

# Códigos lineares via corpos ciclotômicos\*

Antonio Aparecido de Andrade

Depto de Matemática, IBILCE, UNESP,

15054-000, São José do Rio Preto, SP

E-mail: andrade@ibilce.unesp.br

## 1 Introdução

Neste trabalho, veremos o conceito de corpos ciclotômicos enfocando suas principais propriedades. Consideramos os anéis de inteiros algébricos destes corpos que são domínios de ideais principais. Sendo o quociente desses anéis por um elemento irredutível um corpo finito, tomamos um elemento em cada classe lateral para representar cada elemento do corpo finito. Deste modo, construímos códigos sobre esses corpos com capacidade de corrigir um erro que pertence ao grupo cíclico do grupo multiplicativo do corpo finito. Neste sentido, construímos códigos lineares sobre esses corpos finitos para sinais com dimensão maior que 2.

Na Seção 2, apresentamos os conceitos de corpos ciclotômicos e suas principais propriedades. Na Seção 3, apresentamos a decomposição de ideais primos em corpos ciclotômicos. Na Seção 4, damos construções de códigos de bloco lineares sobre certos corpos obtidos via os anéis de inteiros de uma classe de corpos ciclotômicos.

## 2 Corpos ciclotômicos

Nesta Seção, apresentamos os corpos ciclotômicos. Esses corpos tem um papel fundamental na Teoria Algebrica dos Números, uma vez que é possível caracterizar o anel dos inteiros algébricos de um corpo ciclotômico, e conseqüentemente, seu discriminante.

**Definição 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  $\xi$  é uma raiz  $n$ -ésima primitiva da unidade se  $\xi^n = 1$  e  $\xi^m \neq 1$ , para todo  $0 < m < n$ .*

Se  $\xi_n$  é uma raiz  $n$ -ésima primitiva da unidade, então  $\xi_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ , onde  $n \in \mathbb{N}$ . Neste trabalho,  $\xi_n$  será sempre uma raiz  $n$ -ésima primitiva da unidade.

**Definição 2** *Um corpo ciclotômico é um corpo gerado por uma raiz  $n$ -ésima da unidade.*

**Definição 3** *O polinômio  $\phi_n(x) = \prod_{j=1}^n (x - \xi_n^j)$ , onde  $\text{mdc}(j, n) = 1$ , é chamado de  $n$ -ésimo polinômio ciclotômico.*

**Lema 1** *Se  $n$  é um inteiro positivo, então  $x^n - 1 = \prod_{h|n} \phi_h(x)$ .*

**Teorema 1** *Se  $\xi_n$  é uma raiz  $n$ -ésima primitiva da unidade, então  $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$ , onde  $\varphi$  é a função de Euler.*

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

**Teorema 3** *Se  $\text{mdc}(m, n) = 1$ , então  $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{mn})$ .*

**Teorema 4** *Se  $\mathbb{K}$  é um corpo de característica zero e  $\mathbb{L} = \mathbb{K}(\xi_n)$ , então  $\mathbb{L}$  é uma extensão Galoisiana de  $\mathbb{K}$  e o grupo de Galois de  $\mathbb{L}$  sobre  $\mathbb{K}$  é isomorfo a um subgrupo de  $(\mathbb{Z}_n)^*$ .*

**Definição 4** *Se  $\alpha \in \mathbb{Q}(\xi_n)$  definimos a norma de  $\alpha \in \mathbb{Q}(\xi_n)$  como  $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=1}^{\varphi(n)} \sigma_i(\alpha)$ , onde  $\varphi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$  e  $G$  é o grupo de Galois de  $\mathbb{Q}(\xi_n)$  sobre  $\mathbb{Q}$ .*

**Lema 2** *Se  $\alpha \in \mathbb{Q}(\xi_n)$ , então  $N(\alpha) \geq 0$ .*

**Lema 3** *Seja  $p$  um número primo ímpar. Se  $t$  e  $s$  são números inteiros tal que  $\text{mdc}(p^r, ts) = 1$ , então  $\frac{\xi_{p^r}^t - 1}{\xi_{p^r}^s - 1}$  é uma unidade em  $\mathbb{Z}[\xi_{p^r}]$ , onde  $\xi_{p^r}$  é uma raiz  $p^r$ -ésima primitiva da unidade.*

**Lema 4** *Seja  $\mathcal{O}_{\mathbb{K}}$  o anel de inteiros algébricos de  $\mathbb{K} = \mathbb{Q}(\xi_{p^r})$ , onde  $p$  é um número primo. Se  $r$  e  $i$  são números inteiros tal que  $\text{mdc}(p^r, i) = 1$ , então  $\langle 1 - \xi_{p^r} \rangle$  é um ideal primo de  $\mathcal{O}$  e  $\langle 1 - \xi_{p^r} \rangle^{p-1} = \langle p \rangle$ .*

**Observação 1** *Pelo Lema 4, temos que  $p$  se ramifica totalmente em  $\mathbb{Q}[\xi_{p^r}]$ .*

**Teorema 5** *O anel de inteiros de  $\mathbb{Q}(\xi_n)$  é  $\mathbb{Z}[\xi_n]$ .*

\*Este trabalho foi parcialmente financiado pela FAPESP - 02/07473-7

Se  $n \not\equiv 2 \pmod{4}$ , então  $\mathbb{Z}[\xi_n]$  é um domínio de ideais principais se, e somente se,  $n \in \{1\} \cup A$ , onde  $A = \{3, 2, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$ . Para os resultados a seguir, consideremos sempre  $n \in A$ .

**Lema 5** *Seja  $\mathbb{Q}(\xi_n)$  um corpo ciclotômico. Se  $p$  é um número primo tal que  $p$  não divide  $n$ , então  $p\mathbb{Z}[\xi_n]$  é um produto de ideais primos distintos  $\mathcal{P}_1 \dots \mathcal{P}_t$  em  $\mathbb{Z}[\xi_n]$ , onde  $t = \frac{[\mathbb{Q}(\xi_n) : \mathbb{Q}]}{s} = \frac{\varphi(n)}{s}$  e  $s$  é o menor inteiro positivo tal que  $p^s \equiv 1 \pmod{n}$ . Além disso,  $[\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}_j} : \frac{\mathbb{Z}}{(p)}] = s$ , para  $j = 1, \dots, t$ .*

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

**Corolário 2** *Seja  $\varphi(n)$  o menor inteiro positivo tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$ . Se  $p$  é um número primo da forma  $p = nk + 1$ , então  $p\mathbb{Z}[\xi_n]$  é um ideal primo em  $\mathbb{Z}[\xi_n]$ . Além disso,  $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$  é isomorfo ao corpo  $GF(p^{\varphi(n)})$ .*

**Lema 6** *Se  $\alpha$  é um elemento irreduzível tal que  $N(\alpha) = p$ , onde  $p$  é um número primo em  $\mathbb{Z}$ , então  $N(\sigma(\alpha)) = p$ , para cada  $\alpha \in \text{Gal}(\mathbb{Q}(\xi_n) : \mathbb{Q})$ .*

**Proposição 1** *Se  $\alpha, \beta \in \mathbb{Z}[\xi_n]$  são elementos irreduzíveis, então  $\langle \alpha\beta \rangle = \langle \alpha \rangle \langle \beta \rangle$ .*

**Teorema 6** *Sejam  $\alpha \in \mathbb{Z}[\xi_n]$  e  $N(\alpha) = p$ . Se  $p$  é um número primo tal que  $p$  não divide  $n$ , então  $\alpha$  é um elemento irreduzível em  $\mathbb{Z}[\xi_n]$  e  $p = nk + 1$ . Além disso,  $\frac{\mathbb{Z}[\xi_n]}{\langle \alpha \rangle}$  é um corpo com  $p$  elementos.*

**Proposição 2** *Seja  $(G, \cdot)$  um grupo cíclico multiplicativo de um corpo ciclotômico  $\mathbb{Q}[\xi_n]$  com  $p^m - 1$  elementos, onde  $p = nk + 1$  é um número primo em  $\mathbb{Z}$ ,  $k \in \mathbb{Z}$  e  $m \in \mathbb{N}$ . Se  $n$  é ímpar, então existe um único subgrupo cíclico com  $2n$  elementos.*

**Proposição 3** *Seja  $(G, \cdot)$  um grupo cíclico multiplicativo de um corpo ciclotômico  $\mathbb{Q}[\xi_n]$  com  $p^m - 1$  elementos, onde  $p = nk + 1$  é um número primo em  $\mathbb{Z}$ ,  $k \in \mathbb{Z}$  e  $m \in \mathbb{N}$ . Se  $n$  é par, então existe um único subgrupo cíclico com  $n$  elementos.*

**Teorema 7** *Sejam  $\alpha$  um elemento irreduzível em  $\mathbb{Z}[\xi_n]$  tal que  $N(\alpha) = p = nk + 1$ , onde  $p$  é um número primo ímpar.*

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

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

**Lema 7** *Sejam  $n$  um número ímpar e  $p$  um número primo ímpar. Se  $\xi_n^j$  é uma raiz  $1 < d = \frac{n}{\text{mdc}(n, j)}$ -ésima primitiva da unidade tal que*

$$\begin{cases} N(1 + \xi_n^j) = pN(\beta) & \text{se } 1 \leq j \leq n \\ N(1 - \xi_n^j) = pN(\beta) & \text{se } 1 \leq j < n, \end{cases}$$

então nem  $N(1 + \xi_n^j)$  e nem  $N(1 - \xi_n^j)$  são divisores de  $p$ .

**Proposição 4** *Se  $\alpha$  é um elemento irreduzível tal que  $N(\alpha) = p = nk + 1$ , onde  $p$  é um número primo ímpar e  $n$  é um número ímpar, então qualquer dois elementos distintos estão em classes laterais distintas módulo o ideal  $\langle \alpha \rangle$ .*

**Teorema 8** *Se  $\alpha$  é um elemento irreduzível em  $\mathbb{Z}[\xi_n]$  tal que  $N(\alpha) = p = nk + 1$  e  $n$  ímpar, então podemos tomar o conjunto  $\{\pm 1, \pm \xi_n, \dots, \pm \xi_n^{n-1}\}$  como sendo um conjunto completo do subgrupo cíclico com  $2n$  elementos do grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{\langle \alpha \rangle}$ .*

**Lema 8** *Sejam  $n$  um número par e  $p$  um número primo ímpar. Se  $\xi_n^j$  é uma raiz  $d = 2^k$ -ésima primitiva da unidade para  $k \geq 2$  tal que*

$$\begin{cases} N(1 - \xi_n^j) = pN(\beta) & \text{se } 1 \leq j \leq \frac{n}{2} \\ N(1 + \xi_n^j) = pN(\beta) & \text{se } 1 \leq j < \frac{n}{2}, \end{cases}$$

então nem  $N(1 + \xi_n^j)$  e nem  $N(1 - \xi_n^j)$  são divisores de  $p$ .

**Lema 9** *Sejam  $n$  um número par e  $p$  um número primo ímpar. Se  $\xi_n^j$  é uma raiz  $d = 2^k m$ -ésima primitiva da unidade, onde  $k \geq 1$  e  $\text{mdc}(2, m) = 1$  tal que*

$$\begin{cases} N(1 - \xi_n^j) = pN(\beta) & \text{se } 1 \leq j \leq \frac{n}{2} \\ N(1 + \xi_n^j) = pN(\beta) & \text{se } 1 \leq j < \frac{n}{2}, \end{cases}$$

então nem  $N(1 + \xi_n^j)$  e nem  $N(1 - \xi_n^j)$  são divisores de  $p$ .

**Lema 10** *Sejam  $n$  um número par e  $p$  um número primo ímpar e  $\xi_n^j$  a raiz  $d$ -ésima primitiva da unidade, onde  $d$  é um número ímpar tal que*

$$\begin{cases} N(1 - \xi_n^j) = pN(\beta) & \text{se } 1 \leq j \leq \frac{n}{2} \\ N(1 + \xi_n^j) = pN(\beta) & \text{se } 1 \leq j < \frac{n}{2}, \end{cases}$$

então nem  $N(1 + \xi_n^j)$  e nem  $N(1 - \xi_n^j)$  são divisores de  $p$ .

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

1. *Se  $n$  é ímpar, então o grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$  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.*

**Lema 11** *Sejam  $\varphi(n)$  o menor inteiro tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$ ,  $p$  número primo ímpar e  $n$  um número ímpar. Se  $\xi_n^j$  é uma raiz  $n$ -ésima primitiva da unidade, então*

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

para  $1 \leq j < 2n$ .

**Lema 12** *Sejam  $\varphi(n)$  o menor inteiro tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$ ,  $p$  número primo ímpar e  $n$  um número ímpar. Se  $\xi_n^j$  é uma raiz  $n$ -ésima primitiva da unidade, então*

$$N(1 + \xi_n^j) = 2^{\varphi(n)} \cos^2\left(\frac{\pi j j_1}{n}\right) \dots \cos^2\left(\frac{\pi j j_{\varphi(n)}}{n}\right),$$

para  $1 \leq j < 2n$ .

**Proposição 5** *Se  $\varphi(n)$  é o menor inteiro tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$ , onde  $p$  é um número primo ímpar e  $n$  é um número ímpar, então quaisquer dois elementos distintos estão em classes laterais distintas módulo o ideal  $\langle p \rangle$  em  $\mathbb{Z}[\xi_n]$ .*

**Teorema 10** *Sejam  $\varphi(n)$  o menor inteiro tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$  e  $p$  um primo ímpar. Se  $n$  é ímpar, então podemos tomar o conjunto  $\{\pm 1, \pm \xi_n, \dots, \pm \xi_n^{n-1}\}$  como sendo um conjunto completo do subgrupo cíclico com  $2n$  elementos do grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ .*

**Observação 2** *Se  $n$  for par, os Lemas 11, 12 e a Proposição 5 também são válidas, com a ressalva que  $j$  varia de 1 a  $n$ , para  $N(1 \pm \xi_n^j)$ , onde  $\xi_n^j$  é uma raiz  $n$ -ésima primitiva da unidade.*

**Teorema 11** *Sejam  $\varphi(n)$  o menor inteiro tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$  e  $p$  um primo ímpar. Se  $n$  é par, então podemos tomar o conjunto  $\{1, \xi_n, \dots, \xi_n^{n-1}\}$  como sendo um conjunto completo do subgrupo cíclico com  $n$  elementos do grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ .*

**Teorema 12** *Se  $\varphi(n)$  é o menor inteiro tal que  $2^{\varphi(n)} \equiv 1 \pmod{n}$ , então o grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$  contém um único subgrupo*

*cíclico com  $n$  elementos. Além disso, o conjunto  $\{1, \xi_n, \dots, \xi_n^{n-1}\}$  é um conjunto completo do subgrupo cíclico do grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ .*

### 3 Decomposição em corpos ciclotômicos

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

**Teorema 13** *(Lema de Kummer) Seja  $A$  um anel de Dedekind com corpo quociente  $\mathbb{K}$ . Seja  $\mathbb{L}$  uma extensão finita separável de  $\mathbb{K}$ . Seja  $\mathcal{O}_{\mathbb{L}}$  o fecho integral de  $A$  em  $\mathbb{L}$  e assumamos que  $\mathcal{O}_{\mathbb{L}} = A[\alpha]$  para algum elemento  $\alpha$ . Sejam  $m(x)$  o polinômio irredutível de  $\alpha$  sobre  $\mathbb{K}$  e  $\mathcal{P}$  um ideal primo de  $A$ . Se  $\bar{m}(x)$  é a redução de  $m(x)$  e se  $\bar{m}(x) = \bar{\mu}_1(x)^{e_1} \dots \bar{\mu}_r(x)^{e_r}$  é a fatoração de  $\bar{m}(x)$  em potências de fatores irredutíveis sobre  $\bar{A} = \frac{A}{\mathcal{P}}$ , com coeficiente dominante 1, então*

$$\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{B}_1^{e_1} \dots \mathcal{B}_r^{e_r}$$

*é a fatoração de  $\mathcal{P}$  em  $\mathcal{O}_{\mathbb{L}}$ , de modo que  $e_i$  é o índice de ramificação de  $\mathcal{B}_i$  sobre  $\mathcal{P}$  e que*

$$\mathcal{B}_i = \mathcal{P}\mathcal{O}_{\mathbb{L}} + \mu_i(\alpha)\mathcal{O}_{\mathbb{L}},$$

*onde  $\mu_i(x) \in A[x]$  é um polinômio com coeficiente dominante 1 cuja redução módulo  $\mathcal{P}$  é  $\bar{\mu}_i(x)$ .*

**Teorema 14** *Se  $\mathbb{K}$  é um corpo de números, então um ideal primo  $p\mathbb{Z}$  de  $\mathbb{Z}$  se ramifica em  $\mathbb{K}$  se, e somente se,  $p$  divide  $D_{\mathbb{K}}$ .*

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

**Lema 13** *Sejam  $m = \varphi(n)$ ,  $p$  um número primo e  $\mathcal{O}_n(p)$  ordem de  $p$  módulo  $n$ . Se  $p$  não divide  $n$ , então  $p\mathbb{Z}[\xi_n]$  se decompõe em  $\frac{m}{\mathcal{O}_n(p)}$  ideais primos distintos de  $\mathbb{Z}[\xi_n]$ .*

**Exemplo 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  $\xi_{15}$  sobre  $\mathbb{Q}$ . Vamos obter a fatoração de  $3\mathcal{O}_{\mathbb{K}}$ . Como  $m(x) \equiv (x^4 + x^3 + x^2 + x + 1)^2 \pmod{\mathbb{Z}_3[x]}$ , temos que  $g = 1$ ,  $\bar{\mu}_1(x) = x^4 + x^3 + x^2 + x + 1$ ,  $e_1 = 2$  e  $f_1 = \text{gr}(\bar{\mu}_1(x)) = 4$ . Assim, segue que  $\mathcal{P}_1 = 3\mathcal{O}_{\mathbb{K}} + (\xi_{15}^4 + \xi_{15}^3 + \xi_{15}^2 + \xi_{15} + 1)\mathcal{O}_{\mathbb{K}}$ . Portanto,  $3\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^2$  é o único ideal primo de  $\mathcal{O}_{\mathbb{K}}$  acima de  $3\mathbb{Z}$  com norma  $3^4$ . Note que neste caso,  $3\mathbb{Z}$  se ramifica em  $\mathbb{K}$ , mas não é totalmente ramificado em  $\mathbb{K}$ .*

Pelo Lema 13 e considerando  $\frac{m}{\mathcal{O}_n(p)} > 1$ , temos que a menor decomposição possível do ideal  $p\mathbb{Z}[\xi_n]$

em produto de ideais primos distintos de  $\mathbb{Z}[\xi_n]$  ocorre primeiramente em  $n = 3$  e  $p \equiv 1 \pmod{3}$ , pois  $p\mathbb{Z}[\xi_3]$  se decompõem em dois ideais primos distintos de  $\mathbb{Z}[\xi_3]$ . Por exemplo, pelo Lema de Kummer, a fatoração do ideal  $13\mathbb{Z}[\xi_3]$ , como  $13 \equiv 1 \pmod{3}$  e o polinômio minimal de  $\xi_3$  sobre  $\mathbb{Q}$  é  $x^2 + x + 1$ , temos que  $x^2 + x + 1 \equiv (x + 4)(x + 10) \pmod{13\mathbb{Z}[x]}$ ,  $g = 2$ ,  $\bar{\mu}_1(x) = x + 4$ ,  $\bar{\mu}_2(x) = x + 10$ ,  $e_1 = e_2 = f_1 = f_2 = 1$ . Assim,  $13\mathbb{Z}[\xi_3] = \mathcal{P}_1\mathcal{P}_2$ , onde  $\mathcal{P}_1 = 13\mathbb{Z}[\xi_3] + (\xi_3 + 4)\mathbb{Z}[\xi_3]$  e  $\mathcal{P}_2 = 13\mathbb{Z}[\xi_3] + (\xi_3 + 10)\mathbb{Z}[\xi_3]$ .

Agora, sejam  $\mathbb{K} \subseteq \mathbb{L}$  corpos de números com  $\mathbb{L}$  uma extensão galoisiana de  $\mathbb{K}$  de grau  $n$ . Veremos que em uma extensão galoisiana a decomposição de um ideal em  $\mathcal{O}_{\mathbb{L}}$ , dado como no Lema de Kummer, assume certas características particulares. Seja  $\mathcal{G}$  o grupo de Galois de  $\mathbb{L}$  sobre  $\mathbb{K}$ . Se  $\mathcal{G}$  for um grupo abeliano diremos que  $\mathbb{L}$  é uma extensão abeliana de  $\mathbb{K}$ . Decorre do Teorema 4, que toda extensão ciclotômica de  $\mathbb{K}$  é abeliana, e em particular, todo subcorpo de um corpo ciclotômico é uma extensão abeliana de  $\mathbb{Q}$ . Reciprocamente, se  $\mathbb{K}$  é uma extensão abeliana de  $\mathbb{Q}$ , então existe um inteiro  $n$  tal que  $\mathbb{K} \subset \mathbb{Q}(\xi_n)$ . Este resultado é conhecido como Teorema de Kronecker-Weber.

Sejam  $\mathcal{O}_{\mathbb{K}}$  e  $\mathcal{O}_{\mathbb{L}}$  os anéis de inteiros de  $\mathbb{K}$  e  $\mathbb{L}$ , respectivamente. Se  $\alpha \in \mathcal{O}_{\mathbb{L}}$ , então aplicando  $\sigma \in \mathcal{G}$  na equação de dependência inteira de  $\alpha$  sobre  $\mathcal{O}_{\mathbb{K}}$  temos que  $\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$ , isto é,  $\sigma(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{L}}$ , para todo  $\sigma \in \mathcal{G}$ , onde  $\mathcal{G}$  é o grupo de Galois de  $\mathbb{L}$  sobre  $\mathbb{K}$ . Por outro lado, se  $\mathcal{P}$  é um ideal primo de  $\mathcal{O}_{\mathbb{K}}$  e  $\mathcal{Q}$  é um ideal primo de  $\mathcal{O}_{\mathbb{L}}$  tal que  $\mathcal{Q}$  contém  $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ . Assim,  $\mathcal{Q} \cap \mathcal{O}_{\mathbb{K}} = \mathcal{P}$ , então  $\sigma(\mathcal{Q}) \cap \mathcal{O}_{\mathbb{K}} = \mathcal{P}$ , para todo  $\sigma \in \mathcal{G}$ , ou seja,  $\sigma(\mathcal{Q})$  contém  $\mathcal{P}\mathcal{O}_{\mathbb{L}}$  e tem o mesmo expoente de  $\mathcal{Q}$ . Neste caso, dizemos  $\mathcal{Q}$  e  $\mathcal{Q}' = \sigma(\mathcal{Q})$  são ideais primos conjugados contidos em  $\mathcal{O}_{\mathbb{L}}$ .

**Proposição 6** *Se  $\mathcal{P}$  é um ideal primo em  $\mathcal{O}_{\mathbb{K}}$ , então os ideais primos  $\mathcal{P}_i$  de  $\mathcal{O}_{\mathbb{L}}$  acima de  $\mathcal{P}$  são dois a dois conjugados, têm o mesmo grau residual  $f$  e o mesmo índice de ramificação  $e$ . Portanto,*

$$\mathcal{P}\mathcal{O}_{\mathbb{L}} = \left( \prod_{i=1}^g \mathcal{P}_i \right)^e \quad e \quad n = efg.$$

Seja  $\mathbb{F} = \mathbb{F}_{p^h}$  um corpo finito de ordem  $p^h$ , onde  $p$  é um número primo. O conjunto  $\mathbb{F}^*$  das unidades de  $\mathbb{F}$  é um grupo cíclico de ordem  $p^h - 1$  e para cada  $m \mid p^h - 1$  existe  $\varphi(m)$  raízes  $m$ -ésima primitiva da unidade em  $\mathbb{F}^*$ . Além disso, temos que  $p^j - 1$  divide  $p^k - 1$  se, e somente se,  $j$  divide  $k$ .

**Definição 5** *Dizemos que a ordem de  $p$  módulo  $m$  é  $h$  se  $p^h \equiv 1 \pmod{m}$  e  $p^j \not\equiv 1 \pmod{m}$  para todo  $j = 1, 2, \dots, h - 1$ .*

**Lema 14** *Uma raiz  $m$ -ésima primitiva da unidade  $\xi_m$  gera  $\mathbb{F}$  se, e somente se, a ordem de  $p$  módulo  $m$  é  $h$ .*

Segue do Lema 14 que se  $\xi_m$  é uma raiz  $m$ -ésima primitiva da unidade, então  $\mathbb{F} = \mathbb{Z}(\xi_m)$ . Agora, se  $\xi_n$  é uma raiz  $n$ -ésima primitiva da unidade, onde  $n = p^e m$ ,  $e \geq 0$ , então  $\mathbb{Z}[\xi_n] = \left\{ \sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i, a_i \in \mathbb{Z} \right\}$ , e portanto, os elementos  $\sum_{i=0}^{\varphi(n)-1} a_i \xi_n^i$  estão em bijeção com as sequências de elementos inteiros  $(a_0, a_1, \dots, a_{\varphi(n)-1})$ .

Além disso, temos, pela Proposição 6, que o ideal  $p\mathbb{Z}[\xi_n] = (\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r)^{\varphi(p^e)}$ , onde  $\mathcal{P}_1, \dots, \mathcal{P}_r$  são ideais primos distintos de  $\mathbb{Z}[\xi_n]$  tais que  $\mathcal{P}_i \cap \mathbb{Z} = \langle p \rangle$ ,  $\varphi(m) = hr$  e  $\frac{\mathbb{Z}[\xi_n]}{\mathcal{P}_i} \simeq \mathbb{Z}_p[\xi_m] = \mathbb{F}$ , para todo  $i = 1, \dots, r$ , onde o isomorfismo aplica  $\xi_n$  em  $\xi_m = \xi_m$ . Assim, cada elemento de  $\mathbb{F}$  é escrito como  $\bar{a} = a + \mathcal{P}_i$  onde  $a \in \mathbb{Z}[\xi_n]$ .

Se  $n = 4$  temos que  $\mathbb{Z}[\xi_4]$  é o anel dos inteiros Gaussianos  $\mathbb{Z}[i]$ . Logo,  $p \equiv 1 \pmod{4}$ . Note que, o ideal primo  $\mathcal{P}$  tal que  $\frac{\mathbb{Z}[i]}{\mathcal{P}} \simeq \mathbb{Z}_p$  é o ideal principal gerado por  $a + bi$  com  $a^2 + b^2 = p$ .

## 4 Códigos e decodificação via corpos ciclotômicos

Nesta Seção, veremos o conceito de códigos via os corpos ciclotômicos e introduzimos alguns resultados que serão necessários para a construção do algoritmo de decodificação desses códigos.

**Teorema 15** *Seja  $\alpha$  um elemento irredutível em  $\mathbb{Z}[\xi_n]$  tal que  $N(\alpha) = p = nk + 1$ . Se  $p$  é um número primo, então  $T_p = \{0, 1, \dots, p - 1\}$  é isomorfo ao corpo  $\frac{\mathbb{Z}}{\langle \alpha \rangle}$ .*

**Teorema 16** *Seja  $\varphi(n)$  o menor inteiro positivo tal que  $p^{\varphi(n)} \equiv 1 \pmod{n}$ . Se  $p$  é um número primo ímpar, então  $T_{p^{\varphi(n)}} = \{a_0 + a_1\xi_n + \dots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : |a_j| \leq \frac{p-1}{2}, j = 0, 1, \dots, \varphi(n)-1\}$  é um conjunto completo das classes laterais do corpo  $\frac{\mathbb{Z}[\xi_n]}{p\mathbb{Z}[\xi_n]}$ .*

**Teorema 17** *Seja  $\varphi(n)$  o menor inteiro positivo tal que  $2^{\varphi(n)} \equiv 1 \pmod{n}$ . Se  $p$  é um número primo ímpar, então  $T_{2^{\varphi(n)}} = \{a_0 + a_1\xi_n + \dots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : 0 \leq |a_j| \leq 1, j = 0, 1, \dots, \varphi(n)-1\}$  é um conjunto completo das classes laterais do corpo  $\frac{\mathbb{Z}[\xi_n]}{2\mathbb{Z}[\xi_n]}$ .*

**Proposição 7** *Sejam  $w(-)$  uma função peso consecutiva num corpo finito  $\mathbb{F} = \mathbb{Z}(\xi_m)$  e  $d(-, -)$  a distância em  $\mathbb{F}^l$  induzida pela função peso. Se  $C \subset \mathbb{F}^l$  é um código com distância mínima  $d_w > 0$ , então  $C$  é um código corretor de  $t$   $w$ -erros, mas não um código corretor de  $(t + 1)$   $w$ -erros.*

**Corolário 3** Se a distância mínima de Mannheim de um código  $C$  sobre  $\mathbb{F} = \mathbb{Z}_p[\xi_m]$  é  $d_{\bar{w}}$ , então a capacidade de correção de erros de Mannheim do código  $C$  é  $\lfloor \frac{d_{\bar{w}}-1}{2} \rfloor$ .

**Proposição 8** Sejam  $\alpha$  um gerador do grupo multiplicativo  $\mathbb{F}^*$  e  $p^h - 1 = lk$ . Se  $C$  é um código linear com matriz controle de paridade dada por

$$H = ( 1 \quad \alpha \quad \dots \quad \alpha^{l-1} ),$$

então  $C$  pode corrigir um erro que pertence a  $\{1, \alpha^l, \alpha^{2l}, \dots, \alpha^{(k-1)l}\}$ .

**Observação 3** Se tomarmos  $n = m = 4$  e  $p \equiv 1 \pmod{4}$ , então obtemos um código linear sobre o anel de inteiros Gaussianos, que corrige um erro de Mannheim. Este resultado é o mesmo que foi obtido por Hubber, mesmo que os conceitos do peso de Mannheim sejam definidos de forma diferente.

Agora, consideremos os seguintes conjuntos  $A = \{3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$ , e

$$A_n = \begin{cases} \{1, \xi_n, \dots, \xi_n^{n-1}\} & \text{se } n \text{ par} \\ \{\pm 1, \pm \xi_n, \dots, \pm \xi_n^{n-1}\} & \text{se } n \text{ ímpar.} \end{cases}$$

Sejam  $\alpha$  um elemento irredutível em  $\mathbb{Z}[\xi_n]$  tal que  $N(\alpha) = p^h$ , onde  $p$  não divide  $n$ ,  $n \in A$  e  $h = 1$  ou  $h = \varphi(n)$ . Seja o conjunto  $T_{p^h}$  como nos Teoremas 15, 16 e 17. Fazendo analogia deste conjunto como sendo o grupo multiplicativo do corpo  $\frac{\mathbb{Z}[\xi_n]}{\langle \alpha \rangle}$ , por esses Teoremas, segue que existe um único subconjunto  $S_n \subset T_{p^h}$  tal que cada elemento em  $S_n$  está na mesma classe lateral de algum elemento do conjunto  $A_n$  módulo o ideal  $\langle \alpha \rangle$ . Assim, obtemos a seguinte definição:

**Definição 6** O conjunto completo da classe lateral do corpo  $\frac{\mathbb{Z}[\xi_n]}{\langle \alpha \rangle}$ , é definido como

$$R_{p^h}^n = \{a - [\frac{a}{\alpha}]\alpha : a \in T_{p^h} - S_n\} \cup A_n,$$

onde  $[\frac{a}{\alpha}] \in \mathbb{Z}[\xi_n]$ ,  $S_n$ ,  $A_n$  e  $T_{p^h}$  são definidos como anteriormente.

**Definição 7** Um código linear  $C$  de comprimento

$$l = \begin{cases} \frac{p^h-1}{n} & \text{se } p \text{ é primo ímpar e } n \text{ par} \\ \frac{p^h-1}{2n} & \text{se } p \text{ é primo ímpar e } n \text{ ímpar} \\ \frac{2^{\varphi(n)}-1}{n} & \text{se } p = 2 \text{ e } h = \varphi(n), \end{cases}$$

sobre  $R_{p^h}^n$  e  $R_{2^{\varphi(n)}}^n$ , respectivamente, para os primos ímpares e para  $p = 2$ , é definido como sendo o conjunto das palavras-códigos  $(\alpha_0, \alpha_1, \dots, \alpha_{l-1})$ , onde os  $\alpha_i \in R_{p^h}^n$  ou  $R_{2^{\varphi(n)}}^n$  são tais que

$$\alpha_0 + \alpha_1\beta + \dots + \alpha_{l-1}\beta^{l-1} = 0,$$

sendo  $\beta$  um elemento primitivo do corpo  $\frac{\mathbb{Z}[\xi_n]}{\langle \alpha \rangle}$ .

**Observação 4** A matriz controle de paridade  $H$  do código  $C$  é dada por

$$H = ( 1 \quad \beta \quad \dots \quad \beta^{l-1} )$$

e a matriz geradora do código  $C$  é dada por

$$G = \begin{pmatrix} -\beta & 1 & \dots & 0 \\ -\beta^2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\beta^{l-1} & 0 & \dots & 1 \end{pmatrix}.$$

**Teorema 18** Se  $p$  é um número primo e se  $n$  é um número par, então o código linear  $C$  de comprimento  $l = \frac{p^h-1}{n}$  sobre  $R_{p^h}^n$  é capaz de corrigir um erro com valores em  $\{1, \xi_n, \dots, \xi_n^{n-1}\}$ .

**Teorema 19** Se  $p$  é um número primo ímpar e se  $n$  é um número ímpar, então o código linear  $C$  de comprimento  $l = \frac{p^h-1}{n}$  sobre  $R_{p^h}^n$  é capaz de corrigir um erro com valores em  $\{\pm 1, \pm \xi_n, \dots, \pm \xi_n^{n-1}\}$ .

**Teorema 20** O código linear  $C$  de comprimento  $l = \frac{2^{\varphi(n)}-1}{n}$  sobre  $R_{2^{\varphi(n)}}^n$  é capaz de corrigir um erro com valores em  $\{1, \xi_n, \dots, \xi_n^{n-1}\}$ .

Para um código linear  $C$  de comprimento  $l = \frac{p^h-1}{n}$  sobre  $R_{p^h}^n$  ou de comprimento  $l = \frac{2^{\varphi(n)}-1}{n}$  sobre  $R_{2^{\varphi(n)}}^n$ , temos que o algoritmo de decodificação é dado por:

1. Calcule a síndrome  $S = Hr^t$ .
2. A localização e a magnitude do erro são dadas, respectivamente, por  $L = \log_{\beta}(S) \equiv j \pmod{l}$  e  $u = S\beta^{-j}$ , para  $0 \leq j \leq l-1$ .
3. A palavra transmitida é dado por  $c = r - e$ , onde  $r$  é a palavra recebida e  $e$  é o erro transmitido.

**Exemplo 2** Seja  $p = 97 = 16 \times 6 + 1$ , onde  $n = 16$ . O elemento irredutível  $\alpha$  tal que  $N(\alpha) = p = 97$  é  $\alpha = 1 + 2\xi_{16} + \xi_{16}^2 + \xi_{16}^3$ . Como  $p$  é primo ímpar e  $n$  é par, segue que  $A_{16} = \{1, \xi_{16}, \dots, \xi_{16}^5\}$ . Logo, o código linear  $C$  tem comprimento  $l = \frac{p^h-1}{n} = \frac{97-1}{16} = 6$ , sendo  $h = 1$  sobre  $R_{97}^{16}$ . Temos que  $\beta = 5 - [\frac{5}{1+2\xi_{16}+\xi_{16}^2+\xi_{16}^3}](1 + 2\xi_{16} + \xi_{16}^2 + \xi_{16}^3) = 1 + \xi_{16}^3 - \xi_{16}^5$  é um elemento primitivo do corpo  $\frac{\mathbb{Z}[\xi_{16}]}{\langle 1 + 2\xi_{16} + \xi_{16}^2 + \xi_{16}^3 \rangle}$ , onde 5 é um elemento primitivo do corpo  $\frac{\mathbb{Z}}{\langle 97 \rangle}$ . Logo, o conjunto  $R_{97}^{16}$  consiste

de todos os elementos  $a_0 + a_1\xi_{16} + \dots + a_7\xi_{16}^7$  com  $a_i \in \mathbb{Z}$ , para  $i = 0, 1, \dots, 7$ , expressados na forma vetorial. Assim,  $\beta = 1 + \xi_{16}^3 - \xi_{16}^5$ , pode ser escrito como  $\beta = (1, 0, 0, 1, 0, -1, 0)$ . A matriz verificação de paridade  $H$  e a matriz geradora  $G$ , são dadas,

respectivamente, por

$$H = \begin{pmatrix} 1 & \beta & \dots & \beta^5 \end{pmatrix}$$

$$G = \begin{pmatrix} -\beta & 1 & \dots & 0 \\ -\beta^2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\beta^{l-1} & 0 & \dots & 1 \end{pmatrix}.$$

**Exemplo 3** Pelo Exemplo 2, para transmitir sinais de dimensão 8, consideremos

$$\alpha_1 = (-1, 0, 1, 0, -1, 0, 0, 0) = -1 + \xi_{16}^2 - \xi_{16}^4 = \beta^{11}$$

$$\alpha_2 = (1, 0, -1, 0, 0, -1, 0, 0) = 1 - \xi_{16}^2 - \xi_{16}^5 = \beta^{43}$$

$$\alpha_3 = (0, 0, 0, 0, 0, -1, -1, -1) = -\xi_{16}^5 - \xi_{16}^6 - \xi_{16}^7 = \beta^{75}$$

$$\alpha_4 = (-1, 0, 0, -1, 0, 1, 0, 0) = -1 - \xi_{16}^3 + \xi_{16}^5 = \beta^{49}$$

$$\alpha_5 = (-1, -1, -1, 0, 0, 0, 0, 0) = -1 - \xi_{16} - \xi_{16}^2 = \beta^{81}.$$

Assim,  $\alpha_0 + \alpha_1\beta + \alpha_2\beta^2 + \alpha_3\beta^3 + \alpha_4\beta^4 + \alpha_5\beta^5 = 0$ , e portanto

$$\alpha_0 = -\alpha_1\beta - \alpha_2\beta^2 - \alpha_3\beta^3 - \alpha_4\beta^4 - \alpha_5\beta^5 = -\beta^{11}\beta - \beta^{43}\beta^2 - \beta^{75}\beta^3 - \beta^{49}\beta^4 - \beta^{81}\beta^5 = -\beta^{12} - \beta^{45} - \beta^{78} - \beta^{53} - \beta^{86} = \beta^{21}.$$

**Exemplo 4** Considerando o mesmo elemento primitivo do Exemplo 2, suponhamos que ocorra um erro dado por  $e = \beta^{12} = (0, 0, 0, 0, 0, 0, 1, 0) = \xi_{16}^6$ . Seja o vetor recebido dado por  $r = ((0, 0, -1, -1, -1, 0, 0, 0), (-1, 0, 1, 0, -1, 0, 0, 0), (1, 0, -1, 0, 0, -1, 0, 0), (0, 0, 0, 0, 0, -1, 0, -1), (-1, 0, 0, -1, 0, 1, 0, 0), (-1, -1, -1, 0, 0, 0, 0, 0)) = (\beta^{21}, \beta^{11}, \beta^{43}, ?, \beta^{49}, \beta^{81})$ . Aplicando o algoritmo de decodificação, temos que:

1. A síndrome é dada por  $s = Hr^T = \beta^{15}$ .

2. A localização e a magnitude do erro são dadas, respectivamente, por  $L = 15 \equiv j \pmod{l}$ , onde  $l = 6$ , assim,  $j = 3$  e  $u = \beta^L\beta^{-j} = \beta^{15}\beta^{-3} = \beta^{12} = (0, 0, 0, 0, 0, 0, 1, 0) = \xi_{16}^6$ .

## Referências

- [1] X-dong Dong, C.B. Soh and E. Gunawan, *Codes over finite fields for multidimensional signals*, Journal of Algebra, Vol. 233, pp. 105-121, 2000.
- [2] Y. Fan; Y. Gao, “Codes over Algebraic Integer Rings of Cyclotomic Fields,” *Dept. of Mathl, Wuhan University*, to appear.
- [3] K. Huber, “Codes over Eisenstein-Jacobi integers”, *AMS, Contemp. Math.*, Vol. 158, pp. 165 – 179, 1994.
- [4] K. Huber, “Codes over Gaussian integers”, *IEEE Trans. Inform. Theory*, Vol. 40, pp. 207 – 216, Jan. 1994.
- [5] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Company, New York, 1970.
- [6] T. P. Nóbrega Neto; O. M. Favareto; J. C. Interlando; R. Palazzo Jr, “Lattice Constellations and Codes from Quadratic Number Fields”, *IEEE Trans. Inform. Theory*, Vol. 47, pp. 1514 – 1527, May 2001.
- [7] P. Samuel, *Algebraic Theory of Numbers*, Herman, Paris, 1967.
- [8] L. C. Washington, *Introduction to Cyclotomic Fields*, GTM vol. 83, Springer-Verlag, New York, 1982.