $OACB$ determinado pelos vetores $\vec{OA} = \vec{\pi} = (a, b)$ e $\vec{OB} = i\vec{\pi} = (-b, a)$. Assim, temos que os pontos com coordenadas inteiras no quadrado $OACB$ ou no lado OA (sem o ponto A) e o lado OB (sem o ponto B) forma um sistema completo de representantes das classes laterais de $\dfrac{\mathbb{Z}[i]}{\mathcal{I}}$. Deste modo, para um ponto de coordenadas inteiras D, o vetor $\vec{OD}$ representa um inteiro Gaussiano e os vetores $\vec{AD}$, $\vec{BD}$ e $\vec{CD}$ também pertencem a classe lateral contendo o inteiro gaussiano $\vec{OD}$. Dentre os quatros vetores, o vetor de comprimento de Manhattan mínimo é o representante procurado para essa classe lateral, conforme a Figura II. Assim, o objetivo é determinar qual dos vértices O, A, C e B está mais próximo do ponto D via a distância de Manhattan.

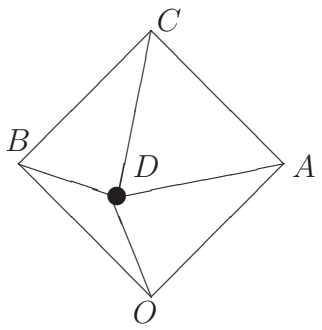

Figura II

Definição 3.4.1. *Definimos a linha equidistante de dois pontos A e B no plano como o conjunto de pontos T do plano (não necessariamente com coordenadas inteiras) tal que $d_{\mathcal{M}}(T, A) = d_{\mathcal{M}}(T, B)$, na qual $d_{\mathcal{M}}$ é a distância de Manhattan.*

Observação 3.4.1. *A linha equidistante de dois pontos A e B não é uma linha reta, uma vez que a distância de Manhattan é um ziguezague.*

Seja um retângulo com lados horizontais e verticais e com diagonal AB. Sejam C e D dois pontos nos lados do retângulo que tem a mesma distância de A e B. Sejam CE e DF linhas perpendiculares aos lados do retângulo, conforme da figura abaixo.

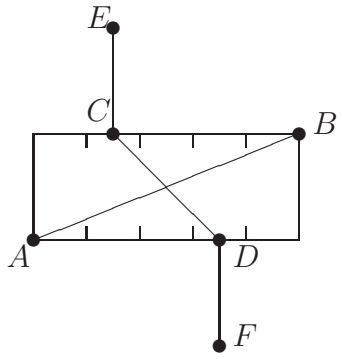

Figura III

Observação 3.4.2. *O ziquezaque determinado por $ECDF$ na Figura III é o conjunto T (não necessariamente de coordenadas inteiras) tal que $d_{\mathcal{M}}(T, A) = d_{\mathcal{M}}(T, B)$.*

Lema 3.4.1. *([9], p. 13) Sejam A e B dois pontos de coordenadas inteiras no plano complexo. Se $d_{\mathcal{M}}(A,B)$ é ímpar, então não existe um ponto T com coordenadas inteiras tal que $d_{\mathcal{M}}(T,A) = d_{\mathcal{M}}(T,B)$, isto é, não existe um ponto com coordenadas inteiras na linha equidistante de A e B.*

Demonstração: Se o ponto T está dentro do retângulo, então $d_{\mathcal{M}}(A,T)+d_{\mathcal{M}}(T,B) = d_{\mathcal{M}}(A,B)$. Caso contrário, temos que $d_{\mathcal{M}}(A,T) + d_{\mathcal{M}}(T,B) = d_{\mathcal{M}}(A,B) + 2k$ para algum $k > 0$. Como $d_{\mathcal{M}}(A,B)$ é ímpar e $d_{\mathcal{M}}(A,T)$ e $d_{\mathcal{M}}(T,B)$ são inteiros, segue que $d_{\mathcal{M}}(A,T) = d_{\mathcal{M}}(T,B)$ não pode ocorrer, o que prova o Lema. ■

Na Figura II, temos que o comprimento do lado do quadrado $OACB$ é $d_{\mathcal{M}}(O,A) = a + b$ que é ímpar. Usando o conceito de linha equidistante e o Lema 5.5, transformamos a Figura II na Figura IV, em que o centro $Z = (\frac{a-b}{2}, \frac{a+b}{2})$ do quadrado tem coordenadas não inteiras e tem a mesma distância dos quatros vértices. Assim, as quatro linhas equidistantes dos quatro lados do quadrado passam pelo ponto Z. Deste modo, essas linhas dividem o quadrado em quatro regiões, conforme a Figura IV. Novamente, pelo Lema 3.4.1, segue que nenhum dos pontos das linhas equidistantes tem coordenadas inteiras.

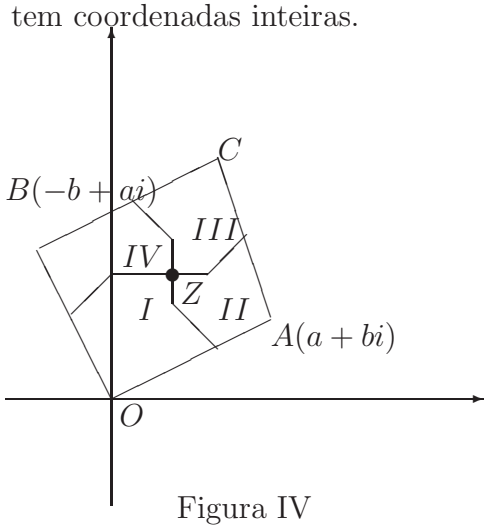

Figura IV

Proposição 3.4.1. *([9], p. 14) Sejam $\pi = a + bi \in \mathbb{Z}[i]$ tal que $N(\pi) = a^2 + b^2 = p$ é um número primo ímpar e $\mathcal{I} = \langle \pi \rangle$ é um ideal primo em $\mathbb{Z}[i]$. Então,*

1. *Em cada classe lateral de $\frac{\mathbb{Z}[i]}{\mathcal{I}}$ existe um único elemento r tal que $w_{\mathcal{M}}(r) = min_{x \in\ r+\mathcal{I}} w_{\mathcal{M}}(x)$.*

2. *Se R é um sistema de representantes de $\frac{\mathbb{Z}[i]}{\mathcal{I}}$ formado pelos únicos elementos obtidos no caso* 1*, então*

$$max_{r\in R} w_{\mathcal{M}}(r) = max\{|a|, |b|\} - 1.$$

Demonstração:

1. Conforme a Figura IV, temos que os pontos de coordenadas inteiras na região onde a origem está contido estão mais próximo do vértice O. O mesmo também vale para as outras regiões. Como não existem pontos de coordenadas inteiras na linha equidistante, segue que é impossível que um ponto com coordenadas inteiras sobre o quadrado tem a menor distância de dois vértices do quadrado. Portanto, em cada classe lateral de $\frac{\mathbb{Z}[i]}{\mathcal{I}}$, existe um único $r \in \mathbb{Z}[i]$ tal que $w_{\mathcal{M}}(r) = min_{x\in r+\mathcal{I}} w_{\mathcal{M}}(x)$.

2. É suficiente considerar a região onde o ponto O está contido. Nesta região, temos que o ponto Z está mais afastado da origem da distância de Manhattan $|a|$, mas não é um ponto de coordenadas inteiras. Dessa forma, os pontos de coordenadas inteiras nesta região tem distância de Manhattan no máximo $|a|-1$. Por outro lado, os pontos de coordenas inteiras da região que está mais próxima do centro Z tem distância de O igual a $a-1$. ■

Um método geométrico para transformar a Figura IV na Figura V, de modo que o sistema de representantes R tenha a forma de um cata-vento é o seguinte: um ponto de coordenadas inteiras na região II na Figura IV corresponde ao vetor de A a esse ponto, que é um representante da classe lateral. Assim, transladamos a região de modo que A coincide com a origem O e obtemos a região II, conforme a Figura V. As regiões IV e II da Figura IV, podem ser transladadas de modo análogo obtendo as regiões da Figura V. A Figura V, toma a forma de um cata-vento. Tomando os pontos de coordenadas inteiras na Figura V e observando que não existem pontos de coordenadas inteiras nos lados, obtemos o sistema de representante procurado. Observamos que nas Figuras IV e V, tomando $a = 5$, $b = 2$ e $p = 29$, segue que a Figura V é exatamente a Figura II.

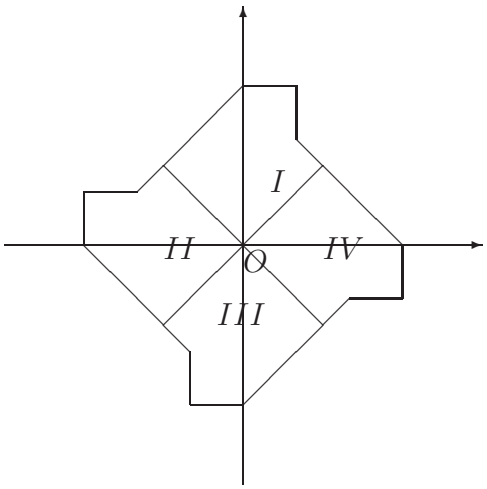

Figura V

O algoritmo para rotular os elementos da região R é dado por:

1. Sejam p número primo tal que $p \equiv 1 \ (mod\ 4)$ e $\mathcal{I} = \langle \pi \rangle$ em $\mathbb{Z}[i]$ é um ideal primo tal que $N(\pi) = a^2 + b^2 = p$, em que $\pi = a + bi$, para $a, b \in \mathbb{Z}$.

2. Seja a única solução da equação $a + bs \equiv 0 \ (mod\ p)$, na qual $0 \leq s \leq p - 1$.

3. O elemento $l \in GF(p)$ será o rótulo do ponto $\alpha_l = x + yi$ se $x + yr \equiv l \ (mod\ p)$.

Exemplo 3.4.1. *Seja* $p = 17 \equiv 1 \ (mod\ 4)$. *Aplicando, o algoritmo temos que*

1. *Uma solução para* $a^2 + b^2 = p = 17$ *é* $a = 4$ *e* $b = 1$. *Assim, tomamos* $\mathcal{I} = \langle 4 + i \rangle$ *em* $\mathbb{Z}[i]$.

2. *A única solução da equação* $a + bs = 4 + s \equiv 0 \ (mod\ 17)$, *em que* $0 \leq s \leq 16$ *é* $s = 13$.

3. *Assim,* $l \in GF(17)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *se* $x + 13y \equiv l \ (mod\ 17)$. *Assim, obtemos a Tabela 3.3 e a Figura* 3.1.

(x, y)	$x + 13y \equiv l \ (mod\ 17)$	(x, y)	$x + 13y \equiv l \ (mod\ 17)$
$(0, 0)$	0	$(0, 2)$	9
$(1, 0)$	1	$(1, 2)$	10
$(2, 0)$	2	$(-2, 1)$	11
$(-1, -1)$	3	$(-1, 1)$	12
$(0, -1)$	4	$(0, 1)$	13
$(1, -1)$	5	$(1, 1)$	14
$(2, -1)$	6	$(-2, 0)$	15
$(-1, -2)$	7	$(-1, 0)$	16
$(0, -2)$	8		

Tabela 3.3: Constelação com 17 sinais rotulados por $GF(17)$

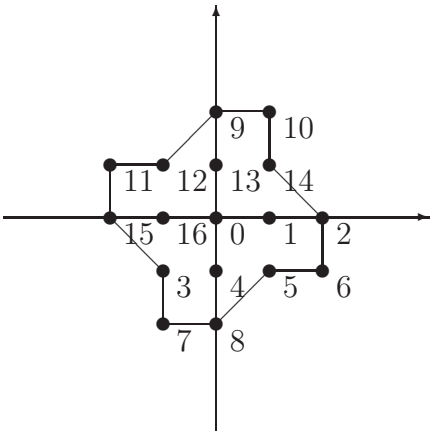

Figura 3.1

Observação 3.4.3. *Observamos que a constelação com* 17 *sinais com o conceito de peso Mannheim de Fan [7] é igual a constelação obtida por Huber [1], como podemos ver pelo Exemplo 2.3.9.*

Exemplo 3.4.2. *Seja* $p = 29 \equiv 1\ (mod\ 4)$. *Aplicando, o algoritmo temos que:*

1. *Uma solução para* $a^2 + b^2 = p = 29$ *é* $a = 5$ *e* $b = 2$. *Assim, tomamos* $\mathcal{I} = \langle 5 + 2i \rangle$ *em* $\mathbb{Z}[i]$.

2. *A única solução da equação* $a + bs = 5 + 2s \equiv 0\ (mod\ 29)$, *em que* $0 \leq s \leq 28$ *é* $s = 12$.

3. *Assim,* $l \in GF(29)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *se* $x + 12y \equiv l\ (mod\ 29)$. *Assim, obtemos a Tabela 3.4 e a Figura* 3.2.

(x, y)	$x + 12y \equiv l \ (mod\ 29)$	(x, y)	$x + 12y \equiv l \ (mod\ 29)$
$(0, 0)$	0	$(-2, -1)$	15
$(1, 0)$	1	$(-1, -1)$	16
$(2, 0)$	2	$(0, -1)$	17
$(3, 0)$	3	$(1, -1)$	18
$(-1, -2)$	4	$(2, -1)$	19
$(0, -2)$	5	$(3, -1)$	20
$(1, -2)$	6	$(-1, -3)$	21
$(0, 3)$	7	$(0, -3)$	22
$(1, 3)$	8	$(-1, 2)$	23
$(-3, 1)$	9	$(0, 2)$	24
$(-2, 1)$	10	$(1, 2)$	25
$(-1, 1)$	11	$(-3, 0)$	26
$(0, 1)$	12	$(-2, 0)$	27
$(1, 1)$	13	$(-1, 0)$	28
$(2, 1)$	14		

Tabela 3.4: Constelação com 29 sinais rotulados por $GF(29)$

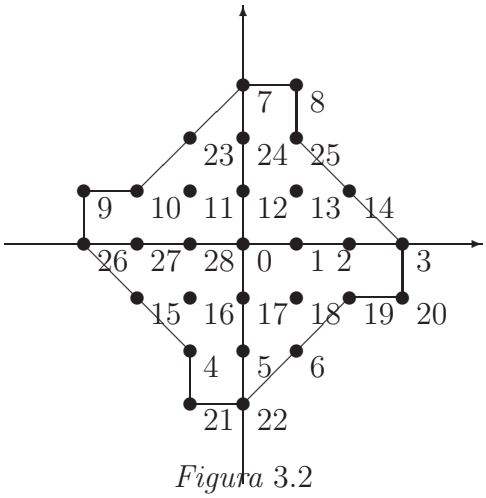

Figura 3.2

Exemplo 3.4.3. *Seja* $p = 37 \equiv 1 \ (mod\ 4)$. *Aplicando, o algoritmo temos que:*

1. *Uma solução para* $a^2 + b^2 = p = 37$ *é* $a = 6$ *e* $b = 1$. *Assim, tomamos* $\mathcal{P} = \langle 6 + i \rangle$ *em* $\mathbb{Z}[i]$.

2. *A única solução da equação* $a + bs = 6 + s \equiv 0 \ (mod\ 37)$, *em que* $0 \leq r \leq 36$ *é* $s = 31$.

3. *Assim,* $l \in GF(37)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *se* $x + 31y \equiv l \ (mod\ 37)$. *Assim, obtemos a Tabela 3.5 e a Figura* 3.3.

(x, y)	$x + 31y \equiv l \ (mod\ 37)$	(x, y)	$s + 31y \equiv l \ (mod\ 37)$
$(0, 0)$	0	$(0, 3)$	19
$(1, 0)$	1	$(1, 3)$	20
$(2, 0)$	2	$(2, 3)$	21
$(3, 0)$	3	$(-3, 2)$	22
$(-2, -1)$	4	$(-2, 2)$	23
$(-1, -1)$	5	$(-1, 2)$	24
$(0, -1)$	6	$(0, 2)$	25
$(1, -1)$	7	$(1, 2)$	26
$(2, -1)$	8	$(2, 2)$	27
$(3, -1)$	9	$(-3, 1)$	28
$(-2, -2)$	10	$(-2, 1)$	29
$(-1, -2)$	11	$(-1, 1)$	30
$(0, -2)$	12	$(-1, 1)$	31
$(1, -2)$	13	$(1, 1)$	32
$(2, -2)$	14	$(2, 1)$	33
$(3, -2)$	15	$(-3, 0)$	34
$(-2, -3)$	16	$(-2, 0)$	35
$(-1, -3)$	17	$(-1, 0)$	36
$(0, -3)$	18		

Tabela 3.5: Constelação com 37 sinais rotulado por $GF(37)$

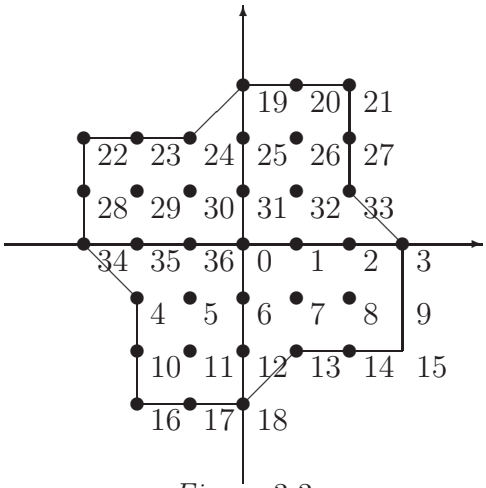

Figura 3.3

Observação 3.4.4. *Observamos que a constelação com* 37 *sinais com o conceito de peso de Mannheim de Fan [7] é igual a constelação obtida por Huber [1], como podemos ver pelo Exemplo 2.3.11.*

Exemplo 3.4.4. *Seja* $p = 41 \equiv 1\ (mod\ 4)$. *Aplicando, o algoritmo temos que:*

1. *Uma solução para* $a^2 + b^2 = p = 41$ *é* $a = 5$ *e* $b = 4$. *Assim, tomamos* $\mathcal{I} = \langle 5 + 4i \rangle$ *em* $\mathbb{Z}[i]$.

2. *A única solução da equação* $a + bs = 5 + 4s \equiv 0 \ (mod\ 41)$, *em que* $0 \leq s \leq 40$ *é* $s = 9$.

3. *Assim,* $l \in GF(41)$ *será o rótulo do ponto* $\alpha_l = x + yi$ *se* $x + 9y \equiv l \ (mod\ 41)$. *Assim, obtemos a Tabela 3.6 e a Figura* 3.4*:*

(x, y)	$x + 9y \equiv l \ (mod\ 41)$	(x, y)	$x + 9y \equiv l \ (mod\ 41)$
$(0, 0)$	0	$(-2, -2)$	21
$(1, 0)$	1	$(-1, -2)$	22
$(2, 0)$	2	$(0, -2)$	23
$(3, 0)$	3	$(1, -2)$	24
$(4, 0)$	4	$(2, -2)$	25
$(-4, 1)$	5	$(-1, 3)$	26
$(-3, 1)$	6	$(0, 3)$	27
$(-2, 1)$	7	$(1, 3)$	28
$(-1, 1)$	8	$(-3, -1)$	29
$(0, 1)$	9	$(-2, -1)$	30
$(1, 1)$	10	$(-1, -1)$	31
$(2, 1)$	11	$(0, -1)$	32
$(3, 1)$	12	$(1, -1)$	33
$(-1, -3)$	13	$(2, -1)$	34
$(0, -3)$	14	$(3, -1)$	35
$(1, -3)$	15	$(4, -1)$	36
$(-2, 2)$	16	$(0, 4)$	37
$(-1, 2)$	17	$(-3, 0)$	38
$(0, 2)$	18	$(-2, 0)$	39
$(1, 2)$	19	$(-1, 0)$	40
$(2, 2)$	20		

Tabela 3.6: Constelação com 41 sinais rotulados por $GF(41)$

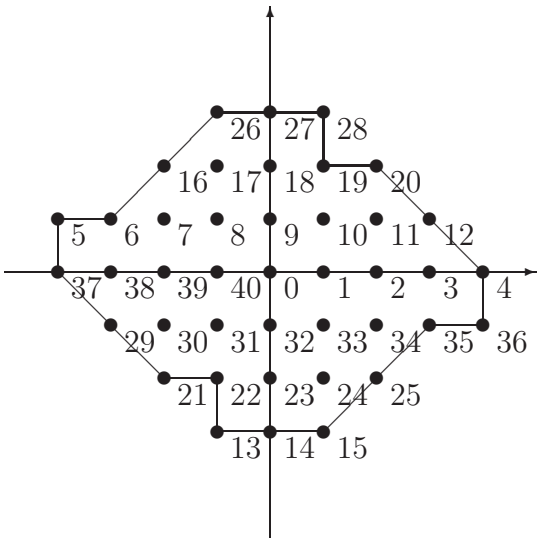

Figura 3.4

Observação 3.4.5. *É relevante observar que a construção das constelações de sinais via corpos ciclotômicos tem o caráter geométrico, com o objetivo de transformá-las num formato de cata-vento. Já a construção das constelações com p sinais via corpos quadráticos, como vimos no Capítulo 2, visa minimizar a norma dos elementos da constelação de sinais.*

Capítulo 4

Rotulamento de reticulados e região de Voronoi

4.1 Introdução

Uma maneira de construir constelações de sinais n dimensionais é tomar um subconjunto finito num reticulado Λ de dimensão n. Dessa forma, a constelação S de cardinalidade n, pode ser facilmente encontrada selecionando os n pontos do reticulado Λ. Neste capítulo, veremos o conceito de rotulamento linear de um reticulado introduzido por [4], no qual consiste em encontrar uma forma explícita do isomorfismo entre o grupo de Galois $GF(p)$ e o quociente $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}$, em que $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de um corpo de números $\mathbb{K}$ e $\mathcal{P}$ é um ideal primo em $\mathcal{O}_{\mathbb{K}}$. Para finalizar, determinamos a região de Voronoi da origem S, $\mathcal{V}_S(O)$, na qual S é reticulado de $\mathbb{Z}[\rho]$ gerado por $\{\pi, \rho\pi\}$ e $\pi = a + b\rho$ tal que a e b são inteiros.

4.2 Rotulamento de reticulados

Nesta seção, veremos o conceito de rotulamento de reticulados.

Definição 4.2.1.

1. *Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subseteq \mathbb{K}$*

um anel e $v_1, \ldots, v_m$ *vetores de* V *linearmente independentes sobre* $\mathbb{K}$*, com* $m \leq n$*. Definimos um reticulado, com base* $B = \{v_1, \ldots, v_m\}$*, ao conjunto dos elementos de* V *da forma*

$$\Lambda_p = \{x = \sum_{i=1}^{m} a_i v_i \ ; \ a_i \in A\}.$$

2. *Um subreticulado* Λ' *do reticulado* Λ *é um subgrupo do grupo aditivo* Λ*.*

Para obtermos reticulados Λ em $\mathbb{R}^n$ identificados com os elementos de um anel de inteiros proveniente de um corpo de números $\mathbb{K}$ de grau n, estabelecemos um homomorfismo de anéis $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1+2r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

chamado de homomorfismo canônico de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, em que $\sigma_j : \mathbb{K} \ \to \mathbb{C}$ são n monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, dizemos que σ_j é real, caso contrário, dizemos σ_j é imaginário. Quando todos os monomorfismos são reais dizemos que $\mathbb{K}$ é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um corpo totalmente imaginário. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$ temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$ e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$ podemos reordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+1}, \ldots, \sigma_{r_2}$ sejam os monomorfismos imaginários. Logo, $n = r_1 + 2r_2$. Identificando $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$, tem-se que o homomorfismo canônico também pode ser visto como

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

na qual $x \in \mathbb{K}$, $\Re$ representa a parte real e $\Im$ representa a parte imaginária do número complexo.

Exemplo 4.2.1. *Sejam* $\mathbb{K} = \mathbb{Q}(i)$, *em que* $i = \sqrt{-1}$ *e* $\{\sigma_1, \sigma_2\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *tal que* σ_1 *é a aplicação identidade e* $\sigma_2(a+bi) = a-bi$, *com* $a, b \in \mathbb{Q}$. *Assim,* $r_1 = 0$ *e* $r_2 = 1$. *Se* $x = a + bi \in \mathbb{K}$, *com* $a, b \in \mathbb{Q}$, *então* $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b)$.

Proposição 4.2.1. *([10], p. 56) Sejam* $\mathbb{K}$ *um corpo de números de grau* n *e* $\mathbb{M} \subseteq \mathbb{K}$ *um* $\mathbb{Z}$*-módulo livre de posto* n. *Se* $(x_j)_{1\leq j\leq n}$ *é uma* $\mathbb{Z}$*-base de* $\mathbb{M}$, *então* $\sigma_{\mathbb{K}}(\mathbb{M})$ *é um reticulado no* $\mathbb{R}^n$.

Demonstração: Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \quad (4.1)$$

Agora calculemos o determinante da matriz A que tem a j-ésima coluna dada pela Equação (4.1) fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z+\overline{z})$ e $\Im(z) = \frac{1}{2i}(z-\overline{z})$ para z em $\mathbb{C}$ e das transformações elementares do determinante, a saber pela adição da (r_1+2l)-ésima linha a sua anterior e em seguida pela subtração da (r_1+2l-1)-ésima coluna da sua posterior, para $l = 1, \ldots, r_2$, obtemos que

$$\begin{aligned}
\det(A) &= \det \begin{pmatrix}
\sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\
\sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\
\Re(\sigma_{r_1+1}(x_1)) & \ldots & \Re(\sigma_{r_1+1}(x_j)) & \ldots & \Re(\sigma_{r_1+1}(x_n)) \\
\Im(\sigma_{r_1+1}(x_1)) & \ldots & \Im(\sigma_{r_1+1}(x_j)) & \ldots & \Im(\sigma_{r_1+1}(x_n)) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\Re(\sigma_{r_1+r_2}(x_1)) & \ldots & \Re(\sigma_{r_1+r_2}(x_j)) & \ldots & \Re(\sigma_{r_1+r_2}(x_n)) \\
\Im(\sigma_{r_1+r_2}(x_1)) & \ldots & \Im(\sigma_{r_1+r_2}(x_j)) & \ldots & \Im(\sigma_{r_1+r_2}(x_n))
\end{pmatrix} \\
&= \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} \det(A_1),
\end{aligned}$$

em que

$$A_1 = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{pmatrix}.$$

Assim,

$$\det(A) = (-1)^{r_2} \left(\frac{1}{2}\right)^{\frac{r_2}{2}} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} \det(A_2),$$

na qual

$$A_2 = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_j)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{pmatrix}.$$

Deste modo,

$$\det(A) = \left(\frac{1}{2i}\right)^{r_2} \det(A_3),$$

em que

$$A_3 = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{pmatrix}.$$

Portanto, $\det(A) = (2i)^{-r_2}\det(\sigma_j(x_k))$, para j, $k = 1, \dots, n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que $\det(\sigma_j(x_k)) \neq 0$ e portanto, $A \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(\mathbb{M})$, ou seja, $\sigma_{\mathbb{K}}(\mathbb{M})$ é um reticulado do $\mathbb{R}^n$. ■

Corolário 4.2.1. *([10], p. 57) Sejam $\mathbb{K}$ um corpo de número de grau n, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Então, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{A})$ são reticulados do $\mathbb{R}^n$.*

Demonstração: Como $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{A}$ são $\mathbb{Z}$-módulos livres de posto n, segue da Proposição 4.2.1, que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{A})$ são reticulados do $\mathbb{R}^n$. ■

Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$, em que $\alpha \in \mathbb{C}$ é uma raiz de um polinômio mônico irredutível $m(x) \in \mathbb{Z}[x]$. Sejam $\alpha_1, \dots, \alpha_n$ as n raízes distintas de $m(x)$ e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. A aplicação $\sigma_{\mathbb{K}} : \mathcal{O}_{\mathbb{K}} \to \Lambda$, na qual $\Lambda = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é uma bijeção e portanto, existe $\sigma_{\mathbb{K}}^{-1} : \Lambda \to \mathcal{O}_{\mathbb{K}}$.

Definição 4.2.2. *Uma aplicação $l : \Lambda \to GF(p^t)$ é chamada um rotulamento linear se:*

$$l(\sigma(a_1w_1 + \ldots + a_nw_n)) = a_1l(\sigma(w_1)) + \ldots + a_nl(\sigma(w_n)),$$

em que $a_i \in \mathbb{Z}$, para $i = 1, \dots, n$, $t \in \mathbb{N}$ com $t \neq 0$ e $\{w_1, \dots, w_n\}$ é uma base de $\mathbb{K}$.

Da Definição 4.2.2 e do Lema de Kummer, temos a seguinte proposição:

Proposição 4.2.2. *([4], p. 4) Se* $\varphi : \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_j} \rightarrow GF(p^{d_j})$ *é um isomorfismo e* $\pi_j : \mathcal{O}_{\mathbb{K}} \rightarrow \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_j}$ *é a projeção natural, então* $l = \varphi \circ \pi_j \circ \sigma^{-1}$ *é um rotulamento linear de* Λ *em* $GF(p^{d_j})$.

Demonstração: Consideremos a seguinte sequência de aplicações

$$\Lambda = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) \overset{\sigma^{-1}}{\rightarrow} \mathcal{O}_{\mathbb{K}} \overset{\pi_j}{\rightarrow} \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_j} \overset{\varphi}{\rightarrow} GF(p^{d_j}).$$

Temos, para $\alpha = a_1w_1 + \ldots + a_nw_n \in \mathcal{O}_{\mathbb{K}}$, que

$$\begin{aligned}
l(\sigma(\alpha)) &= l(\sigma(a_1w_1 + \ldots + a_nw_n)) = (\varphi \circ \pi_j \circ \sigma^{-1})(\sigma(a_1w_1 + \ldots + a_nw_n)) \\
&= (\varphi \circ \pi_j)(\sigma^{-1}(\sigma(a_1w_1 + \ldots + a_nw_n))) = (\varphi \circ \pi_j)(a_1w_1 + \ldots + a_nw_n) \\
&= \varphi(\pi_j(a_1w_1 + \ldots + a_nw_n)) = \varphi(\pi_j(a_1w_1) + \ldots + \pi_j(a_nw_n)) \\
&= \varphi(\pi_j(a_1w_1)) + \ldots + \varphi(\pi_j(a_nw_n)) = a_1\varphi(\pi_j(w_1)) + \ldots + a_n\varphi(\pi_j(w_n)) \\
&= a_1(\varphi(\pi_j(\sigma^{-1} \circ \sigma(w_1)))) + \ldots + a_n(\varphi(\pi_j(\sigma^{-1} \circ \sigma(w_n)))) \\
&= a_1(\varphi \circ \pi_j\sigma^{-1}(\sigma(w_1))) + \ldots + a_n(\varphi \circ \pi_j\sigma^{-1}(\sigma(w_n))) \\
&= a_1(l(\sigma(w_1))) + \ldots + a_n(l(\sigma(w_n))).
\end{aligned}$$

Portanto, l é um rotulamento linear de Λ em $GF(p^{d_j})$. ■

Corolário 4.2.2. *([4], p. 4) Se* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$, *então* l *pode ser completamente especificada tomando* $l = \sigma(\alpha) = \bar{\alpha}$, *na qual* $\bar{\alpha}$ *é uma raiz do polinômio* $\overline{m_j(x)}$ *sobre* $GF(p)$.

Demonstração: Consequência da Proposição 4.2.2. ■

Corolário 4.2.3. *([4], p. 4)* $l(\sigma(x)) = l(\sigma(y))$ *se, e somente se,* x *e* y *são elementos da mesma classe lateral* $\mathcal{P}_j$ *em* $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Segue da Proposição 4.2.2. ■

Exemplo 4.2.2. *([5], p. 54) Seja* $\mathbb{K} = \mathbb{Q}(\alpha)$, *em que* α *é uma raiz complexa do polinômio minimal* $m(x) = x^3 - x + 1$. *O anel de inteiros de* $\mathbb{K}$ *é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$. *Tomando* $m(x)$ *módulo* 11, *obtemos que*

$$m(x) = (x - 5)(x^2 + 5x + 2) \ (mod\ \mathbb{Z}_{11}[x]).$$

Assim, pelo Lema de Kummer, temos que

$$11\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1\mathcal{P}_2,$$

tal que $\mathcal{P}_1 = \langle 11, \alpha - 5\rangle$ *e* $\mathcal{P}_2 = \langle 11, \alpha^2 + 5\alpha + 2\rangle$. *Como* $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_1} \cong GF(11)$, *segue que* $\alpha \equiv 5 \ (mod\ \mathcal{P}_1)$. *Deste modo, o rotulamento linear é dado por*

$$\begin{aligned} l(\sigma(a_0 + a_1\alpha + a_2\alpha^2)) &= a_0 l(\sigma(1)) + a_1 l(\sigma(\alpha)) + a_2 l(\sigma(\alpha^2)) \\ &= a_0 + 5a_1 + (5)^2 a_2 \\ &= a_0 + 5a_1 + 25a_2 \\ &= a_0 + 5a_1 + 3a_2 \ (mod\ 11), \end{aligned}$$

na qual $a_i \in \mathbb{Z}$, *para* $i = 0, 1, 2$.

Exemplo 4.2.3. *Seja* $\mathbb{K} = \mathbb{Q}(\alpha)$, *em que* α *é uma raiz complexa do polinômio minimal* $m(x) = x^4 - 2x^3 + 2x^2 - x + 1$. *O anel de inteiros de* $\mathbb{K}$ *é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$. *Tomando* $m(x)$ *módulo* 37, *obtemos que*

$$m(x) = (x + 17)(x + 19)(x^2 + 36x + 11) \ (mod\ \mathbb{Z}_{37}[x]).$$

Assim, pelo Lema de Kummer, temos que

$$37\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3,$$

onde $\mathcal{P}_1 = \langle 37, \alpha + 17\rangle$, $\mathcal{P}_2 = \langle 37, \alpha + 19\rangle$ *e* $\mathcal{P}_3 = \langle 37, \alpha^2 + 36\alpha + 11\rangle$. *Como* $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_1} \cong GF(37)$, *segue que* $\alpha \equiv 17 \ (mod\ \mathcal{P}_1)$. *Deste modo, o rotulamento linear é dado por*

$$\begin{aligned} l(\sigma(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3)) &= a_0 l(\sigma(1)) + a_1 l(\sigma(\alpha)) + a_2 l(\sigma(\alpha^2)) + a_3 l(\sigma(\alpha^3)) \\ &= a_0 + 17a_1 + (17)^2 a_2 + (17)^3 a_3 \\ &= a_0 + 17a_1 + 30a_2 + 29a_3 \ (mod\ 37), \end{aligned}$$

na quala$_i \in \mathbb{Z}$, *para* $i = 0, 1, 2, 3$.

Exemplo 4.2.4. *Seja* $\mathbb{K} = \mathbb{Q}(\xi_8)$, *em que* ξ_8 *é uma raiz* 8*-ésima primitiva da unidade com polinômio minimal* $m(x) = x^4 + 1$. *O anel de inteiros de* $\mathbb{K}$ *é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_8]$. *Tomando* $m(x)$ *módulo* 41, *obtemos que*

$$m(x) = (x + 38)(x + 3)(x + 14)(x + 27) \ (mod\ \mathbb{Z}_{41}[x]).$$

Assim, pelo Lema de Kummer, temos que

$$41\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4,$$

onde $\mathcal{P}_1 = \langle 41, \xi_8 + 38\rangle$ *e* $\mathcal{P}_2 = \langle 41, \xi_8 + 3\rangle$, $\mathcal{P}_3 = \langle 41, \xi_8 + 14\rangle$ *e* $\mathcal{P}_4 = \langle 41, \xi_8 + 27\rangle$. *Como* $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_1} \cong GF(41)$, *segue que* $\alpha \equiv 10 \ (mod\ \mathcal{P}_1)$. *Deste modo, o rotulamento linear é dado por*

$$\begin{aligned} l(\sigma(a_0 + a_1\xi_8 + a_2\xi_8^2 + a_3\xi_8^3)) &= a_0 l(\sigma(1)) + a_1 l(\sigma(\xi_8)) + a_2 l(\sigma(\xi_8)^2) + a_3 l(\sigma(\xi_8)^3)) \\ &= a_0 + 38a_1 + (38)^2 a_2 + (38)^3 a_3 \\ &= a_0 + 38a_1 + 9a_2 + 14a_3 \ (mod\ 41), \end{aligned}$$

na qual $a_i \in \mathbb{Z}$, *para* $i = 0, 1, 2$.

Exemplo 4.2.5. *Seja* $\mathbb{K} = \mathbb{Q}(\xi_{20})$, *em que* ξ_{20} *é uma raiz* 20*-ésima primitiva da unidade com polinômio minimal* $m(x) = x^8 - x^6 + x^4 - x^2 + 1$. *O anel de inteiros de* $\mathbb{K}$ *é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_{20}]$. *Tomando* $m(x)$ *módulo* 17, *obtemos que*

$$m(x) = (x^4 + 31x^3 + 36x^2 + 6x + 1)(x^4 + x^3 + 36x^2 + 31x + 1) \ (mod\ \mathbb{Z}_{17}[x]).$$

Assim, pelo Lema de Kummer, temos que

$$17\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1\mathcal{P}_2,$$

onde $\mathcal{P}_1 = \langle 17, \xi_{20}^4 + 31\xi_{20}^3 + 36\xi_{20}^2 + 6\xi_{20} + 1\rangle$ *e* $\mathcal{P}_2 = \langle 17, \xi_{20}^4 + 6\xi_{20}^3 + 36\xi_{20}^2 + 31\xi_{20} + 1\rangle$. *Como* $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_1} \cong GF(17^4)$, *pelo Corolŕio 4.2.2 segue que* $\varphi(\xi_{20} \ (mod\ \mathcal{P}_1)) = \beta$, *onde* $\beta \in GF(17^4)$ *é uma raiz do polinômio* $m_1(x) = x^4 + 31x^3 + 36x^2 + 6x + 1$ *em* $GF(17)[x]$. *Logo,* $\beta^4 + 31\beta^3 + 36\beta^2 + 6\beta + 1 = 0$, *ou seja,* $\beta^4 = 3\beta^3 + 15\beta^2 + 11\beta + 16$ $(mod\ 17)$ *e assim,* $\beta^5 = \beta^4\beta = 7\beta^3 + 5\beta^2 + 15\beta + 14$, $\beta^6 = \beta^5\beta = 9\beta^3 + \beta^2 + 6\beta + 10$ *e* $\beta^7 = \beta^6\beta = 11\beta^3 + 5\beta^2 + 7\beta + 8$ $(mod\ 17)$. *Deste modo, o rotulamento linear é dado por*

$$\begin{aligned} l(\alpha) &= a_0 l(\sigma(1)) + a_1 l(\sigma(\xi_{20})) + a_2 l(\sigma(\xi_{20})^2) + a_3 l(\sigma(\xi_{20})^3)) + \ldots + a_7 l(\sigma(\xi_{20})^7)) \\ &= a_0 + a_1\beta + a_2(\beta)^2 + a_3(\beta)^3 + \ldots + a_7(\beta)^7 \\ &= a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 + a_4(3\beta^3 + \beta^2 + 6\beta + 10) \\ &= (a_0 + 16a_4 + 14a_5 + 10a_6 + 8a_7) + (a_1 + 11a_4 + 15a_5 + 6a_6 + 7a_7)\beta \\ &\quad + (a_2 + 15a_4 + 5a_5 + a_6 + 5a_7)\beta^2 + (a_3 + 3a_4 + 7a_5 + 9a_6 + 11a_7)\beta^3 \ (mod\ 17), \end{aligned}$$

n qual $\alpha = \sigma(a_0 + a_1\xi_{20} + a_2\xi_{20}^2 + a_3\xi_{20}^3 + \ldots + a_7\xi_{20}^7)$ *e* $a_i \in \mathbb{Z}$, *para* $0 \leq i \leq 7$.

Exemplo 4.2.6. *No Exemplo 4.2.5 tomando $m(x)$ módulo 41, obtemos que*

$$m(x) = (x+20)(x+8)(x+36)(x+2)(x+39)(x+21)(x+33)(x+5) \ (mod\ \mathbb{Z}_{41}[x]).$$

Assim, pelo Lema de Kummer, temos que

$$41\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1\mathcal{P}_2\ldots\mathcal{P}_8,$$

onde $\mathcal{P}_1 = \langle 41, \xi_{20}+20\rangle$, $\mathcal{P}_2 = \langle 41, \xi_{20}+8\rangle, \ldots,$ $\mathcal{P}_8 = \langle 41, \xi_{20}+5\rangle$. Como $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_1} \cong GF(41)$, segue que $\alpha \equiv 20\ (mod\ \mathcal{P}_1)$. Deste modo, o rotulamento linear é dado por

$$\begin{aligned} l(\alpha) &= a_0 l(\sigma(1)) + a_1 l(\sigma(\xi_{20})) + a_2 l(\sigma(\xi_{20})^2) + a_3 l(\sigma(\xi_{20})^3) + \ldots + a_7 l(\sigma(\xi_{20})^7) \\ &= a_0 + 20a_1 + (20)^2 a_2 + (20)^3 a_3 + (20)^4 a_4 + (20)^5 a_5 + (20)^6 a_6 + (20)^7 a_7 \\ &= a_0 + 20a_1 + 31a_2 + 5a_3 + 18a_4 + 32a_5 + 25a_6 + 8a_7\ (mod\ 41), \end{aligned}$$

na qual $\alpha = \sigma(a_0 + a_1\xi_{20} + a_2\xi_{20}^2 + a_3\xi_{20}^3 + \ldots + a_7\xi_{20}^7)$ e $a_i \in \mathbb{Z}$, para $0 \leq i \leq 7$.

4.3 Região de Voronoi e distância máxima

Nesta seção, veremos o conceito da região de Voronoi, bem como a distância máxima de Mannheim entre os elementos de $A_p[\rho]$, em que $\rho = w = \frac{1+\sqrt{-3}}{2}$, isto é, no caso em que $d = -3$ (para $A_p[i]$ é ánalogo).

Sejam $\mathbb{Z}[w]$, na qual $w = \frac{1+\sqrt{-3}}{2}$, o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{-3})$ e um elemento $\pi = a + bw \in \mathbb{Z}[w]$ com $N(\pi) = a^2 + ab + b^2 = p$, em que $p \equiv 1$ $(mod\ 6)$. Assim, o ideal $p\mathbb{Z}$ decompõe-se completamente em $\mathbb{Z}[w]$. Podemos assumir sempre que $a, b > 0$, uma vez que o anel de inteiros algébricos $\mathbb{Z}[w]$ é um domínio em que vale a fatoração única a menos das unidades. Assim, usando a noção de elementos associados, temos que a fatoração é única a menos de primos associados. As unidades de $\mathbb{Z}[w]$ são w^j, para $j = 0, 1, \ldots, 5$. Se $\pi = a + bw$, então $w\pi = -b + (a+b)w$, $w^2\pi = -(a+b) + aw$, $w^3\pi = -a - bw$, $w^4\pi = b - (a+b)w$ e $w^5\pi = (a+b) - aw$. Expressando em termos de coordenadas cartesianas, se $\pi = (a, b)$, então $w\pi = (-b, a+b)$, $w^2\pi = (-(a+b), a)$, $w^3\pi = (-a, -b)$, $w^4\pi = (b, -(a+b))$

e $w^5\pi = (a+b, -a)$. Se $a, b < 0$, então multiplicando π por $w^3 = -1$, temos que $\pi = -a - bw$, com $-a, -b > 0$. Se $a > 0$ e $b < 0$, então multiplicando π por w tem-se que $\pi w = aw + bw^2 = aw + b(w-1) = (a+b)w - b$. Deste modo, temos dois casos a considerar:

1. Se $a + b > 0$, então $a > -b > 0$.

2. Se $a + b < 0$, então multiplicando π por w^2, temos que $\pi w^2 = (a + bw)w^2 = aw^2 + bw^3 = a(w-1) - b = aw - a - b = -(a+b) + aw$, em que $-(a+b) > 0$ e $a > 0$. Se $a < 0$ e $b > 0$, então é suficiente trocarmos a por b.

Portanto, qualquer relação envolvendo a e b pode ser reduzida ao caso de $a, b > 0$, escolhendo uma unidade conveniente e multiplicando por π.

Definição 4.3.1. *Sejam S um subconjunto discreto do $\mathbb{R}^n$ e $x_0 \in S$. A região de Voronoi de x_0 em S consiste dos pontos do $\mathbb{R}^n$ que estão mais próximos de x_0 do que de qualquer outro ponto de S, ou seja,*

$$\mathcal{V}_S(x_0) = \{x \in \mathbb{R}^n : d(x, x_0) \leq d(x, y), \forall\ y \in S, y \neq x_0\}. \tag{4.2}$$

Dizemos que um ponto y de S, $y \neq x$ é um vizinho de x se $d(x, y) \leq d(x, z)$, para todo z de S.

Os casos mais interessantes são aqueles que o subconjunto discreto S do $\mathbb{R}^2$ tenha estrutura de um $\mathbb{Z}$-módulo, ou seja, quando S é um reticulado. Assim, quando x é um ponto do reticulado S, temos que $\mathcal{V}_S(x) = x + \mathcal{V}_S(O)$ e y é um vizinho de x se, e somente se, $y - x$ é um vizinho da origem.

A imagem via o homomorfismo canônico do anel de inteiros $\mathbb{Z}[\rho]$ pode ser visto como um reticulado no $\mathbb{R}^2$ gerado por $\{1, \rho\}$, na qual $\rho = \sqrt{-1} = i$ se $d = -1$ e $\rho = w = \frac{1+\sqrt{-3}}{2}$ se $d = -3$. Seja S um subreticulado de $\mathbb{Z}[w]$ gerado por $\{\pi, w\pi\}$, em que $\pi = a + bw \in \mathbb{Z}[w]$ e tal que $N(\pi) = p$, com $p \equiv 1\ (mod\ 6)$. Em $\mathbb{Z}[w]$ os vizinhos da origem são as raízes sextas da unidade, isto é, w^j para $j = 0, 1, \ldots, 5$.

Proposição 4.3.1. *([13], p. 80) Os vizinhos da origem do subreticulado S de $\mathbb{Z}[w]$ gerado por $\{\pi, w\pi\}$ são do tipo πw^j, em que $j = 0, 1, \ldots, 5$.*

Demonstração: Se $\alpha \in \langle\pi\rangle$, então $\alpha = \gamma\pi$, onde $\gamma \in \mathbb{Z}[w]$. Se d é a distância euclidiana, então $d^2(\alpha, 0) = \alpha^2 = N(\alpha) = N(\gamma\pi) = N(\gamma)N(\pi)$. Se α é um vizinho da origem, então sua distância a origem deve ser mínima. Logo, $N(\gamma) = 1$. Assim, γ é uma unidade em $\mathbb{Z}[w]$. Portanto, $\gamma = w^j$ e $\alpha = w^j\pi$, $j = 0, 1, \ldots, 5$. ■

Nosso objetivo, é determinar a distância máxima de Mannheim entre os pontos de $A_p[w]$. Para isso, identificamos $\mathbb{Z}[w]$ com um subconjunto de $\mathbb{R}^2$. Se $\pi \in \mathbb{Z}[w]$ com $\pi \neq 0$, então $\pi = a + bw$, com $a, b \in \mathbb{Z}$. Consideramos os segmentos de reta com extremidades na origem e nos pontos $w^j\pi$, para $j = 0, 1, \ldots, 5$. Tomemos a reta perpendicular passando pelo ponto médio de cada um desses segmentos de reta. As intersecções das retas traçadas formam os vértices de um hexágono $\mathcal{H}$, que chamamos de C_l, para $l = 1, 2, \ldots, 6$. Temos que $\pi = a + bw$, com $w = \frac{1+\sqrt{-3}}{2}$, tem coordenadas (a, b) na base $\{1, w\}$ e coordenadas $(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2})$ na base canônica $\{1, i\}$, na qual é associado com as coordenadas de C_l, para $l = 1, 2, \ldots, 6$. Consideramos $\pi' = (\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})$ na base $\{1, i\}$ um vetor ortogonal a π. Queremos agora, determinar as coordenadas dos pontos C_l, para $l = 1, 2, \ldots, 6$, na base $\{1, w\}$ que são os vértices do hexágono $\mathcal{H}$. Temos que

$$\vec{OC_1} = \frac{\pi}{2} + \frac{1}{2}\frac{|\pi'|\sqrt{3}}{|\pi'|}\frac{\sqrt{3}}{3}\pi' = \frac{\pi}{2} + \frac{\sqrt{3}}{6}\pi' = \frac{1}{2}(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}) + \frac{\sqrt{3}}{6}(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2}).$$

Assim, sendo $\pi = (a, b)$, segue que

$$\begin{aligned} 2\vec{OC_1} &= 2[\tfrac{1}{2}(\tfrac{2a+b}{2}, \tfrac{b\sqrt{3}}{2}) + \tfrac{\sqrt{3}}{6}(\tfrac{-b\sqrt{3}}{2}, \tfrac{2a+b}{2})] \\ &= (\tfrac{2a+b}{2}, \tfrac{b\sqrt{3}}{2}) + \tfrac{\sqrt{3}}{3}(\tfrac{-b\sqrt{3}}{2}, \tfrac{2a+b}{2}). \end{aligned}$$

Agora,

$$\begin{aligned} 4\vec{OC_1} &= 2(2\vec{OC_1}) = 2[(\tfrac{2a+b}{2}, \tfrac{b\sqrt{3}}{2}) + \tfrac{\sqrt{3}}{3}(\tfrac{-b\sqrt{3}}{2}, \tfrac{2a+b}{2}) \\ &= (2a+b, b\sqrt{3}) + (-b, \tfrac{(2a+b)\sqrt{3}}{3}) = (2a, \tfrac{2(a+b)\sqrt{3}}{3}). \end{aligned}$$

Logo,

$$\vec{OC_1} = (\frac{a}{2}, \frac{(a+2b)}{6}\sqrt{3}).$$

Também, podemos escrever

$$\begin{aligned}\vec{OC_1} &= \frac{a}{2} + \frac{(a+2b)}{2}w = \frac{a}{2} + (\frac{a+2b}{2})(\frac{1+\sqrt{-3}}{2}) = \frac{a}{2} + \frac{(a+2b)i\sqrt{3}}{2} \\ &= \frac{a}{2} + \frac{a+2b}{3}(\frac{-\sqrt{-3}}{2}) + \frac{a+2b}{6} - \frac{(a+2b)}{6} \\ &= (\frac{a+2b}{3})(\frac{1+\sqrt{-3}}{2}) + \frac{3a-a-2b}{6} = \frac{a-b}{3} + \frac{(a+2b)}{3}w.\end{aligned}$$

Portanto, na base $\{1, w\}$, as coordenadas de C_1 são $C_1 = (\frac{a-b}{3}, \frac{a+2b}{3})$. As coordenadas dos pontos C_l, para $l = 2, 3, \ldots, 6$, podem ser obtidos das coordenadas C_1 como $C_l = w^{l-1}C_1$. Assim, obtemos as coordenadas do hexágono $\mathcal{H}$:

$$\begin{aligned}C_2 &= (\frac{-(a+2b)}{3}, \frac{2a+b}{3}), \\ C_3 &= (\frac{-(2a+b)}{3}, \frac{a-b}{3}), \\ C_4 &= (\frac{-(a-b)}{3}, \frac{-(a+2b)}{3}), \\ C_5 &= (\frac{a+2b}{3}, \frac{-(2a+b)}{3}) \text{ e} \\ C_6 &= (\frac{2a+b}{3}, \frac{-(a-b)}{3}).\end{aligned}$$

Sejam as regiões semi-abertas R_1, R_2 e R_3 limitadas, respectivamentes, pelos pares de retas determinadas por C_1C_6 e C_3C_4, C_1C_2 e C_4C_5, C_2C_3 e C_5C_6, isto é,

$$R_1 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (a+2b)y + (2a+b)x \leq N(\pi)\};$$

$$R_2 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (2a+b)y + (a-b)x \leq N(\pi)\};$$

$$R_3 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (a-b)y - (a+2b)x \leq N(\pi)\}.$$

Seja R a intersecção dessas regiões, ou seja, $R = \bigcap_{i=1}^{3} R_i$. O conjunto R tem como fronteira o hexágono $\mathcal{H}$. Agora, queremos determinar as coordenadas inteiras na base $\{1, w\}$ dos pontos de R mais próximos dos vértices de $\mathcal{H}$ e assim, mais distantes da origem. Deste modo, dado $\pi = a + bw \in \mathbb{Z}[w]$, precisamos analisar três casos da diferença $a - b$. Podemos considerar o caso em que $a, b > 0$ e sem perda de generalidade, podemos supor que $a > b$, pois os resultados para o caso

$b > a$ são obtidos somente trocando a por b. Os resultados a seguir, segue que de ([13], p. 82).

1. Se $a-b \equiv 0\ (mod\ 3)$, então $a-b \equiv 0\ (mod\ 3)$ e $p = a^2+ab+b^2 = 3a^2\ (mod\ 3)$. Isto implica, que p não é primo. Logo, este caso é excluído.

2. Se $a - b \equiv 1\ (mod\ 3)$, então tomando C_j^1, para $j = 1, 2, \ldots, 6$, os pontos de coordenadas inteiras na base $\{1, w\}$ mais próximos de C_j, temos que

$$C_1^1 = (\frac{a-b-1}{3}, \frac{a+2b-1}{3}),$$
$$C_2^1 = (\frac{-a-2b+1}{3}, \frac{2a+b-2}{3}),$$
$$C_3^1 = (\frac{-2a-b+2}{3}, \frac{a-b-1}{3}),$$
$$C_4^1 = (\frac{-a+b+1}{3}, \frac{-a-2b+1}{3}),$$
$$C_5^1 = (\frac{a+2b-1}{3}, \frac{-2a-b+2}{3}) \text{ e}$$
$$C_6^1 = (\frac{2a+b-2}{3}, \frac{-a+b+1}{3}).$$

3. Se $a - b \equiv 2\ (mod\ 3)$, então tomando C_j^2, para $j = 1, 2, \ldots, 6$, os pontos de coordenadas inteiras da base $\{1, w\}$ mais próximos de C_j, temos que

$$C_1^2 = (\frac{a-b-2}{3}, \frac{a+2b-2}{3}),$$
$$C_2^2 = (\frac{-a-2b+2}{3}, \frac{2a+b-1}{3}),$$
$$C_3^2 = (\frac{-2a-b+1}{3}, \frac{a-b-2}{3}),$$
$$C_4^2 = (\frac{-a+b+2}{3}, \frac{-a-2b+2}{3}),$$
$$C_5^2 = (\frac{a+2b-2}{3}, \frac{-2a-b+1}{3}) \text{ e}$$
$$C_6^2 = (\frac{2a+b-1}{3}, \frac{-a+b+2}{3}).$$

Agora, nosso objetivo é encontrar as relações entre os conjuntos $\mathbb{Z}[\rho]$, R, S e $\mathcal{H}$. Assim, consideremos os seguintes resultados.

Lema 4.3.1. *([13], p. 84) Se* $\mathcal{V} = \mathcal{V}_S(O) = \{x \in \mathbb{R}^2 : d(x,O) \leq d(x,y), \forall\ y \in S, y \neq O\}$ *é a região de Voronoi da origem* S*, então* $\mathcal{V} = R$*.*

Demonstração: Seja $\alpha \in \mathcal{V}$ tal que $\alpha \notin R = \bigcap_{i=1}^{3} R_i$. Assim, $\alpha \notin R_i$, para algum $i \in \{1,2,3\}$. Sem perda de generalidade, podemos supor que $\alpha \notin R_1$, ou seja, $d(\alpha,\pi) \leq d(\alpha,O)$ ou $d(\alpha,-\pi) \leq d(\alpha,O)$. Logo, $\alpha \in \mathcal{V}$ que é um absurdo. Portanto, $\mathcal{V} \subset R$. Reciprocamente, sejam $\alpha \in R$ e $x \in S$, $x \neq 0$. Suponhamos, por absurdo, que $d(\alpha,x) < d(\alpha,O)$, isto é, $\alpha \notin V$. Assim, $d(\alpha,x) < d(\alpha,O) \leq \sqrt{\frac{N(\pi)}{3}}$. Logo, $d(x,O) \leq d(x,\alpha) + d(\alpha,O) \leq 2\sqrt{\frac{N(\pi)}{3}}$. Como $x \in S$, segue que $x = \pi\gamma$, com $\gamma \in \mathbb{Z}[w]$. Calculando a norma, temos que $N(x) = N(\pi)N(\gamma)$, o que implica que $N(\gamma) = 1$ ou $N(\gamma) > 1$. Se $N(\gamma) = 1$, então $\gamma = w^j$, para $j = 0,1,\ldots,5$, isto é, γ é uma unidade de $\mathbb{Z}[w]$. Suponhamos que $\gamma = \pm 1$, ou seja, $\gamma = 1$ e $\gamma = w^3 = -1$. Como $\alpha \in R = \bigcap_{i=1}^{3} R_i$, segue que $\alpha \in R_1$, ou seja, $d(\alpha,O) < d(\alpha,\pi)$ e $d(\alpha,O) < d(\alpha,-\pi)$, que é um absurdo, uma vez que $d(\alpha,x) < d(\alpha,O)$, para todo $x \in S$. Portanto, $i \neq 0,3$. Analogamente, tem-se que $i \neq 1,2,4,5$. Agora se, $N(\gamma) > 1$, então $d(x,O) \geq \sqrt{2N(\pi)}$. Assim, $\sqrt{N(\pi)} \leq d(x,O) \leq 2\sqrt{\frac{N(\pi)}{3}}$, que também é um absurdo. Portanto, a nossa hipótese $d(\alpha,x) < d(\alpha,O)$ é falsa e assim, $\alpha \in \mathcal{V}$. Logo, $R \subset \mathcal{V}$. ■

Lema 4.3.2. *([13], p. 84) Os pontos de coordenadas inteiras de* R *formam um conjunto completo de representantes das classes laterais módulo o ideal gerado por* π*, em que* $\pi \in \mathbb{Z}[w]$*.*

Demonstração: Seja $\mathcal{V}_S(O)$ a região de Voronoi da origem do subreticulado S. Pelo Lema 4.3.1, temos que $R = \mathcal{V}_S(O)$. Também tem-se que $\mathcal{V}_S(O)$ é um mosaico do $\mathbb{R}^2$, isto é, $\mathbb{R}^2 = \bigcup_{x \in S}(x + \mathcal{V}_S(O))$. Temos que esta união é disjunta exceto possivelmente pelas arestas que podem se auto-interceptarem. Logo, para qualquer $y \in \mathbb{Z}[w]$, tem-se que existe um único $x \in S$ tal que $y \in x + \mathcal{V}_S(O)$ e assim, $y - x = \tilde{y} \in \mathcal{V}_S(O) = R$. Portanto, para todo $y \in \mathbb{Z}[w]$, temos que $y \equiv \tilde{y}\ (mod\ \langle\pi\rangle)$, isto é, em R sempre existe um representante do conjunto de classes laterais $(mod\ \langle\pi\rangle)$. Para a unicidade, suponhamos que existem $\alpha, \beta \in R$ tal que $\alpha \equiv \beta\ (mod\ \langle\pi\rangle)$.

Assim, $\alpha - \beta = \gamma\pi$, para algum $\gamma \in \mathbb{Z}[w]$ e $d(\alpha, \beta) = d(\alpha - \beta, O) = d(\gamma\pi, O) = \sqrt{N(\gamma\pi)} = \sqrt{N(\gamma)N(\pi)}$. Deste modo, temos as seguintes possibilidades:

1. Se $N(\gamma) \geq 2$, então $\sqrt{2N(\pi)} \leq d(\alpha, \beta) \leq d(\alpha, O) + d(\beta, O) \leq 2\sqrt{\frac{N(\pi)}{3}}$. Logo, $2N(\pi) \leq 4\frac{N(\pi)}{3}$, que é um absurdo.

2. Se $N(\gamma) = 1$, então $\alpha - \beta = \gamma\pi = w^j\pi$, para $j = 0, 1, \ldots, 5$. Se $j = 0$, então $\alpha - \beta = \pi$, ou seja, $\alpha = \pi + \beta$. Como $\beta \in R = \bigcap_{i=1}^{3} R_i$, segue que $\pi + \beta \notin R_1$ e portanto, $\alpha \notin R_1$. Logo, $\alpha \notin R$, que é um absurdo. De modo análogo, para $j = 1, 2, 3, 4, 5$. Deste modo, temos a unicidade. ■

Lema 4.3.3. *([13], p. 85) O conjunto S é obtido a partir de $\mathbb{Z}[w]$ através de uma rotação seguida de uma homotetia. Além disso, a região de Voronoi da origem de S é obtida da região de Voronoi da origem de $\mathbb{Z}[w]$ pela mesma ação. A rotação é determinada por $\theta = arg(\pi)$ e a homotetia sendo a multiplicação por $\sqrt{N(\pi)}$, em que $\pi = a + bw \in \mathbb{Z}[w]$, com $a, b \in \mathbb{Z}$.*

Demonstração: Seja $\pi \in \mathbb{Z}[w]$. Temos que π pode ser escrito como $\pi = e^{i\theta}\sqrt{N(\pi)}$. Como o ideal gerado por π é o mesmo ideal gerado por $w^j\pi$, para $j = 0, 1, \ldots, 5$, podemos considerar $0 \leq \theta \leq 60^o$, uma vez que $w = \frac{1+\sqrt{-3}}{2}$ é uma raiz sexta da unidade e deste modo, existe $j \in \{0, 1, \ldots, 5\}$ tal que $0 \leq arg(w^j\pi) \leq 60^o$. Assim, podemos considerar sem perda de generalidade, que $0 \leq \theta \leq 60^o$. Seja a rotação $\psi : \mathbb{R}^2 \to \mathbb{R}^2$ definida por:

$$\psi(x, y) = (x\cos(\theta) - y\text{sen}(\theta), x\text{sen}(\theta) + y\cos(\theta)),$$

e a homotetia $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ definida por:

$$\phi(x, y) = (x, y)\sqrt{N(\pi)}.$$

Seja $\Psi = \phi \circ \psi$. Identificando S como um subconjunto de $\mathbb{R}^2$, temos que 1 e

$w = \frac{1+\sqrt{-3}}{2}$ podem ser vistos como os pares $(1,0)$ e $(\frac{1}{2}, \frac{\sqrt{3}}{2})$ e portanto,

$$\begin{aligned}
\Psi(1) &= \sigma(1,0) = \Psi(\psi(1,0)) = \phi(\cos(\theta), \text{sen}(\theta)) = (\cos(\theta), \text{sen}(\theta))\sqrt{N(\pi)} = \pi \quad \text{e} \\
\Psi(w) &= \Psi(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}) = \phi(\psi(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2})) = \phi(\tfrac{1}{2}\cos(\theta) - \tfrac{\sqrt{3}}{2}\text{sen}(\theta), \tfrac{1}{2}\text{sen}(\theta) + \tfrac{\sqrt{3}}{2}\cos(\theta)) \\
&= \sqrt{N(\phi)}(\tfrac{1}{2}\cos(\theta) - \tfrac{\sqrt{3}}{2}\text{sen}(\theta), \tfrac{1}{2}\text{sen}(\theta) + \tfrac{\sqrt{3}}{2}\cos(\theta)) \\
&= \sqrt{N(\phi)}(\cos(\theta) + i\text{sen}(\theta))(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}) \\
&= w\pi.
\end{aligned}$$

Assim, Ψ leva 1 em π e w em $w\pi$ e por linearidade, Ψ leva $\mathbb{Z}[w] = \mathbb{Z} + \mathbb{Z}w$ em $S = \mathbb{Z}\pi + \mathbb{Z}w\pi$. Além disso, Ψ leva a região de Voronoi da origem de $\mathbb{Z}[w]$ na região de Voronoi da origem de S. ■

O próximo teorema estabelece as relações entre $\mathbb{Z}[w]$, R, S e $\mathcal{H}$.

Teorema 4.3.1. *([13], p. 86)*

1. *Os pontos de coordenadas inteiras na base $\{1, w\}$ localizados no interior de $\mathcal{H}$ formam um conjunto completo de representantes das classes laterais módulo o ideal gerado por π, em que $\pi \in \mathbb{Z}[w]$.*

2. *O conjunto R pode ser visto como uma região de Voronoi da origem do sub-reticulado S.*

3. *A região R pode ser vista como uma rotação seguida de uma homotetia da região de Voronoi da origem do reticulado $\mathbb{Z}[w]$.*

Demonstração: Segue do Lemas 4.3.1, 4.3.2 e 4.3.3. ■

Observação 4.3.1.

1. *Se $\mathcal{Q}$ é um quadrado de vértices:*

$$\begin{aligned}
C_1 &= (\frac{a-b}{2}, \frac{a+2b}{2}), \\
C_2 &= (\frac{-(a+2b)}{2}, \frac{2a+b}{2}), \\
C_3 &= (\frac{-(a-b)}{2}, \frac{-(a+2b)}{2}) \quad e \\
C_4 &= (\frac{a+2b}{2}, \frac{-(2a+b)}{2}),
\end{aligned}$$

então as coordenadas de R mais próximos do vértices de $\mathcal{Q}$ e mais distantes da origem são:

- *Se $a-b \equiv 1 \pmod 2$, então*

$$C_1^1 = (\frac{a-b-1}{2}, \frac{a+2b-1}{2});$$
$$C_2^1 = (\frac{-a-2b+1}{2}, \frac{2a+b-2}{2});$$
$$C_3^1 = (\frac{-a+b+1}{2}, \frac{-a-2b+1}{2}) \quad e$$
$$C_1^4 = (\frac{a+2b-1}{2}, \frac{-2a-b+2}{2}).$$

- *Se $a-b \equiv 2 \pmod 2$, então*

$$C_1^2 = (\frac{a-b-2}{2}, \frac{a+2b-2}{2});$$
$$C_2^2 = (\frac{-a-2b+2}{2}, \frac{2a+b-1}{2});$$
$$C_3^2 = (\frac{-a+b+2}{2}, \frac{-a-2b+2}{2}) \quad e$$
$$C_4^2 = (\frac{a+2b-2}{2}, \frac{-2a-b+1}{2}).$$

2. *Para os corpos quadráticos $\mathbb{Q}(\sqrt{d})$, com $d \equiv 2, 3 \pmod 4$, temos que as regiões R são retângulos.*

Exemplo 4.3.1. *Sejam $d = -3$ e $p = 13$, pelo Exemplo 2.3.2, podemos tomar $\pi = -1 + 4w = (-1, 4)$, em que $a = -1$ e $b = 4$. Como $a - b \equiv 1 \pmod 3$, segue que a região Voronoi R é um hexágono de vértices: $C_1^1 = (-2, 2)$, $C_2^1 = (-2, 0)$, $C_3^1 = (0, -2)$, $C_4^1 = (2, -2)$, $C_5^1 = (2, 0)$ e $C_6^1 = (0, 2)$. Assim, o hexágono $\mathcal{H}$ tem coordenadas: $A = (\frac{-5}{3}, \frac{7}{3})$, $B = (\frac{-7}{3}, \frac{2}{3})$, $C = (\frac{-2}{3}, \frac{-5}{3})$, $D = (\frac{5}{3}, \frac{-7}{3})$, $E = (\frac{7}{3}, \frac{-2}{3})$ e $F = (\frac{2}{3}, \frac{5}{3})$. A Figura 4.5, mostra o conjunto de sinais $A_{13}[w]$ representado na região R.*

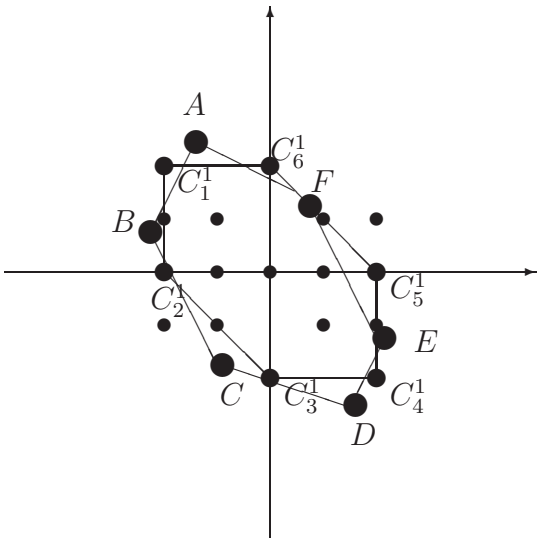

Figura 4.5

Exemplo 4.3.2. *Sejam* $d = -3$ *e* $p = 19$*, pelo Exemplo 2.3.3, podemos tomar* $\pi = -5 + 2w = (-5, 2)$*, em que* $a = -5$ *e* $b = 2$*. Como* $a - b \equiv 2 \pmod 3$*, segue que a região de Voronoi* R *é um hexágono de vértices* $C_1^2 = (-3, -1)$*,* $C_2^2 = (1, -3)$*,* $C_3^2 = (3, -3)$*,* $C_4^2 = (3, 1)$*,* $C_5^2 = (-1, 3)$ *e* $C_6^2 = (-3, 3)$*. Assim, o hexágono* $\mathcal{H}$ *tem coordenadas:* $A = (\frac{-7}{3}, \frac{-1}{3})$*,* $B = (\frac{1}{3}, \frac{-8}{3})$*,* $C = (\frac{8}{3}, \frac{-7}{3})$*,* $D = (\frac{7}{3}, \frac{1}{3})$*,* $E = (\frac{-1}{3}, \frac{8}{3})$ *e* $F = (\frac{-8}{3}, \frac{7}{3})$*. A Figura* 4.6*, mostra o conjunto de sinais de* $A_{19}[w]$*, representado na região* R*.*

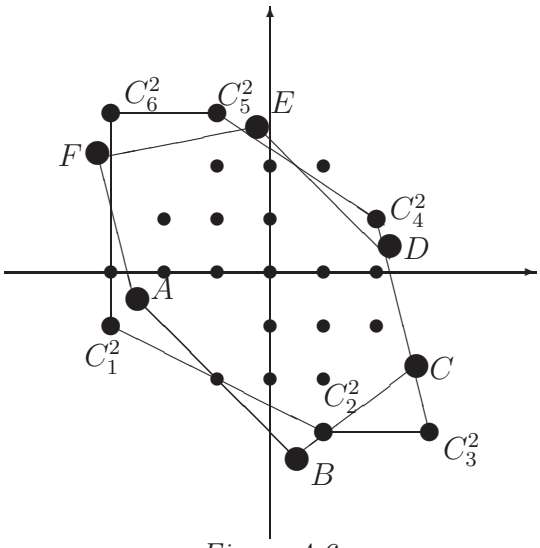

Figura 4.6

Exemplo 4.3.3. *([13], p. 88) Sejam* $d = -3$ *e* $p = 43$*, pelo Exemplo 2.3.6, podemos tomar* $\pi = 6 + w = (6, 1)$*, em que* $a = 6$ *e* $b = 1$*. Como* $a - b \equiv 2 \pmod 3$*, segue*

que a região de Voronoi R é um hexágono de vértices $C_1^2 = (1,2)$, $C_2^2 = (-2,4)$, $C_3^2 = (-4,1)$, $C_4^2 = (-1,-2)$, $C_5^2 = (2,-4)$ e $C_6^2 = (4,-1)$. Assim, o hexágono $\mathcal{H}$ tem coordenadas $A = (\frac{5}{3}, \frac{7}{3})$, $B = (\frac{-7}{3}, \frac{13}{3})$, $C = (\frac{-13}{3}, \frac{5}{3})$, $D = (\frac{-5}{3}, \frac{-7}{3})$, $E = (\frac{7}{3}, \frac{-13}{3})$ e $F = (\frac{13}{3}, \frac{-5}{3})$. A Figura 4.7, mostra o conjuto de sinais $A_{43}[w]$ representado na região R.

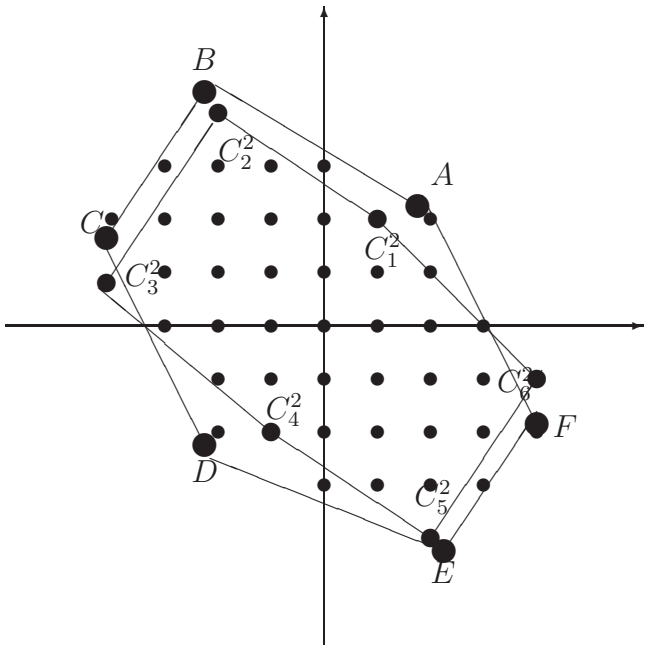

Figura 4.7

Exemplo 4.3.4. *Sejam $d = -1$ e $p = 13$, pelo Exemplo 2.3.8, podemos tomar $\pi = 3 + 2i = (3,2)$, em que $a = 3$ e $b = 2$. Como $a - b \equiv 1 \pmod 2$, segue que a região de Voronoi R é um quadrado de vértices $C_1^1 = (0,3)$, $C_2^1 = (-4,3)$, $C_3^1 = (0,-3)$ e $C_4^1 = (4,-3)$. Assim, o quadrado $\mathcal{Q}$ tem coordenadas $A = (\frac{1}{2}, \frac{7}{2})$, $B = (\frac{-7}{2}, 4)$, $C = (\frac{-1}{2}, \frac{-7}{2})$ e $D = (\frac{7}{2}, -4)$. A Figura 4.8, mostra o conjunto de sinais $A_{13}[i]$ representado na região R.*

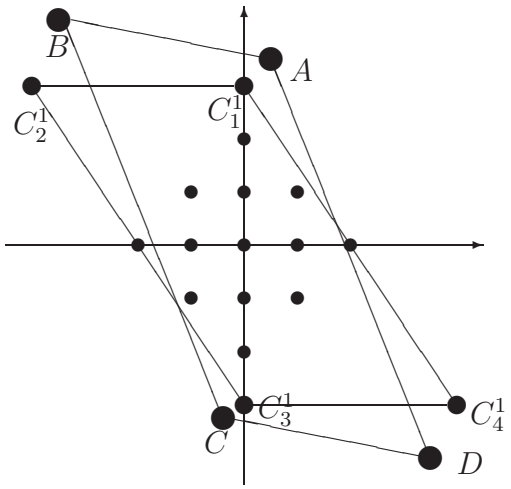

Figura 4.8

Exemplo 4.3.5. *Sejam* $d = -1$ *e* $p = 17$*, pelo Exemplo 2.3.9, podemos tomar* $\pi = 4 + i = (4, 1)$*, em que* $a = 4$ *e* $b = 1$*. Como* $a - b \equiv 1 \ (mod\ 2)$*, segue que a região de Voronoi* R *é um quadrado regular de vértices* $C_1^1 = (1, \frac{5}{2})$*,* $C_2^1 = (\frac{-5}{2}, \frac{7}{2})$*,* $C_3^1 = (-1, \frac{-5}{2})$ *e* $C_4^1 = (\frac{5}{2}, \frac{-7}{2})$*. Assim, o quadrado* $\mathcal{Q}$ *tem coordenadas* $A = (\frac{3}{2}, 2$*,* $B = (-3, \frac{9}{2})$*,* $C = (\frac{-3}{2}), -3$ *e* $D = (3, \frac{-9}{2})$*. A Figura* 4.9*, mostra o conjunto de sinais* $A_{17}[i]$ *representado na região* R*.*

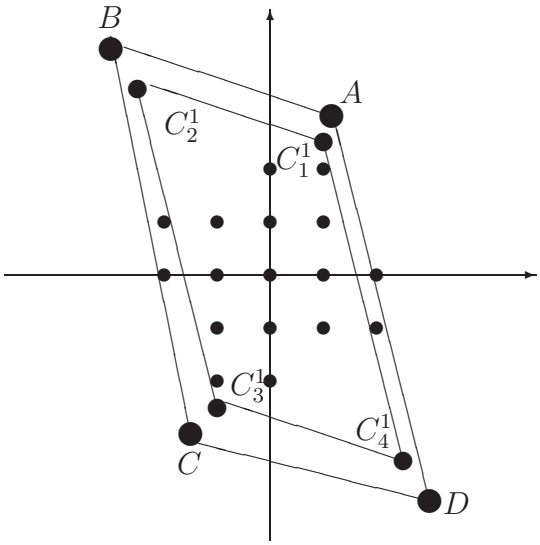

Figura 4.9

Exemplo 4.3.6. *([13], p. 87) Sejam* $d = -1$ *e* $p = 29$*, pelo Exemplo 2.3.10, podemos tomar* $\pi = 5 + 2i = (5, 2)$*, em que* $a = 5$ *e* $b = 2$*. Como* $a - b \equiv 1 \ (mod\ 2)$*, segue que a região de Voronoi* R *é um quadrado regular de vértices* $C_1^1 = (1, 4)$*,* $C_2^1 = (-4, 5)$*,* $C_3^1 = (-1, -4)$ *e* $C_4^1 = (4, -5)$*. Assim, o quadrado* $\mathcal{Q}$ *tem coordenadas* $A = (\frac{3}{2}, \frac{9}{2})$*,* $B = (\frac{-9}{2}, 6)$*,* $C = (\frac{-3}{2}, \frac{-9}{2})$ *e* $D = (\frac{9}{2}, -6)$*. A Figura* 4.10*, mostra o conjunto de sinais* $A_{29}[i]$ *representado na região* R*.*

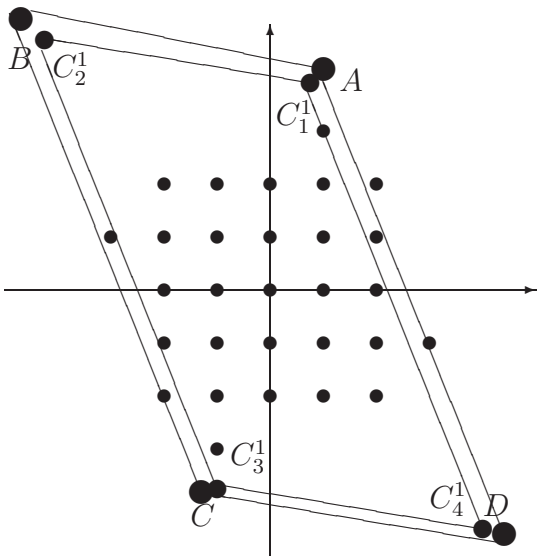

Figura 4.10

Capítulo 5

Códigos via corpos quadráticos e ciclotômicos

5.1 Introdução

Via o anel de inteiros Gaussianos e o anel de inteiros de Eisenstein-Jacobi, Huber ([1] e [2]) apresentou um método de construir códigos sobre corpos finitos para sinais bi-dimensionais. A idéia foi considerar um corpo finito sendo o quociente destes anéis por um ideal primo. Através da norma de Galois juntamente com o algoritmo da divisão euclidiana mostrou que em cada classe lateral existe um único elemento de norma mínima. Assim, Huber introduziu a distância de Mannheim e construiu códigos lineares com capacidade de correção de um erro de Mannheim. Nóbrega et. al [3], propuseram uma nova classe de códigos lineares via a métrica de Mannheim também sobre os anéis de inteiros de Eisenstein-Jacobi. Fan et.al [7] considerou os anéis de inteiros de corpos ciclôtomicos e via um ideal primo, que é um corpo finito, construiu códigos lineares para sinais multidimensionais definindo uma métrica que também chamou de Mannheim que é sutilmente diferente da métrica definida por Huber. Por sua vez, Dong et. al [8] e [9], considerou os anéis de inteiros algébricos de corpos ciclôtomicos que são domínios de ideais principais e, via o quociente desses anéis por um elemento irredutível, que é um corpo finito, construiu

códigos sobre esses corpos com capacidade de corrigir um erro que pertença ao grupo cíclico do grupo multiplicativo do corpo finito. Neste sentido, códigos lineares sobre corpos finitos para sinais multidimensionais foram construídos, mas não encontrou um norma conveniente para estender o peso de Mannheim.

Assim, neste capítulo, veremos códigos corretores de um erro via os corpos quadráticos e via os corpos ciclotômicos.

5.2 Códigos via corpos quadráticos

Nesta seção, nosso objetivo é definir códigos constacíclicos sobre o corpo finito $A_p[\rho]$, em que $\rho = w = \frac{1+\sqrt{-3}}{2}$ ou $\rho = i$, obtido via os anéis de inteiros algébricos $\mathbb{Z}[w]$ e $\mathbb{Z}[i]$, respectivamente. A definição desses códigos depende da cardinalidade do grupo das unidades de $\mathbb{Z}[w]$, que tem ordem 6 e de $\mathbb{Z}[i]$, que tem ordem 4.

Definição 5.2.1. *Um código linear C sobre $A_p[\rho]$ é chamado um código constacíclico (ou um código θ-cíclico) se para toda palavra-código $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ implicar que $(\theta c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, na qual θ é uma unidade em $\mathbb{Z}[\rho]$.*

Se p é um número primo tal que $p \equiv 1 \ (mod\ 6)$, então p se decompõe em $\mathbb{Z}[w]$, isto é, $p = \pi\bar{\pi}$, com π um elemento primo em $\mathbb{Z}[w]$ tal que $N(\pi) = p$. Seja β um elemento de $A_p[w] \cong \dfrac{\mathbb{Z}[w]}{\langle\pi\rangle}$ de ordem $p-1$ e tal que $\beta^n = w$, em que $n = \frac{p-1}{6}$. Assim, β é um elemento primitivo e portanto, podemos considerar $A_p[w] = \langle\beta\rangle \cup \{0\}$.

Seja C um código com matriz verificação de paridade H dada por

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \ldots & \beta^{n-1} \\ 1 & \beta^7 & (\beta^7)^2 & \ldots & (\beta^7)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{6t+1} & (\beta^{6t+1})^2 & \ldots & (\beta^{6t+1})^{n-1}. \end{pmatrix}, \tag{5.1}$$

na qual $0 \leq t \leq n-1$. A matriz geradora do código C é dada por

$$G = \begin{pmatrix} -\beta & 1 & \dots & 0 \\ -\beta^2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\beta^{n-1} & 0 & \dots & 1 \end{pmatrix}. \tag{5.2}$$

Um vetor $c = (c_0, c_1, \dots, c_{n-1})$ de $A_p^n[w]$ pertence a C se, e somente se, $Hc^T = 0$, isto é,

$$\begin{cases} c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1} = 0 \\ c_0 + c_1\beta^7 + \dots + c_{n-1}(\beta^7)^{n-1} = 0 \\ \vdots \\ c_0 + c_1\beta^{6t+1} + \dots + c_{n-1}(\beta^{6t+1})^{n-1} = 0. \end{cases}$$

Assim, identificando uma palavra-código $c = (c_0, \dots, c_{n-1})$ com o polinômio código $c(x) = \sum_{i=0}^{n-1} c_i x^i$, temos que $c(\beta^{6k+1}) = 0$, para $k = 0, 1, \dots, t$. Sejam $g(x) = (x-\beta)(x-\beta^7)\dots(x-\beta^{6t+1})$ um polinômio de grau $t+1$ e $S = \{\beta, \beta^7, \dots, \beta^{6t+1}\}$ o conjunto de elementos distintos de $A_p[w]$. Os elementos de S são raízes de $c(x)$ e são todas as $t+1$ raízes de $g(x)$. Agora, como $(\beta^{6k+1})^n - w = \beta^{6nk}\beta^n - w = \beta^n - w = 0$, para $k = 0, 1, 2, \dots, t$, segue que $g(x)$ divide $x^n - w$.

Teorema 5.2.1. *([13], p. 90) O polinômio $g(x) = (x-\beta)(x-\beta^7)\dots(x-\beta^{6t+1})$ é o polinômio gerador do código C e C é um ideal principal do anel $\dfrac{A_p[w][x]}{\langle x^n - w\rangle}$.*

Demonstração: Temos que c pertence a C se, e somente se, $c(x)$ tem $\beta, \beta^7, \dots, \beta^{6t+1}$ como raízes se, e somente se, $c(x)$ é um múltiplo de $g(x)$. Como $g(x)$ é o polinômio de menor grau que tem $\beta, \beta^7, \dots, \beta^{6t+1}$ como raízes, segue que $c(x)$ é um múltiplo do polinômio $g(x)$ que divide $x^n - w$. Portanto, $g(x)$ é o polinômio gerador do código C. ■

Se $c = (c_0, c_1, \dots, c_{n-1}) \in C$, então multiplicando o polinômio código $c(x)$ por x $(mod\ x^n - w)$, tem-se que

$$xc(x) - c_{n-1}(x^n - w) = wc_{n-1} + c_0x + \dots + c_{n-2}x^{n-1} \in C,$$

e obtemos:

1. Um deslocamento para a direita de uma posição da palavra-código.

2. O coeficiente c_{n-1} é rotacionado de 60º e torna-se o primeiro símbolo da nova palavra-código.

Portanto, o código C pertence a família dos códigos constacíclicos, ou seja, são invariantes por rotação de 60º.

Exemplo 5.2.1. *Sejam $p = 13 \equiv 1 \ (mod\ 6)$, $d = -3$ e $n = \frac{p-1}{6} = 2$. Sejam $A_{13}[w]$ como rotulados no Exemplo 2.3.2 e $\beta = -2 - w = \alpha_2$, usando as Equações 2.2 e considerando $t = 1$, temos a seguinte matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta \\ 1 & \beta^7 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_2 \\ 1 & \alpha_1 \end{pmatrix} = \begin{pmatrix} 1 & -2-w \\ 1 & 1 \end{pmatrix}.$$

Exemplo 5.2.2. *Sejam $p = 19 \equiv 1 \ (mod\ 6)$, $d = -3$ e $n = \frac{p-1}{6} = \frac{19-1}{6} = 3$. Sejam os elementos de $A_{19}[w]$ como rotulados no Exemplo 2.3.3 e $\beta = 2 = \alpha_2$, usando as Equações 2.2 e considerando $t = 1$, temos a seguinte matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^7 & \beta^{14} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_2 & \alpha_4 \\ 1 & \alpha_{14} & \alpha_6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1+2w \\ 1 & -2w & 1+2w \end{pmatrix}.$$

Agora, se p é um número primo em $\mathbb{Z}$ tal que $p \equiv 1 \ (mod\ 4)$, então p se decompõe em $\mathbb{Z}[i]$, isto é, $p = \pi\bar{\pi}$, com π um elemento primo em $\mathbb{Z}[i]$ tal que $N(\pi) = p$. Seja α um elemento de $A_p[i] \cong \dfrac{\mathbb{Z}[i]}{\langle \pi \rangle}$ de ordem $p-1$ tal que $\beta^n = i$. Logo, β é um elemento primitivo e portanto, podemos considerar $A_p[i] = \langle \alpha \rangle \cup \{0\}$. Seja C o código definido pela matriz controle de paridade dada por

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^5 & (\beta^5)^2 & \dots & (\beta^5)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{4t+1} & (\beta^{4t+1})^2 & \dots & (\beta^{4t+1})^{n-1} \end{pmatrix}, \tag{5.3}$$

onde $0 \leq t \leq n-1$. A matriz geradora G do código C é dada por

$$G = \begin{pmatrix} -\beta & 1 & 0 & \dots & 0 \\ -\beta^2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\beta^{n-1} & 0 & 0 & \dots & 1 \end{pmatrix}. \tag{5.4}$$

Teorema 5.2.2. *([13], p. 91) O polinômio $g(x) = (x-\beta)(x-\beta^5)\dots(x-\beta^{4t+1})$ é o polinômio gerador do código C e C é um ideal principal do anel $\dfrac{A_p[i][x]}{\langle x^n - i\rangle}$.*

Demonstração: A demonstração é análoga a do Teorema 5.2.1. ■

Se $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \in C$, então multiplicando o polinômio código $c(x)$ por x $(mod\ x^n - i)$, tem-se que

$$xc(x) - c_{n-1}(x^n - i) = ic_{n-1} + c_0x + \ldots + c_{n-2}x^{n-1} \in C$$

e obtemos,

1. Um deslocamento para a direita de uma posição da palavra-código.
2. O coeficiente c_{n-1} é rotacionado de 90º e torna-se o primeiro símbolo da nova palavra-código.

Portanto, o código C pertence à família dos códigos constacíclicos, ou seja, são invariantes por rotação de 90°.

Exemplo 5.2.3. *Sejam $p = 17 \equiv 1\ (mod\ 4)$, $d = -1$ e $n = \frac{p-1}{4} = \frac{17-1}{4} = 4$. Sejam os elementos $A_{17}[i]$ rotulados como no Exemplo 2.3.9 e $\beta = 1 + i = \alpha_{14}$, usando as Equações 2.2 e considerando $t = 1$ temos a seguinte matriz verificação de paridade dada por*

$$\begin{aligned} H &= \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_{14} & \alpha_9 & \alpha_7 \\ 1 & \alpha_{12} & \alpha_8 & \alpha_{11} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1+i & 2i & -1-2i \\ 1 & -1+i & -2i & -2+i \end{pmatrix}. \end{aligned}$$

Exemplo 5.2.4. *Sejam* $p = 29 \equiv 1 \ (mod\ 4)$, $d = -1$ *e* $n = \frac{p-1}{4} = \frac{29-1}{4} = 7$. *Sejam os elementos* $A_{29}[i]$ *como no Exemplo 2.3.10 e* $\beta = -1 - 2i = \alpha_{24}$, *usando as Equações 2.2 e considerando* $t = 1$ *obtemos a seguinte matriz verificação de paridade dada por*

$$\begin{aligned} H &= \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} & \beta^{20} & \beta^{25} & \beta \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_4 & \alpha_{16} & \alpha_6 & \alpha_{24} & \alpha_9 & \alpha_7 \\ 1 & \alpha_9 & \alpha_{23} & \alpha_4 & \alpha_7 & \alpha_5 & \alpha_4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1-2i & -1-i & 1-2i & 2i & -3+i & 2-2i \\ 1 & -3+i & -1+2i & -1-2i & 2-2i & -2i & -1-2i \end{pmatrix}. \end{aligned}$$

5.2.1 Algoritmo de decodifição

Nesta seção, apresentamos um algoritmo de decodificação para correção de um erro do códigos definidos na seção anterior. Primeiramente, veremos os códigos definidos sobre $A_p[w]$. Seja $\beta \in A_p[w]$ um elemento de ordem $p-1$ tal que $\beta^n = w$, em que $n = \frac{p-1}{6}$.

O próximo teorema, fornece um algoritmo de decodificação para correção de um erro para códigos com matriz controle de paridade formado por apenas uma linha.

Teorema 5.2.3. *([2], p. 168) Se* C *é um código definido pela matriz controle de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \dots & \beta^{n-1} \end{pmatrix}, \tag{5.5}$$

então C *é capaz de corrigir todo padrão de erro da forma* $e(x) = e_i x^i$, *no qual* $w_{\mathcal{M}}(e_i) = 1$ *e os padrões de erro* $e(x) = \pm w^2 x^i$, *em que* $w_{\mathcal{M}}(\pm w^2) = 2$. *Portanto,* $d_{\mathcal{M}}(C) \geq 3$, *na qual* $d_{\mathcal{M}}(C)$ *é a distância mínima de Mannheim de* C.

Demonstração: Os elementos de peso um do alfabeto $A_p[w]$ são ± 1 e $\pm w$, em que $w = \frac{1+\sqrt{-3}}{2}$ é uma raiz sexta da unidade. As outras raízes da unidade são $\pm w^2 = w - 1$, que possuem peso dois. O conjunto $\{\pm 1, \pm w, \pm w^2\}$ pode ser representado por $\{\beta^{nu}; u = 1, 2, \dots, 6\}$. Sem perda de generalidade, podemos supor que a palavra

toda nula tenha sido a palavra transmitida. Assim, se $r = (0, \ldots, \beta^{nu}, \ldots, 0)$ é o vetor recebido, então a síndrome $S = rH^T$ é dada por

$$S = \beta^{j+nu} = \beta^L,$$

na qual $0 \leq j, L \leq n-1$. Reduzindo L módulo n, determinamos j e u é determinado por $u = \frac{L-j}{n}$, que são respectivamente, a localização e a magnitude do erro. ■

Exemplo 5.2.5. *Se* $p = 13 \equiv 1 \ (mod\ 6)$, *então* $n = \frac{p-1}{6} = \frac{13-1}{6} = 2$. *Sejam* $A_{13}[w]$ *rotulado como no Exemplo 2.3.2 e* $\beta = 2 - w = \alpha_5$. *Assim, os elementos* $\alpha_l = x + yw \in A_{13}[w]$ *são rotulados por* $l \in GF(13)$, *em que* $l \equiv x + 10y \ (mod\ 13)$ *e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta \end{pmatrix} = \begin{pmatrix} 1 & \alpha_5 \end{pmatrix} = \begin{pmatrix} 1 & 2-w \end{pmatrix}.$$

Seja $r = (0, \beta^8)$ *a palavra recebida, na qual* $\beta^8 = \alpha_1 = 1$ *tal que* $w_{\mathcal{M}}(\beta^8) = 1$. *Aplicando o algoritmo, temos que a síndrome é dada por* $S = rH^T = \beta^9 \neq 0$. *Portanto, ocorreu um erro. Logo,* $L = 9 \equiv j(mod\ n) \equiv j(mod\ 2) \equiv 1(mod\ 2)$. *Assim, sua localização e magnitude são, repectivamente,* $j = 1$ *e* $u = \frac{L-j}{n} = \frac{9-1}{2} = 4$. *Logo, o erro ocorreu na segunda posição e sua magnitude é dada por* $\beta^{nu} = \beta^{2.4} = \beta^8 = \alpha_1 = 1$. *Portanto,* $e = (0, 1)$ *é o vetor erro e* $c = r - e = (0, 0)$ *foi a palavra transmitida.*

Exemplo 5.2.6. *Se* $p = 19 \equiv 1 \ (mod\ 6)$, *então* $n = \frac{p-1}{6} = \frac{19-1}{6} = 3$. *Sejam* $A_{19}[w]$ *rotulado como no Exemplo 2.3.3 e* $\beta = 2 = \alpha_2$. *Assim os elementos* $\alpha_l = x + yx \in A_{19}[w]$ *são rotulados por* $l \in GF(19)$, *onde* $l \equiv x + 12y \ (mod\ 19)$ *e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_2 & \alpha_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1+2w. \end{pmatrix}$$

Seja $r = (0, \beta^6, 0)$ *uma palavra recebida, onde* $\beta^6 = \alpha_7 = 1+2w$ *tal que* $w_{\mathcal{M}}(\beta^6) = 3$. *Aplicando o algoritmo, temos que a síndrome é dada por* $S = rH^T = \alpha_{14} = -2w = \beta^7 \neq 0$. *Portanto, ocorreu um erro. Logo,* $L = 7 \equiv j(mod\ n) \equiv j(mod\ 3) \equiv 1(mod\ 3)$. *Assim, sua localização e magnitude são, respectivamente,* $j = 1$ *e* $u =$

$\frac{L-j}{n} = \frac{7-1}{3} = 2$. *Logo, o erro ocorreu na segunda posição e sua magnitude é* $\beta^{nu} = \beta^{3.2} = \beta^6 = \alpha_7 = 1 + 2w$. *Portanto,* $e = (0, \beta^6)$ *e* $c = r - e = (0, 0)$ *foi a palavra transmitida.*

O próximo teorema, fornece um processo de decodificação para correção de um erro de um código com matriz controle de paridade com apenas duas linhas.

Teorema 5.2.4. *([13], p. 97) Se* C *é um código definido pela matriz controle de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^7 & (\beta^7)^2 & \dots & (\beta^7)^{n-1} \end{pmatrix}, \tag{5.6}$$

então C *é capaz de corrigir todo padrão de erro da forma* $e(x) = e_i x^i$, *em que* $1 \leq w_{\mathcal{M}}(e_i) \leq d_{\mathcal{M},max}(A_p[w])$, *na qual* $d_{\mathcal{M},max}(A_p[w]) = max\{|a|, |b|, |a+b|\} - 1$ *é a distância de Mannheim e* $\pi = a + bw \in \mathbb{Z}[w]$.

Demonstração: Se $r = (0, 0, \dots, \beta^u, 0, \dots, 0)$ é a palavra recebida, então a síndrome é dada por

$$S = rH^T = \begin{pmatrix} \beta^{j+u} & \beta^{7j+u} \end{pmatrix} = \begin{pmatrix} S_1 & S_7 \end{pmatrix}.$$

Fazendo $S_1 = \beta^{L_1}$ e $S_7 = \beta^{L_2}$, em que L_j é o logaritmo de S_j na base β, para $j = 1, 7$, temos que

1. Se $\beta^{j+u} = S_1$, então $j + u \equiv L_1 (mod\ (p-1))$.
2. Se $\beta^{7j+u} = S_7$, então $7j + u \equiv L_2 (mod\ (p-1))$.

Desta maneira, obtemos o seguinte sistema linear:

$$\begin{cases} j + u \equiv L_1 (mod\ (p-1)) \\ 7j + u \equiv L_2 (mod\ (p-1)), \end{cases}$$

que possui somente uma solução dada por:

$$\begin{cases} j \equiv \frac{L_1 - L_2}{6} (mod\ n) \\ u \equiv L_1 - j (mod\ (p-1)), \end{cases}$$

Assim, concluímos que o erro ocorreu na posição $\frac{L_2 - L_1}{6}$ $(mod\ n)$ e sua magnitude é β^u, na qual $u \equiv L_1 - j\ (mod\ p-1)$. ■

Exemplo 5.2.7. *Se* $p = 31 \equiv 1\ (mod\ 6)$*, então* $n = \frac{p-1}{6} = \frac{31-1}{6} = 5$*. Sejam* $A_{31}[w]$ *rotulado como no Exemplo 2.3.4 e* $\beta = 3 - 2w = \alpha_{22}$*. Assim, os elementos* $\alpha_l = x + yw \in A_{31}[w]$ *são rotulados por* $l \in GF(31)$*, em que* $l \equiv x + 6y\ (mod\ 31)$ *e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada por*

$$\begin{aligned} H &= \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_{22} & \alpha_{19} & \alpha_{15} & \alpha_{20} & \alpha_6 \\ 1 & \alpha_{14} & \alpha_{10} & \alpha_{16} & \alpha_7 & \alpha_5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3-2w & -2w & 3+2w & 1-2w & w \\ 1 & 2+2w & -2+2w & -3-2w & 1+w & -1+w \end{pmatrix}. \end{aligned}$$

Se $r = (0, 0, \beta^{10}, 0, 0)$ *é a palavra recebida, na qual* $\beta^{10} = \alpha_5 = -1 + w$ *tal que* $w_{\mathcal{M}}(\beta^{10}) = 2$*, então a síndrome é dada por* $S = rH^T = \begin{pmatrix} \beta^{12} & \beta^{24} \end{pmatrix} = \begin{pmatrix} \alpha_2 & \alpha_{23} \end{pmatrix} = \begin{pmatrix} 2 & -2-w \end{pmatrix} = \begin{pmatrix} S_1 & S_7 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \end{pmatrix}$*. Portanto, ocorreu um erro e* $j \equiv \frac{L_2 - L_1}{6}(mod\ n) \equiv \frac{24-12}{6}(mod\ 5) \equiv 2(mod\ 5)$*, isto é,* $j = 2$*. Assim, o erro se localiza na terceira posição e sua magnitude é dada por* $u \equiv L_1 - j(mod\ p-1) \equiv 12 - 2(mod\ 30) \equiv 10(mod\ 30)$*, ou seja,* $u = 10$*. Deste modo,* $\beta^{10} = \alpha_5 = -1 + w$*. Portanto,* $e = (0, 0, \beta^{10}, 0)$ *é o vetor erro e* $c = r - e = (0, 0, 0, 0)$ *foi a palavra transmitida.*

Agora, veremos os códigos definidos sobre $A_p[i]$. Deste modo, seja $\beta \in A_p[i]$ um elemento de ordem $p - 1$ tal que $\beta^n = i$ em que $n = \frac{p-1}{4}$.

O próximo teorema fornece o algoritmo de decodificação para correção de um erro de um código com matriz verificação de paridade com apenas uma linha.

Teorema 5.2.5. *([1], p. 208) Se* C *é um código definido pela matriz controle de paridade*

$$H = \begin{pmatrix} 1 & \beta & \dots & \beta^{n-1} \end{pmatrix}, \tag{5.7}$$

então C *é capaz de corrigir um erro de Mannheim via o anel de inteiros gaussiano. Portanto,* $d_{\mathcal{M}}(C) \geq 3$*, na qual* $d_{\mathcal{M}}(C)$ *é a distância mínima de Mannheim de* C*.*

Demonstração: A demonstração é análoga ao Teorema 5.2.3. ∎

Exemplo 5.2.8. *Se* $p = 13 \equiv 1 \ (mod\ 4)$*, então* $n = \frac{p-1}{4} = \frac{13-1}{4} = 3$*. Sejam* $A_{13}[i]$ *rotulado como no Exemplo 2.3.8 e* $\beta = 1 + i = \alpha_6$*. Assim, os elementos* $\alpha_l = x + yi \in A_{13}[i]$ *são rotulados por* $l \in GF(13)$*, em que* $l \equiv x + 10y \ (mod\ 13)$ *e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_6 & \alpha_{10} \end{pmatrix} = \begin{pmatrix} 1 & 1+i & 2i \end{pmatrix}.$$

Suponhamos que $r = (0, 0, \beta^9)$ *seja a palavra recebida, na qual* $\beta^9 = \alpha_5 = i$ *tal que* $w_{\mathcal{M}}(\beta^9) = 1$*. A síndrome é dada por* $S = rH^T = 2 = \alpha_2 = \beta^{11} \neq 0$*. Logo, ocorreu um erro. Assim* $L = 11 \equiv j(mod\ n) \equiv j(mod\ 3) \equiv 2(mod\ 3)$ *e* $u = \frac{L-j}{n} = \frac{11-2}{3} = 3$*. Portanto, como* $j = 2$*, segue que o erro ocorreu na terceira posição e como* $u = 3$*, temos que a magnitude é* $\beta^{nu} = \beta^{3.3} = \beta^9 = i$*. Assim,* $e = (0, 0, \beta^9)$ *é o vetor erro e deste modo,* $c = r - e = (0, 0, 0)$ *foi a palavra transmitida.*

Exemplo 5.2.9. *Se* $p = 29 \equiv 1 \ (mod\ 4)$*, então* $n = \frac{p-1}{4} = \frac{29-1}{4} = 7$*. Sejam* $A_{29}[i]$ *rotulado como no Exemplo 2.3.10 e* $\beta = 2 + 2i = \alpha_{26}$*. Assim, os elementos* $\alpha_l = x + yi \in A_{29}[i]$ *são rotulados por* $l \in GF(29)$*, em que* $l \equiv x + 12y \ (mod\ 29)$ *e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada por*

$$\begin{aligned} H &= \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_{26} & \alpha_9 & \alpha_2 & \alpha_{23} & \alpha_{18} & \alpha_4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2+2i & -3+i & 2 & -1+2i & 1-i & -1-2i \end{pmatrix}. \end{aligned}$$

Supohamos que $r = (0, 0, \beta^{21}, 0, 0, 0, 0)$ *é a palavra recebida, na qual* $\beta^{21} = i$ *e* $w_{\mathcal{M}}(\beta^{21}) = 1$*. Calculando a síndrome é dada por* $S = rH^T = -1 - 3i = \alpha_{21} = \beta^{23} \neq 0$*. Logo, ocorreu um erro e assim,* $L = 23 \equiv j(mod\ 7) \equiv 2(mod\ 7)$ *e* $u = \frac{L-j}{n} = \frac{23-2}{7} = 3$*. Como* $j = 2$*, segue que o erro ocorreu na terceira posição, e como* $u = 3$*, segue que a magnitude do erro é dada por* $\beta^{nu} = \beta^{7.3} = \beta^{21} = \alpha_{12} = i$*. Assim,* $e = (0, 0, \beta^{21}, 0, 0, 0, 0)$ *é o vetor erro e* $c = r - e = (0, 0, 0, 0, 0, 0, 0)$ *foi a palavra transmitida.*

O próximo teorema fornece um processo de decodificação de um código capaz de corrigir um erro de Mannheim, com matriz controle de paridade possuindo duas

linhas.

Teorema 5.2.6. *([13], p. 107) Se C é um código definido pela matriz controle de paridade*

$$H = \begin{pmatrix} 1 & \beta & \dots & \beta^{n-1} \\ 1 & \beta^5 & \dots & (\beta^5)^{n-1} \end{pmatrix}, \tag{5.8}$$

então C é capaz de corrigir todo padrão de erro da forma $e(x) = e_j x^j$, em que $1 \leq w_{\mathcal{M}}(e_j) \leq d_{\mathcal{M},max}(A_p[i])$, para $0 \leq j \leq n-1$ e $d_{\mathcal{M},max}(A_p[i])$ é a distância máxima de Mannheim em $A_p[i]$.

Demonstração: Se $r = (0, 0, \dots, \beta^u, \dots, 0)$ é a palavra recebida, então a síndrome S é dada por

$$S = rH^T = \begin{pmatrix} \beta^{j+u} & \beta^{5j+u} \end{pmatrix} = \begin{pmatrix} S_1 & S_5 \end{pmatrix}.$$

Fazendo $S_1 = \beta^{L_1} = \beta^{j+u}$ e $S_5 = \beta^{L_2} = \beta^{5j+u}$, em que L_j é o logaritmo de S_j na base β, para $j = 1, 5$, obtemos o seguinte sistema linear

$$\begin{cases} j + u \equiv L_1 (mod\ p-1) \\ 5j + u \equiv L_2 (mod\ p-1), \end{cases}$$

que possui somente uma solução dada por

$$\begin{cases} j \equiv \frac{L_2 - L_1}{4}\ (mod\ n) \\ u \equiv L_1 - j\ (mod\ p-1). \end{cases}$$

Deste modo, temos que o erro ocorreu na posição $\frac{L_2-L_1}{4}$ $(mod\ n)$ e sua magnitude é dado por β^u, na qual $u \equiv L_1 - j\ (mod\ p-1)$. ■

Exemplo 5.2.10. *Se $p = 17 \equiv 1\ (mod\ 4)$, então $n = \frac{p-1}{4} = \frac{17-1}{4} = 4$. Sejam $A_{17}[i]$ rotulado como no Exemplo 2.3.9 e $\beta = 1 + i = \alpha_{14}$. Assim, os elementos $\alpha_l = x + yi \in A_{17}[i]$ são rotulados por $l \in GF(17)$, em que $l \equiv x + 13y\ (mod\ 17)$ e usando as Equações 2.2, obtemos a seguinte matriz verificação de paridade dada*

por

$$\begin{aligned} H &= \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_{14} & \alpha_9 & \alpha_7 \\ 1 & \alpha_{12} & \alpha_8 & \alpha_{11} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1+i & 2i & -1-2i \\ 1 & -1+i & -2i & -2+i \end{pmatrix}. \end{aligned}$$

Se $r = (0, \beta^{12}, 0, 0)$ *é a palavra recebida, na qual* $\beta^{12} = \alpha_4 = -i$ *tal que* $w_{\mathcal{M}}(\beta^{12}) = 1$. *A síndrome é dada por* $S = rH^T = \begin{pmatrix} \beta^{13} & \beta^{17} \end{pmatrix} = \begin{pmatrix} 1-i & 1+i \end{pmatrix} = \begin{pmatrix} \alpha_5 & \alpha_{14} \end{pmatrix} = \begin{pmatrix} S_1 & S_5 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \end{pmatrix}$. *Logo, ocorreu um erro e assim*

$$j \equiv \frac{L_2 - L_1}{4} \ (mod\ n) \equiv \frac{1-13}{4} \ (mod\ 4) \equiv -3 \ (mod\ 4) \equiv 1 \ (mod\ 4).$$

Logo, $j = 1$ *e* $u \equiv L_1 - j \ (mod\ p-1) \equiv 13 - 1 \ (mod\ 16) \equiv 12 \ (mod\ 16)$, *isto é,* $u = 12$. *Dessa forma, o erro se encontra na segunda posição e tendo* $u = 12$, *tem-se que a magnitude do erro é* $\beta^u = \beta^{12} = \alpha_4 = -i$. *Portanto,* $e = (0, \beta^{12}, 0, 0)$ *é o vetor erro e* $c = r - e = (0, 0, 0, 0)$ *foi a palavra transmitida.*

5.3 Códigos via corpos ciclôtomicos

Nesta seção, veremos o conceito de códigos via os corpos ciclôtomicos introduzido por Dong [8] e [9], na qual constitui um conceito mais geral dos trabalhos de Fan [7], como vimos no Capítulo 3. Veremos resultados que serão necessários para a construção do algoritmo de decodificação desses códigos. Para isso, sejam ξ_n uma raiz n-ésima primitiva da unidade e $\mathbb{Z}[\xi_n]$ o anel de inteiros de $\mathbb{Q}(\xi_n)$. Seja $n \in \{1\} \cup A$, em que $A = \{3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$.

Lema 5.3.1. *([9]) Seja* p *um número primo. Se* α *é um elemento irredutível em* $\mathbb{Z}[\xi_n]$ *tal que* $N(\alpha) = p$, *então* $\langle \alpha \rangle \cap \mathbb{Z} = \langle p \rangle$.

Demonstração: Segue da Proposição 1.4.3 que $N(\alpha) = p \in \langle \alpha \rangle$. Portanto, $\langle p \rangle \subseteq \langle \alpha \rangle \cap \mathbb{Z}$. Por outro lado, temos que $\langle p \rangle \subseteq \langle \alpha \rangle \cap \mathbb{Z} \subseteq \mathbb{Z}$. Se $\langle \alpha \rangle \cap \mathbb{Z} = \mathbb{Z}$, então $1 \in \langle \alpha \rangle$

o que não ocorre, uma vez que α é irredutível. Portanto, $\langle\alpha\rangle \cap \mathbb{Z} \subseteq \mathbb{Z}$ e como $\langle p\rangle$ é um ideal maximal, segue que $\langle p\rangle = \langle\alpha\rangle \cap \mathbb{Z}$. ■

Teorema 5.3.1. *([9], p. 114) Seja p um número primo. Se α é um elemento irredutível em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk + 1$, então $GF(p) = \{0, 1, \ldots, p-1\}$ é isomorfo ao corpo $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$.*

Demonstração: Seja α um elemento irredutível em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p = nk+1$, na qual p é um número primo. Pelo Teorema 3.2.1, tem-se que $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ é um corpo com p elementos. Consideremos a aplicação inclusão $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[\xi_n]$ definida por $i(a) = a$, $a \in \mathbb{Z}$, e a aplicação projeção $\pi : \mathbb{Z}[\xi_n] \to \dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ definida por $\pi(\beta) = \beta + \langle\alpha\rangle$, com $\beta \in \mathbb{Z}[\xi_n]$. Assim, temos a seguinte composição

$$\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{Z}[\xi_n] \overset{\pi}{\to} \frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}.$$

Seja $\pi \circ i : \mathbb{Z} \to \dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ a função composta definida por $(\pi \circ i)(a) = a + \langle\alpha\rangle$, em que $a \in \mathbb{Z}$. Temos que $\pi \circ i$ é um homomorfismo e $Ker(\pi \circ i) = \langle p\rangle$, uma vez que $x \in Ker(\pi \circ i) = \{x \in \mathbb{Z} : (\pi \circ i)(x) = \bar{0}\}$ se, e somente se, $(\pi \circ i)(x) = \bar{0} = 0 + \langle\alpha\rangle$ se, e somente se, $x + \langle\alpha\rangle = 0 + \langle\alpha\rangle$ se, e somente se, $x \in \langle\alpha\rangle$ se, e somente se, $x \in \langle\alpha\rangle \cap \mathbb{Z}$. Portanto, pelo Lema 5.3.1, tem-se que $Ker(\pi \circ i) = \langle p\rangle$. Deste modo, $GF(p) = \dfrac{\mathbb{Z}}{\langle p\rangle}$ pode ser identificado como um subcorpo de $\dfrac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$. Como estes dois corpos tem a mesma cardinalidade, segue que são isomorfos. ■

Teorema 5.3.2. *([9], p. 114) Seja p um número primo qualquer. Se $\varphi(n)$ é o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$, então*

$$GF(p^{\varphi(n)}) = \{a_0 + a_1\xi_n + \ldots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : |a_j| \leq \frac{(p-1)}{2}, j = 0, 1, \ldots, \varphi(n)-1\}$$

é um conjunto completo das classes laterais do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$.

Demonstração: Seja $\varphi(n)$ o menor inteiro positivo tal que $p^{\varphi(n)} \equiv 1 \ (mod\ n)$. Pelo Corolário 1.7.2, segue que $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ é um corpo com $p^{\varphi(n)}$ elementos. Logo, p é um elemento irredutível em $\mathbb{Z}[\xi_n]$, uma vez que $\langle p\rangle$ em $\mathbb{Z}[\xi_n]$ é um ideal maximal. Temos que o conjunto $GF(p^{\varphi(n)}) = \{a_0 + a_1\xi_n + \ldots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : |a_j| \leq \frac{(p-1)}{2}, j =$

$0, 1, \ldots, \varphi(n)-1\}$ tem $p^{\varphi(n)}$ elementos. Agora, se $b_0 + b_1\xi_n + \ldots + b_{\varphi(n)-1}\xi_n^{\varphi(n)-1}$ e $c_0 + c_1\xi_n + \ldots + c_{\varphi(n)-1}\xi_n^{\varphi(n)-1}$ são elementos de uma mesma classe lateral módulo o ideal $p\mathbb{Z}[\xi_n]$, então $\overline{b_0 + b_1\xi_n + \ldots + b_{\varphi(n)-1}\xi_n^{\varphi(n)-1}} = \overline{c_0 + c_1\xi_n + \ldots + c_{\varphi(n)-1}\xi_n^{\varphi(n)-1}}$ se, e somente se, $(b_0 + b_1\xi_n + \ldots + b_{\varphi(n)-1}\xi_n^{\varphi(n)-1}) + p\mathbb{Z}[\xi_n] = (c_0 + c_1\xi_n + \ldots + c_{\varphi(n)-1}\xi_n^{\varphi(n)-1}) + p\mathbb{Z}[\xi_n]$ se, e somente se, $(b_0 + b_1\xi_n + \ldots + b_{\varphi(n)-1}\xi_n^{\varphi(n)-1}) - (c_0 + c_1\xi_n + \ldots + c_{\varphi(n)-1}\xi_n^{\varphi(n)-1}) \in p\mathbb{Z}[\xi_n]$ se, e somente se, $(b_0 - c_0) + (b_1 - c_1)\xi_n + \ldots + (b_{\varphi(n)-1} - c_{\varphi(n)-1})\xi_n^{\varphi(n)-1} = p\beta$, para algum $\beta \in \mathbb{Z}[\xi_n]$. Assim,

$$p \mid (((b_0 - c_0) + (b_1 - c_1)\xi_n + \ldots + (b_{\varphi(n)-1} - c_{\varphi(n)-1})\xi_n^{\varphi(n)-1}))$$

e portanto,

$$p \mid (b_j - c_j), \tag{5.9}$$

para $j = 1, \ldots, \varphi(n)-1$. Por outro lado, pela definição do conjunto $GF(p^{\varphi(n)})$, tem-se que $|b_j|, |c_j| \leq \frac{p-1}{2}$ e assim, $|b_j - c_j| \leq |b_j| + |c_j| \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$. Logo, pela Equação (5.9), temos que $b_j = c_j$, para $j = 0, 1, \ldots, \varphi(n)-1$. Portanto, o conjunto $GF(p^{\varphi(n)})$ é um conjunto completo das classes laterais do corpo $\dfrac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$. ■

Teorema 5.3.3. *([9], p. 114) Se $\varphi(n)$ é o menor inteiro positivo tal que $2^{\varphi(n)} \equiv 1 \pmod{n}$, então*

$$GF(2^{\varphi(n)}) = \{a_0 + a_1\xi_n + \ldots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : 0 \leq |a_j| \leq 1, j = 0, 1, \ldots, \varphi(n)-1\}$$

é um conjunto completo das classes laterais do corpo $\dfrac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$.

Demonstração: Segue do Teorema 5.3.2, tomando $p = 2$. ■

Consideremos o seguinte conjunto

$$A_n = \begin{cases} \{1, \xi_n, \ldots, \xi_n^{n-1}\} \text{ se } n \text{ par} \\ \{\pm 1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\} \text{ se } n \text{ ímpar,} \end{cases}$$

na qual $n \in \{1\} \cup A$. Sejam p um número primo e α um elemento irredutível em $\mathbb{Z}[\xi_n]$ tal que $N(\alpha) = p^h$, em que $p \nmid n$, $n \in A$, $h = 1$ ou $h = \varphi(n)$. Seja o conjunto $GF(p^h)$ como nos Teoremas 5.3.1, 5.3.2 e 5.3.3. Pelos Teoremas 3.2.2, 3.2.4 e 3.2.7, temos que existe um único subconjunto $S_n \subset GF(p^{\varphi(n)})$ tal que cada elemento de S_n está na mesma classe lateral de algum elemento do conjunto A_n módulo o ideal $\langle\alpha\rangle$. Assim, obtemos a seguinte definição:

Definição 5.3.1. *Um conjunto completo das classes laterais do corpo* $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ *é definido como*

$$R^n_{p^h} = \{a - [\frac{a}{\alpha}]\alpha \ : \ a \in GF(p^{\varphi(n)}) - S_n\} \cup A_n,$$

na qual $[\frac{a}{\alpha}] \in \mathbb{Z}[\xi_n]$.

Definição 5.3.2. *Um código linear* C *de comprimento*

$$l = \begin{cases} \dfrac{p^h - 1}{n} \text{ se } p \text{ é primo ímpar e } n \text{ par} \\ \dfrac{p^h - 1}{2n} \text{ se } p \text{ é primo ímpar e } n \text{ ímpar} \\ \dfrac{2^{\varphi(n)-1} - 1}{n} \text{ se } p = 2 \text{ e } h = \varphi(n), \end{cases}$$

sobre $R^n_{p^h}$ *e* $R^n_{2^{\varphi(n)}}$, *repectivamente, para os primos ímpares e para* $p = 2$ *é definido como sendo o conjunto das palavras-códigos* $(\alpha_0, \alpha_1, \ldots, \alpha_{l-1})$, *com os coeficientes* $\alpha_i \in R^n_{p^h}$ *ou* $R^n_{2^{\varphi(n)}}$, *respectivamente tal que*

$$\alpha_0 + \alpha_1\beta + \ldots + \alpha_{l-1}\beta^{l-1} = 0,$$

onde β *é um elemento primitivo do corpo* $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$.

Observação 5.3.1. *A matriz controle de paridade* H *e a matriz geradora* G *são dadas respectivamente por*

$$H = \begin{pmatrix} 1 & \beta & \ldots & \beta^{l-1} \end{pmatrix} \quad e \quad G = \begin{pmatrix} -\beta & 1 & \ldots & 0 \\ -\beta^2 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\beta^{l-1} & 0 & \ldots & 1 \end{pmatrix}. \tag{5.10}$$

5.3.1 Algoritmo de decodificação

Nesta seção, daremos o algoritmo de decodificação para os códigos definidos na seção anterior.

Teorema 5.3.4. *([9], p. 116) Se* p *é um número primo e* n *é um número par, então um código linear* C *de comprimento* $l = \frac{p^h-1}{n}$ *sobre* $R^n_{p^h}$ *é capaz de corrigir um erro com valores em* $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$.

Demonstração: Sejam C um código linear de comprimento $l = \frac{p^h-1}{n}$ sobre $R^n_{p^h}$ e β um elemento primitivo de $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ com $N(\alpha) = p^h$, em que $p \nmid n$, $n \in A$, $h = 1$ ou $h = \varphi(n)$ tal que $\alpha_0 + \alpha_1\beta + \ldots + \alpha_{l-1}\beta^{l-1} = 0$, na qual $\alpha_k \in R^n_{p^h}$ para $k = 0, 1, \ldots, l-1$. Temos que, $o(\beta) = p^h - 1$, pois $\langle\beta\rangle$ é o grupo multiplicativo do corpo $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$ que tem p^h elementos, uma vez que $p^h = N(\alpha) = \#\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$. Como $o(\beta) = p^h - 1$, segue que $o(\beta^l) = n$, em que l é o comprimento do código C, pois

- $o(\beta^l)^n = \beta^{ln} = \beta^{\frac{p^h-1}{n}n} = \beta^{p^h-1} = 1$ e
- Se existe $m \in \mathbb{N}$ tal que $0 < m < n$ e $o(\beta^l) = m$, então $(\beta^l)^m = 1$, ou seja, $\beta^{lm} = 1$. Como $o(\beta) = p^h - 1$, segue que $p^h - 1 \mid lm$. Assim, $lm = (p^h - 1)k$, para algum k em $\mathbb{Z}$. Dividindo ambos os lados da equação por n obtemos que $\frac{lm}{n} = \frac{(p^h-1)}{n}k = \frac{lm}{n} = lk$. Assim, $n \mid m$, ou seja, $n \leq m$, o que é um absurdo devido a escolha de m.

Portanto, $o(\beta^l) = n$. Como $\langle\beta^l\rangle = \{\beta^l, \ldots, \beta^{nl}\}$ e $\langle\xi_n\rangle = \{1, \xi_n, \ldots, \xi_n^{n-1}\}$ são ambos subgrupos cíclicos com n elementos do grupo multiplicativo do corpo $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$, segue pelo Teorema 3.2.2 a unicidade destes subgrupos, ou seja, $\{\beta^l, \ldots, \beta^{nl}\} = \{1, \xi_n, \ldots, \xi_n^{n-1}\}$. Portanto, o código linear C definido pela matriz controle de paridade H dada pela Equação (5.10) corrige um erro no conjunto $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$, uma vez que esta classe de erro produz síndromes diferentes. ■

Teorema 5.3.5. *([9], p. 116) Se p é um número primo ímpar e n é um número ímpar, então o código linear C de comprimento $l = \frac{p^h-1}{2n}$ sobre $R^n_{p^h}$ é capaz de corrigir um erro com valores em $\{\pm1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$.*

Demonstração: A demonstração é análoga ao Teorema 5.3.4, com a ressalva de que $\langle-\beta^l\rangle = \{\pm\beta^l, \ldots, \pm\beta^{nl}\}$ e $\langle-\xi_n\rangle = \{\pm1, \pm\xi_n, \ldots, \pm\xi_n^{n-1}\}$ são subgrupos ciclícos com $2n$ elementos do grupo multiplicativo do corpo $\frac{\mathbb{Z}[\xi_n]}{\langle\alpha\rangle}$. ■

Teorema 5.3.6. *([9], p. 119) O código linear C de comprimento $l = \frac{2^{\varphi(n)-1}-1}{n}$ sobre $R^n_{2^{\varphi(n)}}$ é capaz de corrigir um erro com valores em $\{1, \xi_n, \ldots, \xi_n^{n-1}\}$.*

Demonstração: A demonstração é análoga ao Teorema 5.3.4. ■

Seja C um código linear de comprimento $l = \frac{p^h-1}{n}$ sobre $R^n_{p^h}$ ou de comprimento $l = \frac{2^{\varphi(n)-1}-1}{n}$ sobre $R^n_{2^{\varphi(n)}}$. Pelos Teoremas 5.3.1, 5.3.2 e 5.3.3, obtemos o seguinte algoritmo de decodificação dado por:

1. Calcule a síndrome $S = rH^T$.

2. A localização e magnitude do erro são dadas, respectivamente, por $L = log_\beta(S) \equiv j \ (mod\ l)$ e $u = S\beta^{-j}$, para $0 \leq j \leq l-1$.

3. A palavra transmitida é dado por $c = r - e$, na qual r é a palavra recebida e e é o vetor erro.

Observação 5.3.2. *Sejam* $\alpha = x + y\xi_8 + z\xi_8^2 + w\xi_5^3 \in \mathbb{Q}(\xi_8)$ *e* $m(x) = x^4 + 1$ *o polinômio minimal de* $\mathbb{Q}(\xi_8)$. *O grupo de Galois de* $\mathbb{Q}(\xi_8)$ *sobre* $\mathbb{Q}$ *é dado por* $Gal_{\mathbb{Q}}\mathbb{Q}(\xi_8) = \{1, \sigma, \tau, \sigma\tau\}$, *em que* $\sigma(\xi_8) = \xi_8^3$ *e* $\tau(\xi_8) = \xi_8^5$. *Logo,* $N(\alpha) = N(x + y\xi_8 + z\xi_8^2 + w\xi_8^3) = (x + y\xi_8 + z\xi_8^2 + w\xi_8^3)\sigma(x + y\xi_8 + z\xi_8^2 + w\xi_8^3)$ $\tau(x+y\xi_8+z\xi_8^2+w\xi_8^3)\sigma\tau(x+y\xi_8+z\xi_8^2+w\xi_8^3) = (x^2-z^2+2yw)^2+(w^2-y^2+2xz)^2$.

Exemplo 5.3.1. *([8], p. 71) Sejam* $p = 41 = 8.5 + 1$, *onde* $n = 8$ *e* $\alpha = 1 + \xi_8 + \xi_8^2 + 2\xi_8^3$ *um elemento irredutível de* $\mathbb{Z}[\xi_8]$, *pois pela Observação 5.3.2 temos que* $N(\alpha) = 41$. *Como* $N(\alpha) = 41$ *é um número primo tal que* $N(\alpha) = 41 \nmid n = 8$, *segue que pelo Teorema 3.2.1, que* α *é um elemento irredutível em* $\mathbb{Z}[\xi_8]$. *O elemento*

$$\begin{aligned}
\beta &= 6 - [\frac{6}{(1+\xi_8+\xi_8^2+2\xi_8^3)}](1+\xi_8+\xi_8^2+2\xi_8^3) \\
&= 6 - [\frac{6\sigma(\alpha)\tau(\alpha)\sigma(\tau(\alpha))}{(1+\xi_8+\xi_8^2+2\xi_8^3)\sigma(\alpha)\tau(\alpha)\sigma(\tau(\alpha))}](1+\xi_8+\xi_8^2+2\xi_8^3) \\
&= 6 - [\frac{6(9-14\xi_8-\xi_8^2-3\xi_8^3)}{41}](1+\xi_8+\xi_8^2+2\xi_8^3) \\
&= 6 - [\frac{54-84\xi_8-6\xi_8^2 18\xi_8^3}{41}](1+\xi_8+\xi_8^2+2\xi_8^3) \\
&= 1 + \xi_8 + \xi_8^2,
\end{aligned}$$

em que $\sigma(\alpha) = 1+2\xi_8-\xi_8^2+\xi_8^3$, $\tau(\alpha) = 1-\xi_8+\xi_8^2-2\xi_8^3$ *e* $\sigma(\tau(\alpha)) = 1-2\xi_8-\xi_8^2-\xi_8^3$, *é o elemento primitivo do corpo* $\frac{\mathbb{Z}[\xi_8]}{\langle\alpha\rangle}$, *uma vez que* 6 *é um elemento primitivo de* $GF(41)$.

Através de cálculo computacional, obtemos a tabela de logaritmo de Zech's, onde $1+\beta^j = \beta^{z(j)}$ *e* $\beta^{-\infty} = 0$ *e a Tabela 5.2 que ilustra os elementos do corpo* $\frac{\mathbb{Z}[\xi_8]}{\langle\alpha\rangle}$. *Assim, temos um código* C *de comprimento* $l = 5 = \frac{p-1}{n} = \frac{41-1}{8}$ *com matriz verificação de paridade dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \end{pmatrix}.$$

Sejam $u = ((1,-1,0,1),(1,1,0,-1),(-1,1,-1,0),(0,1,-1,1))$ *o vetor informação e*

$$G = \begin{pmatrix} -\beta & 1 & 0 & 0 & 0 \\ -\beta^2 & 0 & 1 & 0 & 0 \\ -\beta^3 & 0 & 0 & 1 & 0 \\ -\beta^4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

a matriz geradora do código C, *então* $uG = ((1,1,0,-1),(1,-1,0,1),(1,1,1,-1),(-1,1,-1,0),(0,1,-1,1))$. *Suponhamos que* $r = ((1,1,0,-1),(1,-1,0,1),(1,1,1,-1),(-1,1,-1,0),(0,1,-1,1))$ *é o vetor recebido. Usando a Tabela 5.1 e cálculos computacionais, a síndrome é dada por* $S = rH^t = \beta^{12} \neq 0$. *Logo, ocorreu um erro. Assim,* $L = 12 \equiv j(mod\ n) \equiv 2(mod\ 5)$. *Como* $j = 2$, *segue que o erro ocorreu na terceira posição e a magnitude do erro é dada por* $\beta^{12}\beta^{-2} = \beta^{10} = (0,0,1,0) = \xi_8^2$. *Portanto, a palavra transmitida foi* $c = r - e = ((1,1,0,-1),(1,-1,0,1),(1,1,0,-1),(-1,1,-1,0),(0,1,-1,1))$.

j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$
1	39	6	20	11	7	16	9	21	2	26	15	31	25	36	13
2	32	7	23	12	22	17	5	22	1	27	31	32	35	37	24
3	27	8	3	13	4	18	19	23	28	28	10	33	16	38	30
4	17	9	34	14	29	19	21	24	33	29	36	34	14	39	38
5	11	10	18	15	12	20	$-\infty$	25	37	30	8	35	6	40	26

Tabela 5.1: Tabela de logaritmo de Zech's do corpo $\frac{\mathbb{Z}[\xi_8]}{\langle\alpha\rangle}$

L	β^L	L	β^L	L	β^L	L	β^L
1	$(1,1,1,0)$	11	$(-1,0,1,1)$	21	$(-1,1,-1,0)$	31	(1,0,-1,-1)
2	$(0,2,3,2)$	12	$(-3,-2,0,2)$	22	$(0,-2,-3,-2)$	32	(3,2,0,-2)
3	$(2,0,-2,3)$	13	$(2,-3,2,0)$	23	$(-2,0,2,-3)$	33	$(-2,3,2,0)$
4	$(1,-1,0,1)$	14	$(0,-1,1,-1)$	24	$(-1,1,0,-1)$	34	$(0,1,-1,1)$
5	$(0,-1,0,0)$	15	$(0,0,0,-1)$	25	$(0,1,0,0)$	35	$(0,0,0,1)$
6	$(0,-1,-1,1)$	16	$(1,1,0,-1)$	26	$(0,1,1,1)$	36	$(-1,-1,0,1)$
7	$(2,0,-2,-3)$	17	$(2,3,2,0)$	27	$(-2,0,2,3)$	37	$(-2,3,-2,0)$
8	$(3,-2,0,2)$	18	$(0,-2,3,-2)$	28	$(3,2,0,-2)$	38	$(0,2,-3,2)$
9	$(1,-1,1,0)$	19	$(-1,0,1,-1)$	29	$(-1,1,-1,0)$	39	$(1,0,-1,1)$
10	$(0,0,1,0)$	20	$(-1,0,0,0)$	30	$(0,0,-1,0)$	40	$(1,0,0,0)$

Tabela 5.2: Tabela de elementos do corpo $\frac{\mathbb{Z}[\xi_8]}{\langle\alpha\rangle}$

Observação 5.3.3. *Sejam* $\alpha = a+b\xi_{16}+c\xi_{16}^2+d\xi_{16}^3+e\xi_{16}^4+f\xi_{16}^5+g\xi_{16}^6+h\xi_{16}^7 \in \mathbb{Q}(\xi_{16})$ *e* $m(x) = x^8+1$ *o polinômio minimal de* $\mathbb{Q}(\xi_{16})$. *O grupo de Galois de* $\mathbb{Q}(\xi_{16})$ *sobre* $\mathbb{Q}$ *é dado por* $Gal_{\mathbb{Q}}\mathbb{Q}(\xi_{16}) = \{1,\sigma,\tau,\sigma\tau,\delta,\eta,\sigma\delta,\sigma\eta\}$, *onde* $\sigma(\xi_{16}) = \xi_{16}^7$, $\tau(\xi_{16}) = \xi_{16}^9$, $\sigma\tau(\xi_{16}) = \xi_{16}^{15}$, $\delta(\xi_{16}) = \xi_{16}^3$, $\eta(\xi_{16}) = \xi_{16}^{13}$, $\sigma\delta(\xi_{16}) = \xi_{16}^5$ *e* $\sigma\eta(\xi_{16}) = \xi_{16}^{11}$.

Exemplo 5.3.2. *([9], p. 119) Seja* $p = 97 = 16.6+1$, *onde* $n = 16$. *Pela Tabela 5.4, o elemento irredutível* α *tal que* $N(\alpha) = p = 97$ *é* $\alpha = 1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3$. *O elemento*

$$\begin{aligned}\beta &= 5-[\frac{5}{1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3}](1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3)\\ &= 5-[\frac{5\sigma(\alpha)\tau(\alpha)\ldots\sigma\delta(\alpha)\sigma\eta(\alpha)}{(1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3)\sigma(\alpha)\tau(\alpha)\ldots\sigma\delta(\alpha)\sigma\eta(\alpha)}](1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3)\\ &= 1+\xi_{16}^3-\xi_{16}^5,\end{aligned}$$

em que $\sigma(\alpha) = 1+2\xi_{16}^7+\xi_{16}^{14}+\xi_{16}^5$, $\tau(\alpha) = 1+2\xi_{16}^9+\xi_{16}^2+\xi_{16}^{11}$, $\sigma\tau(\alpha) = 1+2\xi_{16}^{15}+\xi_{16}^{14}+\xi_{16}^{13}$, $\delta(\alpha) = 1+2\xi_{16}^3+\xi_{16}^6+\xi_{16}^9$, $\eta(\alpha) = 1+2\xi_{16}^{13}+\xi_{16}^{10}+\xi_{16}^7$, $\sigma\delta(\alpha) = 1+2\xi_{16}^5+\xi_{16}^{10}+\xi_{16}^{15}$ *e* $\sigma\eta(\alpha) = 1+2\xi_{16}^{11}+\xi_{16}^6+\xi_{16}$ *é um elemento primitivo do corpo* $\frac{\mathbb{Z}[\xi_{16}]}{\langle\alpha\rangle}$, *uma vez que* 5 *é um elemento primitivo do corpo* $GF(97)$.

Através de cálculo computacional, obtemos a a tabela de logaritmo de Zech's, onde $1+\beta^j = \beta^{z(j)}$ *e* $\beta^{-\infty} = 0$ *e a Tabela 5.4 que ilustra os elementos do corpo* $\frac{\mathbb{Z}[\xi_{16}]}{\langle\alpha\rangle}$. *Assim, temos um código* C *de comprimento* $l = \frac{97-1}{16} = 6$ *com matriz*

verificação de paridade dada por

$$H = \begin{pmatrix} 1 & \beta & \dots & \beta^5 \end{pmatrix}.$$

Considere o vetor informação $u = ((-1,0,1,0,-1,0,0,0),(1,0,-1,0,0,-1,0,0),$ $(0,0,0,0,0,-1,-1,-1),(-1,0,0,-1,0,1,0,0),(-1,-1,-1,0,0,0,0,0))$

$$G = \begin{pmatrix} -\beta & 1 & 0 & 0 & 0 & 0 \\ -\beta^2 & 0 & 1 & 0 & 0 & 0 \\ -\beta^3 & 0 & 0 & 1 & 0 & 0 \\ -\beta^4 & 0 & 0 & 0 & 1 & 0 \\ -\beta^5 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

a matriz geradora do código C *. Dessa forma,* $uG = ((0,0,-1,-1,-1,0,0,0),$ $(-1,0,1,0,-1,0,0,0),(1,0,-1,0,0,-1,0,0),(0,0,0,0,0,-1,0,-1),$ $(-1,0,0,-1,0,1,0,0),(-1,-1,-1,0,0,0,0,0))$. *Seja* $r = ((0,0,-1,-1,-1,0,0,0),$ $(-1,0,1,0,-1,0,0,0),(1,0,-1,0,0,-1,0,0),(0,0,0,0,0,-1,0,-1),$ $(-1,0,0,-1,0,1,0,0),(-1,-1,-1,0,0,0,0,0))$ *é o vetor recebido. Então, usando a Tabela 5.3 e cálculos computacionais, a síndrome é dada por* $S = Hr^T = \beta^{15} \neq 0$. *Logo, ocorreu um erro. Assim,* $L = 15 \equiv j \ (mod\ l) = (mod\ 6)$. *Como* $j = 3$*, segue que o erro ocorreu na quarta posição e a magnitude é dada por* $\beta^{15}\beta^{-3} = \beta^{12} = (0,0,0,0,0,0,1,0) = \xi_{16}^6$. *Portanto, a palavra transmitida foi* $c = r - e = ((0,0,-1,-1,-1,0,0,0),(-1,0,1,0,-1,0,0,0),(1,0,-1,0,0,-1,0,0),$ $(0,0,0,0,0,-1,1,-1),(-1,0,0,-1,0,1,0,0),(-1,-1,-1,0,0,0,0,0))$.

j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$	j	$z(j)$
1	8	13	9	25	65	37	55	49	20	61	51	73	90	85	39
2	59	14	62	26	94	38	83	50	28	62	36	74	60	86	42
3	13	15	84	27	32	39	4	51	66	63	93	75	12	87	37
4	58	16	91	28	29	40	89	52	87	64	80	76	2	88	23
5	24	17	73	29	72	41	88	53	21	65	71	77	76	89	78
6	44	18	3	30	41	42	25	54	79	66	11	78	81	90	38
7	85	19	95	31	6	43	64	55	47	67	43	79	56	91	19
8	31	20	22	32	16	44	35	56	49	68	1	80	75	92	54
9	46	21	33	33	30	45	15	57	61	69	5	81	69	93	10
10	52	22	82	34	70	46	74	58	45	70	68	82	48	94	57
11	50	23	17	35	86	47	67	59	18	71	40	83	92	95	7
12	26	24	77	36	63	48	$-\infty$	60	27	72	53	84	14	96	34

Tabela 5.3: Tabela de logaritmo de Zech's do corpo $\dfrac{\mathbb{Z}[\xi_{16}]}{\langle\alpha\rangle}$

L	β^L	L	β^L	L	β^L
1	$(1,0,0,1,0,-1,0,0)$	33	$(1,1,1,0,0,0,0,0)$	65	$(0,0,0,-1,0,1,0,-1)$
2	$(1,1,0,-1,-1,0,1,0)$	34	$(0,0,0,1,-1,1,0,0)$	66	$(0,-1,0,0,0,0,0,0)$
3	$(0,-1,-1,-1,0,0,0,0)$	35	$(-1,0,0,0,1,0,-1,0)$	67	$(0,0,0,1,0,1,0,1)$
4	$(0,0,0,0,-1,1,-1,0)$	36	$(0,0,1,0,0,0,0,0)$	68	$(1,0,1,-1,1,0,1,0)$
5	$(0,1,0,0,0,-1,0,1)$	37	$(1,0,0,0,-1,0,-1,0)$	69	$(0,0,1,1,1,0,0,0)$
6	$(0,0,0,-1,0,0,0,0)$	38	$(1,0,0,0,-1,-1,-1,-1)$	70	$(-1,0,0,1,0,-1,0,0)$
7	$(-1,0,0,-1,0,0,-1,0)$	39	$(0,0,0,1,1,1,0,0)$	71	$(1,0,-1,0,0,0,1,0)$
8	$(-1,-1,0,0,0,1,1,1)$	40	$(1,0,0,0,0,0,-1,1)$	72	$(0,0,0,0,1,0,0,0)$
9	$(0,0,0,0,1,1,1,0)$	41	$(0,-1,0,1,0,0,0,-1)$	73	$(1,0,1,0,0,0,-1,0)$
10	$(1,-1,0,0,0,0,0,1)$	42	$(0,0,0,0,0,-1,0,0)$	74	$(1,0,-1,0,1,1,0,-1)$
11	$(-1,0,1,0,-1,0,0,0)$	43	$(1,0,-1,0,0,-1,0,0)$	75	$(0,0,0,0,0,-1,-1,-1)$
12	$(0,0,0,0,0,0,1,0)$	44	$(-1,-1,-1,-1,0,0,0,1)$	76	$(-1,0,0,1,0,0,-1,0)$
13	$(0,-1,0,1,0,0,1,0)$	45	$(-1,0,0,0,0,0,1,1)$	77	$(0,1,0,-1,0,1,0,-)$
14	$(1,1,1,1,1,0,0,0)$	46	$(0,-1,1,-1,0,0,0,0)$	78	$(0,0,0,0,0,0,0,-1)$
15	$(1,1,0,0,0,0,0,-1)$	47	$(0,0,-1,0,1,0,-1,0)$	79	$(0,-1,0,-1,0,-1,0,0)$
16	$(1,0,-1,0,0,1,0,0)$	48	$(-1,0,0,0,0,0,0,0)$	80	$(-1,1,-1,0,-1,0,1,0)$
17	$(0,0,0,1,0,-1,0,1)$	49	$(-1,0,0,-1,0,1,0,0)$	81	$(-1,-1,-1,0,0,0,0,0)$
18	$(0,1,0,0,0,0,0,0)$	50	$(-1,-1,0,1,1,0,-1,0)$	82	$(0,0,0,-1,1,-1,0,0)$
19	$(0,0,0,-1,0,-1,0,-1)$	51	$(0,1,1,1,0,0,0,0)$	83	$(1,0,0,0,-1,0,1,0)$
20	$(-1,0,-1,1,-1,0,-1,0)$	52	$(0,0,0,0,1,-1,1,0)$	84	$(0,0,-1,0,0,0,0,0)$
21	$(0,0,-1,-1,-1,0,0,0)$	53	$(0,-1,0,0,0,1,0,-1)$	85	$(-1,0,0,0,1,0,1,0)$
22	$(1,0,0,-1,0,1,0,0)$	54	$(0,0,0,1,0,0,0,0)$	86	$(-1,0,0,0,1,1,1,1)$
23	$(-1,0,1,0,0,0,-1,0)$	55	$(1,0,0,1,0,0,1,0)$	87	$(0,0,0,-1,-1,-1,0,0)$
24	$(0,0,0,0,-1,0,0,0)$	56	$(1,1,0,0,0,-1,-1,-1)$	88	$(-1,0,0,0,0,0,1,-1)$
25	$(-1,0,-1,0,0,0,1,0)$	57	$(0,0,0,0,-1,-1,-1,0)$	89	$(0,1,0,-1,0,0,0,1)$
26	$(-1,0,1,0,-1,-1,0,1)$	58	$(-1,1,0,0,0,0,0,-1)$	90	$(0,0,0,0,0,1,0,0)$
27	$(0,0,0,0,0,1,1,1)$	59	$(1,0,-1,0,1,0,0,0)$	91	$(-1,0,1,0,0,1,0,0)$
28	$(1,0,0,-1,0,0,1,0)$	60	$(0,0,0,0,0,0,-1,0)$	92	$(1,1,1,1,0,0,0,-1)$
29	$(0,-1,0,1,0,-1,0,0)$	61	$(0,1,0,-1,0,0,-1,0)$	93	$(1,0,0,0,0,0,-1,-1)$
30	$(0,0,0,0,0,0,0,1)$	62	$(-1,-1,-1,-1,-1,0,0,0)$	94	$(0,1,-1,1,0,0,0,0)$
31	$(0,1,0,1,0,1,0,0)$	63	$(-1,-1,0,0,0,0,0,1)$	95	$(0,0,1,0,-1,0,1,0)$
32	$(1,-1,1,0,1,0,-1,0)$	64	$(-1,0,1,0,0,-1,0,0)$	96	$(1,0,0,0,0,0,0,0)$

Tabela 5.4: Tabela de elementos do corpo $\dfrac{\mathbb{Z}[\xi_{16}]}{\langle\alpha\rangle}$

Referências Bibliográficas

[1] HUBER, K., Codes over Gaussian integers, *IEEE Trans. Inform. Theory*, v. 40, p. 207 – 216, jan., 1994.

[2] HUBER, K., Codes over Eisenstein-Jacobi integers, *AMS, Contemp. Math.*, v. 158, p. 165 – 179, 1994.

[3] NÓBREGA NETO, T. P.; FARAVETO, O. M.; INTERLANDO, J. C.; PALAZZO Jr., R., Lattice Constellations and Codes from Quadratic Number Fields, *IEEE Trans. Inform. Theory*, v. 47, p. 1514 – 1527, may, 2001.

[4] INTERLANDO, J. C.; ELIA, M., On the Linear Labeling of Lattice Constellations from Algebraic Number Fields, *Combinatorics - 2000*, Gaeta, Italy, p. 1 – 9.

[5] CARVALHO, E. D., *Construção e Rotulamento de Constelação de Sinais Geometricamente Uniformes em Espaços Eucledianos e Hiperbólicos*, 113f, Tese de Doutorado, FECC-UNICAMP, Campinas-SP, 2001.

[6] CARVALHO, E. D.; PALAZZO Jr., R.; FIRER, M., Construção e Rotulagem de Constelações de Sinais Geometricamente Uniformes em R^n Casadas a Grupos, *Revista da Sociedade Brasileira de Telecomunicações*, v. 19, nº. 1, p. 13 – 20, abril, 2003.

[7] FAN, Y.; GAO, Y., Codes over Algebraic Integer Rings of Cyclotomic Fields, *Dept. of Math*, Wuhan university, to appear.

[8] DONG, X-d; SOH C. B.; GUNAWAN, E., Linear block codes for four-dimensional signals, *Finite Fields Appl.*, v. 5, 1999, p. 57 − 75.

[9] DONG, X-d; SOH C. B.; GUNAWAN, E., Codes over finite fields for multidimensional signals, *Journal of Algebra* 233, p. 105 − 121, 2000.

[10] SAMUEL, P., *Algebraic Theory of Numbers*, Herman, Paris, 1967, 109p.

[11] OLIVEIRA, C. M., *Discriminante, ramificação e diferente*, 131f, Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2005.

[12] STEWART, I.; TALL, D., *Algebraic Number Theory*, New York: Chapman-Hall, 1987, 189p.

[13] CARLOS, T. B., *Constelações e Códigos sobre Corpos Numéricos Quadráticos*, 113f, Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2003.

[14] CAZETTA, M. *Caracteres de Dirichlet e Aplicações*, 103f, Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 1998.

[15] LANG, S., *Algebra*, New York, Addison-Wesley, 1965, 508p.

[16] MAURCUS, D. A., *Number Fields*, New York: Springer-Verlag, 1977, 279p.

[17] WASHINGTON, L. C., *Introduction to Cyclotomic Fields*, New York: Board, 1982, 389p.

[18] LANG, S., *Algebraic Number Theory*, New York: Addison-Wesley Publishing Company, 1970, 354p.

[19] GONÇALVES, A. *Introdução à Algebra*, Rio de Janeiro-RJ, Instituto de Matemática Pura e Aplicada, 1979, 194p.

[20] ALVES, C., *Reticulados via Corpos Ciclotômicos*, 125f, Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2005.